WILEY
29. JAHRGANG
NOVEMBER 2020
11
30 926

GIT SICHERHEIT + MANAGEMENT

MAGAZIN FÜR SAFETY UND

#zusammenhalten

Nutzen Sie unser kostenfreies ePaper!
GIT-SICHERHEIT.de/printausgabe
Abo-Nummer 247 eingeben

Wiley Industry Days
WIN DAYS
16.–19. November 2020
Jetzt kostenfrei registrieren:
www.WileyIndustryDays.com
Vorbericht im Heft

GIT SICHERHEIT AWARD
Die Sieger für 2021 ab S.10

RUBRIKEN
Mit Praxisberichten, Trends und Produktneuheiten aus allen Bereichen der Sicherheit

VIP: Tomislav Milovanovic
S. 114

Titelthema Seite 90:

WEICHEN EFFIZIENT STELLEN
MIT SOFTWARE VON PILZ

Mit Heft im Heft ab S. 33

WILEY

frogblue™

Jederzeit flexibel
... natürlich drahtlos!

SMART BUILDING
TECHNOLOGY
GERMANY

KNX MEMBER

frogblue.com

Terra Incognita

Was Ende März dieses Jahres noch als vage Idee im Raum stand, wird nun (virtuelle) Realität. Es ist wie mit so Vielem in letzter Zeit. Dinge, die vor nicht allzu langer Zeit noch eher Zukunftsmusik waren, sind plötzlich ganz real in der Umsetzung begriffen. So auch unsere virtuelle Messe, die Wiley Industry Days.

Mit diesem digitalen Format geben wir unseren Partnern und Kunden aus den Bereichen Safety & Security sowie Automation und Machine Vision die Möglichkeit, ihr Know-how unter Beweis zu stellen, ihre Produkte zu präsentieren, aber vor allem Kontakte zu knüpfen und ihr Netzwerk zu erweitern – und das Ihre, liebe Leserinnen und Leser. Denn nachdem im Angesicht strenger Hygienevorschriften und täglich steigender Corona-Fallzahlen beinahe alle Präsenzmessen im Herbst abgesagt wurden, ist der virtuelle Austausch vielerorts die einzige verbliebene Möglichkeit.

Doch die Virtualität hält auch ihre eigenen Regeln und Herausforderungen parat. In vielerlei Hinsicht ist die Planung und Durchführung einer digitalen Messe wie die Landung an den Gestaden des viel zitierten unbekannten Neulandes. Als unser Publishing Director Steffen Ebert mir vor einigen Wochen mit den Worten „Hier hast du den Hut auf" die Projektleitung übertrug, war mir schnell klar, dass es eine echte Herausforderung sein würde. Doch zum Glück stand ich nicht allein: Vor allem unser Layout – Ruth Herrmann, Elli Palzer, Maria Ender – und natürlich unser Team mit Miryam Reubold, Lisa Holland, Jörg Wüllner und Dr. Heiko Baumgartner, aber auch viele andere Kollegen aus anderen Wiley-Bereichen packten und packen tatkräftig mit an – voran Simone Tremmel und das Tec-Team um Anke Grytzka. Wichtig: Matthias Erler und Eva Kukatzki haben dafür gesorgt, dass das gedruckte Heft ordentlich organisiert ist. Ebenfalls mit vollem Eifer wurde das Projekt Wiley Industry Days auch von unseren Partnern, den Ausstellern angegangen. Vielen Dank! Denn das sei an dieser Stelle einmal gesagt: Ohne das unermüdliche Engagement so Vieler wäre die Realisierung dieses Events unmöglich.

Wenn am 16. November die Wiley Industry Days eröffnen, freuen wir uns, freue ich mich persönlich auch auf Sie. Daher registrieren Sie sich als Besucher kostenlos auf unserer Login-Seite www.WileyIndustryDays.com, schauen Sie bei den Vorträgen und Ständen vorbei, sprechen und chatten Sie live mit den Ausstellern.

Trotz aller Virtualität bleibt die GIT SICHERHEIT natürlich unser zentraler Dreh- und Angelpunkt. Daher haben wir auch für den November ein Heft mit vielen Highlights für Sie zusammengestellt. Unter anderem werden die Sieger des GIT SICHERHEIT AWARDS bekanntgegeben (ab S. 10) und unser Heft im Heft (ab S. 33) setzt sich intensiv mit dem Schwerpunkt Cyber Security auseinander, einem Thema, das gerade in den letzten Monaten an Bedeutung gewonnen hat. Also lesen Sie rein und entdecken Sie auch die vielseitigen Beiträge zu Safety, Security und Brandschutz.

In diesem Sinne: Stay safe, stay secure, stay with us!

Herzlichst,
Ihr

T. Gimbel

Timo Gimbel
für das Team von Wiley
und GIT SICHERHEIT

Wiley Industry Days
WIN DAYS
16.–19. November 2020

Registrieren Sie sich hier:
www.WileyIndustryDays.com

TITELTHEMA

Weichen effizient stellen

...dank übertragbarer Software und dem Automatisierungssystem PSS 4000-R bei den Verkehrsbetrieben Zürich (VBZ): Eine Softwarelösung und die sicheren bahntauglichen Module von Pilz steuern und überwachen Weichen unterschiedlichen Typs.

Seite 90

INNENTITEL SAFETY

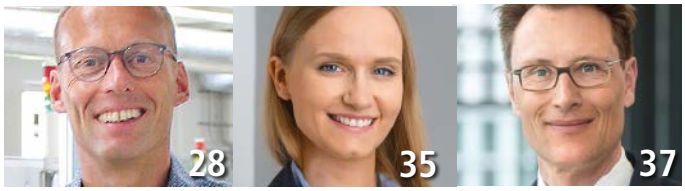
Der Schlüssel für sichere Lebensmittel

Flexibles Zugriffsmanagement in der Nahrungsmittelindustrie.

Seite 85

Gültig für 2020/21:
GIT Sonderausgabe PRO-4-PRO anfordern per Mail an GIT-GS@Wiley.com

EDITORIAL

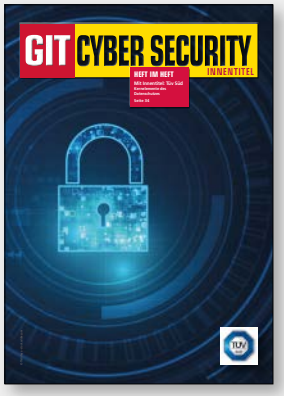


Thomas Taferner *Mareike Vogt* *Volker Wagner*

MANAGEMENT

SECURITY

HEFT IM HEFT • CYBER SECURITY



Werner Neugebauer *Mark Zhu* *Thorsten Wulff*

BRANDSCHUTZ

SAFETY

TITELTHEMA

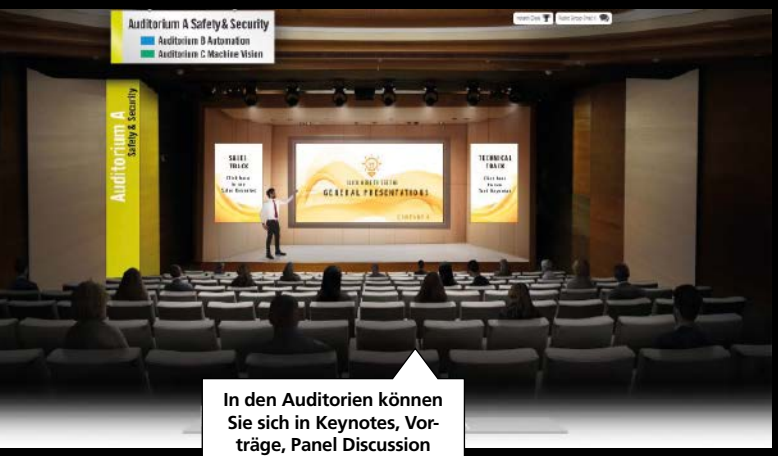
RUBRIKEN

ORGANISATIONEN INSTITUTIONEN UND UNTERNEHMEN IM HEFT

INDEX

SCHNELLFINDER

Wiley Industry Days
WIN>DAYS
16.–19. November 2020

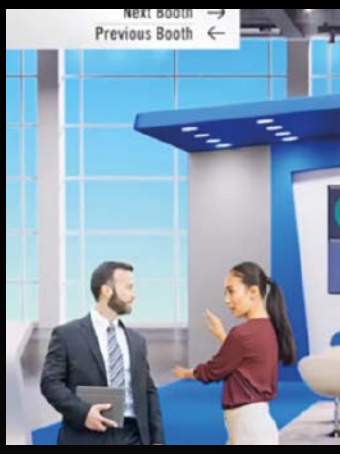


In den Auditorien können Sie sich in Keynotes, Vorträge, Panel Discussion einklicken, zuhören und Fragen stellen

Klick auf Hallen oder Auditorium und Sie gelangen direkt dort hin

Registrieren Sie sich kostenfrei als Besucher: www.wileyindustrydays.com

Sie sehen an jedem Stand, welcher Ansprechpartner virtuell gerade da ist und können mit ihm audio-/videochatten



Sicherheitsverantwortliche, Planer, Errichter, Händler, Architekten ebenso wie Qualitätsingenieure, Automatisierer, Programmierer, Anlagenplaner und Messtechniker sind eingeladen, sich als Besucher kostenfrei auf den WIN>DAYS zu registrieren und sich vier Tage lang, vom 16.-19. November 2020, über Neuheiten, Best Practices, Konzepte und Lösungen zu informieren.

Aussteller aus den Bereichen Security, Safety, Automation und Machine Vision präsentieren sich in den Hallen des WIN>DAYS-Messegeländes. Es erwarten die Besucher unter anderem Trends zu den Themen Sicherheitsmanagement, Videosicherheit, Zutrittslösungen, Cobots & Robots, Antriebstechnik, hyperspektrale Bildverarbeitung, Künstliche Intelligenz – und freilich auch eine ganze Menge Industrie 4.0. Abgerundet werden die WIN>DAYS durch das zeitgleich stattfindende Konferenzprogramm in den digitalen Auditorien.

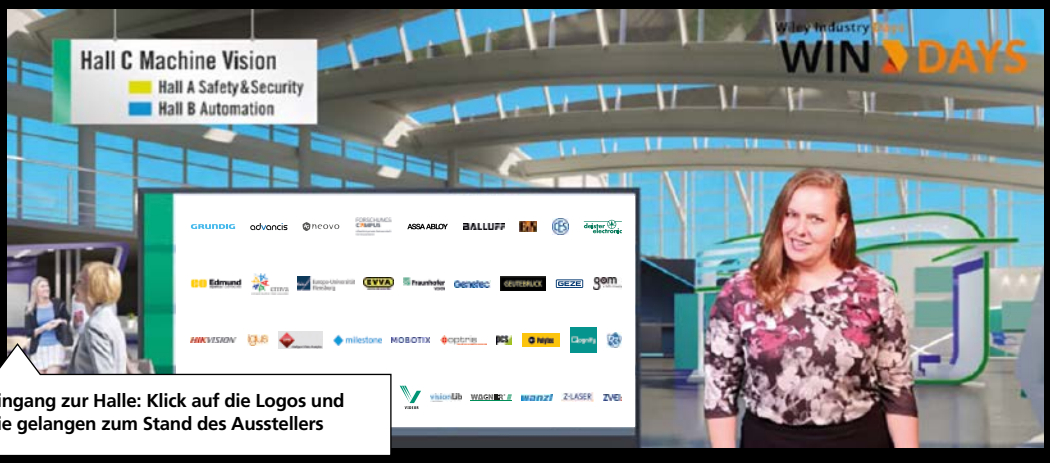
Messe, wie man es kennt – nur digital

Das Messegelände der Wiley Industry Days ist aufgebaut wie eine physische Messe. Zur Orientierung dient die Lobby mit Info-Punkten. Dort erhalten die Besucher den richtigen Überblick über die Räumlichkeiten. Mit der Navigationsleiste, auf den Bildschirmen jeweils run-of-site am unteren Bildrand, und mit Wegweisern lässt es sich bequem per Klick durch das Gelände navigieren. Eine Lounge und ein Meeting-Raum können genutzt werden, um mit Ausstellern und anderen Messebesuchern zu sprechen.

Der Fokus der WIN>DAYS liegt auf Vernetzung und Austausch. Besucher können sich auf dem gesamten Messegelände gegenseitig Chatanfragen stellen. Jeder Teilnehmer hat jederzeit den Überblick, wer sich auf dem Gelände und in den verschiedenen Räumen oder Ständen befindet. Außerdem gibt es in jedem Raum auch einen öffentlichen Chat.

Ein Vorbericht zu der virtuellen Messe in diesem Herbst: Was die Besucher erwartet, wen die Veranstalter und Partner erwarten und vor allem, warum Sie das nicht verpassen dürfen.

Die Fachzeitschriften messtec drives Automation, inspect und GIT SICHERHEIT veranstalten mit rund 30 namhaften Unternehmen und Institutionen die virtuellen „Wiley Industry Days", kurz **WIN>DAYS**. Die Entscheider der Branchen treffen sich dabei vom 16. bis 19. November 2020 virtuell auf **www.WileyIndustryDays.com**. Die Teilnahme ist kostenfrei – erforderlich ist lediglich eine Vorab-Registrierung.



Eingang zur Halle: Klick auf die Logos und Sie gelangen zum Stand des Ausstellers

Klickbare Flächen geben Ihnen an jedem Stand weitere Ressourcen zur Auswahl

An den Ständen finden Sie die Ansprechpartner der Aussteller und können sich direkt unterhalten – hier die (echten) Ansprechpartner des Ausstellers Advancis

Am virtuellen Messestand

Für die Aussteller stehen zudem weitere Networking-Funktionen zur Verfügung. Beispielsweise kann zusätzlich zur Ankündigung per Mail ein Audiosignal anzeigen, dass ein Besucher an einen Stand kommt. So lässt sich schnell und bequem in Kontakt treten. Ebenso finden Besucher eine Liste des Standpersonals und können so Austeller über die Chatfunktion, aber auch per E-Mail ansprechen. Bei Bedarf kann dann in einen privaten Raum zum Videochat gewechselt werden. Sollten einmal alle beschäftigt sein, gibt der Besucher seine digitale Visitenkarte ab und kann im Nachgang der Messe vom Aussteller kontaktiert werden.

Jeder Besucher besitzt außerdem eine „digitale Messetasche" – für Infomaterialien, Broschüren und sogar Videos. Nach der Messe wird die Tasche ganz einfach heruntergeladen oder per E-Mail versendet.

Kompaktes Konferenzprogramm

Der Fokus des Events ist die Ausstellung und das Netzwerken – begleitet von einem kompakt angelegten Konferenzprogramm. An jedem Vormittag findet jeweils eine Panel Discussion mit hochkarätigen Gästen statt. Danach kommen ausgewählte Key-Note-Speaker zu Wort, um neueste Entwicklungen aus Industrie und Forschung zu erklären. An den Nachmittagen laden Aussteller zu Vorträgen ein. Das digitale Konferenzprogramm lässt sich über die Auditorien einsehen – Interessierte können sich direkt in die Vorträge einklicken.

Mit den Wiley Industry Days, den WIN>DAYS, bieten der Verlag Wiley und rund 30 Partner eine Möglichkeit für einen Austausch in den Communities, die aktuell auf physische Veranstaltungen weitgehend verzichten müssen. Wer das virtuelle Event besucht, erklärt sich bei der Registrierung damit einverstanden, zumindest mit seinem Namen sichtbar zu sein. Das ermöglicht den freien und bequemen Austausch untereinander. Die Teilnahme ist für alle Besucherinnen und Besucher kostenfrei – erforderlich ist lediglich eine Vorab-Registrierung.

Konferenzprogramm

Montag

10:00–10:15 Eröffnung der Messe mit den Organisatoren – Team messtec drives Automation, Team inspect, Team GIT SICHERHEIT

10:30–11:30 Key Note Universität Flensburg: *Prof. Dr. Tabea Scheel* – „Was wir vom Home Office erwarten, und warum das nicht funktioniert"

11:30–12:00 Key Note Forschungscampus Stuttgart: *David Korte* – Autonome und sichere mobile Roboter mit der Hilfe von KI

Auditorium A Security/Safety – Themenschwerpunkt Zutrittskontrolllösungen
14:00–15:30 Evva
15:30–16:00 Deister Electronic
16:00–17:00 Assa Abloy

Auditorium B Automation/Machine Vision – Themenschwerpunkt Cobots & Robots // Bin Picking, Embedded Vision
14:00–14:30 R3 – Reliable Realtime Radio
14:30–15:00 Igus
15:00–15:30 Optris

Dienstag

Auditorium A+B
10:00–11:00 Podiumsdiskussion Sicherheit in der Chemischen Industrie – Mit den Sicherheitsexperten von Merck und Bayer: *Bernd Sassmannshausen, Dr. Peter Schäfer* und *Christian Daniel* sowie *Matthias Kleemeier* von PCS Systemtechnik und *Ralf Aubele* von Wanzl

11:00–11:30 Key Note ZVEI: Chefvolkswirt *Dr. Andreas Gontermann*: „Wie geht es der Elektroindustrie wirklich?"

Auditorium A Security/Safety

11:30–12:30 Key Note Genetec: *Kay Ohse* – Videoanalyse: Was Sie heute schon von der Technologie erwarten können

Auditorium B Automation/Machine Vision

11:30–12:30 Key Note EMVA: *Prof. Dr. Bernd Jähne* – EMVA 1288 Release 4 – Objektive Charakterisierung von industriellen Kameras

Auditorium A Security/Safety – Themenschwerpunkt Sicherheitsmanagement
14:00–14:30 Genetec
14:30–15:00 Advancis
15:00–15:30 Wagner
15:30–16:00 Milestone

Auditorium B Automation/Machine Vision – Themenschwerpunkt zentral vs. dezentral // Hyperspektrale Bildverarbeitung, 3D-Sensorik, optisches Vermessen
14:00–14:30 GOM: Visualisierung und Analyse von CT-Daten

Mittwoch

Auditorium A+B
10:00–11:00 Podiumsdiskussion „Augmented Reality – Experten aus der Automatisierungsbranche" – Mit Experten von: Fraunhofer IGD, VDMA, Visometry, Ubimax und weiteren

Auditorium A Security/Safety

11:00–11:30 Key Note United Nations und Global Health Security Alliance: *Colonel Dr. Stefan Göbbels* – Sichere Patientenversorgung und Standardisierung in der Krise
11:30–12:00 Key Note Milestone: Cloudspeicherung

Auditorium B Automation/Machine Vision
11:00–11:30 Key Note Spectronet: *Sprecher N.N.* – „Supporting & Enhancing Collaboration in Photonics & Machine Vision" New Approaches for Digital Services and Concepts

Auditorium A Security/Safety – Themenschwerpunkt Videoüberwachungslösungen
14:00–14:30 Mobotix
14:30–15:00 Hikvision
15:00–15:30 Geutebrück
16:00–17:00 Verleihung des GIT SICHERHEIT AWARDS

Auditorium B Automation/Machine Vision
15:30–16:00 Verleihung des inspect Awards

Donnerstag

Auditorium A+B
10:00–11:00 Podiumsdiskussion „Dezentral & modular – so automatisieren wir morgen!" – Mit den Branchenexperten: Optris, R3, Balluff und Turck

Auditorium A Security/Safety

11:00–11:30 Key Note Onvif – *Per Björkdahl,* Chairman of the Onvif Steering Committee

Auditorium B Automation/Machine Vision

11:00–11:30 Key Note Fraunhofer Vision: *Dr. Robin Gruna,* Fraunhofer IOSB Karlsruhe, und *Dr. Jochen Aderhold,* Fraunhofer WKI Braunschweig: Hyperspektrale Bildverarbeitung

Auditorium A Security/Safety – Themenschwerpunkt Sicherheitslösungen
15:30–16:00 Geze

Dienstag, 17. November ab 17:00 Happy Hour
Mit Bier-Tasting. Sie wollen dabei sein?

Registrieren Sie sich auf www.WileyIndustryDays.com
und schreiben Sie eine formlose Mail an Simone.Tremmel@Wiley.com mit „Happy Hour"

EVVA
access to security

Besuchen Sie
uns auf den
Win›Days 2020
16. - 19.11.

Xesar

Einfach vielfältig

Das elektronische Zutrittssystem Xesar bietet Ihnen eine große Produktauswahl. Das Interface der Verwaltungssoftware ist benutzerfreundlich gestaltet. Für große und kleine Schließanlagen geeignet.

Xesar-Top-Features

- Mehrplatzbetrieb mit Benutzerrollen
- Vielfältige Produktauswahl
- Attraktive Bezahlmodelle
- Flexible Anlagenerweiterung

www.evva.com

GIT SICHERHEIT AWARD

GIT SICHERHEIT AWARD 2021 – die Gewinner

In diesen Zeiten wird alle Welt ja immer wieder aufgerufen, sich auch der schönen Dinge und guter Nachrichten bewusst zu werden. Dazu gehören auch Preise, die man vergibt oder erhält oder beklatschen und sich für Andere mitfreuen darf.
Das wollen wir hier tun – und die Gewinner des GIT SICHERHEIT AWARD 2021 bekannt geben. Gewonnen hatten ohnehin schon alle in Heft 6/20 nominierten Finalisten – weil sie eine neutrale Jury von ihren Vorzügen überzeugt haben. Für jeweils drei Sieger einer jeden Kategorie gibt es hiermit jetzt noch das sprichwörtliche Sahnehäubchen, weil sie außerdem die meisten Leserstimmen eingesammelt haben.

Kategorie A

IT-Security und Safety in der Automation, Cyber Security

1. Sieger

Euchner: CTM

Transpondercodierte Zuhaltung

Speziell für den Einsatz an kleinen Klappen und leichten Türen von Verpackungsmaschinen entwickelt, besticht die neue transpondercodierte Zuhaltung CTM durch ihre geringen Maße. Sie zählt weltweit zu den kleinsten Zuhaltungen auf dem Markt und ermöglicht Prozess- und Personenschutz auf kleinstem Raum. Dies bietet Konstrukteuren neue Freiheiten, denn die Zuhaltung lässt sich nahezu unsichtbar ins Maschinendesign integrieren. Trotz der kompakten Bauform verfügt der CTM über eine Zuhaltekraft von 1000 N und bietet eine zuverlässige Schutztürabsicherung nach Kat. 4/PL e entsprechend EN ISO 13849-1 (höchste Schutzart IP69). Der CTM ist zudem als Hygienevariante verfügbar und bietet dank intelligenter Kommunikationsfähigkeiten Zukunftssicherheit in punkto Industrie 4.0.

3. Sieger

ABB Stotz Kontakt: HD5

Dreistufiges Zustimmgerät

Das neue dreistufige Zustimmgerät HD5 bietet maximale Sicherheit bei außerordentlicher Flexibilität und perfekter Ergonomie. Der optionale Not-Halt, die integrierte Taschenlampe und ein Bewegungssensor sorgen für zusätzliche Funktionen und optimale Sicherheit des Bedieners. Frei programmierbare Tast- und Signal-Elemente für visuelle und haptische Rückmeldung ermöglichen den individuellen und auf Ihre Bedürfnisse angepassten Einsatz. Zudem entspricht das Gehäuse den Richtlinien von „hygienic design" und ist aus hochwertigstem Material gefertigt. Somit ist die Funktionalität auch in anspruchsvollen Einsatzumgebungen gegeben. HD5 entspricht der Schutzklasse IP65 und erhielt Zulassungen nach CE, TÜV-Süd und cULus

2. Sieger

Moxa Europe: Intrusion Prevention System (IPS)

Cybersicherheitslösung für OT und IT

Um sicherzustellen, dass die Netzwerkaktivität in Industrienetzwerken autorisiert ist, ermöglicht die industrielle Cybersicherheitslösung von Moxa die Definition granularer Zugangskontrollen auf verschiedenen Ebenen. Man kann eine Whitelist von Geräten und IP-Ports definieren, denen der Zugriff aufs gesamte Netzwerk oder einen Teil davon gestattet ist. Darüber hinaus lässt sich das autorisierte Protokollformat definieren, um zu verhindern, dass nicht autorisierte Befehle die industriellen IPS oder Firewalls passieren. Außerdem können OT-Ingenieure festlegen, welche Steuerbefehle das Netzwerk passieren dürfen, um menschliche Fehler im Zusammenhang mit dem Senden eines falschen Steuerbefehls zu reduzieren. Darüber hinaus bietet IPS virtuelles Patching von Schwachstellen für Betriebssysteme, Anwendungssoftware und Industrieausrüstung wie SPSen.

Kategorie B

Brandschutz, Ex- und Arbeitsschutz

Securiton: SecuriRAS ASD

Ansaugrauchmelder

1. Sieger

Die Modellfamilie SecuriRAS ASD bietet für jede Anwendung den passenden Ansaugrauchmelder und ermöglicht neben hochempfindlicher Branddetektion einen skalierbaren Einsatz. Der SecuriRAS ASD 535 überwacht Areale bis zu 5.600 m². Er verfügt über einen der stärksten Lüfter auf dem Markt und eignet sich für den Einsatz in großen Hallen, Reinsträumen und Tiefkühllagern. Das Kompaktgerät SecuriRAS ASD 532 kommt dagegen in Aufzugsschächten oder EDV-Racks zum Einsatz. Ergänzt wird die Melderserie durch eine Heavy Duty-Variante, welche für raue Umgebungen konzipiert ist. Die Elektronik widersteht durch einen Schutzlack aggressiven Dämpfen oder Chlorgasen. Die Rauchpartikel-Messempfindlichkeit kann bei allen Geräten zwischen minimalen 0.002%/m und maximalen 10%/m gewählt werden. Ergänzt wird die ASD-Familie durch ein umfangreiches Zubehörsortiment: u. a. verschiedene Ansaugleitungen aus PVC, ABS oder Kupfer, Staubfilter und Wasserabscheider.

Ejendals: Jalas

Sicherheitsschuhe

2. Sieger

Der Hightech-Fußschutz des schwedischen Markenherstellers Ejendals ist die „Schneekette für Arbeitsschuhe" und hat Vorteile in Bezug auf Grip, Standfestigkeit, Laufgeschwindigkeit und Wegrutschgefahr. Rutschiger Boden, vereiste Flächen und glatter Untergrund bergen hohes Unfallpotential. Ejendals hat mit seiner Fußschutz-Serie Jalas Heavy Duty ein Novum im Arbeitsschutz geschaffen: Die Stiefel und Halbstiefel kombinieren die Schutzeigenschaften eines komfortablen Sicherheitsschuhes mit Vibram, hochprofessionellen Extrem-Sohlen.

Die Vibram Artic Grip-Sohlen überzeugen bei Bodenhaftung und Abreibung. Der Träger erlangt zudem eine sicherer und schnellere Gehgeschwindigkeit auf glatten, vereisten oder öligen Oberflächen (herkömmliche Sicherheitsschuhe ca. 0,38 m/s; Ejendals-Produkte 1,00 m/s). Druckmessungen ergaben eine Belastung von 27 kg (10 kg Standard-Schuhe). Weitere Vorteile sind die Sprunggelenkstützen, Stoßdämpfung sowie die ergonomische Form.

3. Sieger

Denios: SpillGuard

Gefahrstoff-Leckage-Sensor

Der SpillGuard als Gefahrstoff-Leckage-Warnsystem operiert vollkommen autark. Er detektiert alle flüssigen Gefahrstoffe mithilfe eines Sensors auf der Unterseite und ist für die ATEX Zone 1 zugelassen. Zudem zeichnet er sich durch seine einfache Bedienung aus – das Gerät wird am tiefsten Punkt einer Auffangwanne platziert und durch Knopfdruck eingeschaltet, Befestigungen sind nicht notwendig. Sobald das Gerät Flüssigkeit detektiert, wird ein visuelles und akustisches Alarmsignal ausgelöst, welches 24 Stunden anhält und durch Knopfdruck wieder auszuschalten ist. Der SpillGuard hat eine Batterielaufzeit von bis zu 5 Jahren und ein robustes elektrisch leitfähiges Gehäuse, um eine lange Lebensdauer zu garantieren.
SpillGuard ist ein Leckage-Sensor, der bei Gefahrstoffdetektion akustisch und optisch alarmiert. So hilft er, bei Gefahrstoffleckagen rechtzeitig zu reagieren und hohe Folgekosten für die Beseitigung sowie Schäden für die Umwelt zu vermeiden.

Award-Verleihung virtuell

Seien Sie dabei, wenn wir die Preise an die Gewinner übergeben: auf den digitalen **Wiley Industry Days,** den WIN>DAYS – am Mittwoch, dem **18. November 2020 um 16 Uhr.**
Registrieren Sie sich am besten gleich für die Show – die Teilnahme ist kostenfrei für alle Teilnehmer möglich: **www.WileyIndustryDays.com**

Kategorie C

Video-Sicherheitssysteme (VSS)

1. Sieger

Mobotix: M73

High-Performance IoT-Kamera

Die Mobotix M73 ist ein dezentrales, cybersicheres und modulares Videoüberwachungssystem der neuesten Generation. Basierend auf der Mobotix 7 Systemplattform profitiert der M73-Besitzer von zahlreichen bereits in die Kamerafirmware integrierten, auf KI basierenden Anwendungen. Mit individuell kombinierbaren 4K-Bildsensor- und Funktionsmodulen ist die M73 an den Einsatzzweck anpassbar. Sie ist sowohl hardware- als auch softwareseitig extrem robust und verfügt über ein wetterfestes Kameragehäuse. Pro M73 können immer ein oder zwei optische Sensormodule genutzt werden. Als dezentrale Edge-Kamera bietet die M73 relevante Systemvorteile: Es wird grundsätzlich kein Videoserver benötigt. Dies macht eine reine Mobotix-Lösung besonders einfach skalierbar und spart Zeit und Arbeit bei Installation und Unterhaltung der Videoanlage.

2. Sieger

Dallmeier Electronic: Panomera S

Überwachungskamera

Die neue Panomera S integriert bis zu acht Sensoren in einem Kamerasystem. Die patentierte Stitching-Technologie gewährleistet eine genau definierbare Mindestauflösungsdichte, dadurch reduziert sich die Anzahl der Bildschirme deutlich und zusätzliche PTZ-Systeme entfallen. Dies sind Grundvoraussetzungen für Gerichtsverwertbarkeit, Übersicht und Analyse und ermöglichen eine wesentlich bessere Kontrolle selbst über größte räumliche Zusammenhänge, eine planbare Datenqualität für Analyse und eine geringere Anzahl an benötigten Systemen.
Die neueste Generation ist eine komplette Neuentwicklung, die sich neben einem innovativen Design durch ein intelligentes Gehäusekonzept mit Vorteilen bei thermischer und mechanischer Widerstandsfähigkeit auszeichnet. Sowohl weite Strecken als auch große Flächen können so mit einer genau definierten Auflösungsdichte abgedeckt werden.

3. Sieger

Abus Security Center: WLAN Akku Cam

WLAN-Kamera

Mit der kabellosen und wetterfesten (Schutzklasse IP65) WLAN Akku Cam bietet Abus die perfekte Lösung für eine flexible und komfortable Grundstücks-, Haustier- oder Innenraumüberwachung. Dank eines Langzeit-Akkus in der Kamera mit bis zu 13 Monaten Laufzeit und einer Basisstation, die die Empfangs-Reichweite zum Router optimiert, kann sie völlig kabelfrei und weitgehend standort-unabhängig montiert werden. Die verschlüsselte Übertragung und Speicherung der Bildaufnahmen erfolgt dabei lokal und sicher in der Basisstation – ganz ohne Cloud. Außerdem liefert ein hochwertiger Sony Chip mit Low-Light-Funktion Tag wie Nacht ein scharfes Farbbild. Die Kamera präsentiert sich in einer Querformat-Bauweise, mit der sie ideal unter Vordächern und Dachvorsprüngen angebracht werden kann. Die Basisstation kann an jeder Steckdose mit WLAN-Empfang im Haus angebracht werden und sichert die Daten auf einer SD-Karte im Hausinneren.

Kategorie D

Zutritt, Einbruch- und Perimeterschutz

1. Sieger

PCS Systemtechnik: Intus 1600PS-II

Handvenenerkennungssystem

Intus 1600PS-II ist ein komfortables und hochsicheres biometrisches Zutrittsterminal, das Personen an Hand des Musters ihrer Handvenen erkennt. Primär entwickelt für den Schutz von Hochsicherheitsbereichen meistert es auch den Einsatz in Komfortanwendungen. Intus 1600PS-II stellt die Sicherheit aller Systembestandteile in den Mittelpunkt. Die Templates werden noch im Sensor verschlüsselt, diese Daten leitet das Terminal dann über gesicherte Leitungen in den geschützten Bereich. Manipulationen am Terminal detektiert der Sabotage-Kontakt. Für höchste Sicherheit bei der Erkennung sorgt die Mehrfaktor-Authentifizierung. Die neue Version erkennt auch Personen mit zittrigen Händen und arbeitet bei 80.000 Lux. Die Innovation liegt in der Kombination der hochsensiblen Sensortechnik, die hochsichere Zutrittskontrolle für besonders schützenswerte Räume ermöglicht, mit der einfachen Anwendung, die dem Nutzer einen hohen Anwendungskomfort bietet.

3. Sieger

Cias: Micro-Ray 100MT

Lineare Mikrowellenbarriere

Der Micro-Ray 100MT ist eine Barriere mit Mikrowellen-Strahlung für die Freilandüberwachung in Umgebungen aller Art. Sie wurde speziell für den Schutz in sehr engen Durchgängen entwickelt und kann im selben Schacht bis zu vier Strahlen erzeugen, wodurch eine lineare empfindliche Zone mit einem Durchmesser von 40cm über die gesamte Reichweite von 100m entsteht und eine fortschrittliche Erkennungsleistung bei Eindringversuchen garantiert werden kann. So kann die Mikrowellentechnologie über die gegenwärtigen Anwendungsbereiche hinaus ausgeweitet werden. Die Zuverlässigkeit der Mikrowellen kann jetzt auch auf engeren Räumen genutzt werden, wo normalerweise Aktiv-Infrarot-Technologie zum Einsatz kommt. Micro-Ray verwendet eine Mikrowellenantenne, die in der Lage ist, einen sehr engen linearen Erfassungsbereich zu erzeugen, und zusammen mit den Fuzzy-Logic-Algorithmen die besten Erfassungsleistungen erzielt.

2. Sieger

Salto: XS4 Locker BLE

Elektronisches Spindschloss

Dank der Integration von BLE (Bluetooth Low Energy) in die neueste Version des elektronischen Spindschlosses XS4 Locker BLE dehnt Salto funkvernetzte Zutrittskontrolle und Mobile Access auf Spinde, Möbel, Vitrinen etc. aus. Der neue XS4 Locker BLE sorgt damit für eine einfachte Verwaltung, schafft flexible und sichere Aufbewahrungsmöglichkeiten und bietet Nutzern die Bedienung mit Smartphones (Mobile Access). Das Spindschloss ist vollständig in die Salto Space Systemplattform integriert und ebenso mit der Cloud-Zutrittslösung Salto KS Keys as a Service kompatibel. Der XS4 Locker BLE basiert auf der bewährten Version des Spindschlosses und bietet Betreibern eine kabellose Steuerung in Echtzeit, konfigurierbare Öffnungsmodi für Nutzer, Aktualisierung der Zutrittsrechte, Übertragung von Blacklists sowie die automatische Erfassung von Protokolldaten und des Batteriestatus.

HINWEIS: Absolut gleiche Stimmenzahl
Die Produkte von Cias und Dormakaba haben tatsächlich die jeweils genau gleiche Stimmenanzahl erhalten – daher vergeben wir den 3. Sieger in dieser Kategorie doppelt.

3. Sieger

Dormakaba: evolo smart 2.0

Smarte Zutrittslösung

Die bequeme Zutrittslösung Dormakaba evolo smart ist eine kostenlose App, die eine einfache Schlüsselverwaltung für Privathaushalte oder kleine Unternehmen bietet. Mit dem Smartphone legt man fest, wer wann Zugang erhält und programmiert die elektronischen Türkomponenten von dormakaba. Der Nutzer öffnet die Türen mit Smartphone, Ausweis oder einem Schlüsselanhänger. Geht ein Zutrittsmedium verloren, wird dieses mit der App aus der Tür gelöscht. Für den Zutritt mit dem Smartphone kann über die App ein digitaler Schlüssel virtuell an neue Nutzer gesendet werden. Der Nutzer bestimmt, wer eine Türe zu welchem Zeitpunkt öffnen darf oder nicht. Alle berechtigten Schlüssel werden auf einem digitalen Schließzylinder von dormakaba gespeichert. Dieser kann gegen den bisherigen Schließzylinder in der Türe mit wenigen Handgriffen ausgetauscht werden und sofort ist die smarte Tür Realität. Eine Verkabelung ist dafür nicht nötig.

Kategorie E

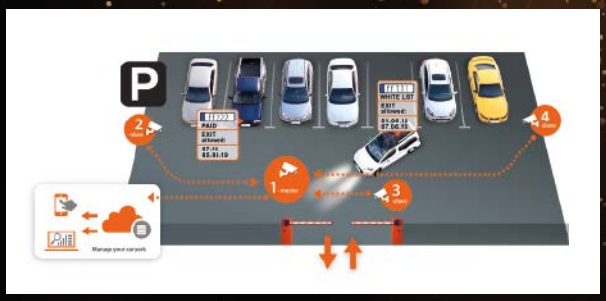
Sicherheitsmanagement, Lösungen und Dienstleistungen

Hanwha Techwin Europe: Wisenet Serverless ANPR

Nummernschilderkennung

1. Sieger

Mit dieser leicht konfigurierbaren Kamera-zu-Kamera-IP-Kommunikationstechnologie können bis zu 4 Wisenet ANPR-Kameras (1 Hauptkamera und 3 Nebenkameras) gekoppelt werden, um Bilder simultan zu erfassen und bequem an eine Benutzeroberfläche zu übertragen. Dank ihrem leistungsstarken Chipsatz kann die leicht konfigurierbare, serverlose ANPR-Lösung die Kennzeichen von Fahrzeugen mit einer Geschwindigkeit von bis zu 50 km/h mit einer Genauigkeit von 95% erfassen. Neben der Überwachung von Parkplätzen, Tankstellen oder auch kleinen Wohnsiedlungen mit mehreren Ein- und Ausfahrten lassen sich mit Hilfe der Wisenet Serverless ANPR auch wertvolle Informationen zur Parkplatzverwaltung Verwaltung wie die Verweilzeit oder Belegung sammeln. Damit die ANPR-Lösung mit Drittanbietersoftware und -systemen interagieren kann, steht zudem eine Programmierschnittstelle (API) zur Verfügung.



2. Sieger

Axis Communications: Body Worn Solution

Bodycam, Andockstation und Systemsteuerung

Die brandneue Axis Body Worn Solution umfasst neben der Kamera selbst, die Kamera-Andockstation (8- oder 1-Schacht) und die Systemsteuerung. Dabei nimmt die Kamera Videos mit bis zu 1080 p, 30 Bildern pro Sekunde und Audio über Dual-Mikrofone mit Rauschunterdrückung auf. Zudem kommt die Wide Dynamic Range-Technologie zum Einsatz, um auch unter anspruchsvollsten Lichtverhältnissen gleichbleibende Bildqualität zu garantieren. Die Systemsteuerung bietet dabei einen zentralen Integrations- und Managementpunkt und lässt eine schnelle, zuverlässige Auslagerung des Videos zu (100 MBit pro Kamera). Alle Daten sind sowohl während der Speicherung als auch bei der Übertragung mit AES256 und TLS verschlüsselt.

3. Sieger

vi2vi: viGate

Temperaturmessung über Wärmebildkamera

Das viGate ist als Kontrollpunkt konzipiert, um das Risiko für Besucher und Mitarbeiter zu minimieren. Die Thermokamera kann die Objekttemperatur mit hoher Genauigkeit in Echtzeit messen und Personen mit einer höheren Gesichtstemperatur entdecken. Für flexible Einsätze unterstützt das Handgerät optimal. Die Traversenkonstruktion als „One Stand" oder Brückenkonstruktion realisiert ein echtes Gate. Zur Fiebermessung können verschiedene Kameramodule ausgewählt werden. Das System umfasst ein Kabelmanagement zur stolperfreien Montage von Versorgungskabeln, ein mobiles Vereinzelungssystem, ein Warteschlangen-Leitsystem, ein optisches und akustisches Alarm- und Meldungsmodul, netzwerkbasierte Analyse- und Interaktionssoftware und Zählsensoren.

intel IoT Solutions Alliance

SAIMOS

milestone

STÄDTE SICHER MACHEN

– Der smarte Weg

Eine intelligentere Zukunft erfordert stärker integrierte Lösungen - Lösungen, die dazu beitragen, Menschen, Eigentum, Infrastruktur und Straßen in den Städten sicherer zu gestalten und gleichzeitig die Netze und Dienste für die Menschen in den Städten der Zukunft effizienter und bequemer zu gestalten.

Wir sind stolz darauf, unsere Partnerschaft mit Best-of-Breed-Anbietern, Intel und Saimos, präsentieren zu können, die es uns ermöglicht, die Stärken von Video und die immensen Möglichkeiten von IoT-Lösungen und fortschrittlicher Videoanalyse freizusetzen.

WILEY INDUSTRY DAYS: 16-19 NOVEMBER

Besuchen Sie unseren gemeinsamen Stand von Milestone, Intel und Saimos auf den Wiley Industry Days vom 16. bis 19. November. Kommen Sie vorbei, um zu sehen, wie unsere Best-of-Breed-Lösungen die Sicherheit und Effizienz für Städte erhöhen können, oder einfach nur für einen Plausch. Wir freuen uns auf Ihren Besuch.

NEWS

Neuer Vorstand des ASW Bundesverbands gewählt

Die Mitglieder der Allianz für Sicherheit in der Wirtschaft (ASW Bundesverband) haben auf ihrer 29. ordentlichen Mitgliederversammlung einen neuen Vorstand gewählt. Diese Sitzung war die erste hybride Sitzung in der Geschichte des Verbands. Ingmar Behrens begrüßte stellvertretend für seinen Fachverband German Council of Shopping Centers die Teilnehmer der Präsenzveranstaltung am Leipziger Platz. Dort wurde Volker Wagner (BASF SE, ASW Baden-Württemberg) als Vorsitzender für weitere drei Jahre einstimmig wiedergewählt. Er freue sich sehr über die Zustimmung und Anerkennung bei den Mitgliedern, so Volker Wagner. Das bestärke ihn in der Arbeit, die in den vergangenen Jahren geleistet wurde. Die neue Corona-Krise stelle auch die Mitglieder im ASW Bundesverband vor viele bisher unbekannte Herausforderungen. Daher sei es ihm wichtig, mit Kontinuität in der Führung die ASW durch diese turbulenten Zeiten zu bringen.

www.asw-bundesverband.de ■

v. l. Carsten Menge, Peter Hutmacher, Marco Kauling und Rainer Lange-Hitzbleck

Raumsystem für das Klinikum in Herford ▲

Das Klinikum in Herford hat ein Raumsystem von Denios erhalten, das als Container für Covid-19-Abstriche eingesetzt werden soll. Das Testzentrum ist durch eine Trennwand in einen Bereich für das medizinische Personal und einen Patientenbereich mit jeweils separaten Ein- und Ausgängen geteilt. Der Abstrich wird durch eine in die Trennwand integrierte Fensterschleuse vorgenommen. Ein permanenter Luftunterdruck im Patientenbereich sorgt dafür, dass bei geöffneter Fensterschleuse eine Übertragung viraler Tröpfchen (Aerosole) auf das medizinische Personal verhindert wird. Aufgrund der mobilen Beschaffenheit des Raumsystems hat das Klinikum Herford die Möglichkeit, das Testzentrum flexibel im Außenbereich aufzustellen und so die Patienten außerhalb des Gebäudes zu untersuchen. Das Testzentrum wurde durch Rainer Lange-Hitzbleck, Director Marketing, sowie Carsten Menge, Director International Operations- und Corona-Beauftragter bei Denios, übergeben. Seitens des Klinikums freuten sich Vorstandssprecher Peter Hutmacher sowie Marco Kauling, Mitglied des Krisenstabs, über das neue Raumsystem.

www.denios.de ■

VdS-Fachtagungen

Auch 2020 müssen Brandschutz- und Sicherheitsprofis nicht auf die VdS-Fachtagungen verzichten, die Anfang Dezember ausgerichtet werden: Am 2. und 3.12.2020 stehen insgesamt sieben Tagungen zur Auswahl, die meisten sowohl in der Koelnmesse als auch im Livestream. Die sonst parallel dazu stattfindenden VdS-Brandschutztage mit ihrer großen internationalen Fachmesse werden dieses Mal coronabedingt ausfallen. Neu in diesem Jahr: Die Fachtagungen sind, bis auf eine Ausnahme, alternativ zur Präsenzveranstaltung auch als Livestream buchbar, sodass sie ganz flexibel per Web verfolgt werden können. Eine coronabedingte Änderung gibt es bei der Fachtagung „Feuerlöschanlagen": Aufgrund der möglichen Reisebeschränkungen wird die sonst alle zwei Jahre als zweitägige, internationale Veranstaltung ausgerichtete Fachtagung dieses Jahr nur eintägig und ohne Simultan-Übersetzung stattfinden.

www.vds.de ■

Neuer Strategic Alliance Manager bei Advancis

David Teppe, Strategic Alliance Manager am Advancis-Hauptsitz

Nach über zehn Jahren als Sales Director von Advancis Middle East hat sich David Teppe entschlossen, wieder nach Deutschland zurückzukehren und die neue Funktion des Strategic Alliance Manager am Advancis-Hauptsitz in Langen/Frankfurt zu übernehmen. Das Unternehmen arbeitet eng mit einer ständig steigenden Anzahl internationaler Partner zusammen. David Teppe steht den OEM-, Technologie- und Solution-Partnern des Unternehmens als Hauptansprechpartner zur Verfügung. Die Zusammenarbeit mit den Partnern gewährleistet den stetigen Informationsaustausch in Bezug auf Entwicklungs-, Technik- und Vertriebsaktivitäten.

www.advancis.net ■

BDSW: Umsatz der Sicherheitsbranche sinkt im 2. Quartal

Die Corona-Pandemie habe im Dienstleistungsbereich im 2. Quartal 2020 Spuren hinterlassen, so der Hauptgeschäftsführer des Bundesverbands der Sicherheitswirtschaft (BDSW), Harald Olschok. Wie das Statistische Bundesamt (Destatis) nach vorläufigen Ergebnissen mitteilt, lagen die Umsätze in ausgewählten Dienstleistungsbereichen im 2. Quartal 2020 um 12,4 Prozent niedriger als im 1. Quartal. Die Sicherheitsbranche sei mit einem Umsatzrückgang von 1,7 Prozent im 2. Quartal 2020 im Vergleich zu den ersten drei Monaten bislang relativ glimpflich durch die Krise gekommen. Besonders von der Corona-Pandemie betroffen seien Sicherheitsunternehmen im Veranstaltungsschutz, in der Passagier- und Gepäckkontrolle sowie die Geld- und Wertdienste. Deren Anteil am Gesamtumsatz der Sicherheitswirtschaft von rund 9,3 Mrd. Euro im vergangenen Jahr lägen bei maximal 15 Prozent. Deshalb habe ihr deutlich höherer Umsatzrückgang die Gesamtbilanz nur geringfügig belastet, so Olschok.

www.bdsw.de ■

Florian Lauw verstärkt Kommunikationsteam bei Bosch

Florian Lauw (43) ist Corporate Communications Manager und Pressesprecher im Kommunikationsteam von Bosch Building Technologies in Grasbrunn bei München. Er berichtet an Carola Hehle, Director Corporate Communications. Zuvor war Florian Lauw bei Abus über acht Jahre für die Presse- und Öffentlichkeitsarbeit der Bereiche Zutrittskontrolle, Videoüberwachung, Alarmsysteme, Türsprechanlagen und Mechatronik verantwortlich, zuletzt als Leiter des PR-Teams und Unternehmenssprecher.

Florian Lauw

www.boschbuildingtechnologies.com ■

Jobsuche beim BVSW

Beim Stellenmarkt des Bayerischen Verbandes für Sicherheit in der Wirtschaft (BVSW) veröffentlichen die Mitgliedsunternehmen regelmäßig ihre Stellenausschreibungen. Die Fokussierung auf das Thema Sicherheit in Kombination mit den Mitgliedsunternehmen sei das große Plus bei diesem Stellenmarkt, so Caroline Eder, Geschäftsführerin des BVSW. Der Stellenmarkt bringe Angebot und Nachfrage zielgerichtet zusammen. Für Interessenten, die eine neue Aufgabe in der Sicherheitsbranche suchen, sei der BVSW ein geeigneter Ansprechpartner. Der Verband engagiere sich außerdem für eine gute Aus- und Weiterbildung in der Sicherheitsbranche, so Caroline Eder. Viele Kursteilnehmer informierten sich auch nach ihrem Abschluss regelmäßig auf der Website des Verbands über neue Bildungsangebote. Das sei vielen Unternehmen bekannt und ein weiterer Grund, weshalb Arbeitgeber auf dem Stellenportal nach neuen Mitarbeitern suchen.

www.bvsw.de ■

BDSW: 30 Jahre Private Sicherheitsdienste

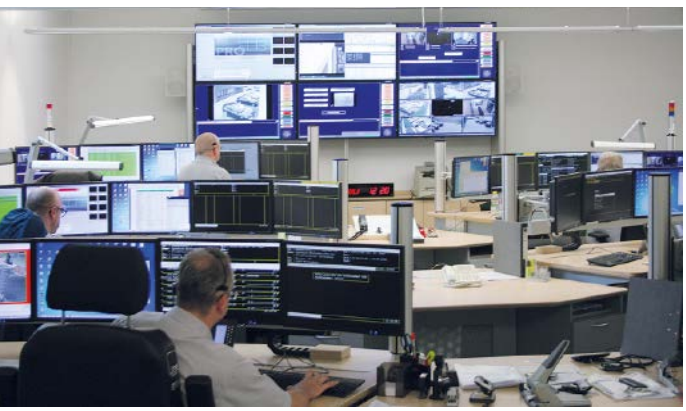
Bereits vor Vollendung der Deutschen Einheit am 3. Oktober 1990 wurden die ersten Wach- und Sicherheitsunternehmen noch in der damaligen DDR gegründet. Daran erinnert Harald Olschok, Hauptgeschäftsführer und geschäftsführendes Präsidiumsmitglied des BDSW. Man habe an zwei Ausbildungsberufen, der Einführung von Studiengängen und der DIN 77200 – Anforderungen an Sicherungsdienstleistungen mitgearbeitet, fasst Olschok die allgemeine Entwicklung des BDSW seit der Deutschen Einheit zusammen. Der Gesetzgeber habe 1996 das Unterrichtungsverfahren und 2002 die Sachkundeprüfung eingeführt. Die Innenministerkonferenz habe das Sicherheitsgewerbe als anerkannten Faktor der Sicherheitsarchitektur in Deutschland identifiziert, es seien Richtlinien für die Notruf- und Serviceleitstellen eingeführt worden und vieles andere mehr.

www.bdsw.de ■

VdS: Neues Dokument sorgt für Klarheit bei der Intervention

Gemeinsam mit der Polizei und drei Sicherheitsverbänden hat VdS Schadenverhütung in 2019 ein bundesweit einheitliches Alarmdienst- und Interventionsattest veröffentlicht. Nach über einem Jahr in der Verwendung wurde das Dokument noch einmal auf seine Praxistauglichkeit überprüft. Nachdem sich das neue Attest ein Jahr in der Praxis bewähren konnte, haben sich Vertreter der beteiligten Institutionen und Verbände erneut getroffen und ein erstes Resümee gezogen: Das Fazit aller Beteiligten sei, dass das neue Dokument von den Anwendern in Summe als sehr praxisorientiert gelobt werde und eine exzellente Hilfestellung im Alltag biete, so Sebastian Brose, Leitung der Abteilung Produktmanagement Produkte & Unternehmen bei VdS. Die Dokumentation in einer standardisierten Form erleichtere sowohl die Erstellung, die Prüfung (etwa bei Versicherungen) als auch die entscheidende Schnelligkeit der Umsetzung.

www.vds.de ■



Das Alarmdienst- und Interventionsattest ergänzt das Attest für Einbruchsmeldeanlagen

Schmersal gehört zu den attraktivsten Arbeitgebern ▲

Bereits zum zweiten Mal wurde die Schmersal Gruppe als „Wuppertals attraktivster Arbeitgeber" ausgezeichnet. Die lokale Bestenliste wurde von Statista, einem Online-Portal für Statistik, gemeinsam mit der Zeitschrift Capital nach einer Befragung von ca. 3.200 Arbeitgebern in 25 deutschen Großstadtregionen zusammengestellt. Nach Auswertung der Umfrage wurden Unternehmen ausgezeichnet, die nach Urteil der befragten Arbeitnehmer besonders gut abschneiden. Bei Schmersal sind gesellschaftliches Engagement und Verantwortung für die Umwelt tief im Unternehmen verankert, nicht zuletzt im Unternehmensleitbild und den Unternehmenswerten, die gemeinschaftlich mit allen Mitarbeitern erarbeitet und 2019 verabschiedet wurden. Diese Werte werden aktiv gelebt: Es haben sich viele Umweltschutzprojekte und Initiativen im Unternehmen gebildet.

www.schmersal.com ■

BDSW begrüßt Razzien gegen kriminelle Unternehmen

Der BDSW begrüßt die vom Zoll und der Steuerfahndung mit 900 Beamten durchgeführten Durchsuchungen wegen organisierter Schwarzarbeit im Sicherheitsgewerbe ausdrücklich. Das sagte BDSW-Hauptgeschäftsführer und geschäftsführendes Präsidiumsmitglied Harald Olschok. Laut des Hauptzollamts Frankfurt am Main habe einer der Hauptverdächtigen „enge Kontakte" zur Rockergruppe Hells Angels. Ein weiterer mutmaßlicher Haupttäter soll außerdem jahrelang Scheinrechnungen über 30 Millionen Euro ausgestellt haben. Durch derartige kriminelle Machenschaften würden Tausende von seriös arbeitenden Unternehmen der Branche geschädigt, so Olschok. Er verwies auf ähnliche Unregelmäßigkeiten bei der Auftragsvergabe von Sicherheitsdienstleistungen in Flüchtlingsunterkünften von der Arbeiterwohlfahrt an ihre eigene Tochtergesellschaft AWO Protect. Auch hier seien Zahlungen verschleiert und mangelhafte Kontrollmechanismen überlistet worden.

www.bdsw.de ■

Kötter: Erfolgreiche Personalentwicklungsstrategie

Während das neue Ausbildungsjahr bereits auf Hochtouren läuft, hat der Abschlussjahrgang in den Ausbildungsbetrieben der Kötter Unternehmensgruppe seine letzten Prüfungen abgelegt. Und die Bilanz für die im Sommer 2020 bzw. Winter 2019/20 erfolgten Abschlüsse kann sich sehen lassen: Im zurückliegenden Ausbildungsjahr haben rund 90 Prozent der Nachwuchskräfte ihre Ausbildung bei dem Familienunternehmen erfolgreich beendet. Coronabedingt liegen erst jetzt alle bundesweiten Prüfungsergebnisse final vor. Diese positive Zahl sei eine klare Bestätigung für die nachhaltige Ausbildungs- und Personalentwicklungsstrategie des Unternehmens, so Volker Hofmann, Leiter Personalwesen. Dies verdeutlicht der Vergleich mit dem Berufsbildungsbericht 2020: Demnach komme es in der deutschen Wirtschaft bei mehr als jedem vierten Ausbildungsverhältnis zur vorzeitigen Vertragsauflösung oder zum Ausbildungsabbruch.

www.koetter.de ■

Infektionsschutz mit smarten Lösungen von Wanzl

Auf der Sicherheitsexpo 2020 in München zeigte Wanzl Access Solutions smarte Zutrittslösungen im Kampf gegen Covid-19. Die Technologien der Zutrittsschleuse Galaxy Gate und des Automaten V21 wurden für den Kampf gegen das Virus passgenau modifiziert. Das Galaxy Gate wurde mit einem Desinfektionsmittelspender und einer Wärmebildkamera zur Messung der Körpertemperatur modifiziert. So verknüpft die Sicherheitsschleuse nun Zutrittskontrolle mit Infektionsschutz. Der Automat V21 wiederum ermöglicht vorausschauendes Besuchermanagement. Er erlaubt die digitale Registrierung und Authentifizierung von Besuchern beim Gebäudezutritt, während die Mitarbeiter durch die softwareseitige Integration des Automaten V21 Personenströme überwachen und nachvollziehen können.

Automat V21 von Wanzl

www.wanzl.com ■

iLoq reduziert CO_2-Emissionen

iLoq wickelt seinen Luft- und Seetransport in Zusammenarbeit mit Kühne + Nagel CO_2-neutral ab. Mit dem Umweltprogramm „Net Zero Carbon" bietet Kühne + Nagel Unternehmen eine einfache Lösung zur Neutralisierung der CO_2-Emissionen beim Transport. Die Projekte sind nach dem Verified Carbon Standard (VCS) oder dem Gold Standard zertifiziert und entsprechen den UN-Zielen der nachhaltigen Entwicklung und unterstützen und verbessern die grundlegenden Lebensbedingungen in Entwicklungsländern. Diese Zusammenarbeit unterstütze die Umweltverantwortung von iLoq, so Pekka Hassi, Senior Sourcing Manager von iLoq. Mit dem Beitritt zum Umweltprogramm „Net Zero Carbon" sei das Unternehmen in der Lage, CO_2-Emissionen seiner Lieferungen leicht auszugleichen und gleichzeitig zu einer saubereren und lebendigeren Umwelt beizutragen.

Jedes Jahr sparten die batteriebetriebenen Lösungen des Herstellers im Vergleich zu mechanischen und batteriebetriebenen Verschlusslösungen 30.000 kg Batterieabfall ein.

www.iloq.com ■

Michael Kiel, Konzernbereichsleiter Operations (4. v. l.) und Florian Pauker, Projektleiter Digitale Projekte bei Evva Sicherheitstechnologie (3. v. l.)

Evva ist „Green Factory 2020"

Auf dem Fabrik-2020-Wettbewerb wurde Evva zur „Green Factory" gekürt. Fraunhofer Austria und das Industriemagazin verleihen bei diesem Wettbewerb die Auszeichnungen für Produktionsunternehmen in Österreich. Der Preis zur nachhaltigsten Fabrik Österreichs bestätige den Weg des Unternehmens, der bereits lange vorher begonnen habe, so Michael Kiel, Konzernbereichsleiter Operations bei Evva Sicherheitstechnologie. Man habe noch viel vor und man hoffe, die hochgesteckten Ziele zur Exzellenz und Digitalisierung bald zu erreichen.

www.evva.com ■

Walter Elsner, Matthias Kleemeier und Ulrich Kastner-Jung (v. l.)

PCS schließt das Geschäftsjahr 2019/20 positiv ab

PCS Systemtechnik beendete zum 30.06. das Geschäftsjahr 2019/20 mit einem sehr guten Umsatzergebnis von 21 Mio. Euro, das entspricht einer Steigerung von 3,5 % gegenüber dem Vorjahr. Dass man in diesen herausfordernden Zeiten so ein gutes Umsatzergebnis erzielt habe, belege, wie stabil das Unternehmen aufgestellt ist, so Geschäftsführer Walter Elsner. Auch die Belegschaft wurde weiter aufgestockt, unter anderem in den Entwicklungsabteilungen: Inzwischen sind 148 Mitarbeiter für die Firma tätig. Trotz der Corona-Pandemie startet das Unternehmen mit einem Auftragspolster auf Vorjahresniveau in das neue Geschäftsjahr. Zum Start des neuen Geschäftsjahres verstärkte das Unternehmen auch die Geschäftsleitung um zwei weitere Mitglieder. Das Führungstrio besteht in Zukunft aus Walter Elsner (65), Matthias Kleemeier (52) und Ulrich Kastner-Jung (52).

www.pcs.com ■

Baby entführt, Senior verirrt, Personal attackiert – damit Kliniken und Gesundheitseinrichtungen nicht zum Tatort werden, verhindern kleine Helfer zur Personenortung, dass kritische Momente eskalieren. Mobile Notruf- und Ortungsgeräte finden und retten Menschen – so etwa die Lösung Securimove von Securiton.

▲ **Securimove von Securiton: Mobile Notruf- und Ortungssysteme**

GESUNDHEITSWESEN

Vertauschte Babys, verirrte Senioren

Dezente Notruf- und Ortungsgeräte entschärfen gefährliche Situationen

Ziellos auf Wanderschaft gehen und nicht mehr zurückfinden, gehört zum Krankheitsbild von Menschen mit Demenz. Wird ihr Verschwinden zu spät bemerkt, sind sie vielleicht schon weit gelaufen, gestürzt, unterkühlt oder dehydriert. Ein dezentes Armband oder ein Anhänger mit RFID-Transponder ermöglichen gefährdeten Personen Spaziergänge innerhalb und außerhalb einer Pflegeeinrichtung und bringen mehr Selbstbestimmung und Lebensqualität. Verlassen häufig desorientierte oder demente Senioren einen zuvor definierten Bereich, schlägt die mobile Notruf- und Ortungsfunktion Securimove von Securiton sofort Alarm. Die betroffene Person wird schnell gefunden, und mögliche Folgeschäden werden abgewendet.

Eingebunden sind die Transponder in das zentrale Kommunikationssystem Visocall IP. Die IP-basierte Systemlösung von Securiton Deutschland bietet neben dem normgerechten Lichtruf nach DIN VDE 0834 (2016) auch weitere Module für Pflege, Information, Service, Organisation und Abrechnung, die nach Bedarf eingesetzt oder zu einem späteren Zeitpunkt nachgerüstet werden können. Mit dem System können auch hochwertige medizinische Geräte mit einem Chip ausgestattet und per Tracking-Funktion lokalisiert werden.

Im falschen Bett

Intelligente Zutrittsberechtigung unterstützt in einer Vielzahl von Fällen den reibungslosen Pflegealltag. Irrt sich etwa ein Bewohner häufig in der Zimmertür, legt sich ins falsche Bett oder sucht in fremden Sachen, sind Konflikte vorprogrammiert. Der Chip am Arm verhindert das Betreten anderer Privatzimmer und beugt Diebstahl vor. Er funktioniert dann wie ein „Funkschlüssel".

Keine Chance für Kidnapper

Babys vertauscht oder gar entführt – das sind Horrorvorstellungen für junge Eltern. Für Sicherheit vom ersten Tag an sorgen Transponder von Securiton. Eine Pairing-Station ordnet sie Mutter und Kind zu. Den ständigen Hautkontakt zum Säugling prüft ein kapazitiver Sensor. Verliert er ihn, gibt der Sender sofort eine Warnmeldung heraus. Babytransponder werden beispielsweise am Namensbändchen befestigt oder ins Söckchen gelegt. So kann das Kind auch innerhalb der Station geortet werden. Mit Securimove-Anhängern für Angehörige und Pflegende haben Kidnapper keine Chance: Beim Versuch, die Station unerlaubt zu verlassen, schlägt das System Alarm.

Beschimpft, bespuckt und bedroht

Immer häufiger eskaliert die Gewalt in deutschen Kliniken: Brennpunkte sind Notaufnahmen, Psychiatrien und Intensivstationen. Mit Notruftastern und zusätzlichen mobilen Funksendern kann der Mitarbeiter einen Hilferuf absetzen. Zusätzlich macht ein optisches und akustisches Signal Kollegen und Anwesende auf die Situation aufmerksam. Bei einem Notruf wird idealerweise ein Videosicherheitssystem aktiv und stellt in Echtzeit Aufnahmen zur Verfügung. Alle eingesetzten Systeme dokumentieren Ereignisse und schaffen so Rechtssicherheit für Krankenhäuser, Angestellte und Patienten. ■

Kontakt

Securiton Deutschland
Achern
Tel.: +49 7841 62230
info@securiton.de
www.securiton.de

TREFFEN SIE ADVANCIS ONLINE

BEI DEN WILEY INDUSTRY DAYS VOM 16.-19. NOVEMBER 2020

Die Gefahrenmanagementplattform WinGuard wird offen für individuelle Software-Entwicklungen: Treffen Sie uns auf der virtuellen Messe und erfahren Sie weitere Details.

Seit über 25 Jahren ist WinGuard eine der marktführenden Gefahrenmanagementplattformen zur einheitlichen Visualisierung und Steuerung technischer Systeme. Durch individuelle Handlungsanweisungen wird das Sicherheitspersonal optimal bei der Ereignisbearbeitung unterstützt, egal ob im Alarmfall oder bei täglich wiederkehrenden Routine- oder Wartungsaufgaben.

Über 450 Schnittstellen zu Anlagen verschiedenster Hersteller bieten größtmögliche Flexibilität bei der Auswahl oder Aktualisierung von Subsystemen (Brand-/Einbruchmeldeanlage, Video etc.). Neue Schnittstellenmodule werden konstant entwickelt und bereits bestehende optimiert.

Als Ergänzung öffnet sich WinGuard künftig für Drittentwicklungen. Mit der neuesten WinGuard-Version, die demnächst erhältlich sein wird, stellt Advancis eine noch offenere Softwareplattform bereit: Partner und Kunden können zusätzlich eigene Programm-Module entwickeln und direkt in WinGuard implementieren.

So lassen sich individuelle Funktionen unabhängig von gängigen Entwicklungszyklen realisieren. Für jedes Projekt kann genau der Funktionsumfang geschaffen werden, der benötigt wird – auch bei sehr spezifischen Anforderungen. Zum Beispiel können externe Tools, die nur im jeweiligen Unternehmen verwendet werden, in WinGuard eingebunden werden. Auch neue Oberflächen lassen sich ganz einfach erstellen.

WinGuard wird offen für Eigenentwicklungen, jedoch auf Basis einer bewährten und leistungsstarken Softwareplattform. Um Eigenentwicklungen für Dritte zu vereinfachen, stellt Advancis ein Schnittstellen- sowie ein UI-SDK zur Verfügung. Damit können externe Entwickler auf die gleichen WinGuard-Programmfunktionen zugreifen wie die Entwickler des Herstellers.

Besuchen Sie uns an unserem Online-Messestand.
Registrieren Sie sich kostenfrei unter:
https://wiley.6connex.eu/event/industrydays

advancis.de

LÖSUNGEN FÜR DIE ABFALLWIRTSCHAFT

Schwer auf ZAK

Videotechnik für die Zentrale Abfallwirtschaft Kaiserslautern

Rund 213 Kilogramm Verpackungsmüll verursacht ein Deutscher durchschnittlich im Jahr. Um die Behandlung, Verwertung und Beseitigung dieser und weiterer Abfälle von mehr als 250.000 Menschen in der Stadt und im Landkreis Kaiserslautern kümmert sich die ZAK – Zentrale Abfallwirtschaft Kaiserslautern. Um reibungslose Abläufe zu gewährleisten und das Gelände des modernen Abfallwirtschaftszentrums auf einer Fläche von rund 88 Hektar zu sichern, setzt die ZAK auf Mobotix-Videosysteme.

Das Gelände der Zentralen Abfallwirtschaft Kaiserslautern (ZAK) setzt auf Mobotix-Videosysteme

Die Mobotix-Kameras sind nicht nur sehr robust und wartungsfrei, die Netzwerkkameras lassen sich auch gut verwalten

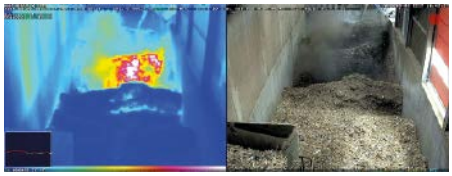
Seit die Deponie im Jahr 1999 aufgrund geplanter Gesetzesänderungen geschlossen wurde, werden die Restabfälle aus Stadt sowie Landkreis Kaiserslautern entweder mechanisch-biologisch aufbereitet und extern entsorgt oder direkt extern thermisch verwertet. Daher stehen auch die Anlagen zur Sammlung und Verwertung der Abfälle im Vordergrund. Alle Anlagen werden kontinuierlich weiterentwickelt, um dem Stand der Technik zu entsprechen.

Dies gilt auch für die Kameralösungen: „Während zunächst noch analoge Videotechnik eingesetzt wurde, um das Tor und die Anlagen1 im Auge zu behalten, sorgen mittlerweile 65 moderne Mobotix-Video-IP-Lösungen für einen reibungslosen Ablauf auf dem Betriebsgelände“, so Michael Hentz, Fachbereichsleiter EDV und Telekommunikation bei der ZAK.

Kamera übernimmt Brandschutz und Branderkennung

So werden zwei M15D Thermalkameras eingesetzt, um die Temperatur im Holzbunker im Allgemeinen zu überwachen – und zum anderen, um die Temperatur des Brennstoffes selbst zu kontrollieren. Die Videosysteme lösen dank einer thermischen Sensor-Technologie und Thermal Radiometrie automatische

65 Mobotix-Video-IP-Lösungen sorgen für einen reibungslosen Ablauf auf dem Betriebsgelände



Zwei M15D Thermalkameras überwachen die Temperatur im Holzbunker und kontrollieren die Temperatur des Brennstoffes selbst

Ereignisse innerhalb eines Temperaturbereiches von -40 bis zu +550 Grad Celsius aus. Daher eignet sich die Technologie sehr gut zur automatischen Alarmierung von Temperaturgrenzen oder -bereichen.

Eine dieser Thermalkameras hängt im Bunker und überwacht den kompletten Bunkerbereich auf hohe Temperaturen. Denn Gärprozesse können leicht dazu führen, dass ein Feuer ausbricht. Dadurch ist schon beim Beladen durch einen LKW ersichtlich, ob Material mit zu hohen Temperaturen eingeführt wird. Die zweite Videolösung ist an der Stelle angebracht, wo das Material mit dem Kran aufgenommen wird, um es der Verbrennung zuzuführen. „So wissen wir genau, wie heiß es im Bunker ist und können rechtzeitig Gegenmaßnahmen einleiten, wenn erforderlich", so Hentz.

Videolösung ersetzt Rückfahrkamera

Neben den Thermalkameras setzt das ZAK zu 90% M25-Videosysteme ein. Diese sind auf dem Gelände verteilt und vor allem dort angebracht, wo niemand sitzt. Dabei handelt es sich um sehr kompakte, kosteneffiziente und leistungsfähige Allround-Kameras mit 6MP-Moonlight-Technik. „Diese Kameras zeichnen sich vor allem dadurch aus, dass sie so robust, wartungsarm und wetterfest sind", erläutert der Fachbereichsleiter. „Das spielt bei uns eine ganz entscheidende Rolle, denn auf dem Wertstoffhof ist ja ständig Schmutz, der setzt sich natürlich aber auf den Kameras fest. Aber die Mobotix-Modelle halten dem sehr gut Stand, sie haben sich wirklich bewährt."

An Gebäuden, wo es sehr eng ist, sind ebenfalls Videosysteme montiert. Die Fahrer der beiden LKWs, die ständig auf dem Gelände hin- und herfahren, machen sich die Bilder dieser Kameras über ein Tablet zu nutze. So haben sie beim engen Rangieren immer alles im Blick wodurch Unfälle vermieden werden sollen. „Rückfahrkameras bringen bei uns nicht viel, die sind sofort verschmutzt", weiß Hentz. „Daher kamen wir auf die Idee, den Fahrern einfach ein Tablet ins Fahrzeug zu geben, das die Bilder der Kameras wiedergibt."

Türstation am Haupttor

Am Haupttor sind innen und außen zwei T25IP-Video-Türstationen angebracht. Sie dienen der Türkommunikation sowie Zutrittskontrolle und machen es mit RFID und Keypad möglich, den Zugang zum Gelände zeitgesteuert sowie protokolliert zu sichern und eine Fotodokumentation zu erstellen. Im Biomassekraftwerk sind rund um die Uhr Mitarbeiter. Daher kann es schon mal sein, dass sich auch nach den Öffnungszeiten des ZAK noch jemand auf dem Gelände befindet, der es verlassen möchte. Derjenige kann dann klingeln und sich von einem Mitarbeiter das Tor öffnen lassen.

Hentz ist sehr zufrieden mit den Lösungen. „Ich arbeite jetzt schon sehr lange mit diesen Videosystemen. Sie sind nicht nur sehr robust und wartungsfrei, die Netzwerkkameras lassen sich auch gut verwalten. Darüber hinaus punkten sie, weil Informationen direkt in den Kameras gespeichert werden können. Außerdem überzeugt mich auch immer wieder die Funktionalität, die sich über die Jahre weiterentwickelt hat. Dennoch funktionieren alle Kameras eigentlich gleich, das ist ein großer Vorteil in der Handhabung. Aufgrund der hohen Bildqualität und der Möglichkeit, verschiedene Objektive zu nutzen, sind die Einsatzmöglichkeiten zudem noch sehr vielfältig." ■

Kontakt

Mobotix AG
Langmeil
Tel.: +49 6302 9816 0
info@mobotix.com
www.mobotix.com

Unterstützung zur Einhaltung von aktuellen Abstandsregeln: Die flexible Zutrittskontrolllösung Scala mit Zählfunktion und stufenloser Skalierbarkeit für bis zu 2.000 Türen

ZUTRITT

Zählt jetzt zum Zutritt

Erweiterbare Zählfunktion in der Zutrittskontrolle unterstützt Anti-Corona-Maßnahmen

Die „AHA-Formel" als effektives Mittel, um der Pandemie zu begegnen, hat sich durchgesetzt. Es ist nicht nur vernünftig, sich danach zu richten. Es ist auch lebensrettend, die Bedeutung der drei Buchstaben zu beachten: Abstand, Hygiene und Alltagsmaske. Was jeden persönlich angeht, gilt für die Sicherheitsverantwortlichen von öffentlichen Infrastrukturen, Gebäuden und Einrichtungen mit großem oder ständig wechselndem Personenverkehr umso mehr. Die Zutrittslösung Scala von Assa Abloy kommt deshalb mit einer erweiterbaren Zählfunktion.

Die Erhebung von Personenzahlen, deren Begrenzung und Maßnahmen zur Kontrolle und Beschränkung des Zutritts in ein Gebäude gewinnt an Gewicht. Hier bewähren sich gerade im Bereich der Zutrittskontrolle Lösungen wie Scala von Assa Abloy. Das System lässt sich flexibel und ohne größeren Aufwand um zusätzliche Funktionen erweitern. Dazu gehört mit der Lizenzerweiterung „Zählfunktion" auch ein frei programmierbarer Zähler zum Definieren von festen Grenzwerten für die Personenanzahl in einem Gebäude und Integrieren automatischer Zutrittsverweigerungen beim Überschreiten von Warnschwellen.

„Scala" wie „skalierbar"

Die Kombinationsmöglichkeiten und nahezu beliebig erweiterbare Skalierbarkeit machen die Zutrittskontrollanlage besonders dort attraktiv, wo Sicherheitsverantwortliche im Zuge der aktuellen Hygiene- und Abstandsregelungen die Anzahl von Personen in einem Gebäude im Blick behalten und jederzeit schnell darauf reagieren müssen. Die flexible Zutrittskontrolllösung passt sich dabei stufenlos an – von einer einzelnen bis hin zu über 2.000 Türen.

Das modulare System eignet sich in seinen drei Varianten Scala Solo, Web/Web+ und 1Net für private, öffentliche sowie gewerbliche Objekte gleichermaßen. Die Skalierbarkeit gilt dabei auch für die Handhabung: Anwender können eine einfache Lösung oder umfangreiche Softwarefunktionen nutzen, die sich jeweils unkompliziert installieren und erweitern lassen. Selbsterklärende Softwareoberflächen erleichtern auch ungeübten Nutzern die Bedienung.

Passt zu Groß und Klein

Anwender können bei dem universellen und jederzeit skalierbaren Zutrittskontrollsystem Scala von Assa Abloy grundsätzlich zwischen drei Lösungspakten wählen:

- **Scala Solo** ist eine Ein-Tür-Lösung. Sie eignet sich vor allem für Privathaushalte und kleinere Objekte, wie Werkstätten, Arztpraxen, Architekturbüros oder Anwaltskanzleien. Bei der PIN-Variante programmiert der Nutzer den Mini-Controller über einen Master-Code und weist einzelne PIN-Codes zu. Alternativ können auch RFID-Transponder für den Zutritt verwendet werden. Ein Anschluss für einen Türkontakt ist ebenfalls vorhanden.
- **Scala Web/Web+** ist das nächstgrößere web-basierte Lösungspaket. Es bietet erweiterte Zutrittskontroll- sowie Zeitfunktionen. Geeignet ist es für kleine und mittelständische Unternehmen ohne technische Vorkenntnisse, die den Zutritt bisher mit mechanischen Zylindern verwaltet haben und ohne große Eingriffe auf eine Zutrittskontrollanlage umrüsten möchten. Mit dem leistungsstärkeren Scala Web+ Controller lassen sich bis zu acht vollverdrahtete Online-Türen einbinden oder bis zu 16 Türen über Elektronikbeschläge oder-zylinder, die über Funk in Echtzeit kommunizieren. Bis zu 95 Offline-Türen können verwaltet werden, die mit batteriebetriebenen Beschlägen und Zylindern ausgerüstet sind und deren Zutritt über Nutzerkarten gesteuert wird. Eine Softwareinstallation ist bei dieser Lösung nicht nötig. Einzel- bis hin zu zeitlich festgelegten Freigaben lassen sich über einen Browser im Endgerät vornehmen. Wächst das Unternehmen und damit die Anforderungen sowie die Zahl der Türen, entwickelt sich das System einfach mit. Die Personendaten können exportiert oder importiert werden, sodass ein Umstieg von Scala Web auf die größte Lösung Scala Net problemlos möglich ist. Die vorhandene Hardware bleibt dabei gleich.
- **Scala Net** wiederum erlaubt eine vollständig in ein Netzwerk integrierte Anlagenstruktur und bietet den vollen Funktionsumfang einer Zutrittskontrolllösung mit Zeitschaltung, Zonenüberwachung oder Aufzugssteuerung. Dank des modularen Aufbaus lässt sich die Lösung durch die Vergabe von Lizenzen wie der Lizenzerweitertung „Zählfunktion" leicht erweitern. So wächst die Struktur mit dem Bedarf des Unternehmens und erfüllt auch spezielle Ansprüche. Dabei können alle gängigen RFID-Technologien verwendet werden.

Mit der Zählfunktion lassen sich pro Scala-Net-Controller bis zu 32 frei programmierbare Zähler konfigurieren und die Anzahl an Personen in einem Bereich genau erfassen und begrenzen

Bitte umblättern ▶

Die Verwaltung von Tausenden von Türen und entsprechend vielen Mitarbeitern ist über die intuitiv bedienbare, selbsterklärende Software-Oberfläche ganz einfach

Lizenzerweiterung „Zählfunktion“

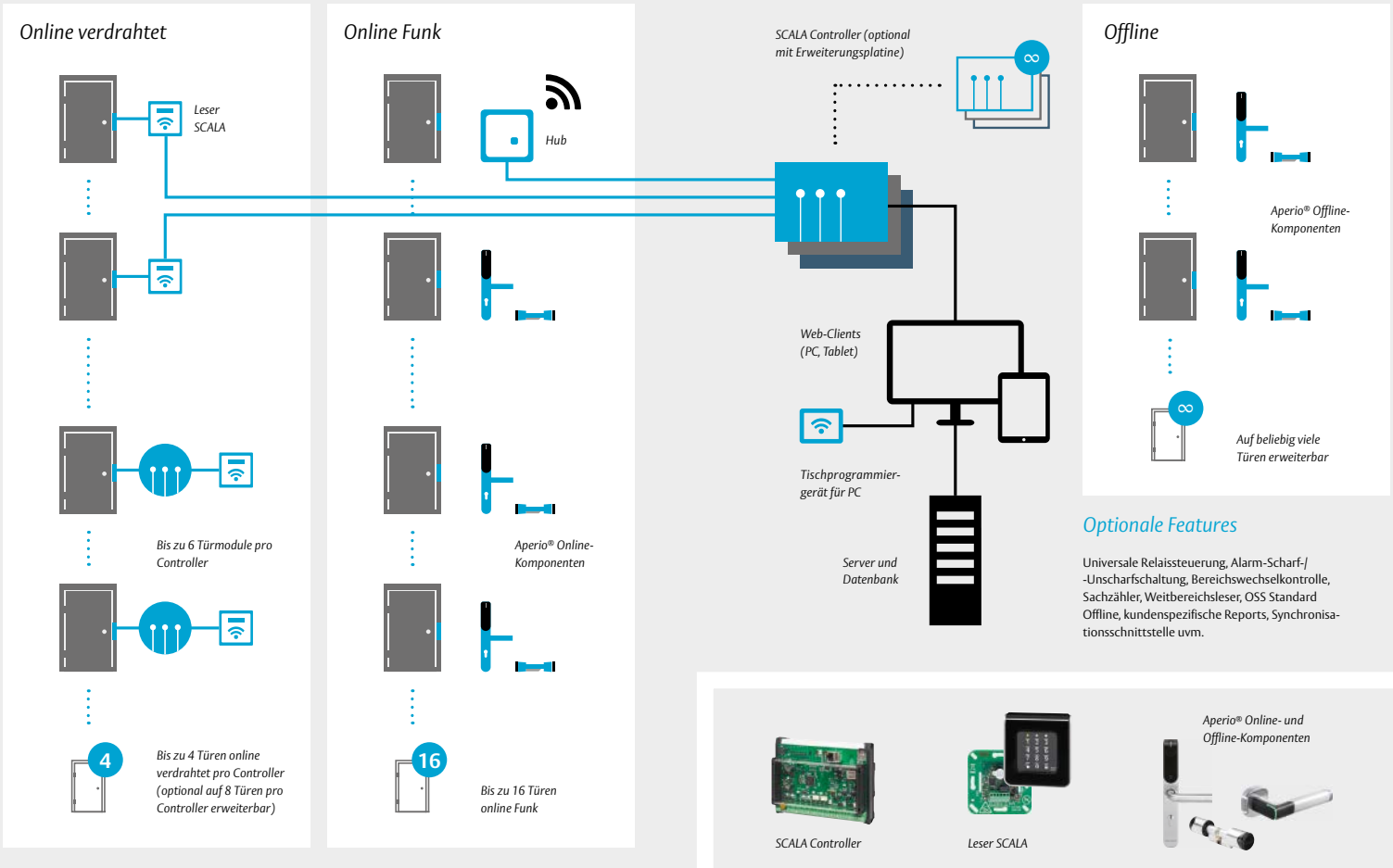
Die Lizenzerweiterung „Zählfunktion“ ist in diesem Zusammenhang exklusiv für Scala Net verfügbar. Dabei handelt es sich um die Client-Server-Lösung für große Unternehmen mit komplexen Anforderungen und speziellen erweiterbaren Zutrittskontrollfunktionen. Mit der Zählfunktion lassen sich pro Controller bis zu 32 frei programmierbare Zähler konfigurieren und die Anzahl an Personen oder die Anzahl an berechtigten Begehungen genau erfassen. Des Weiteren ermöglicht die Lizenz auch die Begrenzung der Anzahl an Personen in einem ganz bestimmten Gebäudebereich – etwa auf einem Parkplatz, einer Kantine oder in einer Eingangshalle.

Über die Vergabe von bestimmten Kategorien lässt sich dabei die Anzahl an Personen je nach Zuordnung steuern. Die weitere Lizenzerweiterung „Online-Abfrage der Zählfunktion“ erlaubt darüber hinaus die Anzeige des aktuellen Zählerstands online über einen Link, ohne dass sich der Nutzer extra im System anmelden muss.

Das klingt auf den ersten Blick kompliziert, ist es aber nicht, wie Sebastian Seisser, Productmanager Scala bei Assa Abloy, erklärt: „Die Lizenzerweiterung bekommt der Kunde von uns ganz bequem als Datei geliefert, die er ganz normal in sein bestehendes Scala-System hochladen kann. Für den Raum, den er dann überwachen möchte, muss lediglich ein Eintritts- und Ausgangsleser definiert werden.“ Sobald das geschehen ist, lassen sich pro Controller bis zu 32 Zähler verwalten. Im Dashboard sind alle Personenzahlen übersichtlich auf einen Blick erfasst. „Zusätzlich lassen sich auch Grenzwerte, Warnschwellen und Reset-Zeitpunkte unkompliziert festlegen. Sobald ein Grenzwert an Personen in einem definierten Kontrollbereich überschritten wird“, so Seisser weiter, „bleibt die Tür geschlossen, auch wenn die betreffende Person prinzipiell über eine Zutrittsberechtigung verfügt“. ■

Kontakt

Assa Abloy Sicherheitstechnik GmbH
Berlin
Tel.: +49 30 8106 0
berlin@assaabloy.com
www.assaabloy.de



▲ **Das Zutrittskontrollsystem Scala Net wächst mit den Bedürfnissen der Kunden mit und hält neben der Zählfunktion auch viele weitere Lizenzerweiterungen und zusätzliche Funkionalitäten bereit**

Axis: Philippe Kubbinga wird Regional Director

Philippe Kubbinga wird neuer Regional Director Middle Europe

Philippe Kubbinga übernimmt die Leitung der Axis-Geschäfte in Deutschland, Österreich, der Schweiz, Liechtenstein, den Niederlanden, Belgien und Luxemburg als neuer Regional Director Middle Europe. Er folgt auf Edwin Roobol. Philippe Kubbinga kam 2015 als Regional Director Middle East and Africa zu Axis. In seiner internationalen beruflichen Laufbahn hat er in verschiedenen Managementpositionen bei Sony Ericsson, Nokia und Microsoft in Europa, Asien und Südafrika gearbeitet, bevor er 2010 nach Dubai ging. Philippe Kubbinga wird von der Geschäftsstelle in Rotterdam aus tätig sein. Edwin Roobol wird die neu geschaffene Position des Director Marketing EMEA übernehmen. Mit seinem Fachwissen und seiner langjährigen Erfahrung bei Axis wird er auf EMEA-Ebene das Marketing strategisch weiterentwickeln und die Kompetenzen der EMEA-Vertriebsregionen bündeln.

www.axis.com ■

BKA: Cybercrime in Deutschland nimmt weiter zu

100.514 Fälle von Cybercrime im engeren Sinne registrierte die deutsche Polizei in 2019, was einem Anstieg von über 15 Prozent gegenüber der Vorjahreszahl entspricht (2018: 87.106 Fälle). Wie aus dem vom Bundeskriminalamt (BKA) veröffentlichten „Bundeslagebild Cybercrime 2019" hervorgeht, erreicht die Anzahl der polizeilich bekannten Taten damit einen neuen Höchststand. Die Schäden, die durch entsprechende Taten entstehen, seien hoch. So schätzt der Branchenverband Bitkom, dass der Wirtschaft 2019 ein Schaden von über 100 Milliarden Euro durch Cyberangriffe entstanden ist. Neben Wirtschaftsunternehmen sind öffentliche Einrichtungen bevorzugte Ziele der Täter, die sich hier hohe kriminelle Gewinne erwarten. Die größte Gefahr gehe weiterhin von Angriffen sogenannter Ransomware aus. Diese Software verschlüsselt die Daten auf dem angegriffenen Rechner. Für deren Entschlüsselung fordern die Täter meist einen Geldbetrag, der in der Regel mit Bitcoins zu entrichten ist.

www.bka.de ■

Denios beruft Ricarda Fleer in den Vorstand

Ricarda Fleer, CFO bei Denios

Der Aufsichtsrat von Denios hat eine Neuzuordnung der Vorstandsressorts beschlossen und Ricarda Fleer als weiteres Vorstandsmitglied berufen. Die gebürtige Bielefelderin übernimmt die Position als Chief Financial Officer (CFO). Internationale Erfahrung sammelte Ricarda Fleer zuletzt als CFO bei Viessmann Industrial Solutions in Allendorf (Eder). In ihrer neuen Funktion bei Denios trägt sie Verantwortung für die Bereiche Finance und Controlling, Human Resources und Qualitätsmanagement. Helmut Dennig kümmert sich als Gründer und Vorstandsvorsitzender weiterhin vorrangig um strategische und gesellschaftsrechtliche Fragen.

www.denios.de ■

Thomas Taferner, Leiter strategischer Vertrieb und Marketing bei Telenot Electronic ▲

SICHERHEITSMANAGEMENT

Partner fürs Leben

Alarm, Brandschutz, Zutritt – Telenot setzt auf Eigenentwicklung und intensive Partnerschaften

Telenot, Hersteller für elektronische Sicherheitstechnik und Alarmanlagen, blickt auf eine beachtliche Geschichte zurück – und hat sich immer wieder verjüngt. Das Portfolio umfasst heute neben der Einbruchmeldetechnik ein umfassendes Lösungsangebot in den Bereichen Brandschutz und Zutritt. Neu gegründet wurde die Firma Telenot Smart Services – außerdem hat das Unternehmen den Marketing-Support für seine Fachpartner erheblich ausgebaut. Matthias Erler von GIT SICHERHEIT hat darüber mit Thomas Taferner, Leiter strategischer Vertrieb und Marketing bei Telenot Electronic, gesprochen.

GIT SICHERHEIT: Herr Taferner, Telenot gehört zu den bekanntesten Unternehmen der Branche – ursprünglich vor allem im Bereich Einbruchmeldetechnik. Sie haben aber Ihr Sortiment in den letzten Jahren ganz erheblich ausgeweitet. Welche Strategie steht dahinter – und wie gehen Sie hier vor?

Thomas Taferner: Die Telenot hat sich während der mehr als 50 Jahre ihres Bestehens einen starken Namen in der elektronischen Sicherheitstechnik gemacht. Am Anfang stand die Übertragungstechnik für Alarme – Thema waren die Erfüllung der sich weiterentwickelnden Normen, die fortlaufende Anpassung an sich verändernde Netztopologien, sichere Protokolle etc. Über die Jahre haben wir die Einbruchmeldetechnik ergänzt, sind damit weiter gewachsen mit unseren Melderzentralen und der dazugehörigen Peripherie wie etwa Lichtvorhängen und Bewegungsmeldern, uvm. Wir haben uns zu einem der führenden Anbieter entwickelt und betreuen mit unseren Fachbetrieben praktisch nahezu jedes DAX-Unternehmen. Auch im Handel sind wir sehr stark – Edeka, Rewe, Decathlon und Hagebaumarkt zählen beispielsweise zu unseren Kunden. Wir haben über die Jahre sehr viel investiert, auch in die Kontakte zu unseren Errichtern und Fachbetrieben sowie in ihre Ausstattung mit innovativen Produkten. Schulungen und Service gehören dazu. Wenn der Errichter bei seinem Kunden vor Ort auf der Leiter steht und ein Problem hat, sind wir da, um ihm zu helfen. In den vergangenen etwa 15 Jahren haben wir diese Entwicklung logisch konsequent ausgebaut: Wir haben uns klar gemacht, welches enorme Wissen sich unsere Errichter nach und nach aufgebaut haben, die VdS-Zulassungen beispielsweise.

◀ **Eine der Telenot-Produktionsstätten: Das Unternehmen erreicht eine Produktionstiefe von 90 Prozent im eigenen Haus – inklusive aller Prüfprozesse**

Professionelle Brandmeldetechnik von Telenot – hier das Brandmeldesystem Hifire 4000 ▶

Wir haben festgestellt, dass sie die idealen Ansprechpartner für Planungsbüros, Architekten und überhaupt alle sind, die bei ihren Planungen mit Sicherheitstechnik in Berührung kommen. Sie sind hochqualifizierte regionale Fachbetriebe, haben das aber sehr häufig einfach nicht richtig kommuniziert. Hier setzen wir mit unserer Unterstützung an – etwa durch die Etablierung Autorisierter Telenot-Stützpunkte auf dem Markt, deren Unterstützung durch geeignete regionale Vertriebs-und Werbeunterlagen, deren Förderung durch nationale Marketingkampagnen im TV-, Print- oder Onlinebereich und durch die Aufbereitung von Beratungswissen, zugeschnitten auf bestimmte Zielgruppen. So haben wir Telenot zur nationalen Marke mit einem umfassenden Lösungsprogramm zum Schutz von Menschenleben, Gebäuden, Sachwerten und Produktionsanlagen ausgebaut, bei dem alles aus einer Hand erhältlich ist und zuverlässig zusammenpasst.

Lassen Sie uns einen näheren Blick auf die neuen Standbeine Brandschutz und Zutrittskontrolle werfen, die Sie in den letzten Jahren aufgebaut haben. Recht neu ist ja der Brandschutz – was gehört alles zu Ihrem Portfolio?

Thomas Taferner: Dieser Verbreiterung unseres Portfolios liegt eine bewusste strategische Entscheidung zugrunde, die wir vor einigen Jahren getroffen haben. Dabei haben wir definiert, zu welchen Wachstumsmärkten wir mit unseren Fachbetrieben und Serviceleistungen einen guten Zugang haben. Da unsere Fachbetriebspartner ja nicht nur im Einbruchschutz, sondern auch in den Themen Zutritt und Brandschutz zuhause sind, überlegten wir uns, was wir seitens Telenot davon selbst, in Kooperation oder durch Firmenzukäufe entwickeln und anbieten können. Vor etwa vier Jahren startete dann unsere Kooperation mit Panasonic in der Brandmeldetechnik. Für die DACH-Staaten sind wir ein idealer Partner für Panasonic. Wir haben seitdem viel gemeinsame Entwicklungszeit investiert, die Telenot-Qualitätsphilosophie implementiert und sind zunächst in den deutschen Markt eingestiegen. Es folgen jetzt zunächst die Schweiz, dann Österreich und Luxemburg, wo wir jeweils mit sämtlichen relevanten Zulassungen ausgestattet sind.

Der Brandschutz entwickelt sich offenbar als neue Telenot-Erfolgsgeschichte…

Thomas Taferner: Das ist in der Tat so. 2018 haben wir unsere Schulungstour gestartet, an denen seither mehrere Hundert Fachbetriebe teilgenommen haben. Wir sind seit etwa zweieinhalb Jahren damit beschäftigt, diesen Markt mit Vertrieb, Hotline und Schulungsangeboten zu bearbeiten. Parallel dazu informieren wir die Planungsabteilungen unserer Kunden sowie Planungsbüros über unser Portfolio – und wir haben uns schon einen guten Ruf auf diesem Gebiet erarbeitet. Die professionelle Brandmeldetechnik mit dem Brandmeldesystem Hifire 4000 und Rauchansaugsystem RAS Grizzle entwickelt sich so als solides zweites Standbein. Gerade gewerbliche Endkunden fragen neben Einbruchmeldetechnik auch unser Angebot im Bereich Brandschutz und Zutritt nach.

… womit wir bei Ihrem dritten Standbein wären, dem Zutritt…

Thomas Taferner: Den Bereich Zutrittskontrolltechnik haben wir durch den Zukauf eines Unternehmens, aufgebaut. Mit der

Bitte umblättern ▶

◀ **Seit Juni 2020 bietet Telenot Schulungen für sein neues Zutrittskontrollsystems Hilock 5000 ZK an**

Einführung des neuen Zutrittskontrollsystems Hilock 5000 ZK starteten wir Ende Juni dieses Jahres – mit Schulungen in Deutschland, Österreich und der Schweiz. Wir konnten bereits mehr als 500 Fachbetriebe in der Auftaktschulungstour begrüßen, mit denen wir nun Schritt für Schritt in diesen vielversprechenden Markt einsteigen wollen. Unser Vorteil liegt dabei vor allem auch darin, dass wir die Systemkompetenz und das Beratungswissen für Einbruchschutz, Brandschutz und Zutrittssysteme gemeinsam anbieten können, denn diese Gewerke werden immer mehr zusammengedacht und -geplant. Mit unseren Gefahrenmelderzentralen Hiplex, dem Zutrittskontrollsystem Hilock und dem Brandmeldesystem Hifire haben wir die Weichen für die Zukunft gestellt.

Worauf legen Sie bei Ihrer Entwicklung vor allem Wert?

Thomas Taferner: Alle unsere Produktlösungen sind in hohem Grade abwärtskompatibel. Das garantiert den Kunden eine hohe Investitionssicherheit – und unsere Kunden können langfristig mit Lieferkapazität, Service, Wartung, etc. rechnen. Diese Nachhaltigkeit ist für uns entscheidend. Auch unser breites Schulungsangebot gehört dazu: Wir schulen in der Regel zwischen 4000 und 6000 Teilnehmer jedes Jahr. Die Rückmeldungen dort und generell aus dem Kundenkontakt fließen wiederum in die Entwicklung ein. Ein weiterer Punkt ist, dass wir bei der Entwicklung und Konstruktion der Hardware bereits an die Reibungslosigkeit des Montageerlebnisses denken. Der Errichter und Fachbetrieb spart mit unserem neuen Gehäusekonzept in erheblichem Maße Arbeitszeit und Geld. Diese Vorteile sieht so Mancher nicht auf den ersten Blick, bezahlt dies jedoch teuer bei der Installation, mit mehr Zeitaufwand und dann Geld. Von Telenot erhält der Kunde hinsichtlich Lebensdauer, Zuverlässigkeit der Installation insgesamt eine der besten Systemlösungen überhaupt. Wir werten zudem quartalsweise die Qualität unserer Produkte aus, indem wir die Zahl der verkauften Artikel und die Zahl der Beanstandungen miteinander vergleichen. In 99,49 Prozent gibt es keine Beanstandung. Wichtig bei der Entwicklung ist außerdem, das Know-how bei uns im

Bitte umblättern ▶

Marketing-Unterstützung

▲ **Telenot unterstützt seine Facherrichter u. a. mit Vertriebs- und Werbeunterlagen – wie etwa mit diesen Beilegern** ▶

Marketing-Unterstützung – etwa in Form von nationale Marketingkampagnen im TV-, Print- oder Onlinebereich ▲

WILEY

VIRTUAL SHOW

Wiley Industry Days

WIN DAYS

16.–19. November 2020

VIRTUELLE SHOW mit Konferenz, Ausstellung und Networking für die Branchen der Automatisierung, Machine Vision und Sicherheit.

Besuchen Sie unsere Aussteller und Partner auf dem virtuellen Branchentreff

VIRTUAL SHOW with conference, exhibition and networking for the automation, machine vision and safety & security industries.

Visit our exhibitors and partners at the virtual industry show

JETZT REGISTRIEREN
REGISTER NOW

www.WileyIndustryDays.com

GRUNDIG advancis neovo FORSCHUNGS CAMPUS ASSA ABLOY BALLUFF CES deister electronic

Edmund optics worldwide emva Europa-Universität Flensburg EVVA Fraunhofer VISION Genetec GEUTEBRUCK GEZE gom

HIKVISION igus IPS milestone MOBOTIX optris pcs Polytec Qognify

Simons Voss technologies spectronet TURCK UBiMAX VDMA VIDEOR visionLib WAGNER wanzl Z-LASER ZVEI

messtec drives Automation inspect inspect award 2021 GIT SICHERHEIT + MANAGEMENT GIT SICHERHEIT AWARD GIT SECURITY EMEA GIT SECURITY AWARD

Haus zu behalten – wir haben aktuell 40 eigene Entwicklungsingenieure, welche auch in unsere aktiven Kooperationen eingebunden sind. Damit sind wir immer sehr gut gefahren. Wir haben auch festgestellt, dass für unsere Systeme und Lösungen derart viel fachspezifisches Wissen nötig ist, das wir über viele Jahre hinweg kumuliert haben, dass es einfach keinen Sinn macht, etwa Softwareprogrammierung extern zu vergeben. Wir kooperieren aber auch mit den sehr guten Hochschulen in unserer Region.

Sie haben gerade das Zutrittskontrollsystem Hilock 5000 ZK eingeführt. Was sind die wesentlichen Merkmale und Features?

Thomas Taferner: Zunächst einmal ist das eine voll marktfähige, hochmoderne, sehr leistungsfähige, modulare und skalierbare Lösung, mit der jedes Projekt realisierbar ist – vom Kleinanwender bis zum großen Industriebetrieb – dank webbasierter Zutrittsverwaltung auch über verschiedene Standorte hinweg. Der Kunde kann klein einsteigen und durch Lizenzerweiterungen sein System beliebig erweitern. Dahinter steht die Einsicht, dass wir es bei jedem Gebäude mit einem hochindividuellen Projekt zu tun haben. Deshalb bieten wir intensive Beratung und ein modulares Baukastensystem, das auf unterschiedlichste Kundenbedürfnisse konkret eingehen kann.

Bislang ist ja die Videotechnik nicht in Ihrem Portfolio enthalten. Wäre das nicht zumindest bei Alarm und Zutritt ein naheliegendes Thema?

Thomas Taferner: Das ist durchaus Teil unserer langfristigen strategischen Überlegungen – derzeit ist das aber noch nicht spruchreif. Entscheidend ist dabei die Integration aller Schnittstellen zwischen Zutritt und Einbruchmeldetechnik.

Die Produktion Ihrer Systeme befindet sich in Deutschland? Es gibt ein neues Produktions- und Logistikgebäude?

Thomas Taferner: Das stimmt. 2019 haben wir es in Betrieb genommen und dabei alle Prozesse und Produktionsabläufe neu strukturiert. Ebenfalls 2019 haben wir unser neues Ausbildungszentrum in Aalen-Hammerstadt eingeweiht. Wir haben überhaupt in den letzten Jahren sehr viel gebaut – 2011 für die Entwicklung, 2013 kam ein neues vierstöckiges Produktionszentrum in Hammerstadt, Einweihung der neuen Produktionsstätte für Metall- und Kunststoff-Fertigung Werk II in Essingen, 2016 eine Kita und 2017 ein neues Vertriebsgebäude in Hammerstadt. Was die Produktion in Deutschland betrifft: Wir erreichen hier eine Produktionstiefe von 90 Prozent im eigenen Haus – inklusive aller Prüfprozesse. Dadurch sind wir sehr beweglich und können eine sehr hohe Lieferverfügbarkeit anbieten.

Herr Taferner, ein weiterer wichtiger Schritt bei Telenot war die Gründung der Firma Telenot Smart Services. Damit im Zusammenhang steht die neue Digitalplattform Hixserver – zur intelligenten Gebäudesicherheit und -steuerung. Könnten Sie uns das bitte einmal erläutern?

Thomas Taferner: In allen Übertragungseinrichtungen gibt es fortan die Option, einen Secure-Baustein (ECC-Verfahren mit 384 Bit) in Form einer CXK-Platine zu integrieren, welche für den verkrypteten und zertifikatsbasierten, hochsicheren Verbindungsaufbau zwischen Nutzerseite und Objekt sorgt. Immer wenn eine Verbindung aufgebaut wird, nutzt die Digitalplattform Hixserver eben für die Kommunikation die hochsichere Verschlüsselung TLS (Trnsport Layer Security) mit beidseitig zertifikatsbasierter Authentifizierung. Hat der sichere Handshake stattgefunden wird ein zweiter 128 AES verschlüsselter Kanal aufgebaut – der Steuerungskanal für den verschlüsselten Zugriff auf das System Ende zu Ende. Eine Cloud kommt dabei nicht ins Spiel. Für den Errichter ergibt sich damit die Möglichkeit, seine installierten Anlagen wie mit einer Objektverwaltungssoftware hochsicher zu verwalten. Er kann seinen Kunden damit einen Remote-Service und schnelle Störungsbeseitigung anbieten – hochsicher, dokumentiert und minutengenau abrechenbar. Das ist Sicherheit 4.0 und ein neues, zukunftsfähiges Geschäftsmodell. Dem Endkunden wird gleichzeitig eine hochsichere Plattform geboten mit Remote-Steuerungsmöglichkeiten. Damit garantieren wir nicht nur die geprüfte Sicherung des Gebäudes selbst durch die Hardware, die anerkannten Einbruch- und Brandmeldesysteme von Telenot, sondern wir garantieren dem Kunden den sicheren Zugriff auf das System, ohne der Gefahr zu unterliegen, gehackt oder manipuliert zu werden. Ebenso ist jegliches Datenfishing ausgeschlossen, da sich keine Daten über das Gebäude, den Anlagenzustand und das Nutzungsverhalten im Netz befinden. Niemand hört hier mit, niemand steuert mit und niemand kann hier reinsehen.

> „Wir haben bislang den Eindruck, dass zumindest das Handwerk insgesamt sehr gut durch die Krise kommt.“

Daran anknüpfend: Sie betreiben ja schon seit vielen Jahren einen ganz besonderen weitgehenden Verkaufs-Support für Ihre Errichter. Wie sieht diese Beratung und Unterstützung genau aus und wie ist sie organisiert?

Thomas Taferner: Wir haben festgestellt, dass die meisten Errichter und Fachbetriebe nicht die Zeit und die Ressourcen haben, mit ihren Angeboten und ihren USPs zu werben, obwohl sie hervorragend aufgestellt sind – einschließlich aller Prüfungen, Nachweisen, Zertifikaten und Referenzen. Sie könnten sich erheblich besser positionieren – nicht nur bei den Bauträgern, Planungsbüros, sondern auch bei gewerblichen und industriellen Endkunden aus ihrer Region. Dabei unterstützen wir sie intensiv. Das sind umfassende Marketingtools von Broschüren bis hin zu vorbereiteten Mailings und zeitlich gestaffelten Musteranschreiben inklusive Logo. Unsere Partner bekommen genaue Reihenfolgen und Vorgaben, so dass er selber kaum noch etwas selber auszuarbeiten braucht. So etwas gibt es in diesem Umfang aus meiner Sicht nur von Telenot und von keinem anderen Anbieter.

Wie verändert sich dieser Support durch die Corona-Pandemie?

Thomas Taferner: Wir haben bislang den Eindruck, dass zumindest das Handwerk insgesamt sehr gut durch die Krise kommt. Das war nach einer ersten kleinen Schockstarre im März auch bei uns so. Wir hatten uns innerhalb von zwei Wochen gut organisiert, die Vorgaben und unser Hygienekonzept umgesetzt. Oberste Priorität für uns war und ist die Lieferverfügbarkeit. Produktion und Versand haben wir aus Hygienegründen streng voneinander getrennt. Eine Zeit lang haben wir durch all das ein paar PS verloren – inzwischen läuft aber alles wieder normal. Vieles läuft heute verstärkt online – etwa in Form von Webinaren oder e-Learning. ■

Kontakt

Telenot Electronic GmbH
Aalen
Tel.: +49 7361 946 451
thomas.taferner@telenot.de
www.telenot.de

GIT CYBER SECURITY

INNENTITEL

HEFT IM HEFT

Mit Innentitel: Tüv Süd
Kernelemente des Datenschutzes

Seite 34

DATENSCHUTZ

Kernelemente des Datenschutzes

Ein Beitrag von Mareike Vogt von der Tüv Süd Sec-IT

Kleinen und mittleren Unternehmen (KMU) fehlt meist das Fachpersonal, um die Anforderungen zum Datenschutz zu identifizieren und umzusetzen. Gleichzeitig steigen technischen Möglichkeiten, gegen die ein Unternehmen seine Daten sichern muss. Wie lässt sich diese Herausforderung meistern? Mareike Vogt, Fachexpertin für Datenschutz bei der Tüv Süd Sec-IT, erklärt, wie Datenschutz rund um die drei Säulen Mensch, Technik und Prozesse auch für KMU funktioniert.

Längst basieren ganze Geschäftsmodelle darauf, Geld mit den Daten anderer Menschen zu machen. Von einem Thema am Rande, über das lediglich Experten diskutierten, avancierte der Datenschutz im letzten Jahrzehnt daher zu einem zentralen Bereich moderner IT-Sicherheit. Im Zuge dieser Aufklärung über die Gefahren unzulänglicher Datenverarbeitung gibt es auf internationaler Ebene unterschiedliche Regulierungen, um die Bürger besser gegen Missbrauch ihrer personenbezogenen Daten zu schützen – in Europa ist es die Europäische Datenschutz-Grundverordnung (EU-DSGVO).

Gleichzeitig stellen die von jedem Nutzer gesammelten Informationen einen wertvollen Rohstoff für Unternehmen aller Art dar, unter anderem in Form von Kundenkontakten oder zur Datenanalyse. Sie sind zu einem wichtigen Aspekt für betriebswirtschaftliche oder strategische Entscheidungen geworden. Wie schaffen aber vor allem kleinere und mittlere Unternehmen (KMU), die besonders unter einem Mangel an Fachkräften leiden, den Spagat zwischen dem Interesse an Daten und Datenschutzkonformität? Eine einfache und effektive Lösung für einen Fachkräftemangel, kann die Unterstützung durch einen unabhängigen externen Berater im Datenschutz darstellen. Gerade bei KMUs bietet es sich sogar an, die Aufgabe des Datenschutzbeauftragen durch externen Fachexperten übernehmen zu lassen. Gemeinsam sollte man sich dann an den drei Säulen des Datenschutzes orientieren.

Faktor Mensch

Die erste Säule, auf die sich EU-DSGVO-konformer Umgang mit personenbezogenen Daten stützt, ist der Mensch. Mitarbeiter, die im Unternehmen mit personenbezogenen Daten zu tun haben, müssen geschult werden. Es muss ein Bewusstsein geschaffen werden, welche Anforderungen zum Datenschutz an die Mitarbeiter und ihre Arbeit bestehen und welche Strafen dem Unternehmen bei Missachtung drohen. Ab einer bestimmten Größe – 20 Mitarbeitende, die regelmäßig mit der automatisierten Verarbeitung personenbezogener Daten befasst sind – müssen Unternehmen in Deutschland zudem einen Datenschutzbeauftragten benennen. Dieser berät nicht nur zielgerichtet, sondern kontrolliert die Einhaltung der EU-DSGVO im Unternehmen und dient als Ansprechpartner für zuständige Aufsichtsbehörden. Dieser Datenschutzbeauftragte fungiert als erste Anlaufstelle für Datenschutzanliegen, muss aber nicht im Unternehmen selbst beschäftigt sein. Unabhängige Dienstleister wie Tüv Süd bieten deshalb nicht nur Mitarbeiterschulungen zum Datenschutz an, sondern können auch den externen Datenschutzbeauftragten stellen.

> „Wer das Vertrauen der Kunden in sein Unternehmen gewinnen und erhalten möchte, kommt seit einigen Jahren nicht mehr am Datenschutz vorbei.“

Mareike Vogt, Fachexpertin für Datenschutz bei der Tüv Süd Sec-IT

© pickup – Stock Adobe

Faktor Prozesse

Als zweite Säule gilt es, die internen Prozesse zur personenbezogenen Datenverarbeitung an die Anforderungen der EU-DSGVO anzupassen. Das beginnt bei der Sammlung solcher Daten, beispielsweise über die eigene Webseite. Zwar ist es möglich, Nutzerdaten mittels Cookies zu erfassen, allerdings muss der Nutzer vorher oftmals einwilligen. Das passiert über Cookie-Banner, die dem Nutzer beim Besuch der Seite angezeigt werden müssen. Welche Informationen darin enthalten sein müssen und wann eine Einwilligung rechtens ist, regelt die EU-DSGVO. Ergänzend helfen Gerichtsurteile sowie Aufsichtsbehörden bei der Auslegung. Eine unabhängige Beratung kann auch hier helfen, Fallstricke zu erkennen und zu vermeiden.

Faktor Technik

Die dritte Säule des Datenschutzes ist die Technik. Sie beinhaltet die angemessene und sichere Verarbeitung der Daten. Wie stark die durch die EU-DSGVO geforderte Sicherheit der Verarbeitung sein muss, ergibt sich unter anderem anhand einer objektiven Bewertung der Daten und Risiken. Es sollte daher eine Abwägung zwischen dem Schutzbedarf der Daten und den möglichen Sicherungsmaßnahmen getroffen werden. Da sich technische Möglichkeiten stets weiterentwickeln, ist es sehr wichtig, dass diese Abwägungen regelmäßig überprüft und angepasst werden. Nur so wird sichergestellt, dass die Sicherheit der Verarbeitung langfristig angemessen bleibt.

Kein Vertrauen ohne Datenschutz

Wer das Vertrauen der Kunden in sein Unternehmen gewinnen und erhalten möchte, kommt seit einigen Jahren nicht mehr am Datenschutz vorbei. Er gilt heute als Qualitätssiegel. Die drei Säulen des Datenschutzes, Mensch, Prozesse und Technik, bieten eine gute Orientierung, um diese Herausforderung erfolgreich zu meisten. Unternehmen, deren eigene Personalressourcen begrenzt sind, finden die passende Unterstützung bei externen Fachexperten. Denn Strafen sind nicht nur schlecht fürs Image, sondern können auch schnell teuer werden. ■

Kontakt

Tüv Süd AG
München
Te.l: +49 89 5791 0
info@tuev-sued.de
www.tuev-sued.de

CYBER SECURITY

Keine Entspannung

Kriminelle Wertschöpfungsketten: Zum Stand der Cyberbedrohung der deutschen Wirtschaft

© oz - stock.adobe.com

Beim Thema Cybersecurity fangen die deutschen Unternehmen nicht von Null an: Sie haben kräftig investiert in IT-Sicherheit – in Technik, Prozesse und Personal. Das hat den Schutz vor Cyberkriminalität zwar verbessert – andererseits steigt die Zahl der erfolgreichen Hackerangriffe. „Das Bewusstsein ist mittlerweile vorhanden, bei der konsequenten Umsetzung von Abwehrmaßnahmen besteht noch Handlungsbedarf, aber auch der Staat muss nachlegen", sagt ASW-Vorstandsvorsitzender Volker Wagner im Gespräch mit GIT SICHERHEIT.

GIT SICHERHEIT: Herr Wagner, als wir uns vor rund vier Jahren hier in der GIT SICHERHEIT über die aktuelle Gefährdungslage der deutschen Wirtschaft unterhielten, diagnostizierten Sie sehr klar eine Zunahme der Cyber-Bedrohung. Angriff und Abwehr beschrieben jeweils ansteigende Kurven, wobei aber die Angriffskurve steiler sei… Würden Sie das heute wieder so formulieren?

Volker Wagner: Ich würde gerne etwas anderes sagen, aber leider ist die Situation nicht besser geworden. Bei der Cybersicherheit erlebe ich nach wie vor, dass die Schere weiter auseinandergeht. Beispielsweise zeigt eine aktuelle Studie des Bitkom auf, dass 2019 drei von vier deutschen Unternehmen Opfer von Sabotage, Datendiebstahl oder Spionage waren. Ende September hat das BKA das aktuelle Lagebild zum Cybercrime veröffentlicht und die Fakten sprechen auch hier eine eindeutige Sprache. 2019 wurde eine Zunahme von Cybercrime um 15 % auf über hunderttausend Fälle registriert. Zudem gab es im letzten Jahr ca. 114 Mio. neue Malware-Varianten. Das BKA zieht dabei u. a. folgendes Fazit: Die Professionalität von Cyberkriminellen steigt weiter an. Cybercrime erschafft und basiert auf kriminellen Wertschöpfungsketten. Ransomware und DDoS-Angriffe sind die größten Bedrohungen. Von einer Entspannung der Situation können wir daher nicht sprechen.

Ist denn das Bewusstsein für diese Problematik in den Unternehmen aus Ihrer Sicht spürbar stärker ausgeprägt – und zieht man die richtigen Schlüsse daraus?

Volker Wagner: Es ist wahnsinnig viel gemacht worden, darauf kann man auch stolz sein. Die großen Unternehmen haben alle ihre IT-Sicherheitsabteilungen ausgebaut und

sachkundiges Personal eingestellt, Prozesse etabliert und neue Technik eingesetzt. Da ist wirklich viel Geld investiert worden. Und der Schutz ist auch deutlich besser als noch vor fünf oder zehn Jahren. Aber die Bedrohungslage hat sich im gleichen Zeitraum extrem verschärft. Mittlerweile sind fast unglaubliche eine Milliarde Varianten von Schadprogrammen im Umlauf. Gleichzeitig stellen wir im Rahmen der Digitalisierung von Wirtschaft und Gesellschaft immer mehr Geräte ins Internet. Je mehr Systeme miteinander vernetzt und ans Internet angeschlossen werden, desto mehr Angriffsfläche bietet sich. Es ist daher auch logische Konsequenz, dass die Anzahl von erfolgreichen Hackerangriffen steigt. Im gerade veröffentlichten Allianz Risk Barometer ist Cybercrime erstmals das am höchsten bewertete Risiko für die Wirtschaft. Das Bewusstsein ist also mittlerweile vorhanden, bei der konsequenten Umsetzung von Abwehrmaßnahmen besteht noch Handlungsbedarf.

Sie sehen sich beim ASW Bundesverband an der Schnittstelle von Staat und Wirtschaft – und gerade jüngst äußerten Sie sich sowohl lobend als auch kritisch bezüglich des geplanten IT-Sicherheitsgesetzes. Derzeit ist wohl der dritte Entwurf in Arbeit…?

Volker Wagner: Die ersten beiden Entwürfe haben wir von der ASW – wie auch einige andere Verbände – zum Anlass genommen, mit unseren Positionspapieren auf entscheidende Verbesserungspotenziale hinzuweisen. Wir erwarten nun den dritten Entwurf und damit den Start der Novelle des IT-Sicherheitsgesetzes noch in diesem Herbst. Nach meiner Kenntnis ist ein Kabinettsbeschluss noch für dieses Jahr vorgesehen und die Verabschiedung im Bundestag für Anfang nächsten Jahres geplant. Selbstverständlich werden wir uns im politischen Diskurs für die wichtigen Punkte aus Sicht der Wirtschaft einsetzen. Dabei möchte ich unterstreichen, dass wir die Novelle ausdrücklich befürworten. Uns geht es mit unseren Punkten darum, die Qualität und Praktikabilität zu erhöhen.

Sie sehen neben den Unternehmen selbst den Staat in der Pflicht, wenn es um „Cyberresilienz" geht. Überhaupt haben Sie ja zu dem Fragenkomplex der Aufgabenteilung zwischen Staat und Wirtschaft bei der Bekämpfung von Cyberkriminalität vor einiger Zeit sogar ein Positionspapier vorgelegt. Was kann denn, in groben Zügen formuliert, der Staat realistischerweise mehr leisten als bisher?

Volker Wagner: Hier sehen wir schon noch deutliches Verbesserungspotenzial. Beispielsweise bedarf es einer Meldepflicht für kritische Schwachstellen in Software und eine Verpflichtung für Software-Updates sowie Haftung bei Nicht-Behebung. Derzeit gibt es keine Haftung für fehlerhafte Software. Es sollte jedoch ein Haftungsanspruch entstehen, wenn bekannte Schwachstellen und Fehler nicht behoben werden.

Es sollte eine Novelle des Produkthaftungsrechts erfolgen, durch die Soft- und Hardwarehersteller gesetzlich verpflichtet werden, für sicherheitskritische Schwachstellen tatsächlich auch zeitnah Sicherheits-Updates bereitzustellen und bei Unterlassung in Haftung genommen werden können. Ebenso müssen Hersteller verpflichtet werden, Transparenz über den jeweiligen Lebenszyklus von softwarebasierten Produkten zu schaffen. Produkte, deren bekannte Schwachstellen nicht vom Hersteller bereinigt wurden, müssen kenntlich gemacht werden. Ebenso sind Verfahren zu definieren, wie mit Software, die ihren End-of-life-Zeitpunkt erreicht hat, umzugehen ist. Veraltete Software, die nicht mehr unterstützt wird, bietet eine große Angriffsfläche. Die Haftung könnte nach diesem Leitgedanken geregelt werden: Hersteller und Betreiber haften für unterlassene Software-Updates, Verbraucher haften für nicht eingespielte Patches, Restrisiken werden über Risikogemeinschaften in Cyberversicherungen abgedeckt.

Darüber hinaus muss sich die Bundesregierung im Rahmen der Cyberaußenpolitik dafür einsetzen, dass jeder Staat seine Bemühungen zur Erhöhung der Cybersicherheit intensiviert und kritische IT-Infrastrukturen besser gegen Attacken geschützt werden sowie intensiv gegen Cyberkriminalität vorgegangen wird. Mittelfristiges Ziel muss die Verabschiedung eines verbindlichen Abkommens für verantwortliches Handeln im Cyberraum sein.

In der Praxis bleibt für einzelne Unternehmen oft unklar, welche Sicherheitsbehörde mit welchen Kompetenzen ausgestattet ist und wie die Aufgaben zwischen Bundes- und Landesämtern abgegrenzt sind. Im konkreten Angriffsfall wird es gerade für kleine und mittelständische Unternehmen zunehmend von Bedeutung sein, dass auch die örtliche Polizeibehörde im Sinne eines Ersthelfers in die Lage versetzt wird, die richtigen Stellen in eine Strafverfolgung einzubeziehen.

Sie wünschen sich bei staatlichem Handeln im Rahmen des künftigen IT-Sicherheitsgesetzes mehr Transparenz für die jeweils betroffenen Unternehmen. Was genau stellen Sie sich vor?

Volker Wagner: Besorgniserregend ist, dass trotz Einführung des ersten IT-SiGe 2015 die

> **Die Bundesregierung muss sich im Rahmen der Cyberaußenpolitik dafür einsetzen, dass jeder Staat seine Bemühungen zur Erhöhung der Cybersicherheit intensiviert und kritische IT-Infrastrukturen besser gegen Attacken geschützt werden."**

Volker Wagner ist Head of Security bei der BASF Group sowie Vorstandsvorsitzender des ASW Bundesverbands (Allianz für Sicherheit in der Wirtschaft)

Bitte umblättern ▶


© xiaoliangge - stock.adobe.com

Bedrohungslage weiter gestiegen ist. Deswegen ist es umso wichtiger, dass bei der Novellierung auf den Erfahrungen der letzten vier Jahre aufgebaut wird. Wir fordern weiterhin den Austausch über eindeutige quantitative und qualitative Schwellenwerte zu Meldepflichten. Vorteilhaft wäre es hier, nicht nach Trial and Error vorzugehen, sondern dazu aus den bisherigen praktischen Erfahrungen zu den Meldungen aus den aktuellen Kritis-Sektoren zu lernen.

Der in der Novelle des IT-Sicherheitsgesetzes eingeführte Begriff „Unternehmen im besonderen öffentlichen Interesse" führt nicht zu Klarheit, sondern zu Rechtsunsicherheit bei den möglicherweise betroffenen Unternehmen. Die Einführung des Terminus „Unternehmen im besonderen öffentlichen Interesse" ist zu unbestimmt. Insbesondere fehlt eine Benennung konkreter Kriterien, warum eine Infrastruktur und deren Anlagen als „im besonderen öffentlichen Interesse" eingestuft werden.

Behörden sollen, Ihrer Auffassung nach, möglichst privates Know-how und Mitwirken ins Boot holen – zum Beispiel in Form von Public-Private-Partnerships. Haben Sie hier bestimmte Vorbildprojekte im Auge, vielleicht auch aus anderen Ländern?

Volker Wagner: Im Angriffsfall bedarf es einer konkreten Hilfestellung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Es sollte daher über ein Rahmenwerk zur Ergänzung bzw. Erweiterung der mobilen Eingreiftruppen durch Public-Private-Partnerships nachgedacht werden. Dazu gehört auch die Einbindung der Wirtschaft in das Nationale Cyber-Abwehrzentrum und ein Konzept zum gemeinsamen Incident Response von Staat und Wirtschaft. Als Beispiel kann die US National Cyber-Forensics & Training Alliance genannt werden, wo staatliche und privatwirtschaftliche Akteure gemeinsam erfolgreich an der Aufklärung von Cyberattacken und an der Analyse von Tatwerkzeugen arbeiten.

Wie genau könnte so eine Public-Private-Partnership aussehen – und wer genau könnten dabei die Protagonisten sein?

Volker Wagner: Unter den vorgenannten Gesichtspunkten ist es erforderlich, dass das Cyber-Threat-Intelligence-System überdacht wird. Aus dem derzeitigen Gesetzestext geht nicht hervor, dass das BSI dazu verpflichtet sein wird, Cyber Threat Intelligence in Echtzeit auszutauschen. Es muss das Ziel sein, diese Informationen möglichst vielen Unternehmen, nicht nur den Kritis-Betreibern oder Betreibern von Infrastruktur im besonderen öffentlichen Interesse, zukommen zu lassen. Aus diesem Grunde fordert die ASW, eine solche Plattform da anzusiedeln, wo die Ressourcen und das Know-how über Einrichtung und Betrieb von Cyber-Threat-Intelligence-Plattformen besteht. Diese Aufgabe können die zahlreich in Deutschland vorhanden und international angesehenen Cybersicherheitsunternehmen übernehmen.

Welche konkreten hoheitlichen Aufgaben könnten aus Ihrer Sicht durch private Stellen – also beliehene Experten – übernommen werden? Es geht ja immerhin um Attacken aus dem Ausland – ist die Lage hier nicht eine andere, als bei Notar, TÜV & Co. oder bei Sicherheitskontrollen am Flughafen, um ein vielleicht passenderes Beispiel zu nennen?

Volker Wagner: Erforderlich hierfür wäre eine klare Regelung, welche Rolle diese Cybersicherheitsunternehmen als Betreiber der Plattformen einnehmen sollen. Ihre Aufgaben und Befugnisse müssen klar festgelegt werden. Insofern ist die Schaffung einer gesetzlichen Regelung erforderlich, die nachfolgende Aspekte zum Gegenstand haben soll: Erstens: Der Rechtscharakter der Einbindung der Cybersicherheitsunternehmen kann als Beliehenenschaft ausgestaltet sein. Zweitens: Erforderlich ist dann eine Registrierung von Unternehmen, die vom Informationsfluss (z. B. Warnung vor Sicherheitslücken) durch die Plattform profitieren wollen. Drittens: Dem BSI kommt die Rolle der Aufsichtsbehörde zu, worüber Kontroll- und Steuerungsrechte des Staates gewahrt werden.

Herr Wagner, lassen Sie uns noch zum derzeit alles beherrschenden Thema kommen – dem Virus und seinen Folgen. Welche Auswirkungen hatte dies auf die Sicherheitsverantwortlichen in der Wirtschaft?

Volker Wagner: Die letzte Zeit war außergewöhnlich. Die globale Pandemie hat unsere komplette Welt auf den Kopf gestellt. In diesen Wochen und Monaten wurde von unseren Sicherheitsverantwortlichen vieles abverlangt. Vor allem mussten die eigenen Mitarbeiter, Kunden und Geschäftspartner geschützt werden. Dabei galt es, wo möglich, die Produktions- und Dienstleistungsprozesse – häufig unter sehr schwierigen Bedingungen – aufrecht zu erhalten. Dies galt insbesondere für die Unternehmen in den sogenannten systemrelevanten Sektoren oder bei den kritischen Infrastrukturen. Dabei waren viele Aspekte zu beachten und die Sicherheitsverantwortlichen unterstützten die Krisenbewältigung – angefangen bei der Einrichtung eines Notfall- und Krisenstabs, über Verhaltensregeln für das Werks- bzw. Firmengelände oder das Büro und Regulierungen von Geschäftsreisen, bis hin zu Vorschriften für die Parteien der Lieferkette.

Welche Folgerungen ziehen Sie verbandsseitig generell aus den Erfahrungen mit dieser Pandemie?

Volker Wagner: Mit den nun seit Mitte Mai geltenden Lockerungen werden wir mit der Idee einer „neuen Normalität" vertraut gemacht. Das Virus ist hier, um zu bleiben, bis wir einen Impfstoff entwickeln. Also müssen wir einen Weg finden, damit zu leben. Wir haben mittlerweile ein viel besseres Verständnis für die konkrete Bedrohung und sind auch besser in der Lage, die damit verbundenen Risiken einzuschätzen. Es ist nicht länger völlig unbekannt, sondern eher unsichtbar. Wir alle müssen lernen, mit diesem neuen Risiko umzugehen, und das wird für jeden von uns unterschiedlich sein. Für mich bedeutet die sogenannte neue Normalität ein Umdenken, was unser gewohntes Handeln betrifft. Dabei geht es um die Abkehr von festen Planungsprämissen – hin zu sich kontinuierlich verändernden Rahmenbedingungen.

Welche Entwicklungen lassen sich erkennen – nach einem Halbjahr des Lebens mit und in der Krise?

Volker Wagner: Für mich lassen sich durchaus einige starke Trends erkennen, die unseren neuen Handlungsrahmen maßgeblich

beeinflussen werden. Erstens: Auch wenn viele durch die wirtschaftlichen Folgen verlieren, gibt es doch auch Gewinner in dieser ungewissen Zeit. Starke Länder und etablierte Unternehmen haben höhere finanzielle Rücklagen und in der Regel auch robustere Notfall- und Krisenprävention. Sie werden zwar auch Einbußen hinnehmen müssen, aber dürften in ihrer Wettbewerbsposition relativ gestärkt aus dieser Krise hervorgehen.

Zweitens: Existierende politische Spannungen werden durch die Corona-Krise verstärkt. Handelskonflikte nehmen an Brisanz zu, beispielsweise der zwischen den USA und China. Aber auch der schwelende Konflikt in Europa zwischen dem reicheren Norden und dem ärmeren Süden erhitzt sich weiter. Dies zeigt sich innerhalb der EU anhand der Diskussionen zur Neuverschuldung für die wirtschaftlichen Hilfen zur Linderung der Corona-Krise. Zudem missbrauchen totalitäre Staaten Corona zur Ausdehnung von Überwachungsmaßnahmen. Drittens: Die zuvor in Teilen von Wirtschaft und Gesellschaft stockende Digitalisierung nahm rasant an Fahrt auf und überwand dank seiner ungeahnten Beschleunigung viele etablierte Hürden. In Zeiten von Social Distancing wurde digitale Kommunikation eine Notwendigkeit. Home-Office oder virtuelle Konferenzräume zogen in unseren Arbeitsalltag ein und sind nun feste Bestandteile, die bleiben werden. Geschäftsreisen und persönliche Kontakte wurden zu Ausnahmen. Diese Entwicklung wird sich nicht mehr komplett zurückdrehen.

Viertens: Die Führungsstärke ist in der Krise essenziell. Eine klare und konsequente Linie, die als Orientierung in ungewissen Zeiten dient, half allen Beteiligten, die Auswirkungen zu bewältigen. Der österreichische Bundeskanzler Kurz ist hierfür ein Paradebeispiel. Er verdeutlichte, wie wichtig es ist, einen klaren Kopf zu behalten und zeigte, dass ein Weitblick im Handeln unablässig ist. In anderen Ländern nahmen die Regierungschefs die Bedrohung zunächst nicht ernst oder veränderten mehrfach den Kurs. Die hohe Zahl von Erkrankten und viele Todesfälle waren dann die bittere Konsequenz.

Sie haben gerade den Finger auf etwas gelegt, was nicht sofort auffällt: Es geht um den Missbrauch des Themas durch totalitäre Staaten – und zwar die missbräuchliche Überwachung unter dem Deckmantel der Corona-Schutzmaßnahmen. Was genau haben Sie hier im Auge – und inwiefern ist unsere Wirtschaft davon bedroht oder betroffen?

Volker Wagner: Präventions- und Kontrollmaßnahmen werden von einzelnen Regierungen für politische Zwecke missbraucht. Kontrollen werden mehr und mehr ausgedehnt, um Oppositionskräfte zu überwachen. Dies zeigt sich in einigen Ländern an der weiteren Ausdehnung von Videoüberwachungssystemen bis hin zu Militäreinsätzen bei Demonstrationen im Inland. Ergänzt wird dies mit Einfuhrbeschränkungen sowie Einreiserestriktionen, womit auch der freie Handel von Gütern und Dienstleistungen betroffen ist. Bei allen Unsicherheiten scheint doch eines gewiss: Wir benötigen aktuell mehr denn je kompetente und leidenschaftliche Security Führungskräfte und Mitarbeiter, um unser aller Schutz zu gewährleisten. ■

Kontakt

ASW Bundesverband
Volker Wagner, Vorstandsvorsitzender
Allianz für Sicherheit in der Wirtschaft e.V.
Berlin
Tel.: 030 200 77 200
wagner@asw-bundesverband.de
www.asw-bundesverband.de

CYBER SECURITY

Noch einiges zu tun

Verband Teletrust: Zur Fortschreibung der „Cyber-Sicherheitsstrategie für Deutschland“

Die „Cyber-Sicherheitsstrategie für Deutschland 2016“ der Bundesregierung wird derzeit fortgeschrieben – bis Mitte 2021 soll die aktualisierte Cyber-Sicherheitsstrategie beschlossen werden. Bis dahin läuft ein Evaluierungsprozess in Form eines Fragebogens. Darin werden Stakeholder aus den Bereichen Wissenschaft, Wirtschaft, Staat und Zivilgesellschaft eingebunden – darunter auch der Bundesverband IT-Sicherheit (Teletrust), dessen Kommentierung wir im Folgenden ausschnittsweise wiedergeben.

Was hat sich bewährt?

Alle vier Handlungsfelder waren in der Vergangenheit und sind in der Zukunft im Prinzip wichtig: Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung; Gemeinsamer Auftrag Cyber-Sicherheit von Staat und Wirtschaft; Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur; Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik.

Dennoch müssen wir feststellen, dass der Level an Cyber-Sicherheit und die notwendige Robustheit unserer IT-Infrastrukturen noch nicht hoch genug ist. Die Handlungsfelder und deren Maßnahmen müssen mit deutlich mehr Energie bearbeitet werden. Ein Ziel zu definieren, reicht nicht aus, es muss auch mit konkreten, nachhaltigen Maßnahmen und einer geeigneten Struktur umgesetzt werden.

Aus diesem Grund sollte mit Hilfe einer sehr gut ausgestatteten Task Force eine geeignete Struktur aufgebaut werden, bei der mit allen Stakeholdern gemeinsam die Fortschreibung der Cyber-Sicherheitsstrategie durchgeführt und auch getragen wird. Durch die gemeinsame Verantwortung werden die notwendigen Maßnahmen auch konkreter, wirkungsvoller und nachhaltiger umgesetzt.

Technisch und rechtlich sind wir sehr weit. Es fehlt an der tatsächlichen Umsetzung. Die öffentliche Hand könnte hier viel bewirken, u. a. durch breite Nutzung des digitalen Personalausweises oder Technologien wir die Smartphone Bürger-ID bei behördlichen Angeboten im Netz (Bürgerportale).

Das ITSiG hat vieles bewegt und zum Positivem verbessert. Eine Ausweitung des Geltungsbereichs von ITSiG auf weitere Branchen, weitere Dienste und auch kleinere Betreiber (mehr in die Breite) ist mittelfristig nötig – evtl. unter Senkung der Anforderungen in weniger kritischen Bereichen.

Unternehmen in Deutschland schützen: Der Schutz der Unternehmen durch den Staat bzw. staatliche Organe ist wichtig – besser wäre es aber, die Unternehmen zu befähigen, sich selbst hinreichend zu schützen. Das Augenmerk muss dabei besonders auf KMU liegen, die mit dieser Aufgabe bisher noch meist überfordert sind.

Was hat sich erledigt?

Die Aktivitäten im Umfeld des „Bundestrojaners" durch die ZITiS im Handlungsfeld.

„Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur" sollten umgehend gestoppt werden, weil sie allen anderen Maßnahmen entgegenwirkt und damit die Cyber-Sicherheitsstrategie unglaubwürdig erscheinen lässt.

Was muss dazukommen?

Der Bundesverband IT-Sicherheit würde es begrüßen, wenn mehr Initiativen für die Verschlüsselung werthaltiger Daten von Unternehmen und zum Schutz der Privatsphäre umgesetzt würden, weil es für die fortschreitende Digitalisierung ein wichtiger und mit hohem Schutzpotenzial nutzbarer Sicherheitsmechanismus ist. Außerdem glauben wir, dass es dringend notwendig ist, eine vertrauenswürdige, digitale Cyber- Sicherheitsinfrastruktur aufzubauen, die z. B.: Extended Zertifikates für mehr Vertrauen von Webanwendungen einfach zur Verfügung stellt, eine Alternative zu „Let´s encrypt" (mit einer Identitätsüberprüfung) schafft und für eine einfache Verschlüsselung von E-Mail-Sicherheit, Chats, usw. sorgt. Teletrust würde es begrüßen, wenn die Initiative GAIA-X für die Schaffung von mehr Unabhängigkeit und höhere Cyber-Sicherheit und Datenschutz als gemeinsames Ziel definiert würde.

Weitere Ziele, die in der Cyber-Sicherheitsstrategie eine höhere Bedeutung erlangen sollten, sind die- Wiederansiedlung von IT-Produktion in Deutschland und Europa, um Versorgung zu sichern und Produkte mit hohen und höchsten Sicherheitsanforderungen unter kontrollierten Bedingungen herzustellen (wie GAIA-X).

Wünschenswert ist außerdem ein starkes Bekenntnis zu Open Source durch Einsatz (auch und insbesondere in der öffentlichen Verwaltung) und Unterstützung der Open-Source-Entwicklungsprojekte. Außerdem wichtig ist die Durchsetzung von Komplexitätsreduktion (Komplexität ist der größte Feind der IT-Sicherheit). Ein stärkerer Fokus sollte auf Dezentralisierung von IT-Systemen und Verantwortung gelegt werden. Dies ist insbesondere relevant im Bereich Digitale Identität, Self-Sovereign Identity (SSI), etc.

Ergänzt werden sollte, dass nicht nur mit Providern und (KRITIS)-Anbietern zusammengearbeitet wird, sondern verstärkt mit den Herstellern und Lieferanten – das sowohl auf Hard- und Software-Ebene. Das ITSiG 2.0 schießt inhaltlich insoweit über die aktuelle Strategie hinaus. Die Rolle des BSI sollte überdies stärker als bisher in der neuen Strategie Berücksichtigung finden, da sich das ansonsten mit dem zunehmenden Befugnisausbau nicht rechtfertigen lässt.

Das Identitätsmanagement ist ein Schüsselfaktor in jeder sicheren IT-Infrastruktur. Generell ist eine stärkere Berücksichtigung von eID und den in der eIDAS-Verordnung genannten Vertrauensdiensten in Technologie- oder IT-Sicherheitsrelevanten (Gesetzes) Initiativen wünschenswert.

Beim Thema „Sichere elektronische Identitäten" ist aus unserer Sicht die mobile eID-Funktion zu ergänzen, die eine hochsichere, datensparsame und nutzerfreundliche Ergänzung zur Online-Ausweisfunktion des Personalausweises darstellt und ihn über ein mobiles Endgerät – allen voran dem Smartphone – nutzbar macht. Zur Stärkung der sicherheitstechnischen Souveränität und Schaffung innovativer, nutzerfreundlicher und sicherer digitaler Angebote ist es notwendig, dass Sicherheitsmechanismen wie bspw. das Secure Element im Smartphone für die Wirtschaft zugänglich sind und der Zugriff darauf durch die Smartphone- Anbieter nicht verhindert wird.

Zu ergänzen wäre ein neuer Punkt: „Verstärkung der Kooperation und Vernetzung mit europäischen Einrichtungen, insbesondere der ENISA", um auch das Thema „nationale Alleingänge" stärker zu adressieren. ■

Kontakt

Bundesverband IT Sicherheit e.V. (TeleTrusT)
Berlin
Tel.: +49 30 400 54 310
info@teletrust.de
www.teletrust.de

Mehr zum Thema auf den WIN>DAYS
Talk mit Genetec „Cybersecurity: Gefahrenpotenzial erkennen und Lösungsansätze finden“

CYBER SECURITY

Cyberversichert?

Warum eine Cyber-Haftpflichtversicherung im Ernstfall entscheidend sein kann

Ob System-Hacks, DDoS-Attacken oder die zunehmende Erpressung von Lösegeldern durch gesperrte Daten: Die Liste an Cyberbedrohungen wird von Jahr zu Jahr länger. Im Allianz Risk-Barometer 2020 belegten Cyberangriffe erstmals Platz eins in der Rubrik Geschäftsrisiken – noch vor Betriebsunterbrechungen.

Zwar wurden in den letzten Jahren weniger große Cybervorfälle bekannt, wie z.B. der Fall Yahoo aus 2017, bei dem die persönlichen Daten von rund 3 Milliarden Nutzern veröffentlicht wurden. Dennoch steigt die Zahl von Angriffen auf kleinere Unternehmen und Mittelständler stetig, so dass sich auch Regierungen genötigt sehen, Richtlinien und Standards wie die Datenschutzgrundverordnung (DSGVO) festzulegen und Organisationen zur Verantwortung zu ziehen.

Die meisten Unternehmen arbeiten mit Hochdruck daran, alle Vorgaben und Richtlinien zu verstehen und die internen Prozesse entsprechend anzupassen. Kommt es dann aber doch zu einem Zwischenfall, z.B. durch Cyberangriffe, kommen nicht selten empfindliche Geldstrafen auf sie zu.

Was man über Cyber-Haftpflichtversicherungen wissen sollten

Unternehmen sind heute gegen zahlreiche Arten von Zwischenfällen versichert. Zu den Standards gehören Versicherungen für Rechtsschutz, Gebäude, Transport, Vertrauensschaden oder höhere Gewalt. Da die Risiken durch Cyberangriffe aber immer größer werden, wandeln sich auch die von Versicherungen angebotenen Policen und Produkte. Zahlreiche Versicherungen bieten heute schon Haftpflichtversicherungen gegen Cybervorfälle an, um die durch Attacken teils immensen Kosten abzufangen. Die Allianz rechnet bei Cyberversicherungen bis 2025 mit einem Marktvolumen von rund 20 Milliarden US-Dollar.

Für diese steigende Nachfrage gibt es sehr gute Gründe. Cyber-Haftpflichtversicherungen ermöglichen es Unternehmen, im Ernstfall die finanziellen Mittel zu haben, um alle Prozesse am Laufen zu halten und entsprechend auf Angriffe reagieren zu können.

Systemintegratoren sollten ihren Kunden Cyber-Haftpflichtversicherungen aktiv anbieten. Das bedeutet nicht, dass man der angebotenen Lösung nicht traut und sich daher besser frühzeitig gegen mögliche Schwachstellen versichern sollte. Im Gegenteil: Security-Lösungen, die für eine solche Versicherungspolice in Frage kommen, müssen strenge Sicherheitsprotokolle befolgen und hohe Standards erfüllen. Bevor eine Police nämlich nach einem Zwischenfall ausgezahlt wird, muss der Integrator nachweisen, dass alle gängigen Maßnahmen von Beginn an umgesetzt wurden. Andernfalls könnte die Versicherung eine Auszahlung verweigern.

Übernahme des Risikos über die Versicherung hinaus

Da es sich bei Cyber-Haftpflichtversicherungen um ein noch recht neues Produkt handelt, tun sich viele Versicherer noch schwer, die Risiken richtig einzuschätzen und zu berechnen. In der Regel basiert die Kalkulation der Deckungssumme auf einem standardisierten Fragebogen über gängige IT-Richtlinien, die Organisationhierarchie, die Größe der vorhandenen IT-Infrastruktur und die Unternehmensform. In vielen Fällen neigen Versicherer dazu, die Haftungssumme zu überschätzen, was am Ende zu höheren Prämien führt.

Unternehmen sollten sich aber nicht nur auf eine Cyber-Haftpflichtversicherung verlassen. Denn wenn diese greift, ist es in der Regel schon zu spät. Vielmehr sollten die IT- und Sicherheitssysteme schon im Vorfeld den höchsten Cyber-Sicherheitsstandards entsprechen. Dazu gehören unterschiedliche Sicherheitsebenen wie eine End-to-End Datenverschlüsselung und sichere Authentifizierungs- und Autorisierungsmechanismen, die für einen höheren Datenschutz und eine ordnungsgemäße Installation von Endgeräten mit starken Passwörtern sorgen. Unternehmen sollten sich außerdem ihren Lösungsanbieter und Partner sorgfältig auswählen und

auf Systeme setzen, die effektiv vor Cyberrisiken schützen, schnell über neue Updates und Patches informieren, und somit unnötige Sicherheitslücken vermeiden. Darüber hinaus sollten die eigenen Mitarbeiter durch interne Richtlinien sensibilisiert werden.

Drei Tipps für die richtige Cyber-Haftpflichtversicherung

Wie die individuell zugeschnittene und passgenaue Cyber-Haftpflichtversicherung im stetig wachsenden Angebot der Versicherungen identifiziert werden kann, dabei helfen die nachfolgenden Tipps:

■ Die individuellen Cyberrisken kennen: Cybersicherheit kann viele unterschiedliche Facetten haben. Gleiches gilt auch für passende Haftpflichtversicherungen. Es ist daher besonders wichtig, sich über mögliche Cyberrisiken für das eigene Unternehmen im Klaren zu sein. Das kann eine ganze Reihe virtueller, aber auch realer Risiken beinhalten, wie Datenverlust oder Diebstahl von Unternehmenswerten. Erst wenn das Unternehmen genau weiß, wo die größten Gefahren liegen, kann es sich für eine Versicherung entscheiden, die den individuellen Bedürfnissen entspricht.

■ Wissen, was versichert ist: Eine Cyber-Haftpflichtversicherung kann durch zusätzliche Versicherungspolicen ergänzt werden. Es kann auch sinnvoll sein, unterschiedliche Versicherungen miteinander zu kombinieren, um im Ernstfall die bestmögliche Abdeckungssumme zu erhalten. Deshalb ist es von zentraler Bedeutung, die Bedingungen und Auszahlungsvoraussetzungen der einzelnen Policen genau zu kennen, falls ein Unternehmen für einen etwaigen Datenverstoß haftbar gemacht werden sollte. Darüber hinaus kann es mitunter schwierig sein, den aus Cyberangriffen entstandenen Schaden finanziell zu beziffern. Daher ist es sehr wichtig, mögliche Risiken in ein Finanzmodell umzuwandeln. Auch wenn die Cybersicherheit ein Geschäftsrisiko bleibt, sollten sicherheitsrelevante Aspekte von einem Experten für Cybersicherheit untersucht werden. Optimalerweise kennt sich dieser gleichermaßen im wirtschaftlichen Kontext aus und kennt die Risiken für Cybersicherheit.

■ Was passiert nach dem Ernstfall: Neben der Höhe der Abdeckungssumme sollten Unternehmen auch wissen, wie der Schadensersatzprozess vonstattengeht. Denn jeder Versicherer hat eigene Verfahren, um die Authentizität des Anspruchs zu prüfen, und einen eigenen zeitlichen Rahmen, in dem die Summe ausgezahlt wird. Unternehmen sollten sich daher frühzeitig darüber informieren, wie schnell sie im Schadensfall mit der Versicherungssumme und anderen Hilfsleistungen rechnen können. Einige Versicherungen bieten neben finanzieller Entschädigung nämlich auch die Vermittlung von Cyber-Ermittlern und Kommunikationsagenturen an, die nach einem Cyberangriff unterstützen und in der Krise so eine große Entlastung sein können. ■

Autor
Kay Ohse
Country Manager DACH und ECE bei Genetec

Kontakt

Genetec Deutschland
Frankfurt
Tel.: +49 69 506028 255
www.genetec.com/de

Partner unterstützen digitale Dialogplattform

Ein umfangreiches Anbieter- und Lösungsverzeichnis, interaktive Dialogformate und Neues aus der Welt der Cybersicherheit bietet It-sa 365. Die seit dem 6. Oktober ganzjährig verfügbare IT-Sicherheitsplattform knüpfe ein Band zwischen den Messeterminen, so Frank Venjakob, Executive Director It-sa. Die dann unter itsa365.de erreichbare Plattform ist für registrierte Teilnehmer an 365 Tagen im Jahr frei zugänglich. Anbieter können aus verschiedenen Beteiligungsmöglichkeiten wählen. Wie mit der It-sa Expo & Conference spreche man die richtigen Zielgruppen an und biete Anbietern professioneller IT-Sicherheitslösungen damit ein zusätzliches Instrument für den Marketing-Mix an, so Venjakob. Unterstützt wird das Konzept von Partnern. Allen voran engagieren sich das Bundesamt für Sicherheit in der Informationstechnik und der Digitalverband Bitkom sowie der Bundesverband IT-Sicherheit Teletrust.

www.it-sa.de ■

BSI und EASA vereinbaren strategische Zusammenarbeit

Gemeinsames Ziel des Bundesamts für Sicherheit in der Informationstechnik (BSI) und der Agentur der Europäischen Union für Flugsicherheit (EASA, European Union Aviation Safety Agency) ist es, die Cybersicherheit in der internationalen Luftfahrt nachhaltig zu steigern. Dazu haben die beiden Aufsichtsbehörden eine strategische Zusammenarbeit vereinbart. Ein entsprechendes Abkommen (Memorandum of Cooperation, MoC) unterzeichneten BSI-Präsident Arne Schönbohm und EASA-Generaldirektor Patrick Ky. Fliegen werde gemeinhin als sicherste Art der Fortbewegung angesehen. Angesichts der auch in der Luftfahrt zunehmenden Digitalisierung und Vernetzung sei die Cybersicherheit ein wesentlicher Faktor dafür, dass dies weiterhin so bleibt, so BSI-Präsident Arne Schönbohm. In der Luftfahrt könne nur dann erfolgreich digital durchgestartet werden, wenn die Informationssicherheit von Anfang an mitfliegt.

www.bsi.bund.de ■

GESUNDHEITSWESEN

Attacken aufs Gesundheitssystem

Cyber-Angriff auf Uniklinik Düsseldorf zeigt Dringlichkeit des Themas

Der IT-Sicherheitsvorfall im Universitätsklinikum Düsseldorf (UKD) im September beschäftigt Behörden und Öffentlichkeit. Die Täter hatten ein Erpresserschreiben hinterlassen und es wird wegen eines Todesfalls als Folge des Angriffs ermittelt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützte das Klinikum vor Ort mit einem mobilem Einsatzteam. Auch nach Einschätzung des Softwareunternehmens Kaspersky zeigt der Vorfall, wie real die Gefahr für das Gesundheitssystem ist.

Nach dem Ausfall der IT-Systeme am 10. September war die Uniklinik Düsseldorf insgesamt dreizehn Tage von der Versorgung abgemeldet. Am 23.9. hat es sich wieder für die Notfallversorgung im Großraum Düsseldorf angemeldet. Damit konnte der Rettungsdienst die Zentrale Notaufnahme (ZNA) des UKD wieder anfahren.

Bekannte Schwachstelle

Der Cyber-Angriff wurde durch eine Schwachstelle in VPN-Produkten der Firma Citrix ermöglicht: Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) ist sie seit Dezember 2019 bekannt. Dem Amt würden zunehmend Vorfälle bekannt, bei denen Citrix-Systeme bereits vor der Installation der im Januar 2020 bereitgestellten Sicherheitsupdates kompromittiert wurden. Dadurch hätten Angreifer auch nach Schließung

der Sicherheitslücke weiterhin Zugriff auf das System und dahinterliegende Netzwerke. Diese Möglichkeit werde aktuell vermehrt ausgenutzt, um Angriffe auf betroffene Organisationen durchzuführen.

„Angreifer verschaffen sich Zugang zu den internen Netzen

und Systemen und können diese auch Monate später noch lahmlegen", so BSI-Präsident Arne Schönbohm: „Ich kann nur mit Nachdruck appellieren, solche Warnungen nicht zu ignorieren oder aufzuschieben, sondern sofort entsprechende Maßnahmen zu ergreifen. Der Vorfall zeigt zum wiederholten Male, wie ernst man diese Gefahr nehmen muss. Auch deswegen hat die Bundesregierung im Entwurf des Krankenhaus-Zukunftsgesetzes vorgesehen, dass mindestens 15 Prozent der beantragten Fördermittel für Maßnahmen zur Verbesserung der Informationssicherheit eingesetzt werden müssen".

Einfallstor in interne Netze

Die seit Januar 2020 bekannte Schwachstelle in den VPN-Produkten von Citrix stellt je nach lokaler Netzkonfiguration ein mögliches Einfallstor in interne Netze dar, so das BSI. Entsprechende Sicherheitsupdates stehen bereits seit Januar 2020 zur Verfügung und sollten, falls noch nicht geschehen, dringend eingespielt werden. Von der Ausnutzung betroffen können jedoch auch Systeme sein, die im Januar 2020 gepatcht wurden. Diese wurden unter Umständen bereits vor der Installation der Citrix-Sicherheitsupdates kompromittiert und können somit Angreifern auch jetzt noch den Zugriff auf interne Netze und weitergehende Aktivitäten erlauben, wie etwa die Ausleitung oder Verschlüsselung sensibler Daten oder die Manipulation bzw. Stilllegung von Systemen, Geschäftsprozessen und Betriebsabläufen.

Anwender der Produkte Citrix Gateway (ehemals Netscaler Gateway) und Citrix Application Delivery Controller sollten ihre Netzinfrastruktur und Systeme auf mögliche Anomalien hin überprüfen und ihre Schutzmaßnahmen zwingend anpassen, betont das BSI.

Gefahr für das Gesundheitssystem

Auch nach Einschätzung des Softwareunternehmens Kaspersky zeigt der Vorfall, wie real die Gefahr für das Gesundheitssystem sei. Ransomware, so das Unternehmen, gehörten „in jüngster Zeit zu den häufigsten Angriffsformen auf das Gesundheitswesen". In Krankenhäusern seien kritische Daten gespeichert - somit sei für Hacker die Verschlüsselung dieser Daten mit anschließender Lösegeldforderung erfolgversprechend. Während der Covid-19-Pandemie habe aber auch die Zahl der Phishing-Betrügereien zugenommen, die die gesamte medizinische Lieferkette betrafen. So habe es Fake-Verkäufe von Schutzausrüstung und Angriffe auf Hersteller von Beatmungsgeräten und Prüflabors gegeben.

Die Sicherheitsexperten von Kaspersky verzeichneten in den ersten Wochen der Pandemie einen Anstieg von Phishing, bösartigen Websites und Malware um 30.000 Prozent. Laut Kaspersky-Daten gab es in der ersten Märzwoche dieses Jahres außerdem einen Anstieg auf eine Million Cyberangriffe pro Tag mit Covid-19-Bezug.

Eugene Kaspersky, Gründer und CEO von Kaspersky, bewertet Angriffe auf Gesundheitsorganisationen als terroristischen Akt: „Cyberkriminelle sind es gewohnt, von zu Hause aus zu arbeiten und von dort aus Unternehmen und Einzelpersonen anzugreifen; ihre Umstände haben sich nicht drastisch geändert. Unsere Aufgabe ist es, weiterhin intensiv daran zu arbeiten, unsere Kunden zu schützen. Jeder Angriff auf ein Krankenhaus zu diesem Zeitpunkt kann als gleichbedeutend mit einem Terroranschlag eingestuft werden." ■

Rechtssichere Grundlagen für Cloud-Dienste: Unternehmen müssen aktiv werden

CLOUD SECURITY

Deal geplatzt

Cloud-Daten rechtssicher speichern – nach Scheitern des Privacy-Shield-Datenschutzabkommens mit den USA

Am 16. Juli hat der Europäische Gerichtshof das EU-USA-Datenschutzabkommen „Privacy Shield" als ungültig erklärt. Unternehmen brauchen jetzt dringend eine rechtssichere Grundlage für die Nutzung ihrer Cloud- und Collaboration-Dienste. Das IT-Sicherheitsunternehmen Rohde & Schwarz Cybersecurity rät dazu, selber aktiv zu werden.

Die EU hatte das Privacy-Shield-Abkommen 2016 mit den USA ausgehandelt, um europäische Daten, die in die USA übertragen werden, vor dem Zugriff Dritter abzusichern. Der Europäische Gerichtshof hat diese Datenschutzvereinbarung am 16. Juli für ungültig erklärt. Als Grund gab der EuGH die zu großen Unterschiede zwischen dem Datenschutzniveau der EU-Mitglieder und dem der USA an. Bei Datentransfers in die USA können europäische Unternehmen sich nun nicht mehr auf die Angemessenheit des Datenschutzniveaus gem. Art. 45 EU-DSGVO berufen. Das Urteil wurde sofort wirksam.

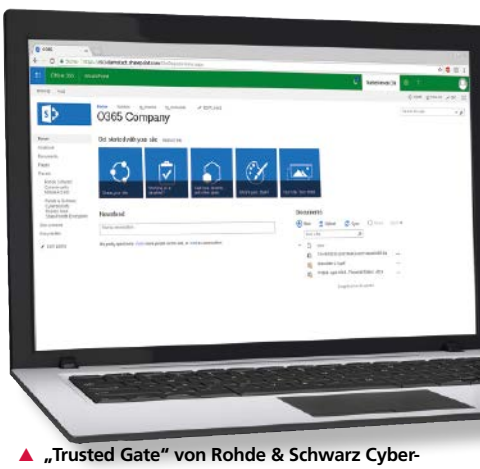
Was der Europäische Gerichtshof jetzt untermauert hat, wurde von Anfang an von Datenschützern kritisiert: Der „Privacy Shield" lässt dem US-Recht Vorrang. Der „Clarifying Lawful Overseas Use of Data Act", besser bekannt als Cloud Act, verpflichtet US-amerikanische Cloud-Provider, den US-Behörden Zugriff auch auf nicht in den USA gespeicherte Daten zu gewähren – und unterläuft damit die EU-DSGVO. Nachdem im Januar 2017 die Behörden in den USA per Dekret aufgefordert wurden, den Datenschutz für Ausländer vollends aufzuheben, war es nur noch eine Frage der Zeit, bis der „Privacy Shield" kippt.

Zukunftsfähige Geschäftsmodelle

Mit dem Ende des „Privacy Shield" geht das Ringen um den Schutz personenbezogener Daten, die aus der EU in die USA übermittelt werden, in eine neue Runde. Leidtragende sind die europäischen Unternehmen. Sie brauchen schnell eine rechtssichere Lösung. Denn für sie werden cloud-basierte Anwendungen immer wichtiger, um zukunftsfähige Geschäftsmodelle umzusetzen. Hinzu kommt: Die marktführenden Cloud-Plattformanbieter sind überwiegend US-amerikanische Unternehmen, und treiben „Cloud-only"-Lösungen mit Nachdruck voran. Immer mehr Daten aus europäischen Unternehmen liegen längst in Rechenzentren amerikanischer Konzerne – und sind dort nicht sicher vor dem Zugriff Dritter.

Auch der Bundesverband der Deutschen Industrie schlägt Alarm. Präsident Dieter Kempf fordert: Europäische Unternehmen brauchen dringend Rechtssicherheit im globalen Daten- und Wirtschaftsverkehr.

Das Problem: Auch die Nutzung der Standardvertragsklauseln, die den



▲ „Trusted Gate" von Rohde & Schwarz Cybersecurity lässt sich in gängige Public Clouds einbinden

Datentransfer in Drittländer regeln, ist durch das Urteil vom 16. Juli ins Wanken gekommen. Zwar hat der EuGH an diesen nichts zu beanstanden. Doch werden die Aufsichtsbehörden dazu verpflichtet, die Übermittlung von Daten auszusetzen oder zu verbieten, sofern die vertraglich festgehaltenen Standards in einem Drittland nicht eingehalten werden oder eingehalten werden können. Für europäische Unternehmen bedeutet dies, dass sie vor einem Datentransfer in jedes Drittland prüfen müssen, ob die Regelungen eingehalten werden. Insbesondere für kleine und mittlere Unternehmen ist der hohe Verwaltungsaufwand nur schwer zu stemmen. Die komplexen Beurteilungen gehen zudem mit einem hohen Risiko einher.

Deutsche Cloud-Standorte keine Lösung

Ausländische Cloud-Provider bieten ihren Kunden nun zunehmend die Möglichkeit, ihre Daten in Deutschland zu speichern. Aber auch solche deutschen und europäischen Cloud-Standorte sind keine Lösung. Denn auch dann können Cloud-Anbieter gezwungen werden, Zugriff auf die bei ihnen gespeicherten Daten zu gewähren.

Aber wie kann eine rechtssichere Lösung aussehen? Der „Privacy Shield" war bereits der zweite Versuch, eine solche zu schaffen. Auch der Vorgänger, die „Safe-Harbour-Entscheidung", war gescheitert. Beiden Vereinbarungen ist es nicht gelungen, amerikanische Unternehmen zu verpflichten, die Daten europäischer Bürger und Unternehmen besser zu schützen.

Die Erfahrung zeigt: US-Gesetze lassen sich nicht zugunsten europäischer Datenschutzvorschriften zähmen. Die Abkommen wurden zudem als machtpolitische Spielbälle missbraucht. Es besteht die Gefahr, dass auch eine neue Regelung Sicherheit vortäuscht, ohne sie garantieren zu können. Eine schnelle Lösung ist zudem aufgrund der Präsidentschaftswahlen in den USA aussichtslos.

Daten entkoppeln

Anstatt auf Vereinbarungen mit den USA zu hoffen, sollten Unternehmen auf innovative technische Lösungen setzen, die ihnen die Kontrolle über ihre Daten zurückgeben. Auf diese Weise legen sie eine nachhaltige Basis für ihre Digitalisierungsstrategie. Dazu müssen sensitive Daten von den Cloud-Diensten entkoppelt werden. Dann lassen sich diese an jedem beliebigen Ort speichern. US-Anbieter Microsoft hat diesen Weg bereits gemeinsam mit dem deutschen IT-Sicherheitsunternehmen Rohde & Schwarz Cybersecurity eingeschlagen.

Während die Workflows von Microsoft Teams und Microsoft Sharepoint Online weiterhin für die Nutzer aktiv bleiben, werden die Daten mit Hilfe der Datensicherheitslösung für Cloud-Umgebungen aus den Prozessen herausgelöst. Durch die gewonnene Datensouveränität können europäische Unternehmen die EU-DSGVO weltweit ohne Rechtsunsicherheiten erfüllen. „R&S Trusted Gate" lässt sich nahtlos in gängige Public Clouds wie Microsoft Azure, Google, AWS und Collaboration-Tools wie Microsoft Office 365 und Sharepoint einbinden.

Mit Hilfe einer solchen datenzentrischen Lösung gewinnen Unternehmen nicht nur eine rechtssichere Grundlage für die Übertragung ihrer Daten in die USA. Sie machen sich unabhängig von Gesetzen und politischen Entscheidungen in jedem Drittland, in das sie Daten übermitteln. Insbesondere für global agierende Unternehmen spielt dieser Faktor eine große Rolle. Ein weiterer Vorteil einer solchen datenzentrischen Lösung: Die sensiblen Daten, die von den Clouddiensten entkoppelt werden, lassen sich besser vor Hackern schützen. Denn immer wieder kommt es zu schwerwiegenden Angriffen auf öffentliche Clouds. Wenn die Dateien auf dem Server des Unternehmens verbleiben, kann dieses selbstbestimmt für ein hohes Sicherheitsniveau sorgen. ■

Kontakt

Rohde & Schwarz Cybersecurity GmbH
Tel.: +49 30 65 884 222
cybersecurity@rohde-schwarz.com
www.rohde-schwarz.com/cybersecurity

▲ **Schutz vor Cyberangriffen auf die Cloud**

CYBER SECURITY

Störfeuer auf Produktionsnetzwerke

Studie: „Cybersecurity-Niveau in der Operational Technology“

Eine von Baramundi in Auftrag gegebene Studie untersucht, wie deutsche Industrieunternehmen mit den Gefahren für ihre Produktionsumgebung umgehen

© Baramundi/Adobe Stock

Wo stehen deutsche Industrieunternehmen bei der Absicherung ihrer Produktionsnetzwerke? Dieser Frage widmet sich eine neue Studie, die das Research- und Analystenhaus Techconsult mit Unterstützung des Augsburger Software-Spezialisten Baramundi Software durchgeführt hat. Die Untersuchung trägt den Titel „Cybersecurity-Niveau in der Operational Technology“ – dafür wurden 156 deutsche produzierende Unternehmen befragt.

Vor dem Hintergrund des digitalen Wandels hin zu einer zukunftsweisenden Industrie 4.0 sind Fertigungsunternehmen mit neuen Sicherheitsherausforderungen konfrontiert. Die zunehmende Vernetzung moderner Produktionsanlagen setzt den Schutz des Produktionsnetzwerks nach außen mittels „Air Gap“ außer Kraft: Laut der neuen Techconsult-Studie sind heute bereits in rund 84 Prozent der deutschen Industrieunternehmen sämtliche IT-Geräte im Produktionsumfeld miteinander verbunden. In nahezu all diesen Netzwerken (98 Prozent) besteht eine Verbindung nach außen – und die Quote von direkten Angriffen auf Produktionsinfrastrukturen steigt. Von den in der Studie befragten produzierenden Unternehmen verzeichneten in den letzten 12 Monaten fast 44 Prozent solche Angriffe. Die Dunkelziffer noch unentdeckter Angriffe könnte dabei noch weitaus höher liegen.

Für deutlich mehr als jedes zweite betroffene Unternehmen kam es dabei zu einer Produktionsstörung, und in jedem dritten Unternehmen wurde die Produktivität zumindest beeinträchtigt. Der Anteil der Unternehmen mittlerer Größe liegt in dieser Gruppe sogar bei 58 Prozent. 19 Prozent der attackierten Unternehmen mussten den direkten Ausfall ihrer Produktion infolge von Cyberangriffen in Kauf nehmen. Und bei mehr als jedem vierten betroffenen Unternehmen (26 Prozent) führten Hackerattacken auf ihre Produktionsinfrastruktur sogar zu schweren Reputationsschäden. Die mit solchen Angriffen einhergehenden Produktionsausfälle oder Betriebsunterbrechungen ziehen neben Mehrkosten in der Regel auch Lieferverzüge

und damit einen Vertrauensverlust bei Kunden und Partnern nach sich.

Auch Mittelständler im Fokus

Nach den Zahlen scheinen in der Mehrheit vor allem größere Unternehmen mit 1.000 und mehr Beschäftigten, die über komplexe und gewachsene Produktionsinfrastrukturen verfügen, von Cyberangriffen betroffen zu sein – ihr Anteil liegt hier bei über 65 Prozent. Allerdings ist ihr Risiko durch die höhere Anzahl von Mitarbeitern, die durch unachtsames Verhalten ein potenzielles Risiko für die Netzwerksicherheit darstellen können, auch größer. Vermutlich werden aber auch kleinere Unternehmen deutlich häufiger Opfer von Internetkriminellen, als sie selbst annehmen und angeben. Viele Attacken bleiben evtl. aufgrund unzureichender technischer Sicherheitsausstattung der Produktionsinfrastruktur unbemerkt. Unternehmen unter 1.000 Mitarbeitern erleiden Produktionsstörungen infolge von Cyberattacken deutlich häufiger als größere Unternehmen. Dies weist darauf hin, dass ein umfassendes Security-Konzept mit der dazugehörigen technischen Ausstattung auf hohem Niveau die Auswirkungen von Cyberattacken abschwächen kann.

Wie wird angegriffen?

Neben klassischem Phishing und gezielten Angriffen über ungepatchte Schwachstellen waren vor allem manipulierte Speichermedien die häufigste Waffe der Angreifer. Bei mehr als jedem zweiten erfassten Angriff der letzten zwölf Monate handelte es sich bei den befragten Studienteilnehmern um eine typische Phishing-Attacke. 45 Prozent der im Produktionsumfeld durch Malware ausgelösten Sicherheitsvorfälle zählten zu den sogenannten „Advanced Persistent Threats" (APT)-Angriffen, die mit 58 Prozent vor allem mittelgroße Unternehmen unter 1.000 Mitarbeitern betreffen. Fast jeder dritte Angriff auf Produktionsinfrastrukturen basiert auf manipulierten mobilen Datenspeichern – hier sind mit 33 Prozent vor allem kleinere und mittlere Unternehmen gefährdet. Direkten Hackerangriffen auf ihr Produktionsnetzwerk mit Zugang über Sicherheitslücken im IT- oder Produktionsnetzwerk waren kleinere und größere Unternehmen gleichermaßen ausgesetzt

Mangelnder Schutz der Produktionssysteme

Laut Studie verfügt nur jedes vierte Industrieunternehmen (24 Prozent) über ausreichende Security-Ressourcen, um eine vollständige Sicherheit ihrer Produktionsinfrastruktur zu gewährleisten. Schutzmaßnahmen müssen dabei nicht nur Schwachstellen des Netzwerks ausfindig machen, sondern auch ungewöhnliches Netzwerkverhalten erkennen und Bedrohungen abwenden. In rund einem Drittel der befragten Unternehmen findet eine derartige Netzwerküberwachung statt – allerdings zeigt sich auch hier, dass kleinere Unternehmen im Vergleich zu Großunternehmen technisch schlechter aufgestellt sind. Und lediglich 15 Prozent der Industrieunternehmen verfügen über ausreichendes Personal, um die IT-Security im Produktionsumfeld im vollen Umfang zu gewährleisten.

Sicherheitsstrategie muss zur industriellen Fertigung passen

Schutz vor Angriffen bietet beispielsweise die Segmentierung der Netzwerke und Betriebsfunktionen: Rund ein Viertel der Unternehmen verbesserte dadurch ihre Sicherheit erheblich. Lediglich 18 Prozent der Unternehmen setzen laut Studie produktionsspezifische Management- und Sicherheitstools ein. Eine Mehrheit nutzt dagegen Security-Lösungen der IT – diese IT-Lösungen kommen jedoch an ihre Grenzen, da die verschiedenen Systeme, Geräte und proprietären Netzwerk-Protokolle unterschiedliche Sicherheitsanforderungen stellen. Eine für die Produktionsumgebung zugeschnittene Sicherheitslösung muss vor allem Systeme, Anlagen und Geräte genau erfassen. Mittlerweile gibt es bereits Unified-Endpoint-Management (UEM)-Lösungen, die sich auch auf Operational-Technology-Endgeräte spezialisieren. Bisher nutzt aber laut Studie nur ein gutes Drittel der Unternehmen – und hier vor allem auch größere Unternehmen – technische Lösungen, die sämtliche produktionsnahen Endpunkte automatisiert scannen und erfassen, um mögliche Schwachstellen zu identifizieren, Patches einzuspielen oder Konfigurationsanpassungen vorzunehmen.

Ausblick

Industrieunternehmen müssen damit rechnen, dass ihre Produktionsanlagen jederzeit ins Visier von Hackern gelangen können. Neben geeigneten Maßnahmenplänen für mögliche Angriffe, ausreichenden technischen Ressourcen und qualifiziertem Personal kann auch eine Netzwerksegmentierung sowie der Einsatz von UEM-Lösungen zur automatisierten Erfassung und Inventarisierung aller im Produktionsumfeld eingesetzten Endpoints einen verbesserten Schutz ermöglichen. ■

Kontakt

Baramundi Software AG
Augsburg
Tel.: +49 821 567 08 0
info@baramundi.com
www.baramundi.com

SICHERE AUTOMATISIERUNG

Wenn IT und OT sich treffen

Anforderungen für Betreiber, Integratoren und Gerätehersteller an die OT-Security

Egal ob Hersteller oder Betreiber, Industrie oder kritische Infrastruktur: Das Thema Cyber-Security ist für alle Industriebereiche wichtig, denn die Automatisierungstechnik wächst immer stärker mit der IT-Welt zusammen. Anlagengrenzen lösen sich auf und auch der Austausch von Daten und Informationen erhöht sich kontinuierlich. Aufgrund dieser Vernetzung und Anbindung an das Internet sind die industriellen Automatisierungssysteme zunehmend Cyber-Angriffen ausgesetzt. Doch wie kann man sich davor effektiv schützen?

Mit dem im Juli 2015 verabschiedeten IT-Sicherheitsgesetz werden die Betreiber kritischer Infrastrukturen dazu verpflichtet, die für die Erbringung ihrer wesentlichen Dienste erforderliche IT gemäß dem Stand der Technik abzusichern. Andere industrielle Bereiche handhaben das Thema Security unterschiedlich. Produktionsanlagen und Fernzugriff sind hier oftmals kaum geschützt. Das liegt meist nicht am fehlenden Bewusstsein, dass etwas getan werden sollte, sondern es mangelt am benötigten Wissen sowie einem Leitfaden, wie vorzugehen ist. In diesem Zusammenhang treten folgende Fragen auf:

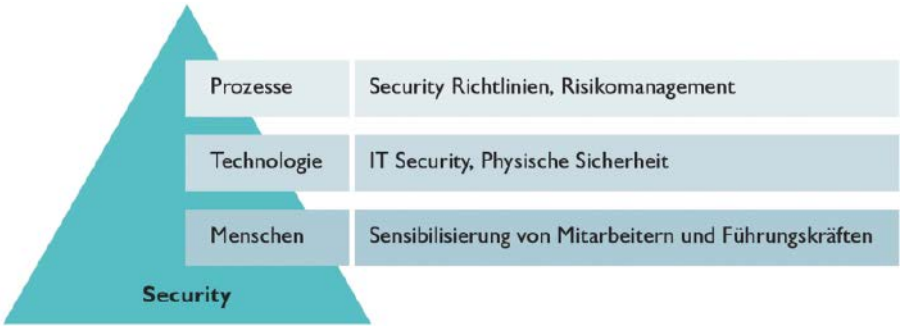
- Was ist notwendig?
- Wie sollte der Sachverhalt angegangen werden?
- Wo lässt sich Unterstützung anfordern?
- Welchen Standards sollte entsprochen werden?

Unterschiedliche Herausforderungen in IT und OT

Industrial Security muss ein ganzheitlicher Ansatz sein, der in den Köpfen des Managements sowie

der Mitarbeiter beginnt. Neben technischen Maßnahmen, wie dem Einsatz von Industrial Security-Produkten (Technologie), dürfen organisatorische Maßnahmen in Form eines Security-Managements (Prozesse) nicht vernachlässigt werden. Eine sichere IT bildet die Grundlage für die Security im Unternehmen, die Kundendaten, Entwicklung und Fertigung, aber reicht das aus?

Im Vergleich zur IT (Information Technology)-Security ist die OT (Operational Technology)-Security, auch Industrial Control Systems (ICS)-Security genannt, bei identischen Themen mit anderen Herausforderungen konfrontiert. Um die Zugriffssicherheit in der OT komplett zu bedienen, sind die von der IT definierten Maßnahmen durch zusätzliche relevante Aktivitäten zu erweitern. Die Norm IEC 62443 beschreibt die Anforderungen für Betreiber, Integratoren und Geräteheresteller zur Umsetzung der Security in der OT. Das Design einer Automatisierungslösung muss daher ergänzend zur eigentlichen Automatisierungsaufgabe auch Security berücksichtigen, wobei die Teile 2-4 und 3-3 der IEC 62443 zu beachten sind.



Security als ganzheitlicher Ansatz

Genaue Erfassung aller Anlageninformationen

Die Konzeption einer Automatisierungslösung unter Security-Aspekten geschieht generell in enger Zusammenarbeit zwischen dem Integrator/Dienstleister und dem Betreiber. Zunächst werden alle Anlageninformationen hinsichtlich der Umgebung (freie Fläche, Gebäude etc.), der Struktur (Netzwerk, Auflistung der Komponenten und deren Installationsort etc.) und des Prozesses (Abläufe, Kommunikationsbeziehungen, schützenswerte Daten etc.) erfasst. Das betrifft sowohl neue ebenso wie bestehende Anlagen. Daran schließen sich folgende Schritte an:

Security-Spezifikation

Auf der Bestandsaufnahme aufbauend erfolgt die Security-Spezifikation für die Anlage. Sie beinhaltet das Netzwerkkonzept sowie eine Asset-Liste sämtlicher vernetzter Geräte und definiert bereits Härtungsmaßnahmen. Für die zukünftige Zugriffssicherheit ist es ein Muss, dass die Realisierung aller bereits zu diesem und zu späteren Zeitpunkten veranschlagten Security-Maßnahmen bei der Übergabe der Anlage verifiziert werden. Deshalb entsteht schon bei der Security-Spezifikation die Testspezifikation, die später die Maßgabe bei der Anlagenabnahme bildet.

Schutzbedarfsanalyse

Im nächsten Schritt erfolgt eine Schutzbedarfsanalyse. Dabei werden die schutzbedürftigen Assets, Daten und Kommunikationswege ermittelt und dokumentiert. Diese Analyse geschieht auf der Grundlage von drei Schutzzielen: Verfügbarkeit, Integrität und Vertraulichkeit. Damit einhergehend findet eine Festlegung der zu schützenden Zonen und Conduits (Verbindungskanäle) in der Anlage statt. Am Ende liegt eine Schutzbedarfsfeststellung für die Automatisierungslösung vor, die für die eingesetzte Informationstechnik ausreichend und angemessen ist.

Bedrohungsanalyse

Hierauf aufbauend erfolgt eine Bedrohungsanalyse. Sie gründet sich beispielsweise auf den Top-10-Bedrohungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) und wird gegebenenfalls durch betreiberspezifische Themen erweitert. Gemeinsam mit dem Betreiber werden die Gefährdungen hinsichtlich der Relevanz für die Automatisierungslösung bewertet und schriftlich festgehalten. Der Bedrohungsanalyse liegen ebenfalls die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit zugrunde.

Risikoanalyse

Im Anschluss daran wird auf Basis der festgestellten Bedrohungen eine Risikoanalyse vorgenommen. Das Risiko bemisst sich an den möglichen Schäden und der daran geknüpften Eintrittswahrscheinlichkeit für ein solches Szenario.

- Für Risiken, die für das Unternehmen nicht akzeptabel sind, werden Maßnahmen erarbeitet und die Auswirkung auf die Bewertung geprüft.
- Sofern sich das Risiko auf ein akzeptables Niveau mindern lässt, sollten die Maßnahmen unter Beachtung der Wirtschaftlichkeit realisiert werden.

Im Ergebnis erhält der Betreiber eine Handlungsempfehlung für ein ganzheitliches, individuelles und produktneutrales Sicherheitskonzept, das auf die speziellen Anforderungen seines Unternehmens abgestimmt ist.

Prozess zum Design einer Security-Automatisierungslösung

Risikobehandlung

Im Rahmen der Risikobeurteilung wird entschieden, wie mit den verbleibenden Risiken umzugehen ist. Mögliche Risikobehandlungs-Optionen sind:

- Risiken lassen sich vermeiden, weil beispielsweise die Risikoursache ausgeschlossen wird.
- Eine Reduzierung des Risikos ist möglich, indem eine Modifizierung der Rahmenbedingungen stattfindet, die zur Risikoeinstufung beigetragen haben.
- Risiken werden durch ihre Teilung mit anderen Parteien transferiert.
- Der Betreiber akzeptiert die Risiken.

Durch eine regelmäßige Prüfung der Maßnahmenumsetzung sowie der Bedrohungslage erfolgt ein stetiges Risk Monitoring.

Risk Monitoring

Unternimmt das Unternehmens nichts zur Verminderung eines bestehenden Risikos, so wird dieses akzeptiert. Hier sollte das Management mit dem Ziel einbezogen werden, alle identifizierten, analysierten, bewerteten und priorisierten Risiken angemessen zu behandeln. Sich daraus ergebende zusätzliche Security-Maßnahmen fließen in die Security- und Testspezifikation ein. Generell gilt dabei:

- Sämtliche Prozessschritte müssen nach dem aktuellen Stand der Technik geschehen.
- Die Ergebnisse werden dokumentiert und
- der Betreiber zeichnet die Ergebnisse der Analysen ab.

Implementierung/Verifikation

Der Integrator/Anlagenlieferant führt die festgelegten Maßnahmen der Security-Spezifikation in der Anlage durch. Vor ihrer Übergabe an den Betreiber wird die Realisierung der Security-Maßnahmen anhand der Testspezifikation verifiziert und ist damit Bestandteil der Anlagenabnahme (Site Acceptance Test, SAT). In einem definierten Zeitraum – beispielsweise jährlich – muss überprüft werden, ob neue Bedrohungen oder Risiken vorhanden sind, die eine erneute Bewertung erfordern.

Zertifizierter Dienstleister zur Unterstützung

Zur Bearbeitung der beschriebenen Security-Maßnahmen empfiehlt es sich, dass der Betreiber einen geeigneten Dienstleister auswählt, mit dem er die Themen gemeinsam festlegt. Hierbei sollte es sich um ein Unternehmen handeln, welches gemäß IEC 62443-2-4 als Security-Dienstleister zertifiziert ist. So wird sichergestellt, dass das notwendige Wissen und die Prozesse vorliegen, um eine Automatisierungsanlage nach den Normenanforderungen zu designen.

ICS-Security	IT-Security
Prioritäten	
Verfügbarkeit Integrität Vertraulichkeit	**Vertraulichkeit** Integrität Verfügbarkeit
Eigenschaften	
Verfügbarkeit	
100 %	99 % ausreichend
Neustart	
Schwierig	Möglich
Patch Management	
Große Herausforderung	Automatisiert möglich
Lebenszeit Hardware	
7 - 20 Jahre	3 - 5 Jahre

ICS-Security versus IT-Security

Vielfältiges Leistungsangebot

Phoenix Contact wurde im April 2019 vom Tüv Süd als eines der ersten Unternehmen in Deutschland nach der Normenreihe für OT-Sicherheit IEC 62443-2-4 zertifiziert. Die Zertifizierung bestätigt, dass das Unternehmen gemeinsam mit seinen Kunden sichere Automatisierungslösungen entwickeln und realisieren kann. Folgende Security-Dienstleistungen werden angeboten:

- Erarbeitung von individuellen Lösungen und Konzepten für ausfallsichere Netzwerkstrukturen, zur Absicherung oder Fernwartung von Maschinen sowie für leistungsfähige Funknetzwerke auf der Grundlage der verschiedenen Branchenstandards
- Umsetzung der Security- und Netzwerkanforderungen hinsichtlich Konfiguration und Dokumentation, Einführung von Managementsystemen, Erkennung und Beseitigung von Anomalien, Wartung des Netzwerks sowie Test der in Betrieb genommenen Systeme
- Unterstützung bei der Installation von Sicherheits-Updates sowie der Anpassung der Firewall-Regeln
- Durchführung von Security-Grundlagen- und Expertenschulungen, Security-Awareness-Schulungen, Ethernet-Grundlagenschulungen sowie individuellen Praxistrainings, die speziell auf die jeweiligen Bedürfnisse zugeschnitten sind. ■

Autoren
Werner Neugebauer
Vertical Market Management
Phoenix Contact Electronics GmbH
Bad Pyrmont

Torsten Gast
Leiter Competence Center Services
Phoenix Contact Electronics GmbH
Bad Pyrmont

Kontakt

Phoenix Contact GmbH & Co. KG
Blomberg
services@phoenixcontact.de
www.phoenixcontact.de/security

Funk-Netzwerklösung für digitale Produktion ▲

Die Funk-Netzwerklösung „Nexy" aus dem Geschäftsbereich „Wireless" von Steute ermöglicht die Übertragung von Sensordaten in das Internet der Dinge (IoT) oder andere übergeordnete IT-Systeme. Unterschiedliche Sensoren und elektromechanische Schaltgeräte, aber auch Aktoren und Bediensysteme können in diese kabellose Netzwerklösung einge¬bunden werden. Sie senden und empfangen Daten über den Funkstandard sWave Net, den das Unternehmen für eben diesen Einsatzfall entwickelt hat. Access-Points sammeln die Daten der Funksensorik und -Aktorik und übertragen sie an eine Sensor-Bridge, die als Service-Manager den Datentransfer an übergeordnete IT Systeme des Anwenders übernimmt. So entsteht eine durchgängige Kommunikation von der „Shopfloor"-Ebene bis in die Management-Ebenen der Unternehmens-IT. Ein übersichtlich gestaltetes Dashboard sorgt für die Statusvisualisierung aller in das Netzwerk eingebundenen Endgeräte.

www.steute.com ■

Blitzstrom- und Überspannungsableiter

Die kombinierten Blitzstrom- und Überspannungsableiter der Geräteserie Blitzductorconnect von Dehn schützen Automatisierungs- und MSR-Technik im industriellen Um-

feld wie informationstechnische Schnittstellen. Ein hohes Blitzstrom-Ableitvermögen und ein niedriger Schutzpegel machen sie zu idealen Bausteinen für einen sicheren Endgeräteschutz. Es gibt sie kompakt oder modular aufgebaut mit einer Baubreite von 6 mm. Funktionen wie die Sec-R-Entriegelungstasten und die Push-in-Technik helfen, den Installationsaufwand zu minimieren. Statusanzeige und passende FM-Einheit melden Ausfälle bei Überlast sofort. Für eigensichere Signalkreise stehen Ableiter mit Zulassung für Ex-Anwendungen zur Verfügung. Die Ableiter sind in verschiedenen Varianten verfügbar. Sie schützen zwei Einzeladern mit gemeinsamem Bezugspotenzial (unsymmetrische Schnittstellen) oder eine erdpotenzialfrei betriebene Doppelader (symmetrische Schnittstelle).

www.dehn.de ■

©Kalyakan - stock.adobe.com

GÜTERVERKEHR

Damit die Fracht auch ankommt

Cyberbedrohungen in der Schifffahrt: Güterverkehr als strategisches Angriffsziel

Jährlich werden im weltweiten Handel mehr als zehn Milliarden Tonnen an Gütern auf dem Seeweg verschifft, Tendenz steigend. Die Vernetzung in der Seeverkehrstechnik reicht von den Systemen an Bord wie elektronischen Seekarten und Satelliten-Navigationssystemen bis hin zur Hafenlogistik. So wird ein Cyberangriff auf ein einzelnes Schiff genauso wie auf einen Hafen oder eine Reederei möglich.

Die digitale Piraterie in der Logistik, vor allem in der Hafen-Logistik und Seefahrt ist ein Thema, das bisher selten beleuchtet wurde, und doch wirtschaftliche Schäden in Millionenhöhe anrichten kann. Wolfgang Kiener, Cybersecurity-Experte bei Tüv Rheinland, erklärt: „Containerschiffe bilden den Kern unseres globalen Wirtschaftsverkehrs. Dabei sind sie mittlerweile voll in die digitale Welt integriert. Das sorgt für eine reibungslos funktionierende Lieferkette, macht das System aber auch angreifbar für Cyberkriminelle". Die Vernetzung in der Seeverkehrstechnik reicht von den Systemen an Bord wie elektronischen Seekarten und Satelliten-Navigationssystemen bis hin zur Hafenlogistik. So wird ein Cyberangriff auf ein einzelnes Schiff genauso wie auf einen Hafen oder eine Reederei möglich und wirtschaftliche Schäden sind die Folge.

Cyberangriffe mit wirtschaftlichem und geopolitischem Ziel

Prinzipiell lassen sich drei Arten von Angreifern unterscheiden. Bereits sogenannte Scriptkiddies, die über relativ geringe Kenntnisse verfügen, können mit vorgefertigten Schadprogrammen in die Computersysteme eindringen. Entstehender Schaden ist hier meist singulär und noch recht überschaubar. Zur zweiten Gruppe zählen organisierte Banden, die beispielsweise Erpressersoftware, sogenannte Ransomware, einschleusen und so Containerschiffen den Zugriff auf ihre eigenen digitalen Systeme verwehren – auch um die geordnete Kommunikation im Güterverkehr zu erschweren und um Lösegeld zu erpressen. Der wirtschaftliche Schaden dieser digitalen Piraterie kann schnell hohe Millionenbeträge erreichen.

Ein Beispiel dafür ist der Angriff auf die Reederei Mærsk im Jahr 2017. Cyberkriminelle konnten auf die Logistiksteuerung des Weltkonzerns zugreifen und die Systeme verschlüsseln – mit der Folge, dass per Computer nicht mehr nachvollziehbar war, wo welche Fracht auf den Containerschiffen unterwegs war und wo unterschiedliche Waren lagern. In nur zwei Wochen entstand dem Unternehmen ein Schaden in Höhe von 300 Millionen US-Dollar. „Ein solcher Angriff kann die Existenz eines Global Players bedrohen – und damit erhebliche Auswirkungen für den weltweiten Warenwirtschaftsverkehr verursachen", unterstreicht Kiener.

Schwachstellen im System aktiv aufdecken

„Die Absicherung der Systeme hält mit der zunehmenden digitalen Vernetzung der Seeschifffahrt nicht Schritt. Deshalb ist es umso wichtiger, dass sich die Unternehmen ihrer Schwachstellen bewusst sind und mit einem aktiven Risikomanagement Cyberbedrohungen vorbeugen", rät Kiener. Auf Basis von Risikoanalysen lässt sich feststellen, wo mögliche Einfallstore für Angreifer liegen und wie viel das Unternehmen investieren müsste, um diese zu schließen.

Die zunehmende Bedrohung durch Cyberangriffe in der Schifffahrt ist eines von insgesamt sieben Themen der Cybersecurity Trends 2020 von Tüv Rheinland. Der vollständige Trendreport steht unter www.tuv.com/cybersecurity-trends-2020 zum Download zur Verfügung. ■

Kontakt

Tüv Rheinland Service GmbH
Köln
Tel.: 0221 806 3060
www.tuv.com

Besuchermanagementsystem erweitert

Das Besuchermanagementsystem Visit von Astrum wurde um ein weiteres intelligentes Feature ergänzt. Eine Thermalmessung wurde in den Selbstanmeldeprozess integriert: Präzise Thermalkameras messen aus einer Entfernung von bis zu drei Metern die Temperatur der Besucher. Wird ein Schwellenwert überschritten, können eine vordefinierte Stelle informiert und entsprechende Maßnahmen eingeleitet werden (z. B. Messung über Stirnthermometer o. Ä.). Nach einer Voranmeldung durch einen Mitarbeiter kann sich der Besucher an einem Kiosksystem selbstständig vor Ort anmelden. Der Besucher erhält alle relevanten Informationen und wird um die datenschutzrechtlich notwendige Zustimmung zur Temperaturmessung gebeten. Werden nach seiner Einwilligung keine Unregelmäßigkeiten festgestellt, kann der Anmeldeprozess ohne Verzögerungen in gewohnter Weise fortgesetzt werden.

www.astrum-it.de ■

Switche mit Abwehrmaßnahmen

Die Switche der RY-28-Serie von Barox können so konfiguriert werden, dass sie Sicherheitsnetzwerke und Geräte von Drittanbietern, wie Kameras und Server, vor Ripple20-Cyberangriffen schützen. Ripple20 ist eine Reihe von 19 Schwachstellen in einer Low-Level-TCP/IP-Softwarebibliothek und stellt eine unmittelbare Bedrohung dar.

Wenn es aktiviert wird, könnte es entfernten Angreifern ermöglichen, die vollständige Kontrolle über die Zielgeräte zu erlangen, ohne dass eine Interaktion des Benutzers erforderlich ist. Um Geräte und Netzwerke vor Ripple20-Schwachst ellen zu schützen, müsse ein zweckspezifischer Filter so konfiguriert werden, dass er niemals fragmentierte UDP akzeptiert, so Rudolf Rohr, geschäftsführender Gesellschafter von Barox. Mit den Switchen der RY-28-Serie kann der Deep Cyber Protection so konfiguriert werden, dass fragmentiertes UDP automatisch erkannt und über die integrierten ACL-Switch-Menüoptionen gestoppt wird, dass fragmentiertes UDP blockiert und Netzwerke und ihre Geräte wie IP-Kameras, VMS und Server vor illegalem Zugriff geschützt werden.

www.barox.de ■

Fortschritt für KI-basierte Cybersicherheit

Die „Eberbacher Gespräche" des Fraunhofer SIT bieten ein Forum für einen Dialog, der sich mit KI-basierter Cybersicherheit beschäftigt. Um der Verwendung von KI als Angriffswaffe entgegenzuwirken, empfehlen die Teilnehmer des Eberbacher Gesprächs die Entwicklung eines nachprüfbaren Code of Conduct. KI könne in der Cybersicherheit wesentlich dazu beitragen, auf aktuelle und zukünftige Bedrohungen in Wirtschaft und Gesellschaft geeignet zu reagieren. Eine Voraussetzung dafür sei, dass die Systeme und ihre Leistungen technisch bewertbar bleiben und spezifische Mindestanforderungen für unterschiedliche Branchen und Anwendungsfelder entwickelt werden, so Michael Waidner, Leiter des Fraunhofer-Instituts für Sichere Informationstechnologie und Athene-Direktor.

www.sit.fraunhofer.de ■

Wie sicher sind vernetzte Produktionsumgebungen?

Die von Baramundi in Auftrag gegebene Studie „Cybersecurity-Niveau in der Operational Technology" des Analystenhauses Techconsult untersucht die Gefährdungslage der vernetzten Produktion in deutschen Industrieunternehmen. Sie zeigt, dass die Gefahren für die Produktionsinfrastruktur vielfach noch deutlich unterschätzt werden. Laut der Studie registrierten knapp die Hälfte der befragten Unternehmen im Verlauf der letzten zwölf Monate einen Cyberangriff auf ihre Produktionsinfrastruktur. Neben klassischem Phishing (Abgreifen von (persönlichen) Daten über gefälschte Websites, E-Mails etc.) und gezielten Angriffen über ungepatchte Schwachstellen waren vor allem manipulierte Speichermedien die häufigste Waffe der Angreifer. In jedem dritten Industrieunternehmen kam es aufgrund von Cyberangriffen schon zum Ausfall oder zur Beeinträchtigung der Produktion.

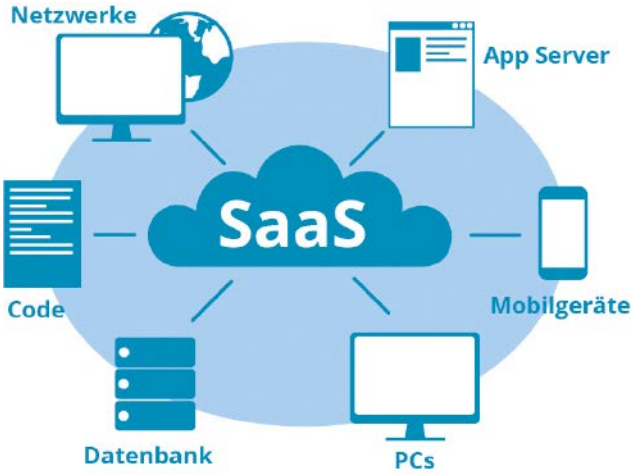
www.baramundi.com ■

SAAS

Wolkig ist das neue heiter

Mit Cloud-Services Geld verdienen: Neue Geschäftsmodelle für Facherrichter

Die Cloud ist der Motor der Digitalisierung. Cloud-Services und speziell der Software-as-a-Service-Markt (SaaS) boomen. Von Microsoft 365 bis zur Dropbox – wir alle kennen oder nutzen diese Programme und Services, viele von uns täglich. Und seit Beginn der Corona-Krise, die den Arbeitsplatz von Millionen Menschen in die eigenen vier Wände verlegt hat, ist die Nachfrage nach cloudbasierten Anwendungen noch einmal steil angestiegen.



War die Cloud vor einigen Jahren noch in erster Linie als besonders sicherer Datenspeicherort interessant, geraten mit SaaS weitere Möglichkeiten in den Blick

Auch hierzulande boomt der SaaS-Markt nicht erst seit Corona. Kleine und mittelständische Unternehmen in Deutschland – zu diesem Schluss gelangt KfW Research – packen die Digitalisierung seit einigen Jahren an. Allerdings wirkt die Pandemie als mächtiger Beschleuniger: „Gerade jetzt", so die Chefvolkswirtin der KfW-Bankengruppe, „zeigt sich besonders, welche Wettbewerbsvorteile sich durch digitalisierte Geschäftsmodelle, Produkte und Prozesse ergeben." Branchenübergreifend gefragt sind Lösungen, die Prozesse straffen und die Qualität der eigenen Produkte und Dienstleistungen steigern.

Neue Geschäftsmodelle für Facherrichter

In diesem Sinne ist auch über der Sicherheitsbranche der Himmel seit geraumer Zeit schon „aussichtsreich bewölkt": War die Cloud hier vor einigen Jahren noch in erster Linie als besonders sicherer Datenspeicherort interessant, geraten mit SaaS zunehmend weitere, spannende Möglichkeiten in den Blick, die mit der Verfügbarkeit von Services über das Internet einhergehen.

▲ **Branchenübergreifend gefragt sind Lösungen, die Prozesse straffen und die Qualität der eigenen Produkte und Dienstleistungen steigern.**

So verschiebt sich auch in der Physical Security der Fokus von der Hardware zur Software, vom Produkt zum Service. Für den Kunden ist dies attraktiv, weil Lizenz-, Abo- und Pay-per-Use-Modelle nicht als Investitionsausgaben, sondern als Betriebskosten zu Buche schlagen, mehr Flexibilität bieten und natürlich günstiger sind. Anbieter wiederum können sich auf jahrelang regelmäßig wiederkehrende Einnahmen und eine hohe Kundenbindung freuen.

Auch der klassische Facherrichter kann vom enormen Wachstum attraktiver SaaS-Produkte profitieren, die Anwendern intelligente Services mit echten Mehrwerten in Form von Komfort, Zeitgewinnen oder Sicherheit bieten – denn bei cloudbasierten SaaS-Lösungen im B2B-Umfeld, wie sie z. B. über das Videor-Partnernetzwerk für die vertikalen Märkte Einzelhandel, Öffentlicher Raum und Transportwesen vertrieben werden, gehören Anbieter, Distributor und Facherrichter zum Geschäftsmodell. Errichter des Partnernetzwerkes werden gemeinsamen von Videor und Herstellern geschult und zertifiziert und treten in ihrer Region eigenständig als Multiplikatoren auf.

Beispiel Termin- und Warteschlangenmanagement

Der Partnernetzwerk-Errichter installiert also zunächst die Hardware vor Ort beim Kunden und richtet den Cloud-Service ein. Zum

Cloud-Services bieten neue Geschäftsmodelle für Facherrichter

Beispiel Clever Q, eine Lösung für das digitale Termin- und Wartezeitenmanagement, dessen Nutzen angesichts des bevorstehenden Corona-Herbstes (und Winters) unmittelbar einleuchtet: Herzstück der von der Business Intelligent Cloud GmbH (B.I.C.) entwickelten Lösung ist die gleichnamige App, die das orts- und zeitungebundene digitale Ziehen von Wartenummern sowie Terminbuchungen und -absagen ermöglicht und den Nutzer über Wartezeiten informiert. Dadurch reduziert sich die Wartezeit und damit das Kontaktrisiko mit SARS-CoV-2 auf ein Minimum.

Die Mehrwerte der Lösung bleiben über die Pandemie hinaus, schließlich zahlt der Service auf Kundenerlebnis und Kundenzufriedenheit ein und reduziert den Personalaufwand. Die Finanzämter in Schleswig-Holstein sowie etliche Gemeinden und Kreise nutzen Clever Q bereits für die Steuerung ihres Kundenverkehrs, doch auch immer mehr Ärzte, Frisöre und Einzelhändler entdecken die Vorteile des cloudbasierten Services für sich.

Regelmäßig kassieren

Die Installation und Einrichtung der Hardware und Software rechnet der Partnernetzwerk-Errichter wie üblich ab. Der Kunde zahlt aber natürlich auch für seine Clever Q-Lizenzen. Und an diesen monatlich oder quartalsweise anfallenden Lizenzgebühren verdient der Errichter über die gesamte Laufzeit mit, ohne weiter etwas tun zu müssen.

Abgesehen von diesen regelmäßig wiederkehrenden Einnahmen spricht für den Einstieg in den SaaS-Markt, dass der Errichter wertvolle Erfahrungen sammelt im lukrativen Zukunftsgeschäft mit cloudbasierten Services, das gerade erst Fahrt aufnimmt. Neben dem digitalen Termin- und Wartezeitmanagement bergen video- und sensorbasierte Analytics-Lösungen für Einzelhandel, Verkehr und Logistik sowie der große Bereich der biometrischen Zugangskontrolle und Zeiterfassung beachtliche Umsatz- und Wachstumschancen für Errichter aus der Sicherheitsbranche. ■

Herzstück der Lösung Clever Q ist die gleichnamige App

Kontakt

Videor E. Hartig GmbH
Rödermark
Tel.: +49 6074 888 0
info@videor.com
www.videor.com/de/cloud-based-services

VIDEO

Die Qual der Wahl

Bereichsüberwachung: Ultra-HD, multidirektional, 360-Grad oder PTZ-Kameras?

Systemdesigner haben viele Möglichkeiten, wenn es um die Auswahl geeigneter Kameras für die Videoüberwachung großer Flächen geht. Uri Guterman, Head of Product & Marketing bei Hanwha Techwin Europe, gibt einen Überblick über die gängigsten Kameratypen.

PTZ-Kameras

PTZ-Kameras werden üblicherweise zur Überwachung von Städten oder Großflächen wie Flughäfen, Parkhäuser, Einkaufszentren, Sportstadien und Lagerhäuser eingesetzt. Nutzer sind damit in der Lage, Bewegungen von Objekten zu verfolgen und heranzuzoomen, um jede Aktivität aus nächster Nähe zu beobachten.

Dank dieser Möglichkeit können Sicherheitsverantwortliche schnell auf jeden Vorfall reagieren. Darüber hinaus verfügen viele PTZ-Kameras über eine automatische Nachführung, kontinuierliche Schwenkfunktion und eine voreingestellte Positionssteuerung, so dass ein sich bewegendes Objekt auch dann erfasst und aufgezeichnet wird, wenn das Sicherheitspersonal abgelenkt oder nicht am Arbeitsplatz ist. Auch die abschreckende Wirkung von PTZ-Kameras, die automatisch einen Bereich absuchen, sollte nicht unterschätzt werden. Potenzielle Straftäter fühlen sich beobachtet, selbst wenn die aufgenommenen Bilder nicht in Echtzeit überwacht werden.

8K-Kameras

PTZ-Kameras spielen nach wie vor eine große Rolle bei der Absicherung gegen kriminelle Aktivitäten, doch neue Entwicklungen in der Videoüberwachungstechnologie haben innovative Kameratypen ermöglicht, die je nach Anwendung noch besser geeignet sein können. Die Schärfe und Klarheit der Bilder von 8K-Videoüberwachungskameras beispielsweise hätte man noch vor kurzem nicht für möglich gehalten.

In der Regel werden 8K-Kameras nicht nur für die Überwachung eines Sichtfelds eingesetzt. Der besondere Vorteil dieser Kamera ist die Leistungsfähigkeit ihrer Bilder, die 16 mal 1080p Full HD-Bildern entspricht. Damit erfasst und verarbeitet eine einzige Kamera eine beeindruckende Menge an Informationen. Sicherheitsverantwortliche können so digital in einen sehr kleinen Teil hereinzoomen, ohne dass das Bild verpixelt wird. Fußballstadien sind beispielsweise Einsatzgebiete für 8K-Kameras, da sie beweiskräftige Bilder von 20.000 oder mehr Fans auf einer Tribüne erfassen. Aufgrund ihres sehr guten Preis-Leistungs-Verhältnisses sind 8K-Kameras eine praktikable und kostengünstige Alternative zum Einsatz mehrerer stationärer oder PTZ-Kameras.

Für jede Situation die passende Lösung

Bei der Entscheidung zwischen 8K- oder PTZ-Kameraformat kommt es auf das konkrete Ziel des Kunden an. Auch die Budgetgröße beeinflusst die Auswahl. Eine 8K-Kamera ist eine leistungsstarke Option, wenn das Sichtfeld einer Kamera kontinuierlich aufgezeichnet werden soll, während das Personal gleichzeitig in einen bestimmten Bildbereich hineinzoomen können muss. PTZ-Kameras sind hingegen deutlich günstiger und eignen sich beispielsweise, wenn ein großer Sichtbereich ständig abgesucht und gleichzeitig bei Bedarf schnell herangezoomt werden soll, um das Geschehen im Detail zu beobachten.

Wenn die Echtzeit-Überwachung wichtiger ist als die Videoaufzeichnung zu Beweiszwecken, spricht das für den Einsatz von PTZ-Kameras. Dies gilt umso mehr für die neueste Generation, die mit adaptiver IR-Technologie ausgestattet ist. Das bedeutet, das sich der Winkel der eingebauten IR-LEDs an die jeweilige Zoomstufe anpasst.

Multisensorische und multidirektionale Kameras

Multidirektionale Kameras bieten die Funktionen von zwei, drei oder vier Geräten in einem einzigen Gehäuse. Da sie jedoch nur über eine einzige IP-Verbindung verfügen, müssen Nutzer auch nur eine VM-Lizenz erwerben.

Die mit zwei getrennten Objektiven ausgestatteten Kameras sind für die Erfassung von hochauflösenden Bildern benachbarter Bereiche konzipiert. Je nach erforderlichem Sichtfeld gibt es eine Auswahl an Modulen mit austauschbaren, einfach zu montierenden Objektiven. Diese Multi-Streaming-Kameras reduzieren die Installationskosten deutlich, denn L-förmige Bereiche wie Korridore oder zwei Seiten eines Gebäudes können nun mit nur einer Kamera überwacht werden.

Auch multidirektionale Kameras mit vier separaten Sensoren sind erhältlich. Mit diesen können Sicherheitsverantwortliche aus einer breiten Palette von anpassbaren Winkeln und Zoom-Einstellungen pro Sensor wählen. Dies bedeutet spürbare Kosteneinsparungen sowohl für Systemintegratoren als auch für Endkunden, da Multisensor-Kameras die Aufgaben von bis zu vier herkömmlichen Geräten übernehmen können, dabei aber weniger Kabel, Leitungen und Montagematerial nötig sind. Da weniger Netzwerkverbindungen erforderlich sind, bedarf es auch weniger Switches.

Konzipiert für die Überwachung großer offener Flächen mit nur einer Kamera,

können die von den vier Sensoren erfassten Bilder nahtlos zu einem Panoramabild zusammengefügt werden, das bis zu 220° abdeckt. Werden Modelle mit motorisierten PTRZ-Kardanringen eingesetzt, erleichtert dies die Installation deutlich. Das Sicherheitspersonal kann das Objektiv ferngesteuert schwenken, neigen und drehen, um das Sichtfeld der Kamera einzustellen.

Eingebautes PTZ

Einige Hersteller wie Hanwha Techwin bieten 4-Kanal-Multisensorkameras mit einer zusätzlichen integrierten PTZ-Kamera an. Diese kann so konfiguriert werden, dass sie automatisch heranzoomt und ein sich bewegendes Objekt verfolgt oder sich zu einer konfigurierten voreingestellten Position bewegt, wenn die Bewegungsmelderfunktion der Kamerasensoren eine Aktivität feststellt.

Diese zusätzliche PTZ-Kamera bedeutet geringere Investitions-, Installations- und Wartungskosten im Vergleich zur Installation von fünf separaten Kameras für die Überwachung eines großen Bereichs bei gleicher Funktionalität.

360-Grad Kameras

Eine einzige 360-Grad-Kamera ist in manchen Fällen die effizienteste und kostengünstigste Möglichkeit, einen großen Bereich zu überwachen. Dies gilt gerade dann, wenn üblicherweise mehrere Standardkameras nötig wären, um tote Winkel zu vermeiden. Für Einzelhändler oder andere Einsatzgebiete, bei denen die Ästhetik eine Rolle spielt, ist die 360°-Kamera eine praktische Kompaktlösung.

Da die 360-Grad-Modelle keine beweglichen Teile haben, sind die Wartungskosten niedriger als bei anderen Kameratypen. Die meisten 360-Grad- oder „Fischaugenobjektiv"-Kameras bieten eine Vielzahl alternativer Betrachtungsmodi wie Einzelpanorama-, Doppelpanorama- und Vierfachansicht. Sie verfügen häufig auch über ein digitales PTZ, das es dem Nutzer ermöglicht, bestimmte Bereiche für eine detailliertere Ansicht elektronisch zu schwenken, zu neigen und zu zoomen, während sie weiterhin die gesamte 360-Grad-Ansicht überwachen und aufzeichnen. Manche Kameras bieten dabei eine integrierte Entzerrungsfunktion. Falls diese nicht vorhanden ist, kann eine Videomanagementsoftware wie Wisenet WAVE diese Aufgabe übernehmen.

Die Qual der Wahl

Bei der Vielzahl verschiedener Kameraformate stehen Sicherheitsberater, Systemdesigner und Integratoren vor einer großen Herausforderung bei der Entscheidung über die richtigen Kameras für ihr Videoüberwachungsprojekt.

Eine Möglichkeit ist dabei die Risikobewertung unter Berücksichtigung der betrieblichen Anforderungen des Endkunden. Eine 8K-Kamera bietet sich zum Beispiel an, wenn große Menschenmengen in weitläufigen Bereichen überwacht werden müssen, während sich multidirektionale Kameras ideal für die Erfassung von Bildern angrenzender Bereiche eignen. PTZ-Kameras sind wiederum dann sinnvoll, wenn die aufgenommenen Bilder in Echtzeit betrachtet werden sollen, da sie den Nutzern ein hohes Maß an Kontrolle bieten und sie die Bewegung von Personen aktiv verfolgen können. Auch ihre größere Abschreckungswirkung sollte nicht unterschätzt werden.

In der Praxis ist für die meisten Hochsicherheitsanwendungen meist eine Kombination von zwei oder mehr Kameratypen erforderlich. Abhängig ist das je nach Projekt von den verschiedensten Faktoren. Dazu gehören möglicherweise die erforderliche Bildauflösung oder die Notwendigkeit eingebauter IR-Beleuchtung, um unabhängig von den Lichtverhältnissen hochwertige Bilder aufzuzeichnen. Auch der Bedarf an Videoanalyse und die Frage, ob die Kameras in der Lage sein müssen, Spezialanwendungen von Drittanbietern zu unterstützen, sollte berücksichtigt werden. Das gilt genauso für Aspekte wie die Anforderungen an die Bandbreite. Wir empfehlen, mit vertrauenswürdigen Herstellern zusammenzuarbeiten und diese um eine Live-Demonstration der verschiedenen Kameratypen zu bitten. So können Anwender fundiert beurteilen, welche Kameras über das richtige Preis-Leistungs-Verhältnis für Ihre spezifischen Anforderungen verfügen. ■

Kontakt

Hanwha Techwin Europe
Eschborn
Tel.: +49 6196 7700 494
htesecurity@hanwha.com
www.hanwha-security.eu/de

Aufzugsnotruf modernisieren ▲

Schneider Intercom bietet normkonforme Notrufeinrichtungen. Die Betriebssicherungsverordnung (BetrSichV) für Aufzüge, die von Personen genutzt werden, verschärft die Vorschriften für Aufzugbetreiber, wie das Unternehmen mitteilt. Aufzüge gelten weitestgehend als Arbeitsmittel. Das erfordert Aktionen des Arbeitgebers (Betreibers). Die Anlagen werden strenger geprüft, Modernisierungen und moderne Notrufsysteme werden zur Pflicht. Im Fahrkorb muss bis spätestens 31.12.2020 ein wirksames Zweiwege-Kommunikationssystem entsprechend der DIN EN 81-28 installiert sein, über das ein Notruf ständig erreicht werden kann. Das Kommunikationssystem könne dabei ausdrücklich auch mit einer Mobilfunkverbindung zum Notdienst arbeiten. Es sei somit kein Festnetzanschluss mehr erforderlich. Das betreffe alle Aufzugsanlagen, die zu wirtschaftlichen oder gewerblichen Zwecken von Personen genutzt werden.

www.schneider-intercom.de ■

Outdoor-Switch für Signalverlängerung

Der ALL-PR2013O-30W ist ein kleiner 2-Port PoE-Switch oder PoE-Repeater und verlängert das PoE-Signal um jeweils 100 Meter. Diese Länge ist normalerweise die maximale Entfernung für die PoE-Versorgung aus Strom und Daten. Mithilfe des Repeaters können bis zu 300 Meter PoE erreicht werden, wenn alle 100 Meter ein neues Gerät installiert ist. Dies ist nur möglich, weil es sich um ein aktives Gerät handelt und das Signal immer wieder neu aufbereitet wird. Durch die Zertifizierung für Schutzklassen IP67 ist das Produkt für den Outdoorbereich geeignet, da es staubdicht und gegen starkes Spritzwasser und kurzes Untertauchen geschützt ist. Genutzt werden kann das Gerät z. B., um eine Outdoor-IP-Kamera und einen Accesspoint gleichzeitig mit Strom und Daten zu versorgen, bei Anbindung von zwei IP-Kameras bei gleichzeitiger Stromversorgung, ein Notfall-IP-Telefon außerhalb des Firmengebäudes zu installieren oder um eine längere Strecke zwischen zwei Gebäuden zu überbrücken.

www.allnet.de ■

Videosicherheitslösungen in Bildungseinrichtungen

Mobotix hat Videosicherheitslösungen für den Bereich Bildung & Wissenschaft im Portfolio, die Schule, Lernen und Studieren sicher machen. Primär gilt es, unberechtigten Zutritt zum Schulgelände zu verhindern und nur autorisierte Besucher zuzulassen. Weiteres Gefahrenpotenzial besteht intern: Vandalismus, Mobbing und Gewalt von bzw. unter den Schülern sind Themen, die hier und da auftreten können. Natürlich sind auch Rauch- und Brandfrüherkennung wichtige Bausteine für ein sicheres Lern- und Lebensumfeld. Zusätzlich sind durch die Covid-19-Pandemie neue Anforderungen rund um den Gesundheitsschutz in den Fokus gerückt. In all diesen Bereichen kann Videotechnologie zuverlässige Unterstützung leisten.

Sicherheit auf dem Campus mit Videotechnologie von Mobotix

Mobotix sichert Außenbereiche

Die Videotechnologie des Herstellers hilft, unberechtigten Zutritt zu verhindern und den Zugang zu Gebäuden oder einzelnen Bereichen gezielt zu regulieren. Zudem kann die Türöffnung, beispielsweise über RFID-Chipkarten, Zutrittscodes und Identifizierung autorisierter Personen anhand ihres Gesichts, völlig kontaktlos erfolgen. Eine Übersicht in Echtzeit ist möglich und hilft auch in Notsituationen – z. B. bei Evakuierungen – herauszufinden, ob und welche Personen sich wo aufhalten. Dasselbe funktioniert auch mit Fahrzeugen: An Einfahrten und Parkplätzen können diese über das Kennzeichen automatisch erfasst und mit Datenbanken abgeglichen werden.

Über die offene Video-Systemplattform Mobotix 7 lassen sich zahlreiche Kamera-Apps für eine intelligente Videoanalyse nutzen. Sie registrieren z. B. herrenlose Gepäckstücke, entwendete Einrichtungsgegenstände, können verdächtige Personen aufspüren, zählen Personen, erkennen Überfüllungssituationen oder alarmieren beim Überschreiten von virtuellen Sperrlinien zum Einbruchschutz. Spezielle Gehäuse und Ausführungen schützen die Videotechnologie zudem vor Vandalismus. In speziellen Bereichen empfiehlt sich der Einsatz von Thermalbildkameras. So kann z. B. eine E-Mail an die Gebäudewartung gesendet werden, wenn das auf die unsichtbare Wärmestrahlung reagierende System eine ansteigende Überhitzung in einem IT-Serverraum oder Labor noch vor Ausbruch eines gefährlichen Brandes feststellt.

Für den Außenbereich bieten die Videosysteme in robuster, wetterfester Ausführung mehrere simultane Sensoren. Die breite Auswahl an austauschbaren Sensormodulen kann auf die Bedürfnisse der jeweiligen Bildungseinrichtung konfiguriert werden. Es gilt, Gefahren rechtzeitig zu erkennen und zu vereiteln: So könnte z. B. automatisch ein Flutlicht erstrahlen, falls ein Unbefugter außerhalb der Öffnungszeiten den Campus betritt. Auf Wunsch auch kombiniert mit einer akustischen Warnmeldung.

www.mobotix.com ■

Analog-HD-Mini-Dome-Kamera

Die Analog-HD-Mini-Dome-Kamera von Abus ist gut für eine Nachrüstung geeignet. Die Kamera nutzt die bestehende CCTV-Infrastruktur, wie Koaxialkabel oder 2-Draht. Somit müssen nur die Kameras und Rekorder getauscht werden. Mit ihrer 2 Megapixel-Auflösung und True-WDR gleicht sie Hell/Dunkel-Kontraste wirksam aus. Die Funktion sorgt in kontrastreichen Licht-Situationen für gleichmäßige Vorder- und Hintergrundszenarien. Eine leistungsstarke IR-LED-Technik sorgt für eine gute Ausleuchtung bis zu 20 Meter bei Nacht. Die Kamera ist wettergeschützt (IP 67) und damit für den Außeneinsatz geeignet. Leitungslängen bis zu 500 Meter sind verlustfrei möglich. Die Kamera wird für die Überwachung weitläufiger Areale im Innen- und Außenbereich eingesetzt und hat einen hochwertigen Bildaufnehmer. Dieser sorgt für ein gestochen scharfes und flüssiges Bild, wodurch Details besser erkannt werden können.

www.abus-sc.de ■

Rundumblick mit 12-MP-360°-Kamera

Die 12-Megapixel-360-Grad-Kamera GD-CI-BT12617F von Grundig Security mit Panomorph-Objektiv sorgt für eine gute Auflösung und Darstellung einzelner Bildbereiche. Die integrierte Dewarping-Funktion ermöglicht insgesamt 18 Anzeigemodi, darunter auch 360°-Panoramen mit digitaler PTZ-Ansicht. Die Bilder können wahlweise in Form einer Kuppel oder eines Zylinders dargestellt werden. Beide Darstellungen bieten umfassende Möglichkeiten, das Bild nach Bedarf anzupassen. Die Kamera kann eine „Heatmap" erstellen. Auf diese Weise können bestimmte Bewegungsabläufe dargestellt werden, deren Intensität durch verschiedene Farben sichtbar gemacht wird. Verschiedene Berichte (täglich, monatlich usw.) stehen zur Verfügung und können exportiert werden. Bewegungen können an einem Schnittpunkt oder einer Kreuzung analysiert und dargestellt werden. Die Kamera hat eine integrierte Softwarelösung zur Personenzählung.

www.grundig-security.com ■

Sicherheitslösung für Sportveranstaltungen

EPS stellt zusammen mit seinem Partner Accellence Technologies Sicherheitslösungen für Sportvereine und Veranstalter vor. Mit Vimacc, Videomanagement in Verbindung mit mobilen Terminals, können Besucher vor den Standardkontrollen auf die Einhaltung der Vorschriften (Mund-Nasen-Bedeckung) sowie deren Körpertemperatur kontrolliert werden. Wenn dabei ein Risikofall detektiert wird, werden durch intelligentes Videomanagement nötige Fachkräfte automatisch informiert und der betroffene Zuschauer in einen separaten Bereich geleitet. So lässt sich auch der Risikofaktor gegenüber den restlichen Zuschauern minimieren. Durch diese technische Lösung werden zusätzlich mögliche Fehler oder Manipulationsversuche des Personals minimiert. Die Terminals sind nicht nur mobil, sondern können auch individuell konfiguriert werden.

www.eps-vertrieb.de ■

VIDEO

Wieder geöffnet

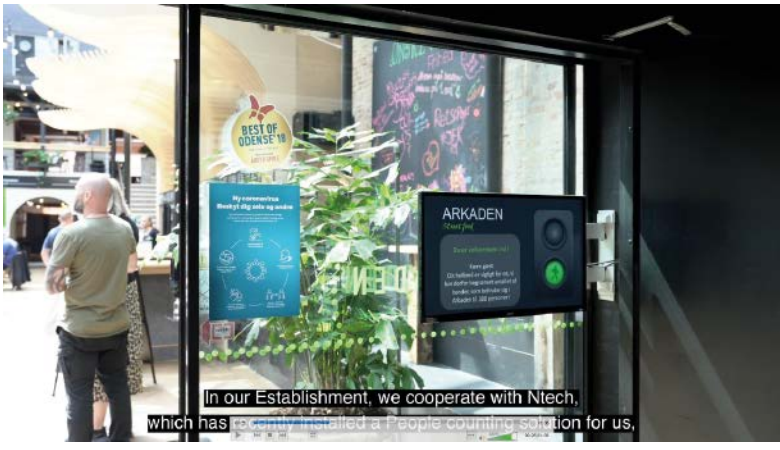
Dänisches Restaurant nutzt Lösung zur Personenzählung und Flusskontrolle

Seit dem Beginn der Covid-19-Ausbreitung in Dänemark hat die dänische Regierung alle Restaurants, Bars und andere Geschäftsbereiche geschlossen. Um den Back-to-Business-Richtlinien der Regierung gerecht zu werden, ist Arkaden Street Food, eine beliebte Schlemmermeile in Odense mit Platz für 308 Personen, verpflichtet, die Anzahl der Gäste pro Quadratmeter unter einem bestimmten Wert zu halten. Aus Verantwortung für ihre Kunden und Mitarbeiter setzte die Markthalle die Lösung zur Personenzählung und Flusskontrolle von Dahua ein, um damit eine reibungslose und sichere Wiedereröffnung nach der Pandemie zu gewährleisten.

Manuelles Zählen überflüssig

Die Markthalle verfügt mit 14 Essensständen und 2 Bars über zwei Eingänge. Die Gästezahlen an diesen beiden Eingängen sollen zusammengerechnet und auf Bildschirmen präsentiert werden, um bestimmen zu können, ob es noch genug Platz für die Kunden gibt und sie eintreten dürfen oder kurzzeitig vor der Tür warten müssen.

Die auf die Bedürfnisse der Markthalle abgestimmte Lösung besteht aus fünf Kameras der Serie IPC (HDW5442E-ZE) an den beiden Eingängen, zwei 2 DPB18-AI und zwei DHL32-F600 und der DSS Pro Lizenz für 64 Kanäle und dem BI-Modul. Die KI-betriebene Kamera zur Personenzählung von Dahua kann automatisch und präzise in Echtzeit die Anzahl der Personen berechnen, die das Restaurant betreten. Dadurch wird nicht nur Staubildung vermieden, sondern auch die Ausbreitung der Pandemie eingedämmt. Die DSS PRO-Plattform mit Personenzählung und Flusskontrolle in Verbindung mit Monitoren und DPB18A ermöglicht es den Gästen, verschiedene Videos oder Bilder sowie editierbare Inhalte anzuzeigen. Wenn die Anzahl der Gäste den voreingestellten Wert überschreitet, werden die ankommenden Kunden durch die Plattform benachrichtigt und mithilfe der Anzeige „Der Grenzwert wurde erreicht" auf der digitalen Beschilderung am Eingang der Markthalle sowie auf Monitoren darum gebeten, an der Tür zu warten. Da die Kameras zur Personenzählung außerdem



Die Ampel am Eingang zeigt den Status

einfach und leicht zu installieren sind, konnte der Installateur das gesamte Projekt in nur einem Tag abschließen.

Sicherheit und wertvolle Daten

„Die Lösung zur Personenzählung hat uns wertvolle Statistiken und Informationen über das Verhalten unserer Kunden geliefert. Das spart uns eine Menge Ressourcen, da wir die Kunden nicht mehr physisch an der Tür zählen müssen. Nicht nur das, wir können unsere Gäste am Eingang über die Monitore auch noch mit wichtigen Informationen versorgen. Wir sind mit unserer Zusammenarbeit sehr zufrieden. So wie es aussieht, gibt es auf dem Markt sehr viele innovative Lösungen, die wir gerne ausprobieren würden. Wir sind überzeugt, dass diese Lösungen uns in vieler Hinsicht intelligenter und effizienter arbeiten lassen werden", sagte Sanne Brigsted, Geschäftsentwicklungsmanagerin der Markthalle.

Mithilfe der Lösung zur Personenzählung und Flusskontrolle von Dahua werden angesichts der Auswirkungen von COVID-19 das Sicherheitsniveau und die Wettbewerbsfähigkeit von Geschäftseinrichtungen wie der Arkaden Markthalle gesteigert und gleichzeitig eine angenehme Gastronomieumgebung für die Gäste geschaffen. Vor allem hat das Restaurant dank dieser Lösung sein Hauptziel, die Wiedereröffnung der Speisehalle, erfolgreich erreicht. Nun ist der Betreiber in der Lage, den Kundenverkehr in Echtzeit zu überwachen und Sicherheitsmaßnahmen rechtzeitig zu ergreifen, bevor das Restaurant mit Kunden überfüllt ist. Mit diesem intelligenten System werden zusätzliche Mitarbeiter zum manuellen Abzählen der Kunden an der Tür überflüssig. Dadurch werden die Arbeitskosten erheblich gesenkt und die Effizienz der Restaurantverwaltung verbessert. Darüber hinaus kann der Monitor des Systems als eine Informationstafel für die Kunden oder als ein Mehrzweck-Werbebildschirm mit Ergebnissen des Eventmarketings und der Planung auf der Grundlage der intelligenten Datenanalyse von DSS Pro dienen. Das stellt ein großes Expansionspotenzial für die Plattform dar und schafft neue Geschäftsmöglichkeiten für das Restaurant. ■

Kontakt

Dahua Technology
Düsseldorf
Tel: +49 211 2054 4120
sales.de@dahuatech.com
support.de@dahuatech.com
www.dahuasecurity.com/de

Primion Technology: Zutrittskontrolle, Zeiterfassung und Sicherheitsmanagement auf einer einzigen Plattform

ZUTRITT

Fitnesskur für die Zukunft

Neustrukturierung bei Primion Technology

Jorge Pons Vorberg

Jorge Pons Vorberg steht seit Anfang des Jahres als CEO an der Spitze der Time & Security Division der Azkoyen-Gruppe. Als solcher ist er unter anderem verantwortlich für die Geschäfte der Primion Technology, die in diesem Jahr ihr 25jähriges Bestehen feiert. Matthias Erler von GIT SICHERHEIT sprach mit Jorge Pons Vorberg u. a. über den Umgang des Unternehmens mit der Corona-Krise und die neuen Geschäftsbereiche „Manufacturing“ und „Integration“.

GIT SICHERHEIT: Herr Pons, Sie sind für Primion ja bereits seit vielen Jahren in verschiedenen Funktionen tätig, zuletzt als Finanzchef, später (zunächst interimsweise) CEO für die gesamte Time & Security Division der Azkoyen-Gruppe, zu der Primion gehört. Gleich in die Anfangszeit in diesem Amt fiel nun die Pandemie, mit der wir am besten gleich mal beginnen: Wie erleben Sie diese Krise?

Jorge Pons: Diese Krise wirkt sich geschäftlich je nach Bereich ganz unterschiedlich aus – und zum anderen natürlich auf unsere Mitarbeiter. Geschäftlich gesehen sahen sich Primion und die Töchter in Europa vor große Herausforderungen gestellt, besonders in Spanien und Frankreich, wo das Geschäft zeitweilig coronabedingt stillstand. In Deutschland ging das Geschäft weiter, aber mit Einschränkungen. Den Auftragsrückgang von etwa 12 Prozent und einen Umsatzrückgang von 20 Prozent im Zeitraum März bis Mai, also während des Lock-Downs, konnten wir auffangen. In Deutschland, aber auch in Belgien konnten

▲ Die Lösungen von Primion finden sich praktisch in allen Branchen – von Öffentlicher Verwaltung und Gesundheitswesen bis zu Flughäfen, Logistik und Industrie

▲ Die Advanced Data Terminals 1100 von Primion kommen im eleganten Aluminumrahmen und Echtglas-Display – mit anpassbaren Buchungsarten und aussagestarker Menüführung

wir auf einen guten Auftragsbestand zurückgreifen. Die Gesundheit unserer Mitarbeiter und ihrer Familien steht an vorderster Stelle. Das bedeutet zum Beispiel, dass, wo möglich, im Home-Office gearbeitet werden konnte. Zumindest in Deutschland brauchten wir nicht auf Kurzarbeit zurückzugreifen. Insgesamt haben wir zum Glück in der Belegschaft nur sehr wenige Fälle, bei denen das Virus positiv getestet wurde.

Welche Veränderungen sehen Sie bei Ihren Kunden und im Sicherheitsmarkt im Allgemeinen?

Jorge Pons: Wir beobachten bei unseren Kunden eine deutliche Veränderung in den Anforderungen für die Identifizierung von Besuchern im Unternehmen. Auch werden neue Arbeitsmodelle entwickelt. Der Trend zum Work-Life-Blending bekommt unter Corona-Bedingungen eine höhere Relevanz – das betrifft nicht nur die Zeiterfassung. Auch beim Zutritt brauchen wir flexiblere Lösungen in den Berechtigungen, die auf die ortsunabhängigere Arbeitsweise der Mitarbeiter Rücksicht nimmt. Die Software muss diesen gesamten Workflow und alle veränderten Prozesse abbilden. Das alles muss schnell gehen, benutzerfreundlich und für den Administrator gut organisierbar sein. Der Mitarbeiter, der sich auf ein Schiff ins Mittelmeer zurückzieht, um dort eine Software zu programmieren, ist kein Exot mehr. Für den Arbeitgeber ist das ein machbares Modell – man muss es nur darstellen.

◀ Das Advanced Data Terminal 1100 von Primion

Diese Entwicklungen werden vermutlich auch langfristig unsere Arbeitswelt verändern?

Jorge Pons: Ja genau, denn hier geht es um die zuverlässige Vernetzung von Systemen. Für uns bedeutet das, dass wir unsere flexiblen Lösungen stetig weiterentwickeln. Es geht um die Konnektivität zwischen Türen, Ausweisen und Lesern. NFC und BLE spielen eine wichtige Rolle. Der Bedarf steigt – und wir werden die Antworten liefern. Ein weiteres Stichwort: Schnittstellen. Die vielen verschiedenen Sicherheitssysteme innerhalb eines Gebäudes müssen zusammenarbeiten und übersichtlich verwaltet werden können. Außerdem werden Biometrie und Videotechnik in der Zutrittskontrolle immer wichtiger. In Corona-Zeiten macht es z. B. Sinn, dass ein Mitarbeiter vor Betreten des Gebäudes seinen Ausweis an einen Leser hält, parallel dazu die angeschlossene Thermalkamera die Körpertemperatur misst und der Leser dann bei Überschreiten eines Grenzwertes den Zugang blockiert. Ähnliche Szenarien gibt es auch für externe Besucher. Wir setzen solche Lösungen verstärkt ein – insbesondere an internationalen Flughäfen mit großem Publikumsverkehr etablieren sie sich

immer mehr. Langfristig werden aus unserer Sicht zwei Themen zunehmend wichtiger. Zunächst einmal das Identity-Management: Die Anforderungen an den Umgang mit persönlichen Daten, z. B. durch Ausweisverwaltungssysteme, werden immer größer. Hier geht es verstärkt um Sicherheitsüberprüfungen und Datensicherheit und nicht wie in der Vergangenheit nur um das Ausdrucken von Karten. Man möchte wissen, wer da ins Unternehmen kommt – das ist ein unabdingbarer Beitrag zur Sicherheit. Diese Notwendigkeit ist umso stärker, je größer das Unternehmen ist. Für Kritische Infrastrukturen gilt das zum Beispiel ganz besonders. Das andere ist das bereits erwähnte Thema Konnektivität.

Der Fokus liegt für Primion ja nach wie vor auf dem Zutrittsthema – neben der Zeiterfassung. Wie sind hier die Proportionen? Wird das auch künftig so bleiben?

Jorge Pons: Zutrittskontrolle und Zeiterfassung werden ergänzt durch unser PSM (Physical Security Management) und die Software für die Besucherverwaltung. Was das Volumen angeht, kann man sagen, dass Zutritt bei uns mehr als die Hälfte des Geschäftes ausmacht. Das liegt auch daran, dass bei Zutrittssystemen mehr Komponenten benötigt werden– wohingegen bei der Zeiterfassung die Dienstleistungen im Vordergrund stehen. Generell muss man aber anmerken, dass alle Lösungen individuell sind. Jedes Unternehmen hat eigene Prozesse. Es geht also nicht mehr so sehr darum, welche Zeiterfassungs- und Zutrittslösung besser ist, sondern darum wie gut und schnell diese an den jeweiligen Kundenprozess angepasst werden kann. Wir bewegen uns also in einer gegenseitigen Abhängigkeit von Menschen, Sicherheit und Prozessen. Letztere müssen effektiv und zuverlässig sein: neue Berechtigungen, mehr Türen, oder ein neuer Tarifvertrag.

Sie haben vor kurzem den neuen Geschäftsbereich „Integration" eingeführt – den Rahmen dafür bildet eine Restrukturierung. Neben Integration sind das die Bereiche Manufacturing und Central Management. Welche strategischen Erwägungen stecken hinter dieser Entscheidung?

Jorge Pons: Zunächst einmal haben wir festgestellt, dass wir im Grunde zwei verschiedene Geschäftsmodelle betreiben: Auf der einen Seite steht der Bereich Manufacturing mit der Aufgabe, Produkte und Lösungen in enger Zusammenarbeit mit dem Kunden zu entwickeln und zu fertigen. Über den Bereich Integration werden die Kunden betreut und die Aufträge abgewickelt. Das umfasst unter anderem die Beratung in den Prozessen, das Projektieren usw. Durch die stärkere Trennung dieser beiden Bereich kann sich jede Seite besser auf ihre eigentliche Aufgabe fokussieren. Durch die Einführung einer dritten Einheit (Central Management) profitieren alle Beteiligten von erheblichen Synergieeffekten, da wir hier die Finanzen, das Marketing und die gesamte Administration für die Bereiche Integration und Manufacturing zusammenhalten. Außerdem ist diese neue Aufstellung auch Ausdruck unserer Werte bei Primion Technology.

Inwiefern?

Jorge Pons: Die neue Struktur stärkt unsere Kundenbindung, die Ergebnisorientierung und Teamarbeit, die Professionalität und das Vertrauen. Wir wollen Worthalten – und das setzt Fokussierung und Effizienz voraus. Unsere Mitarbeiterinnen und Mitarbeiter können so noch gezielter und mit einem klaren Rollenverständnis noch effizienter arbeiten.

Welche Wachstumspläne verfolgen Sie in der näheren Zukunft – sei es organisch oder durch Zukäufe? Oder wollen Sie sich im Gegenteil von Bereichen trennen?

Jorge Pons: Unsere Priorität ist zurzeit erst mal die Restrukturierung im Sinne der eben besprochenen drei Einheiten. Wir wollen die Zeit der Krise so gut wie möglich nutzen, um uns verstärkt der Stabilisierung und Stärkung unseres Unternehmens zu widmen. Anschließend werden wir uns wieder Gedanken machen, wie es weitergeht und wie wir wachsen können.

Sie feiern bei Primion in diesem Jahr Ihr 25. Firmenjubiläum. Wie begehen Sie dieses erste Vierteljahrhundert?

Jorge Pons: Größeren Feiern steht leider in der Tat die Corona-Krise im Wege. Wir hoffen, dass die Bedingungen im kommenden Jahr günstiger sind und wir die Feier dann nachholen können. Aber auch wenn wir nicht feiern können: Wir sehen das Jubiläum als wichtigen Meilenstein und als Verpflichtung, unsere Erfolgsgeschichte in den nächsten mindestens 25 Jahren fortzuschreiben. ■

Kontakt

Primion Technology GmbH
Stetten am kalten Markt
Tel.: +49 75 73 95 20
info@primion.de
www.primion.de

Antimikrobielle Beschläge

Um die in der Corona-Pandemie erforderlichen Hygienemaßnahmen zu unterstützen, hat Dom Security antimikrobielle Oberflächen für digitale Beschläge, digitale Zylinder und Panikstangen entwickelt. Durch das Anfassen von Türgriffen und -knäufen im Alltag gehören diese zu den beiden am häufigsten berührten Oberflächen in einem Gebäude. An hoch frequentierten Stellen können sie der ideale Nährboden für schädliche Bakterien und Viren sein. Die Panikstangen, digitalen Beschläge und Zylinder wurden mit einer antimikrobiellen Beschichtung versehen. Diese Nanosilber-/Silberionen-Beschichtung bekämpft jede Art von Schimmel, Bakterien, Viren und Pilzen. Basierend auf einer Studie des deutschen Bundesministeriums für Bildung und Forschung weist Silber bereits bei Verwendung von kleinsten Partikeln ein antimikrobielles Verhalten auf. Bis zu 99,9 % der schädlichen Mikroorganismen werden abgetötet.

Wenn eine beschichtete Oberfläche mit Feuchtigkeit aus der menschlichen Haut in Kontakt kommt, reagieren die Silberionen mit der DNA der Bakterien und töten die Bakterien schließlich ab. Ein ähnlicher Effekt tritt bei Pilzen und Viren auf. Darüber hinaus greift Nanosilber laut einer Studie nicht in das Gleichgewicht der Mikroflora unserer menschlichen Haut ein. Die Nanosilberbeschichtung wird auf den Metallelementen der Türgriffe der Guard-Familie, den Metallknäufen des digitalen Schließzylinders Pro sowie auf den Griffflächen der Panikstangen verwendet.

www.dom-security.com ■

Testsieger: Einbruchschutz von Burg-Wächter überzeugt

Die Griffseiten-Sicherung Winsafe WS 33 von Burg-Wächter setzte sich mit der Test-Note „sehr gut“ (0,9) durch. „Stiftung Warentest“ hat in der aktuellen Ausgabe ihres Magazins „Test“ (10/2020) nachrüstbare Fenster- und Türsicherungen untersucht, die den Einbruchschutz deutlich steigern. Gleichzeitig erzielte das Modell die Bestnote aller Test-Kategorien. Den Testern gelang es in der vorgegebenen Zeit von zweimal drei Minuten trotz Werkzeugeinsatz nicht, die Sicherung zu überwinden. Mit der Zeitvorgabe simulierten die Tester einen echten Einbruch. Denn ist das Fenster oder die Terrassentür nicht nach wenigen Augenblicken geöffnet, gehen Einbrecher erfahrungsgemäß kein weiteres Risiko ein und suchen das Weite.

Das Ergebnis von 0,9 sei eine absolute Traumnote bei den Vergleichen von „Stiftung Warentest“, so Gerrit Lüling, Geschäftsbereichsleiter Vertrieb von Burg-Wächter. Die Fenstersicherung ist für Fenster aus Holz, Aluminium und Kunststoff mit Metalleinlage VdS-geprüft und ECB-S-zertifiziert. Die Sicherung wird mit wenigen kleinen Bohrungen und ein paar einfachen Handgriffen stabil befestigt. Die Ver- und Entriegelung per Schiebemechanismus ist einfach. Befindet sich der Schließzylinder in einer geöffneten Position, kann das Schloss auch ohne Schlüssel durch

Drehen entriegelt werden. In einer geschlossenen Position wird zum Entriegeln der Schlüssel benötigt. Eine rote Markierung zeigt den Bewohnern, ob sich die Fenstersicherung in einem verriegelten Zustand befindet. Lästiges Kontrollieren entfällt.

Ein zweites Produkt des Herstellers wurde im Test mit „sehr gut“ bewertet. Die Fenstersicherung Winsafe WS 22 kam auf die Note 1,1. Mit diesem Modell kann man wahlweise ein oder zwei Fenster per Doppelriegel schützen.

www.burg.biz ■

PVD-Beschichtung für Schließzylinder

Die elektronischen Schließzylinder sowie der elektronische Türdrücker von Uhlmann & Zacher werden im Edelstahldesign gefertigt. Um individuellen Ansprüchen gerecht zu werden, bietet der Hersteller das Veredeln von Oberflächen mit einer PVD-Beschichtung an. Diese Beschichtungen bilden eine zusätzliche robuste Hülle um den Griff oder Knauf, sodass die Produkte auch bei intensiver Nutzung widerstandsfähig bleiben. Die Farbpalette reicht bei den elektronischen Schließzylindern von Anthrazit über Gold bis hin zu Bronze.

www.UundZ.de ■

SCMS-App für Videoüberwachung

SCMS ist eine Überwachungs-App von Grundig für Mobiltelefone und Tablets. Unterstützt wird das gesamte Spektrum an Produkten für die Videoüberwachung, einschließlich NVRs, DVRs sowie Netzwerkkameras und Speed Domes, die die Funktion „P2P Cloud“ unterstützen. Bei einem Alarm vor Ort wird der Anwender sofort von der App benachrichtigt. Die App hat unter anderem folgende Features: Echtzeit-Videovorschau von bis zu 16 Kanälen; Wischen für PTZ-Steuerung und Kamerabewegung, Ziehen zum Ein- und Auszoomen im Vorschaumodus. www.abetechs.com ■

ZUTRITT

Kartenlesen nach Maß

VF-Feintechnik erweitert Zutrittskontrolllösungen

Das Unternehmen VF-Feintechnik GmbH aus dem bayerischen Wiesentheid hat sich auf die Entwicklung und Herstellung von maßgeschneiderten Kartenlese- und Zutrittskontrollsystemen spezialisiert. Nun wird das kompakte Komplettsystem zur Identifikation, Personalisierung und Automatisierung der Zutritte mit einem neuen Touchdisplay ausgestattet und bietet dem Anwender noch mehr Flexibilität und Benutzerfreundlichkeit.

◀ **Das Touchdisplay bietet mehr Flexibilität und Benutzerfreundlichkeit**

Die Kartenlese- und Kartenspendesysteme der VF-Feintechnik findet man an Zufahrts- und Zutrittskontrollen – an Drehkreuzen, Schranken, Toren. Das Unternehmen beliefert Banken- und Gebäudeausstatter, Parkplatz- und Parkhaus-Ausrüster, Industriekunden sowie Sicherheits- und Kontrollunternehmen weltweit. Abgestimmt auf die jeweiligen Anforderungen des Kunden werden sowohl einzelne Komponenten der Zutrittskontrolle als auch Komplettsysteme für den Innen- und Außenbereich individuell entwickelt und gefertigt – auch bei kleinen und mittleren Stückzahlen.

Kompaktes Zutrittskontrollsystem

Das sehr kompakte Zutrittskontrollsystem mit universellem motorischen Einzugskartenleser der Baureihe Hybrid eignet sich für kundenspezifische Aufbauten und kann in jede Art von Gehäuse oder Terminal im Innen- und Außenbereich eingebaut werden. Der Kartenleser kann mit sämtlichen Lesetechnologien für die Verarbeitung von Chip-, Magnet- und RFID-Karten im ISO-Format ausgestattet werden. Er verfügt standardmäßig über eine USB- oder Ethernetschnittstelle. Das Zutrittskontrollsystem läuft autark im Stand-Alone-Betrieb, was die Netzlast senkt, und kann per mitgelieferter Software schnell eingerichtet und integriert werden. Zahlreiche Netzwerkschnittstellen sind realisierbar.

Der Kunde hat die Möglichkeit, den Kartenleser individuell zu konfigurieren. Der Shutter kann mit einer Beleuchtung ausgestattet werden und bietet außerdem Schutz vor Umwelteinflüssen und Fremdkörpern. Ein Anti-Skimming-Sensor und Ausbauschutz stehen auch zur Verfügung.

Für optionale Anwendungen können bis zu acht Relais und Optokoppler programmiert werden. Dadurch ist auf Wunsch eine einfache binäre Anbindung an übergeordnete Anlagen wie Ampeln, Schranken, Türöffner oder Signalgeber möglich, die ohne eigene Steuerung betrieben werden.

Touchdisplay für Nutzerfreundlichkeit

VF-Feintechnik GmbH stattet nun das bewährte Zutrittskontrollsystem zur Erfassung und Automatisierung der Personenzutritte bzw. der Fahrzeugzufahrten auf Wunsch mit einem neuen Touchdisplay aus. Das Farbdisplay ist standardmäßig 4,3 Zoll groß, abweichende Displaygrößen sind ebenfalls möglich. So ist eine praktische Programmierung des verbauten Kartenlesers direkt über das Display möglich. ■

Kontakt

VF-Feintechnik GmbH
Wiesentheid
Tel.: +49 9383 90318 0
sales@vf-feintechnik.de
www.vf-feintechnik.de

Einbruchmelderzentrale mit neuen Funktionen

Die Gefahren- und Einbruchmelderzentrale Hiplex 8400 von Telenot lässt sich an aktuelle Anforderungen der Sicherheitsbranche anpassen. Die sechste und siebte Ausbaustufe der Anlage hat zahlreiche neue Funktionen in allen Bereichen hervorgebracht. Dazu gehören unter anderem ein Tagalarmmodul, ein KNX-Interface, verschiedene Discounterfunktionen oder umfassende Zeitmodelle. Die Systemarchitektur der Anlage hat statische Systemgrenzen komplett aufgehoben.

Gut acht Jahre entwickelte das Team von Telenot an der Plattform, um diese serienreif zu machen. Seitdem haben weitere Ausbaustufen den Leistungsumfang kontinuierlich erweitert. Dies gilt auch für die aktuellen Updates mit den Kürzeln F06 sowie F07, die der Hersteller gemeinsam mit der dazugehörigen neuen Version Parametriersoftware Hipas veröffentlicht hat. Die Firmware bildet einen wesentlichen Baustein für die stetig wachsende Vielseitigkeit der Einbruch- und Gefahrenmelderzentrale. Dank der grafischen Software lässt sich jede Hiplex schnell und auf intuitive Weise mit einfachen Klicks, sowie Drag & Drop parametrieren. Das System erkennt dabei, welche Komponente an welchen Schnittstellen angeschlossen werden kann.

Zu den neu integrierten Hardwarekomponenten gehört beispielsweise die Erweiterungsplatine Hislave 8000. Sie erlaubt unter anderem die Erweiterung der Einbruchmelderzentrale um zwei zusätzliche getrennte Bus-1-Stränge mit jeweils 63 Bus-1-Adressen plus 16 konventionelle Meldergruppen. Maximal können bis zu acht Hilsaves 8000 angeschlossen werden, was im Maximalausbau 1.134 Bus-1-Adressen ergibt. Auch die Erweiterungsplatine ISO-Expander C2B für den Anschluss von rückwirkungsfreien, galvanisch getrennten com2Bus-Strängen zur Erhöhung der Anzahl der VdS-gemäßen Sicherungsbereiche ist eine Neuerung der aktuellen Ausbaustufe. Die neue Firmware-Version ist Grundvoraussetzung, um das Tagalarmmodul TM2 C2B zu parametrieren. Mit diesem lassen sich etwa Notausgangstüren überwachen, um deren unberechtigtes Öffnen zu verhindern. Auch ein KNX-Interface oder ein Gebäude-Management-System lassen sich in der neuen Ausbaustufe bedienen.

Die grafische Parametriersoftware Hipas


Einbruchmelderzentrale Hiplex 8400H von Telenot

www.telenot.com ■

Bedienungs-App 2.0 mit smarter Bedienung

Mit der zertifizierten Cross-Plattform-App MCVisu.cloud-App 2.0 von Abi-Sicherheitssysteme werden mobile Geräte wie Smartphones und Tablets zum Smart-Bedienteil für die Gefahrenmelde- und Zutrittskontrollzentralen MC 1500. Die Benutzeroberfläche (GUI) ist in einem zeitgemäßen Design gestaltet und stellt die Benutzerfreundlichkeit in den Fokus. Die Schnittstelle in der Zentrale zum Fernzugriffs- und Applikationsportal MCConnect.cloud wird über den Net-Device-Server NDS realisiert. Der NDS basiert auf einem 32-bit Embedded-System-Modul mit dem Echtzeitbetriebssystem NET+OS. Die Bedienungs-/Visualisierungs-App ist mehrfach zertifiziert (VdS, VSÖ, AV-TEST) und eine Multiplattform-APP (Android, iOS, WEB, WIN). Die App 2.0 ist von AV-Test, einem unabhängigen Forschungsinstitut für IT-Sicherheit in Deutschland, als sicher zertifiziert worden.

www.abi-sicherheitssysteme.de ■

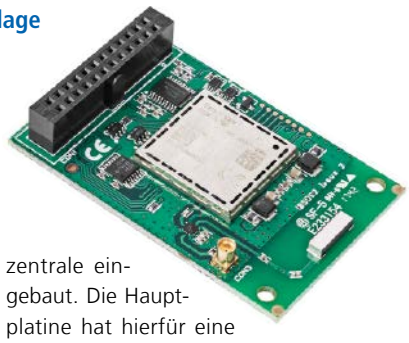
Bewegungsmelder und Snapshot-Kamera

Die PIR Netzwerkkamera V3 von Lupus-Electronics vereint Bewegungsmelder und Überwachungskamera: Mit dem Gerät werden Bewegungen am Gebäude direkt erkannt, per Mini-Snapshot-Kamera aufgezeichnet und an eine App weitergeleitet. Integriert in eine Alarmanlage bietet sie Schutz vor unerwünschten Besuchern und hilft zeitgleich bei der sofortigen Identifikation. Der Bewegungsmelder ist vor allem für Eingangsbereiche geeignet. Sobald der RAS-Sensor eine sich bewegende Person wahrnimmt, wird eine Bildaufnahme erstellt. Die Bewegung wird an die Zentrale weitergeleitet und das Bild umgehend auf ein mit der App verknüpftes mobiles Gerät gesendet. So besteht die Möglichkeit, sofort zu identifizieren, wer oder was die Meldung ausgelöst hat, und gegebenenfalls zu reagieren.

Dank eingebauter IR-LED kann die Netzwerkkamera auch nachts für Schutz sorgen: Bei schlechten Lichtverhältnissen und vollkommener Dunkelheit werden klare Bilder aufgezeichnet. Die Kamera ist batteriebetrieben, die Kommunikation zur Alarmanlage funktioniert über Funk. Somit benötigt man keine zusätzlichen Kabel zur Signalübertragung oder zur Stromversorgung. Die drei Bereiche elektronische Alarmanlage, Smarthome und Videoüberwachungstechnik werden in den Systemen des Herstellers in einer professionellen Anlage vereint.

www.lupus-electronics.de ■

Mobilfunkmodul für Funkalarmanlage



Abus hat ein optionales Zusatzmodul zur redundanten Kommunikation für die Secvest Funkalarmanlage in sein Portfolio aufgenommen. Damit kann ein zusätzlicher Übertragungsweg eingerichtet werden. Bei Ausfall des Festnetzanschlusses ist eine Sprach- und Datenübertragung über das Mobilfunknetz von der Alarmanlage an stationäre und mobile Endgeräte – wie Festnetz- und Mobiltelefone, Tablets oder Desktop-Rechner – und umgekehrt möglich. Das Mobilfunkmodul ist GSM- und LTE-fähig (2G und 4G). Damit können IP-basierte Leitstellenprotokolle (über 2G und 4G), DTMF- und FSK-basierte Leitstellenprotokolle (nur über 2G) und Sprachnachrichten (nur über 2G) sowie SMS übertragen werden. Das Modul wird direkt in die Alarmzentrale eingebaut. Die Hauptplatine hat hierfür eine entsprechende Steckverbindung. Das Modul kann mit einer auf der Platine integrierten oder einer externen Antenne betrieben werden. Die externe Antenne wird direkt am Modul angeschlossen. Das Mobilfunkmodul überträgt Alarmmeldungen an eine Leitstelle oder an ein privates Kommunikationsendgerät via Mobilfunk.

www.abus-sc.de ■

Multitransmitter für intelligente Sicherheitssysteme

Ajax Systems hat einen Multitransmitter auf den Markt gebracht. Das Modul erlaubt das Verbinden veralteter kabelgebundener Melder mit einem Ajax-System, wodurch flexible Einstellungen für Benutzer, Automatisierungsszenarien, Steuermöglichkeiten für Smartphones und weitreichende Aktualisierungsmöglichkeiten genutzt werden können. Das Modul ersetzt die alte Steuereinheit des Sicherheitssystems und dient zum Anschließen kabelgebundener Geräte an eine kabellose Steuereinheit – eine Hub-Zentrale. Dabei werden alle Modelle unterstützt. Das Modul hat 18 Anschlussmöglichkeiten zum Verbinden von Geräten und Manipulationsschutzeinrichtungen, die vier Arten von Kontakten unterstützen: NO, NC (ohne Widerstand), EOL (NC mit Widerstand), EOL (NO ohne Widerstand). Neben den 18 Anschlussmöglichkeiten hat das Modul drei 12-V-Stromausgänge: zwei Hauptausgänge und einen separaten Ausgang für Feuermelder.

www.ajax.systems ■

Zutrittslösung schützt fünffach

Irm-Guard ist eine intelligente Lösung von de Jong, mit der sich fünf wesentliche Aufgaben im Zugangsbereich durchführen lassen: Fieber messen, Masken erkennen, Hände desinfizieren, Besucher registrieren und Zutritt steuern. Das Gerät ist mit einem 5-Liter-Desinfektionsmittelspender, einem 7-Zoll-Monitor und einem 7-Zoll-Terminal ausgestattet. Es desinfiziert sensorgesteuert und kontaktlos. Zudem kann die Zutrittslösung die Körpertemperatur messen und erkennen, ob eine Alltagsmaske getragen wird. Optional lassen sich Personen über eine Gesichtserkennung automatisch für den Zutritt verifizieren und auch eine kontaktlose Registrierung über QR-Code ist möglich. Die Lösung ist eine Schnittstelle für externe Zutrittskontrollen und vielfältig kombinierbar für die Verifizierung und Steuerung von Türen, Toren oder Drehkreuzen. So lässt sie sich eigenständig einsetzen oder auch in vorhandene Sicherheitskonzepte integrieren.

www.irm-guard.de ■

Die GIT SICHERHEIT ist für mich wichtig, weil so viele interessante Artikel darin enthalten sind.“

Stefanie Siemer, Inhaberin und Geschäftsführerin der Elektro Siemer GmbH

SYSTEM 3060

Digitale Schließanlagen mit Zutrittskontrolle

The finest in keyless security

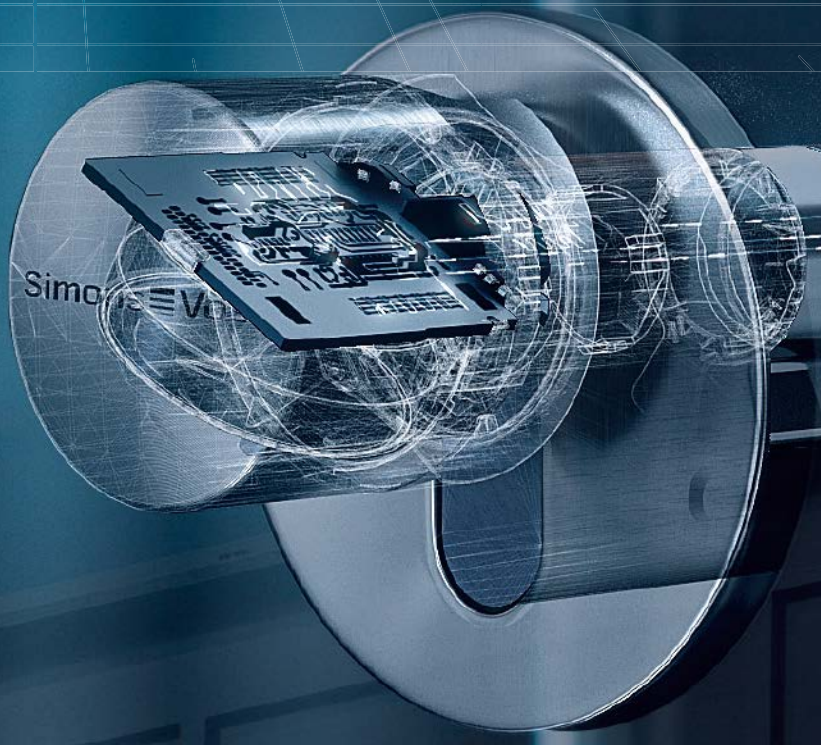
Simons Voss technologies

// **KABELLOS**

// **LEICHTE UND BOHRUNGSFREIE MONTAGE**

// Batteriebetrieben,
bis zu 10 Jahren Stand-by

// Keine Probleme bei Schlüsselverlust,
mehr Kontrolle und Sicherheit



www.simons-voss.com

ZUTRITT

Wo viele Menschen wohnen

Digitale Schließlösung für mehrere Mietparteien und große Wohnanlagen

Baugenossenschaften und Wohnungsbaugesellschaften profitieren auf vielfältige Weise von digitalen Schließsystemen. Einfache Verwaltung von Zugangsrechten und minimale Wartung sind nur zwei der vielen Vorteile. Mit der 5-Serie von iLoq sind Nutzer noch flexibler.

Die Schließlösung iLoq 5 erleichtert Baugenossenschaften und Wohnungsbaugesellschaften das Leben: Durch eine einheitliche Plattform und Systemarchitektur können sowohl das Smartphone, ein digitaler Schlüssel oder ein Key Fob zum Öffnen der Schließzylinder verwendet werden. Der Clou: Alle Geräte kommunizieren miteinander und Zugangsrechte werden ständig aktualisiert. iLoq bietet somit eine clevere Lösung für verlorene Schlüssel, unerlaubte Schlüsselkopien oder missbräuchliche Nutzung von Gemeinschaftsräumen.

Hohe Kapazitäten für große Wohnanlagen

Bei großen Wohnanlagen mit vielen Mietparteien wird das Zugangsmanagement oft zur Herausforderung. Verlorene Schlüssel oder Schlüsseltausch bei Mieterwechsel gehören zur Tagesordnung. Dies geht für die Betreiber mit einem enormen Zeit-, Kosten- und Verwaltungsaufwand einher, insbesondere wenn jedes Haus in der Wohnanlage eine eigene Schließanlage hat. Gleiches gilt, wenn bestehende Schließanlagen in großen Wohnanlagen an ihre Kapazitätsgrenzen stoßen.

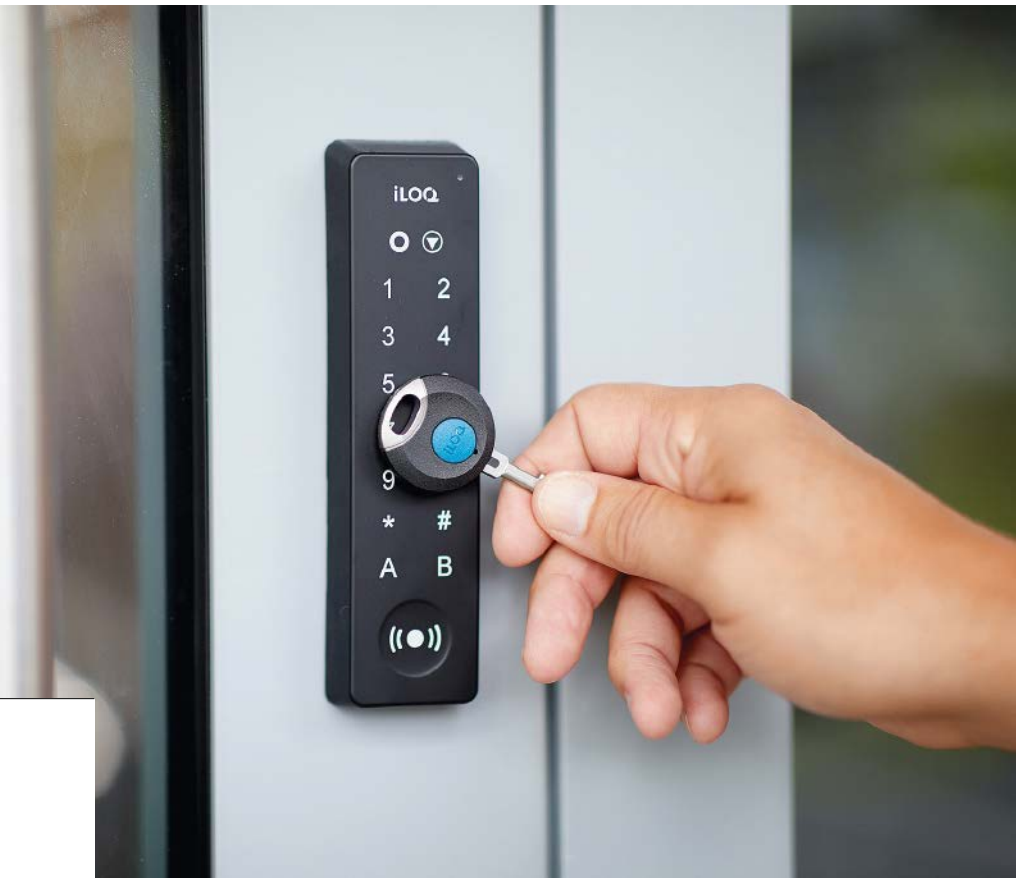
Die neue Generation der digitalen iLoq-Schließlösung S5 schafft hier Abhilfe: Mit einer Kapazität von bis zu einer Million Schließzylinder und zwei Millionen Schlüsseln ist sie insbesondere für sehr große Wohnanlagen geeignet.

Sicherheit bei Schlüsselverlust oder Mieterwechsel

Bei Verlust eines Schlüssels ist der Ablauf denkbar einfach: Innerhalb kurzer Zeit ist ein neuer Schlüssel programmiert, der alte wird im System gesperrt und verliert seine Zugangsrechte. Dank der Gerät-zu-Gerät-Kommunikation kann die Hausverwaltung sogar auf Vorort-Termine mit den Mietern verzichten, um vorhandene Schlüssel neu zu programmieren oder Zugangsrechte neu zu vergeben. Schließzylinder, Schlüssel und Lesegeräte kommunizieren miteinander und sind immer auf dem aktuellen Stand.

Auch beim Mieterwechsel gibt das digitale Schließsystem zusätzliche Sicherheit. Neue Bewohner können sicher sein, dass keine weiteren passenden Schlüssel zu ihrer Wohnung im Umlauf sind. Sollten zusätzliche Schlüssel für Verwandte oder Pflegekräfte benötigt werden, sind auch diese schnell und unkompliziert nachbestellt.

Unerlaubte Schlüsselkopien sind hingegen ausgeschlossen: Der digitale Schlüssel hat keine spezifischen Einfräsungen, die kopiert werden könnten. Der iLoq-Schlüssel ist vor Kopien nicht durch seine Form oder Gültigkeit eines Patents geschützt, sondern durch eine starke, vielschichtige digitale Verschlüsselung. Die Software verfügt immer über



◀ **Digitale Schließsysteme: Vielfältiger Nutzen für Baugenossenschaften und Wohnungsbaugesellschaften**

▲ **Die neue Generation der digitalen iLoq-Schließlösung S5 eignet sich mit einer Kapazität von bis zu einer Million Schließzylinder und zwei Millionen Schlüsseln insbesondere für große Wohnanlagen**

aktuelle Daten von allen programmierten Schlüsseln und Schließzylindern.

Ein Schlüssel für alles

Für Mieter gibt es weitere praktische Vorteile: So kann ein einziger Schlüssel mit allen Zugangsrechten einschließlich Wohnungsabschlusstür, Gemeinschaftsräume, Briefkasten, Aufzug-Schlüsselschaltern, Garageneinfahrten und Vorhängeschlössern programmiert werden. Gleichzeitig ist man vor missbräuchlicher Benutzung von Gemeinschafträumen geschützt. Der iLoq-Zylinder protokolliert jede Türöffnung bzw. den Versuch, den Schließzylinder zu öffnen. Dank des Zugangsprotokolls kann jeglicher Missbrauch einfach nachverfolgt und somit verhindert werden.

Einfache und kostengünstige Wartung

In der tagtäglichen Praxis punktet das Schließsystem neben seiner Sicherheit und Flexibilität durch den minimalen Wartungsaufwand. Schließlich sind für den Betrieb weder Batterien oder Kabel erforderlich. Die benötigte Energie wird allein durch den Schlüsseleinschub generiert – bei der smartphonebasierten Schließlösung fungiert das Handy als Energiequelle und Schlüssel. Somit entfällt das lästige Wechseln der Batterien und Schließzylinder und Schlüssel sind immer funktionsfähig. ■

Kontakt

iLoq Deutschland GmbH
Düsseldorf
Tel.: +49 211 97 177 480
germany@iloq.com
www.iloq.de

Einsatz-Drehsperre mit Desinfektionsmittelspender

Hygienekonzepte für Unternehmen

Zur Unterstützung von Unternehmen hat Wanzl ein Whitepaper „Sicherheits- und Hygienekonzepte für Unternehmen – so schützen Sie Ihren Betrieb" konzipiert – es dient als Praxisleitfaden für die Entwicklung eines individuellen Krisenplans. Vor und nach Corona – für einen Großteil der deutschen Betriebe gilt seit dem Frühjahr 2020 eine neue Zeitrechnung. Der Arbeitsalltag vieler Mitarbeiter wurde genauso auf den Kopf gestellt wie die internen Arbeits- und Produktionsprozesse. Um dies künftig zu vermeiden, ist ein umfassendes und flexibel anwendbares Hygiene- und Sicherheitskonzept für Betriebe unumgänglich. Oberstes Ziel: die Vereinbarung von Mitarbeiter- und Unternehmensschutz. Es ist eine Gratwanderung, den drohenden Umsatzausfall zu minimieren und gleichzeitig den Schutz und die Sicherheit der Mitarbeiter zu maximieren.

Einsatz-Drehsperre Sirio von Wanzl

Richtlinien für Mitarbeiterschutz sind im Arbeitsschutzgesetz der Bundesregierung vorgegeben, aber nicht allgemeingültig anwendbar. Um festzustellen, wie Vorgaben zur Infektionsprävention im Betrieb individuell umzusetzen sind, ist eine grundlegende Fallanalyse der Unternehmensstruktur notwendig: Interne Prozesse, Eigenheiten der Büro- und Gebäudearchitektur sowie die Einbindung in wirtschaftliche Versorgungsketten müssen identifiziert werden. Ausschlaggebend für die Wahl der passenden Vorgehensweise ist auch die Übertragungsart der Krankheit. Im Falle von Covid-19, das hauptsächlich durch die Tröpfcheninfektion über Mund, Nase oder die Hände übertragen wird, hat sich das AHA-Konzept bewährt. Abstand, Hygiene und Alltagsmasken können präventiv Infektionen vorbeugen und Infektionsketten durchbrechen.

Um ein entsprechendes Verhalten im Betrieb durchzusetzen, bedarf es neben einer klaren Kommunikation zielgerichtete, infrastrukturelle Maßnahmen. Wie diese aussehen können, zeigt das Unternehmen selbst an seinen Firmenstandorten in Deutschland. Es entwickelte dafür die eigenen Access-Lösungen für einen effektiven Infektionsschutz weiter. Diese infrastrukturellen Prozess- und Produktoptimierungen waren ein zentraler Baustein im ganzheitlichen Sicherheits- und Hygienekonzept von Wanzl.

www.wanzl.com ■

LCD/TFT-Monitor

Grundig Security hat den Monitor GD-ML-BC2230HD aus der Produktlinie „Essential" auf den Markt gebracht. Mit Full-HD-Auflösung, LED-Hintergrundbeleuchtung und einer Diagonalen von 54,6 cm (22") wurde der 16:9-Monitor für den professionellen Einsatz rund um die Uhr entwickelt. Das schlanke Design beinhaltet einen extrem schmalen Rand. Der Monitor kann mit dem im Lieferumfang enthaltenen Standfuß aufgestellt werden, lässt sich jedoch mithilfe einer VESA-Halterung an der Wand befestigen. Angeschlossen wird der Monitor entweder über VGA oder über das mitgelieferte HDMI-Kabel. Ein Netzteil für die 12-VDC-Stromversorgung ist im Lieferumfang enthalten. Der Monitor ersetzt das Modell GD-ML-AC2230HD.

www.abetechs.com ■

Produktportfolio erweitert

Ces hat sein Portfolio erweitert. Mit dem RFID-Möbelschloss stellt der Hersteller eine Zutrittslösung für Möbel und Schränke vor. Die Lösung ist einfach zu montieren, passt auf viele bereits mechanisch ausgerüstete Schränke und lässt sich nahtlos in das Omega-Flex-System integrieren. Ein Renovierungsbeschlag speziell für Innentüren ergänzt die Palette der Elektronikbeschläge. Das Edelstahl-Schild kann ohne Änderungen an der Tür direkt auf die Bohrungen vorhandener Beschläge geschraubt werden. Durch das flexible Befestigungssystem ist auch dieser Beschlag einfach und ohne weitere Bohrungen an der Tür einsetzbar. Bestehende mechanische Beschläge an den Innenseiten können, wenn gewünscht, beibehalten werden. Für Serverschränke, Maschinentüren oder große Sicherungskästen, die mit Schwenkhebelgriffen ausgestattet sind, wurde ein neuer Schließzylinder-Typ konzipiert. Der Vorteil des Zylinders liegt darin, dass sich der Schwenkhebel ohne vorherige Identifikation komfortabel wieder verschließen lässt. Der Schwenkhebelgriff rastet mitsamt dem Schließzylinder automatisch ein, sobald die Schließposition erreicht ist. Zum Öffnen werden RFID-Schließmedien verwendet.

www.ces.eu ■

Produktkatalog für Datennetzwerkprofis erschienen

Der neue Katalog von EFB-Elektronik zeigt Produkte rund um Lichtwellenleiter, Kupferverkabelung, Schranksysteme und Multimedia sowie aktive Komponenten. Der Glossarteil beinhaltet ein umfassendes Produktwissen, das dort schnell nachgeschlagen werden kann. Neben technischen Details informiert der Katalog auch über Produktneuheiten.

www.efb-elektronik.de ■

Bedieneinrichtungen in neuem Design ▲

Abi-Sicherheitssysteme hat die VdS-anerkannten Bedieneinrichtungen, die Farb-Touch-Panel BC 230-E und die LCD-/LED-Bedienteile BC 85-E, in sein Portfolio aufgenommen. Die Bedieneinrichtungen haben ein modernes Aussehen sowie eine klare Formgebung. Eine „Schattenfuge" zwischen Ober- und Unterschale der flachen Gehäuse stellt ein weiteres stilistisches Element dar. Die Gehäuseober- und -unterschale ist in der Farbkombination weiß/schwarz gehalten. Durch die klappbare Oberschale sind die Bedieneinrichtungen montagefreundlich. Die Farb-Touch-Panel und LCD-/LED-Bedienteile sind über den Peripherie-Bus (P-Bus) an die Abi-Systemzentralen anschaltbar.

www.abi-sicherheitssysteme.de ■

Rahmenlose LCD-Monitore

Eizo stellt mit dem 27 Zoll großen Flexscan EV2795 und dem 24,1 Zoll großen Flexscan EV2495 zwei nahezu rahmenlose LCD-Monitore vor, die sich dank USB-C-Docking gut für Büro und Homeoffice eignen. Die Monitore bieten eine Auflösung von 2560×1440 bzw. 1920×1200 Bildpunkten, sind entspiegelt, flimmerfrei und mit Ergonomie- und Energieeinsparungsfunktionen ausgestattet. Die Monitore sorgen durch USB-C-Docking und USB-C-Daisy-Chain für weniger Kabel und mehr Freiheit auf dem Schreibtisch. Für Videosignal, Ladestrom, Audio-Out, USB-Daten und Netzwerk reicht ein einziges Kabel zum Rechner. Sogar verkettete Monitore beziehen über dieses eine Kabel ihr Signal. Insbesondere Notebook- und Tablet-Nutzer profitieren von dieser Multifunktionalität. Notebooks, die mittlerweile häufig keinen LAN-Anschluss mehr besitzen, werden so wieder LAN-fähig und nebenbei wird deren Akku mit bis zu 70 Watt aufgeladen. Mehrschirmsysteme lassen sich mit USB-C-Daisy-Chain in einer Verkettung von Monitor zu Monitor einrichten. Durch zwei USB-Upstream-Ports können die Bildschirme als Tastatur-/Maus-Umschalter (KVM-Switch) eingesetzt werden.

www.eizo.de ■

Flexscan EV2495 von Eizo

Die aktuelle Ladenfront, seit dem letzten Umzug in 2004. Auf die andere Straßenseite – direkt am Amtsgerichtsplatz

ERRICHTER

Von wegen „kleen“

Werner Sicherheitstechnik: Eine Berliner Erfolgsgeschichte wurde dieses Jahr 50

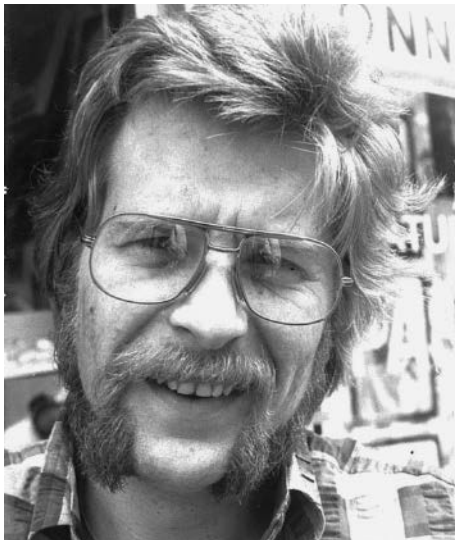
Es begann mit einer Übernahme: Als neuer Pächter eines Schloss- und Schlüsseldienstes begann Wolfgang Werner 1970 die Weichen für seinen Erfolg zu stellen: Mit großzügigen Öffnungszeiten, Montagezeiten in den Morgen- und Abendstunden – und mit schrittweiser Ausweitung der Verkaufsfläche und konsequenter Modernisierung des Sortiments, bis hin zur eigenen Notruf-Service-Leitstelle. Heute besteht das Unternehmen mit Werner Sicherheitstechnik und Werner Alarmanlagen aus einem Verbund zweier spezialisierter Firmen mit 28 hochqualifizierten Mitarbeitern. GIT SICHERHEIT hat mit dem Firmengründer und Geschäftsführer Wolfgang Werner aus Anlass seines 50jährigen Jubilums gesprochen.

GIT SICHERHEIT: Herr Werner, vor etwa 50 Jahren waren Sie noch der „Kleene Werner“ – jedenfalls für die Schauspieler an den Theatern rund um Ihren ersten Schlüsseldienst herum. Waren bekannte Leute darunter…?

Wolfgang Werner: Das waren oft sogar meine Kunden. Wolfgang Spier und Wolfgang Gruner zum Beispiel – aber es wohnten natürlich viele Schauspieler in der Umgebung, viele leben heute nicht mehr. Vor allem nach Generalproben haben sie heftig gefeiert und kamen dann nachts oft nicht mehr in ihre Garderoben. Ich habe dort damals zum Beispiel eine Einbruchsicherung mit besseren Schlössern eingebaut, die das Problem lösten. Wolgang Gruner von den Stachelschweinen meinte damals „Mein Kleener, ich kaufe was ich will, und nicht, was du mir verkaufen willst“.

Aber es kam ja anders…

Wolfgang Werner: Das stimmt. Aber als ich mit dem klassischen Schlüsseldienst anfing, wusste ich gar nicht, dass es da noch mehr gibt, als Schlüssel herzustellen und zu verkaufen, Schlösser zu reparieren, Türen zu öffen, u.s.w. Das habe ich auch gemacht, bis ich merkte, dass der geschlossene Berliner



Der Seniorchef Wolfgang Werner – damals…

…und heute

50 Jahre Werner Sicherheitstechnik

Mit Sicherheit aus einer Hand hat sich die heutige Firma Werner Sicherheitstechnik im Berliner und Brandenburger Raum einen Namen gemacht. Die vom VdS anerkannten Facherrichter bieten Alarmanlagen, mechanische Sicherheitselemente und Videotechnik – inklusive firmeneigener Notruf-Service-Leitstelle. Zum Portfolio des ISO 9001-zertifizierte Unternehmen gehören außerdem Tür- und Fenstersicherungen, Brandschutztechnik, Schließanlagen und Zutrittskontrollen, Tresore, Rollgitter und Terrassentüren – und manches mehr.

Das Ladengeschäft von Werner Sicherheitstechnik in der Berliner Kantstraße präsentiert die gesamte Bandbreite des erfolgreichen Jubilars. Betreute werden heute jeweils etwa zur Hälfte private und gewerbliche Kunden – fast alle ihrer Alarmsysteme sind auf die unternehmenseigene Notruf-Service-Leitstelle aufgeschaltet.

Markt besetzt und der Kuchen verteilt war. Also habe ich neue Wege gesucht. So habe ich zum Beispiel 1974 angefangen, Alarmsysteme und deren Montage in mein Angebot aufzunehmen. Damit waren wir ziemlich erfolgreich, auch wenn wir auf der ersten Security-Messe damals als „einfacher Schlüsseldienst" nicht ernst genommen und gar nicht erst beliefert wurden. Wir haben deshalb ein kleines Alarmsystem für Wohnungen bauen lassen – das war der Einstieg. Ein Jahr später gründete ich die Werner Alarmanagen GmbH und wir wurden vom VdS anerkannt. Schon auf der zweiten Security 1976 hatten wir keine Schwierigkeiten mehr, von den Herstellern beliefert zu werden. Nach und nach haben wir uns mit Sicherheitstechnik in Berlin etabliert, also mit höherwertiger Schließtechnik. Wichtig waren damals zum Beispiel Stangenschlösser für Doppelflügeltüren. Ich begann mit der Optimierung von Stangenschlösser aus Italien, das damals in Europa am weitesten damit war. Nach und nach haben wir uns vergrößert und bekamen mehr Platz für Alarmtechnik, Mehrfachverriegelungen, Zylinder und die ersten Schutzbeschläge. Vieles an sicherheitstechnischen Lösungen, die die meisten anderen verschlafen hatten, haben wir damals selber entwickelt. 1981 wurden wir in den Interkey-Verband aufgenommen – das war ein Ritterschlag.

Auch Weiterbildungen und Zertifizierungen brachten kräftige Entwicklungsschübe mit sich…?

Wolfgang Werner: Ich stand vor allem in der Anfangszeit im Wettbewerb mit Schlossern und Elektrikern. Es gibt ja bis heute keine Lehrberufe für Alarm- oder Schließtechnik. Ich verschaffte mir das nötige Wissen zu Betriebsplanung, Personalführung und Unternehmensmanagement am Schmidt-College und am Helfrecht-Institut. Was die Zertifizierungen betrifft: Vor allem unsere VdS-Anerkennung im Bereich mechanische Sicherheitstechnik 1996 hat den Betrieb umgekrempelt. Zu den Schlössern kam damals auch Sicherheitstechnik für Türen und Rollläden hinzu. Es gab damals außer uns kaum jemanden in Berlin, der das alles aus einer Hand liefern konnte – bis heute bieten wir alle Sicherheitsbereiche von A bis Z aus einer Hand. Inzwischen haben wir schon lange vier Zertifizierungen – und zwar für Einbruchmeldetechnik, mechanische Sicherungssysteme, als Errichter für Videotechnik – und wir sind ISO- und VdS-zertifiziert. Seit 1990 betreiben wir außerdem eine eigene Leitstelle, auf der unsere Alarmanlagen aufgeschaltet sind. Es war sehr schwierig und kostenintensiv, da wir inklusive Wachdienst und Schlüsselnotdienst rund um die Uhr Mitarbeiter beschäftigen müssen. Erst nach 300 Aufschaltungen begann sich das Angebot zu rechnen.

Das war ja auch die Zeit des Mauerfalls. Wie hat sich das aufs Geschäft ausgewirkt?

Wolfgang Werner: Der Mauerfall hat an der relativen Geschlossenheit des Berliner Marktes nichts geändert. Dafür kam aber viel Wettbewerb aus dem Osten, wo sehr viele Stasi-Leute auf den Sicherheitsmarkt kamen. Das hatte einen harten Wettbewerb und einen extremen Preiskampf zur Folge.

Noch mal zurück zur Technik… Gerade die Zutritts- und Schließtechnik hat sich extrem weiterentwickelt – das gleiche gilt für die immer wichtiger werdende Videotechnik?

Wolfgang Werner: Mit Video beschäftigen wir uns etwa seit dem Jahr 2000. Sie spielt bei uns vor allem im Einzelhandel, bei Garagen und im Außenbereich und allgemein im Perimeterschutz eine Rolle. Der Ausbau der Zutrittstechnik und Schließanlagentechnik kam vorher – mit Transpondern, Karten, etc. Hier haben wir früh mit den wichtigsten Herstellern wie Uhlmann und Zacher, SimonsVoss

Bitte umblättern ▶

Das erste Ladengeschäft in den 70ern – gerade mal 1,68 m breit

Sommer 1970 nach dem ersten Umzug in eine ehemalige Bäckerei im selben Haus in der Kantstraße

Nach dem Umbau 1986

Mehr Platz auch in den Schaufenstern – da passte auch mal ein Motorrad oder eine Zündapp rein

und Assa Abloy, Zeiss Ikon, Dom und Kaba zusammengearbeitet. Wir waren sehr früh mit elektronischen Schließzylindern am Markt und haben dieses Segment ständig erweitert.

Wer sind heute Ihre Kunden – und was umfasst Ihr Portfolio heute?

Wolfgang Werner: Unsere Kunden kommen jeweils etwa zur Hälfte aus dem gewerblichen und dem privaten Bereich. Dabei sind übrigens die Privatleute im Vergleich zu früher heute viel vermögender. Sie kaufen nicht nur Einbruchmeldeanlagen sondern zum Beispiel auch Sicherheitsfenster und sichere Haustüren. Ähnliches gilt für den gewerblichen Bereich. Corona hat natürlich vieles auf den Kopf gestellt.

Das smarte Heim ist ja ein starker Trend – wie sehen Sie das?

Wolfgang Werner: Hier gibt es aus meiner Sicht immer noch Sicherheitsprobleme. Die Täter werden immer intelligenter. Schon die elektronischen Verschlusssysteme für Autos wurden ja bereits geknackt – bei den Smarthome-Systemen ist das ähnlich. Die Systeme werden am Laptop ausgelesen. Allerdings gibt es ständig neue Transpondergenerationen auf den Markt, die die Auslesesicherheit verbessern. Wir empfehlen unseren Kunden, bei ihrer Smart-Home-Anlage, die Scharf- und Unscharfschaltung der Alarmanlage per Handy wegzulassen, denn damit kann man die Anlage außer Betrieb nehmen. Das Ein- und Ausschalten muss zu 100 Prozent sicher sein.

Wo liegen für Sie die in der Praxis wichtigsten Trends?

Wolfgang Werner: Sehr und wichtig ist der Trend zur Digitalisierung – darin sehe ich auch die Zukunft. Ein Beispiel dafür sind Stand-alone-Alarmsysteme, die sich vernetzen lassen, ohne von außen angreifbar zu sein. Trotzdem bleibt ein hoher Widerstandswert der Mechanik wichtig. Die Anforderungen werden höher, weil auch die Täter anders vorgehen und zum Beispiel mit Rettungsmitteln der Feuerwehr Türen öffnen. Das Zusammenwirken von Mechanik und Elektronik ist die Zukunft. Auch das Thema Fernüberwachung wird noch weiter ausgebaut werden. Das gilt zum Beispiel für Brandmelder. Und wir unterstützen heute immerhin 1.500 Kunden durch Überwachung ihrer Objekte, wo wir uns schon per Video aus der Ferne ein Bild verschaffen können. ■

Kontakt

Werner Sicherheitstechnik GmbH
Berlin
Tel.: 030 323 40 50
info@alarmundschloss.de
www.alarmundschloss.de

Smarte Bewegungsmelder

Abi-Sicherheitssysteme hat sein Portfolio um smarte Bewegungsmelder und einen Funk-Magnetkontakt erweitert. Durch ihre geringe Baugröße und das Design integrieren sich die Funk-Melder diskret in die Wohn- bzw. Büroumgebung. Dadurch sind sie äußerst unauffällig und besonders für Anlagen im Bereich „Home & Office" geeignet. Der Funk-PIR-Bewegungsmelder FIR-868/S ist ein passiver Infrarot-Bewegungsmelder zur Überwachung von Räumen. Der Melder reagiert auf Bewegungen im Erfassungsbereich. Der Funk-Magnetkontakt FMK-868/S ist zur Anschaltung an das Funk-Interfacemodul vorgesehen. Er ermöglicht die Überwachung von z. B. Fenstern und Türen. Durch seine kompakten Abmessungen passt der Magnetkontakt an fast jedes Fenster oder jeden Türrahmen. Der Funk-PIR Vorhangmelder FIV-868 ist ein passiver Infrarot-Bewegungsmelder zur Außenhautüberwachung (z. B. auf Durchstieg) in Innenbereichen.

www.abi-sicherheitssysteme.de ■

Panik-Druckstange mit vollintegriertem Touch-Display

Auf der Ausstellung architect@work zeigt Assa Abloy eine Druckstange für Fluchttüren mit vollintegriertem Touch-Display. Das Fachevent für Architekten tourt ab Herbst durch Deutschland, diesmal unter Hygienebedingungen. Auftakt der architect@work-Reihe war am 7. und 8. Oktober mit der Edition in Berlin. Weitere Stationen sind Wiesbaden vom 25. bis 26.11. und Stuttgart vom 2. bis 3.12. Mit der E-Ped-Panik-Druckstange ist es dem Hersteller gelungen, sämtliche Funktionen und ein digitales Display-Terminal in einem einzigen Element an der Tür zu vereinen. Die Systemlösung integriert das Fluchttürsteuerterminal vollständig in die Druckstange. Somit ist kein separates Bauteil an der Wand mehr notwendig.

www.assaabloy openingsolutions.de ■

German Design Award 2021 für Zutrittsleser

Der Zutrittsleser Intus 700slim von PCS ist mit dem German Design Award 2021 für Excellent Product Design – Building and Elements ausgezeichnet worden. Trotz seiner geringen Gehäusegröße ist der Zutrittsleser mit zukunftsfähiger Technik ausgestattet und beweist mit RFID, Bluetooth-Anbindung an Smartphones und verschlüsselter Datenübertragung seine innovative Produktausprägung. Ein integrierter RFID-Leser liest Mitarbeiterausweise, eine zusätzliche Tastatur ermöglicht zur Sicherheit eine Zwei-Faktor-Authentifizierung mit Zahlen-Code und Karte. Die PIN-Tastatur ist optional hinterleuchtet, um die Bedienung bei Dunkelheit zu erleichtern, während die taktile Folientastatur die Bedienung für sehbehinderte Mitarbeiter erleichtert. Mit Kunstharz versiegelt ist der Leser für den Außeneinsatz bis zur Schutzklasse IP68 geeignet.

Der prämierte Zutrittsleser Intus 700slim von PCS

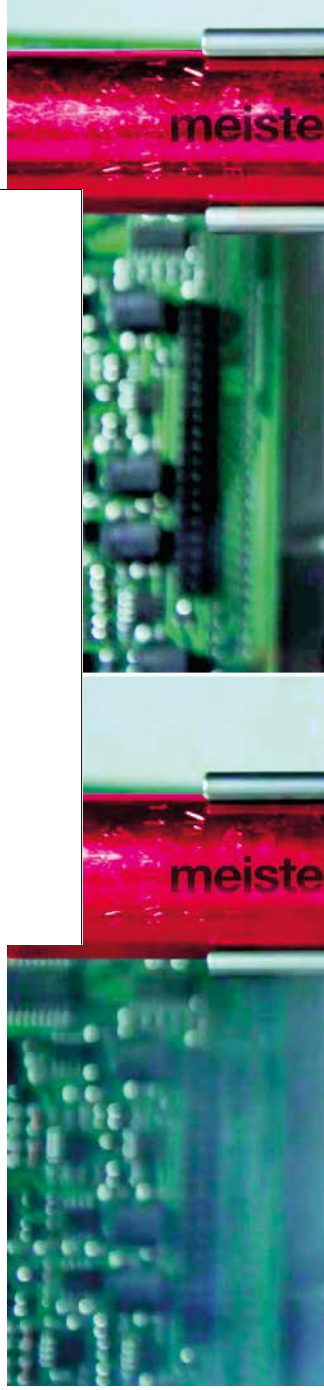
www.pcs.com ■

BRANDFRÜHERKENNUNG UND -LÖSCHUNG

Wächter im Schrank

Geräteintegrierter Brandschutz für den Schaltschrank

Die automatische Mini-Feuerlöscheinheit AMFE von Job wird exklusiv von Meister Automation (vormals Deiring) vertrieben. Das System dient der frühzeitigen Erkennung und zuverlässigen Löschen von Gerätebränden und geschlossenen Rauminhalten. Anwendungsgebiete sind z. B. die Steuerungstechnik, Schaltschränke für den Maschinenbau aber auch ganze Serverfarmen. Diese teuren und betriebswichtigen Investitionsgüter können damit ohne Einsatz von CO_2 geschützt werden. Die Installation können auch ungeschulte Mitarbeiter anhand der Installationsanleitung einfach durchführen.



▶ Der Hersteller nutzt 3M Novec und kein CO_2

Die aktuelle Statistik des Instituts für Schadensforschung IFS in Kiel sowie die Statistiken des VdS und GdV zeigen: In der Bundesrepublik Deutschland wird alle zwei bis drei Minuten ein Brand gemeldet, über 30 % aller Brände werden durch Elektrizität verursacht. Laut VDS legen gerade die Brandschutzversicherungen ein sehr großes Augenmerk auf den proaktiven Brandschutz. Jedes Jahr werden allein in Deutschland von den Versicherern über zwei Milliarden Euro für Brandschäden ausgezahlt.

Trotz dieser enormen Hilfen werden immer noch 74 Prozent der betroffenen Unternehmen in die Insolvenz gezwungen, da bei langen Betriebsausfällen selbst die besten Kunden oft andere Alternativen finden müssen. Es sind gerade KMU, die den Brandschutz oft nur oberflächlich behandeln und nur das vom Gesetzgeber vorgeschriebene Minimum umsetzen, ohne sich der wirtschaftlichen Folgen bewusst zu sein.

Fehlerhäufigkeit bei Elektronikkomponenten

Erfahrungsgemäß fallen bei der Fertigung von Elektronikkomponenten von einer Million hergestellter Baugruppen, etwa fünf bis sechs Stück aus. Kalte Lötstellen, fehlerhafte Komponenten oder Steckverbindungen können zu einem Brand führen. Alle Hersteller von elektrischen und elektronischen Komponenten können hiervon betroffen sein – das zeigen z.B. die Rückrufe von Consumer Produkten wegen Brandgefahr der letzten Jahre (vgl. CPSC Statistik in den USA). Die Dunkelziffer dürfte, vor allem in der Industrie, noch viel höher liegen, da nicht jeder Entstehungsbrand der Meldepflicht unterliegt.

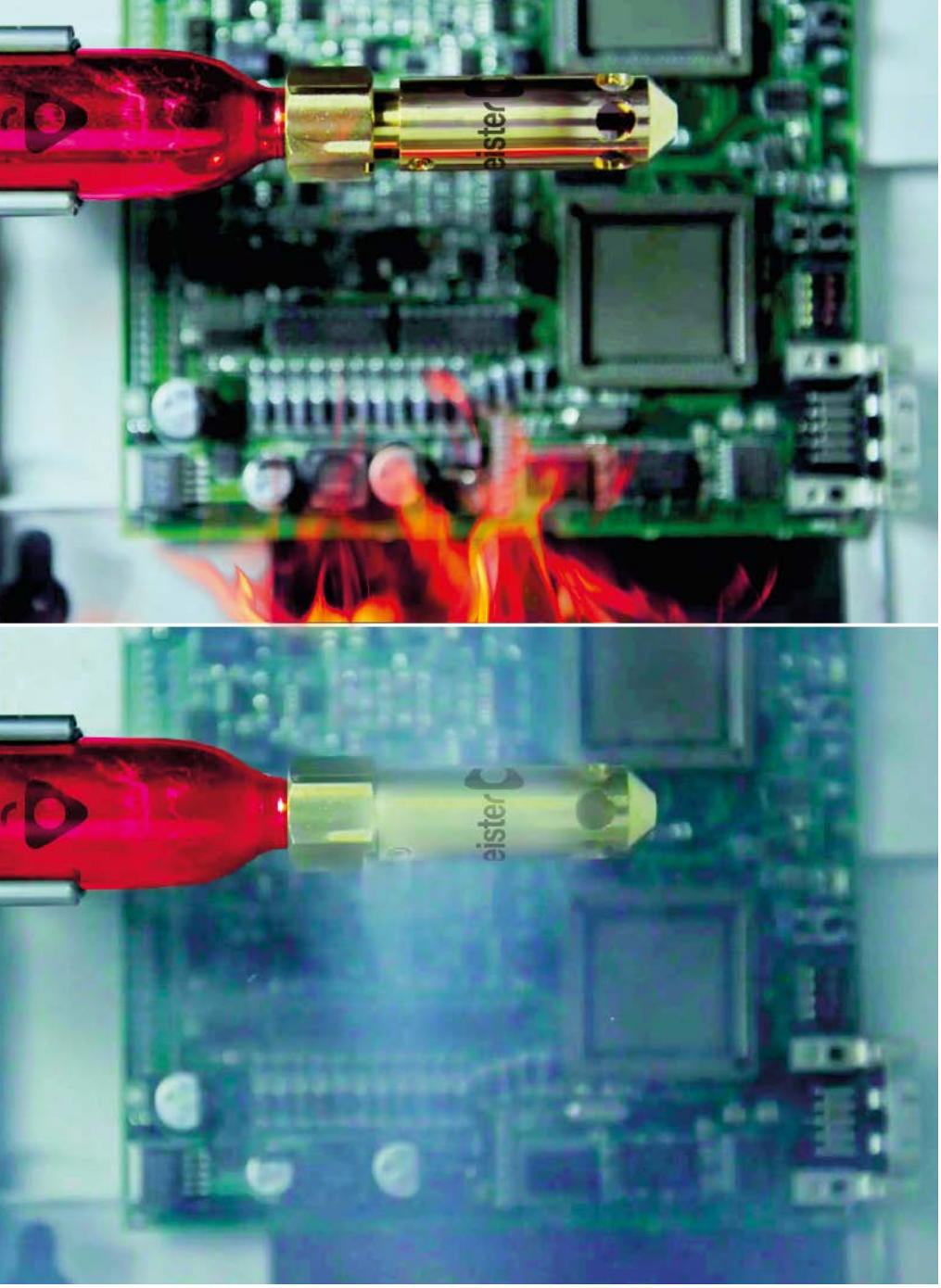
Bestehende Brandschutzkonzepte optimieren

Aktuelle Brandschutzkonzepte in der Industrie und dem Maschinenbau sind oft rein passiver Natur. Sie berücksichtigen eher das Minimieren von Brandschäden durch Brandschutzwände oder Alarmierungen durch Brandmelder, anstatt proaktiv direkt am Entstehungsort zu löschen. Sprinkleranlagen in Gebäuden sind bisher das effektivste Mittel, um die Großbrände gar nicht erst entstehen zu lassen und somit viele Leben und Sachwerte zu retten.

Zum Nachteil kann allerdings das großflächige Gießkannenprinzip werden. Bei den großen Mengen an Wasser, die zum Löschen offener Brände verwendet werden, entstehen auch bei nur kleinen Bränden erhebliche Folgeschäden. So sind z. B. alle durch das Brackwasser benetzte Waren unbrauchbar, Elektrogeräte an Arbeitsplätzen meistens durch den Wassereintritt defekt. Dieses Problem betrifft alle produzierenden Branchen, insbesondere die Lebensmittelbranche und Logistikzentren.

Hier setzt Meister Automation mit seinem AMFE-Konzept an und erkennt den Brand so frühzeitig wie möglich am Entstehungsort, um diesen zuverlässig und vor einer folgenschweren Ausbreitung löschen zu können. Eine Erweiterung und Optimierung bereits

▲ Die automatische Mini-Feuerlöscheinheit AMFE



bestehender Brandschutzanlagen wird dadurch sehr einfach möglich.

Zertifizierte Funktion und Nachrüstung

Branderkennung und Auslösung erfolgen nach einem thermodynamischen Aktivierungsprinzip wie bei einer Sprinkleranlage – durch eine VDS-zugelassene Thermo-Glasampulle. Durch die steigende Wärme z. B. in einem Schaltschrank, zerplatzt im Brandfall die Thermo-Glasampulle und öffnet stromunabhängig die angeschlossene Löschmittelkartusche und setzt das zugelassene Löschmittel Novec von 3M frei.

Der Hersteller nutzt 3M Novec und kein CO_2, da dieses Löschmittel eine sieben Mal höhere Löschfähigkeit habe, also sieben Mal weniger Menge benötigt und eine schnellere Inkubationszeit hat. Außerdem ist es nicht wiederentflammbar durch Sauerstoff (Kein Flash-Over). Das Mittel ist zudem für Menschen unschädlich und auch elektrische Komponenten bleiben unbeschädigt. Außerdem sei es rückstandsfrei und habe ein sehr geringes Treibhauspotential.

In allen Schaltschrank- und Elektroverteilern lässt sich die AMFE einfach und kostengünstig nachrüsten. Somit können die Systeme von Schaltschrankbauern und Systemherstellern für Neuprojekte eingesetzt werden, aber auch Bestandsanlagen können mit geringem Aufwand sofort geschützt werden. ■

Kontakt

Meister Automation GmbH
Wertheim
Tel.: +49 9342 911010
info@meister-automation.de
www.amfe.de

Rauchwarnmelder in allen Wohnungen vorgeschrieben

Wie der Bundesverband Brandschutz-Fachbetriebe (BVBF) mitteilt, müssen spätestens bis Silvester in allen Häusern und Wohnungen in

Berlin und Brandenburg Rauchwarnmelder installiert sein. Hierfür verantwortlich sind die Eigentümer. Ist eine Mietwohnung noch nicht mit Rauchwarnmeldern ausgestattet, sollte sich der Mieter jetzt an seinen Vermieter wenden. Bewohnt ein Eigentümer seine Immobilie, muss er Raumwarnmelder anbringen. Die Pflicht gilt für alle Aufenthaltsräume sowie Flure, die als Rettungsweg dienen. Auf jeden Fall gehören die Geräte in Schlaf- und Kinderzimmer sowie explizit auch in Wohnzimmer. Küchen sind von der Regel ausgenommen, außer sie sind Durchgangsraum oder Teil eines offenen Wohnbereichs.

www.bvbf.de ■

Data Center Hybrid: Seminar und Exkursion

Die Themen des Data-Center-Hybrid-Events, an dem sich Wagner beteiligt, drehen sich um nachhaltigen Brandschutz in Rechenzentren. Hochsichere Rechenzentren, Breitbandnetze und Cloud-Computing bilden die Basis der digitalen Transformation. Sie ermöglichen es Unternehmen, neue Prozesse, Produkte und Geschäftsmodelle für das digitale Zeitalter zu entwickeln – zuverlässig geschützt durch passgenaue und zeitgemäße Brandschutzlösungen. Die Data Center Hybrid wird am 19. November 2020 in Gütersloh als Präsenzveranstaltung stattfinden. Das Event besteht aus einer Führung in einem lokalen Rechenzentrum, Arvato Systems Bertelsmann, und einer Konferenz mit Vorträgen zu verschiedenen Themen rund um die Planung und den Betrieb eines hochmodernen Rechenzentrums.

www.wagner.de ■

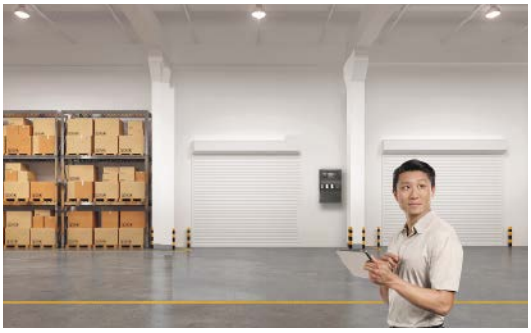
Zu viele Eigenheime ohne Rauchwarnmelder ▲

Eine von Ei Electronics in Auftrag gegebene repräsentative Studie ergab, dass trotz gesetzlicher Installationspflicht die Hälfte der deutschen Eigenheimbesitzer ihren Wohnraum nicht ausreichend mit Rauchwarnmeldern ausgestattet hat. Sind Rauchwarnmelder vorhanden, werden überwiegend Geräte mit wechselbaren Batterien verwendet. Lediglich in 25 Prozent der Eigenheime sind Rauchwarnmelder mit fest installierten 10-Jahres-Lithiumbatterien vorhanden. Nur 11 Prozent der Eigentümer nutzen vernetzte Rauchwarnmelder. Zwar haben 84 Prozent der Befragten mindestens einen Rauchwarnmelder in ihrem Eigenheim installiert, genau die Hälfte aller selbstgenutzten Häuser (50 Prozent) entsprechen jedoch nicht den gesetzlichen Vorschriften. Besonders gefährlich: In Schlaf- und Kinderzimmern ist nur in 62 Prozent der Fälle ein Rauchwarnmelder vorhanden. In Treppenhäusern, Fluren und Eingängen haben immerhin 75 Prozent der Befragten einen Rauchwarnmelder installiert.

www.eielectronics.de ■

Brandmelderzentralen mit grafischer Benutzeroberfläche

Bosch Building Technologies bringt unter dem Namen Avenar eine neue Generation von Brandmelderzentralen auf den Markt. Die Serie unterstützt den Wandel der Gebäudetechnik hin zu Lösungen auf Basis des Internets der Dinge. Avenar Panel 2000 und 8000 sind vollständig abwärtskompatibel mit aktuellen Brandmeldeanlagen. Avenar Panel 2000 ersetzt die Brandmelderzentrale der Serie 1200 für kleinere Projekte; sie unterstützt bis zu vier Ringe statt wie bisher zwei beim Vorgängermodell und dient damit als erweiterte Lösung für kleine bis mittelgroße Anwendungen mit bis zu 512 angeschlossenen Brandmeldern und Meldepunkten. Avenar Panel 2000 kann als über ein Gebäude verteiltes Netzwerk von Brandmelderzentralen betrieben werden. Darüber hinaus vereinfacht sich der Planungs- und Einkaufsprozess für Systemintegratoren, weil es sich hier um ein vorkonfiguriertes Baukastensystem handelt, das nach Bedarf modular erweitert werden kann. Avenar Panel 8000 ersetzt die modulare Brandmelderzentrale der Serie 5000 und ermöglicht bis zu 32 Ringe mit bis zu 4096 Brandmeldern und Meldepunkten.



Brandmelderzentrale Avenar von Bosch Building Technologies

Grafische Benutzeroberfläche E-Matrix mit 7-Zoll-Bildschirm

Beide Brandmelderzentralen unterstützen die heutige Generation von Brandmeldern basierend auf Local Security Network (LSNi)-Verbindungen sowie manuelle Melder und andere wichtige Systemkomponenten. Sie können in bestehende Netzwerkarchitekturen integriert werden, etwa in die modulare Brandmelderzentrale der Serie 5000. Beide Brandmelderzentralen unterstützen aktuelle Ethernet-Systemarchitekturen mit schneller 100-Mbit-Datenübertragung. Vier externe Ethernet-Schnittstellen ermöglichen die Verbindung von Brandmelderzentralen und Sprachalarmierungsanlagen des Herstellers zu einem Netzwerk sowie die Anbindung an Gebäudemanagementsysteme und weitere Sicherheitstechnik, einschließlich Remote Services für cloud-basierte Steuerung und Wartung. Eine technische Neuheit stellt die grafische Benutzeroberfläche E-Matrix mit ihrem 7-Zoll-Bildschirm dar. Die übersichtliche Darstellung zeigt jederzeit den Status der angeschlossenen Brandschutzeinrichtungen und Evakuierungszonen. Sie dient auch der Steuerung des Sprachalarms, der Türsteuerung sowie der Steuerung von Heizung, Lüftung und Klimatisierung. Es erlaubt dem Sicherheitspersonal, automatisch ausgelöste Evakuierungen zu überwachen und wenn nötig manuell einzugreifen.

www.boschbuilding technologies.com ■

Safety Academy qualifiziert Mitarbeiter

Für IEP Technologies besteht das oberste Ziel darin, explosionsgefährdete Arbeitsumgebungen zu einem sicheren Ort zu machen. In der Safety Academy werden Mitarbeiter zu verantwortungsbewussten Explosionsschutzexperten ausgebildet. Das Unternehmen entwickelt maßgeschneiderte Komplettsysteme, die unter anderem hochentwickelte Technologien zur Unterdrückung anlaufender Explosionen und zur Druckentlastung umfassen. Die Arbeit der Safety-Experten basiert auf drei Säulen: Menschen und Vermögenswerte schützen, die Betriebsstabilität sichern und dadurch Unternehmen bei der Optimierung der Anlagenverfügbarkeit unterstützen. Die dritte Säule betrifft die wirtschaftliche Umsetzung. Ein optimales Schutzsystem kann schließlich nur dann Leben retten, wenn es auch installiert wird und ins monetäre Budget eines Betreibers passt.

www.ieptechnologies.com ■

Firefit Championships: Erstmals als Indoor-Wettkampf

Am 12. Dezember 2020 findet der erste Firefit Championships Indoor-Wettkampf in Europa statt, organisiert von der Messe Hannover, dem Betriebssportverband Hannover und dem Funktionsschuhhersteller Haix. Die Halle der Messe Hannover bietet wetterunabhängig die notwendige Fläche und Höhe für den ausladenden Wettkampf-Parcours. Im Zentrum steht der zwölf Meter hohe Wettkampfturm. Die Deutsche Messe und das Team der Interschutz begleiten den gesamten Tag mit einem Livestream im Netz. Neben dem Sport bietet der „Interschutz Community Day" online zusätzliches Programm mit Hintergrundinformationen, Live-Interviews und interaktiven Elementen. Vor Ort werden sich weiterhin Aussteller präsentieren. Mit der Verschiebung der Interschutz auf Juni 2021 verzögert sich auch die erste Europameisterschaft der Firefit Championships. Vom 14. bis 19. Juni 2021 werden sich an allen fünf Messetagen die besten Athleten im Feuerwehrsport messen.

www.interschutz.de ■

Hekatron Brandschutz Planerdialog

Der Hekatron Brandschutz Planerdialog 2020 wurde coronabedingt kurzfristig online als Live-Stream durchgeführt. Die ursprünglich ausgebuchte Veranstaltung stand dadurch jedem offen, sodass insgesamt über 250 Teilnehmer zugeschaltet waren. Die Referenten vermittelten den Teilnehmern des Streams einen 360-Grad-Blick auf das komplexe Thema „Anlagentechnischer Brandschutz in multifunktionalen Gebäuden – von der Planung bis zum wirtschaftlichen Betrieb".

www.hekatron-brandschutz.de ■

Live-Seminar zum Brandschutz im Rechenzentrum

Mit Live-Übertragungen zum Thema Brandschutz im Rechenzentrum wird Wagner an der Datacenter-Experience-Veranstaltungsreihe, die coronabedingt digital stattfindet, teilnehmen. „Vorbeugender Brandschutz: Von den Schutzzielen über die Risikoanalyse zum nachhaltigen Brandschutzkonzept – Verlässlichen Brandschutz auch in Pandemiezeiten sicherstellen" lautet das Thema des Vortrags von Dominik David, Vertriebsexperte für Rechenzentren bei Wagner. Trotz der Modernität der neu gebauten Zentren habe das in diesen Gebäuden vorhandene Brandrisiko nicht abgenommen. Die jeweilige Brandschutzlösung müsse auf die Bedürfnisse des Rechenzentrums zugeschnitten sein. Eine sorgfältige, individuelle Risikoanalyse sowie eine Schutzzieldefinition des Kunden seien notwendige erste Schritte. Ziel sei die Definition einer angepassten Brandschutzlösung, bestehend aus Branddetektion, Brandvermeidung und/oder Brandlöschung.

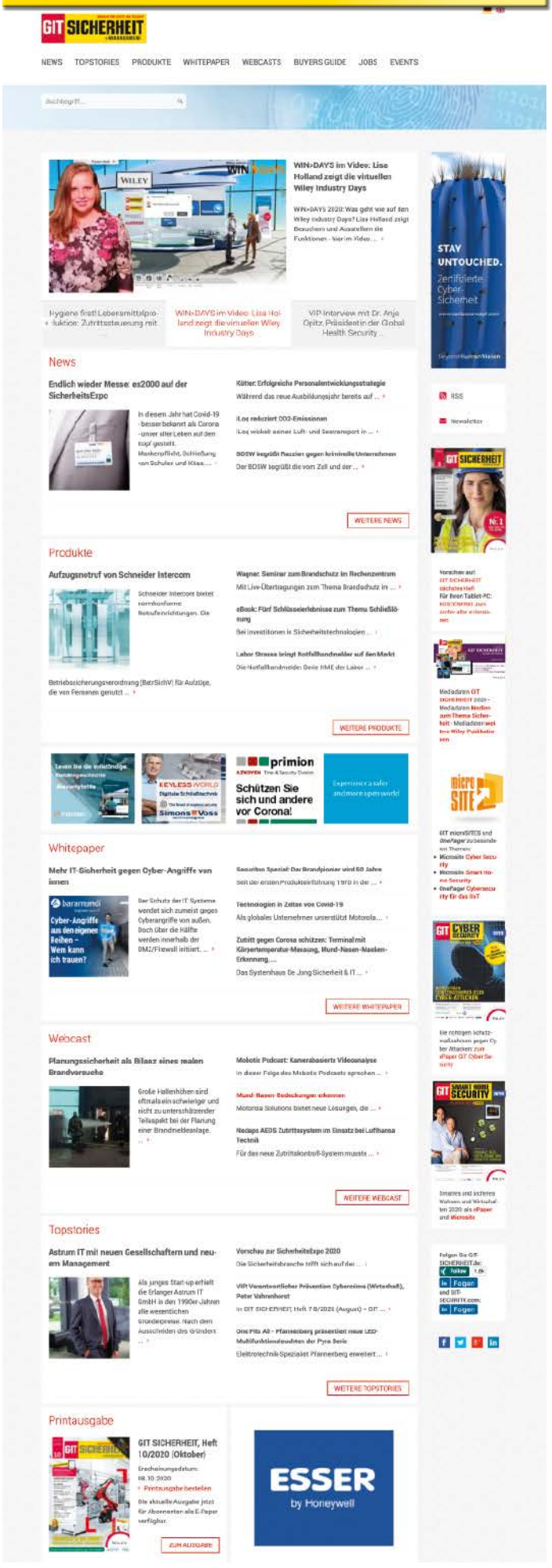
www.wagner.de ■

Feuertrutz Digital 2020: Fachmesse & Kongress

Die Feuertrutz Digital 2020 bot eine Kombination aus Fachmesse und Kongress als Online-Event. Nürnberg Messe und Feuertrutz Network haben alle Aspekte der gewohnten Präsenzveranstaltung mit begleitendem Kongress in die digitale Welt übertragen. Die Basis der Messe waren die Firmenprofile der teilnehmenden Aussteller. Über verschiedene Kommunikationstools wie Chats und Videocalls konnten die dem Profil zugeordneten Mitarbeiter des Unternehmens mit Kunden und Partnern in Kontakt treten. Ergänzt wurde die Basis der Feuertrutz Digital 2020 durch ein Rahmenprogramm mit zahlreichen Vorträgen von Ausstellern rund um bauliche, anlagentechnische und organisatorische Produkte und Dienstleistungen.

www.feuertrutz-messe.de ■

DIESEN MONAT AUF GIT-SICHERHEIT.DE



IMPRESSUM

Herausgeber
Wiley-VCH GmbH

Geschäftsführer
Sabine Haag, Dr. Guido F. Herrmann

Geschäftsleitung
Wiley Corporate Solutions
Roy Opie, Dr. Heiko Baumgartner,
Steffen Ebert, Dr. Katja Habermüller

Beirat
Erich Keil, FraSec Fraport Security Services GmbH, Frankfurt
Prof. Dr. Frithjof Klasen, Institut f. Automation u. Industrial IT, FH Köln
Volker Kraiß, Kraiss Consult, Bruchköbel
Prof. Dr. Norbert Pohlmann, Institut f. Internet-Sicherheit, FH Gelsenkirchen
Bernd Saßmannshausen, Merck, Darmstadt
Dr. Burkhard Winter, Dechema e.V., Frankfurt

Publishing Directors
Dipl.-Betriebswirt Steffen Ebert
Dr. Heiko Baumgartner

Wissenschaftliche Schriftleitung
Dipl.-Verw. Heiner Jerofsky (1991–2019) †

Anzeigenleitung
Miryam Reubold
+49 6201 606 127

Commercial Manager
Jörg Wüllner
+49 6201 606 748

Redaktion
Dr. Heiko Baumgartner
+49 6201 606 703
Dipl.-Betrw. Steffen Ebert
+49 6201 606 709
Matthias Erler ass. iur.
+49 6129 50 25 300
Dr. Timo Gimbel
+49 6201 606 049
Lisa Holland M.A.
+49 6201 606 738
Eva Kukatzki
+49 6201 606 761

Textchef
Matthias Erler ass. iur.
+49 6129 50 25 300

Herstellung
Jörg Stenger
+49 6201 606 742
Claudia Vogel (Anzeigen)
+49 6201 606 758

Satz + Layout Ruth Herrmann
Lithografie Ramona Scheirich

Sonderdrucke
Miryam Reubold
+49 6201 606 172

Wiley GIT Leserservice (Abo und Versand)
65341 Eltville
Tel.: +49 6123 9238 246
Fax: +49 6123 9238 244
E-Mail: WileyGIT@vuservice.de
Unser Service ist für Sie da von Montag–Freitag zwischen 8:00 und 17:00 Uhr

Wiley-VCH GmbH
Boschstr. 12, 69469 Weinheim
Telefon +49 6201 606 0
E-Mail: git-gs@wiley.com
Internet: www.git-sicherheit.de

Verlagsvertretungen
Dr. Michael Leising
+49 36 03 89 42 800

Bankkonten
J.P. Morgan AG, Frankfurt
Konto-Nr. 6161517443
BLZ: 501 108 00
BIC: CHAS DE FX
IBAN: DE55501108006161517443

Zurzeit gilt Anzeigenpreisliste vom 1.10.2019. Die namentlich gekennzeichneten Beiträge stehen in der Verantwortung des Autors.

2020 erscheinen 10 Ausgaben
„GIT SICHERHEIT"
Druckauflage: 30.000
inkl. GIT Sonderausgabe PRO-4-PRO

Abonnement 2020: 10 Ausgaben (inkl. Sonderausgaben) 118,00 €, zzgl. MwSt. Einzelheft 16,30 € zzgl. Porto + Mwst. Schüler und Studenten erhalten unter Vorlage einer gültigen Bescheinigung einen Rabatt von 50 %. Abonnement-Bestellungen gelten bis auf Widerruf; Kündigungen 6 Wochen vor Jahresende. Abonnementbestellungen können innerhalb einer Woche schriftlich widerrufen werden, Versandreklamationen sind nur innerhalb von 4 Wochen nach Erscheinen möglich.

Alle Mitglieder der Verbände ASW, BHE, BID, BDSW, BDGW, PMeV, Safety Network International, vfdb und VfS sind im Rahmen ihrer Mitgliedschaft Abonnenten der GIT SICHERHEIT sowie der GIT Sonderausgabe PRO-4-PRO. Der Bezug der Zeitschriften ist für die Mitglieder durch Zahlung des Mitgliedsbeitrags abgegolten.

Originalarbeiten
Die namentlich gekennzeichneten Beiträge stehen in der Verantwortung des Autors. Nachdruck, auch auszugsweise, nur mit Genehmigung der Redaktion und mit Quellenangabe gestattet. Für unaufgefordert eingesandte Manuskripte und Abbildungen übernimmt der Verlag keine Haftung.

Dem Verlag ist das ausschließliche, räumlich, zeitlich und inhaltlich eingeschränkte Recht eingeräumt, das Werk/den redaktionellen Beitrag in unveränderter oder bearbeiteter Form für alle Zwecke beliebig oft selbst zu nutzen oder Unternehmen, zu denen gesellschaftsrechtliche Beteiligungen bestehen, sowie Dritten zur Nutzung zu übertragen. Dieses Nutzungsrecht bezieht sich sowohl auf Print- wie elektronische Medien unter Einschluss des Internet wie auch auf Datenbanken/Datenträger aller Art.

Alle etwaig in dieser Ausgabe genannten und/oder gezeigten Namen, Bezeichnungen oder Zeichen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein.

Druck
westermann DRUCK | pva
Printed in Germany, ISSN 0948-9487

WILEY

GIT SAFETY

INNENTITEL

Diesen Monat Schwerpunkt:

Flexibles Zugriffs-management in der Nahrungsmittelindustrie

ab Seite 86

EUCHNER

More than safety.

MASCHINEN- UND ANLAGENSICHERHEIT

Der Schlüssel für sichere Lebensmittel

Flexibles Zugriffsmanagement in der Nahrungsmittelindustrie

Das elektronische Schlüsselsystem EKS von Euchner ermöglicht eine effiziente Zugriffskontrolle in unterschiedlichen Produktionsbereichen der Lebensmittelindustrie

Ob bei Löwensenf, Ritter Sport oder in der Backindustrie, bei der industriellen Herstellung von Lebensmitteln genießen Sicherheits- und Qualitätsstandards oberste Priorität. Das frei programmierbare Electronic-Key-System EKS von Euchner leistet hierbei einen entscheidenden Beitrag, da es eine effiziente Zugriffskontrolle in unterschiedlichen Produktionsbereichen ermöglicht.

Lebensmittelsicherheit ist für jeden Verbraucher ein hohes Gut. Das setzt hohe Qualitäts- und Sicherheitsstandards der bei der Produktherstellung angewandten Verfahren voraus. International maßgeblich dabei ist der IFS International Food Standard, der regelmäßig überarbeitet und erweitert wird. Unternehmen, die sich dafür zertifizieren lassen, müssen in wiederkehrenden Audits die Rückverfolgbarkeit aller Rohstoffe und Zutaten vom fertigen Produkt bis zum jeweiligen Lieferanten nachweisen. Unabhängig davon muss jeder Nahrungs- und Genussmittelhersteller sicherstellen, dass Rohmaterialien, Inhaltsstoffe, Verarbeitungsschritte sowie Verpackungen den einschlägigen Vorschriften und Richtlinien genügen und dies dokumentieren. Gleichzeitig gilt es, alle Risiken, die zu einer Kontaminierung oder unerwünschten Manipulation des von ihm hergestellten Produktes führen können, so weit wie möglich auszuschließen.

Zu den Sicherheitsstandards gehört die Überwachung von sensiblen Fertigungsprozessen über die Vergabe von Zugriffsberechtigungen. Dies erfolgt in vielen Fällen elektronisch. So greifen viele Lebensmittelhersteller auf das leistungsfähige Electronic-Key-System EKS von Euchner zurück. Es fungiert als intelligente Alternative zu mit

Passwort arbeitenden Systemen. Größter Vorteil des RFID-basierten EKS: Es lässt sich frei programmieren und daher besonders flexibel einsetzen. Außerdem sind Varianten mit unterschiedlichen Leistungsstufen erhältlich – vom einfachen EKS Light mit eingebauter Schlüsselerkennung und digitalen Ausgängen bis zur Variante mit Datenschnittstelle für mehr Datenübertragung und maximal flexibler Handhabung.

Für Lebensmittel- und Pharmaindustrie prädestiniert

EKS eignet sich für eine Vielzahl von Industrieanwendungen. Euchner hat das System für den Einsatz in der Lebensmittel- und Pharmaindustrie durch eine besondere Bauform der Schlüsselaufnahme ergänzt. Dafür wurden speziell Materialeinsatz und Produktdesign für Anwendungen in hygienisch sensiblen Bereichen angepasst. Im Vordergrund stehen einfache Reinigung und hohe Beständigkeit gegenüber Hochdruck-Wasserstrahlen. So erfüllt das robuste System die höchste Schutzart IP69K für elektrische Betriebsmittel. Das heißt: Es hält mühelos den regelmäßig bei Reinigungsarbeiten mit Heißwasser-Dampfstrahlern auftretenden hohen Temperaturen bei hohem Strahldruck stand.

Das Gehäuse der EKS-Schlüsselaufnahme besteht aus einem hochmolekularen Kunststoff, der speziell für die Lebensmittelindustrie zugelassen ist und die Anforderungen der FDA-Konformität erfüllt. Dank der geschlossenen Bauform lässt sich das System zudem sehr leicht reinigen. EKS ermöglicht die Zugriffskontrolle ganz und gar ohne Tastatur, die in einem hygienisch sensiblen Umfeld oft eher hinderlich ist. Der Benutzer muss den elektronischen Schlüssel nur „auflegen“: Die Kommunikation zwischen Schlüssel und Schreib-/ Lesestation erfolgt berührungslos. Das gleiche gilt für die Energieübertragung zwischen beiden Komponenten.

Qualitätssicherung mit EKS Light bei Löwensenf

Löwensenf in Düsseldorf nutzt mit EKS Light die einfachste Variante des Electronic-Key-Systems von Euchner. Bei ihr handelt es sich um ein Nur-Lese-System mit interner Benutzerkennung für kleinere und dezentrale Applikationen. Der Benutzer identifiziert sich lediglich per Schlüssel mit RFID-Transponder an der Schlüsselaufnahme. War die Identifizierung erfolgreich, erteilt ihm das System die vorab zugewiesene Zugriffsberechtigung, in diesem Fall die im Bereich Qualitätssicherung.

Rechts an der Bedienungseinheit: die modulare Schlüsselaufnahme von EKS Light

Dort überprüfen Kameras jede Senftube darauf, ob die aufgedruckten Produktionsdaten und der Tubenfalz in Ordnung sind, bevor sie zur Verpackungsmaschine weitergeleitet wird. „Uns war es vor allem wichtig, die Systemparameter zu schützen“, erläutert dazu Rainer Lang, Technischer Leiter bei dem traditionsreichen Lebensmittelhersteller. Laut Lang hätten die Steuerungen auch Passwortfunktionen erlaubt, „doch Passwörter machen schnell die Runde“. Aus diesem Grund zog er den elektronischen Schlüssel vor, der jedem Benutzer nur selektiv Zugriff auf die Systemparameter des Kamerasystems gewährt und so zuverlässig Fehlbedienungen von QM-System und Verpackungsmaschine blockiert.

Dabei unterscheidet EKS Light zwischen vier Berechtigungsstufen. Die erste bezieht sich auf den einfachen User, der ohne Chip die Anlage in ihren Grundfunktionen bedienen darf; die zweite auf Techniker, die nach erfolgreicher Identifizierung einzelne Einstellungen verändern dürfen; die dritte ist dem Qualitätsmanagement vorbehalten, während die vierte Administratorrechte freigibt.

Steuerung der Rohwarenlogistik bei Ritter Sport mit EKS Datenschnittstelle

Bei Deutschlands bekanntem Schokoladenproduzenten Ritter Sport im baden-württembergischen Waldenbuch ist EKS mit Datenschnittstelle im Einsatz. Dabei stellt das Electronic-Key-System sicher, dass Zutaten und Kakao-Rohmassen bei der Anlieferung im Rohwarenlager in die richtigen Behälter gefüllt werden. Üblicherweise wären dafür 32 Schlüsselschalter und ein hoher Verwaltungsaufwand nötig gewesen. Mit EKS erfolgt dies erheblich effizienter: Das Euchner-System benötigt lediglich vier Schreib-/ Lesestationen plus die Schlüssel-Chips.

Bei Anlieferung der Rohwaren wird ein EKS-Chip ausgegeben. Für jeden Abgabepunkt und Zielbehälter gibt es genau einen entsprechend programmierten und gekennzeichneten Chip. Nur wenn dessen Code eindeutig vom Lesegerät erkannt wird, erfolgt die Zutrittsberechtigung, sodass die Lieferung an der richtigen Annahmestation und im richtigen Zielbehälter abgeladen werden kann. Diese ist zusammen mit anderen Informationen in einer zentralen Datenbank hinterlegt. Die Schreib-/ Lesegeräte sind per PROFINET an die Steuerung gekoppelt, die alle relevanten Daten verarbeiten kann. Auf diese Weise lässt sich eindeutig rückverfolgen, wem, wann und wie lange Zugang zu der jeweiligen Anlieferungsstation gewährt wurde. Neben PROFINET sind Schnittstellen über USB, Ethernet TCP/IP und PROFIBUS erhältlich.

EKS mit Datenschnittstelle für umfassendes Zugriffsmanagement in der Backwarenindustrie

Die EKS-Variante mit Datenschnittstelle lässt sich aber auch ohne großen Aufwand für ein umfassendes Zugriffsmanagement nutzen. Ein interessantes Anwendungsfeld ist die Backindustrie. Insbesondere industrielle Backwarenhersteller profitieren von den vielen Einsatzmöglichkeiten des EKS-Systems. So kann es z. B. in Bäckereimaschinen zur Verarbeitung von Teigwaren wie Brot, Brezeln oder Croissants integriert werden.

Für die Rezepturverwaltung lassen sich auf dem EKS-Schlüssel beispielsweise Informationen zu Mischungsverhältnis, Zutaten oder Temperaturen speichern

Das Anwendungsspektrum reicht von der jeweils individuell zugänglichen Rezepturverwaltung mit Informationen zu Mischungsverhältnis, Zutaten und Temperaturen, die codiert auf dem Schlüssel gespeichert sind, bis zur damit verbundenen Berechtigung für die Umstellung der Backwarenproduktion. Nach Verarbeitung der entsprechenden Informationen kann die Steuerung den Prozess vollautomatisch lenken. Mit dem System können Zugriffe eindeutig zugeordnet und auch Produktionsstörungen nachvollzogen werden, die sich so für die Zukunft vermeiden lassen. Somit trägt das System dazu bei, die Anlagenverfügbarkeit zu erhöhen sowie die Produktivität und Qualität zu steigern. ■

Kontakt

Euchner GmbH + Co. KG
Leinfelden-Echterdingen
Tel.: +49 711 7597 0
www.euchner.de
info@euchner.de

In jeder Ausgabe erklären Sicherheitsexperten Begriffe aus der Maschinen- und Anlagensicherheit.

WAS IST EIGENTLICH… …RFID?

TORSTEN SINGER VON GEORG SCHLEGEL

Torsten Singer, Produktmanager, erklärt, was Georg Schlegel unter RFID versteht

© Georg Schlegel

Fast jeder kennt die grauen Kunststoff-Chips an Kleidungsstücken oder Elektroartikeln, die verhindern sollen, dass Waren aus Geschäften entwendet werden. Diese in den 60er Jahren entwickelte Diebstahlsicherung ist im Grunde die einfachste Form von RFID (Radio Frequency Identification): Der Transponder, der an der Ware angebrachte ist, auch Tag genannt, besteht aus einer Spule und einem Kondensator. Am Geschäftsausgang befindet sich ein Detektor, der ein elektromagnetisches Wechselfeld erzeugt. Wenn der Kunde das Geschäft verlässt, quert er dieses Wechselfeld. Befindet sich zu diesem Zeitpunkt der Transponder noch an der Ware, wird durch die Bewegung eine Spannung über die Spule des Tags induziert und der Kondensator geladen. Dieser minimale Energieentzug wird vom Detektor erkannt und durch ein entsprechendes Signal gemeldet.

Für komplexere Anwendungen war diese Technik nicht geeignet. Erst als der Kondensator durch einen Mikrochip ersetzt wurde, konnten größere Mengen an Daten auf den Transponder gespeichert werden. Damit war es auch möglich personen- oder produktspezifische Informationen zu übertragen und auszuwerten. Dies eröffnete weitere sinnvolle Einsatzbereiche für die RFID-Technologie.

RFID wird heutzutage unter anderem bei industriellen Anwendungen eingesetzt, etwa um Zugriffsberechtigungen zu verwalten, Prozesse zu steuern oder Produkte zu identifizieren. Aber auch im Sinne

der Industrie 4.0 spielt RFID eine große Rolle, denn viele Vorgänge können mit Hilfe dieser Technologie digitalisiert werden. Mit RFID ist es zum Beispiel möglich, in der Fertigung die Einzelteile eines Produkts zu identifizieren. Dadurch kann die Quote von fehlerhaft zusammengebauten Produkten signifikant reduziert werden.

Auch die Georg Schlegel GmbH & Co. KG setzt auf RFID-Technologie. Wurde bisher etwa für die Steuerung einer Maschine eine Schlüsseltaste eingesetzt, kann diese Funktionalität nun einfach per RFID umgesetzt werden. RFID hat den Vorteil, dass damit theoretisch beliebig viele Schalterstellungen möglich sind, wohingegen ein Schlüsselschalter aufgrund seiner Mechanik irgendwann an seine Grenzen stößt.

Über das RFID-System können zudem Zugangsberechtigungen für geschützte Unternehmensbereiche unkompliziert verwaltet werden, ohne dass dazu ein komplexes Schlüsselsystem notwendig ist. Neben der einfachen Verwaltung der individuellen Berechtigungen werden durch das RFID-System die Missbrauchsrisiken nach Verlust minimiert. Kann der Verlust eines Schlüssels im herkömmlichen System ein Sicherheitsleck bedeuten – verbunden mit hohem Aufwand und Folgekosten um dieses zu stopfen – wird bei RFID ein verlorener Schlüssel (Transponder) einfach und schnell aus dem System entfernt und durch einen neuen ersetzt. Der verlorene Tag kann somit nicht mehr eingesetzt werden.

RFID Standard von Georg Schlegel

Der RFID Standard ist ein flexibles, frei konfigurierbares System. Mit Hilfe von Kommando-Befehlen lässt sich das Lese-/Schreibgerät über eine externe Steuerung (SPS oder IPC) mit USB- oder RS232-Anschluss nach eigenen Bedürfnissen programmieren. Der Anwender kann die Datenstruktur auf dem Transponder beliebig definieren und über die externe Steuerung auswerten. Mit dem RFID Standard lassen sich durch das individuelle System theoretisch beliebig viele Transponder und Berechtigungsstufen verwalten.

RFID SKS

Schlegel RFID SKS ist ein eigenständiges RFID System, das für die einfache und schnelle Integration in bestehende Betriebsumgebungen konzipiert wurde. Es benötigt keine speziellen Anschlüsse, wie z. B. USB oder RS232, und es kann direkt auf die Ausgänge zugegriffen werden. Das System besteht aus vier aufeinander abgestimmten Komponenten: einem Lesegerät, einer Auswerteelektronik, einem Master Key (Admin Transponder) und den User Keys (Benutzer Transponder). Somit ist sichergestellt, dass das Lesegerät nur mit der passenden Auswerteelektronik kommunizieren kann und das Einrichten des Systems nur mit dem entsprechenden Master Key möglich ist. Die Validierung der Transponder erfolgt beim RFID SKS über das Lesegerät und muss nicht über eine externe Steuerung programmiert werden.

RFID TMS

Das RFID-TMS von Schlegel ist im Aufbau dem SKS sehr ähnlich, wird aber um eine Software zur Verwaltung der Transponder erweitert. Anders als beim SKS liegt beim TMS die Information im Transponder. Zur Programmierung der Transponder ist die Software zwingend, da sie mit einer kundenspezifischen Seriennummer erstellt wird, die beim Programmieren der Transponder mit abgespeichert wird. Somit können die Transponder nur von der Auswerteelektronik verarbeitet werden, die die gleiche Seriennummer ausweist. Damit ist sichergestellt, dass keine Funktionen durch fremde Transponder freigeschaltet werden können. ■

Kontakt

Georg Schlegel GmbH & Co. KG
Dürmentingen
Tel.: +49 7371 502 0
vertrieb@schlegel.biz
www.schlegel.biz

▲ Retrofit parallel zum laufenden Betrieb: Die Installations- und Validierungsphase stellte die Ingenieure vor besondere Herausforderungen

TITELTHEMA

Weichen effizient stellen

… dank übertragbarer Software und PSS 4000-R von Pilz

Produktabkündigungen sorgten bei der von den Verkehrsbetrieben Zürich (VBZ) betriebenen Dolderbahn und der Rigi Bahnen AG für innovative Retrofits: Eine generische, nur einmalig zu zertifizierende Softwarelösung und die sicheren bahntauglichen Module des Automatisierungssystems PSS 4000-R von Pilz steuern und überwachen Weichen unterschiedlichen Typs. Das Automatisierungsunternehmen zeichnete dabei nicht nur für die Softwareentwicklung, sondern auch für die Projektleitung, Validierung, Inbetriebnahme und Dokumentation verantwortlich. Ein Komplettpaket, das Pilz aus Sicht des Auftraggebers VT Verkehrs- und Industrietechnik AG höchst professionell, mit fundierter Fachkenntnis und in kürzester Zeit erbracht hat.

Auf die Sekunde pünktlich verlässt die Dolderbahn die Talstation Römerhof östlich der Zürcher Altstadt. Etwa sechs Minuten benötigt die elektrisch angetriebene Zahnradbahn, um auf dem Meterspur-Gleis bei einer mittleren Steigung von 19 Prozent 160 Höhenmeter zu überwinden. Nach rund 600 Streckenmetern begegnet sie an einer Ausweichstelle der talwärts fahrenden Bahn. In einem Schaltkasten am Rande des Gleisfeldes sorgen PSSuniversal Steuerungs- und E/A-Module von Pilz seit April 2020 für die sichere Ansteuerung der beiden nicht alltäglichen Schwenkweichen. Betriebsstörungen aufgrund falsch gestellter Weichen sind dadurch ausgeschlossen.

Die eingesetzten Module sind Bestandteile des bewährten sicheren Automatisierungssystems PSS 4000-R für maßgeschneiderte und wirtschaftliche Lösungen in der Bahnindustrie. Diese sind, den CENELEC-Normen EN 50121, EN 50126, EN 50128, EN 50129, EN 50155 und EN 45545 entsprechend, grundsätzlich bis SIL-4-fähig. Das Automatisierungssystem ist modular aufgebaut und eignet sich selbst für knifflige digitale Steuerungs- und Retrofit-Aufgaben optimal.

Investitionen auf der richtigen Bahn

Ob Fernzüge, Regional-, Straßen- oder Bergbahnen: der Schienenverkehr in der Schweiz gilt als besonders zuverlässig, komfortabel und sicher. Die Schweizer Bahnbetreiber investieren kontinuierlich in ihre Infrastruktur sowie in das rollende Material. Mitunter geben die vom Gesetzgeber an einen sicheren Bahnbetrieb gestellten Anforderungen den Anstoß, innovative und zukunftsweisende Lösungen zu entwickeln.

Bei der Zürcher Dolderbahn wie auch bei den Rigi Bahnen am Vierwaldstätter See wurden im Jahr 2018 die für die Weichensteuerung eingesetzten Produktlösungen abgekündigt. Die Bahnbetreiber wandten sich an die Schweizer VT Verkehrs- und Industrietechnik AG (VT AG). Das Unternehmen mit Sitz in Neuenhof bietet ein breites Leistungsangebot sowie den dazu passenden Service in den Bereichen Oberbau, Sicherung und Depot für die gesamte Infrastruktur von Bahn, Nahverkehr und Industrie.

Eine Lösung für drei Weichentypen

Leistungsfähige effiziente Systeme, die die geltenden CENELEC-Normen erfüllen, sollten an die Stelle der abgekündigten Weichensteuerung treten. Die aus drei unterschiedlichen Weichentypen bestehenden acht Weichen mit divergierenden Anforderungen an die Steuerung erwiesen sich als echte Herausforderung. So werden die beiden Schwenkweichen der Dolderbahn (Typ 1) von einem übergeordneten Stellwerk angesteuert und verfügen über keine eigenen Gleisfreimelder. Die Anzeige der Weichenlage erfolgt im Stellwerk. Erreicht die Weiche ihre Endlage nicht, generiert das System einen Fehler: Das Bahnpersonal muss die Position der Weiche vor Ort kontrollieren und diese ggf. von Hand in die Endlage bringen, damit der Betrieb aufrechterhalten werden kann.

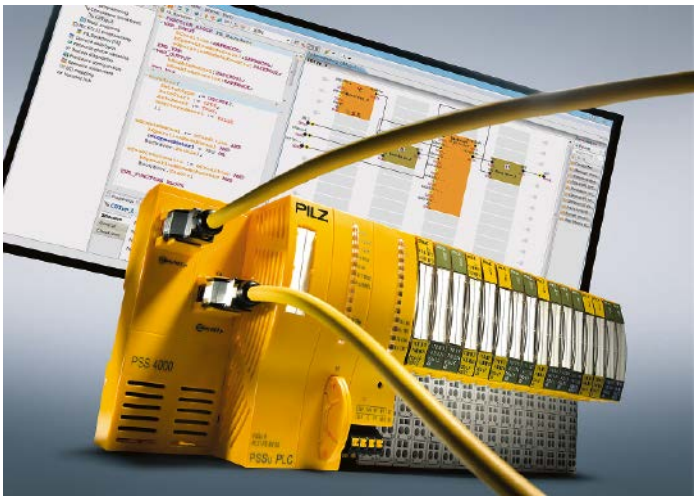
Der Weichentyp 2 (Rigi Bahnen) erhält den Stellbefehl primär per Funk. Zusätzlich ist eine Handbetätigung möglich. Die Weichen verfügen über eigene Gleisfreimelder und die Anzeige ihrer Lage erfolgt über einen Weichenlagemelder. Wird die Endlage nach dem Auslösen eines Stellbefehls nicht innerhalb eines definierten Zeitraumes erreicht, versucht die Steuerung die Weiche zurück in die Ausgangslage zu setzen. Weichentyp 3 verfügt zusätzlich über ein bewegliches Herzstück, das ebenfalls über die Weichensteuerung gestellt und überwacht wird.

Retrofit nach Fahrplan

„Allein schon aus Zeit- und Kostengründen – der Umbau respektive die Installation musste ja teilweise parallel zum laufenden Betrieb erfolgen – dachten wir an eine weitgehend standardisierte Hard- und Softwarelösung, die für alle Weichentypen gleichermaßen anwendbar sein sollte“, betont Daniel Rufener, Projektleiter bei der VT AG.

Schwenkweiche oberhalb der Station Rigi-Kaltbad. In der Steuerkabine ist die Weichensteuerung untergebracht, die auf den PSSuniversal Steuerungs- und E/A-Modulen von Pilz basiert

Die Lösung von Pilz trägt zur sicheren Weichenstellung bei – unabhängig von den Witterungsbedingungen



Das Automatisierungssystem PSS 4000-R von Pilz wurde für Railway-Anwendungen entwickelt und übernimmt sämtliche Automatisierungs- und Sicherheitsaufgaben

Die VT AG schrieb das Projekt aus, Pilz erhielt den Zuschlag. „Mit Pilz pflegen wir seit Jahren eine enge Partnerschaft. Das Unternehmen genießt nicht nur in Schweizer Bahnkreisen einen exzellenten Ruf. Darüber hinaus bietet Pilz mit den Rail-Modulen des Automatisierungssystems PSS 4000-R Komponenten „off the shelf", die sich in der Bahnpraxis bewährt haben", begründet Daniel Rufener die Wahl. Diese sind gegenüber den im Bahnumfeld oftmals eingesetzten proprietären Steuerungslösungen sowohl bei den Anschaffungs- als auch bei den Unterhaltungskosten deutlich günstiger. „Sehr überzeugend fanden wir, dass Pilz die Entwicklung einer so genannten generischen Software vorschlug", so Daniel Rufener. „Die erfüllt die geforderte CENELEC-Norm EN50128 sowie die SIL-2 Anforderung, muss aber nur einmal zertifiziert werden und ist in der Folge auf sämtliche Weichentypen übertragbar."

Steuert mehr als die Weichen

Die von Pilz entwickelte Steuerungslösung erfüllt unterschiedliche Aufgaben und Funktionen: Beim Weichentyp 1 ist sie ausschließlich für die Umstellung der Weiche respektive für die Ansteuerung der Hydraulik zuständig. Die Stellbefehle hingegen kommen von einer übergeordneten Steuerung im Stellwerk. Die Stelltechnik der Dolderbahn entspricht nun dem Stand der Technik, weichentypbedingt muss der Lokführer nach wie vor per Augenschein überprüfen, ob die Stellung der Weiche korrekt ist.

Bei Typ 2 und Typ 3 (Rigi Bahnen) übernimmt das Automatisierungssystems PSS 4000-R zusätzlich die Aufgabe einer übergeordneten Steuerung respektive die eines Stellwerks. D. h. es steuert sowohl die Hydraulik als auch die elektrischen Komponenten zur Umstellung der Weiche. Das Automatisierungssystem von Pilz überprüft darüber hinaus Stellbefehle, die per Funk oder von Hand gegeben werden, sowie die Weichenlage und Gleisfreimelder und verarbeitet die Informationen in der Software ziel- und sicherheitsgerichtet. „Jede einzelne Weichensteuerung musste dabei umgebaut und anschließend geprüft werden, da ein Test der Software mit der alten Steuerung nicht durchgeführt werden konnte", erläutert Daniel Rufener.

Logikfehler ausgeschlossen

Vorteil der generischen Lösung ist, dass die Hardware für alle drei Weichentypen identisch ist: „Die Auswahl des Weichentyps erfolgt durch einen spezifischen Hardwareeingang, der beim Aufstarten der Steuerung eingelesen wird. Die Steuerung überprüft anschließend alle nicht verwendeten Eingänge auf deren Signal und meldet automatisch, falls der falsche Typ ausgewählt wurde oder ein falsches Signal anliegt", erläutert Marco Biasca, Teamleiter Systemintegration bei Pilz.

Gemeinsam mit Kollegen Bernd Maier und Christian Korupp von Pilz war er neben der umfangreichen Software-Entwicklung für die Erstellen des Sourcecode, Inbetriebnahme, Validierung, den Ablauf des V-Models nach EN 50128 sowie für die komplette Dokumentation verantwortlich. „Wir sehen nicht alle Tage eine so sauber aufbereitete Projektdokumentierung", lobt der Gutachter André Rüegg von der Schweizerische Südostbahn (SOB).

Eine nur einmal zu zertifizierende generische Steuerungslösung bietet mehrere Vorteile: Installation und Inbetriebnahme beanspruchen weniger Zeit als konventionelle Lösungen. Das ist überall dort von Vorteil, wo ein Retrofit zumindest teilweise während des laufenden Betriebes erfolgen muss. Darüber hinaus lässt sich die Lösung einfach und zeitsparend auch auf künftig anstehende Weichensteuerungs-Retrofits übertragen.

Bei der Schweizer Verkehrs- und Industrietechnik AG stehen absehbar weitere Bahnprojekte und Retrofits an. „Von unserer Seite wollen wir auch in Zukunft weder auf die fachliche Kompetenz noch auf die ausgeprägten Normen-Kenntnisse und den angenehmen persönlichen Kontakt mit Pilz verzichten", fasst Daniel Rufener zusammen. ■

Kontakt

Pilz GmbH & Co. KG
Ostfildern
Tel.: +49 711 3409 0
info@pilz.de
www.pilz.de

Sicherheitskonzept für Antriebssysteme

Zusammen mit dem Abkantpressenhersteller Accurpress America erarbeitete Fiessler Elektronik ein Sicherheitskonzept für ein Antriebssystem. Innovationen und neue Konzepte für Antriebssysteme im Bereich der Abkantpressen erfordern neue Sicherheitskonzepte und somit Anpassungen. So auch am Beispiel des E-Prax-Systems der Firma Hawe (ehemals Hoerbiger). Das erarbeitete Sicherheitskonzept wurde sowohl für die kompakte Sicherheitssteuerung FPSC als auch für die modulare Sicherheitssteuerung FMSC umgesetzt und geprüft. Vor allem die FMSC unterstützt durch ihre freie Programmierbarkeit als auch schnellen Zykluszeiten die Adaptierung an vorgegebene Antriebskonzepte. Zusammen mit dem Know-how des Unternehmens und dem jeweiligen Maschinenhersteller können so effiziente und technisch hochwertige Lösungen für Abkantpressen erarbeitet werden. www.fiessler.de ■

Softwarepaket für Management der Prozesssicherheit ▲

ABB hat mit Ability Safetyinsight eine Suite von digitalen Softwareanwendungen auf den Markt gebracht, die Unternehmen aus der Energie- und Prozessindustrie das Management der Prozesssicherheit über den gesamten Lebenszyklus erleichtert. Ausgelegt als zentrale Informationsquelle digitalisiert die Software frühe Daten der Engineering-Technologie (ET), um ein digitales Abbild für die Prozesssicherheit zu erstellen. Diese Daten bilden dann den Kontext für die enorme Datenmenge, die durch informationstechnische (IT) und betriebstechnische (OT) Systeme generiert wird. Das Softwarepaket kombiniert IT- und OT-Daten mit ET-Daten und ermöglicht dadurch die Digitalisierung wertvoller Engineering-Informationen (wie PAAG-Verfahren und LOPA-Analyse). Diese werden dem Betriebs- und Wartungspersonal dann in vereinfachten, intuitiven und leicht verständlichen visuellen Formaten zugänglich gemacht.

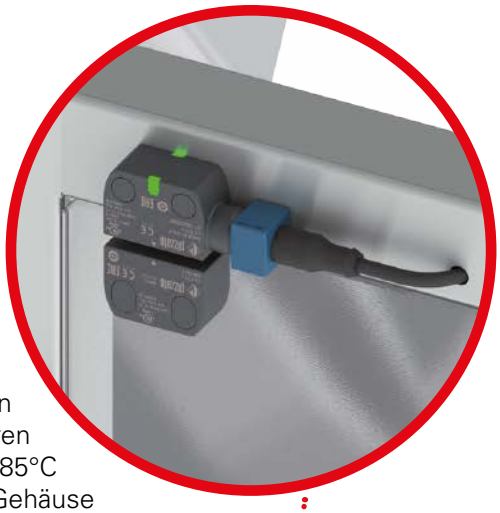
www.abb.com ■

Funk-Positionsschalter und Funksensoren

Mit „Wireless Ex" hat der Steute-Geschäftsbereich „Extreme" eine Technologie entwickelt, die Montage und Betrieb von Schaltgeräten in explosionsgefährdeten Bereichen erleichtert. Die Schaltgeräte sind nicht über ex-konforme Leitungen mit den Auswerteeinheiten im Schaltschrank verbunden, sondern über ein energiearmes Funkprotokoll, das gemäß Atex und IECEX zertifiziert ist. Konstrukteure von Anlagen und Geräten für explosionsgefährdete Bereiche können zum Beispiel die elektromechanischen Funk-Positionsschalter Ex RF 96 in schlanker Rechteck-Bauform verwenden, wenn die Position von beweglichen Anlagenkomponenten oder von Werkstückträgern abgefragt werden soll. Alternativ kann die Position auch berührungslos abgefragt werden – mit den Funk-Induktivsensoren Ex RF IS in Zylinderbauform (M 12, M 18 und M 30). . www.steute.com ■

pizzato

PASSION FOR QUALITY



Sicherheits-Sensoren
Serie ST G

> Mit mehreren Betätigern mit hoher Kodierungsstufe verwendbar
> Für jeden Betätiger kann eine andere Sensorantwort festgelegt werden
> Kann mit einer SPS kommunizieren
> Erweiterter Temperaturbereich von -35°C bis +85°C
> Kompakte Abmessungen, symmetrisches Gehäuse
> Ideal auch für den Lebensmittel- und Pharmabereich
> Auf dem Markt bisher nicht verfügbare Lösung

Befehlsgeber-Einheiten
Serie BN

> Modulares Gehäuse für 3... 8 Befehlsgebern
> Große Auswahl an verfügbaren Befehlsgebern
> Drehbare Module für maximale Flexibilität bei der Installation
> Konfigurierbar mit verschiedenen Typen von Anschlussabgängen
> Minimaler Platzbedarf 40x40 mm
> Gleiche Abmessungen und Materialien wie die RFID-Schalter der Serie NS

Sicherheit und Qualität gemäß EN ISO 14119

Sicherheits-Zuhaltung
Serie NS

> Verlängertes Gehäuse bietet die Möglichkeit, 3 oder 4 Befehlsgeber unterzubringen
> Große Auswahl an verfügbaren Befehlsgebern
> Drehbare Module für maximale Flexibilität bei der Installation
> Konfigurierbar mit verschiedenen Typen von Anschlussabgängen
> Kompatibel zu den Sicherheits-Türgriffen P-KUBE Krome

Entdecken Sie Pizzatos innovative Komponenten für die Industrieautomatisierung

Sicherheits-Türgriffe, Serie P-KUBE Krome

SICHERHEITS-TÜRGRIFFE, SERIE P-KUBE KROME

- Kompatibel zu den Serien NG und NS, also Zuhaltungen mit RFID-Technologie, gemäß EN ISO 14119.
- Integrierter, beleuchtbarer Taster für Signalgabe: Öffnen, Schließen, Zurücksetzen, etc.
- Griff kann an Schwing- oder Schiebetüren, in rechter oder linker Position, verwendet werden. Reduzierte Lagerhaltung.
- In der Griff-Fläche vollintegrierte RGB-LEDs zur lokalen Statusanzeige an der Schutzvorrichtung.

pizzato

PASSION FOR QUALITY

Online-Shop für Maschinensicherheit

Schmersal bietet seinen Kunden in Deutschland einen neuen Webshop für Komponenten der funktionalen Maschinensicherheit. Das Unternehmen hat seinen Online-Katalog mit einem automatisierten Bestell- und Versandprozess gekoppelt und damit ein sichereres Einkaufstool geschaffen, das den Kunden nach Registrierung 24 Stunden am Tag, sieben Tage die Woche zur Verfügung steht. Über den Webshop können rund 6.000 Sicherheits- und Automatisierungsprodukte direkt bestellt werden – vom einfachen elektromechanischen Sicherheitsschalter über programmierbare Sicherheitssteuerungen bis hin zu Software. Für jedes Produkt stehen darüber hinaus aktuelle, umfangreiche Produktinformationen zur Verfügung, die jederzeit abrufbar sind. Auch die Betriebsanleitungen und Zertifikate der Komponenten sowie viele weitere Dokumente werden als Download bereitgestellt.

www.schmersal.com ■

Abgrenzeinheit schützt Rohrleitungssysteme

Systeme wie Rohrleitungen mit einem hohen Ausbreitungs- und Vernetzungsgrad, die durch Fremdspannungen unterschiedlichster Störquellen beeinflusst werden, können sicher durch die kompakte Abgrenzeinheit DASD 45 LP 100 T von Dehn geschützt werden. Die Abgrenzeinheit ist eine kapazitive Abgrenzeinheit. Sie begrenzt sowohl stationäre, temporäre als auch transiente Überspannungen. Zudem werden alle auftretenden Fremdspannungen abgeleitet, ohne das Potenzial des kathodischen Korrosionsschutzes (DC-Potenzial) nachteilig zu beeinträchtigen. Die Auswirkungen dieser gefährlich hohen Überspannungen im unmittelbaren Einsatzbereich werden auf ein ungefährliches, sicherheitstechnisch vertretbares Maß begrenzt. Personen, die an der Pipeline arbeiten, sind so mit der Abgrenzeinheit vor gefährlichen Berührungsspannungen geschützt.

www.dehn.de ■

Sensorlose Drehzahlüberwachung

Dina Elektronik hat den Safeone DN3PD2 auf den Markt gebracht. Damit wird die sensorlose Drehzahlüberwachung vereinfacht. Durch die sensorlose Technik entfällt die Notwendigkeit eines zusätzlichen Gebers. Das ist vor allem bei schnell drehenden Teilen, an denen kein Geber angebracht werden kann, von Vorteil. Gerade bei Platzmangel im Schaltschrank stellt das Gerät aufgrund seiner kompakten Größe eine Alternative dar. Durch den direkten Anschluss an die drei Phasen des Motors wird auch die Konfiguration vereinfacht. Über ein eigens entwickeltes Softwaretool können per USB-Schnittstelle die Parameter eingestellt werden. Dies ermöglicht eine zuverlässige Validierung sowie eine vereinfachte Dokumentation. Der Frequenzbereich bis 1200 Hz erweitert die Einsatzmöglichkeiten des Drehzahlwächters.

www.dina.de ■

Prozessleitsystem sorgt für sichere Anlagen ▲

Um Anlagen sicher vor Cyberattacken zu schützen, hat B&R das Benutzermanagement des Prozessleitsystems Aprol weiterentwickelt. Verteilte autonome Sicherheitszellen schützen Anlagen effizient vor Schadsoftware und Hackerangriffen. Zum wirkungsvollen Schutz im World Wide Web werden große Anlagen in Sicherheitszellen aufgeteilt. Wird eine Sicherheitszelle von außen angegriffen, können alle anderen Zellen ohne Beeinträchtigung weiterarbeiten. Ein möglicher Schaden wird damit minimiert und zugleich die Verfügbarkeit der Anlage erhöht. Um dies zu erreichen, wird die Anlage zuerst in autonom funktionierende Automatisierungszellen (process cells) unterteilt. Diese bestehen aus produktionsrelevanten Zonen, Abschnitten, Teilbereichen oder Teilanlagen. Anschließend werden eine oder mehrere Automatisierungszellen wiederum in Sicherheitszellen (security cells) zusammengefasst.

www.br-automation.com ■

Schutzmaßnahmen für IT-Sicherheitskonzept

Schon sehr früh – parallel mit den ersten Profinet-Spezifikationen – veröffentlichte die Profibus Nutzerorganisation ein umfassendes Security-Konzept, das in mehreren Schritten weiter detailliert und angepasst wurde. Dabei reiche es nicht, Anlagennetze und Automatisierungskomponenten zu schützen, sondern die eingesetzten Schutzmechanismen und Konzepte dürften den laufenden Produktionsbetrieb nicht stören, so die Organisation. Zudem müssten Schutzkonzepte einfach umsetzbar und bezahlbar bleiben. Der wichtigste Aspekt sei jedoch, dass die Konzepte immer wieder an die aktuellen Entwicklungen angepasst werden müssen. Die Nutzerorganisation hat nun ihr IT-Sicherheitskonzept ergänzt. Zu der Erweiterung der bisherigen Schutzmaßnahmen gehören ein Credential Management, z. B. für eine Authentifizierung der Geräte, und eine End-to-End-Security-Erweiterung für die Profinet-Kommunikation als Konfigurationsoption.

www.profibus.com ■

Die GIT SICHERHEIT ist für mich wichtig, weil sie kompetent über Sicherheitskonzepte in den Bereichen Safety, Security, Ex- und Brandschutz informiert.“

Dr. Markus Winzenick, Geschäftsführung Fachverband Automation, Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI) e.V.

MASCHINEN- UND ANLAGENSICHERHEIT

So viele Ziegel, noch mehr Sicherheit

Das Schlüsseltransfersystem von Dold machts möglich

Bei der Produktion von Tondachziegeln herrschen sehr raue Umgebungsbedingungen. Systeme, die in diesem Umfeld zum Einsatz kommen, müssen dementsprechend robust sein. In der Materialaufbereitung von Creaton kommt deswegen das Sicherheitsschalter- und Schlüsseltransfersystem Safemaster STS zum Einsatz, um für die nötige Arbeitssicherheit zu sorgen.

Das Dachdecken mit Tonziegeln auf Steildächern ist eine sehr alte Technik, die bereits im antiken Rom vor über 2.000 Jahren gängig war. In dieser Tradition steht heute das Unternehmen Creaton, das auf eine lange Firmengeschichte zurückblicken kann. 1884 gründete Alois Berchtold in Wertingen eine Ziegelei und erwarb sich schnell einen Ruf als Qualitätshersteller von Tondachziegeln. Heute gehört das Unternehmen Creaton zur Etex-Gruppe und brennt allein in Wertingen jährlich rund 20 Millionen Pressdachziegel. Nach einer Brandkatastrophe im Mai 2007 wurde das komplette Werk saniert und im Anschluss modernisiert wieder aufgebaut. Heute zählt es zu einem der modernsten Tondachziegelstandorte in Europa.

Naturprodukt fürs Dach

Die Produktion von Dachziegeln basiert auf natürlichen Rohstoffen: Ton und Lehm wird in einem bestimmten Mischungsverhältnis verarbeitet und darf nicht zu nass sein. Für das Werk in Wertingen werden 75.000 Tonnen Rohmaterial pro Jahr in der Materialaufbereitung angeliefert. Dort gelangen drei verschiedene Rohstoffe über Förderbänder in einen Kollergang. Dessen tonnenschweren Läufer zermahlen das Rohmaterial und pressen es schließlich durch einen Rost. Für die gleichbleibende Qualität des Endprodukts ist das Dosierverhältnis der drei Rohstoffe, die aus verschiedenen Gruben stammen, von entscheidender Bedeutung.

Nach dem Kollergang folgen zwei Walzwerke, in denen das Material weiter zerkleinert wird. Im Anschluss gelangt das fertige Material ins Sumpfhaus, in dem es rund drei Wochen reifen muss. Am Ende dieser Zeit liegt der Wassergehalt bei 19,5 % und 20 %. Nun gelangt das Material vom Sumpfhaus zu den Pressanlagen, die es vollautomatisch in die richtige Form bringen. Nach dem Trocknen werden die so entstandenen Rohlinge in den Brennofen transportiert. Sollen die Dachziegel farbig oder glasiert sein, werden sie vor dem eigentlichen Brennen noch mit

der entsprechenden Farbe bzw. dem Glasurmaterial besprüht.

Absicherung von Türen zu den Aufbereitungsanlagen

In der Fertigung sind rund 50 Mitarbeiter in den verschiedenen Bereichen teilweise im Zwei-Schicht-Betrieb tätig. Im vollautomatischen 24-Stunden-Betrieb hat immer ein Mitarbeiter Bereitschaftsdienst, der bei einer Störung benachrichtigt wird. „Selbstverständlich wollen wir die geforderte Produktionsleistung immer erfüllen", so der Werksleiter: „Dabei hat aber die Sicherheit der Mitarbeiter stets oberste Priorität."

Gerade in der Materialaufbereitung hat das Unternehmen in den vergangenen Monaten daher viel in die Sicherheit investiert. So wurde der Zugang zu sämtlichen Anlagenteilen mit Zäunen gesichert. Für Reinigungs- und Wartungsarbeiten sind mehrere Türen und Tore integriert. In den meisten Fällen wird die Anlage von einem einzelnen Mitarbeiter bedient. Die Überwachung durch einen Kollegen zur erhöhten Sicherheit scheidet deswegen aus. Daher wurden die Zugänge so gesichert, dass der Mitarbeiter nur dann Zugang erhält, wenn die Maschine steht.

Bei der Realisierung der Sicherheitstechnik hat man sich für ein System von Dold & Söhne entschieden. Das Sicherheitsschalter- und Schlüsseltransfersystem Safemaster STS kombiniert die Vorteile von Sicherheitsschalter, Zuhaltung, Schlüsseltransfer und Befehlsfunktionen und kann modular ausgebaut werden. Das Schlüsseltransfersystem ist in der Leitwarte der Materialaufbereitung an eine Sicherheits-SPS angebunden. Möchte ein Mitarbeiter Zugang zu einer der Türen erhalten, muss er diesen zunächst über die Benutzerschnittstelle der Steuerung anfordern.

Er kann den Schlüssel allerdings erst entnehmen, wenn die Maschine zum Stillstand gekommen ist. Mit dem Schlüssel ist es dem betreffenden Mitarbeiter dann möglich, die entsprechende Tür zu öffnen. Wenn er alle Arbeiten innerhalb des Schutzbereichs erledigt hat, schließt er die Tür wieder, entnimmt den Schlüssel und steckt ihn wieder in das zentrale System an der Leitwarte. Erst dann lässt sich die Anlage wieder einschalten.

Auch ein Schutz gegen versehentliches Einsperren eines Mitarbeiters ist im Safemaster STS integriert. Dazu ist an den Türen eine LOTOTO-Funktion (Log Out Tag Out) vorgesehen. Jeder Mitarbeiter hängt beim Betreten der Anlage sein persönliches Vorhängeschloss in das LOTOTO-Modul am STS-System ein. Dadurch werden ein versehentliches Schließen der Tür und ein mögliches Starten der Maschine wirkungsvoll verhindert.

Robustes System, einfach zu installieren

Einer der Vorteile von Safemaster STS, ist die hohe Widerstandsfähigkeit, wie Instandhaltungsleiter Wolfgang Schülein betont: „Die Komponenten bestehen aus Edelstahl und sind dadurch sehr robust – eine ideale Lösung also für die rauen Umgebungsbedingungen in unserer Materialaufbereitung." In diesem Bereich der Tondachziegelproduktion ist es durch das Ausgangsmaterial sowohl staubig als auch feucht. Weniger widerstandsfähige Komponenten können unter diesen schwierigen Bedingungen nur schlecht eingesetzt werden.

Die Installation des Systems und die Anbindung an die Sicherheits-SPS hat das Team aus der Instandhaltung in Eigenregie realisiert. Besonders hilfreich war dabei, dass die elektrotechnische Anbindung nur an einer Stelle erfolgen muss. Die Verriegelungen an den Türen arbeiten rein mechanisch.

Manuell bedienen mit Zustimmtaster

Die Zäune und die Absicherung der Türen und Tore haben allerdings auch Nachteile, wie W. Schülein berichtet: „Bei Reparaturen und Wartungen an der Anlage können die Antriebe nicht gestartet werden. Das ist aber manchmal notwendig, um etwa zu überprüfen, ob alles richtig funktioniert." Für solche Fälle wurde ein kabelloser Zustimmtaster aus der Serie Safemaster W in das Sicherheitskonzept integriert.

Das System besteht aus einem kompakten Handsender und einem Funk-Sicherheitsschaltgerät, das an die Sicherheits-SPS angebunden wird. Der Mitarbeiter meldet sich mit dem Zustimmtaster über Funk an und kann dann einzelne Antriebe gezielt anschalten. Welcher Antrieb ausgewählt ist, erkennt er auf dem integrierten Display.

Das System ist besonders sicher, da es sowohl einen Totmanntaster mit einem Paniktaster kombiniert. Lässt der Mitarbeiter den Taster los, schaltet der Antrieb sofort ab. Gleiches passiert, wenn er den Taster komplett durchdrückt. Die Möglichkeit der Festlegung einer Startzone per Infrarot stellt dabei sicher, dass sich nur Antriebe im direkten Umfeld des Bedieners über das Funksystem einschalten lassen.

Durchweg positive Erfahrungen

Das installierte System mit der Türzuhaltung über das Safemaster STS ist inzwischen von der zuständigen Berufsgenossenschaft

▲ Sicherheitszäune schützen vor den gefährlichen Anlagenteilen in der Materialaufbereitung.

▲ Mit dem Zustimmtaster der Safemaster W Serie meldet sich der Mitarbeiter über Funk an und kann dann einzelne Antriebe gezielt anschalten

▲ Ein LOTOTO-Modul an der Tür verhindert, dass diese geschlossen wird, wenn sich noch ein Mitarbeiter an der Anlage befindet

Bitte umblättern ▶

abgenommen. „Sämtliche Sicherheitsmaßnahmen im Werk besprechen wir in unserem Arbeitssicherheits-Ausschuss“, sagt F. Kanefzky. In diesem sind neben den ausgebildeten Sicherheitsfachkräften auch der Betriebsrat, die Schichtführer und Mitglieder der Berufsgenossenschaft vertreten.

„Bei der Planung der Sicherheitseinrichtungen für die Materialaufbereitung war es uns besonders wichtig, dass auch die Mitarbeiter, die täglich an der Anlage arbeiten, mit ins Boot geholt wurden“, betont der Werksleiter. Denn nur wenn die Mitarbeiter mit dem System zufrieden sind, können sie auch optimal damit arbeiten. Werden z. B. tägliche Tätigkeiten behindert, sinkt nicht nur die Produktivität, sondern Mitarbeiter sind dann eher versucht, die Systeme zu manipulieren.

Insgesamt hat Creaton mit den Komponenten und Systemen von Dold sehr gute Erfahrungen gemacht. „Diese haben ganz wesentlich dazu beigetragen, dass wir die Arbeitssicherheit in der Materialaufbereitung erheblich verbessern konnten“, bringt F. Kanefzky seine Meinung auf den Punkt. ■

Kontakt

E. Dold & Söhne KG
Furtwangen
Tel.: +49 7723 654 0
dold-relays@dold.com
www.dold.com

Bert Spiller, Vice President Product Creation bei Timberland Pro

Mark Zhu, Market Segment Manager for Footwear, Sports and Leisure bei BASF

SICHERHEITSSCHUHE

Zwei starke Partner schreiten voran

Die nächste Evolutionsstufe des Sicherheitsschuhs

Wer hat gesagt, dass Arbeitsstiefel langweilig und unbequem sein müssen? Bert Spiller, Vice President Product Creation bei Timberland Pro und Dr. Mark Zhu, Market Segment Manager for Footwear, Sports and Leisure bei BASF Performance Materials sprechen mit GIT SICHERHEIT über den neuen Sicherheitsschuh Timberland Pro Reaxion.

GIT SICHERHEIT: Was macht den Reaxion Ihrer Meinung nach zu einer solchen Innovation auf dem Sicherheitsschuhmarkt?

Bert Spiller: Nun, der Reaxion Sicherheitsschuh ist mit dem geschützten Aerocore Energy System von Timberland Pro ausgestattet, das den Komfort und die Flexibilität eines Sportschuhs mit der Leistung und Haltbarkeit eines Arbeitsstiefels verbindet. Wir wollten den Arbeitern eine neue Erfahrung bieten - einen Schuh, der so attraktiv ist wie ihr Lieblingssportschuh und der die Energie zurückgibt, die sie den ganzen Tag lang in Bewegung hält. Der Reaxion wird sowohl als Sport- als auch als Wanderschuh angeboten, ist in wasserfester und nicht wasserfester Ausführung erhältlich und wird mit einer Sicherheitszehenkappe aus einem gewichtsreduzierenden Verbundwerkstoff geliefert.

Warum hat Timberland Pro mit BASF und BASF mit Timberland Pro zusammengearbeitet?

Bert Spiller: Wir arbeiten mit BASF seit 1995 zusammen, als Timberland den atmungsaktiven Polyurethanschaum der BASF als kostengünstige, leistungsfähigere Alternative zu EVA für Einlegesohlen einführte. BASF hat über 40 Jahre Erfahrung mit Schuhmaterialien und bietet einen einzigartigen und integrierten Lösungsbaukasten. BASF und Timberland verbindet darüber hinaus ein ausgeprägtes Nachhaltigkeitsdenken. Das Motto der BASF lautet „Wir schaffen Chemie für eine nachhaltige Zukunft", und es ist schön, mit einem Unternehmen zusammenzuarbeiten, das man herausfordern kann, innovativ zu sein, und das sich dieser Herausforderung stellt. BASF hat Timberland bereits einen biobasierten Polyurethan-Werkstoff für Einlegesohlen zur Verfügung gestellt, und wir arbeiten weiterhin mit BASF an anderen Lösungen.

Mark Zhu: Timberland ist ein führendes und innovatives Unternehmen in der Schuhindustrie. Und wie Bert erwähnte, ist auch die Nachhaltigkeit ein wichtiges Bindeglied. Bis zum Jahr 2030 will Timberland 100 % seiner Produkte für den Kreislauf konzipieren und 100 % der Materialien aus regenerativer Landwirtschaft beziehen, um nicht nur Klimaneutralität zu erreichen, sondern einen positiven Effekt auf die Natur zu erzielen.

Die meisten Menschen denken wahrscheinlich nicht an Chemie, wenn es um Schuhkomfort geht. Wie hat die Chemie die Innovation beim Design des Reaxion vorangetrieben? Was ist das Besondere an den Polyurethanen (PU) und Thermoplastischen Polyurethanen (TPU), die BASF herstellt?

Mark Zhu: Das Aerocore Energy System besteht aus drei Schichten: einer TPU-umwickelten Zwischensohle, dem Anti-Ermüdungs-Fußbett mit Anti-Ermüdungstechnologie und einer nicht abfärbenden Laufsohle. Die Schichten arbeiten zusammen und bieten eine hervorragende Energierückgabe, Komfort und Griffigkeit. Diese Eigenschaften führen zu einem besonders vielseitigen Arbeitsschuh, der den Timberland Pro Reaxion ideal für Arbeiten in Innenräumen wie Lager und Fertigung sowie für Außenarbeiten auf dem Bau und in anderen Bereichen macht.

Das Elastollan TPU von BASF wird in der Laufsohle wegen seiner hervorragenden Abriebfestigkeit und Traktionseigenschaften eingesetzt. Elastopan PU-Schaum mit hoher Rückprallelastizität wird in der Zwischen- und Brandsohle verwendet, um ganztägigen Halt und Komfort zu bieten. BASF war in der Lage, die Formulierung des PU auf molekularer Ebene individuell so anzupassen, wie das Timberland Pro-Team es für seinen neuen Reaxion-Sicherheitsschuh benötigte. Die Fähigkeit, die Kundenbedürfnisse zu verstehen und dies in eine Materiallösung umzusetzen, ist eine Expertise der BASF.

Wird das Aerocore System in zukünftigen Schuhmodellen von Timberland PRO zu sehen sein?

Bert Spiller: Auf jeden Fall!

Wo kann man den Reaxion kaufen?

Bert Spiller: In EMEA ist der Herrenschuh jetzt erhältlich. Der Damenschuh wird im Jahr 2022 erhältlich sein. In Nordamerika sind sowohl Herren- als auch Damenschuhe online unter timberlandPRO.com sowie bei unseren Einzelhandelspartnern im ganzen Land erhältlich.

Was war die größte Herausforderung bei der Reaxion?

Bert Spiller: Einen Weg zu finden, einen Schuh, der traditionell unbequem war und keinen Spaß macht, zu einem Schuh zu machen, den die Leute ständig tragen wollen. BASF und ihr Material-Know-how haben es uns ermöglicht, dies in die Realität umzusetzen.

Welches Feedback haben die Träger des Schuhs gegeben?

Bert Spiller: Das Feedback, das wir erhalten haben, war sehr positiv. Die Leute sagen uns, dass es der leichteste Timberland Pro Schuh ist, den sie je ausprobiert haben und der bequemste. Probieren Sie ihn aus und überzeugen sie sich selbst davon! ■

▲ Der Timberland Pro Reaxion in unterschiedlichen Designs

Kontakt

BASF
Ludwigshafen
Tel.: +49 621 60 422 42
footwear@basf.com
www.basf.com

PSA

Kosten runter, Sicherheit rauf

Ganzheitliches Standortkonzept gefragt

In vielen Unternehmen muss aktuell der Rotstift angesetzt werden. Gewichtige Ausgaben kommen hierbei auf den Prüfstand, auch die Persönliche Schutzausrüstung (PSA). Denn mit einer Konsolidierung der PSA-Artikel und einer Verschlankung der damit verbundenen Beschaffungsprozesse lassen sich die Kosten senken und gleichzeitig die Sicherheit erhöhen. Ein ganzheitliches, standortübergreifendes Konzept bildet dafür die Grundlage.

Checkliste:

PSA-Konsolidierung und Prozessoptimierung

- Bilden einer Task Force mit Vertretern aller beteiligten Interessengruppen
- Analyse der aktuellen IST-Situation
- Bilden standortübergreifender Cluster für Arbeitsumfeld- und Gefährdungen
- PSA-Produktportfolio/Bestellprozesse
- Definition von Mindestanforderungen und Schutzklassen
- Lieferantenauswahl/Konsolidierung der Vendorenliste
- Standardkatalog: Produktauswahl unter Berücksichtigung der Corporate-Design-Richtlinien
- Überarbeitung der Einkaufsrichtlinien
- Einführung von PSA-Ausgabeautomaten
- Automatisierung des Bestellprozesses

Das Angebot an PSA-Artikeln auf dem Markt ist in den letzten Jahren kontinuierlich gewachsen. In vielen Unternehmen wurden die Einkaufslisten dadurch länger und unübersichtlicher. Oftmals kamen neue Produkte hinzu, und die Mitarbeiter meldeten zusätzlich ihre Sonderwünsche an.

Wildwuchs beschneiden

Vor allem in größeren Organisationen mit mehreren Standorten und dezentralem Einkauf hat sich vielerorts ein regelrechter „Wildwuchs" entwickelt. Ein konsolidierter und unternehmensweit verbindlicher PSA-Standardkatalog und überarbeitete Einkaufsrichtlinien helfen, die PSA-Beschaffung zu vereinfachen und Sonderbestellungen auf ein Mindestmaß zu reduzieren. Davon kann auch die Arbeitssicherheit profitieren, weil nur noch einheitlich getestete und überprüfte PSA verwendet wird.

▲ Ausgabeautomaten beschleunigen die Beschaffungsprozesse und versorgen die Mitarbeiter zuverlässig rund um die Uhr

Garant Tool24 PickOne (links) & Garant Tool24 Locker (rechts)

Qualitätsstandards hochhalten

Für den Erfolg in der Umsetzung ist es wichtig, dass alle betroffenen Interessensgruppen in den Entscheidungsprozess eingebunden und angehört werden. Je nach Unternehmensgröße und Organisation sind das zum Beispiel: Strategische Einkäufer, Betriebsarzt, Sicherheitsingenieure, Produktionsleiter, Niederlassungsleiter und natürlich die Mitarbeiter als Träger der PSA. Dabei ist erfahrungsgemäß vor allem dann schnell ein tragfähiger Konsens zu finden, wenn die Qualitätsstandards hochgehalten werden und die Mitarbeiter die Lösung nicht nur begutachten, sondern auch probetragen können.

Für die Definition der Mindestanforderungen und Schutzklassen ist es notwendig, unternehmensweit die Arbeitsplatzanforderungen zu klassifizieren und zu clustern. Dazu müssen ausführliche Arbeitsplatzbegehungen und eine Gefahrenanalyse durchgeführt werden. Zusätzlich gilt es, das komplette PSA-Produkt-Portfolio sowie die zugehörigen Bestellprozesse unter die Lupe zu nehmen, mit dem Ziel, einen Standardkatalog und einheitliche Bestellprozesse zu definieren.

Mehrstufig zum Ziel

Die Mitarbeiter sollten schon sehr früh in das Projekt einbezogen werden. Dabei ist jedoch Fingerspitzengefühl gefragt. Um die Akzeptanz des Projektes zu erhöhen, fängt man mit unkritischeren Produktbereichen wie Kopfschutz an und bearbeitet jene Bereiche, die bei einem anstehenden Produktwechsel einen höheren Aufwand verursachen, erst zum Schluss.

Ein komplexeres Thema ist zum Beispiel der Fußschutz, denn jeder Fuß ist anders. Für den perfekt passenden Sicherheitsschuh müssen die Füße der Mitarbeiter genau vermessen und etwaige gesundheitliche Anforderungen geprüft und aufgenommen werden. Bei den Sicherheitsschuhen ist es häufig sinnvoll, zwei Modelle zur Auswahl anzubieten. Besonders komfortabel sind Schuhe mit Mehrweitensystem und verschiedenen Dämpfungsklassen. Diese werden sowohl schmaleren als auch breiteren Füßen gerecht und können auf das Körpergewicht der Träger abgestimmt werden. Bei den Schuhen spielt außerdem das Design eine wichtige Rolle. Denn Schuhe sollen auch gefallen und möglichst zum Corporate Design des Unternehmens passen.

Anders verhält es sich mit dem Gehörschutz. Hier stehen Tragekomfort und Qualität im Vordergrund. Das gilt auch für Hand-, Kopf-, Augen- und Atemschutz.

Schwieriger wird es wiederum, Schutzkleidung auszuwählen. Schließlich wollen die Mitarbeiter nicht nur gut geschützt und bequem ausgestattet sein, sondern sich auch wohlfühlen und gut aussehen.

Weil der Tragekomfort für die Mitarbeiterakzeptanz ein wichtiges Kriterium ist, sollten außerdem sämtliche Produkte über einen längeren Zeitraum von kleinen Pilotgruppen probegetragen werden, bevor sie in den Standardkatalog kommen. Ein Tragetest dauert in der Regel vier bis sechs Wochen.

Bei einer internationalen Belegschaft ist dabei zu berücksichtigen, dass Konfektionsgrößen in den verschiedenen Ländern variieren. Aus diesem Grund ist es wichtig, dass bei europaweiten Projekten Mitarbeiter aus allen Ländern in die Tragetests eingebunden und vor Ort intensiv betreut werden.

Individualität im Einheitslook

Weil eine einheitliche Ausrüstung das Zusammengehörigkeitsgefühl und die Mitarbeiterbindung stärkt, stellen immer mehr Unternehmen auch Arbeitskleidung für ihre Mitarbeiter bereit. Dabei wird besonderer Wert auf die Einhaltung von Corporate-Design-Vorgaben gelegt. Dennoch sollten die Mitarbeiter Wahlmöglichkeiten haben.

Bei der Oberbekleidung kann das zum Beispiel so aussehen: ein T-Shirt, ein Sweatshirt und ein Polo-Shirt stehen zur Wahl; der Mitarbeiter kann sich zwei Oberteile aussuchen. Um die Corporate Identity zu unterstreichen, werden die Textilien in der Regel mit dem Firmen-Logo veredelt. Das kann per Direkteinstickung, Stickemblem, Transferdruck und Lasergravur geschehen.

Gebündelte Bestellungen

Nach dem PSA-Sortiment kommen die Beschaffungsprozesse auf den Prüfstand, denn häufig kann auch eine stärkere Bündelung der Auftragsvergabe beachtliche Einsparpotenziale erschließen. Fachhändler mit einem sehr tiefen Produktsortiment haben hier die Nase vorn. Weil PSA jedoch

▲ Der Weg zu passenden Schuhen führt über Fußvermessungen und Tragetests

beratungsintensiv ist, sollte der PSA-Kooperationspartner auch über einen professionellen Beratungsservice verfügen. Dieser muss vor Ort Fachfragen klären und die Niederlassungen aktiv bei Tragetests, Schulungen und der Einweisung der Mitarbeiter unterstützen können. Sonderbestellungen sollten ebenfalls möglich sein, um die notwendige Flexibilität zu erhalten.

Wie sich der Beschaffungsprozess für persönliche Schutzausrüstung effizienter gestalten und um 75 % beschleunigen lässt, zeigt das Beispiel von Man Energy Solutions am Standort Zürich. Dort wurden die Bestellungen auf die Hoffmann Group als Hauptlieferant konzentriert, der Einzelausgabesystem Garant Tool24 PickOne eingeführt und der Beschaffungsprozess für PSA vollautomatisiert.

Vollautomatisierte Prozesse

Bei Erreichen eines Mindestbestands schickt Garant Tool24 PickOne automatisch eine Bestellung an die Hoffmann Group. Dadurch entfallen Bestellanforderungen und Einzelbestellungen. Es gibt nur noch eine Wertrahmenbestellung über einen bestimmten Betrag, von dem die automatisch ausgelösten Bestellungen abgezogen werden. Ist dieser ausgeschöpft, erfolgt die nächste Rahmenbestellung, mit der die zugehörige Wareneingangsbuchung vorgenommen wird. Etwaige Abweichungen bei Soll- und Ist-Menge werden beim Befüllen des Systems festgestellt.

Die PSA geht direkt vom Wareneingang in den Automaten. Den Beschaffungsprozess hat das Unternehmen damit von fünf bis acht Tagen auf zwei Tage verkürzt. Die Hoffmann Group liefert die Ware binnen 24 Stunden nach Auftragseingang. Anschließend wird Garant Tool24 PickOne von Man-Mitarbeitern aufgefüllt.

24/7-Verfügbarkeit

Warenausgabesysteme wie Garant Tool24 PickOne sorgen außerdem dafür, dass die erforderliche PSA rund um die Uhr zur Verfügung steht. Zusätzlich ermöglichen sie es, mit Hilfe des integrierten Reportings den Nachweis zu erbringen, dass jeder Mitarbeiter jederzeit die für ihn erforderliche PSA entnehmen konnte und das auch getan hat. Dazu lassen sich Anwenderprofile so anlegen, dass die Mitarbeiter nur auf die für ihren jeweiligen Arbeitsbereich zugelassenen PSA-Artikel Zugriff erhalten.

Fazit

Eine Vereinheitlichung der zu beschaffenden PSA-Artikel in einem Standardkatalog und eine Lieferantenkonsolidierung in Kombination mit einer weiteren Automatisierung der Beschaffungsprozesse kann zu deutlichen Kosteneinsparungen führen. Zusätzlich lässt sich dadurch sichergestellen, dass nur jene PSA beschafft wird, die exakt den Sicherheitsanforderungen entspricht. Das erhöht die Arbeitssicherheit. ■

Autorin
Alexandra Kovacs
Projektmanagerin PSA bei der Hoffmann Group

Kontakt

Kontakt
Hoffmann SE
München
Tel.: +49 89 8391 0
info@hoffmann-group.com
www.hoffmann-group.com

Gesetzliche Mengengrenzen ermitteln

Denios hat mit seiner Mengen-Checker-App über 100 Seiten Gesetzestext aus drei Regelwerken in einem Tool vereint. Mit der Mengen-Checker-App werden Fragen beantwortet, ob Gefahrstoffe gesetzeskonform gelagert werden, ab welchen Mengen ein Gefahrstoffschrank oder ein Gefahrstofflager benötigt wird und wie viel außerhalb gelagert werden darf. In der App wird der gewünschte Gefahrstoff eingestellt und folgende Infos können abgelesen werden: die Menge, die über die Bereitstellung hinaus außerhalb eines Gefahrstofflagers aufbewahrt werden darf; die Mengengrenze, bis zu der der Gefahrstoff in einem Sicherheitsschrank eingelagert werden darf; die Mengengrenze, ab der ein speziell ausgelegtes Gefahrstofflager benötigt wird und die Lagerklasse, um die gesetzeskonforme Zusammenlagerung mit anderen Stoffen nach TRGS 510 prüfen zu können. Beim Klick auf die jeweilige Information erhält der Nutzer weiterführende Hinweise zu allgemeinen Sicherheitsmaßnahmen und relevanten Gesetzesquellen.

www.denios.de ■

Portable Energie

Die Powerbanks Flex7 und Flex3 von Ledlenser versorgen mobile Geräte über den USB-A-Anschluss schnell mit frischer Energie. Im Gegensatz zu fest verbauten Akkus lassen sich die hochwertigen Li-Ion-Akkus vom Typ 18650 bequem wechseln und auch bei anderen Geräten verwenden. Die Powerbanks lassen sich bequem öffnen und dienen damit als stabile Aufbewahrungsbox für den sicheren Transport der Akkus. So sind auch unterwegs zwei Akkus zur Hand, die per Speed Charge mit bis zu zwei Ampere geladen werden. Das flammenhemmende Gehäuse ist IP65-zertifiziert, alle USB-Ports sind zudem wassergeschützt. Die Schutzplatine bewahrt die Energiespender vor Überspannung, Überladung, Kurzschluss oder Tiefenentladung. Dank der beiden unabhängigen LED-Anzeigen bleibt die Kapazität jederzeit im Blick. Wer unterwegs eine Reserve von zwei Akkus benötigt, erhält mit der Batterybox7 ein robustes Gehäuse für den sicheren Transport.

www.ledlenser.com ■

Upgrade für Umluftfilteraufsatz

Asecos bietet ein Upgrade-Set für Sensoren des Umluftfilteraufsatzes (UFA). Der UFA vermeidet zuverlässig eine gefährliche, explosionsfähige Atmosphäre in und um den Sicherheitsschrank herum und

bietet dauerhafte Flexibilität bei der Wahl des Aufstellorts. Um all diese Aufgaben sicher zu erfüllen, sind im UFA sensible Sensoren und eine leistungsfähige Überwachungselektronik verbaut. Diese wird durch die Dauerbelastung stark beansprucht und damit können die Messergebnisse nach Jahren unzuverlässig werden. Das Upgrade-Set beinhaltet: eine werksseitig kalibrierte Sensorik (Gassensor und Temperatursensor) zur weiterhin sicheren Filtersättigungsüberwachung, eine Universalelektronik mit erweitertem Funktionsumfang, zusätzlich als Upgrade gibt es einen energiesparenden Radialventilator der neuesten Generation und einen digitalen Differenzdruckwächter zur permanenten Luftstromüberwachung.

www.asecos.com ■

In Corona-Zeiten Desinfektionsmittel sicher lagern

Mit einem breit gefächerten Sortiment an kleinen und großen Gefahrstoffcontainern bietet die Marke Safe von Säbu geeignete Lager für jede Art von desinfizierenden Mitteln. Durch den Ausbruch der weltweiten Corona-Pandemie ist die regelmäßige Nutzung von Desinfektionsmitteln unerlässlich geworden und gehört zum festen Bestandteil unseres heutigen Alltags.

www.saebu.de ■

Absturzsicherung für Sandwichdächer ▲

ABS-Lock X-SW-6 heißt der Anschlagpunkt für Sandwichdächer von ABS Safety. Die aus Edelstahl gefertigte Anschlageinrichtung sichert bis zu drei Personen zeitgleich bei Arbeiten auf einem Sandwichdach. Die Besonderheit des Anschlagpunkts ist seine deutlich vereinfachte Montage: Die Absturzsicherungslösung ist in Varianten für verschiedene Sickenabstände verfügbar und wird mit geringem Aufwand komplett von oben verbaut. Sechs Schrauben genügen zur Montage der Grundplatte des Anschlagpunkts über zwei Sicken, direkt über den Holzbalken oder Z-Pfetten unter dem Sandwichblech. Die Schrauben werden durch Blech und Dämmschicht in die tragende Unterkonstruktion gesetzt. Selbstklebende Dichtungs-Patches verhindern, dass Wasser und Feuchtigkeit eindringen. Nach Montageabschluss ist die Anschlageinrichtung umgehend nutzbar, die Öse am Kopf dient der Befestigung der persönlichen Schutzausrüstung gegen Absturz (PSAgA).

www.absturzsicherung.de ■

Die Vorteile digitaler Videosysteme kommen bereits bei der Brandfrüherkennung zum Tragen: Gerade für große Firmengebäude, unübersichtliche Industriegelände oder kritische Produktionsumgebungen reichen klassische Rauchmelder meistens nicht aus. Sie lösen gegebenenfalls teure Fehlalarme aus oder reagieren im Ernstfall nur mit Zeitverzögerung. Deshalb bieten sich kamerabasierte Detektionssysteme an, die dank intelligenter Kombination ausgereifter Hard- und Software schon geringste Rauchentwicklungen automatisch und präzise erkennen sowie deutlich schneller als klassische Systeme alarmieren. Auch integrierbare, IP-basierte Thermalkamerasysteme, die bei ungewöhnlichen Temperaturanstiegen sofort Alarm schlagen, liefern hier zuverlässige Dienste auf technisch modernem Niveau. So ist die Belegschaft zuverlässig geschützt, Kosten durch Brandschäden oder Produktionsausfälle werden vermieden und im Ernstfall erforderliche Rettungseinsätze deutlich beschleunigt.

Prozessüberwachung mit Sicherheitsabstand

Gerade an Arbeitsplätzen mit hohem Gefährdungspotenzial, wie beispielsweise in der Stahlindustrie, ist es entscheidend, für einen zuverlässigen Personenschutz zu sorgen. Denn wenn Mitarbeiter Produktionsabläufe dank Videobeobachtung nicht aus nächster Nähe, sondern aus ausreichender Entfernung in der Leitstelle verfolgen und analysieren, sinkt das Risiko für Arbeitsunfälle deutlich. Deshalb empfiehlt es sich, im Zuge einer Anlagenmodernisierung auf digitale Lösungen

ARBEITSSICHERHEIT

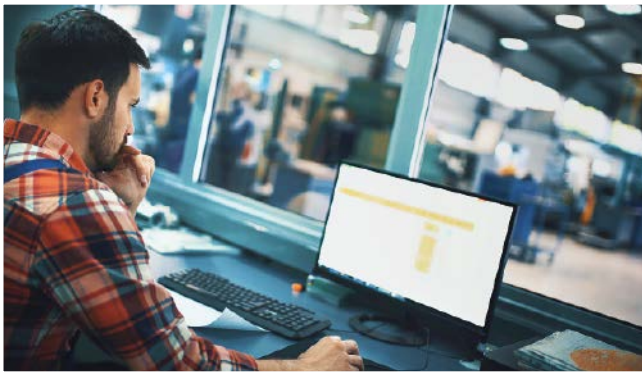
Adleraugen für den Arbeitsschutz

Sichere Arbeitsumgebung mit kamerabasierter Prozessbeobachtung

Um industrielle Fertigungsprozesse auch in extremen Umgebungen präzise zu verfolgen, kommen immer häufiger digitale, kamerabasierte Überwachungssysteme zum Einsatz. Diese Lösungen spielen ihre Stärken ebenfalls aus, wenn es um den Schutz der Mitarbeiter geht: Mit einer vernetzten, IP-basierten Videobeobachtung schaffen Industriebetriebe eine rundum sichere Arbeitsumgebung für ihre Belegschaft.

▲ Gerade an Arbeitsplätzen mit hohem Gefährdungspotenzial, wie beispielsweise in der Stahlindustrie, ist es entscheidend, für einen zuverlässigen Personenschutz zu sorgen

▲ Videoüberwachung dient der Prozessüberwachung – und dem Schutz der Mitarbeiter



▲ Analysefähige Kameras übernehmen bei Bedarf zusätzliche Aufgaben – etwa die Kontrolle der Einhaltung von Arbeitsschutzmaßnahmen über in die Leitstelle übertragene Live-Bilder

zu setzen, die dank hoch entwickelter Software und vernetzter Prozesse auf allen Ebenen für zusätzliche Sicherheit sorgen.

Beispielsweise kann in der Stahlproduktion am Hochofen das Abflussverhalten von Eisen und Schlacke an der Abstichbühne über thermografische oder visuelle Kameras exakt und ganz ungefährdet kontrolliert werden. Durch den Einsatz hochentwickelter Thermovision lassen sich zudem Maschinenfehlfunktionen und Materialermüdungen, die ein Mitarbeiter vor Ort noch gar nicht wahrnehmen könnte, frühzeitig erkennen und so Gefahrensituationen vermeiden. Zeitgleich erhöht die visuelle Prozessüberwachung auch die Produktivität der Anlage, da sie dank Software-gestützter Mess- und Auswertungsfunktionen Qualitätseinbußen und kostenintensive Stillstände verhindert.

Für höchste Arbeitssicherheit übernehmen die analysefähigen Kameras bei Bedarf zusätzliche Aufgaben: Beispielsweise erlauben sie die Kontrolle der Einhaltung von Arbeitsschutzmaßnahmen wie die Helmpflicht der Mitarbeiter durch in die Leitstelle übertragene Live-Bilder. Die Sicherung von Gefahrenzonen erfolgt zudem durch in die Kameras integrierte Bewegungsmelder, die bei Betreten eines zuvor definierten, kritischen Bereichs einen Alarm auslösen.

Daten- und Arbeitsschutz garantiert

Auch wenn bei diesen Überwachungsmaßnahmen der Personenschutz im Vordergrund steht, darf der Datenschutz nicht vernachlässigt werden: Jede Form der Videobeobachtung muss gesetzeskonform betrieben und installiert werden. So sind Kameras in öffentlich zugänglichen Bereichen wie Kundenparkplätzen zwar gestattet, müssen jedoch durch Hinweisschilder oder vergleichbare Maßnahmen kenntlich gemacht werden. Überwachungen am Arbeitsplatz dürfen nicht ohne Wissen der Mitarbeiter durchgeführt werden und erfordern entsprechende Betriebsvereinbarungen, die ein berechtigtes Interesse des Arbeitsgebers ausreichend begründen – selbst, wenn die Kameras ausschließlich der Prozessbeobachtung dienen sollen.

Innovative Videosysteme bieten hier sinnvolle technische Lösungen, um sowohl die Privatsphäre der Mitarbeiter als auch ihre Sicherheit zu gewährleisten. Werden Personen von Übersichtskameras erfasst, lassen sie sich dynamisch während einer Bewegung maskieren. Alternativ ist es möglich, mit Privatzonen zu arbeiten und festgelegte Bereiche dauerhaft auszublenden oder zu verpixeln. Auch mit Wärmebildkameras ist die Anonymisierung von Personen sichergestellt, da hier keinerlei Personendetails erkennbar sind.

Sicherheit von Belegschaft und Eigentum

Mit digitalen Lösungen für Video-Security und industrielle Prozessüberwachung können Unternehmen für höchste Arbeitssicherheit sorgen und zugleich kostenintensive Fehlfunktionen, Produktionsstillstände sowie Diebstahl oder Vandalismus verhindern. Hier ist es sinnvoll, die individuellen Anforderungen genau zu analysieren und in Zusammenarbeit mit einem Spezialisten für Videosicherheit ein passgenaues System zu entwickeln, das sich bei Bedarf auch in bestehende, analoge Anlagen integrieren lässt. Wenn die Sicherheitslösung sämtliche relevanten Prozesse automatisiert überwacht, dokumentiert und im Falle von Unregelmäßigkeiten zuverlässig Alarm schlägt, ist die Sicherheit von Belegschaft und Eigentum dauerhaft gewährleistet. ■

Autor
Dipl.-Ing. Thorsten Wulff
Geschäftsführer bei
Pieper

Kontakt

Pieper GmbH
Schwerte
Tel.: +49 2304 4701-0
info@pieper-video.de
www.pieper-video.de

Liebe Leserinnen und Leser,

In BusinessPartner, dem „Who is who in Sachen Sicherheit“, präsentieren sich Ihnen die kompetentesten Anbieter aus allen Sicherheitsbereichen. Die hier vertretenen Firmen legen Wert auf den Kontakt mit Ihnen.
Alle Einträge finden Sie auch in www.git-sicherheit.de/buyers-guide mit Links zu den Unternehmen!

Sie gehören selbst zu den wichtigen Anbietern und wollen mit jeder Ausgabe 30.000 Entscheider direkt erreichen? Dann kontaktieren Sie uns für eine Aufnahme.

BusinessPartner im Buyers Guide auf GIT-SICHERHEIT.de

SICHERHEITS MANAGEMENT

Sicherheitsmanagement

ABUS Security-Center GmbH & Co. KG
Linker Kreuthweg 5 · D-86444 Affing
Tel. +49(0)8207/95990-0
Fax +49(0)8207/95990-100
info.de@abus-sc.com · www.abus.com
ABUS Security-Center ist Hersteller innovativer Alarmanlagen, Videoüberwachungssysteme und Zutrittskontrollsysteme. Als Teil der ABUS Gruppe ist das Unternehmen sowohl auf branchenspezifische Sicherheitsbedürfnisse, als auch auf die Anforderungen von Privatanwendern spezialisiert.

Sicherheitsmanagement

Armantis GmbH
Seebachring 74
67125 Dannstadt
Tel.: +49 621 95 04 08 0
Mail: info@armantis.de
Web: armantis.de

Systemanbieter individueller Sicherheitskonzepte für Anforderungen im mittleren bis hohen Risikobereich:
SMAVID Videoüberwachungssysteme, Video-Sprechanlagen und Management-Software, zertifizierter Partner AxxonSoft.

Sicherheitsmanagement

ASSA ABLOY Sicherheitstechnik GmbH
Bildstockstraße. 20 · 72458 Albstadt
www.assaabloyopeningsolutions.de
albstadt@assaabloy.com
Das Unternehmen entwickelt, produziert und vertreibt unter den traditionsreichen und zukunftsweisenden Marken IKON, effeff, KESO und Yale hochwertige Produkte und vielseitige Systeme für den privaten, gewerblichen und öffentlichen Bereich.

Sicherheitsmanagement

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5 · 85630 Grasbrunn
Tel. 0800/7000444 · Fax 0800/7000888
Info.service@de.bosch.com
www.bosch-Sicherheitssysteme.de
Produkte und Systemlösungen für Videoüberwachungs-, Einbruchmelde-, Brandmelde-, Sprachalarm- und Managementsysteme sowie Zutrittskontrolle, professionelle Audio- und Konferenzsysteme. In ausgewählten Ländern bietet Bosch Lösungen und Dienstleistungen für Gebäudesicherheit, Energieeffizienz und Gebäudeautomation an.

Sicherheitsmanagement

Daitem / Atral-Secal GmbH
Eisleber Str. 4 · D-69469 Weinheim
Tel. +49(0)6201/6005-0 · Fax +49(0)6201/6005-15
info@daitem.de · www.daitem.de
www.brandwarnanlage.de
Funk-Einbruch- und Brandschutzlösungen vom Technologieführer. Vertrieb über qualifizierte Sicherheitsfacherrichter.

Sicherheitsmanagement

deister electronic GmbH
Hermann-Bahlsen-Str. 11
D-30890 Barsinghausen
Tel. +49(0)5105/516-111 · Fax +49(0)5105/516-217
info.de@deister.com · www.deister.com
Zutritts- und Zufahrtskontrollsysteme; biometrische Verifikation; Wächterkontrollsysteme; Verwahrung und Management von Schlüsseln und Wertgegenständen

Sicherheitsmanagement

EVVA Sicherheitstechnik GmbH
Höffgeshofweg 30 | 47807 Krefeld | Germany
T +49 2151 37 36-0 | F +49 2151 37 36-5635
office-krefeld@evva.com | www.evva.de

Föpplstraße 15 | 04347 Leipzig | Germany
T +49 341 234 090-5 | F +49 341 234 090-5760
office-leipzig@evva.com | www.evva.de

Mechanik, mechatronische & elektronische Schließsysteme, Zutrittskontrolle, Zusatzsicherungen und Türbeschläge

Sicherheitsmanagement

Funkwerk video systeme GmbH
Thomas-Mann-Str. 50 · D-90471 Nürnberg
Tel. +49(0)911/75884-0 · Fax +49(0)911/75884-100
info@funkwerk-vs.com · www.funkwerk.com
CCTV, Systemlösung, Systemintegration, Videoüberwachung, Security, Gebäudemanagement

Sicherheitsmanagement

Honeywell Security Group
Novar GmbH
Johannes-Mauthe-Straße 14 · 72458 Albstadt
Tel.: +49(0)74 31/8 01-0 · Fax: +49(0)74 31/8 01-12 20
www.honeywell.com/security/de
E-Mail: info.security.de@honeywell.com
Biometrie, Einbruchmelde-, Management-, Rettungsweg-, Video-, Zeiterfassungs- und Zutrittskontrollsysteme

Sicherheitsmanagement

NSC Sicherheitstechnik GmbH
Lange Wand 3 · 33719 Bielefeld
Tel.: +49 (0) 521/13629-0
Fax: +49 (0) 521/13629-29
info@nsc-sicherheit.de · www.nsc-sicherheit.de
Brandmeldetechnik, Videotechnik, Sprach-Alarm-Anlagen

ALARM MANAGEMENT

Alarmmanagement

Digisound Electronic GmbH
Oststraße 54 · 22844 Norderstedt
Tel. 040/526869-0 · Fax 040/526869-13
contact@digisound.de · www.digisound.de
Akustische Signalgeber, Piezoelektrische Sirenen, Elektronische Blitzlampen, Lautsprecher- und Transducer

Alarmmanagement

EPS Vertriebs GmbH
Lütke Feld 9 · 48329 Havixbeck
Tel.: 02507/98750-0 · Fax: 02507/98750-29
info@eps-vertrieb.de · www.eps-vertrieb.de
Brandschutz und sicherheitstechnische Produkte. Systemlieferant für Alarm, Brand und Video.

Alarmmanagement

TAS
Telefonbau Arthur Schwabe GmbH & Co. KG
Langmaar 25 · D-41238 Mönchengladbach
Tel. +49 (0) 2166 858 0 · Fax: +49 (0) 2166 858 150
info@tas.de · www.tas.de
Spezialist für Alarm-Übertragungstechnik und Alarmierungssysteme, Komplette Sicherheitslösungen für Industrie, Handel, Finanzdienstleister, Behörden und Tankstellen

GEBÄUDE SICHERHEIT

Gebäudesicherheit

GEZE

GEZE GmbH
Reinhold-Vöster-Str. 21-29 · D-71229 Leonberg
Tel. 07152/203-0 · Fax 07152/203-310
info.de@geze.com · www.geze.com
Flucht- und Rettungswegsysteme, Zutrittskontrollsysteme, RWA, Feststellanlagen

PERIMETER SCHUTZ

Gebäudesicherheit

WINKHAUS

Aug. Winkhaus GmbH & Co. KG
Hessenweg 9 · 48157 Münster
Tel. +49 251 4908-0 · Fax +49 251 4908-145
zutrittsorganisation@winkhaus.de
www.winkhaus.de
Zutrittsorganisation, elektronische und mechanische Schließsysteme, Tür- und Fenstertechnik, Notausgangs- und Anti-Panik-Verriegelungen

Gebäudesicherheit

Simons Voss technologies

SimonsVoss Technologies GmbH
Feringastr. 4 · D-85774 Unterföhring
Tel. +49(0)89/99228-180 · Fax +49(0)89/99228-222
marketing-simonsvoss@allegion.com
www.simons-voss.de
Digitale Schließ- und Zutrittskontrolle; intelligente Schließkomponenten und modernste Software. System 3060 Anlagen erfüllen auch hochkomplexe Anforderungen in großen Gebäuden, sind einfach und schnell erweiterbar und funktionieren konsequent kabellos.

Perimeterschutz

inova

Berlemann Torbau GmbH
Ulmenstraße 3 · 48485 Neuenkirchen
Tel.: +49 5973 9481-0 · Fax: +49 5973 9481-50
info@berlemann.de · www.berlemann.de
INOVA ist die Marke für alle Komponenten der Freigeländesicherung aus einer Hand! Als Qualitätshersteller für Schiebetore, Drehflügeltore, Zaun-, Zugangs- und Detektionssysteme haben Sie mit INOVA auf alle Fragen des Perimeterschutzes die passende Antwort.

Gebäudesicherheit

deister electronic

deister electronic GmbH
Hermann-Bahlsen-Str. 11
D-30890 Barsinghausen
Tel. +49(0)5105/516-111 · Fax +49(0)5105/516-217
info.de@deister.com · www.deister.com
Zutritts- und Zufahrtskontrollsysteme; biometrische Verifikation; Wächterkontrollsysteme; Verwahrung und Management von Schlüsseln und Wertgegenständen

Perimeterschutz

MAGOS
REINVENTING RADARS

MAGOS Europa
Hochstädter Str. 7c · 64342 Seeheim-Jugenheim
Tel. (49) 170-2648364
eric@magosys.com · www.magossystems.com
Radar, Perimeter Security, Perimetersicherheit, Perimeterschutz, Freilandüberwachung, AI, Objektklassifizierung

Gebäudesicherheit

DICTATOR

Dictator Technik GmbH
Gutenbergstr. 9 · 86356 Neusäß
Tel. 0821/24673-0 · Fax 0821/24673-90
info@dictator.de · www.dictator.de
Antriebstechnik, Sicherheitstechnik, Tür- und Tortechnik

Gebäudesicherheit

Südmetall

Süd-Metall Beschläge GmbH
Sägewerkstraße 5 · D – 83404 Ainring/Hammerau
Tel.: +49 (0) 8654 4675-50 · Fax: +49 (0) 8654 3672
info@suedmetall.com · www.suedmetall.com
Funk-Sicherheitsschlösser made in Germany, Mechanische & elektronische Schließsysteme mit Panikfunktion und Feuerschutzprüfung, Zutrittskontrollsysteme modular und individuell erweiterbar, Systemlösungen, Fluchttürsteuerung

Perimeterschutz

SENSTAR

Senstar GmbH
An der Bleicherei 15 · D-88214 Ravensburg
Tel +49 751 76 96 24-0
info@senstar.de · www.senstar.de
Freigeländeüberwachung, Zaunmeldesysteme, Bodendetektionssysteme, Alarmmanagementsysteme, Planungsunterstützung, Beratung, Inbetriebnahme, Service, Videomanagement- und Videoanalysesysteme, Zutrittskontrolle

Gebäudesicherheit

DOM

DOM Sicherheitstechnik GmbH & Co. KG
Wesselinger Straße 10-16 · D-50321 Brühl / Köln
Tel.: + 49 2232 704-0 · Fax + 49 2232 704-375
dom@dom-group.eu · www.dom-security.com
Mechanische und digitale Schließsysteme

Gebäudesicherheit

U&Z Uhlmann & Zacher

Uhlmann & Zacher GmbH
Gutenbergstraße 2-4 · 97297 Waldbüttelbrunn
Tel.: +49(0)931/40672-0 · Fax: +49(0)931/40672-99
contact@UundZ.de · www.UundZ.de
Elektronische Schließsysteme, modular aufgebaut und individuell erweiterbar

VIDEO ÜBERWACHUNG

Gebäudesicherheit

EFAFLEX
schnelle und sichere Tore

EFAFLEX Tor- und Sicherheitssysteme
GmbH & Co. KG
Fliederstraße 14 · 84079 Bruckberg
Tel. 08765 82-0 · Fax 08765 82-200
info@efaflex.com · www.efaflex.com
Schnelllauftore, Rolltore, Falttore, Industrietore, Hallentore, Sicherheitstore.

Gebäudesicherheit

wurster
Ideen in Blech

Walter Wurster GmbH
Heckenrosenstraße 38-40
70771 Leinfelden-Echterdingen
Tel.: 0711/949 62-0 · kontakt@wurster-online.de
www.wurster-online.de · www.ideeninblech.de
Geldübergabeschalter feuerbeständig bis F90 und beschusshemmend bis FB7, Durchreichen für Geld, Wertsachen und Dokumente, Hochsicherheits-Durchreichen, Bankschalter, Nachtschalter, Tankstellenschalter, Apothekenschalter, Ticketschalter für Sport- und Kulturstätten

Videoüberwachung

TKH GROUP

AASSET security
TKH SECURITY SOLUTIONS

AASSET Security GmbH
TKH Security Solutions
Max-Planck-Straße 15 a-c | D-40699 Erkrath
Tel.: +49 211 247016-0 | Fax: +49 211 247016-11
info@aasset.de | www.aasset.de
Videoüberwachung, Zutrittskontrolle, Sicherheitsmanagement, mobile Videoüberwachung und Videomanagement

Videoüberwachung

AUS GUTEM GRUND GRUNDIG

Abetechs GmbH (Grundig Security)
Steinhof 39 · D-40699 Erkrath
Tel: +49 211 5380 6832
info@grundig-security.com · www.grundig-security.com
Das neue Programm von GRUNDIG Security enthält alles, was Sie für eine moderne und professionelle Videoüberwachungsanlage benötigen.

Videoüberwachung

DEKOM VIDEO SECURITY & NETWORK GMBH

Ihr zuverlässiger Partner für professionelle Videoüberwachung

DEKOM Video Security & Network GmbH
Hoheluftchaussee 108 • 20253 Hamburg
Tel. +49 (0) 40 47 11 213-0 • info@dekom-security.de
Member of Dallmeier
www.dekom-security.de • www.dekom-security.at

Videoüberwachung

HIKVISION

HIKVISION Deutschland GmbH
Flughafenstr. 21 · D-63263 Neu-Isenburg
Tel. +49 (0) 69/40150 7290
sales.dach@hikvision.com · www.hikvision.com/de
Datenschutzkonforme Videoüberwachung, Panorama-Kameras, Wärmebild-Kameras, PKW-Kennzeichenerkennung

Videoüberwachung

ABUS Security Tech Germany

ABUS Security-Center GmbH & Co. KG
Linker Kreuthweg 5 · D-86444 Affing
Tel. +49(0)8207/95990-0
Fax +49(0)8207/95990-100
info.de@abus-sc.com · www.abus.com
ABUS Security-Center ist Hersteller innovativer Alarmanlagen, Videoüberwachungssysteme und Zutrittskontrollsysteme. Als Teil der ABUS Gruppe ist das Unternehmen sowohl auf branchenspezifische Sicherheitsbedürfnisse, als auch auf die Anforderungen von Privatanwendern spezialisiert.

Videoüberwachung

digivod®

digivod gmbh
Breite Straße 10, 40670 Meerbusch
Tel. +49 21 59/52 00–0 · Fax. +49 21 59/52 00–52
info@digivod.de · www.digivod.de
Videomanagement Software der Königsklasse. Flexibel für jeden Bedarf. Komplettsysteme und attraktive Bundle-Angebote. Lokaler Support!

Videoüberwachung

lunaHD
High Definition Video
www.luna-hd.de

Videoüberwachung

AXIS COMMUNICATIONS

Axis Communications GmbH
Adalperostraße 86 · 85737 Ismaning
Tel. +49 (0)89/35 88 17 0 · Fax +49 (0)89/35 88 17 269
info-de@axis.com · www.axis.com
Netzwerk-Sicherheitslösungen:
Axis ist Technologieführer im Bereich Netzwerk-Video und bietet intelligente Sicherheitslösungen.

Videoüberwachung

EIZO

EIZO Europe GmbH
Helmut-Grashoff-Str. 18
41179 Mönchengladbach
Tel.: +49 2161 8210 0
info@eizo.de · www.eizo.de/sicherheit
Professionelle Monitore für den 24/7-Einsatz in der Videoüberwachung, IP-Decoder-Lösungen für den computerlosen Anschluss an IP-Kameras.

Videoüberwachung

MOBOTIX
BeyondHumanVision

MOBOTIX AG
Security-Vision-Systems
Kaiserstraße · D-67722 Langmeil
Tel. +49 (0) 6302/9816-0 · Fax +49 (0) 6302/9816-190
info@mobotix.com · www.mobotix.com
Beyond Human Vision „Made in Germany":
MOBOTIX ist Vorreiter auf dem Markt für Videosicherheit

Videoüberwachung

BALTER STAY AHEAD

Balter GmbH
Elisabeth-Selbert-Str. 19 · D-40764 Langenfeld
Tel.: +49(0)211-22975915 · Fax: +49(0)211-22975927
info@balter.de · www.balter.de
Hersteller und Distributor von hochwertigen IP- und Analog HD-Videoüberwachungssystemen, Video-Türsprechanlagen, Alarmanlagen und Smart Home Systemen.

Videoüberwachung

eps®
Weil jede Sekunde zählt.

EPS Vertriebs GmbH
Lütke Feld 9 · 48329 Havixbeck
Tel.: 02507/98750-0 · Fax: 02507/98750-29
info@eps-vertrieb.de · www.eps-vertrieb.de
Brandschutz und sicherheitstechnische Produkte. Systemlieferant für Alarm, Brand und Video.

Videoüberwachung

MORPHEAN

Morphean SA – Headquarter
Rte du Château 112
1763 Granges-Paccot · Switzerland
Tel. +41 26 422 00 90
info@morphean.ch · www.morphean.com
Video Surveillance as a Service (VSaaS) und Access Control as a Service (ACaaS) – Videoüberwachung und Zugangskontrolle mit KI und Cloud.

Videoüberwachung

a)hua TECHNOLOGY

Dahua Technology GmbH
Monschauer Straße 1 · 40549 Düsseldorf
Tel: +49 1514 0418815
sales.de@global.dahuatech.com
www.dahuasecurity.com/de
IP-Produkte, HDCVI Produkte, Intelligente Gebäude, Machine Vision, Übertragungen & Display

Videoüberwachung

Hanwha Techwin Europe Limited
Kölner Strasse 10
65760 Eschborn
Tel: +49 (0)6196 7700 490
hte.dach@hanwha.com · www.hanwha-security.eu/de
Hanwha Techwin Europe
Hersteller von Videoüberwachungsprodukten wie Kameras, Videorekorder und weiteren IP-Netzwerkgeräten. Sowie Anbieter von Software-Lösungen wie beispielsweise Videoanalyse, Lösungen für den Vertical-Market und Videomanagementsoftware (VMS).

Videoüberwachung

Panasonic BUSINESS

Panasonic Deutschland
Winsbergring 15 · 22525 Hamburg · Deutschland
www.panasonic.business.com/sicherheitslosungen
info@panasonic.business.de
Hochwertige CCTV-Lösungen (IP & analog), Video-Automatisierung und KI, Technologien für hohe Ansprüche (FacePro, Personen-Maskierung), Schutz vor Cyber-Attacken im Einklang mit DSGVO, VMS: Video Insight

Videoüberwachung

Dallmeier

Dallmeier electronic GmbH & Co. KG
Bahnhofstraße 16 · 93047 Regensburg
Tel. 0941/8700-0 · Fax 0941/8700-180
info@dallmeier.com · www.dallmeier.com
Videosicherheitstechnik made in Germany: Multifocal-Sensortechnologie Panomera®, IP-Kameras, Aufzeichnungsserver, intelligente Videoanalyse, Videomanagementsoftware

Videoüberwachung

PHIHONG

HN-Power

HN Electronic Components GmbH & Co. KG
Birkenweiherstr. 16 · 63505 Langenselbold
Tel.: +49 6184 92780 · Fax: +49 6184 62316
info@hn-electronic.de · www.hn-electronic.de
Ihr Spezialist für PoE von 16W-800W mit neuestem BT Standard. Topmodelle i.d.R auf Lager.

Videoüberwachung

Qognify

Qognify GmbH
Werner-von-Siemens-Str. 2–6 · 76646 Bruchsal
Tel. +49 (0) 7251 9290-0 · Fax +49 (0) 7251/9290-815
Info.emea@qognify.com · www.qognify.com
Führender Anbieter von Video und Incident Management Software; Software-Lösungen für Sicherheitsanwendungen; zusätzliche branchenspezifische Lösungen in Bereichen Transport & Logistik, Handel, Finanzen sowie kritische Infrastruktur & Städte; basierend auf dem Systemkonzept der Multi Solution Platform, Erweiterungsmöglichkeiten und Schnittstellen zu Drittsystemen.

Videoüberwachung

SANTEC BW AG
An der Strusbek 31 ▪ 22926 Ahrensburg ▪ Germany
Tel. +49 4102 4798 0 ▪ Fax +49 4102 4798 10
santec_info@burg.biz ▪ www.santec-video.com
Videoüberwachung ▪ Netzwerktechnik
IR-Freilandsensorik ▪ Dienstleistungen

Zeit + Zutritt

deister electronic GmbH
Hermann-Bahlsen-Str. 11
D-30890 Barsinghausen
Tel. +49(0)5105/516-111 · Fax +49(0)5105/516-217
info.de@deister.com · www.deister.com
Zutritts- und Zufahrtskontrollsysteme; biometrische Verifikation; Wächterkontrollsysteme; Verwahrung und Management von Schlüsseln und Wertgegenständen

Zeit + Zutritt

Morphean SA – Headquarter
Rte du Château 112
1763 Granges-Paccot · Switzerland
Tel. +41 26 422 00 90
info@morphean.ch · www.morphean.com
Video Surveillance as a Service (VSaaS) und Access Control as a Service (ACaaS) – Videoüberwachung und Zugangskontrolle mit KI und Cloud.

Videoüberwachung

Securiton GmbH
IPS Intelligent Video Analytics
Kronstadter Str. 4 · 81677 München
Tel. +49 (0)89 4626168-0 · Fax +49 (0)89 46261688
info@ips-analytics.com · www.ips-analytics.com
Hersteller von high-end Videomanagementsoftware und intelligenter Videoanalysesoftware zur Echtzeiterkennung von potentiellen Gefahrensituationen.

Zeit + Zutritt

ELATEC GmbH
Zeppelinstr. 1 · 82178 Puchheim
Tel.: +49 89 552 9961 0
info-rfid@elatec.com · www.elatec.com
Entwickler und Hersteller für zukunftssichere RFID Reader. Flexible Module für spezifische Lösungen (LF, HF, NFC, BLE). Unterstützt mehr als 60 Technologien und ist in über 100+ Ländern zertifiziert.

Zeit + Zutritt

PCS Systemtechnik GmbH
Pfälzer-Wald-Straße 36 · 81539 München
Tel. 089/68004-550 · Fax 089/68004-555
intus@pcs.com · www.pcs.com
Zeiterfassung, Zutrittskontrolle, BDE/MDE, Biometrie, Video, SAP, Handvenenerkennung

ZEIT ZUTRITT

Zeit + Zutritt

FEIG ELECTRONIC GMBH
Lange Straße 4 · 35781 Weilburg
Tel. 06471/3109-0 · Fax 06471/3109-99
obid@feig.de · www.feig.de
Elektronische Schließsysteme, Güteridentifizierung Zutritts-und Zufahrtskontrolle

Zeit + Zutritt

phg Peter Hengstler GmbH + Co. KG
Dauchinger Str. 12 · D-78652 Deißlingen
Tel. +49(0)7420/89-0 · Fax +49(0)7420/89-59
datentechnik@phg.de · www.phg.de
RFID-Komponenten für Zutrittskontrolle, Zeiterfassung, BDE, Kantinendaten, Freizeitapplikationen, Aufputzgeräte, Einbaumodule, Biometrie, Identifikationsmedien und Zubehör

Zeit + Zutritt

AceProx Identifikationssysteme GmbH
Bahnhofstr. 73 · 31691 Helpsen
Tel: +49(0)5724-98360
info@aceprox.de · www.aceprox.de
RFID-Leser für Zeiterfassung, Zutrittskontrolle und Identifikation

Zeit + Zutritt

GANTNER Electronic GmbH
Bundesstraße 12 · 6714 Nüziders · Österreich
Tel. +43 5552 33944
info@gantner.com · www.gantner.com
Systemlösungen in Zutrittskontrolle/Biometrie, Zeiterfassung, Betriebsdatenerfassung, Schließsysteme, Zugriffsschutz, Schrankschließsysteme

Zeit + Zutritt

primion Technology GmbH
Steinbeisstraße 2-4 · 72510 Stetten a.K.M.
Tel. 07573/952-0 · Fax 07573/92034
info@primion.de · www.primion.de
Arbeitszeitmanagement, Zugangsmanagement, Personaleinsatzplanung, grafisches Alarmmanagement, SAP-Kommunikationslösungen, Ausweiserstellung, Biometrie

Zeit + Zutritt

AZS System AG
Mühlendamm 84 a · 22087 Hamburg
Tel. 040/226611 · Fax 040/2276753
www.azs.de · anfrage@azs.de
Hard- und Softwarelösungen zu Biometrie, Schließ-, Video-, Zeiterfassungs- und Zutrittskontrollsysteme, Fluchtwegsicherung, Vereinzelungs- und Schrankenanlagen, OPC-Server

Zeit + Zutritt

IntraKey technologies AG
Wiener Str. 114-116 · 01219 Dresden
Tel. 0351/31558-0 · Fax 0351/31558-129
info@intrakey.de · www.intrakey.de
Zutrittskontrolle, Zeiterfassung, Raumvergabe, Elektronische Schließfächer, Fuhrparkmanagement, Bezahlen, BikeParkBox

Zeit + Zutritt

SALTO Systems GmbH
Schwelmer Str. 245 · 42389 Wuppertal
Tel.: +49 202 769579-0 · Fax: +49 202 769579-99
info.de@saltosystems.com · www.saltosystems.de
Vielseitige und maßgeschneiderte Zutrittslösungen - online, offline, funkvernetzt, Cloud-basiert und mobil.

Zeit + Zutritt

Cichon+Stolberg GmbH
Wankelstraße 47-49 · 50996 Köln
Tel. 02236/397-200 · Fax 02236/61144
info@cryptin.de · www.cryptin.de
Betriebsdatenerfassung, Zeiterfassung, cryptologisch verschlüsselte Zutrittskontrolle

Zeit + Zutritt

ISGUS GmbH
Oberdorfstr. 18–22
78054 Villingen-Schwenningen
Tel. 07720/393-0 · 07720/393-184
info@isgus.de · www.isgus.de
Betriebsdatenerfassung, Personaleinsatzplanung, Zeiterfassung, Zutrittskontrolle

Zeit + Zutritt

Senstar GmbH
An der Bleicherei 15 · D-88214 Ravensburg
Tel +49 751 76 96 24-0
info@senstar.de · www.senstar.de
Freigeländeüberwachung, Zaunmeldesysteme, Bodendetektionssysteme, Alarmmanagementsysteme, Planungsunterstützung, Beratung, Inbetriebnahme, Service, Videomanagement- und Videoanalysesysteme, Zutrittskontrolle

NOTRUF SERVICE LEITSTELLE

Notruf- und Service-Leitstelle

HWS

HWS Wachdienst Hobeling GmbH
Am Sportpark 75 · D-58097 Hagen
Tel. (0 23 31) 47 30 -0 · Fax -130
hobeling@hobeling.com · www.hws-wachdienst.de
VdS-Notruf- und Service-Leitstelle, Alarmempfangsstelle DIN EN 50518, Alarmprovider, Mobile Einsatz- und Interventionskräfte, Objekt- und Werkschutz

Notruf- und Service-Leitstelle

FSO Fernwirk-Sicherheitssysteme Oldenburg GmbH
Am Patentbusch 6a · 26125 Oldenburg
Tel: 0441-69066 · info@fso.de · www.fso.de
Alarmempfangsstelle nach DIN EN 50518
Alarmprovider und Notruf- und Service Leitstelle nach VdS 3138, zertifiziertes Unternehmen für die Störungsannahme in der Energieversorgung.

BRAND SCHUTZ

Brandschutz

EPS Vertriebs GmbH
Lütke Feld 9 · 48329 Havixbeck
Tel.: 02507/98750-0 · Fax: 02507/98750-29
info@eps-vertrieb.de · www.eps-vertrieb.de
Brandschutz und sicherheitstechnische Produkte.
Systemlieferant für Alarm, Brand und Video.

Brandschutz

Novar GmbH a Honeywell Company

Dieselstraße 2 · D-41469 Neuss
Tel.: +49(0)2131/40615-600
FAX: +49(0)2131/40615-606
info@esser-systems.com · www.esser-systems.com
Brandmeldesysteme, Sprachalarmierung, Notbeleuchtung, Sicherheitsmanagement

Brandschutz

HEKATRON Brandschutz

Hekatron Vertriebs GmbH
Brühlmatten 9 · 79295 Sulzburg
Tel. 07634/500-0 · Fax 07634/6419
info@hekatron.de · www.hekatron.de
Brandmeldesysteme, Rauchschaltanlagen, Rauchwarnmelder, Sicherheitsleitsysteme

Brandschutz

Labor Strauss Gruppe
Firmensitz: Wiegelestraße 36 · A-1230 Wien
Tel.: +43 1 521 14-0
office@lst.at · www.laborstrauss.com
Standorte: Wien, Graz, Innsbruck, Pockau-Lengefeld, Mönchengladbach, Hamburg
Die Spezialisten für Brandmeldeanlagen und Löschsteuersysteme

Brandschutz

Prymos GmbH
Siemensstraße 18 · 63225 Langen
Tel. 06103/4409430 · Fax 06103/4409439
info@prymos.com · www.prymos.com
ASR A2.2 kompatible Feuerlöscher-Sprays.
Bis zu 10 Jahre wartungsfreie DIN EN 3 Feuerlöscher.

Brandschutz

STANLEY Security Deutschland GmbH
Haupstr. 40 a · 82229 Seefeld
Tel. +49(0)8152/9913-0 · Fax +49(0)8152/9913-20
info@setec-security.de · www.setec-security.de
Handfeuermelder, Lineare Wärmemelder, Feuerwehr Schlüsseldepots, Feuerwehr Schlüsselmanager, Feuerwehrperipherie, Feststellanlagen, Störmeldezentralen

GASMESS TECHNIK

Gasmesstechnik

GfG Gesellschaft für Gerätebau mbH
Klönnestraße 99 · D-44143 Dortmund
Tel. +49 (0)231/ 564000 · Fax +49 (0)231/ 516313
info@gfg-mbh.com · www.gasmessung.de
Gaswarntechnik, Sensoren, tragbare und stationäre Gasmesstechnik

ARBEITS SICHERHEIT

Arbeitssicherheit

GÜNZBURGER STEIGTECHNIK

GÜNZBURGER STEIGTECHNIK GMBH
Rudolf-Diesel-Straße 23 · D-89312 Günzburg
Tel. +49 (0) 8221/3616-01 · Fax +49 (0) 8221/3616-80
info@steigtechnik.de · www.steigtechnik.de
Das Sortiment der Günzburger Steigtechnik umfasst Leitern für den gewerblichen, öffentlichen und privaten Gebrauch, Rollgerüste, Podeste, Überstiege, Rettungstechnik sowie maßgefertigte Sonderkonstruktionen – alles „Made in Germany" mit 15 Jahren Qualitätsgarantie.

MASCHINEN ANLAGEN SICHERHEIT

Maschinen + Anlagen

EUCHNER
More than safety.

EUCHNER GmbH + Co. KG
Kohlhammerstraße 16
D-70771 Leinfelden-Echterdingen
Tel. 0711/7597-0 · Fax 0711/753316
www.euchner.de · info@euchner.de
Automation, MenschMaschine, Sicherheit

Maschinen + Anlagen

SCHMERSAL
THE DNA OF SAFETY

K.A. Schmersal GmbH & Co. KG
Möddinghofe 30 · 42279 Wuppertal
Tel. 0202/6474-0 · Fax: 0202/6474-100
info@schmersal.com · www.schmersal.com
Sicherheitsschalter mit Personenschutzfunktion, Berührungslos wirkende Sicherheitsschalter, Sicherheitszuhaltungen, Sicherheits-Compact-Steuerung PROTECT SRB, Positionsschalter

Maschinen + Anlagen

Leuze electronic
the sensor people

Leuze electronic GmbH & Co. KG
In der Braike 1 · D-73277 Owen
Tel. +49(0)7021/573-0 · Fax +49(0)7021/573-199
info@leuze.de · www.leuze.com
Optoelektronische Sensoren, Identifikations- und Datenübertragungssysteme, Distanzmessung, Sicherheits-Sensoren, Sicherheits-Systeme, Sicherheits-Dienstleistungen

Maschinen + Anlagen

PEPPERL+FUCHS

Pepperl+Fuchs AG
Lilienthalstraße 200 · 68307 Mannheim
Tel. 0621/776-1111 · Fax 0621/776-27-1111
fa-info@de.pepperl-fuchs.com
www.pepperl-fuchs.com
Sicherheits-Sensoren, Induktive-, Kapazitive-, Optoelektronische und Ultraschall-Sensoren, Vision-Sensoren, Ident-Systeme, Interface-Bausteine

GEFAHRSTOFF MANAGEMENT

UNTER BRECHUNGSFREIE STROMVERSORGUNG

Maschinen + Anlagen

SSP Safety System Products

SSP Safety System Products GmbH & Co. KG
Max-Planck-Straße 21 · DE-78549 Spaichingen
Tel.: +49 7424 980 490 · Fax: +49 7424 98049 99
info@ssp.de.com · www.safety-products.de
Dienstleistungen & Produkte rund um die Maschinensicherheit: Risikobeurteilung, Sicherheitssensoren, -Lichtvorhänge, - Zuhaltungen, -Steuerungen sowie Schutzumhausungen, Zustimmtaster uvm.

Gefahrstoffmanagement

asecos

asecos GmbH
Sicherheit und Umweltschutz
Weiherfeldsiedlung 16–18 · 63584 Gründau
Tel. +49 6051 9220-0 · Fax +49 6051 9220-10
info@asecos.com · www.asecos.com
Gefahrstofflagerung, Umwelt- und Arbeitsschutz, Sicherheitsschränke, Chemikalien- und Umluftschränke, Druckgasflaschenschränke, Gefahrstoffarbeitsplätze, Absauganlagen, Raumluftreiniger uvm.

Unterbrechungsfreie Stromversorgung

NSGate

NSGate
2F, No.53-16, Shcherbakovskaya Straße
105187 Moskau, Russland
Tel.: +7 495 139 6903
www.nsgate.eu · sales@nsgate.com
DC-USVs 150-500VA, off-grid solar systems und hochwertige Produkte für Videoüberwachungssysteme im Außenbereich. Mikroklima-Komponenten für Außengehäuse: Heizgerät, Kühlen, Thermostate. Industrielle PoE-Switches, Ethernet-Extenders und Überspannungsschutzgeräte.

Maschinen + Anlagen

.steute

steute Schaltgeräte GmbH & Co. KG
Brückenstr. 91 · 32584 Löhne
Tel. 05731/745-0 · Fax 05731/745-200
info@steute.de · www.steute.de
Hersteller von Sicherheits-, Sicherheits-Scharnier-, Seilzug-Notschaltern, Schaltgeräten mit Funktechnologie, Fuß-, Positions-, Bandschieflauf/Schlaffseil- & Türgriffschaltern, Magnetsendoren, Ex-Schaltgeräten & Stelleinrichtungen für die Medizintechnik

Gefahrstoffmanagement

BAUER SÜDLOHN

BAUER GmbH
Eichendorffstraße 62 · 46354 Südlohn
Tel.: + 49 (0)2862 709-0 · Fax: + 49 (0)2862 709-156
info@bauer-suedlohn.de · www.bauer-suedlohn.de
Auffangwannen, Brandschutz-Container, Fassregale, Gefahrstofflagerung, Regalcontainer, Wärmekammern, individuelle Konstruktionen

Unterbrechungsfreie Stromversorgung

SLAT for safer buildings

SLAT GmbH
Leitzstraße 45 · 70469 Stuttgart
Tel.: 0711 89989 008 · Fax: 0711 89989 090
www.slat.com · info@slat-gmbh.de
DC-USVs nach DIN EN 54-4/A2 + DIN EN 12 101-10 (BMT, SAA, ELA), nach DIN EN 50131-6/3 + VdS 2115 (ZKT, EMT)
DC-Mikro-USVs m. integr. Li-Backup: Video, Zutritt, Übertragungs- u. Netzwerktechnik, Gebäudeleittechnik, Smart Metering, Medizin. Systeme, In- u. Outdoorbereich.

Gefahrstoffmanagement

SÄBU BAUEN MIT SYSTEM

SÄBU Morsbach GmbH
Zum Systembau 1 · 51597 Morsbach
Tel. 02294 694-23 · Fax 02294 694-38
safe@saebu.de · www.saebu.de
Gefahrstofflagerung, Arbeits- + Umweltschutz, Auffangwannen, Fassregale, Regalcontainer, Brandschutz- Schränke + Container, Gasflaschenlagerung

DIE VIP COUCH

Tomislav „Milo“ Milovanovic

Director Corporate Security, Head of Security Operations bei Adidas AG

- Rufname „Milo“
- Jahrgang 1981
- Politikwissenschaftler mit Fokus auf der Entwicklung des Themenbereichs „Sicherheit“ zu einer wissenschaftlichen Disziplin
- 2002–2011: Staatsdienst im In- und Ausland (diverse Standorte)
- 2011–2017: Continental AG (Hannover)
- Seit 2017: Adidas AG (Herzogenaurach)

Menschen machen Märkte
In jeder Ausgabe Ihrer GIT SICHERHEIT bitten wir wichtige Personen, Entscheider, Menschen aus der Sicherheitsbranche, auf unserer VIP-Couch Platz zu nehmen.

Ihr Berufswunsch mit 20 war:
Berufsboxer

Was hat Sie dazu bewogen, eine Aufgabe im Bereich Sicherheit zu übernehmen?
Die 9/11-Anschläge spielten eine große Rolle für mich, eine Tätigkeit bei nationalen und später auch internationalen Sicherheitsbehörden anzustreben. Ferner habe ich einen ausgeprägten Sinn dafür, stets Hilfe leisten zu wollen, und denjenigen Schutz zu bieten, die sich nicht selbst schützen können.

Welche sicherheitspolitische Entscheidung oder welches Projekt sollte Ihrer Meinung nach schon längst umgesetzt sein?
Eine „echte“ gemeinsame EU-Sicherheits- und Außenpolitik – mit den jüngsten Entwicklungen rund um den Brexit oder den griechisch-türkischen Konflikt im Mittelmeer sehe ich hierfür momentan leider noch schwarz.

Ein Erfolg, den Sie kürzlich errungen haben, war:
Die Fertigstellung meiner Dissertation.

Welche Reform bewundern Sie am meisten?
Jegliche Gesellschaftsreform weg von einem Zustand der Ungerechtigkeit hin zu einer gerechteren Form des gesellschaftlichen Zusammenlebens.

Wer hat Ihrer Meinung nach eine Auszeichnung verdient?
Ich würde unseren Planeten auszeichnen – für die Widerstandskraft, die er an den Tag legt. Trotz all der Dinge, die wir Menschen ihm antun, bietet er uns eine Umwelt, die Tag für Tag unser Überleben sichert.

Worüber können Sie sich freuen?
Ein einfaches „Grüß Gott“ auf der Straße von einer unbekannten Person (im Idealfall zusammen mit einem Lächeln) und die damit verbundene Hoffnung, dass wir noch nicht völlig anonymisiert durch die Welt schreiten.

Wobei entspannen Sie?
Es mag sich widersprüchlich lesen, aber tatsächlich beim Kampfsport – Sparring. Covid-19-bedingt war dies in der Vergangenheit nicht oft möglich, daher zitiere ich den Schauspieler Ron Perlman: „Some people meditate, I smoke cigars“.

Welchen Urlaubsort können Sie empfehlen?
Ich denke, es kommt weniger auf den Ort an und mehr auf die Gesellschaft, in die man sich begibt;…aber wenn ich mich festlegen müsste, würde ich als Stadt absolut die serbische Hauptstadt Belgrad empfehlen und als Land Israel.

Wie würde ein guter Freund Sie charakterisieren?
Meinungsstark und selbstbewusst, aber stets bedingungslos loyal.

Welche Zeitschriften lesen Sie regelmäßig?
Der Spiegel, das Manager Magazin und natürlich liegt die GIT SICHERHEIT auch regelmäßig auf meinem Schreibtisch.

Welche Musik hören Sie am liebsten?
Stimmungs- und situationsabhängig, aber von klassischer Musik über klassischen Rock bis hin zu Old-School Hip-Hop ist alles dabei. Nicht zu vergessen: auch Musik aus meiner Heimat Serbien (…oft zum Leidwesen meiner nicht-serbischen Umwelt).

Was motiviert Sie?
Menschen, die ihren Beruf als Berufung verstehen und andere Menschen inspirieren können, sowie klassische Underdog-Erfolgsgeschichten im Sport, in der Politik und im Leben allgemein.

Die beste Erfindung im Bereich Sicherheit ist Ihrer Meinung nach:
Die Notrufnummer, egal ob 110, 112 oder eine unternehmenseigene Rufnummer.

Ihre gegenwärtige Geistesverfassung ist:
Meine aktuelle Selbstdiagnose: ruhig und stabil.

S74

Videosystem

Dezent im Einsatz – herausragend im Nutzen

MOBOTIX

BeyondHumanVision

WILEY

Wiley Industry Days

WIN DAYS

16.–19. November 2020

VIRTUELLE SHOW mit Konferenz, Ausstellung und Networking für die Branchen der Automatisierung, Machine Vision und Sicherheit.

Besuchen Sie unsere Aussteller und Partner auf dem virtuellen Branchentreff

VIRTUAL SHOW with conference, exhibition and networking for the automation, machine vision and safety & security industries.

Visit our exhibitors and partners at the virtual industry show

JETZT REGISTRIEREN
REGISTER NOW

www.WileyIndustryDays.com

GRUNDIG advancis neovo FORSCHUNGS CAMPUS ASSA ABLOY BALLUFF B&R CES deister electronic

Edmund optics worldwide emva Europa-Universität Flensburg EVVA Fraunhofer VISION Genetec GEUTEBRÜCK GEZE gom

HIKVISION igus IPS Intelligent Video Analytics milestone MOBOTIX optris pcs Polytec Qognify R3

Simons Voss technologies ICC spectronet TURCK UBiMAX VDMA VIDEOR visionLib WAGNER wanzl Z-LASER ZVEI

messtec drives Automation inspect inspect award 2021 GIT SICHERHEIT + MANAGEMENT GIT SICHERHEIT AWARD GIT SECURITY EMEA GIT SECURITY AWARD