

WILEY

30. JAHRGANG
JAN./FEB. 2021

1-2

GIT

MAGAZIN FÜR SAFETY & SECURITY
SICHERHEIT
+ MANAGEMENT

Wiley Industry Days
WIN DAYS
7.-9. Juni 2021
Jetzt kostenfrei registrieren:
www.WileyIndustryDays.com

VIRTUELLE MESSE

Wiley Industry Days s. 10

CORONA-PANDEMIE

Anja Opitz zur Logik von Pandemien – und dem klugen Umgang mit ihnen s. 14

KONZERNSICHERHEIT

Mit Sicherheits-Chef Enno Münster im Gespräch s. 18

SICHERHEITSDIENSTLEISTUNG

Das neue Gesetz – die Positionen von BVSU und BDSU s. 22/24

INTERNET OF THINGS

Bosch-CEOs Tanja Rückert und Hartmut Schaper über offene Plattformen s. 26

SENSOREN

Scanner zum Überwachen von Automattüren s. 74



VIP: Arno Weber s. 98



Titelthema Seite 46:

ÜMANAGEMENT 2.0
SÜDMETALL-SCHLÖSSER FÜR GEBÄUDE JEDER GRÖSSE

Mit Heft im Heft ab S. 37



WILEY

MEHR SICHERHEIT WENIGER KOSTEN



iLOQ - die batterielose, digitale, mobile Zugangslösung

Bringen Sie die Sicherheit Ihrer Immobilien mit dem einzigartigen digitalen Schließsystem von iLOQ auf den neuesten Stand der Technik. Mit einer skalierbaren Zugangslösung, die von einer intelligenten, benutzerfreundlichen Software-Plattform aus verwaltet wird.

Die iLOQ 5-Serie erhöht die Sicherheit und Nachhaltigkeit Ihrer Einrichtungen, reduziert den Verwaltungsaufwand, senkt die Betriebskosten und steigert den Wert Ihrer Immobilien.



Erfahren Sie mehr über iLOQ unter
marketing.iloq.com/sicherheit

www.iloq.de

iLOQ
Making life accessible

Alles wird gut

Liebe Leserin, lieber Leser, der Start ins Jahr 2021 war ja schon mal ganz vielversprechend: Es wird jetzt geimpft, und am Horizont scheint langsam die Hoffnung auf, sich draußen bald wieder weitgehend normal bewegen oder gar reisen zu können – vielleicht auch wieder in die hoffentlich bald Wiedervereinigten Staaten von Amerika.

Einen guten Start hinlegen wollen auch wir von Wiley und GIT SICHERHEIT: Wir läuten 2021 mit einer, wie wir finden, besonders gut gelungenen Ausgabe ein: Unsere Doppelausgabe für Januar und Februar versorgt Sie mit dem nötigen Hintergrundwissen für alle wichtigen Sicherheitsthemen, verschafft Ihnen aktuelle Einblicke praktisch-technischer Art – und wir haben für Sie wieder alle relevanten Neuheiten aus der Welt der Sicherheit gesammelt.

Auf Seite 14 sprechen wir mit Dr. Anja Opitz über die Logik von Pandemien – und zum klugen Umgang mit ihnen. Enno Münster erzählt uns ab Seite 18, wie Sicherheit bei der Lufthansa organisiert wird – auch und gerade in Corona-Zeiten. Das neue Sicherheitsdienstleistungsgesetz thematisieren wir mit den Verbandsbossen Caroline Eder (BVSU) und Dr. Harald Olschok (BDSU). Von Bosch haben wir zwei CEOs auf unserem Interviewsofa: Dr. Tanja Rückert und Hartmut Schaper (S. 26).

Manch einer spricht ehrfürchtig vom Videoanalyse-Guru, wenn von Kay Ohse von Genetec die Rede ist. Er sagt uns auf Seite 34, was wir von dieser Technologie erwarten können – und was nicht. Einen großen Schwerpunkt bringen wir ab Seite 37: mit unserem „Heft im Heft“ zum Thema „Zutritt & Smart Building“: Praxis- und Technikberichte vom Feinsten.

Cybersicherheit für Krankenhäuser ist Thema eines Webseminars, das Wiley mit den Experten von Veeam und unserer Zeitung „Management & Krankenhaus“ veranstaltet. IT-Security in diesem sowie in weiteren Kritis-Bereichen sind Teil Ihres Jobs? Dann melden Sie sich gerne unter <https://bit.ly/35Gnkvi> an, die Teilnahme ist für Sie kostenfrei. Infos dazu auf Seite 63.

Mit Dr. Ruth Westheimer können wir nicht aufwarten – trotzdem geht's um Aufklärung, und zwar die in Sachen Brandschutz in unserer Bevölkerung. Dazu befragen wir auf Seite 66 mit Frieder Kircher den Vorsitzenden des Gemeinsamen Ausschusses für Brandschutzzerziehung und Brandschutzaufklärung des DFV und der vfdb.

Hot and spicy wird es in unserer Rubrik Safety mit Pilz, wenn wir Sicherheit und die damit einhergehende Effizienz beim Tortilla-Chips-Hersteller Poco Loco vorstellen. Vorsicht, knabbern Sie nicht aus Versehen die Seite 76 an. Weitere Beiträge zum Thema Maschinen- und Anlagensicherheit, ein Interview mit Tobias Authmann von Denios zum Umgang mit Gefahrstoffen (S. 88) und „Was ist eigentlich... ein innovativer Sicherheitsschuh?“ (S. 91) mit Andreas Himmelreich von Haix machen das Heft so richtig rund. In diesem Sinne:

Bleiben Sie sicher – und gesund.



Herzlichst,
Ihr

Steffen Ebert
für das Team von Wiley
und GIT SICHERHEIT

P.S.: Ab Seite 10 zeigen wir Ihnen Highlights unserer virtuellen Messe vom vergangenen November. Auf www.WileyIndustryDays.com können Sie sich schon jetzt als Besucher kostenfrei für die **nächsten WIN>DAYS (7.–9. Juni 2021)** registrieren.

SALTO
inspired access



VIELSEITIGE ELEKTRONISCHE ZUTRITTLÖSUNGEN

SYSTEMARCHITEKTUR je nach Anforderung online, offline, funk- vernetzt, Cloud-basiert und mobil.

SYSTEMPLATTFORM mit Türbeschlägen und -zylindern, Wandlesern, Spindschlossern, Software, Apps u. v. m.

SYSTEMKOMPONENTEN für Innen- und Außentüren, automatische Türsysteme, Tore, Aufzüge, Spinde, Möbel, Zufahrten u. v. m.

SALTO Systems GmbH
info.de@saltosystems.com
www.saltosystems.de



TITELTHEMA

Ganz beiderseits

Schlösser mit Panikfunktion und Zutrittsverwaltungssoftware für Gebäude jeder Größe: Sicherheit auf beiden Seiten der Tür bieten die ÜLock-B-Schlösser von Südmetall – zum Schutz von Menschenleben und Sachwerten.

Seite 46

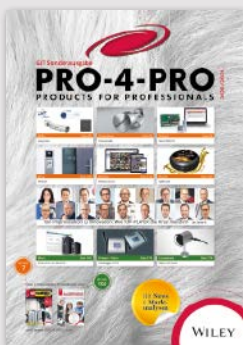


INNENTITEL SAFETY

Lautlos nach dem Lauf des Lichts

Solid-State-Scanner zum Überwachen automatischer Drehflügel und Karusselltüren

Seite 73



Gültig für 2020/21:

GIT Sonderausgabe PRO-4-PRO anfordern per Mail an GIT-GS@Wiley.com

EDITORIAL

03 Alles wird gut
Steffen Ebert

MANAGEMENT

10 Das waren die
Wiley Industry Days 2020
Nachbericht und Vorschau auf die nächste Messe

CORONA-PANDEMIE

14 Risiken einer
globalisierten Welt

Zur Logik von Pandemien – und zum klugen Umgang mit ihnen

KONZERNSICHERHEIT

18 Unter den Wolken
Unternehmenssicherheit bei
Lufthansa



Anja Opitz

Tanja Rückert

Frieder Kircher

SDLG

22 Qualität oder Kommerz
Das neue Sicherheitsdienstleistungsgesetz stellt die Weichen

24 Verbindliche
(An)forderungen
Die Eckpunkte: Warum wir das Sicherheitsdienstleistungsgesetz brauchen – und wie genau

INTERNET OF THINGS

26 Ready for IoT
Bosch und S&ST setzen auf offene Plattformen als Innovationsmotor

BRANCHENGEPRÄCH

30 Ein Errichter für Errichter
Im Interview mit den Geschäftsführern der TAS: Warum das Modell der plattformbasierten Fernzugriffe auf Alarmsysteme die Zukunft ist

SECURITY

SICHERHEITSNETZWERKE

32 Innere Sicherheit
Barox-Switche schützen Sicherheitsnetzwerke und Geräte von Drittanbietern vor Ripple20-Cyberangriffen

VIDEOÜBERWACHUNG

34 Videoanalyse
Was wir heute schon von der Technologie erwarten können – und was nicht

HEFT IM HEFT • ZUTRITT & SMART BUILDING



INNENTITEL: ZUTRITTSORGANISATION

38 Allrounder für die
intelligente Gebäudeorganisation
Maßgeschneiderte Lösungen für öffentliche Bauten

PRAXISBERICHT RECHENZENTRUM

42 Bunker digital
ColocationIX optimiert Zutrittskontrolle in bunkergeschütztem Rechenzentrum durch digitale Schließtechnik

TITELTHEMA

46 Ganz beiderseits
Südmetall: Schlösser mit Panikfunktion und Zutrittsverwaltungssoftware für Gebäude jeder Größe

PRAXISBERICHT INDUSTRIE

50 Einfach und filigran
Virtuell und funkvernetzte Zutrittslösung für MBG Group

PRAXISBERICHT KLINIK

54 Infektionsschutz
am Entrée
Zutrittsschleuse im Klinikum Herford knüpft Gebäudezutritt an Kontrolle der Körpertemperatur und die Einhaltung der Maskenpflicht

SCHLIESSYSTEME

56 Drei Mal Silber
für die Sicherheit
Antimikrobielle Oberflächen für Beschläge, Zylinder und Panikstangen

SYSTEMLÖSUNGEN

58 Bereit fürs Neue
Zukunftsorientierte Planung lässt die Zutrittskontrolle mit den Anforderungen an die Gebäudesicherheit mitwachsen

KRITISCHE INFRASTRUKTUREN

60 KRITIS:
Kriterien für ganzheitliche Sicherheit
Mechanische und elektronische Schließanlagen im Wandel der Sicherheitstechnik



Michael Badeja

Tobias Authmann

Andreas Himmelreich

IT-SECURITY

WEBSEMINAR

62 Bevor die Hacker kommen
Cyber-Angriffe auf Krankenhäuser werden häufiger und zerstörerischer – was tun? Ein Webseminar von Wiley und Veeam am 23. Februar gibt Aufschluss

CYBER SECURITY

64 Cybersicherheit und Resilienz
Wie mobiles Arbeiten und Arbeiten im Homeoffice sicher gelingt

BRANDSCHUTZ

VERHALTEN IM BRANDFALL

66 Nicht jeder weiß Bescheid!
Richtiges Verhalten im Brandfall: Zehn Fragen an den Experten

NAHRUNG UND GENUSSMITTEL

70 Süßes gut geschützt
Diamant Zucker: Brandschutzlösung mit Sauerstoffreduzierung

SAFETY

SENSOREN

74 Lautlos nach dem Lauf des Lichts
Solid-State-Scanner zum Überwachen automatischer Drehflügel- und Karusselltüren

MASCHINEN- UND ANLAGENSICHERHEIT

76 „Hot and Spicy“
Kleinsteuerung PNOZmulti 2 sorgt für optimierte Sicherheit und Effizienz

80 So könnte vorgegangen werden
Prüfung und Messung an Maschinen

84 Intralogistik im Outdoor-Bereich auf einem neuen Level
Der Sicherheitslaserscanner outdoor-Scan3 im Stresstest bei Basf

GEFAHRSTOFFE

88 Training ist alles
In jeder Ausgabe erklären Sicherheitsexperten Begriffe, Methoden und Technologien

RUBRIKEN

72 Impressum
92 GIT BusinessPartner
98 VIP Couch

ORGANISATIONEN INSTITUTIONEN UND UNTERNEHMEN IM HEFT

INDEX

SCHNELLFINDER

APB Tutzing	14	IntraKey	41
Apem	79	Kaspersky	65
ASC	86	Kentix	45
Asecos	9, 67, 87	Kötter	9, 25
Assa Abloy	41, 53, 60	Ksenia	7
Aug. Winkhaus	37, 38	Leuze	8
Axis	51	Mewa	90
B&R	8, 79	Mobotix	36, 49
Barox	32, 45	Moxa	65
Bauer	75	NürnbergMesse	68
Baumüller	83	Paul H. Kübler	90
BDSW	8, 24	PCS	31, 58
Bernstein	83	Pepperl+Fuchs	74
BHE	69	Pfannenberg	83
Bihl & Wiedemann	U4	Phoenix Contact	80
Bosch	26, 49	Pieper	45
BVSW	22	Pilz	76
C.Ed. Schulte	9, 23	PMev	6
De Jong	57	Rohde & Schwarz	65
Dehn	79, 87	Rose+Krieger	87
Denios	88, 90	Salto	3, 50
Deutsche Lufthansa	18	Schlentzek & Kühn	6
Deutsche Messe	71	Sick	84
Dom	40, 45, 56	SimonsVoss	17, 42
Drägerwerk	90	SSB Electronic	45
E. Dold & Söhne	79	Süd-Metall	Titel, 46
Eizo	45, 53	TAS	19, 30
FM Global	64	Telenot	6
Franz Schneider Brakel	41, 53, 57	Teletrust	6
Gefran	83	Trend Micro	65
Genetec	34	VDSI	98
Genua	79	Veeam	63
Georg Schlegel	83	vfdb	66
Geze	6	Wagner Group	70
Haix	91	Wanzl	35, 54
Helly Hansen	90	Wilka	49, 53
Hymmer	86	ZVEI	8
Iloq	U2, 8, 40		

Kostenfrei registrieren!
www.WileyIndustryDays.com

Wiley Industry Days

WIN DAYS
7.-9. Juni 2021



Willkommen im Wissenszeitalter. Wiley pflegt seine 200-jährige Tradition durch Partnerschaften mit Universitäten, Unternehmen, Forschungseinrichtungen, Gesellschaften und Einzelpersonen, um digitale Inhalte, Lernmittel, Prüfungs- und Zertifizierungsmittel zu entwickeln. Wir werden weiterhin Anteil nehmen an den Herausforderungen der Zukunft – und Ihnen die Hilfestellungen liefern, die Sie bei Ihren Aufgaben weiterbringen. Die GIT SICHERHEIT ist ein wichtiger Teil davon.

WILEY

NEWS

Erneute Top-Platzierung für Telenot

Bei der von der „Wirtschaftswoche“ durchgeführten Bewertung der innovativsten mittelständischen Unternehmen rückt Telenot 2020 in die Top Ten auf den sechsten Platz vor und übertrifft damit sein Ergebnis des Vorjahres. Zugleich ist der Hersteller elektronischer Sicherheitstechnik auch Branchenprimus in dieser Rangliste. Grund für die gute Platzierung sind die Produkt- und Serviceoffensive des Unternehmens. In die Wahl kamen ausschließlich Mittelständler mit einem Jahresumsatz

zwischen zehn Millionen und rund einer Milliarde Euro. Für die Bewertung hat Munich Strategy in einem ersten Schritt die Innovationstätigkeit sowie die Wettbewerbsposition der Unternehmen ermittelt. Bei den besten 400 untersuchten die Wirtschaftsexperten im Anschluss die Performance. Dabei flossen Kriterien wie „Top Branchen-Player“, „Image als Innovationsführer“ oder „aktuelle Innovationen“ ein.

www.telenot.com ■



Geze bietet Auszubildenden und dual Studierenden die Chance auf eine moderne Ausbildung

Neue Auszubildende bei Geze ▲

Geze empfängt auch 2020 wieder 13 Auszubildende und 10 dual Studierende am Firmensitz in Leonberg. Eine aktive Nachwuchsförderung sei für das Unternehmen selbstverständlich und spiele für die Entwicklung und das Wachstum der Firma eine bedeutende Rolle – vor allem in diesen besonderen Zeiten, so Sinem Turan, Leitung Personal. Gerade der erste Schritt ins Berufsleben sei wichtig, komme es doch darauf an, den richtigen „Partner“ zu finden: Ein

Partner, der die Talente und Fähigkeiten der jungen Menschen erkennt, entwickelt und zielgerichtet fördert. Um auch in Zeiten von Hygienevorschriften ein attraktiver Partner für Absolventen zu sein, erweitert das Unternehmen in diesem Jahr den digitalen Auswahlprozess und das Angebot für seine Bewerber: Vorstellungsgespräche werden online und sicher von zu Hause aus gehalten.

www.geze.de ■



Eröffnung von Terminal 1 des BER

BER: Schlentzek & Kühn maßgeblich an RWA beteiligt ▲

Passend zum 25-jährigen Jubiläum des Berliner Sicherheitsfachrichters Schlentzek & Kühn begann mit der Eröffnung des Berliner Flughafens BER am 31. Oktober auch die öffentliche Nutzung der Rauch- und Wärmeabzugsanlage (RWA) in Terminal 1. Für das Unternehmen ein Ereignis mit hohem Symbolwert, ist der Brandschutzspezialist doch seit mehr als zehn Jahren am Aufbau der RWA beteiligt. Schlentzek & Kühn installierte dort zahlreiche vernetzte

Nachströmöffnungen von Kingspan Light + Air STG-Beirkirch. Die RWA in Terminal 1 sei mit Abstand das bisher umfangreichste Projekt des Unternehmens gewesen, so Geschäftsführer Christian Kühn. Die größte Herausforderung seien die zahlreichen Planänderungen während der gesamten Projektdauer gewesen. Die waren nur durch das außerordentlich hohe Engagement des BER-Teams zu stemmen, so Kühn.

www.sicherheitdirekt.de ■

Teletrust gegen staatliche Hintertüren

Wie der Bundesverband IT-Sicherheit (Teletrust) mitteilt, haben sich Medienberichten zufolge die Regierungen der EU-Mitgliedsstaaten darauf verständigt, sichere Verschlüsselung EU-weit zu verbieten. Demnach sollen Technologieanbieter und Dienstbetreiber dazu gezwungen werden, Hintertüren in ihre Verschlüsselung einzubauen. Eine Aushöhlung der Verschlüsselung bedeute aber, die ohnehin träge Digitalisierung in der EU zu gefährden. Denn diese gelinge nur nachhaltig, wenn

man das Vertrauen in IT fördere – und nicht mindere. Lösungen mit Hintertür könnten nicht als dem „Stand der Technik“ entsprechend betrachtet werden. Das Zurückfallen auf einen schlechteren Technologiestand habe nicht nur massive Auswirkungen auf die IT-Sicherheit, es sei rechtlich auch nicht mit der DSGVO und dem IT-Sicherheitsgesetz vereinbar, so Rechtsanwalt Karsten U. Bartels, stellvertretender Teletrust-Vorstandsvorsitzender.

www.teletrust.de ■

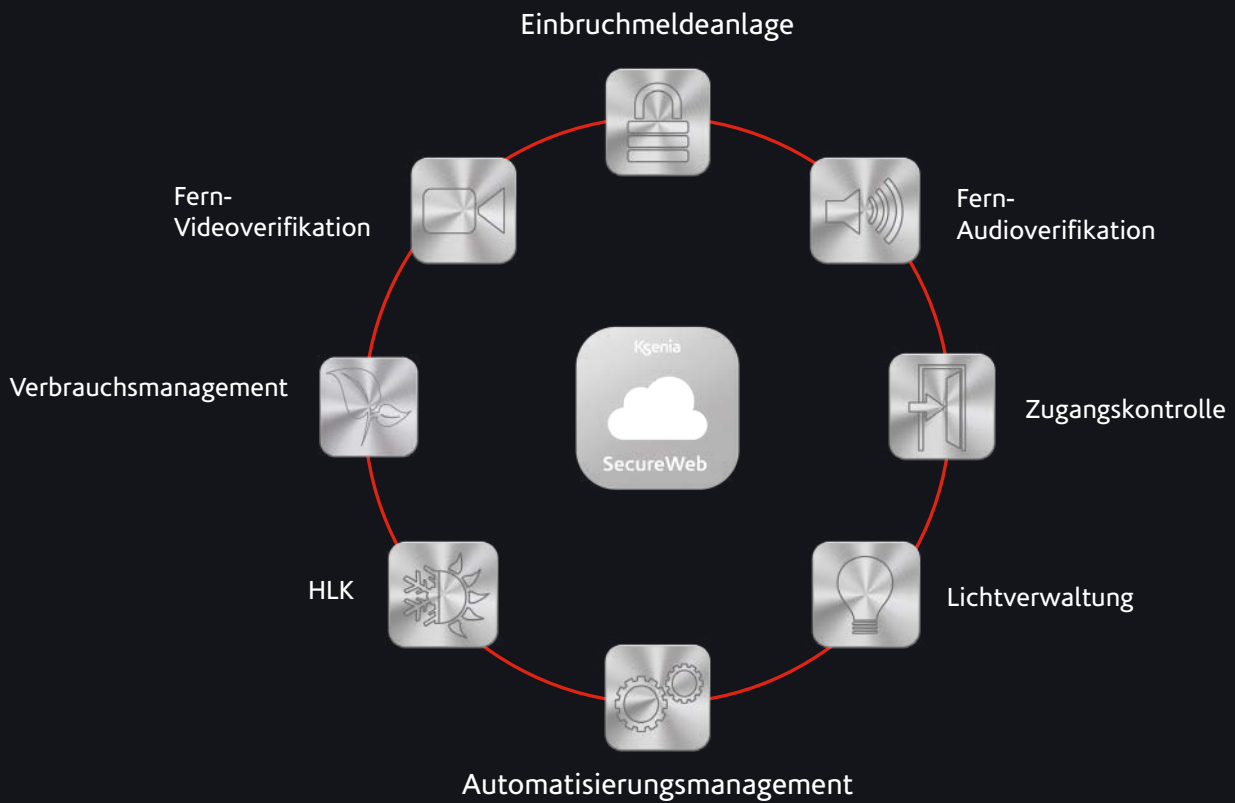
PMeV: Videogespräche auf der digital PMRExpo 2020

Der PMeV – Netzwerk sichere Kommunikation, ideeller Träger der digital PMRExpo, hat während der virtuellen Messe zu digitalen Gesprächsterminen mit Bernhard Klinger, Vorsitzender des PMeV, eingeladen. Das Thema der Videogespräche war: „Aktuelle und zukünftige Entwicklungen des Professionellen Mobilfunks der Sicherheitskritischen Kommunikation“. Darüber

hinaus hat der Verband an allen drei Messetagen Gespräche ohne Fokussierung auf ein vorgegebenes Thema angeboten. Sie dienten der Fortsetzung oder dem Start des Dialogs mit dem Verband. Gesprächspartner für den Dialog während der drei Messetage waren: Uwe Jakob, Geschäftsführer des PMeV und Jochen Müller, Pressesprecher.

www.pmev.de ■

Nennen Sie es nicht einfach "Alarmsystem"!



SCHAUEN SIE DAS GANZE VIDEO AN!



iLoq arbeitet mit Cellnex Telecom zusammen

iLoq hat einen langfristigen Rahmenvertrag unterzeichnet, mit dem das Unternehmen einer der bevorzugten Prioritätslieferanten für die Zugangskontrolle des Cellnex-Netzwerks von Telekommunikationsmasten und Rechenzentren wird. Cellnex Telecom bietet Dienstleistungen in Italien, den Niederlanden, Großbritannien, Frankreich, der Schweiz, Irland, Portugal und Spanien an und ist ein wichtiger Infrastrukturbetreiber für drahtlose Telekommunikation in Europa und der zweitgrößte Betreiber von Telekommunikationsmasten in der Welt. Das Unternehmen bietet seinen Kunden eine Reihe von Dienstleistungen an, um die Voraussetzungen für eine zuverlässige und qualitativ hochwertige Übertragung von Sprache, Daten und audiovisuellen Inhalten zu gewährleisten. Es entwickelt Lösungen im Bereich der „Smart City“-Projekte, die öffentliche Dienstleistungen über Netze und Dienste optimieren, mit denen die kommunale Verwaltung unterstützt wird. Zudem spielt das Unternehmen eine wichtige Rolle bei der Einrichtung von Sicherheits- und Notfallnetzen für Sicherheitskräfte.

Mit der Vergabe der Sicherheits- und Zugangskontrollprioritäten für den Cellnex-Betrieb würdigte das

Unternehmen die Qualität und Innovation der S50-Produktreihe von iLoq. iLoq S50 ist eine schlüssellose Lösung, die etwa speziell für Einrichtungen entwickelt wurde, die wesentlicher Teil der Infrastruktur sind. Die zum Entsperren benötigte Energie wird von einem Smartphone geliefert, auf dem die mobile App iLoq S50 läuft. Zugriffsrechte können per Fernzugriff in Echtzeit aktualisiert und mehrere Standorte bequem in einer benutzerfreundlichen und sicheren Cloud-basierten Software-Plattform zusammengeführt werden. Durch die batteriefreie Lösung kann Cellnex die Wartungskosten senken und Batterieverschwendung sowie Umweltbelastungen durch Reisen zwischen Standorten und Verwaltungsstellen zur Aktualisierung von Zugriffsrechten vermeiden. Diese wichtige Vereinbarung, die sieben Länder in Europa umfasst, sei ein weiterer Beweis für die bedeutenden Kundenvorteile, die die Technologie von iLoq bieten kann. Es sei ein riesiger Meilenstein für die iLoq-S50-Produktreihe für den mobilen Zugriff, und man freue sich, Cellnex in ihrem Bestreben, die Sicherheit zu optimieren, unterstützen zu können, so Heikki Hiltunen, Präsident und CEO von iLoq.

www.iloq.com ■

ZVEI: IT-Sicherheitsgesetz in jetziger Form unzureichend

Der vom Bundesinnenministerium (BMI) vorgelegte Entwurf zum sogenannten zweiten IT-Sicherheitsgesetz sei weiterhin nicht zufriedenstellend und bleibe hinter den Erwartungen der Elektroindustrie zurück, so der ZVEI – Zentralver-

band Elektrotechnik- und Elektronikindustrie. Es sei anzuzweifeln, ob das Schutzziel Cybersicherheit auf die vorgeschlagene Weise effizient und zielführend adressiert werde.

www.zvei.org ■

B&R: Clemens Sager wird Interims-Präsident

Weil der B&R-Geschäftsführer Hans Wimmer zum Ende des Jahres das Unternehmen verlassen wird, wurde Clemens Sager zum Interims-Präsidenten bestimmt. Bis ein neuer Division-Präsident gefunden wurde, wird Clemens Sager diese Rolle übernehmen. Hans Wimmer leitete in den vergangenen 16 Jahren das Unternehmen als Geschäftsführer. Integrität, die Nähe zum Kunden sowie ein starkes Führungsteam standen immer im Mittelpunkt seiner Arbeit. Hans Wimmer hat den Weg bereitet, dass das Unternehmen auch in Zukunft weiterwachsen und seine Profitabilität steigern kann. Nach insgesamt 34 Jahren bei B&R wird Hans Wimmer seinen zukünftigen beruf-



Clemens Sager, CFO und Interims-Präsident von B&R

lichen Weg außerhalb des Unternehmens gestalten. Clemens Sager war seit 2006 für ABB im Bereich Finanzen tätig. Dort bekleidete er diverse leitende Funktionen, unter anderem als CFO der Division Turbocharging. Bei B&R ist er seit 2017 CFO.

www.br-automation.com ■

Leuze bleibt Weltmarktführer im Bereich Optosensorik

Auch 2021 ist Leuze als Wachstumsschampion im Weltmarktführerindex 2021 der Henri B. Meier Unternehmensschule der Universität St. Gallen und der Akademie Deutscher Weltmarktführer (ADWM) gelistet. Jedes Jahr im November werden die aktuellen Weltmarktführer (WMF) veröffentlicht. Leuze ist als einer von 458 Wachstumsschampions wieder mit dabei. Das Unternehmen freute sich über dieses positive Ergebnis. Seit 2016 ist das Unternehmen im WMF-Index gelistet. Und auch 2021 darf sich Leuze weiterhin als Weltmarktführer im Bereich Optosensorik titulieren. Leuze sei ein Hochtechnologieunternehmen und auf eine konsequente Fokussierungs- und Differenzierungspolitik



Ulrich Balbach, CEO bei Leuze

ausgerichtet, sagt Ulrich Balbach, CEO bei Leuze, auf die Frage, wie man Weltmarktführer wird. Das Unternehmen beherrsche seine Technologien sehr gut und gestalte diese für seine Kunden so, dass für deren spezifische Applikation ein konkreter Nutzen und Mehrwert entsteht.

www.leuze.com ■

BDSW: Veranstaltungsordnungsdienst ist kein Sicherheitsdienst

Wie der BDSW mitteilt, sind nach einer Entscheidung des Amtsgerichts Köln Personen, die Karten-, Personen-, Taschen-, oder Körperkontrollen im Einlassbereich eines Stadions durchführen, keine „Wachpersonen“ im Sinne der Gewerbeordnung. Diese Entscheidung liege voll auf der Linie des BDSW, so der Vorsitzende des Arbeitskreises VOD des Verbandes Martin Houbé. Seit Jahren vertrete der Verband diese Rechtsauffassung, der nun endlich ein Gericht uneingeschränkt gefolgt

sei und das Verfahren endgültig eingestellt habe. Das Verfahren betraf den Sicherheits- und Ordnungsdienst im Rheinenergiestadion in Köln. Nach den Leitsätzen der rechtlichen Argumentation zählen Personen, die körperliche, mechanische Tätigkeiten wie Karten-, Personen-, Taschen- oder Körperkontrollen durchführen, zum Veranstaltungsordnungsdienst (VOD) nach den versammlungsstättenrechtlichen Vorschriften.

www.bdsw.de ■

Verleihung des CES-Preises

Die jährlich stattfindende Preisverleihung des CES-Preises, den der VDI seit 1990 an herausragende Nachwuchsingenieure der Produktionstechnik verleiht, wurde in diesem Jahr durch die Corona-Pandemie erschwert. Die Jury und der VDI haben sich im November dazu entschlossen, die Urkunden mit der Post zuzustellen und die Preisgelder zu überweisen. Preisträger im Jahr 2020 sind Alina Timmermann und Lukas Wurzer, deren herausragende Masterarbeiten mit jeweils 1.500 € Preisgeld prämiert wurden. Alina Timmermann studiert an der TU Dortmund bei Professor Dirk Biermann am Institut für Spanende Fertigung der TU Dortmund. Sie hat ihre Masterarbeit zum Thema „Grundlagenuntersuchungen zur Oberflächenkonditionierung des Einsatzstahls 18Cr-NiMo7-6 mittels Microfinishen“ geschrieben.

Hier wurde die Optimierung der Endbearbeitung von Getriebeteilen in Windkraftträdern durch Microfi-



Alina Timmermann

nischen (Kurzhubhonen) am Beispiel eines Einsatzstahlwerkstoffs untersucht. Die Analyse zeigt, dass der zweistufige Endbearbeitungsprozess durch Microfinishen mithilfe der Streulichtmesstechnik hinsichtlich Prozesszeit und Bearbeitungsergebnis optimiert werden kann. Timmermann arbeitet aktuell am Institut für Spanende Fertigung der TU Dortmund als wissenschaftliche Mitarbeiterin. Sie habe sich riesig über die Auszeichnung ihrer Masterarbeit gefreut. Der Preis habe ihre Entscheidung bestätigt, weiterhin in Forschung und Entwicklung tätig zu sein, so Alina Timmermann



Lukas Wurzer

Lukas Wurzer schrieb seine Masterarbeit bei Prof. Jörg Franke am Lehrstuhl für Fertigungsautomatisierung und Produktionssystematik an der Friedrich-Alexander-Universität in Erlangen-Nürnberg zum Thema „Evaluierung der Zuverlässigkeit unterschiedlicher Metallisierungen auf LDS-basierten Schaltungsträgern unter thermomechanischer Beanspruchung“. Im Rahmen der Masterarbeit wurde die Zuverlässigkeit von MID unter thermomechanischem Einfluss untersucht. Ergebnis der Masterarbeit sind fundierte Kenntnisse über die Herstellung zuverlässiger MID unter wechsell-

der Temperaturbelastung. Dadurch ermöglichte Wurzer neue Erkenntnisse über die Zuverlässigkeit und Leitfähigkeit von LDS-MID, was deren Einsatz in rauer Umgebung und dadurch neue Applikationsfelder ermöglicht und die Herstellung von qualitativ hochwertigen MID möglich machen wird.

In der Forschung dauere es oft, bis ersichtlich werde, wie wichtig der Beitrag für das Projekt ist, an dem er mitgewirkt habe. Durch den CES-Preis und die Arbeit in einem Unternehmen, das MID-Produkte produziert, wisse er nun, dass dieser Baustein wichtig war. Damit habe er nicht nur sein Studium abgeschlossen, sondern auch die Produkte verbessern können, die er aktuell betreue, so Lukas Wurzer. Seit Februar 2020 arbeitet er als Projektleiter bei 2E Mechatronic in Kirchheim Teck, unter anderem auch an Projekten zur Realisierung von MID-Produkten.

www.ces.eu ■



Asecos liefert ab sofort selbst ▲

Von der zertifizierten Serienfertigung der Typ-90-Gefahrstoffschränke von Asecos bis hin zu deren Verpackung, Lieferung und Inbetriebnahme direkt beim Kunden – alles geschieht ab sofort im DACH-Bereich vollständig aus einer Hand. Die am Stammsitz im hessischen Gründau produzierten Sicherheitsschränke werden ab sofort durch ein internes Team von 19 Logistikprofis mit langjähriger Erfahrung ausgeliefert. Dieses Vorgehen hat sich bereits für andere Produkte

des Unternehmens, wie die Luftreiniger und Raucherkabinen der „Smoke & talk“-Reihe, bewährt. Sie werden seit vielen Jahren durch ein eigenes Logistik-Team zugestellt. Ab sofort gilt dieser Service auch für die Gefahrstoffschränke. Alle zehn Lkws des Fuhrparks sind mit der neuesten Technik ausgestattet. Mit einer abgestimmten Tourenplanung trägt der Hersteller zudem dazu bei, dass Lieferwege effizient gestaltet werden.

www.asecos.com ■

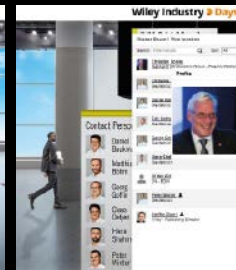
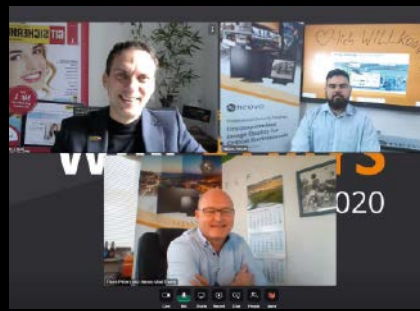
Kötter Security-Mitarbeiter ausgezeichnet

BASF Münster hat Security-Mitarbeiter von Kötter mit dem BASF-Security-Award ausgezeichnet. Den Preis für Arbeitsschutz und Unternehmenssicherheit erhielt Robert Marschall, Mitarbeiter der Niederlassung Münster von Kötter Security. Er ist seit mittlerweile mehr als fünf Jahren für das Familienunternehmen aktiv und genauso lange beim Kunden BASF in Hilstrup tätig. Robert Marschall habe durch seine Ausbildung als IHK-geprüfte Werkschutzfachkraft und weitere Zusatzqualifikationen umfassendes Know-how auf dem Gebiet der Unternehmenssicherheit und des Arbeitsschutzes. Außerdem kenne er das BASF-Gelände quasi wie seine Westentasche. Dementsprechend gebe es kaum eine potenzielle Gefahrenquelle oder -stelle, für die er auf dem weiträumigen Gelände während seiner Streifengänge nicht sensibilisiert wäre, so Ditmar Nachtigal, Leiter Responsible Care Management EMEA, der gemeinsam mit Eberhard Krude, Leiter Werkfeuerwehr und Werksicherheit,

den Preis übergab. Dies verdiene besondere Anerkennung und großen Respekt.

Diesem Lob schloss sich Jürgen Ballmann, Leiter der Niederlassung Münster von Kötter Security, an. Man sei stolz auf Mitarbeiter wie Robert Marschall, die mit solcher Akribie und Leidenschaft ihrer Arbeit nachgingen. Gleichzeitig sah er den Preis auch als Bestätigung für die gute Arbeit des gesamten Teams sowie das Engagement des Unternehmens im Bereich der Arbeitssicherheit an. So hat die Niederlassung neben der SCC-Zertifizierung für die Petrochemie auch eine Anerkennung nach Arbeitsschutzmanagementsystem AMS. Das Unternehmen ist seit fast vier Jahrzehnten mit vielfältigen Leistungen für die Sicherheit in der Dom- und Universitätsstadt sowie dem umliegenden Münsterland engagiert. Diese reichen von Revierwachdiensten über Werkschutz (Empfangs-, Pforten-, Streifendienste etc.) bis zu Sonderdiensten wie z. B. vorbeugendem Brandschutz.

www.koetter.de ■



Impressionen der Messestände, des Videocall-Tools (obere Reihe, 2. v. l.) und die Ansicht, wenn man noch alles auf einem bestimmten Stand treffen kann (2. Reihe, 4. v. l.)



Das waren die ...

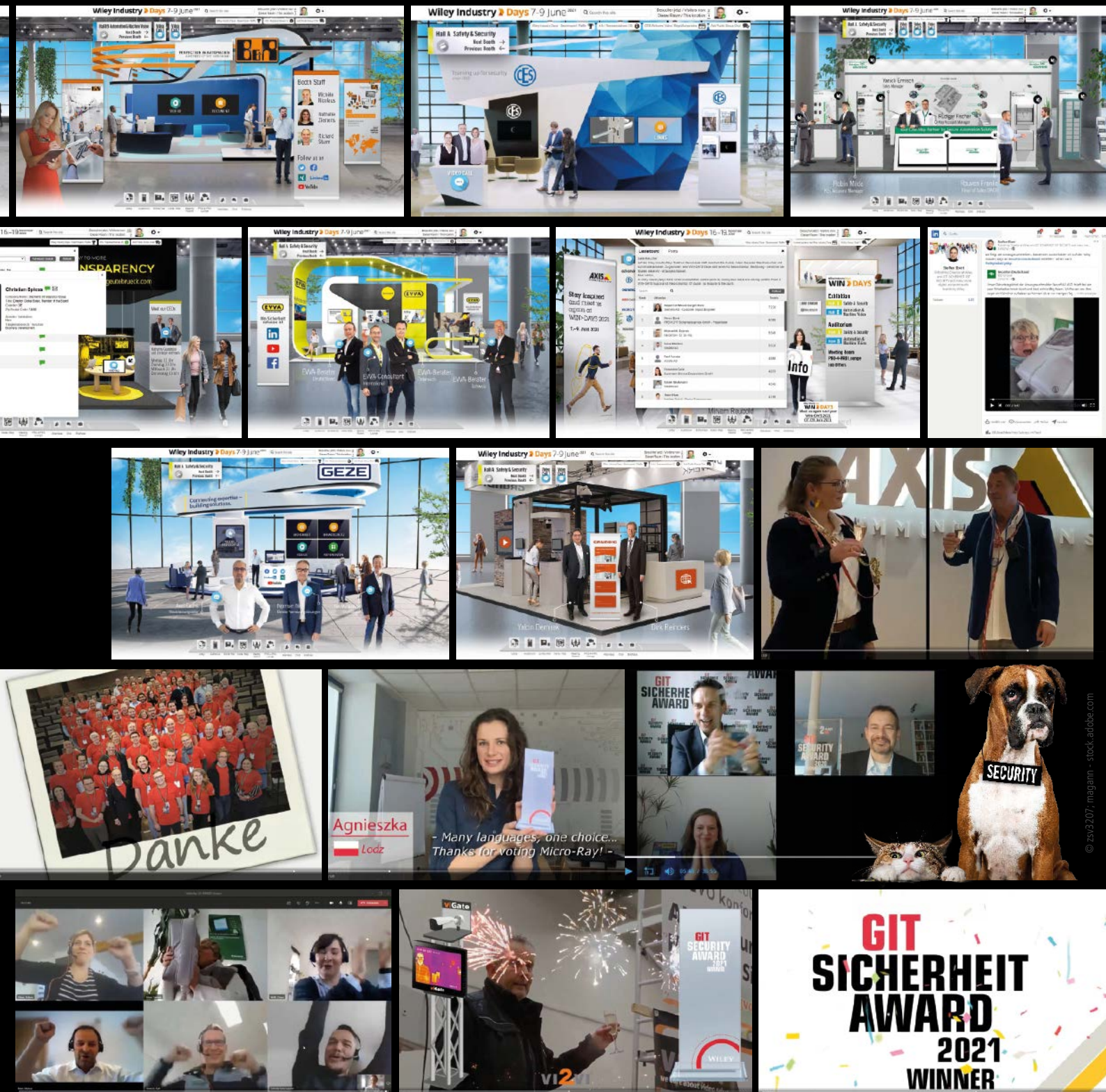
Wiley Industry Days

WIN > DAYS

16.-19.11.2020

„Let’s meet virtually“ hieß es vom 16. bis 19. November, bei den ersten virtuellen Wiley Industry Days. Als digitales Event für Sicherheit und angrenzende Branchen fanden die „WIN>DAYS“ ausschließlich im Netz statt – und boten den Besuchern ein vielfältiges Programm, um sich zu informieren und zu vernetzen.





Messestände, das Besuchergewinnspiel (2. Reihe, 2. v. r.), Freude auf LinkedIn über den Award für Securiton (2. Reihe, 1. v. r.). Über den GIT SICHERHEIT AWARD freuten sich außerdem auch virtuell mit: Axis (3. Reihe, 1. v. r. und 4. Reihe, 1. v. I.), Cias (4. Reihe, 2. v. I.), Securiton (5. Reihe, 1. v. I.) VIZVI (5. Reihe, 2. v. I.) und unsere Redaktionshaustiere Miezi und Wuffgang

Die Illustrationen zeigen: das virtuelle Gelände war einer physischen Messe nachempfunden, an den Ständen der Aussteller waren Avatare der richtigen Ansprechpartner anzutreffen.

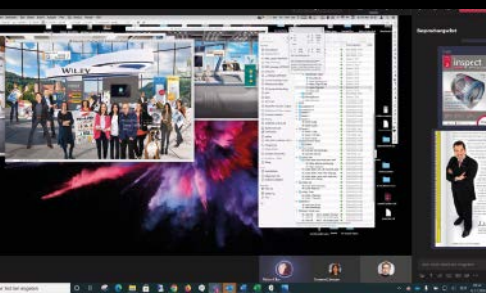
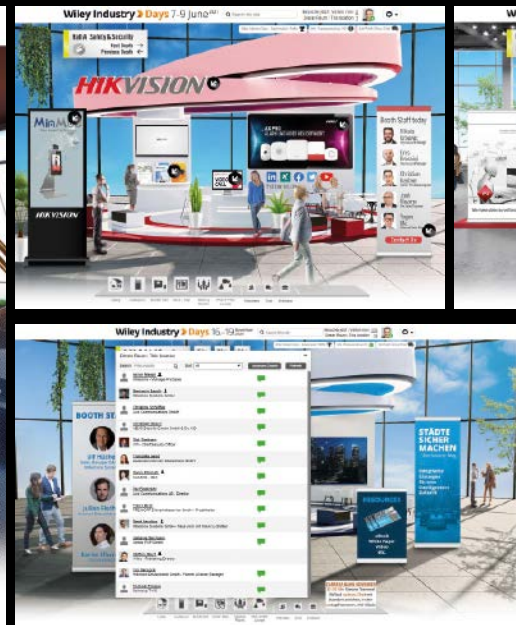
30 Stände wurden für die Besucher errichtet, 37 Vorträge organisiert und durchgeführt. Zudem wurden an einem der Nachmittage

die Sieger der GIT SICHERHEIT AWARDS gekürt und in Video-Clips gewürdigt.

1400 Besucher hatten sich für diese erste virtuelle Show registriert, mehr als 1000 waren dann – verteilt auf die vier Messetage – vor Ort. Wer vor Ort war, hatte Gelegenheit, sich nach Lust und Laune mit den Ausstellern auszutauschen. Per Chat – aber auch per Video-Call in Einzel- oder Multi-Chats.

Zur ersten Orientierung diente dabei die Lobby, wo die Besucher einen Überblick über die Hallen, Auditorien und weitere Meeting-Räume sowie das Career Center mit Stellenangeboten erhielten. In einer digitalen Messtasche konnte eine jede Besucherin, ein jeder Besucher seine ganz persönlichen Infomaterialien, Broschüren und Videos einsammeln – was auch ausgiebig genutzt wurde.

© zsv3207, magam - stock.adobe.com



Bei einigen WIN>DAYS-Gewinnspielen gab es schicke Sachpreise der Top-Sponsoren **Evva** und **Milestone** zu gewinnen – zudem Monitore von **AG Neovo**: Einen EX-24E Monitor direkt am Stand des Qualitätsanbieters mit dem hochrobusten Sicherheitsglas hat **Herr Udo Ziemer** von Scanvest gewonnen – beim Messe-Gewinnspiel hat **Frau Raquel de Moura Gurgel Silva** von Siemens einen AG Neovo RX-24EW abgeräumt.
Herzlichen Glückwunsch!



3 Fragen an die Gewinnerin

Raquel de Moura Gurgel Silva, herzlichen Glückwunsch – Sie haben beim WIN>DAYS-Besuchergewinnspiel einen Monitor von AG Neovo gewonnen. Was ist Ihre berufliche Tätigkeit und welches war Ihr Anlass, die Wiley Industry Days 2020 zu besuchen?

Raquel Silva: Ich bin Customer Impact Engineer bei Siemens, für unser Security-Portfolio im Bereich Smart Infrastructure mit Fokus auf PSIM und arbeite von München aus an Kundenbetreuung und F&E. Ich habe Ihre tolle GIT SECURITY abonniert und war auf der virtuellen Messe Wiley Industry Days 2020, um mit möglichen Partnern und Kollegen aus dem Sicherheitsbereich in Kontakt zu kommen.



Was hat Ihnen gut gefallen auf der Messe?

Die virtuelle Plattform war super! Sehr realistisch und mit klasse Inhalten. An jedem Tag der Messeweche hatte ich Zugang zu neuem Material, erhielt Einblicke und hatte tolle Gespräche. Es war alles sehr inspirierend und hat mir neue Verbindungen und Ideen für meine Arbeiten und Projekte eröffnet.

Was hat Ihrer Ansicht nach vielleicht gefehlt und woran sollten wir fürs nächste Mal (7.-9. Juni 2021) arbeiten?

Ich hätte mir vielleicht noch mehr Beteiligung von Endnutzern und Partnern in den Chaträumen gewünscht. Ich könnte mir außerdem vorstellen, dass ein Raum oder eine spezielle Session nach dem Motto „Voice of the Customer“ noch sehr interessant sein könnten.





© fenske - stock.adobe.com

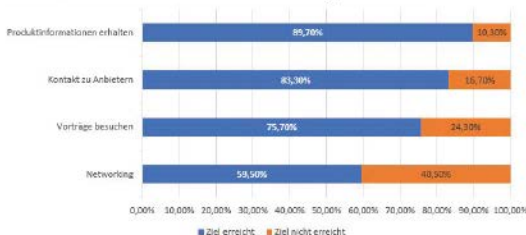


Biertasting am zweiten Messetag mit anschließenden Multi-Video calls (linke Seite, ganz oben links), weitere Messestandimpressionen, Video-Call mit Assa Abloy (3. Reihe, 3. v. r.) - und ein Blick auf den Photoshop-Schreibtisch unserer Layout-Abteilung (linke Seite, ganz links außen), bei der die Uhrzeit beachtenswert ist: Freitag auf Samstag, nachts um 1:22 Uhr. Hut ab vor so viel Engagement - und vielen Dank, all (!) Ihr lieben Layoutis :-)

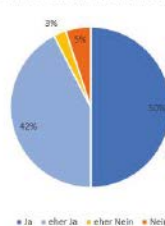
Umfrage-Ergebnisse

Wiley Industry Days WIN > DAYS

Besucher - Welche Ziele haben Sie mit Ihrem Messebesuch verfolgt; welche erreicht?



Besucher - Planen Sie bei den Wiley Industry Days vom 7.-9. Juni 2021 wieder mit dabei zu sein?

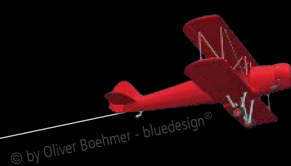


Aussteller, Referenten und der Wiley Verlag als Organisator richten ein großes Dankeschön an alle Beteiligten. Die digitale Herausforderung wurde angenommen, es wurden neue Kommunikationsformen organisiert, umgesetzt und angeboten, dabei auch experimentiert und daraus Schlüsse für die Neuaufgabe gezogen.

Das Feedback der Besucherinnen und Besucher war ausnehmend positiv: die übergroße Mehrheit hat ihre Ziele erreicht, etwa Produkt- und Service-Informationen oder Kontakt zu Anbietern zu erhalten. So planen mehr als 90 % eine erneute Teilnahme bei den WIN>DAYS 2021 vom 7.-9. Juni 2021. Dann heißt es erneut: Let's meet virtually.

Wir freuen uns auf Sie im Juni!

Wiley Industry Days
WIN > DAYS
7.-9. Juni 2021



© by Oliver Boehmer - bluedesign

www.WileyIndustryDays.com



CORONA-PANDEMIE

Risiken einer globalisierten Welt

Zur Logik von Pandemien –
und zum klugen Umgang mit ihnen

Dr. Anja Opitz verantwortet bei der Akademie für Politische Bildung Tutzing den Bereich „Internationale Politik und Sicherheitspolitik“. Für verschiedene Multiplikatoren konzipiert und leitet sie Fachtagungen, Expertenforen oder Seminare – aktuell beispielsweise eine Tagung zur Strategiefähigkeit der Bundeswehr im Kontext der globalen Sicherheitsarchitektur. Die Akademie will Wissenschaft und Praxis vereinen – so befasst sich Opitz auch mit der Forschung über den Nexus zwischen Gesundheit und Sicherheit sowie mit der Europäischen Sicherheits- und Verteidigungspolitik. Sie ist außerdem Präsidentin der Global Health Security Alliance (GloHSA). Matthias Erler von GIT SICHERHEIT hat mit Dr. Anja Opitz gesprochen.



GIT SICHERHEIT: Frau Dr. Opitz, die Akademie für Politische Bildung Tutzing will ja seit ihrer Gründung 1957 zur politischen Bildung beitragen – für Politik, Wissenschaft bis zur Öffentlichkeit. Welche Zielgruppen haben Sie mit dieser Forschung vor allem im Auge? Können auch Unternehmen daraus Nutzen ziehen?

Dr. Anja Opitz: Die Akademie ist ein Forum der Information, Forschung und des diskursbasierten Austausches und zugleich ein Ort der Vernetzung für Akteure aus Politik, Wirtschaft, Wissenschaft, Öffentlichkeit, Medien oder Bildung. Dabei setzen wir in unseren unterschiedlichen Angeboten auf einen interdisziplinären Ansatz. Auch Unternehmen gehören zu unseren Multiplikatoren, die diese Angebote wahrnehmen, denn sie gelangen so an auf spezifisch für sie zugeschnittene Expertise. Um ein Beispiel aus meinem Bereich zu nennen: Es gibt Unternehmen, die in Regionen investieren, die von Konflikten betroffen sind. Entsprechend können sich Mitarbeiter bei uns über entsprechende Konfliktstrukturen oder Sicherheitszusammenhänge fort- bzw. ausbilden.

Es gab von Ihrer und generell wissenschaftlicher Seite schon seit längerem Warnungen auch vor globalen Pandemien. 2012 gab es eine Risikoanalyse für die Bundesrepublik, in der sogar der Coronavirus schon erwähnt wurde?

Dr. Anja Opitz: Ja, in der jüngsten Vergangenheit waren es insbesondere die beiden Ebola-Epidemien 2014/2016 in Westafrika und 2018/2020 in der Demokratischen Republik Kongo sowie auch die Sars-Pandemie 2002/2003, die das Bewusstsein für derartige Herausforderungen wieder stärker in den Fokus rückten. Auch der von Ihnen angesprochene Bericht zur Risikoanalyse im Bevölkerungsschutz 2012 umfasste das Szenario einer Pandemie, ausgelöst durch einen fiktiven Virus „Modi-Sars“ und lieferte ein entsprechendes Risiko-Portfolio für Deutschland. Derartige Analysen bilden jedoch nur dann eine sichere Präventionsgrundlage, wenn sie regelmäßig überprüft und aktualisiert werden und das war hier leider nicht der Fall.

Dann lassen Sie uns einmal näher über die aktuelle Corona-Pandemie sprechen. Zunächst einmal: So eine Pandemie ist im Grunde etwas recht häufig Vorkommendes – nur nicht so sehr in unseren Breiten oder gar weltweit wie jetzt?

Dr. Anja Opitz: Epidemien, also das Auftreten einer hoch ansteckenden Krankheit in einem regional begrenzten Gebiet, treten häufiger auf. Das Risiko einer globalen Ausbreitung zur Pandemie erhöht sich in einer globalisierten Welt aus unterschiedlichen Gründen signifikant. Sars breitete sich 2002/2003 schneller aus, als dessen Erreger, ein bis dahin unbekanntes Coronavirus, identifiziert werden konnte. Sogenannte Zoonosen, Infektionskrankheiten, die zwischen Tier und Mensch übertragen werden, stellen eine der Hauptursachen für Epidemien dar. Die Mobilität der Menschen nimmt zu; sie sind potentielle Träger von Pathogenen und begünstigen so deren globale Ausbreitung, das hat Covid-19 gezeigt. Auch Europa kann Ausbruchsort für endemische Infektionskrankheiten sein. 2019 wurden in Deutschland die ersten Infektionsfälle mit dem West-Nil-Virus beim Menschen diagnostiziert. Das Virus ist in der Lage, hier zu überwintern; längere und wärmere Sommerperioden begünstigen eine Ausbreitung, so die Einschätzung des RKI. In Griechenland oder Italien erlebten wir die Rückkehr von Malariafällen, um nur wenige Beispiele zu nennen.

Man könnte also im Prinzip sagen, das Wissen über den besten Umgang mit Pandemien ist weitgehend in der Welt – wir müssen nur die richtigen Schlüsse daraus ziehen?

Dr. Anja Opitz: Auf Pandemien kann natürlich kein Staat zu hundert Prozent vorbereitet sein. Dennoch gibt es bestimmte Erfahrungswerte, Forschungsergebnisse und Best-Practice-Strategien, auf die man zurückgreifen kann und aus denen man Lehren für die Zukunft ableiten muss. Es verwundert, dass etwa der Global Health Security Index 2019 im Ergebnis zeigt, dass Staaten kaum bis gar nicht auf Großereignisse wie Pandemien oder Epidemien vorbereitet sind. Ich möchte damit sagen: Wir müssen über den wesentlichen Kern von Präventionsmaßnahmen intensiver und anders nachdenken. Ignorieren wir mit Blick auf „Gesundheitssicherheit“ weiterhin die Zusammenarbeit mit dem Veterinärsektor? Wie binden wir das Thema Digitalisierung zur Ursachenanalyse ein? Gelingt es, globale Indikatorensysteme zur Identifikation von potentiellen Gefahren zu entwickeln und vor allem, sind Staaten bereit, hier zu investieren?

Sie nannten in unserem Vorgespräch ein Beispiel dafür, dass auch große, global präsente Unternehmen nur vermeintlich, jedenfalls nicht ausreichend, auf Corona vorbereitet waren. Wo lag das Problem?

Dr. Anja Opitz: Vergleicht man die Ergebnisse des jährlich erscheinenden Global Risk Reports des World Economic Forums, wird deutlich, wo das Problem lag: Ein Verständnis dafür, dass derartige Krisen nicht nur den Gesundheitssektor betreffen, sondern massive Einschnitte für Wirtschaft und Gesellschaft bedeuten, war immer vorhanden. Aber die Wahrscheinlichkeit, dass diese Großereignisse global und in dem Ausmaß, wie wir es jetzt mit Covid-19 erleben, eintreten, wurde in den letzten Jahren konsequent unterschätzt.

Müssen sich Unternehmen auf Pandemien in ähnlicher Weise vorbereiten wie auf andere globale Phänomene wie zunehmende Cyberkriminalität, Klimawandel etc.?

Dr. Anja Opitz: Ja. Das Auftreten derartiger hybrider Herausforderungen oder Bedrohungen wird in Zukunft wahrscheinlicher. Pandemisches Risikomanagement sollte daher integraler Bestandteil einer jeden Business-Continuity-Strategie sein. Oder anders herum: Business-Continuity sollte auf einer Risikobewertung der potentiellen Auswirkungen einer Epidemie bzw. Pandemie auf das Unternehmen beruhen. Und hierfür ist das umfassende Verständnis über die Ursachen dieser sogenannten Kaskadenphänomene erforderlich.

Kann man die generellen Grundsätze des Krisenmanagements auch auf solche Pandemien anwenden? Oft haben die installierten Prozesse ja nicht wirksam greifen können?

Dr. Anja Opitz: Krisenmanagement ist ein weit gefasster Begriff. Mein Blick darauf ist durch mein Verständnis des Sicherheitsbegriffs geprägt. Im Englischen lässt sich der Unterschied gut mit den beiden Begriffen „security“ und „safety“ verdeutlichen. Zum einen geht es darum, Sicherheit durch Reaktion und Prävention zu gewährleisten, zum anderen um die Sicherstellung. Greift man hier den Aspekt der Prävention heraus, geht es also um die Erkennung von Gefahren, um das Verständnis über deren komplexe Ursachen, um die Entwicklung entsprechender Szenarien und, darauf aufbauend, um die Bedarfsermittlung von risikominimierenden Faktoren. Und dafür reicht der gängige Blick auf potentielle Unterbrechungen von Prozessen oder Störungen mit Blick auf (Human-) Ressourcen nicht aus. Das Stichwort ist die Vernetzung der Expertise unterschiedlicher Branchen und ein regelmäßiger Austausch.

◀ **Dr. Anja Opitz leitet den Bereich „Internationale Politik und Sicherheitspolitik“ an der Akademie für Politische Bildung Tutzing – und sie ist Präsidentin der Global Health Security Alliance (GloHSA)**

Gegen die Unterbrechung von Supply Chains dürften bei aller Vorbereitung kaum wirklich wirksame Kräuter gewachsen sein...? Welche grundsätzlichen Optionen gibt es aus Ihrer Sicht, mit denen Unternehmen ihre Geschäftsmodelle über solche Krisen retten bzw. schnell wieder hochfahren können?

Dr. Anja Opitz: Folgende Elemente halte ich für zentral: Pandemien haben ihre eigene Funktionslogik. Ähnlich wie Konflikte unterliegen sie einem, nennen wir es einmal Pandemiezyklus. Sie verlaufen meist über einen langen Zeitraum und durchlaufen verschiedene Phasen. Das bedeutet ein hohes Maß an Anpassungsfähigkeit und Flexibilität der verschiedenen Branchen. Zentral wäre daher die Entwicklung eines unternehmensspezifischen Indikatorensystems, das entsprechende Unsicherheiten und Risikoabhängigkeiten in unterschiedlichen Pandemiephasen identifizieren kann. An diesen Zeiträumen müsste das entsprechende Geschäftsmodell gemessen und getestet werden können, um die Krise zu überleben.

Wie sieht es mit kleineren und mittelständischen Unternehmen aus – haben auch sie ein nennenswertes Potential, sich besser aufzustellen?

Dr. Anja Opitz: Aus dem WHO Influenza Risikomanagement Konzept (2017) ist mir in diesem Zusammenhang ein Satz in Erinnerung: Das Geschäftsmodell selbst kann eine Bedrohung für die Resilienz bzw. Kontinuität des Business darstellen. Daher ist es gerade für kleine und mittelständische Unternehmen so wichtig, sicherzustellen, dass das Geschäftsmodell in der Lage ist, eine gewisse Widerstandsfähigkeit gegenüber äußeren Störungen wie einer Epidemie bzw. Pandemie zu entwickeln. Und hierzu gehört auch das Bewusstsein dafür, dass sich die zeitlichen Phasen zwischen zwei Epidemien oder Pandemien verkürzen werden. Mein Rat wäre es daher, den Fokus jetzt nicht nur auf das Überleben der aktuellen Pandemie zu legen, sondern bereits jetzt die Weichen dafür zu stellen, einer weiteren Krise dieser Art in der Zukunft erneut Stand halten zu können.

Inwiefern und inwieweit können politische Rahmenbedingungen und Maßnahmen verbessert werden, um künftig noch besser mit Pandemien umgehen zu können?

Dr. Anja Opitz: Die aktuelle Pandemie zeigt, dass der gängige Fokus auf die Stärkung der und Investition in die Stabilität und Wirksamkeit von Gesundheitssektoren zu kurz greift. Aspekte wie Ursachenerkennung im Bereich des Veterinärsektors fallen heraus, ebenso wie die Abfederung der Folgen einer Pandemie für die wirtschaftliche, gesellschaftliche und eben auch die sicherheitspolitische Entwicklung, ein Aspekt, der sehr gerne negiert

wird. 50% der nicht erreichten globalen Gesundheitsziele betreffen Staaten, die von Konflikten und Kriegen betroffen sind. Die Sekundäreffekte der Covid-19 Pandemie für diese Länder werden gravierender sein, als die wirtschaftlichen Folgen hier in Europa. Staaten der internationalen Gemeinschaft sollten sich von den gewohnten nationalstaatlichen Denkmustern lösen und in den multilateralen Rahmen investieren: in die VN, die WHO und die EU. Es benötigt eine politische Verpflichtung für ein ressortübergreifendes internationales Krisenmanagement. Und das bedeutet nicht nur die Reaktion auf eine Gesundheitskrise, sondern die ressortübergreifende Prävention. Das bedeutet u.a. die Bedarfsermittlung anhand der Fragen: Sind wir auf Massenfälle wie Pandemien ressourcentechnisch vorbereitet? Verfügen wir über die notwendigen Intelligence-Kapazitäten Gefahren zu erkennen, auch im Bereich des Bioterrorismus? Gibt es ein branchenübergreifendes Berichtswesen?



Unsere Experten eint das gemeinsame Verständnis, dass Gesundheits-, Sicherheits- und Stabilitätsprobleme zunehmende und miteinander verbundene globale Auswirkungen haben, die einen transnationalen und multisektoralen Ansatz zur Minderung von Bedrohungen erfordern.“

Sie sind ja auch Präsidentin der Global Health Security Alliance (GloHSA). Könnten Sie diese Vereinigung, ihre Mitglieder und die Aufgaben die sie sich gesetzt hat, einmal überschlüssig beschreiben?

Dr. Anja Opitz: Das Besondere ist ihr interdisziplinärer Charakter: GloHSA ist eine unabhängige, gemeinnützige Non-Profit-Association; ein Netzwerk internationaler Experten aus Politik, Wissenschaft, dem Privat-, sowie dem Sicherheits- und Gesundheitssektor, das wir 2017 gegründet haben. Unsere Experten eint das gemeinsame Verständnis, dass Gesundheits-, Sicherheits- und Stabilitätsprobleme zunehmende und miteinander verbundene globale Auswirkungen haben, die einen transnationalen und multisektoralen Ansatz

zur Minderung von Bedrohungen erfordern. Das Ziel von GloHSA ist eine effektive Vernetzung verschiedener Interessengruppen mit Entscheidungsträgern zur Erarbeitung von Konzepten zur Lösung globaler Herausforderungen im Bereich der Gesundheitssicherheit.

GloHSA bietet Analysen und Beratung. Welche Rolle spielte und spielt die Vereinigung während der Corona-Pandemie?

Dr. Anja Opitz: Derzeit sind viele der Mitglieder u.a. in den USA, in Frankreich, der Ukraine, Großbritannien, Deutschland, Belgien, Italien im aktiven Einsatz gegen Covid-19 gebunden; sei es von ärztlicher Seite zur Betreuung von Intensivpatienten, durch Unterstützung seitens der Streitkräfte zum Beispiel beim Contract-Tracing sowie im Rahmen der internationalen Unterstützung afrikanischer Staaten oder seitens Experten im Bereich der Health Security Intelligence, hierbei geht es u. a. um die globale Erfassung von Daten zur Ausbreitung des Coronavirus. Darüber hinaus versuchen wir derzeit verstärkt Unterstützung bei der Entwicklung nationaler und transnationaler Strategien oder bei der Durchführung krisenpolitischer Bewertungen und wissenschaftlicher Analysen zu leisten.

Die Coronapandemie ist bei globaler Betrachtung gewissermaßen „nichts Neues“. Wie sehen Sie von diesem Blickwinkel aus die weitere Entwicklung? Kann man aus typischen Verläufen ableiten, wann das Virus weitgehend überwunden sein wird? Würden Sie eine grobe Prognose abgeben?

Dr. Anja Opitz: Es wäre etwas vermessen, würde ich hier eine Prognose abgeben, denn ich bin weder Virologin noch Epidemiologin. Was ich aus meiner Sicht sagen kann ist: Ein Wendepunkt hin zu einem Ende einer Pandemie stellt sicherlich die Entwicklung eines entsprechenden Impfstoffs oder einer anderweitigen medizinischen und medikamentösen Behandlungsmethode dar. Das bedeutet aber nicht zwangsläufig, dass damit auch der Erreger selbst überwunden ist. Ich denke da an andere Infektionskrankheiten wie Masern, HIV, Malaria, Polio usw. Das Ziel ist es, die Ausbreitung durch die Unterbrechung der Infektionsketten einzudämmen bzw. zu beenden und in eine Situation zu gelangen, in der ein Gesundheitssystem durch einen Krankheitsausbruch nicht an Kapazitätsgrenzen gelangt. ■

Kontakt

Dr. Anja Opitz,
Internationale Politik & Sicherheitspolitik
Akademie für Politische Bildung
Tutzing
Tel.: +49 8158 256 54
a.opitz@apb-tutzing.de
www.apb-tutzing.de

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



**INTERESSIERT?
RUFEN SIE AN
089 99 22 8 - 555**

www.simons-voss.com



Enno Münster, Head of
Corporate Business
Security, Lufthansa Group

KONZERNSICHERHEIT

Unter den Wolken

Unternehmenssicherheit bei Lufthansa

Die Luftfahrt ist seit jeher mit besonderen Risiken behaftet. Ein besonderes Sicherheitsmanagement gehört schon immer dazu. Abgesehen von der Luftsicherheit im engeren Sinne gehört dazu aber auch die klassische Unternehmenssicherheit, wie man sie auch in der Industrie und anderen Branchen kennt. Wie sie bei der Lufthansa organisiert ist, erfahren wir im Interview mit Enno Münster, Head of Corporate Business Security, Lufthansa Group.*

GIT SICHERHEIT: Herr Münster, das Sicherheitsmanagement bei Lufthansa ist organisatorisch in zwei Bereiche aufgeteilt. Wie sieht das genau aus – und welche Rolle ist Ihre dabei?

Enno Münster: Zunächst möchte ich betonen, dass Sicherheit bei der Lufthansa ein wesentliches Element ist und zur DNA unseres Unternehmens gehört. Organisatorisch gibt es auf der einen Seite den für Luftfahrtunternehmen spezifischen Bereich der Luftsicherheit, die sich um die Einhaltung sämtlicher weltweiter Luftsicherheitsgesetze und -vorgaben kümmert

und risikobasiert auch darüberhinausgehende Maßnahmen trifft. Dazu gehören beispielsweise auch das Verhängen von Überflugverboten in Krisengebieten und das weltweite Monitoring der Sicherheitslage. Und dann gibt es meinen Verantwortungsbereich, den ich als klassische Unternehmenssicherheit bezeichnen würde und der in jedem größeren Unternehmen so oder so ähnlich vorzufinden ist.

Welche Aufgaben gehören im Einzelnen zu Ihrem Bereich?

Enno Münster: Dazu gehört ein Team, welches sich um die weltweite Sicherheit der Mitarbeiter mit den Schwerpunkten Bedrohungsmanagement und Sicherheit im Ausland (Reisen, Expats) sowie um Objektschutzvorgaben (inklusive des Konzernausweises) kümmert. Ein Team führt interne Ermittlungen durch bei Verdacht auf Straftaten zu Lasten des Lufthansa-Konzerns (z. B. Betrug, Korruption, Diebstahl, sexuelle Belästigung etc.). Ein weiteres Team verantwortet Teile der Informationssicherheit – darunter insbesondere Awareness

und Governance und ein Team sichert den Vorstand und Events ab.

Teils gibt es Überlappungen – so gehörte der neue Lufthansa-Konzernausweis als Teil des Objektschutzes zu Ihrem Bereich: Sie tauschen derzeit gerade die Ausweise gegen neue aus – warum genau?

Enno Münster: Richtig. Der Konzernausweis ist auch im Luftsicherheitsplan meines Kollegen, der die Luftsicherheit verantwortet, als Sicherheitsmerkmal hinterlegt, der Prozess liegt aber in meiner Verantwortung. Für den Tausch des Ausweises sprach neben der Erfüllung neuester regulatorischer Vorgaben aus dem Luftsicherheitsbereich auch das Verbauen neuester Sicherheitstechnologie, so dass Ausweise nicht kopiert werden können.

Mit welchen Systemen arbeiten Sie allgemein im Bereich Zutritt?

Enno Münster: Im Detail möchte ich darauf nicht eingehen, aber wir verwenden jetzt verschlüsselte Chiptechnologie, die den Zugriff auf die hinterlegten Daten blockiert.

Sie haben u. a. eine GmbH gegründet, in der sämtliche Werkschutzseinheiten gebündelt wurden. Welche Vorteile bringt dieser Schritt?

Enno Münster: Wir haben 2019 die Lufthansa Group Security Operations GmbH (LGSO) gegründet, die sämtliche operativen Sicherheitsdienstleistungen des Konzerns in Deutschland bündeln soll. Dazu gehören sowohl selbsterbrachte Leistungen als auch eingekaufte Leistungen. Dies ergibt vielfältigste Synergiepotentiale, die sich insbesondere während der Corona-Krise schon bezahlt gemacht haben und es uns ermöglichen einen siebenstelligen Eurobetrag einzusparen.

Nimmt diese GmbH nur Lufthansa-interne Aufgaben wahr – oder ist auch an eine Öffnung für Dritte gedacht?

Enno Münster: Die Leistungserbringung ist derzeit auf den Konzern beschränkt.



„Sicherheit ist bei der Lufthansa ein wesentliches Element und gehört zur DNA der Lufthansa“, sagt Enno Münster im Gespräch mit GIT SICHERHEIT

Foto: Flughafen Frankfurt: Check-In-Mitarbeiter, Lufthansa. Fotograf: Oliver Roesler

Was bedeutet das für externe Dienstleister, die Sie ja auch in Anspruch nehmen?

Enno Münster: Die LGSO mit ihrem Geschäftsführer Rainer Geng soll auch sämtliche Dienstleistungen am Markt für die Lufthansa in Deutschland einkaufen und tritt dort als professioneller Partner gegenüber den Dienstleistern auf, die auch den Vorteil einer schnelleren Abwicklung haben und dann nur noch einen Ansprechpartner im LH Konzern haben.

Eines der großen Projekte, denen Sie sich bei Lufthansa gewidmet haben, war das „Insider Threat Program“. Könnten Sie uns die Hintergründe dafür erläutern?

Enno Münster: Die ICAO (Internationale Zivilluftfahrt-Organisation) führt Insider Threat als eines der zehn Top-Risiken in der Luftfahrt. Die EU hat zudem eine Richtlinie verabschiedet, die es Luftfahrtunternehmen vorschreibt, ein Insider-Threat-Programm ab 1.1.2022 verpflichtend vorliegen zu haben.

Als Lufthansa haben wir uns daher sehr frühzeitig der Thematik angenommen und haben bereits seit 2018 ein entsprechendes Programm vorliegen.

Wie wurde das Projekt inhaltlich aufgesetzt und organisiert? Welche Maßnahmen wurden im Einzelnen eingeführt?

Enno Münster: Wir haben zunächst mit internen und externen Experten fünf Handlungsfelder identifiziert, die eine Reduktion des Risikos bewirken können. Dabei waren alle größeren Fluggesellschaften im Konzern involviert. Diese Handlungsfelder sind Eingangskontrollen, Sensibilisierung der Führungskräfte und Mitarbeiter, Dienstleistermanagement, Kontrollmaßnahmen im Recruiting-Prozess und ein Bedrohungsmanagement mit einem Reportingkanal über den Verdachtsfälle gemeldet werden können und ausgebildete Bedrohungsmanager, die solche Fälle bewerten können. Für diese Handlungsfelder wurden

Rundum-Sicherheit für Industrie und Handel

Neue Bedrohungslagen erfordern die richtigen Antworten.

Wir sind für Sie da – als Spezialist für vernetzte Sicherheitslösungen und Partner von Industrie und Handel.

TAS

SICHERHEITS- UND
KOMMUNIKATIONSTECHNIK

Tel. 0 21 66 - 858 - 0

Mail: info@tas.de

www.tas.de

dann konkrete Alternativen ausgearbeitet, bewertet und verabschiedet. Es wird in einem risikobasierten Ansatz beschrieben, in welchen Geschäftsfeldern oder Geschäftsvorgängen welche Maßnahmen anzuwenden sind. Diese Umsetzungsvorgaben wurden letztlich über eine Konzernrichtlinie verpflichtend für alle Konzerngesellschaften, die diese dann umgesetzt haben.

Im letzten Jahr, also 2020, mündete das Insider Threat Program in eine Kontrollphase. Wie lief das ab – und mit welchen Ergebnissen?

Enno Münster: Ja die Umsetzungsphase war 2019 – und 2020 war ursprünglich vorgesehen, dass wir als 2nd Line of Defense-Funktion diese Ergebnisse kontrollieren. Das haben wir entsprechend im Rahmen unserer Audits, die wir ohnehin vornehmen, mitgemacht. Allerdings war dies 2020 aufgrund Covid-19 und der dadurch eingeschränkten Reisemöglichkeiten nicht wie gewohnt möglich. Durch Umstellung auf Remote- und Selbst-Audits der Kollegen vor Ort konnten wir aber auch viele Kontrollen vornehmen, ohne vor Ort sein zu müssen.

Sie erwähnten eingangs schon die Informationssicherheit – auch hier nehmen Sie Teilbereiche wahr: Awareness-Schulungen für Mitarbeiter gehören dazu. Und Sie haben ein Escape-Room-Spiel und ein Phishing-Tool getestet. Wie liefen diese Kampagnen ab?

Enno Münster: Um Mitarbeiter zu sensibilisieren, benötigt man immer wieder andere Ansätze, da die immer gleichen WBTs die Mitarbeiter doch ermüden. Daher haben wir 2019 ein Escape-Room-Spiel entwickelt, bei dem die Spieler sich nur befreien können, wenn sie die Informationssicherheitsvorgaben kennen und richtig anwenden. Dabei handelt es sich um eine Spielanleitung, mit deren Ausdruck und Anwendung jeder Büroraum in einen Escape Room verwandelt werden kann. Das

Feedback dazu war überragend. Da man das Spiel in der Gruppe in einem Raum durchführt, konnten wir es 2020 wegen Covid nicht mehr ganz so oft umsetzen. Beim Phishing-Tool geht es im Wesentlichen darum, Mitarbeiter im Alltag zu sensibilisieren, in dem man ihnen selbstdesignte Phishing-Mails schickt. Das Schöne an diesen Tools, von denen es mehrere Anbieter im Markt gibt, ist, dass man dadurch real gelebte Awareness messen kann, z. B. durch die Anzahl an Mitarbeitern, die auf Links geklickt oder Daten eingegeben hat.

Interne Ermittlungen sind eine heikle Angelegenheit – aber auch sie sind an Ihrer Stelle angesiedelt. Könnten Sie uns einen groben Eindruck verschaffen, wie das bei Ihnen organisiert ist?

Enno Münster: Im Regelfall bekommen wir von irgendwoher einen Hinweis auf eine potentielle Straftat. Die Eingangskanäle sind z. B. über den Ombudsmann der Lufthansa, über andere anonyme Reportingsysteme, die als Luftfahrtunternehmen rechtlich vorgeschrieben sind - außerdem von Mitarbeitern oder ehemaligen Mitarbeitern, durch die Revision, wenn dieser etwas in Prüfungen aufgefallen ist sowie von Strafverfolgungsbehörden etc. Die Vorwürfe werden dann validiert und wenn sich der Verdacht erhärtet, ein Ermittlungsvorgang eröffnet, bei dem dann versucht wird, Klarheit in die Angelegenheit zu bringen z. B. durch Interviews, Analyse von strukturierten Daten (wie z. B. Belege im Rechnungswesen) oder Analyse unstrukturierter Daten (wie eMails im Rahmen einer eDiscovery). Handelt es sich bei dem Vorgang um einen Compliance-relevanten Vorfall, wird das Vorgehen immer sehr eng mit dem Compliance Office bzw. der Rechtsabteilung abgestimmt. Zu beachten sind dabei insbesondere der Datenschutz, arbeitsrechtliche Aspekte und die interne Mitbestimmung.

Eine Frage kann natürlich in diesen Zeiten nicht ausbleiben: Wie hat sich Corona in Ihrem Zuständigkeitsbereich ausgewirkt?

Enno Münster: Natürlich hat Corona massive Auswirkungen auf den Luftverkehr, der wahrscheinlich die am meisten getroffene Industrie ist. Entsprechend hatte diese auch deutliche Auswirkungen auf unseren Bereich. Neben Kurzarbeit und Home-Office hatte die Sicherheitsabteilung zwischenzeitlich neue Aufgaben übernommen, insbesondere das Verfolgen sämtlicher internationaler Einreiseregularien, so dass unsere Arbeitslast nicht so stark reduziert war, wie im Rest des Konzerns.

Welche Veränderungen werden Ihrer Einschätzung nach bleiben?

Enno Münster: Im Sicherheitsbereich sind generell durch Corona folgende Entwicklungen erkennbar: Die Sicherheitslage hat sich weltweit um einiges verschärft, z. B. durch Proteste gegen Coronamaßnahmen, soziale Spannungen, erhöhte Armut und dadurch vermehrte Kriminalität, reduzierte Anti-Terror-Einsätze von Regierungen. Kriminelle haben ihre Aktivitäten verstärkt auf das Netz verlegt und eine Zunahme an Internetattacken war auch für uns messbar. Gewohnte Abläufe wie Audits vor Ort oder Interviews vor Ort sind nicht mehr ohne weiteres möglich, so dass wir diese auf Remote-Abläufe umstellen mussten. Das ein oder andere wie Remote-Audits oder vermehrt Home Office hat sich bewährt und wird sicherlich auch bleiben. ■

* Das Interview wurde im Dezember 2020 geführt.

Ab Mitte Januar verlässt Enno Münster die Lufthansa und widmet sich neuen Aufgaben.

Kontakt

Deutsche Lufthansa AG
Frankfurt am Main
www.lufthansagroup.com



Flugzeuge parken auf Startbahn Nordwest wegen Corona-Krise in Frankfurt am 23.03.2020

WILEY

GIT **SICHERHEIT** **AWARD**



GIT
SICHERHEIT
AWARD

Jetzt bis
31. März
anmelden

AWARD FOR SAFETY AND SECURITY
GIT SICHERHEIT
+ MANAGEMENT

www.sicherheit-award.de

SDLG

Qualität oder Kommerz

Das neue Sicherheitsdienstleistungsgesetz stellt die Weichen

Das neue Sicherheitsdienstleistungsgesetz (SDLG) soll die Qualität in der Branche verbessern – darin sind sich die großen Sicherheitsverbände einig. Bei der Frage, wie sich eine solche Qualitätssteigerung erreichen lässt, gehen die Positionen allerdings auseinander. Insbesondere die Zulassungsprüfungen sind ein kritischer Punkt. Ein Beitrag von Caroline Eder.

„Mit dem neuen Sicherheitsdienstleistungsgesetz stellt die Sicherheitsbranche die Weichen für ihre Zukunft. Deshalb sollten nicht die wirtschaftlichen Interessen einzelner Unternehmen im Vordergrund stehen, sondern die Frage, von welchen Regelungen Branche, Staat, Bürger und Unternehmen gleichermaßen profitieren“, sagt Peter H. Bachus, stellvertretender Vorstandsvorsitzender beim ASW Bundesverband. Der Verband

hat im Vorfeld die wichtigsten Schlüsselpositionen in einem Positionspapier erstellt und veröffentlicht.

Neutralität im Vordergrund

Gefragt sind Regelungen, die für mehr Vertrauen in die Sicherheitsbranche sorgen. Das beginnt bereits beim Unterrichtsverfahren, das die gesetzlich vorgeschriebene Mindest-Zugangsvoraussetzung für die Arbeit in der Sicherheitsbranche darstellt, sowie bei den Prüfungsinstitutionen. Die IHK ist derzeit die einzige Einrichtung, die Prüfungen für Sicherheitsberufe durchführt. Durch schriftliche und mündliche Verständnisfragentests werden einheitliche Qualitätsstandards gesichert. Diese Wissensfeststellung und Bescheinigung soll, wenn es nach ASW, VSW und BVSU geht, ausschließlich durch unabhängige Stellen erfolgen.

„Wir befürworten durchaus, dass auch andere Institutionen die Prüfung zukünftig abnehmen dürfen, doch dabei darf der Kommerz nicht im Vordergrund stehen. Ganz wichtig ist für uns die Wahrung der Neutralität“, sagt Peter H. Bachus vom ASW

Bundesverband. „Deshalb muss es sich bei den Prüfstellen um staatliche oder staatlich beliehene Einrichtungen handeln.“

Ganz anders sind in diesem Punkt die Vorstellungen des Bundesverbandes der Sicherheitswirtschaft e. V. (BDSW), der die Sicherheitsdienstleister vertritt: Dieser Verband plädiert dafür, die Prüfungen auch durch vom BDSW zertifizierte Fortbildungsinstitute durchführen zu lassen. Indem sie ihre Mitarbeiter selbst ausbilden und auch selbst die Prüfungen abnehmen, könnten im BDSW organisierte Unternehmen deutlich schneller Mitarbeiter einstellen. Eine übergeordnete neutrale Bewertung wäre hiermit aber nicht mehr möglich. Außerdem ergäbe sich eine deutliche Verzerrung des Wettbewerbs, denn nur große Unternehmen in der Sicherheitsdienstleistungsbranche betreiben ihre eigenen Akademien. Kleinere Unternehmen müssten dann ihre Mitarbeiter bei den großen Wettbewerbern schulen lassen und hätten dann noch größere Schwierigkeiten, passendes Personal auszubilden und langfristig einstellen zu können.



Qualifiziertes Sicherheitspersonal:
Bundesverband ASW befürwortet eine
abgestufte Qualifizierung, die auf den
Aufgabenbereich abgestimmt wird

Steigende Anforderungen

Einigkeit herrscht auch in dem Punkt, dass die Anforderungen an die Ausbildung steigen sollen. Doch die Verbände sind unterschiedlicher Meinung, welches Niveau das Qualitätsentscheidende ist. Der BDSW möchte die Sachkundeprüfung als Voraussetzung für den Einstieg in die Branche etablieren. Diese ist mit 80 Stunden Unterricht und einer anschließenden Prüfung umfangreich. „Die Sachkundeprüfung als zwingende Voraussetzung für eine Tätigkeit im Sicherheitsgewerbe ist nach unserer Erfahrung in der Praxis nicht durchsetzbar“, sagt ASW Geschäftsführer Dr. Christian Endreß. „Nicht jede Tätigkeit in der Sicherheitsbranche erfordert die Qualifikation der Sachkundeprüfung.“ Viele Mitarbeiter wählen deshalb den Weg der Unterrichtung nach §34a GewO, der nur 40 Unterrichtsstunden umfasst. Auch bei dieser Ausbildung wird regelmäßig geprüft, ob der Unterrichtsstoff verstanden wurde und entsprechend angewandt werden kann. Viele Unternehmen beschäftigen seit Jahren Mitarbeiter mit dieser Qualifikation.

Warum sollte die Qualifikation aller Mitarbeiter auf das Niveau der Sachkundeprüfung angehoben werden, wenn sich dadurch weniger Kandidaten finden ließen? Eine höhere formale Ausbildung würde gegenüber den Auftraggebern auch höhere Preise rechtfertigen.

Der ASW Bundesverband befürwortet vielmehr eine abgestufte Qualifizierung, die auf den Aufgabenbereich abgestimmt wird: Für einfache Tätigkeiten, wie beispielsweise Baustellenbewachung, ist laut ASW die Unterrichtung nach §34a GewO ausreichend. Gehobene Tätigkeiten erfordern schon heute die Sachkundeprüfung als nächsthöhere Qualifikation, denn der §34a GewO schreibt sie für besonders konfliktträchtige und sensible Sicherheitstätigkeiten vor. Dazu zählen beispielsweise Kontrollgänge im öffentlichen Verkehrsraum, oder in Hausrechtsbereichen mit tatsächlich öffentlichem Verkehr, wie Citystreife, Bestreifung öffentlicher Parks, Einkaufszentren sowie S-/U-Bahn-Bereich. Ein Einsatz von Mitarbeitern privater Sicherheitsdienstleister im Bereich der kritischen Infrastrukturen erfordert noch höhere Mindestqualifikationen, wie die geprüfte Schutz- und Sicherheitskraft. Auch gleich- und höherwertige Berufsabschlüsse, wie der Ausbildungsberuf Fachkraft für Schutz und Sicherheit, sind im Kritis-Bereich passend. Regelmäßige Nachschulungen sind überall erforderlich.

SDLG auch für „Inhouse Tätigkeiten“?

Ein weiterer kritischer Punkt ist die Regelung von sogenannten „Inhouse Tätigkeiten“, bei denen ein Unternehmen, beispielsweise ein

Hintergrund

Seit dem 1. Juli 2020 gehört die Sicherheitsbranche erstmals zum Verantwortungsbereich des Bundesministeriums des Innern, für Bau und Heimat. Der Zuständigkeitswechsel vom Bundesministerium für Wirtschaft und Energie auf das Bundesministerium des Innern, für Bau und Heimat war der richtige Schritt: Staatliche Sicherheitsbehörden und die private Sicherheit sind damit im gleichen Bundesministerium verortet und werden von dort zentral gesteuert. Jetzt gilt es, ein neues Sicherheitsdienstleistungsgesetz zu schreiben, das als spezifische Rechtsgrundlage für die Sicherheitsbranche dient. In einem Positionspapier hat die Allianz für Sicherheit in der Wirtschaft e. V. (ASW) mit ihren regionalen Verbänden ihre Forderungen formuliert, wie sich mit dem neuen Gesetz sowohl rechtliche als auch qualitative Standards in der Branche verbessern lassen.

Stadionbetreiber oder ein Konzern, seine eigenen Sicherheitsmitarbeiter beschäftigt. Hier möchte der BDSW, dass diese Mitarbeiter auch den Anforderungen des neuen SDLG entsprechen. ASW, VSW und BVSU sind gegen eine solche Regelung, weil sie zu weit in die Verantwortung der Unternehmen eingreift. „Jedes Unternehmen, das seine eigenen Sicherheitsmitarbeiter beschäftigt, hat auch ein ureigenes Interesse daran, dass diese bestens ausgebildet sind“, sagt Alexander Borgschulze, Vorstandsvorsitzender des Bayerischen Verbandes für Sicherheit in der Wirtschaft e. V. (BVSU). „Wir erkennen hier keine Notwendigkeit, Unternehmen mit zusätzlichen Regelungen zu belasten. Insgesamt sehen wir dem neuen SDLG sehr optimistisch entgegen: Wir alle wollen das Ansehen der Branche stärken, indem die Qualitätsstandards besser eingehalten und erhöht werden. Deshalb setzen wir uns dafür ein, dass bei der Verabschiedung des Gesetzes die Qualität als Maßstab angesetzt wird.“ Dies soll sowohl für die Wirtschaft als auch für die Sicherheitsdienstleister gelten. ■



Kontakt

Caroline Eder
Bayerischer
Verband für Sicherheit
in der Wirtschaft e.V.
München
Tel. +49 89 35 74 83 40
caroline.eder@bvsu.de
www.bvsu.de



CES OMEGA FLEX

So sicher kann Individualität sein

Praxisgerecht kombinierbar, einfach zu montieren und flexibel zu integrieren – dafür stehen die elektronischen Zutrittslösungen von CES OMEGA FLEX. Online, offline oder im V-NET.



Weitere Informationen auf [ces.eu](https://www.ces.eu)



SDLG

Verbindliche (An)forderungen

Die Eckpunkte: Warum wir das Sicherheitsdienstleistungsgesetz brauchen – und wie genau

Angesichts der veränderten Verantwortung und der in den letzten Jahren gewachsenen Anforderungen an private Sicherheitsunternehmen ist das Gewerberecht, nicht (mehr) in der Lage, der gewachsenen faktischen Bedeutung der privaten Sicherheitsdienste für die Innere Sicherheit in Deutschland gerecht zu werden. Ein Beitrag von Dr. Harald Olschok.

Die Große Koalition hat auf die Forderung des Bundesverbands der Sicherheitswirtschaft BDSW reagiert und in der Koalitionsvereinbarung unter anderem ausgeführt: „Private Sicherheitsbetriebe leisten einen wichtigen Beitrag zur Sicherheit. Durch die Neuordnung der Regelungen für das private Sicherheitsgewerbe in einem eigenständigen Gesetz werden wir die Sicherheitsstandards in diesem Gewerbe verbessern und so für noch mehr Sicherheit und Verlässlichkeit sorgen.“ Darüber hinaus ist, wie ebenfalls vom BDSW gefordert, am 1. Juli 2020 die Zuständigkeit für die privaten Sicherheitsdienste vom Wirtschaftsministerium auf das Bundesministerium des Innern, für Bau und Heimat übergegangen.

Das Sicherheitsdienstleistungsgesetz (SDLG)

Nach dieser Vereinbarung müssen jetzt die rechtlichen Grundlagen angepasst werden. Um dies zu unterstützen hat der BDSW – zu dessen Mitgliedern rund tausend Unternehmen aus allen Bereichen der

Sicherheitswirtschaft, großteils mit Schwerpunkt Sicherheitsdienstleistungen, zählen – einen eigenen Entwurf für ein neues Sicherheitsdienstleistungsgesetz erarbeitet. Hier sollen für einzelne Aufgabengebiete, die eine enge Zusammenarbeit mit der Polizei erfordern, spezialgesetzliche Regelungen geschaffen werden. Diese sollen verbindliche Anforderungen an die Leistungsfähigkeit, Organisation, Qualifizierung sowie Ausstattung der privaten Sicherheitsdienste und ihrer Sicherheitskräfte zwingend festlegen.

Öffnung der Basis-Qualifizierungen für andere Anbieter

So sind aus Sicht des BDSW eine Überarbeitung und Aktualisierung der bisherigen Inhalte des Unterrichtsverfahrens (URV) notwendig – und aus der bisherigen Unterrichtung muss eine Basis-Qualifizierung werden.

Das bestehende Monopol der Industrie- und Handelskammern (IHK) bei der Durchführung des URV und der Sachkundeprüfung (SK) muss zudem aufgeweicht werden. Als

BDSW sind wir der Auffassung, dass die vom BDSW zertifizierten Sicherheitsfachschulen und die der ASW angeschlossenen Regionalverbände diese geforderte Basis-Qualifizierung genauso gut durchführen können.

Durch die Beschränkung auf die IHKs entstehen für Unternehmen und ihre Mitarbeiter*innen immer wieder unnötige Wartezeiten. URV bzw. SK sind Voraussetzung für die Meldung der Beschäftigten an das Bewacherregister. Erst dann können neue Mitarbeiter*innen eingesetzt werden.

Durch die Aussetzung von URV und SK im Rahmen des Corona-Lockdowns wurde die Rekrutierung von Personal für die Übernahme neuer Aufträge – ganz aktuell Sicherheitsaufgaben für die über 400 Impfzentren – massiv erschwert.

Diesen Problemen muss durch die Einbeziehung anderer Anbieter begegnet werden. Dem BDSW sind bundesweit 14 zertifizierte Sicherheitsfachschulen angeschlossenen, die seit Jahrzehnten Sicherheitspersonal qualifizieren. Auch die Mitgliedsverbände der ASW sind in diesem Segment tätig. Ein

Wettbewerb zwischen den IHKs und anderen zertifizierten Bildungsträgern wird zu einer Qualitätsverbesserung führen. Hierzu muss auch die Möglichkeit einer Online-Durchführung der Basis-Qualifikation zählen.

Beschleunigung des Zuverlässigkeitsverfahrens

Die Einsatzfähigkeit von Mitarbeiter*innen der Sicherheitswirtschaft ist zu optimieren – und es dürfen keine Sicherheitslücken für sensible Schutzbereiche entstehen. Es müssen Regelungen geschaffen werden, nach denen eine zusätzliche gewerberechtliche Zuverlässigkeitsprüfung dann nicht erforderlich ist, wenn bereits eine Zuverlässigkeitsüberprüfung nach einer anderen Rechtsgrundlage – mindestens in gleicher Überprüfungstiefe – innerhalb der letzten fünf Jahre erfolgt ist. In Fachkreisen ist dann vom „Kaskadenmodell“ die Rede.

Ausschreibung nach Qualität

Öffentliche Aufträge werden in der Regel an den billigsten Anbieter vergeben, ohne dass Qualitätskriterien ansatzweise Berücksichtigung finden. Oft kann nicht einmal die Einhaltung eines bestimmten Tarifvertrages zur Bedingung einer Auftragsvergabe erhoben werden. Diese Zustände schaden nicht nur dem Ansehen der Sicherheitswirtschaft in der Öffentlichkeit; sie fördern auch eine Verbreitung nicht akzeptabler Arbeitsbedingungen und können auch zu nicht hinnehmbaren Sicherheitslücken führen. Es müssen daher für öffentliche Ausschreibungen spezieller Einsatzbereiche Regelungen geschaffen werden, nach denen eine angemessene Gewichtung von Qualität und Preis, beispielsweise im Verhältnis 60 zu 40 Prozent, zu erfolgen hat.

Einbeziehung der Inhouse-Security

Schließlich fordert der BDSW vergleichbare Standards auch für betriebseigene Sicherheitskräfte. Wir halten es für unabdingbar, dass an die Mitarbeiter*innen der Inhouse-Security dieselben

Anforderungen im Bereich Qualifikation, Schulung und Weiterbildung gestellt werden wie an diejenigen der Sicherheitsdienstleister. Nur so kann vermieden werden, dass durch – auf Kosten-erwägungen beruhenden – Ausweichbewegungen der Bedarfsträger (Umsetzung mit eigenen Mitarbeiter*innen) die mit dem SDLG angestrebte Erhöhung des Sicherheitsstandards verhindert wird.

Fazit

Die Sicherheitswirtschaft und der sie vertretende Wirtschafts- und Arbeitgeberverband BDSW sind in den letzten 15 Jahren ihrer sicherheitspolitischen Verantwortung für Deutschland gerecht geworden. Wir haben das gesamte System der Aus-, Fort- und Weiterbildung auf komplett neue Füße gestellt. In elf Bundesländern wurden Kooperationsvereinbarungen mit den jeweiligen Landespolizeibehörden unterzeichnet. Der BDSW arbeitet aktiv in der Initiative Wirtschaftsschutz auf Bundesebene mit.

All diese Anstrengungen für noch mehr Qualität und flächendeckende Seriosität in der Sicherheitswirtschaft werden aber nur dann nachhaltig sein, wenn die rechtlichen Rahmenbedingungen für die privaten Sicherheitsdienste auf eine neue, zeitgemäße rechtliche Grundlage gestellt werden. Der BDSW ist willens und bereit, sich mit seinem Know-how und seinem Gesetzentwurf weiter in den politischen Entscheidungsprozess einzubringen. Die Chancen dafür sind so gut wie nie zuvor! ■



Dr. Harald Olschok
Bundesverband der
Sicherheitswirtschaft e.V.
Bad Homburg
Tel. +49 6172 948050
olschok@bdsw.de
www.bdsw.de



Consulting

Personelle Sicherheit

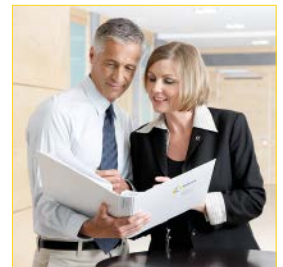
Sicherheitstechnik

SMART SECURITY SOLUTIONS

Vom Kraftwerk bis zum Verwaltungskomplex, vom Krankenhaus bis zum Industriebetrieb, von der öffentlichen Hand bis zum Handel: Jede Branche hat ihr eigenes Bedürfnis nach Sicherheit. Und genauso vielfältig und individuell wie Ihr Sicherheitsbedürfnis sind unsere Lösungen:

■ Consulting

Cyber Security/Digitales Notfall-, Interventions- und Krisenmanagement/ Sicherheits- und Risikomanagement/ Psychologische Akutintervention/ Arbeitssicherheit & Umweltschutz



■ Personelle Sicherheit

Werkschutz & Separatwachdienste/ Kritische Infrastrukturen/Fire & Service/ Aviation & Airport Security/Empfangsdienste/Revierwachdienste/Kurierdienste/ Maritime Security/Justizdienstleistungen/ Verkehrsdienste/Veranstaltungssicherheit



■ Sicherheitstechnik

Alarmmanagementsysteme/Videoüberwachung/Managed Video Solutions/ Remote-Video-Management/Video Tower/ Einbruchmeldesysteme/Brandmeldesysteme/Zutrittskontrolltechnik/ Perimeterschutz/Home Security/Wächterkontrollsysteme/Schließfachsysteme/ Notruf- und Serviceleitstelle/KÖTTER Service Center



KÖTTER
Security

—“Wir sind für Sie da.”—

Wilhelm-Beckmann-Straße 7
45307 Essen
Hotline: +49 201 2788-388
Fax: +49 201 2788-488
E-Mail: info@koetter.de
Internet: koetter.de

KÖTTER Services im Social Web:





INTERNET OF THINGS

Ready for IoT

Bosch und S&ST setzen auf offene Plattformen als Innovationsmotor

GIT SICHERHEIT sprach mit Dr. Tanja Rückert, CEO Bosch Building Technologies, und Hartmut Schaper, CEO Security & Safety Things (S&ST), über den Trend zur Zusammenarbeit mit anderen Herstellern, „denkende Gebäude“ und Sicherheitskameras, die wie ein Smartphone funktionieren.



Tanja Rückert,
CEO Bosch Building
Technologie

GIT SICHERHEIT: Frau Rückert, bei Ihrem Start sind Sie als ausgewiesene IoT-Expertin angetreten, die auf Vernetzung fokussierte Strategie von Bosch für den Bereich Building Technologies voranzutreiben und umzusetzen. In welcher Position sehen Sie Bosch Building Technologies heute?

Tanja Rückert: Wir sind bereits erfolgreich darin, durch die Vernetzung von Technologien das Leben unserer Anwender sicherer, komfortabler und effizienter zu machen. Dabei denke ich zum Beispiel an unsere Lösungen, die Brand- und Evakuierungssysteme kombinieren und damit für reibungslose Reaktionsabläufe sorgen, wenn jede Sekunde zählt. Oder nehmen wir die Vernetzung von Zutrittskontroll- und Videosystemen, die es ermöglicht, ein Gebäude einfach, sicher und kontaktlos zu betreten. Auch dass wir aus der Ferne auf unsere Systeme zugreifen können und uns diese Rückmeldung über ihren Betriebszustand geben – Stichworte „Remote Services“ & „Predictive Maintenance“ –, sind sehr gute Beispiele dafür, dass Vernetzung bereits ein integraler Bestandteil unseres Angebotes ist.

Das Thema Vernetzung muss jedoch weitergedacht werden. Bei Bosch sprechen wir daher von „AIoT“, also von einer Vernetzung physischer Produkte und dem Einsatz künstlicher Intelligenz. Dadurch können wir ganz neue Fragen stellen und Probleme lösen. Ein Beispiel ist unsere VdS-zertifizierte videobasierte Branderkennung „Aviotec“, mit der

wir dank intelligenter Algorithmen wesentlich schneller Brände im Entstehen detektieren können, als dies klassische Brandmelder vermögen. In seiner neuesten Version kann Aviotec dank Infrarotsensibilität im Monochrome-Modus selbst bei 0 Lux – sprich völliger Dunkelheit – zuverlässig Rauch und Flammen erkennen.

Mit unseren zahlreichen vernetzten Lösungen bewegen wir uns in Summe in Richtung „Automatisierte Gebäude“. Wenn wir noch weiter in die Zukunft blicken, werden wir „Denkende Gebäude“ haben, die sich an uns und unsere Bedürfnisse individuell anpassen und sich untereinander vernetzen.

Wie könnte so eine Zukunft konkret aussehen, Frau Rückert?

Tanja Rückert: Ich kann mir gut folgende Szenarien vorstellen: Im privaten Bereich wird Sie in Zukunft Ihr Fahrzeug autonom zum richtigen Ziel fahren, egal ob das ein Krankenhaus, ein Einkaufszentrum, ein Büro oder eine Fabrik ist. Das Gebäude weiß bereits, dass Sie auf dem Weg sind und stellt sich auf Sie ein: Sobald Sie Ihr Fahrzeug verlassen, parkt das Auto selbstständig, die Gebäudetüren öffnen sich für Sie automatisch und der Aufzug steht schon bereit, um Sie direkt in das richtige Stockwerk zu bringen. Gleiches gilt für Produktionsanlagen, die sich durch intelligente Vernetzung den Bedürfnissen des jeweiligen Produktionsprozesses anpassen. So kann die Analyse von Daten dazu führen, den Energieverbrauch deutlich zu senken, indem beispielsweise weniger Druckluft erzeugt wird, wenn weniger benötigt wird, oder indem weniger geheizt wird, wenn die Maschinen mehr Abwärme produzieren.

Wie weit sind wir schon auf diesem Weg?

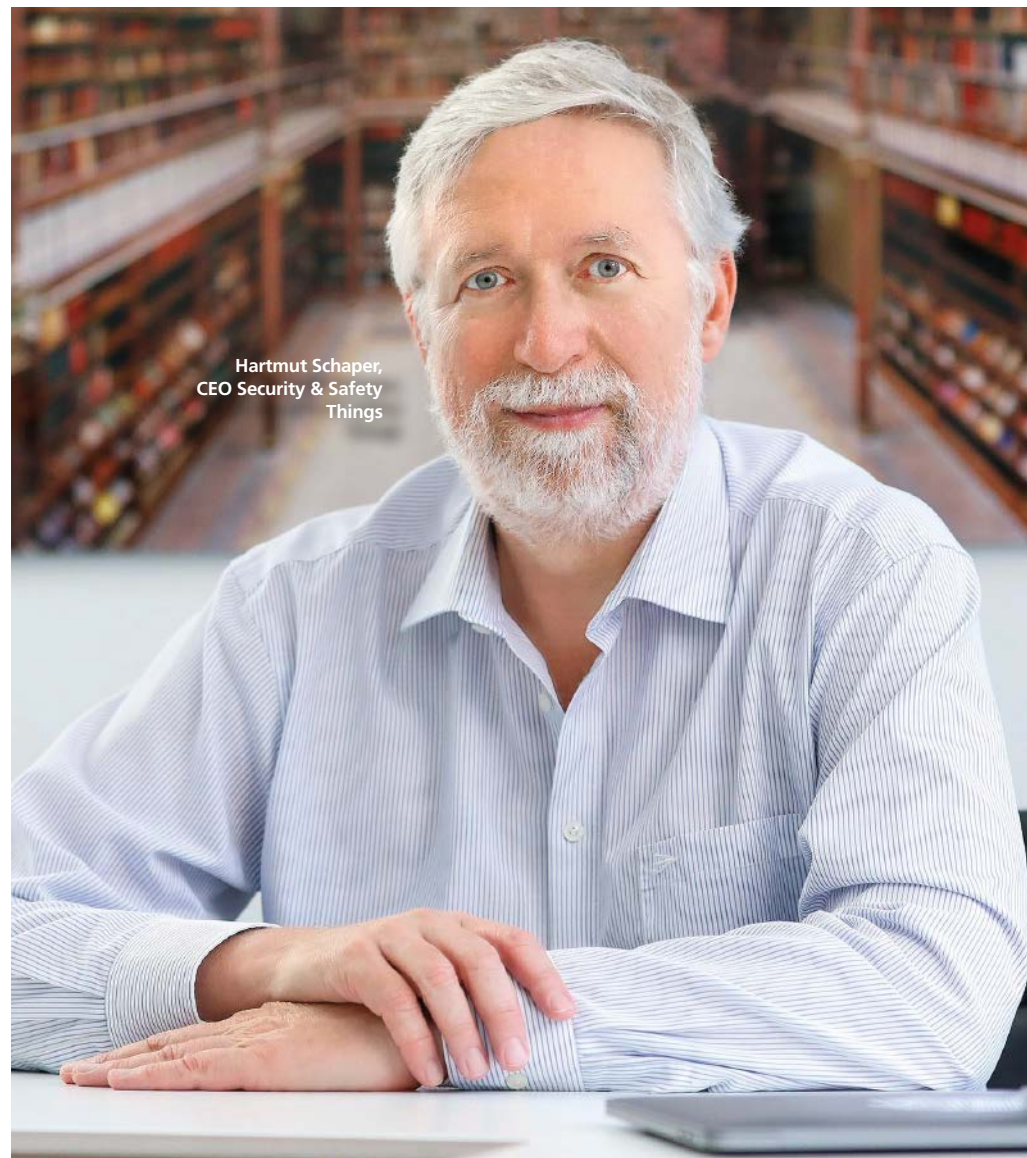
Tanja Rückert: Generell bin ich der Ansicht, dass oft überschätzt wird, was man in einem Jahr umsetzen kann, und oft unterschätzt wird, was man in fünf Jahren erreicht. Bosch ist bereits dabei, zukunftsweisende Technologien erfolgreich in der Gegenwart einzusetzen. Um bei einem der eben genannten

Zukunftsszenarien zu bleiben: Gerade hat Bosch zusammen mit Mercedes-Benz und Apcoa am Stuttgarter Flughafen ein Pilotprojekt in einem Parkhaus gestartet, in dem vollautomatisiertes und fahrerloses Parken in der Praxis getestet wird. Für das sogenannte „Automated Valet Parking“, kurz AVP, setzen wir maßgeblich auf eine intelligente Kamera-Infrastruktur von Bosch Building Technologies, die Fahrwege, freie Parkplätze sowie Hindernisse oder Personen auf der Fahrspur erkennen kann, um damit ein Fahrzeug fahrerlos zu steuern. Hierzu gibt es

auch ein beeindruckendes Video. Bei Bosch sind wir also bereits dabei, diese Zukunft zu gestalten.

Angesichts der zunehmenden Vernetzung, die Sie ansprechen: Sind herstellereigenspezifische Produkte noch relevant oder sehen Sie die Zukunft in offenen Plattformen?

Tanja Rückert: Die Zeit für herstellereigenspezifische Lösungen ist aus meiner Sicht abgelaufen. Offene Ökosysteme, die Hardwarehersteller, Softwareentwickler, Integratoren, Planer, Berater, Nutzer und weitere Parteien



Hartmut Schaper,
CEO Security & Safety
Things



zusammenbringen, sind viel flexibler und bieten insgesamt für alle große Vorteile: Zusammen können wir einfach mehr erreichen, als jeder für sich! Auf Basis offener Plattformen können wir unseren Kunden viel schneller die passende Lösung für ihre Anforderungen anbieten und natürlich auch gemeinsam mit unseren Kunden Lösungen optimieren und individualisieren. Auch dafür sind offene Systeme unabdingbar. Differenzierende Merkmale wird es jedoch weiterhin geben. Für Bosch bedeutet das im Bereich Videosicherheit, dass wir den Fokus weiterhin auf Security und Trust sowie auf eingebaute künstliche Intelligenz „at the edge“, also im Endgerät, richten, sodass sich unsere Produkte darin heute und auch zukünftig deutlich von denen anderer Anbieter unterscheiden. Bei Videodaten handelt es sich ja oft um kritische und sensible Informationen, weshalb wir einen systematischen Ansatz zur Maximierung der Datensicherheit verfolgen. Ein wichtiger Baustein liegt darin, dass die Daten bereits auf der Hardwareebene kryptografisch verschlüsselt werden. Der zugehörige Schlüssel ist dabei sicher auf einem einzigartigen integrierten „Trusted Platform Module“, kurz TPM, oder „Secure Element“ gespeichert.

Zusammen mit anderen führenden Unternehmen aus der Videosicherheitsbranche haben Sie die Open Security & Safety Alliance (OSSA) gegründet, um Standards und Spezifikationen für IoT-Anwendungen in der Sicherheitstechnik zu entwickeln. Frau Rückert, wie weit ist das mittlerweile gediehen?

Tanja Rückert: Im Rahmen der herstellerübergreifenden Open Security & Safety Alliance haben wir mit den anderen Partnern gemeinsame Standards und Spezifikationen für ein offenes Kameraplattformkonzept im Bereich Videosicherheit definiert. Bis heute hat sich bereits eine ganze Reihe namhafter Kamerahersteller angeschlossen, von denen viele bereits auf dem Markt erhältliche „Driven by OSSA“-Kameras herausgebracht oder angekündigt haben. Auch andere Branchenakteure, insbesondere Systemintegratoren, sind an diesem Ökosystem interessiert und

haben sich angeschlossen. Gleichzeitig weitet diese systemoffene Allianz nun ihren Geltungsbereich über den Bereich Videosicherheit hinaus aus und befindet sich hierzu bereits in fortgeschrittenen Gesprächen. Alles in allem führt dies dazu, dass aktuell etwa 40 führende Unternehmen im Rahmen von OSSA zusammenarbeiten, um Innovation – weit über die Grenzen jeder einzelnen Organisation hinaus – in der Sicherheitsbranche voranzutreiben.

Hartmut Schaper: Wir, die „Security & Safety Things GmbH“, kurz S&ST, haben auf Basis der OSSA-Standards ein offenes Betriebssystem entwickelt, den beteiligten Herstellern zur Verfügung gestellt und einen Application Store geschaffen. Dort können Kunden und Integrierte Softwareanwendungen für verschiedene Anwendungszwecke und Branchen kaufen und flexibel auf Kameras laden, die das S&ST Betriebssystem einsetzen. Das funktioniert ähnlich wie bei Apps für Smartphones.

Herr Schaper, was ist das Neue, das S&ST mit seinem Konzept für die Endkunden ermöglicht?

Hartmut Schaper: Hier sind drei wesentliche Punkte zu nennen. Erstens reduziert sich die Abhängigkeit von Hardware und Software, da unterstützte Kameras über unseren Application Store flexibel mit Software-Apps für verschiedene Videoanalyse-Anwendungsfälle ausgestattet werden können, so wie Sie Ihr Smartphone verschiedene Aufgaben erledigen lassen können, indem Sie mehrere Apps darauf installieren.

Zweitens kann jede Kamera, die unser Betriebssystem nutzt, mehr als eine Anwendung parallel ausführen. Haben Kunden früher meist je Videoanalyse-Anwendung eine eigene Kamera gebraucht, können sie nun verschiedene Anwendungen parallel auf einem Gerät laufen lassen. Zum Beispiel kann Nummernschilderkennung unkompliziert mit der automatischen Erkennung der Fahrzeugfarbe und des Automodells kombiniert werden, um so umfassendere und tiefere Analysen durchzuführen.

Drittens, und das ist wohl am wichtigsten, können diese Kameras zu jedem Zeitpunkt mit neuen Apps ausgestattet und so leistungsfähiger gemacht oder für völlig neue Zwecke eingesetzt werden. Man kann also die Funktion einer solchen Kamera über die Anwendungen, die man auf ihr installiert, flexibel über ihre Lebensdauer hin anpassen, damit sie ihren spezifischen Zweck am besten erfüllt.

Wie kann das in der Praxis aussehen?

Hartmut Schaper: Nehmen wir ein Beispielenario mit direktem Bezug zur Pandemie: Ein Elektronikmarkt schafft sich mehrere Kameras mit unserem Betriebssystem an. Vor Beginn der Pandemie platziert er einige an den Ladeneingängen, um eintretende Kunden zu zählen, andere wiederum rüstet er – oder sein Integrationspartner – mit anderen Apps aus, um auf der Ladenfläche Kundenwege zu analysieren und gleichzeitig leere Regale zur Befüllung zu melden. Wiederum andere werden so ausgestattet, dass sie mögliche Diebstähle oder Unfälle – wie eine gefallene Person – erkennen und an das Personal melden. Wenn dann aufgrund der Pandemie neue Gesundheitsrichtlinien umzusetzen sind, kann der Kunde durch den Application Store binnen weniger Tage seine Kameras an den Eingängen so anpassen, dass sie zusätzlich zur Zählung der Kunden auch das Tragen von Gesichtsmasken überprüfen. Kameras auf der Fläche können jetzt mit Apps ausgestattet werden, die Gruppenbildung erkennen und das Personal darauf hinweisen.

Zu erwähnen ist auch, dass das Angebot im Application Store ständig wächst. Selbst, wenn eine benötigte Anwendung noch nicht vorhanden ist, kann diese entwickelt und binnen Wochen verfügbar gemacht werden, je nach Komplexität. In solchen Fällen vermitteln wir auch zwischen App-Entwicklern, Integrierten und Endkunden. Unsere Entwicklungspartner sind sehr daran interessiert, für unsere Plattform und damit für eine globale Klientel zu entwickeln. Genau deswegen sind wir davon überzeugt, dass in Zukunft immer

mehr Anwendungen immer schneller in den Application Store kommen werden.

Bosch Building Technologies ist einer der Partner, die bereits mit dem Betriebssystem von S&ST arbeiten. Frau Rückert, sind zukünftig alle Bosch-Kameras damit ausgestattet und können somit die Apps nutzen?

Tanja Rückert: Wir haben gerade unsere Bosch-Kameraplattform „Inteox“ entwickelt. Als vollständig offene Kameraplattform kombiniert Inteox die intelligente Videoanalyse von Bosch mit dem offenen Betriebssystem von S&ST. Somit haben unsere Kunden auch Zugriff auf den Application Store von S&ST und folglich die Möglichkeit, Softwareanwendungen nach Bedarf hinzuzufügen. Mit einigen unserer Key-Kunden sind wir hier bereits dabei, Pilotprojekte zu realisieren, um weitere Praxiserfahrung zu sammeln. Um den unterschiedlichen Kundenwünschen zu entsprechen, werden zunächst die beweglichen Inteox-Kameras, sprich Mic und Autodome, und Anfang nächsten Jahres die fest installierten Kameras, also Dinion und Flexidome, angeboten.

An welche Zielgruppe bei Anbietern und Anwendern richtet sich das Inteox-Angebot und welche Applikationen stehen schon zur Verfügung?

Tanja Rückert: Durch die stetig wachsende Vielfalt der Softwareanwendungen im Application Store können Bosch-Integratoren bei Projekten viel flexibler als bisher auf Kundenwünsche eingehen. Gibt es bei der Installation von Kameras besondere Anforderungen, die mit der Standardausstattung der Inteox-Kameras nicht erfüllt werden, können wir die entsprechende Softwareanwendung über den Application Store zur Verfügung stellen oder sogar Softwarepartner hinzuziehen, um selbst für ganz spezielle Anforderungen die passende Lösung zu entwickeln. Zum Beispiel im Eingangsbereich, wie Herr Schaper schon ausführte, wo wir je nach Bedarf mehrere Apps mit unserer intelligenten Videoanalyse kombinieren können. Durch unser Inteox-Angebot können wir unser Anwendungsspektrum also deutlich erweitern.

Wie entwickeln sich Ihr offenes Betriebssystem und der Application Store, Herr Schaper?

Hartmut Schaper: Mehr als 30 App-Development-Firmen haben bereits über 70 Apps für Kameras entwickelt, die unser Betriebssystem nutzen – das macht unseren Application Store zum am schnellsten wachsenden Marktplatz für Kamera-Apps. Diese können wir derzeit in 19 Ländern anbieten und werden kommendes Jahr weitere hinzufügen. Dies in Verbindung mit den Kameras, die bereits erhältlich sind oder noch in diesem Jahr von sieben Herstellern erwartet werden, zeigt eindeutig, dass der Markt die Idee unserer Plattform angenommen hat. Tatsächlich werden Kameras mit entsprechenden Apps auch schon gewinnbringend von Kunden eingesetzt, beispielsweise im Kontext von „Retail Analytics“ oder „Parking Management“, um zwei konkrete Anwendungsfelder zu nennen.

Im nächsten Schritt möchten wir unser Ökosystem ausweiten und weitere Partner an Bord holen. Und da wir uns als Plattform für Innovation verstehen, suchen wir auch immer nach neuen spannenden Anwendungsfeldern für Videoanalyse, die von künstlicher Intelligenz gestützt wird. Dies geht dann häufig über die traditionellen Domänen von Security und Safety hinaus. Wir sehen hier Anwendungsfelder in ganz neuen Bereichen, wie beispielsweise in der Produktion, im Gesundheitswesen, in der Landwirtschaft oder durch die Verbesserung des Zuschauererlebnisses in Sport und Unterhaltung. In solchen Bereichen kann Analyse „at the edge“ innovative KI-Lösungen bieten und gleichzeitig die Privatsphäre viel besser schützen.

Tanja Rückert: Die von Herrn Schaper angesprochene Analyse der Daten im Gerät „at the edge“ unterstützen wir ausdrücklich. Bei Bosch Building Technologies ist diese Technologie bereits seit einiger Zeit in allen unseren Kameras Standard und wird von unseren Kunden auch erfolgreich eingesetzt. Wir bieten jedoch auch cloudbasierte Analytics an, je nach Einsatzzweck und Anforderung des Kunden.

Frau Rückert, wie lautet Ihre Erfolgsformel für das richtige Verhältnis von Differenzierung und Systemoffenheit im Wettbewerb um Marktanteile?

Tanja Rückert: Der Kuchen ist groß genug für uns alle. Mit gemeinsamen Standards und einer stetig wachsenden Zahl attraktiver Lösungen wird er sogar noch größer, weil wir nicht nur einen deutlichen Mehrwert in Puncto Sicherheit schaffen, sondern auch dazu beitragen, komplexe Prozesse zu optimieren. Davon werden unterschiedlichste Branchen profitieren.

Dennoch muss es weiterhin für jeden Hersteller die Möglichkeit geben, sich zu differenzieren. Unsere standardmäßig eingebaute, intelligente Videoanalyse von Bosch ist nach wie vor integraler Bestandteil unserer Inteox-Kameras – und bleibt damit ein wesentliches Differenzierungsmerkmal. Wir werden auch weiter bei der Produktentwicklung im Hard- und Softwarebereich an hohen Sicherheitsstandards festhalten.

Dies alles, verbunden mit einem offenen Ökosystem, macht Inteox aus. Ein offenes Ökosystem ist wesentlich attraktiver für die Community der App-Entwickler, als es jemals ein einzelner Hersteller sein kann. Somit können wir Kunden aus verschiedensten Branchen einen großen Mehrwert bieten – sowohl im Bereich Sicherheit als auch darüber hinaus.

Wir danken für das Gespräch!

**Automated
Valet Parking:
Der fahrerlose
Parkservice**



Kontakt

Bosch Building Technologies
Grasbrunn
Tel.: +49 89 6290 0
info.service@de.bosch.com
www.boschsecurity.com
www.boschbuildingtechnologies.com

BRANCHENGESPRÄCH

Ein Errichter für Errichter

Im Interview mit den Geschäftsführern der TAS: Warum das Modell der plattformbasierten Fernzugriffe auf Alarmsysteme die Zukunft ist

Cloud- bzw. plattformbasierte Lösungen sind in der IT eine Selbstverständlichkeit, nicht so im Bereich der klassischen Sicherheitstechnik. Erst allmählich setzt sich auch hier der Gedanke durch, Gefahrenmeldeanlagen nicht mehr als nur rein technische Systeme zu betrachten, die man vor Ort errichtet. „Sicherheit als Service“ rückt zunehmend in den Fokus. Aber was heißt das konkret? Und welche Vorteile sind damit verbunden? GIT SICHERHEIT hat bei den beiden Geschäftsführern der TAS Sicherheits- und Kommunikationstechnik, Frank Lisges und Stephan Holzem, nachgefragt.



GIT SICHERHEIT: Die TAS ist bisher als bundesweiter Anbieter für klassische Sicherheitstechnik bekannt. Sie planen und errichten sicherheitstechnische Anlagen für Industriekonzerne, Behörden, Banken und Filialisten wie Tankstellen und Möbelhäuser. Wie sehen Sie die Entwicklung in der Sicherheitstechnik? Und an welchen Konzepten arbeiten Sie?

Frank Lisges: Nicht nur Sicherheitsgewerke wie z. B. Videoüberwachung und Zutrittskontrolle wachsen zu einer Lösung zusammen, alle Sicherheitsgewerke sind zunehmend miteinander vernetzt und eingebunden in die Gebäudeleittechnik. Hier braucht es als Planer und Errichter sowohl IT- als auch Datenschutz-Know-how. Die Konvergenz von Systemen bedeutet dabei nicht immer mehr Einfachheit. Im Gegenteil, die Komplexität nimmt zu. Reichte es früher, Gebäude abzusichern, unterstützen wir heute Prozesse. Das stellt hohe Anforderungen an Errichter.

Ein weiterer „Trend“ sind plattformbasierte Dienste, die Kunden gegen monatliches Entgelt zur Verfügung gestellt werden – ähnlich zu betrachten wie die bekannten Software-Lizenzmodelle. Hier ändert sich aktuell der Markt rasant. Die Sicherheitstechnik wird zunehmend automatisiert und digital.

Stephan Holzem: Ich möchte das gerne an einem Beispiel erläutern. Seit knapp zwei

Jahren bieten wir mit unserer TAS Secure Platform einen sicheren Fernzugriff (Remote Access) auf Alarmübertragungseinrichtungen und nachgeschalteten Gefahrenmeldeanlagen an. Über die Plattform lassen sich Services wie z. B. Monitoring und Fernwartung von Anlagen sowie Software-Updates von Alarmübertragungseinrichtungen realisieren. Unser Ansatz ist es dabei, die Alarmübertragung ähnlich wie einen Paketservice zu gestalten: Per App kann man komfortabel den Zustand seiner sicherheitstechnischen Anlage verfolgen – egal, wo man sich befindet.

Frank Lisges: Wir nutzen die Secure Platform nicht nur für unsere Kunden in unserem eigenen Service Center, sondern bieten Sie auch anderen Errichtern an. Gerade Großkunden und Filialketten haben ja meist mehrere Partner in diesem Bereich. Zusammenarbeit und Austausch werden hierbei immer wichtiger. Insellösungen sind passé.

Wird die Secure Platform bereits in der Praxis genutzt?

Frank Lisges: Aber ja! So werden die Zugriffe von Servicetechnikern auf die Sicherheitsgewerke von Konzerngesellschaften und deren zig Zweigstellen in Deutschland über die Plattform geregelt und verwaltet. Zu den Gewerken gehören u. a. Einbruch- und

Brandmeldeanlagen, Zutrittskontrolle und Videoüberwachungssysteme. Das ist ein besonderer Vorteil der Plattform: Sie ist flexibel – verschiedenste Alarmsysteme können aufgeschaltet werden. Über die Plattform werden die Massen-Software-Updates von Alarmübertragungseinrichtungen gefahren, sodass diese immer auf dem aktuellen Stand sind. Zudem nutzen der Kunde und seine Errichter die Plattform für das Monitoring und die Fernwartung der Systeme.

Auch hier zeigt sich übrigens wiederum die Flexibilität der Plattform. Der sichere Fernzugang – also der Remote Access – ist ein Basisdienst. Alle anderen Services sind zubuchbare Module.

Welche Vorteile haben Monitoring und Fernwartung von Alarmsystemen?

Frank Lisges: Durch das Monitoring lassen sich mögliche Probleme an der Anlage feststellen bzw. eingrenzen, oft bereits lange vor einer Störung oder einem Ausfall der betreffenden Komponenten. Damit können Servicetechniker wesentlich effektiver eingesetzt werden. Sie sind vorbereitet und haben das richtige Werkzeug zur Hand. Unnötige Fahrten werden vermieden. Übrigens auch dadurch, dass Wartungen aus der Ferne durchgeführt werden. Dieses „Remote Maintenance“ ist in anderen technischen Bereichen schon länger

üblich, die Sicherheitstechnik hinkt hier noch ein wenig hinterher. Das hat aber auch seinen Grund: Wir bewegen uns hier schließlich in einem sensiblen Bereich mit hohen Anforderungen an die Sicherheit.

Stichwort „Sicherheit“ – ist eine solche Plattform nicht Einfallstor für Cyber-Angriffe?

Stephan Holzem: In Zeiten zunehmender Cyberkriminalität wäre es extrem fahrlässig, einen direkten Zugang zu einer Anlage zu realisieren – ohne ein durchdachtes Gesamtkonzept. Dabei geht es um mehr als sichere Verschlüsselungstechnologien und weiteren Mechanismen zur Datensicherheit. Diese alle aufzuzählen, würde hier den Rahmen sprengen. Die Plattform gewährleistet höchste Sicherheitsstandards, aber was wir auch im Blick haben, ist ein sicheres Gesamtkonzept. Es muss klar geregelt sein, wer die Verantwortung für welche Teile der Infrastruktur hat. Das ist alles andere als trivial.

Stellen Sie sich die Brandmeldeanlage einer Schule vor. Diese ist auf die zuständige Feuerwehr aufgeschaltet. Allein hier gibt es drei Verantwortungsbereiche:

- Die Sicherheit der Alarmverbindung liegt in der Verantwortung des „Anbieters für den Alarmübertragungsdienst“ (ATSP). Dieser muss jederzeit die Zustände aller Verbindungen kennen und bewerten. Dazu sind in der gesamten Kette auch regelmäßige Updates bzw. Sicherheitspatches nötig.
- Der Betrieb der Brandmeldeanlage selbst liegt in der Verantwortung des zuständigen Errichters. Im Störfall muss dieser 24/7 auf die Anlage zugreifen können, um Fehlerzustände zu bewerten. Wartungs- und Störeinätze können durch den Fernzugriff effektiv vorbereitet werden.
- Auch die Hersteller der Anlagen selbst sind an einem direkten Zugriff auf die Anlagen interessiert, um Dienstleistungen anzubieten. Beispielsweise kann das Alter und der Verschmutzungsgrad von Meldern überwacht und im Bedarfsfall dem Errichter bzw. dem Endkunden gemeldet werden.

Wie stelle ich mir das dann in der Praxis vor? Installiert dann jeder der drei genannten Verantwortungsträger seinen eigenen Fernzugriff?

Stephan Holzem: Genau hier liegt das Problem. Wie soll ein ATSP (Anbieter für Alarmübertragungsdienste) die Sicherheit der Anlage verantworten, wenn Errichter und Anlagenhersteller mit eigenen Routern direkt auf die Anlage zugreifen?! Im Störfall oder bei einem Cyberangriff wird jeder die Verantwortung auf den anderen abschieben. Mal ganz abgesehen davon, dass es wirtschaftlich keinen Sinn machen kann, wenn jeder seine eigenen Router und Netze an die Anlage anbindet, obwohl mit der Übertragungstechnik

bereits hoch verfügbare und redundante Netze vorhanden sind. Ein weiterer Punkt. Ein direkter Fernzugriff auf eine sicherheitstechnische Anlage wird normativ nicht mehr zulässig sein. Hier entstehen gerade neue Normen: die TS 50136-10 für Remote Access und EN 50710 für Remote Services. Bis dato war der Fernzugriff ein unklar geregelter Bereich mit Haftungsrisiken für den Betreiber von sicherheitstechnischen Anlagen.



Es muss klar geregelt sein, wer die Verantwortung für welche Teile der Infrastruktur hat.“

Stephan Holzem

So einfach ist also der Fernzugriff nicht zu realisieren. Aber wie sieht dann Ihre Lösung dazu aus?

Stephan Holzem: Wenn wir unsere Secure Platform zur Verfügung stellen, sind wir – die TAS – in der Rolle des sog. Remote Access Infrastructure Service Provider (RAISP). Wir stellen nicht einfach nur die Infrastruktur unseren Kunden wie Leitstellen-Betreibern und Errichterfirmen zur Verfügung, sondern sind verantwortlich für den Aufbau und die Sicherheit der Fernzugriffsinfrastruktur und damit für die IT-Sicherheit der Plattform und sämtlicher Komponenten.

Frank Lisges: Und wir nehmen eine Risikobewertung vor, z. B. zur Lage der Objekte, Anforderungen des Auftraggebers oder geltende Richtlinien für die Anlagen im Anwendungsbereich – um nur einige zu nennen. Auch die Einhaltung der Datenschutz-Richtlinien gehört dazu. Für dieses Gesamtpaket braucht es schon sehr viel Know-how.

Ich übertreibe nicht, wenn ich sage: Mit der TAS Secure Platform und dem gesamten Dienstleistungspaket, das sich darüber abwickeln lässt, haben wir als Unternehmen für Sicherheits- und Kommunikationstechnik ein Alleinstellungsmerkmal. Sie ist ein konkretes Beispiel für das, was ich eingangs sagte: Errichter übernehmen zunehmend Prozessverantwortung und „Sicherheit als Service“ ist ein Zukunftsmodell. ■

Kontakt

Telefonbau Arthur Schwabe
Mönchengladbach
Tel.: +49 2166 858 0
info@tas.de
www.tas.de



Kontaktlose hygienische Zutrittskontrolle

Im Zeitalter der Digitalisierung ermöglicht PCS vernetzte Lösungen für maximale Gebäudesicherheit: Biometrie für höchste Sicherheitsansprüche, Zutrittskontrolle mit RFID-Verfahren, mechatronische Türterminals – orchestriert über die Softwareplattform DEXICON. Erweitert um Video- und Besuchermanagement. Der Anschluß an das Gefahrenmanagementsystem sorgt im Alarmfall für schnelle Übersicht.

Als Spezialist für unternehmensweite Gebäudesicherheit entwickelt und produziert PCS seit mehr als 40 Jahren innovative, ausgezeichnete Premium-Produkte.

Geben Sie uns grünes Licht als Ihr Lösungspartner für unternehmensweite Gebäudesicherheit.

Besuchen Sie uns
KonMeGA virtuelle Messe
für Gebäudeautomation
23.03. - 24.03.2021

+49 89 68004-0
www.pcs.com





Barox-Switche schützen Sicherheitsnetzwerke und Geräte von Drittanbietern vor Ripple20-Cyberangriffen

SICHERHEITSNETZWERKE

Innere Sicherheit

Barox-Switche schützen Sicherheitsnetzwerke und Geräte von Drittanbietern vor Ripple20-Cyberangriffen

Ripple20 heißt eine Reihe von 19 Schwachstellen in einer Low-Level-TCP/IP-Softwarebibliothek. Dies stellt eine unmittelbare Bedrohung für viele Produkte dar: Die Aktivierung kann es Angreifern aus der Ferne ermöglichen, die vollständige Kontrolle über die Zielgeräte zu erlangen, ohne dass eine Interaktion des Benutzers erforderlich ist. Switche der RY-28 Managed Ethernet-Reihe von Barox können so konfiguriert werden, dass sie Sicherheitsnetzwerke und Geräte von Drittanbietern, wie Kameras und Server, vor Ripple20-Cyberangriffen schützen.

Vor kurzem vom JSOF-Forschungslabor entdeckt, handelt es sich bei Ripple20 um eine Reihe von mehreren Zero-Day-Schwachstellen in TCP/IP-Stacks, die weltweit in IoT-Geräten weit verbreitet sind. Die Schwachstelle ist in einem proprietären, voll ausgestatteten TCP/IP-Kommunikations-Stack zu finden, der für eingebettete Geräte und Echtzeitbetriebssysteme entwickelt wurde. Als grundlegendes Netzwerkelement ist dieser Stack ein Baustein für jedes Gerät, das über ein Netzwerk

funktioniert. Das weltweite Problem besteht darin, dass nicht bekannt ist, welche eingebetteten TCP/IP-Stacks verwundbar sind. Die betroffenen IoT-, USB- und Server-Geräte sind weit verbreitet, bis hin zu Druckern, Glühbirnen und Smart Metering.

Milliarden Geräte gefährdet

In kürzlich veröffentlichten Hacker-Nachrichten hieß es, dass Ripple20-Fehler „Milliarden von Geräten mit Internetanschluss dem Risiko des Hackens

3 Fragen an ...

... Produktmanager Dieter Hiestand von Barox Kommunikation

GIT SICHERHEIT: Herr Hiestand, Videonetze müssen vor Cyber-Angriffen geschützt werden – das ist die Spezialität von Barox.

Wie schätzen Sie die gegenwärtige Bedrohungslage ein?

Dieter Hiestand: Bis Anfang des Jahres 2020 waren die meisten Bedrohungen innerhalb der Firmen zu verzeichnen. Mit der Covid-19-Pandemie hat sich allerdings einiges geändert. Durch die vielen Homeoffice-Lösungen wird eine neue Dimension der Angriffe auf die Firmennetze eröffnet. Angriffe auf VPN-Tunnels gab es schon immer, aber deren Anzahl ist stark gestiegen. Zudem sind auch häufiger Rechner in den Netzen, die sowohl privat als auch für die Firma genutzt werden. Dies vor allem bei kleineren Firmen. Diese Tatsache bedingt auch in den privaten Netzwerken viel effizientere Schutzmaßnahmen.

Insbesondere um den Schutz von Netzwerken vor den Ripple20-Schwachstellen geht es bei den neuen Barox-Switchen der RY-28 Managed Ethernet-Reihe. Wie wird das erreicht?

Dieter Hiestand: In der neusten Switch-Generation haben wir eine starke ACL (Access Control List) eingebaut. Hier können wir sehr feine Filter für das interne



Netzwerk einsetzen. So auch für fragmentierte Pakete und Schadsoftware. Allerdings müssen solche Einstellungen von einem Fachmann durchgeführt werden.

Worin liegen die wesentlichen Neuerungen?

Dieter Hiestand: Bei den 28xx-Switchen wurde ein komplett neues Hardware-Design verwendet. Es gibt ein neues Bedienkonzept auf vertrautem GUI. Außerdem wurden Konfiguration und Monitoring zusammengelegt. Dies bedeutet wesentlich weniger Mausklicks bei einer Konfiguration, also effizienteres Arbeiten. Non-Stop-PoE ist ein weiteres Feature: Ohne Verlust der Power-Over-Ethernet-Leistung kann der Switch neu gestartet werden. Das heißt bei einem Firmware-Update muss nicht die gesamte Anlage neu gestartet werden. Dies ist sehr hilfreich bei größeren Kamerainstallationen. Außerdem zu nennen: Das ERPS-Protokoll für eine schnelle Umschaltung in redundanten Installationen; verbesserte ACL für den Schutz des privaten internen Netzwerkes sowie ein kontrolliertes Firmware-Upgrade via Device Management System.

aussetzen“. Das von Treck in den USA entwickelte Ripple 20 wurde in Produkten für Haushalte und Verbraucher ebenso wie für Unternehmen, Telekommunikation, Nuklear-, Transport- sowie Öl- und Gasgeräte in kritischen Infrastrukturen entdeckt, wobei eingebettete Echtzeit-Protokolle und eingebettete Geräte bereits seit 1997 verwendet werden. Darüber hinaus konnte eine einzelne Komponente infiltriert werden, um auf andere Netzwerkgeräte überzugreifen. Geräte können auf Fehlfunktionen eingestellt werden, wobei große internationale Anbieter betroffen sein können.

Rudolf Rohr, Mitbegründer und geschäftsführender Gesellschafter von Barox, erläutert das Problem aus dem Blickwinkel von Sicherheitsinstallateuren und Systemdesignern: „Um Geräte und Netzwerke vor Ripple20-Schwachstellen zu schützen, muss ein zweckspezifischer Filter so konfiguriert werden, dass er niemals fragmentierte UDP akzeptiert“.

Mit dem Barox-Switch der RY-28-Serie, so Rohr, könne Deep Cyber Protection so konfiguriert werden, dass fragmentiertes UDP automatisch erkannt und über die integrierten ACL-Switch-Menüoptionen gestoppt wird, so dass fragmentiertes UDP blockiert und Netzwerke und ihre Geräte wie IP-Kameras, VMS und Server vor illegalem Zugriff geschützt werden.

Es sei auch wichtig, so Rudolf Rohr weiter, „eine Netzwerksegmentierung über den Switch zu schaffen. Mit dieser Abwehrmaßnahme mildert Barox die Auswirkungen und hilft Installateuren und Endbenutzern, ihre Netzwerksicherheitssysteme vor potenziellen Ripple20-Bedrohungen zu schützen“ ■

Kontakt

Barox Kommunikation GmbH
Lörrach
Tel.: +49 7621 1593 112
marie-christine.moeller@barox.de
www.barox.de

Mehr Sicherheit, einfachere Bedienung

Eine Reihe von Neuerungen der 28er Serie der RY-L-Switche von Barox sorgt für mehr Sicherheit und einfachere Bedienung. Neben den 10G-Uplinks (in Zeiten von 4K und mehr) gewährleistet das neu strukturierte GUI eine verbesserte Benutzerfreundlichkeit. Das Monitoring befindet sich jetzt im Bereich der Konfiguration und erspart einige Klicks. Das neue Non-Stop-PoE bestromt Kameras auch beim Neustart des Switches ohne Unterbrechung. Dadurch stehen die Kamerabilder sofort wieder zur Verfügung und der Anwender spart wertvolle Zeit.

Ergänzend zu den bisherigen Sicherheitsmerkmalen kann jetzt auch der Netzwerkverkehr gezielter abgesichert werden. So lassen sich etwa Protokolle der höheren Schichten wie z. B. HTTP oder Telnet unterbinden. Mit diesen starken Werkzeugen können ungewollte Unterhaltungen z. B. einer Kamera zu einem Spionageserver verhindert werden.



Für mehr Sicherheit und einfachere Bedienung sorgen viele Neuerungen der 28er Serie der RY-L-Switche von Barox

Absicherung von innen

In den Switchen befinden sich also immer mehr Firewall-Funktionen. Diese sichern das Netz von innen ab. Wo normale Firewalls nur die Verbindung in die Außenwelt kontrollieren, sind Barox-Switche im Inneren des Netzes aktiv und inspizieren den Datenverkehr. Ist dieser Datenverkehr atypisch für Video-Informationen, kann dieser unterbunden werden und somit eine innere Infizierung des Netzes (z. B. durch einen mitgebrachten Memory-Stick) verhindert werden.

Außerdem bietet die Serie mehr PoE-Leistung – was auch bei kleinen Switchen immer wichtiger ist, da zwischenzeitlich Kameras mit 90W erhältlich sind.



VIDEOÜBERWACHUNG

Videoanalyse

Was wir heute schon von der Technologie erwarten können

Cloud, Künstliche Intelligenz, Machine Learning, Deep Learning – diese Begriffe haben die meisten schon einmal gehört und glauben zu wissen, was sich dahinter verbirgt. Viele kommen in der Praxis aber schnell ins Schlingern, wenn solche Fachtermini erklärt und voneinander abgegrenzt werden sollen und welche Rolle sie bei der Videoanalyse spielen.

Wo KI draufsteht, ist meist keine echte KI drin

Künstliche Intelligenz (KI) ist ein weit gefasster Begriff, der erstmals 1956 in der Forschung auftauchte. Die meisten Menschen haben Ihre Vorstellung von KI aus der Popkultur. Sie denken an den Roboter, der Emotionen zeigen kann, oder Maschinen, die die Weltherrschaft übernehmen wollen. Aktuelle Beispiele für das, was viele als KI in

unserem Leben ansehen sind beispielsweise der Schachcomputer Deep Blue, der einen Top-Schachspieler schlägt, Siri, die jeden Song erkennt, oder Amazon, das Kunden immer ein neues Buch vorschlägt. In Wirklichkeit

sind dies aber Beispiele für immer kleiner werdende Computer, die eine Reihe von Algorithmen ausführen, riesige Datenbanken durchsuchen oder viele Berechnungen sehr schnell durchführen.

Der Begriff KI kann dementsprechend unpräzise sein und weckt

oftmals unrealistische Erwartungen. Obwohl Künstliche Intelligenz gerne als Marketing-Label genutzt wird, handelt es sich bei den aktuell am Markt für physische Sicherheit verfügbaren Technologien in den meisten Fällen um das sogenannte maschinelle Lernen (Machine Learning).

Machine Learning, Deep Learning, Self-Learning?

Machine Learning ist ein Teilbereich der Künstlichen Intelligenz. Computer werden dabei mit Daten gefüttert, die ihnen dabei helfen, ihre Leistung zu verbessern, ohne explizit programmiert zu werden. Beim statischen Programmieren erhalten Computer eine Reihe von Anweisungen, die sich im Laufe der Zeit nicht ändern. Beim Machine Learning hingegeben können Programmierer



Kay Ohse,
Regional Sales Director
Germany, Switzerland, Austria,
Eastern Europe

einen Computer in die Lage versetzen, seine Berechnungsprozesse durch Training zu bewerten und zu verändern.

Konkret heißt das: Ein Computer wird mit Algorithmen programmiert, mithilfe derer er selbst entscheidet, welche Merkmale er im Erkennungsprozess verwenden sollte, um das genaueste Ergebnis zu liefern. Vereinfacht ausgedrückt: Der Mensch bringt dem Computer bei, selbst zu erkennen, anhand welcher Kriterien er bestimmte Ereignisse, Prozesse oder Objekte klassifiziert.

Eine Form des Machine Learnings ist das sogenannte Deep Learning. Sie benötigt große Datenmengen, ist dafür aber in der Lage, ähnlich wie das menschliche Gehirn, Prognosen und Entscheidungen zu treffen und diese immer wieder mit neuen Daten abzugleichen und anzupassen. Typischerweise werden mit Deep Learning komplexere Modelle trainiert. Deep Learning kommt beispielsweise bei der Gesichtserkennung zum Einsatz.

Erfolgt ein andauernder, nicht aktiv überwachter Lernprozess durch das System, spricht man von Self-Learning. Diese Technologie existiert heute bislang nur in Ansätzen und ist aufgrund auch unerwünschter Ergebnisse und Entscheidungen umstritten.

Videoanalyse – alles vollautomatisch?

Ebenso verhält es sich beim Thema Videoanalyse. Bei der Entscheidung für eine Lösung, sollten Anwender genau überlegen, was sie tatsächlich benötigen. Wer viel „Intelligenz“ will, zahlt schnell horrenden Summen für die entsprechende Computerpower und Speicherkapazität, braucht für die spezifische Anwendung aber vielleicht gar nicht diesen Intelligenzgrad. Entscheidend ist also weniger die Intelligenz als vielmehr der gewünschte Automatisierungsgrad. Das Spektrum reicht von automatischer Erkennung, Bewertung und Analyse, bis hin zu automatisierter Entscheidungsunterstützung und automatisiertem Lernen. Daraus lässt sich eine Kernfrage ableiten: Wo soll der Schwerpunkt liegen?

Beim Thema Videoanalyse geht es vorrangig darum, Veränderungen und Muster zu erkennen. Das System arbeitet dabei entweder statisch, dynamisch oder anwendungsspezifisch. Je nach Intelligenz des Systems werden also lediglich Veränderungen in einem Bild aufgezeigt oder es werden Muster bzw. bestimmte Dinge „erkannt“. Dies geschieht durch Algorithmen, die in einzelnen Pixeln ein Muster erkennen und das Ergebnis entsprechend interpretieren.

Statische, dynamische oder anwendungsspezifische Videoanalyse

Bei der statischen Videoanalyse lernt das System ein Standardbild, auf dem es dann jede Veränderung erkennt, was anschließend eine vordefinierte Aktion (z. B. Alarm oder Speicherung der Aufnahme) auslöst. Um einem Fehlalarm vorzubeugen, werden zusätzliche Algorithmen als Filter eingesetzt, die z. B. erst ab einem bestimmten Ausmaß der Veränderung einen Prozess auslösen.

Die dynamische Videoanalyse dient vor allem der Erkennung sich bewegender Objekte. Neben der Anwesenheit eines Objekts oder Menschen, wird zusätzlich auch beispielsweise die Anzahl, Bewegungsrichtung und ggf. Geschwindigkeit erkannt. Eingesetzt wird diese Methode unter anderem bei Autos im Verkehrsfluss (z. B. um Falschabbieger zu erkennen), Personengruppen (z. B. zur Erkennung von Helm- oder Maskenträgern) sowie im Perimeterschutz.

Im Rahmen der anwendungsspezifischen Videoanalyse kommen spezielle, für die jeweilige Aufgabe optimierte Algorithmen zum Einsatz. Einen Algorithmus, der alles kann, gibt es nicht. Es gibt jedoch bereits Ansätze, dass das System erkennt, welcher

Bitte umblättern ▶

Jetzt unseren aktuellen
Prospekt anfordern!

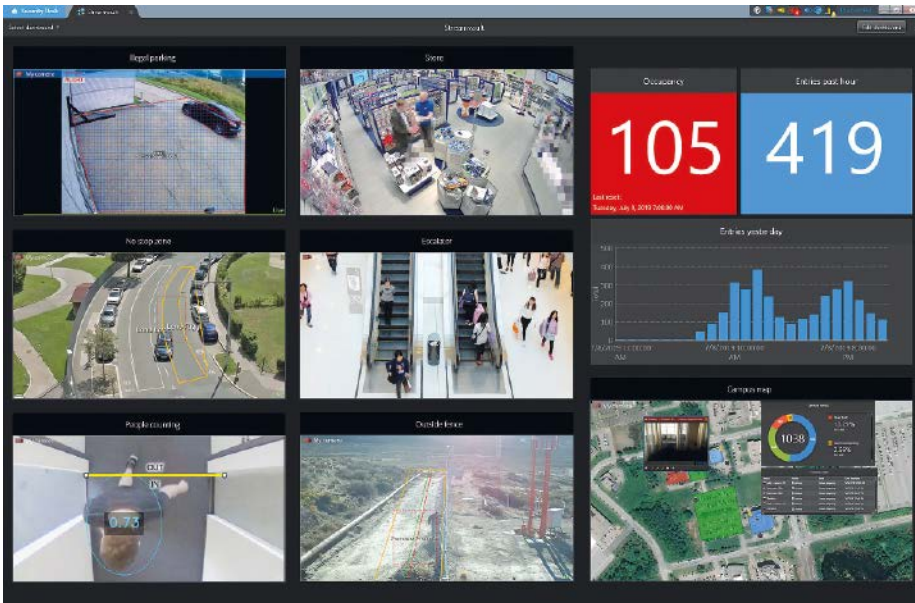
wanzl

Sensible Bereiche schützen

mit der smarten
Galaxy Gate 1.1

- Die elegante Zutrittsschleuse sorgt mit innovativer Sensorik für ein hohes Sicherheitslevel. Alle Prozesse können mit dem Access Manager via remote gesteuert werden. Binden Sie die Zutrittsanlage in Ihr Gebäudemanagement ein und behalten Sie stets die Kontrolle.

Access Solutions
www.wanzl.com
access-solutions@wanzl.com



„Videoanalyse unterstützt Sicherheitsverantwortliche bei der Arbeit“

Fortsetzung von Seite 35 ►

Algorithmus das beste, bzw. ein sinnvolles Ergebnis erzeugt. Anwendungsspezifische Videoanalyse kommt besonders bei der Personen- und Objektidentifikation oder bei der Analyse von Bewegungsmustern zum Einsatz.

Das Einsatzgebiet: Echtzeit oder Analyse gespeicherter Daten

Bei der Analyse unterscheidet man darüber hinaus eine Echtzeitanalyse und die Analyse „historischer“, also aufgezeichneter Daten. Werden Daten aus Videoanalyse-Systemen in Echtzeit genutzt, geht es vor allem um das sofortige Erkennen und die sofortige Reaktion. Diese muss angemessen und unmittelbar erfolgen. Wichtige Aspekte sind dabei Schnelligkeit und die Entlastung des Sicherheitspersonals. In kritischen Situationen sollen die Systeme anhand geeigneter Algorithmen Fehlalarme vermeiden und durch eine Kombination aus Alarmen und Aktionen die richtige Vorgehensweise unterstützen bzw. weitestgehend automatisieren. Dazu gehört auch, dass die Lösung in der Lage ist, Ereignisse in einem dynamischen Umfeld vorherzusagen und/oder operative Daten in die Analyse einzubeziehen (z. B. Wetter, Uhrzeit, zugelassene Personenzahl oder besonders kritische Objekte). All das muss der Software beigebracht werden und erfordert im laufenden Betrieb hohe Rechenleistung und Speicherkapazität. Teilweise sind solche Rechenoperationen bzw. Funktionalitäten bereits in Überwachungskameras integriert. Aber Vorsicht: Diese sind meist auf eine bestimmte Aufgabe fokussiert (Perimeterschutz ist nicht Brandschutz).

Kommt Videoanalyse vor allem nachträglich bei Aufzeichnungen zum Einsatz, sprechen wir von forensischer Suche. Dabei geht es vorwiegend um forensische Analysen bei Vorfällen sowie Auswertungen, um weitere

Erkenntnisse zu gewinnen, z. B. Muster zu erkennen und daraus die richtigen Schlüsse zu ziehen. Ein Anwendungsbeispiel ist die Analyse von Verkehrs- oder auch Kundenströmen. Hier werden intelligente Algorithmen und Lernsysteme eingesetzt, die Korrelationen bei Daten aus unterschiedlichen Quellen erkennen. Der Fokus liegt hierbei also auf der Verarbeitung großer und komplexer Datenmengen. Diese Aufgabe erledigen Rechner mit entsprechender Rechenkapazität besser als eine mit KI-Technologie ausgestattete Kamera.

Fazit: Nicht alles, was möglich ist, macht Sinn

Videoanalyse kann heute bereits sehr viel. Wer sich für den Einsatz eines solchen Systems entscheidet, sollte sich allerdings genau überlegen, welche Lösung für seine individuellen Anforderungen die richtige ist und vor allem die Wirtschaftlichkeit von Anfang an im Auge behalten. Dabei gilt die Faustregel: Je intelligenter ein System sein soll desto teurer wird es. Sollen mehr Daten verarbeitet werden, ist mehr Rechenkapazität notwendig und eine intelligente, datenintensive Echtzeitanalyse treibt den Preis schnell in die Höhe. Nicht immer ist das für den täglichen Betrieb aber notwendig. Egal, für welche Lösung man sich entscheidet, sie muss vor allem wirtschaftlich gerechtfertigt sein. Je nach individuellem Anforderungsprofil kann es dann auch sinnvoll sein, über eine zentrale Sicherheitsplattform nachzudenken, die einen flexiblen, herstellerunabhängigen Einsatz von Endgeräten und Hardware ermöglicht. ■

Kontakt

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

Sicherung von Zugdepots durch intelligente Videoanalyse

Southeastern Rail Network, eines der größten Bahnunternehmen Großbritanniens in öffentlicher Hand, setzt jetzt auf eine intelligente Videosicherheitslösung von Bosch. Mit dieser werden zwölf Zugdepots, darunter fünf unbemannte Standorte, gegen Diebstahl und unbefugten Zutritt geschützt. Das digitale Videosystem stellt eine bedeutende Verbesserung der Sicherheit für das britische Bahnunternehmen dar, das Zugverbindungen zwischen London, Kent und Teilen von East Sussex anbietet und an jedem Wochentag 640.000 Passagiere in seinen 392 Zügen befördert. Kernstück der Sicherheitslösung sind Kameras mit integrierter intelligenter Videoanalyse. Die Lösung wurde vom Bosch-Integrationspartner Taylor Technology Systems innerhalb von sechs Monaten installiert und entsprechend den spezifischen Anforderungen der Zugdepots konfiguriert.



Bosch sichert unbemannte Zugdepots von britischem Bahnbetreiber

Das über zwölf Standorte verteilte System nutzt maschinelles Lernen und Algorithmen, um bei einer Bedrohungslage wie dem unbefugten Eindringen auf das Gelände oder in eine Anlage automatisch Alarme auszulösen. Neben diesen Sicherheitsanwendungen werden über die Kameras auch Metadaten zu den Ankunfts- und Abfahrtszeiten der Züge generiert und ausgewertet. Die in den zwölf Depots neu installierten Kameras ersetzen eine analoge Lösung durch IP-basierte Kameras der Serien Flexidome, Dion und Autodome. Bei diesen Kameras ist die intelligente Videoanalyse (IVA) bereits vorinstalliert. Dadurch wird es möglich, die Videobilder exakt entsprechend den Sicherheitsanforderungen der Zugdepots auszuwerten. Da die Sicherheit bei Nacht besonders in den fünf unbemannten Zugdepots von großer Bedeutung ist, sind die Kameras mit der Starlight-Technologie des Unternehmens ausgestattet. Damit können Videobilder auch nachts und bei schlechten Lichtverhältnissen ohne Einschränkungen ausgewertet werden.

www.bosch.com ■

GIT

ZUTRITT

& SMART BUILDING

INNENTITEL

HEFT IM HEFT

Mit Innentitel: Elektronische
Zutrittsorganisation mit passivem,
schlüsselbetätigtem System und
virtuellem Netzwerk

Seite 38





INNENTITEL: ZUTRITTSORGANISATION

Allrounder für die intelligente Gebäudeorganisation

Maßgeschneiderte Lösungen für öffentliche Bauten

Für die flexible Verwaltung von Liegenschaften der öffentlichen Hand bieten sich elektronische Schließsysteme an. Denn damit können Änderungen in der Organisationsstruktur schnell und kostengünstig umgesetzt werden. Geeignete Technologien verfügen über ein breites Programm, das vielfältige Möglichkeiten eröffnet, individuell auf das Objekt zugeschnittene Konzepte zu realisieren.

Ein solches System ist beispielsweise die von Winkhaus entwickelte Zutrittsorganisation blueSmart. Viele Städte und Kommunen in Deutschland und Europa nutzen bereits die intelligente Lösung von Winkhaus.

Dieses Schließsystem verknüpft auf innovative Weise die Vorteile von Offline- mit dem Nutzen von Online-Lösungen. Denn es kommuniziert in einem virtuellen Netzwerk. Damit steigert sie die Effizienz der elektronischen Schließanlage und unterstützt den wirtschaftlichen Gebäudebetrieb. Darüber hinaus leistet das System auch einen Beitrag zur Hygiene.

Maximaler Komfort und besonders hohe Flexibilität für den Anwender stehen im Fokus der intelligenten Lösung. Einmalig ist die Kombination als passives,

schlüsselbetätigtes System, das seine Daten mittels virtuellem Netzwerk kommuniziert. Die Technologie kann auch in bestehende Systeme wie Gebäudeleittechnik, Zeiterfassung, Kantinenabrechnung oder Alarm- und Energiemanagement eingebunden werden.

Komponenten bilden virtuelles Netz

Das virtuelle Netzwerk funktioniert offline und drahtlos zwischen den installierten elektronischen Komponenten, die miteinander kommunizieren. Im Gegensatz zu konventionellen Netzen entfallen aufwendige Verkabelungen, eine Vielzahl von Umsetzern oder störanfällige Funkstrecken. Mit blueSmart können Schließanlagen mit bis zu 195.000 Komponenten realisiert werden. Dabei ist die Anlage schnell und

unkompliziert installiert, denn bei Nutzung dieses virtuellen Netzwerks ist nur der Aufbuchleser - also die Systemkomponente, die sowohl mit der Software als auch mit den Identifikationsmedien wie Schlüssel oder Karte kommuniziert - konventionell zu verkabeln.

Passiver Schlüssel

Informationen zwischen den elektronischen Zylindern überträgt das System schnell und kabellos. Überträger ist der blueSmart Schlüssel. Der aus Hochleistungskunststoff gefertigte Schlüssel ist wasserdicht (IP 68) und wartungsfrei und trägt einen RFID-Chip im Inneren, der sowohl programmierte Transaktionen als auch aus Türkomponenten ausgelesene Daten transportiert.

© Bild: Winkhaus



◀ Die elektronischen blueSmart Zylinder haben die gleichen Maße wie mechanische Zylinder und brauchen nicht verkabelt zu werden. Daher entfallen beim Umrüsten aufwändige Umbauten von Türen

Auch an Trafostationen kann die elektronische Schließanlage integriert werden ▼

© Bild: Winkhaus



© Bild: Winkhaus

Im Alltag öffentlicher Einrichtungen bewährt: Elektronische Zutrittsorganisation blueSmart von Winkhaus - das passive, schlüsselbetätigte System kommuniziert seine Daten mittels virtuellen Netzwerks

Mit handlichem Format und farbigem Touch-Display punktet die neue Generation Programmiergeräte BXP BS von Winkhaus ▼

Kompakte Zylinder

Die elektronischen Türzylinder haben die gleichen Maße wie mechanische Zylinder und brauchen nicht verkabelt zu werden, so dass bei der Installation aufwändige Umbauten von Türen entfallen. Auch lassen sie sich bedienen wie traditionelle mechanische Zylinder. Der elektronische blueSmart Schlüssel wird in den Zylinder hineingesteckt und gedreht.

Lange Batteriestandzeiten gewährleisten auf Dauer den zuverlässigen elektronischen Betrieb. Daher ist der Wartungsaufwand sehr gering. Auch der Ereignisspeicher der Zylinder ist deutlich größer als bei bisherigen Systemen. So können z.B. im Falle eines Diebstahls die letzten 2.000 Schließereignisse mit Datum und Uhrzeit angezeigt werden.

Winkhaus bietet für die unterschiedlichsten Türen passende Zylinder: Dazu gehören Doppel- und Halbzylinder ohne Knauf, Vorhängeschlösser sowie Zylinder für Spind- oder Schranktüren. Zudem enthält das Programm Knauf-, Doppelknauf- und Knaufhalbzylinder, die anstelle von Schlüsseln auch mit Karten betätigt werden können.

Hygienisches Türöffnen

blueSmart punktet auch mit Blick auf die Hygiene. Je weniger Kontaktflächen es an viel frequentierten Türen gibt, desto besser: Mit dem elektronischen blueSmart Schlüssel können Nutzer Türen bedienen, ohne beispielsweise einen Knauf berühren zu müssen: Schlüssel in den elektronischen Zylinder einführen und drehen – schon zieht die Falle



© Bild: Winkhaus



© Bild: Winkhaus

▲ Dank verschiedener Drücker-Designs und den Farben schwarz und weiß fügt sich der intelligente Türbeschlag stimmig in jedes Objekt ein

zurück und die Tür lässt sich öffnen. Darüber hinaus sind die blueSmart Schlüssel beständig gegen Desinfektionsmittel und vertragen dank ihres wasserdichten Gehäuses (IP 68) sogar eine Wäsche.

Eleganter Look für alle Innentüren

Die neue Türklinke ETB-IM ergänzt das Angebot. Damit lassen sich auch bestehende Anlagen erweitern. Der Beschlag wird werkseitig passend zum Aufmaß vormontiert. Das spart Zeit beim Einbau. Bei Bedarf kann er leicht umgebaut werden, falls verschiedene Türblattstärken und die benötigte Drückerrichtung das verlangen. Zudem ist er kompatibel mit gängigen Innentüren aus Holz, Stahl oder Kunststoff sowie unterschiedlichen Türblattstärken und verschiedenen Einsteckschlössern. Auch Lösungen für Fluchttüren nach EN 179 sind möglich.

Designs und Materialien sind auf die unterschiedlichsten Anwendungsbereiche ausgerichtet: Die Türdrücker aus Edelstahl und die dezenten Kunststoffgehäuse in schwarz und weiß erlauben eine zeitlose Integration in nahezu jedes Objekt.

Programmiergeräte mit vielen technischen Neuerungen

Das umfangreiche Programm eröffnet viele Möglichkeiten, individuelle Konzepte zu realisieren.

Neben den Hardware-Komponenten gehört auch intelligente Software für die Anlagenverwaltung dazu. Zudem unterstützt eine Smartphone-App für iOS den User. Sie ermöglicht durch Berechtigungsvergabe und Programmierung aus der Ferne die Steuerung von Standorten ohne Netzwerkanbindung.

Insbesondere für die Erstprogrammierung der Schließanlage wird jedoch ein Programmiergerät benötigt. Die neue Generation von Winkhaus heißt BXP

BS. Auffälligstes Merkmal ist das Display mit farbiger Touch-Oberfläche. Für gute Lesbarkeit lässt sich die Hintergrundbeleuchtung individuell einstellen. Darüber hinaus bringen die Geräte viele weitere anwenderfreundliche Neuerungen mit: So enthalten sie beispielsweise einen LAN-Port zur einfachen Integration in das Unternehmensnetzwerk, das mit der Verwaltungssoftware kommuniziert. Darüber hinaus verfügen sie über einen USB-Anschluss sowie über ein WLAN-Modul, das alternativ zur USB- oder LAN-Schnittstelle auch eine drahtlose Synchronisation mit der Verwaltungssoftware ermöglicht.

Ein robustes Kunststoffgehäuse in handlichen Maßen umschließt die innovative Technik. Winkhaus liefert die Geräte mit Programmier-Adaptoren für sämtliche blueSmart Türkomponenten wie Schließzylinder, Türbeschläge, Leser oder Möbelschlösser sowie Steckernetzteil und leistungsstarkem Lithium-Ionen-Akku aus. ■

Kontakt

Aug. Winkhaus GmbH & Co. KG
Münster
Tel.: +49 251 4908 0
zutrittsorganisation@winkhaus.de
www.winkhaus.de

Erfolgreicher Start für iLoq S5

Nach gut einem halben Jahr seit dem Launch der neuen Schließsystem-Generation S5 zieht iLoq ein positives Fazit: Die Weiterentwicklung und die neuen Features kommen im Markt sehr gut an. Insbesondere die innovativen Möglichkeiten der Gerät-zu-Gerät-Kommunikation, mit deren Hilfe Zugangsrechte zwischen Schließzylinder, Schlüsseln und Lesegeräten geteilt und aktualisiert werden, finden großen Zuspruch. Komfortablere Zugangsrechtevergabe, höhere Kapazitäten und die Einbindung eines RFID-Pin-Lesers würden sehr gut angenommen, so Geschäftsführer iLoq Deutschland Eric Kewel. Es freue ihn besonders, dass das Unternehmen mit S5 in den wichtigen Zielmärkten der Wohnungswirtschaft, Städten und Gemeinden aber auch bei Pflege- und Bildungseinrichtungen überzeugen konnte. Die Branche der Versorgungsunternehmen würde mit der 5-Serie, die die Vorteile des mobilen smartphonebasierten Zugangsmagementsystems S50 mit den Features verbindet, angesprochen. Auch hier sei das Interesse groß, so Eric Kewel.

Mit S5 und der 5-Serie konnten bereits eine Vielzahl an Neukunden generiert werden, die sich bewusst für die neue Generation des Schließ- und Zugangsmagementsystems entschieden haben: Ein aktuelles Beispiel bildet die Genossenschaft der Franziskanerinnen in Münster, die neben dem Konvent auch ein Seniorenwohnheim betreut. Die Gerät-zu-Gerät-Kommunikation des S5-Schließsystems war hier ein ausschlaggebendes Argument, da



somit die gesamte Zugangsverwaltung sowie Sperrungen und Schlüsselupdates remote geschehen können. Das Ergebnis: mehr Sicherheit ohne großen Verwaltungsaufwand. Neben den Innen- und Außentüren des neugebauten Konvents, des Mutterhauses sowie des Seniorenwohnheims „Haus Heriburg“ wurden Aufzüge und Gartentore mit Online-Wandlesern ausgestattet. Auch die Vinzenz von Paul gGmbH setzte beim Neubau zweier Pflege- und Seniorenheime in Wangen und Göppingen auf das Schließsystem S5. An über 50 Standorten betreibt Vinzenz von Paul Wohn- und Pflegeeinrichtungen für ältere Menschen und Hörgeschädigte sowie Kinder- und Familienzentren. Ziel ist es, in Zukunft alle Einrichtungen mit einem digitalen Schließsystem zu verwalten und somit die Übersicht über Schlüssel und Zugangsrechte zu gewährleisten. An den Standorten in Wangen und Göppingen wurde mit dem Einsatz von 130 iLoq-Zylindern und 280 Schlüsseln der Anfang gemacht.

www.iloq.com ■

Update der Eniq-App

Für die Eniq-App hat Dom ein Update veröffentlicht. Mit der bisherigen Version der App stand nur der Data-on-Device-Programmiermodus (Offline-Modus) zur Verfügung. Das bedeutet, dass Benutzer der App bei Berechtigungsänderungen der Zutrittsrechte die betroffenen Geräte neu programmieren müssen. Bislang war es möglich, bis zu drei Geräte kostenlos zu verwalten. Mit der neuen Version der Eniq-App kann zwischen zwei Programmiermethoden gewählt werden:

Data on Card oder Data on Device (Offline-Programmiermethode). Mit der Data-on-Card-Programmierung erhält der Nutzer mehr Flexibilität durch die Übertragung von Zutrittsrechten auf den Transponder. Bei Änderung der Zutrittsrechte muss nicht mehr zu jedem Gerät gegangen werden, um die Aktualisierung durchzuführen. Die Berechtigungen befinden sich nicht in den Geräten, sondern sind auf den Transpondern (Schließmedien) gespeichert.

www.dom-security.com ■

Net2-Updates & Errichter-Aoo

Optimierte Net2-Updates zum Corona-Schutz sowie eine Errichter-App hat Paxton nun auf den Markt gebracht. Zu Beginn des Jahres 2020 und auch während der Anfangsphase der globalen Pandemie waren bei dem Unternehmen internationale Produkteinführungen noch über das ganze Jahr hinweg geplant. Der Technologiehersteller beschloss jedoch, diese Pläne der aktuellen Situation anzupassen, und begann mit der Entwicklung neuer Updates zur Verringerung des Infektionsrisikos für mit Net2 ausgerüstete Objekte. Parallel zu diesen Software-Erweiterungen hat der Hersteller eine Installer-App für intelligente Geräte entwickelt, die Kunden des Unternehmens durch technische Daten sowie bei Vor-Ort-Installationen unterstützen soll. Net2-Pro-Benutzer kommen jetzt in den Genuss einer ganzen Reihe zusätzlicher Funktionen zum Coro-



na-Schutz, die das Unternehmen in diesem Jahr entwickelt hat. All diese Funktionen arbeiten reibungs- und nahtlos zusammen und verringern so das Risiko einer Ausbreitung des Coronavirus in bewohnten Gebäuden. In den letzten vier Monaten habe das Unternehmen neue Versionen der Net2-Software mit flexiblen Zutrittsberechtigungen, Belegungsmanagement und Kontrollpunkt-Kontrolle herausgebracht und bietet weitere Wärmebildscanner-Integrationen, so Adam Stroud, Global Chief Executive von Paxton.

www.paxton-access.com ■



Fahrradboxen deutschlandweit ▲

Smart ist auch das: Fahrradboxen bieten sowohl Gelegenheits-Nutzern als auch Dauer-Nutzern ein komfortables, sicheres und geordnetes System zum Verwahren wertvoller Fahrräder und persönlicher Gegenstände. BikeParkBoxen sind Fahrradboxen, die mit den Zutrittssystemen von IntraKey ausgestattet sind. Auch die entsprechende Webanwendung und das Betreiberportal wurden von den Dresdnern entwickelt. Komfort und Sicherheit sind vom ADFC getestet und zertifiziert. Radfahrer können das System einfach mit dem Smartphone bedienen: von der Registrierung auf www.bikeparkbox.de,

de, der Buchung und Bezahlung bis zur Öffnung der Fahrradbox. Auch die Integration bestehender Chipkarten und Zahlungssysteme ist möglich. Mit dem innovativen Nutzungskonzept kann jeder interessierte Betreiber seine eigenen Fahrradboxen managen. Sowohl die Buchung und Verwaltung als auch die Abrechnung der Nutzungsgebühren erfolgt über ein gesondertes Betreiberportal der BikeParkBox. Er kann seine Boxen administrieren, mögliche Mietdauern und zugehörige Mietpreise festlegen. Die Datenerhebung erfolgt DSGVO-konform.

info@intrakey.de ■

Für sichere und reibungslose Abläufe in allen Industriebereichen



Für jedes Gebäude und jede Anforderung die passende Schließlösung finden: Download Whitepaper



Egal, was Sie absichern, abschließen oder öffnen wollen: Wir ziehen für jede Situation eine flexible Lösung aus der Schublade – ganz sicher! Überzeugen Sie sich selbst unter www.assaabloyopeningsolutions.de/industrie

ASSA ABLOY
Opening Solutions

Experience a safer
and more open world

PRAXISBERICHT RECHENZENTRUM

Bunker digital

ColocationIX optimiert Zutrittskontrolle in bunkergeschütztem Rechenzentrum durch digitale Schließtechnik



▲ ColocationIX ist professioneller Dienstleistungspartner für das Outsourcing von IT-Serverstrukturen

Kann man einen ehemaligen Atomschutzbunker noch sicherer machen? Das funktioniert, und komfortabler wird's noch dazu. Der Beweis steht in Bremen. Hier hat ColocationIX sein Rechenzentrum in einem umgebauten Atomschutzbunker mit digitaler Schließtechnik der SimonsVoss Technologies aus Unterföhring bei München ausgestattet. Kunden, die hier IT-Kapazitäten buchen, und die Beschäftigten des Dienstleisters profitieren von den Vorteilen des elektronischen Zutrittskontrollsystems.

ColocationIX ist professioneller Dienstleistungspartner für das Outsourcing von IT-Serverstrukturen. 2011 kaufte das Unternehmen einen ehemaligen Atomschutzbunker des Bundes und begann mit den Umbauarbeiten zum Rechenzentrum. Der Standort bietet Schutz vor Erdbeben und Unwettern. Eine direkte Glasfaseranbindung zu den wichtigen Internetknoten DE-CIX, AMS-IX und LINX und eine Verbindung nach China, ermöglichen

eine hohe Verfügbarkeit bei einer hohen Geschwindigkeit.

Design nach ISO EN 50600 Klasse 4 verfügt ColocationIX über größtmöglichen physischen Schutz, selbst ein Flugzeugabsturz könnte dem Bunker nichts anhaben. Die ISO 27001 Zertifizierung garantiert eine ausfallsichere Datensicherheit und ermöglicht eine DSGVO-konforme Datenverarbeitung. Die Sicherheits-Architektur entspricht den Anforderungen Kritischer Infrastrukturen.

Kernkompetenz digitale und physische Sicherheit

Die Kunden, darunter Marktführer aus ganz unterschiedlichen Branchen, geben ihre IT-Hardware in das Rechenzentrum und mieten dafür die Infrastruktur – etwa einen Serverschrank samt Strom, Kühlung, Bandbreite etc. in einem Paket. Oder sie verarbeiten dort nur ihre Daten und nehmen dafür Managed Services wie Private Hosting oder eine Private Cloud in Anspruch. ColocationIX

zählt mit seinem zukunftsfähigen physischen und digitalen Sicherheitsniveau sowie dem prämierten energieeffizienten Klimatisierungskonzept zu den modernsten Rechenzentren Europas.

„Aber es gibt nichts, das sich nicht noch optimieren ließe“, erklärt Andres Dickehut, Gesellschafter von ColocationIX. „Digitale und physische Sicherheit gehören zu unseren Kernkompetenzen – und dazu zählt auch ein hochsicheres Zutrittskontrollsystem, das den Zutritt in Zonen bzw. Räumen verwaltet und genau protokolliert, wer sich wann wo innerhalb des Gebäudes aufgehalten hat.“

Mit der Entscheidung für digitale Schließtechnik kombinierte ColocationIX einerseits die sicherheitstechnische Aufwertung der bis dahin rein mechanischen Außenhautsicherung des Bunkers mit einer maßgeschneiderten Verwaltung und Steuerung aller Zutrittsereignisse.

Definiertes Anforderungsprofil

Das verantwortliche Team des Rechenzentrums erstellte zunächst die Anforderungskriterien und daraus resultierend eine erste Grobplanung. Die Detailplanung der Anlage mit der genauen Konfiguration, die Installation und Inbetriebnahme lag in Händen von Apmann Daten- und Kommunikationstechnik aus Delmenhorst.

Zum Anforderungsprofil des elektronischen Schließsystems zählte unter anderem:

- Höchstes Sicherheitsniveau der Komponenten
- Zuweisung der Berechtigungen auf Ebene der einzelnen Schließung
- Protokollierung des Zutritts
- Einfachheit der Installation und Wartung
- Zentrale Administration
- Langfristiger Support durch den Hersteller

Das Rechenzentrum ColocationIX im Überblick

Gebäude

- Über 2.500 m² Fläche auf 8 Stockwerken
- 2 m dicke Stahlbeton-Außenwände und -decken
- 5 in sich geschlossene Rechenzentren, aufgeteilt in 10 Sicherheitszonen

Physische Sicherheit

- Gebaut nach EN 50600 Klasse 4 und Tier 4, betrieben nach ISO27001
- Mehrstufige Zutrittsauthentifizierung mit Logging: Sicherheitspersonal Pfortner, Code, Transponder, Biometrie, Metalldetektor und Vereinzelungsanlage
- 24 Std./7 Tage Videoüberwachung, Alarmüberwachung
- Blitzschutz nach Klasse 1
- Permanente Sauerstoffreduktion in Server- und Technikräumen
- 10 separate Brandabschnitte
- Separate Löschsysteme in Fluren, Treppenhaus, Büros
- Brandabschnitte je nach Anforderung ausgebaut für F30/T30 bis F120/T120
- Brandfrüherkennung mit Aufschaltung an Alarmzentrale
- VdS Brandmeldeanlage mit Feuerwehr-Aufschaltung

Virtuelle Sicherheit

- Intrusion Prevention Systeme, DDoS Mitigation inklusive Remote Triggered Black Holing (RTBH) und mehrfache Firewalls
- Regelmäßige Security- & Datenschutz-Audits
- Netzwerk- und Services-Monitoring
- Information Security Management System nach ISO 27001
- Zusätzlicher Standort für Datensicherung

Nach intensiver Recherche fiel die Wahl auf das System 3060 von SimonsVoss Technologies. Andres Dickehut: „Durch die Vernetzung steigt der Komfort des gesamten Systems und alle Vorgänge werden protokolliert. So kann der Zutritt individuell nachverfolgt werden. In Kombination mit der bei uns schon vorhandenen Videoüberwachung und Biometrie-Erkennung kann z.B. auch im Notfall schnell festgestellt werden, wer sich aktuell bzw. zu einer bestimmten Zeit in welchem Abschnitt des Gebäudes befindet oder befunden hat.“

Struktureller Aufbau der Anlage

Folgende Komponenten des SimonsVoss-Systems 3060 werden im ColocationIX-Rechenzentrum eingesetzt:

- WaveNet zur Steuerung und Protokollierung der Schließzylinder Events
- Schließzylinder mit LockNodes zur Protokollierung
- SmartRelais im Aufzug und für die RC6-Türen
- Transponder als Schlüssel
- Pin-Code-Tastaturen

Bitte umblättern ►



In diesem ehemaligen Atomschutzbunker hat ColocationIX ein Rechenzentrum eingerichtet – mit digitaler Schließtechnik von SimonsVoss



Um das Sicherheitsniveau maximal hoch zu halten, wurde für den Zugang zu den freigegebenen Etagen, in spezifische Serverräume und zu abgeschlossenen Racks eine Dreifach-Authentifizierung zugrunde gelegt



Authentifizierung über individuelle Freigabe durch das Rechenzentrums-Personal bzw. per Pin-Code, Transponder mit Verschlüsselung und Biometrie-Erkennung (im Bild links: USV-Raum, rechts: RC4-Tür)

■ LSM Software zur Verwaltung der Anlage

Das gesamte Schließsystem ist mit dem Management-System vernetzt. Die Schließzylinder-Vernetzung wird über WaveNet mit Power Over Ethernet (PoE) sichergestellt, die als Access-Points fungieren. Die zugrundeliegenden PoE Netzwerk-Switches sind per Glasfaser verbunden. Die WaveNet-Komponenten sind über eine Switch-Infrastruktur vernetzt, die wiederum mit Glasfaser die Switches untereinander verbindet.

Durch die physische Struktur mit dicken Betonwänden und -decken des Gebäudes wurden in jeder Etage mindestens zwei WaveNet Access-Points installiert, teilweise auch mehr. Der Datenaustausch mit den 3060-Schließzylindern über deren Sender/Empfänger (LockNodes) sowie zu anderen Geräten erfolgt über das vernetzte WaveNet.

An den Hochsicherheitstüren der Widerstandsklasse RC6 steuern SmartRelais die Türentriegelung. Sie werden mit Transpondern in Verbindung mit Pin-Code-Tastaturen eingesetzt. Für ColocationIX spielte auch der Faktor Flexibilität eine wichtige Rolle: „Die digitale Schließanlage kann bei Bedarf jederzeit erweitert und zentral programmiert bzw. konfiguriert werden“, erläutert Andres

Dickehut, „andererseits sind die Komponenten wie Schließzylinder vollkommen autark und funktionieren auch beim Ausfall des Management-Systems.“

Dreifache Personen-Authentifizierung

Der umgebaute Atomschutzbunker verfügt im Inneren über acht Stockwerke, fünf davon sind reine Datacenter-Bereiche. Zutritt erhalten grundsätzlich nur vorher für einen Bereich registrierte und autorisierte Personen. Den Zugang auf das eingezäunte Grundstück des Bunkers kontrolliert Sicherheitspersonal, außerdem gibt es Videoüberwachung und eine Vereinzelungsanlage. Kunden erhalten grundsätzlich nur in Begleitung eines berechtigten Beschäftigten Zutritt zum Rechenzentrum.

Um das Sicherheitsniveau maximal hoch zu halten, wurde für den Zugang zu den freigegebenen Etagen, in spezifische Serverräume und zu abgeschlossenen Racks eine Dreifach-Authentifizierung zugrunde gelegt. Die Authentifizierung erfolgt über individuelle Freigabe durch das Rechenzentrums-Personal bzw. per Pin-Code, Transponder mit Verschlüsselung und Biometrie-Erkennung. Alle Voraussetzungen müssen erfüllt werden, um Zutritt in das Datacenter zu erhalten. Die

drei Systeme haben keinen gemeinsamen Single Point of Failure und führen daher zu höchstmöglicher Sicherheit im Bereich der Zutrittskontrolle.

Verwaltung in Eigenregie

SimonsVoss hat parallel zur Planung der digitalen Schließanlage mit den Administratoren von ColocationIX Schulungen für das System 3060 durchgeführt, um nach Inbetriebnahme einen reibungslosen Ablauf sicherzustellen. Andres Dickehut: „Diese Seminare waren eine ideale Grundlage für unsere internen Experten, die Grundkonfiguration mit allen Komponenten kennen zu lernen und sich mit den notwendigen Schritten und Abläufen im Vorfeld vertraut zu machen. Wir verwalten die Anlage komplett eigenständig einschließlich der Vergabe von Zutrittsberechtigungen und der Programmierung von Schließmedien.“ ■

Kontakt

SimonsVoss
Unterföhring
Tel.: +49 89 992 28 0
marketing@simons-voss.com
www.simons-voss.com
www.colocationix.de

Curved Ultrawide-Monitor

Der EV3895-BK Flex Scan von Eizo ist ein 37,5" Curved Ultrawide-Monitor. Seine 3840 x 1600 Pixel bieten die fast dreifache Auflösung eines Full-HD-Monitors. Mehrere Anwendungen finden auf der großen Bildschirmfläche gleichzeitig Platz, sodass kein weiterer Monitor benötigt wird. Das Curved-Design unterstützt eine komfortable Sicht. Der USB-Hub ist mit vier Downstream-Ports, z. B. für den Anschluss von Tastatur, Maus oder Headset, ausgestattet. Die Dockingfunktion via USB-C-Anschluss inkl. Display-Port-Signal sorgt für Flexibilität. Der Monitor hat eine 85-W-Stromversorgung



für das Aufladen kleiner Rechner und Notebooks über USB-C – ein zusätzliches Rechnernetzteil wird damit überflüssig. Mit KVM-Switch und Picture-by-Picture können bis zu drei Computer mit Picture Swap und USB-Umschaltung bedient werden.

www.eizo.de ■



Fieber-Screening-Set

Kentix hat den Einsatz des Fieber-scanners SmartXcan zur Vermeidung von Corona-Hotspots verbessert. Dazu bietet das Unternehmen ein Set mit allen nötigen Komponenten für den Einsatz des Geräts zum Fieber-Screening – von der Holzstele zur Ausrichtung im richtigen Winkel bis hin zur Stromversorgung. Somit ist das Gerät dank Plug-and-Play

mit nur wenigen Handgriffen einsatzbereit. Zusätzlich kündigt das Unternehmen eine KI-gestützte Erweiterung zur Einschätzung über mögliche Viruserkrankungen an. Mit dem Starter-Set erhalten Schulen oder Einzelhandelsgeschäfte die Möglichkeit, eine automatisierte, schnelle und intuitive Fiebmessung zur Corona-Prävention einzusetzen. Das Gerät misst die Körpertemperatur durch 1024 Sensoren über die Gesichtsarterie an der Augeninnenseite, da die Blutversorgung nur an dieser Stelle eine stabile Temperatur gewährleistet. So erkennt der Fieberscanner eine erhöhte Temperatur sicher in unter einer Sekunde. Das Gerät erfüllt die Norm IEC 80601-2-59.

www.kentix.com ■

Zertifizierte Brandschutzkabel

Die Koaxialkabel der Produktreihe Ecoflex Plus Heatex von SSB-Electronic erfüllen durch ihre Zuordnung zu der Euroklasse „Cca“ moderne Brandschutzbestimmungen und sind für den Einsatz in öffentlichen Gebäuden mit hohem Sicherheitsbedarf geeignet. Die Produkte mit der Bezeichnung Ecoflex-Kabel mit Heatex-Mantel sind schwer entflammbar und haben eine nur geringe Brandfortleitung. Der Kabelmantel ist raucharm, dadurch bleiben die Fluchtwege im Brandfall sichtbar. Das Ecoflex-Heatex ist halogenfrei und enthält keine reaktionsfreudigen Elemente wie

Fluor, Chlor und Brom. Es erzeugt keine korrosiven Gase, die zu hohen Brandfolgeschäden führen können. Mit der Brandschutzklasse „Cca“ wird gewährleistet, dass wichtige Klassifizierungskriterien bezüglich Flammenausbreitung, Wärme-, Rauch- und Säureentwicklung sowie brennender Tropfen erfüllt sind und alle relevanten Normen eingehalten werden. Durch die Verwendung zertifizierter Kabel soll im Brandfall mehr Zeit zur Evakuierung zur Verfügung stehen und die Rettung von Personen erleichtert werden.

www.ssb.de ■

Tapkey-Firmware-Update

Die Tapkey-Firmware von Dom hat ein Update auf Version 3.2 erhalten. Dieses liefert mit seinem optimierten BLE-Handling eine deutlich höhere Kommunikationsstabilität auch in Installationen mit vielen BLE-Geräten. Zusätzlich beinhaltet die Firmware-Version das Lock-Grouping-Feature. Das Update kann nur an Geräten durchgeführt werden, die ab Januar 2020 gefertigt worden sind und damit eine Firmware-Version 3.0 haben. Ein Firmware-Update für Tapkey-Geräte, die vor Januar 2020

mit der Firmware-Version 2.x gefertigt wurden, wird zu einem späteren Zeitpunkt bereitgestellt. Für Tapkey Pro V1 Zylinder ohne BLE kann ein solches Update aus technischen Gründen nicht mehr bereitgestellt werden. Beim iPhone muss nach dem Update der Tapkey-Geräte auf die Firmware V3.2 das Bluetooth auf dem iPhone deaktiviert und danach wieder aktiviert werden, damit das iPhone wieder mit den Geräten kommunizieren kann.

www.dom-security.com ■

Kamera-Anschlusskasten mit integriertem Switch

Pieper hat den Kamera-Anschlusskasten KMF-N-1400-3-A01 im Portfolio. Der Anschlusskasten eignet sich für alle Netzwerkkameras. Ein durchdachtes Konzept ermöglicht den Gebrauch bestehender und zukünftiger Einsteckplatinen für eine Vielzahl von Funktionen. Ein integrierter Layer-2-Switch mit 5

x 100/1000 MBit/s SFP-Steckplatz sorgt für einen konstanten Datenfluss. Der Kamera-Anschlusskasten hat ein integriertes, leistungsstarkes 12-V-DC- und 56-V-DC-Netzteil zur Versorgung der Kameras per PoE und des integrierten Switch-Boards.

www.pieper-video.de ■

Switche für Video

Die neue 28er Serie



- ✓ **Non-Stop PoE**
Firmware aufspielen ohne Übertragungsunterbrechung
- ✓ **Integrierte Cyber Security**
Switche inspizieren Netzverkehr mit interner Firewall Funktion
- ✓ **Kein «Phone Home»**
kein unkontrollierter Zugriff eingesetzter Kameras zu Fremdservern
- ✓ **Kompatibilität**
zu diversen Videomanagement- und PSIM-Systemen
- ✓ **Erweiterte DMS Funktion**
Neu: Massendupdates direkt aus dem DMS (bis max. 25 Switche möglich)

Tel.: 07621-1593100 | www.barox.de

TITELTHEMA

Ganz beiderseits

Schlösser mit Panikfunktion und Zutrittsverwaltungssoftware für Gebäude jeder Größe

Sicherheit auf beiden Seiten der Tür bieten die ÜLock-B-Schlösser von Südmetall – zum Schutz von Menschenleben und Sachwerten: Durch eine Panikfunktion in Fluchtrichtung ist eine sichere Fluchtmöglichkeit im Panikfall gewährleistet. Und die Selbstverriegelung sorgt dafür, dass die Tür immer verriegelt ist. Von außen bietet das Schloss keine Angriffsfläche, da die Elektronik komplett im Schlosskasten eingebaut ist und das Schloss eine hohe Widerstandsklasse gegen mechanische Manipulation aufweist. Die Datenübertragung zwischen Schloss, RFID-Karte und RFID-Leser ist bestmöglich verschlüsselt – das sorgt für optimalen Einbruchschutz. Die Zutrittsverwaltung übernimmt die lizenzfreie Software ÜManagement 2.0.



Das Unternehmen Südmetall

Südmetall steht laut eigenen Angaben für Kompetenz, Zuverlässigkeit, Fairness und herausragende Service-Qualität in den Bereichen Beschläge, Metall- und Glasbau, Objektbereich und Schließsysteme. Mit den Sortimenten Beschläge und Metall- und Glasbau zählt man bereits zu den Marktführern im deutschsprachigen Raum.

Der Schwerpunkt von Südmetall Schließsysteme liegt auf der Entwicklung und Produktion von elektromechanischen Schlössern und Zutrittslösungen „Made in Germany“. Intensiv arbeitet ein erfahrenes und motiviertes Team am Standort Leipzig zusammen mit hochqualifizierten Partnern an smarten Lösungen für elektronisches Zutrittsmanagement.

Weil sich die Bedürfnisse im Laufe der Zeit ändern, ist das Familienunternehmen bestrebt, die eigenen Produkte kontinuierlich zu optimieren und zu verbessern. Dies alles geschieht dem Qualitätsanbieter zufolge aus der Zielsetzung heraus, das Leben ein Stück komfortabler, sicherer und damit besser zu machen.



▲ ÜLock-B von Südmetall ist eine in mehreren Varianten erhältliche Produktgruppe von Schlössern mit Panikfunktion

ÜLock-B von Südmetall ist eine Produktgruppe von Schlössern mit Panikfunktion. Es gibt sie in mehreren Varianten: ÜLock-B Cable, -B Battery und -B Inductive. Ganz neu auf dem Markt ist das ÜLock-Z – dabei handelt es sich um das ÜLock-B mit beidseitiger Zutrittskontrolle, d. h. ohne Panikfunktion für besonders sensible Räume. Auch hier gibt es verkabelte, batteriebetriebene und induktive Varianten.

Entsprechend der Design-Anforderungen des jeweiligen Objekts sind die Beschläge frei wählbar. Zusätzliche bzw. neue Türbeschläge sind nicht zwingend notwendig. Darüber hinaus ist die Begehung für die Nutzer sehr komfortabel: Die gültige Karte wird vor den Leser gehalten und die Tür kann durch Betätigung des Türdrückers geöffnet und begangen werden.

Nachrüstung

Die ÜLock-Schlösser eignen sich sehr gut für die Nachrüstung, da die Türen nicht verkabelt werden müssen: Hinzu kommt, dass durch das Funktionsprinzip der Zutrittskontrolle „Data on Card“ keine Netzwerkverkabelung zwischen den Türen und dem Computer notwendig ist. Kompatibel sind hier sowohl die batteriebetriebenen als auch die induktiven Schlösser. Eine gemeinsame Spannungsversorgung von Leser und dem ÜLock-B Inductive ist möglich. Alternativ können auch batteriebetriebene Leser verwendet werden. Auch ein Einsatz in Brandstutztüren ist möglich, die Schlösser sind entsprechend zertifiziert.

Verwaltungssoftware für die Zutrittskontrolle

ÜManagement 2.0 ist eine lizenzfreie Verwaltungssoftware für die Zutrittskontrolle, mit der einzelne Objekte, wie z. B. Bürogebäude,

Industrie oder Seniorenresidenzen, aber auch kleine bis mittelgroße Hotels oder mehrere Objekte gleichzeitig übersichtlich verwaltet werden können. Durch eine einheitliche Verwaltung verschiedener Schlösser können ÜLocks, Elektronikzylinder und Schrankschlösser angesteuert und, zugeschnitten auf die jeweiligen Anforderungen, individuell verwaltet werden. Über die Software können den einzelnen Schlüsseln direkte Berechtigungen und Berechtigungsgruppen/ Nutzergruppen zugeteilt werden.

Die Installation erfolgt wahlweise über die Standard Installation oder SQL:

- Standard: sehr einfache Installation / Einzelplatz Version
- SQL Server: mehrere Arbeitsplätze (Computer, mit dessen Hilfe das System verwaltet werden kann)

Durch die Software ergeben sich vielfältige Vorteile: Der Nutzer benötigt nur noch einen Transponder, keinen kompletten Schlüsselbund. Bei Verlust des Transponders besteht ein geringes Risiko (der Transponder kann durch wenig Aufwand gesperrt oder auf die Schwarze Liste gesetzt werden).

Für den Betreiber gibt es mehr Komfort und Sicherheit (z. B. durch individuelle Rechte und automatisches Verriegeln). Es fallen keine Lizenzgebühren an und die Software ist optimiert für die Nachrüstung. Sowohl der Haustechniker als auch der Benutzer profitieren von einer übersichtlichen Software und flexiblen Funktionen.

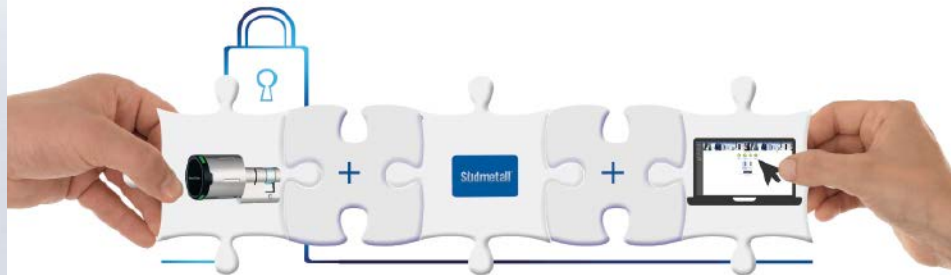
Zwei Betriebsarten

Zugeschnitten auf die spezifischen Anforderungen kann die Software in zwei Betriebsarten konfiguriert werden. Während die Betriebsart

Das Zutrittssystem von Südmetall: Flexibel, übersichtlich und leicht zu handhaben



Das Firmengebäude von Südmetall zeigt, wie ein offline-basiertes Zutrittssystem umgesetzt werden kann, ohne dafür große Umbauarbeiten durchführen zu müssen



Da eine Verkabelung der Eingangstür zu aufwendig wäre, kommt hier ein Elektronikzylinder zur Anwendung

„Management“ durch einfache Handhabung auf kleine bis mittelgroße Anwendungen zugeschnitten ist, ermöglicht die Betriebsart „Professional“ weitere flexible Möglichkeiten für größere Anwendungen, ohne auf die Übersichtlichkeit verzichten zu müssen.

Je Zeitzone sind unterschiedliche Zonen wählbar. Zimmer- und Apartmenttüren können einem Gebäude oder Flur zugeordnet werden, wodurch der Zutritt zu den notwendigen Türen nicht extra eingestellt werden muss. Gemeinschaftsräume können einer Türengruppe zugeordnet werden. Einer Tür können weitere Gruppen zugeordnet werden, sodass die ausgewählte Tür automatisch Berechtigungen zu den ausgewählten Türengruppen (wie z. B. Schwimmbad oder Sauna) erhält. Automatische Entriegelungszeiten werden durch die Zeitzonen ermöglicht.

Ein Beispiel: Die Eingangstür (Mehrpunktverriegelung) mit Elektronikzylinder wird morgens entriegelt und abends wieder verriegelt. Bei der Bürotür mit ÜLock

besteht eine komfortable Begehung via Türdrücker und sie kann optional permanent eingekoppelt werden, solange sich die Person im Büro befindet. Der Schrank im Büro kann mit einem Schrankschloss gesichert und ohne viel Aufwand nachgerüstet werden.

In der Betriebsart „Professional“ lassen sich Gästekarten sehr leicht programmieren, da diese speziell formatiert sind. Weitere Funktionen, wie die Guthabenfunktion runden das System ab. ■

Kontakt

Süd-Metall Beschläge
Ainring
Tel.: +49 8654 4675 50
info@suedmetall.com
www.suedmetall.com

3 Fragen an ...

... Produktmanager Jörg Bärenfänger von Südmetall

GIT SICHERHEIT: Herr Bärenfänger, was sind die wichtigsten Vorteile dieser Lösung?

Jörg Bärenfänger: Eine Nachrüstung in bestehenden Objekten unterschiedlicher Größen ist möglich, ohne auf Sicherheit und Komfort verzichten zu müssen. Dem Betreiber werden keine Kompromisse beim Design abverlangt. Außerdem gibt es bei uns keine in Software-Lizenzen versteckten Folgekosten.



Sie erwähnen die Guthabenfunktion – was ist das genau?

Jörg Bärenfänger: Mit der Guthabenfunktion kann optional die Nutzer-Karte bzw. der Transponder mit Guthaben aufgeladen werden. Bei jeder berechtigten Begehung der jeweiligen Tür (z. B. Sauna) wird das bei der Konfiguration voreingestellte Guthaben abgezogen. Der Nutzer bekommt nur Zutritt bei ausreichendem Guthaben.

Welche sind die Zielgruppen Ihrer Lösung?

Jörg Bärenfänger: Die Zielgruppen sind breit gefächert. Es sind zum Beispiel Bürogebäude und Industrie, Seniorenresidenzen, aber auch kleine Hotels und Apartments oder das Clubhaus eines Vereins mit nur einer Tür, die durch den Vereinsvorsitzenden verwaltet wird.

Perimeterschutz für Molkerei in Waldgebiet

Bosch entwickelte für eine italienische Molkerei ein geeignetes Sicherheitssystem. In der Nähe der Kleinstadt Soliera in Norditalien gelegen, ist die Molkerei des italienischen Lebensmittelherstellers Granarolo alles andere als klein und beschaulich: Mehr als 600 Landwirte, 70 Milchtanklastwagen und 720 weitere Transportfahrzeuge beliefern sie jedes Jahr mit 850.000 Tonnen Milch. Die in der Anlage hergestellten Produkte wie Frischmilch, Joghurt, Eis, Käse und seit Neuestem auch Nudeln und Schinken versorgen täglich mehrere Millionen italienische Familien. Die hohe Produktionskapazität des Werks zeigt sich auch in den Ausmaßen der Anlage: Das Werk Soliera erstreckt sich über 45.000 Quadratmeter. Darüber hinaus befindet es sich in einem bewaldeten Gebiet. Das stellt die Bereitstellung eines Sicherheitssystems zum Schutz der Anlage vor unbefugtem Zutritt vor besondere Herausforderungen. Um jederzeit den höchsten Ansprüchen an den Perimeterschutz des Werks zu genügen, entschied sich Granarolo, das alte analoge Videosicherheitssystem durch ein digitales zu ersetzen.

Zu den besonderen Herausforderungen bei der Entwicklung eines geeigneten Videosicherheitssystems zählten neben der Größe der Anlage die schlecht einsehbare Umgebung des Werks und die Lage in einem Waldgebiet. Die Bewegung der Bäume und Pflanzen sorgt für sich ständig ändernde Lichtverhältnisse und Schatten, die Fehlalarme auslösen können. Der in Neapel ansässige Bosch-Partner Gruppo Sirio entwickelte deshalb ein auf die besonderen geografischen Verhältnisse zugeschnittenes Sicherheitssystem, bei dem Bosch-Kameras mit integrierter intelli-



Virtuelle Grenzlinien schützen vor unbefugtem Zutritt



Molkerei mit Videoüberwachungssystem von Bosch ausgestattet

gener Videoanalyse (IVA) den Kern bilden. Um das Werk vor unbefugtem Zutritt zu schützen, wurden mithilfe der integrierten Videoanalysefunktion der Überwachungskameras virtuelle Grenzlinien um das Werkgelände gezogen. Werden diese Linien überschritten, lösen die programmierten Regeln automatisch Alarme aus und benachrichtigen das Sicherheitspersonal vor Ort. Unabhängig von Lichtverhältnissen erkennen die Kameras bei Tag und Nacht verdächtige Objekte oder Bewegungen und sorgen so für Überwachung rund um die Uhr.

Dafür kommen insgesamt 48 Videokameras der Dinion-Serie zum Einsatz und bilden ein vernetztes Videosicherheitssystem. Das System wird auf einer zentralen Plattform verwaltet und ist völlig autonom und getrennt von jedem anderen System oder Netzwerk der Produktionsanlage. So ist die maximale Sicherheit auch bei potenziellen Ausfällen anderer Systeme am Standort gewährleistet. Granarolo kann sich nun auf ein System verlassen, das speziell auf seine Bedürfnisse zugeschnitten ist. Die neu eingerichtete digitale Videoüberwachungs- und Perimeterschutzlösung unterstützt das Sicherheitspersonal dabei, jederzeit höchste Sicherheit für die weiträumige Anlage zu gewährleisten. Das Sicherheitssystem trägt den hohen Anforderungen an die Lebensmittelsicherheit Rechnung, indem es die Anlage vor Störungen im Betriebslauf durch äußere Einflüsse schützt. So trägt es letztlich auch dazu bei, die sensible Lieferkette der italienischen Lebensmittelversorgung gegen Unterbrechungen abzusichern.

www.bosch.com ■

Hilfreiche Technologie nicht nur in der Corona-Pandemie ▲

Für Flexibilität sorgte die Öffnung der Mobotix7-Plattform im vergangenen Jahr. Einen wesentlichen Beitrag leisten auch die Kamerasysteme

analyse-Apps stehen Anwendern aller Branchen intelligente Hilfsmittel zur Verfügung, um relevante und aktuelle Anforderungen in ihrem Arbeitsalltag gezielt abzudecken. Lösungen, die noch nicht existieren, können maßgeschneidert neu erstellt werden. So ist die Plattform explizit offen für selbst entwickelte Apps von Partnern und Kunden des Unternehmens. Während zahlreiche eingesetzte Technologie-Lösungen zur Bekämpfung von Covid-19 ausschließlich fallbezogen zum Einsatz kommen, bietet Mobotix Videosysteme, die auch über die Pandemie hinaus – über einfache Umrüstungen – wertvollen Nutzen bieten.

www.mobotix.com ■

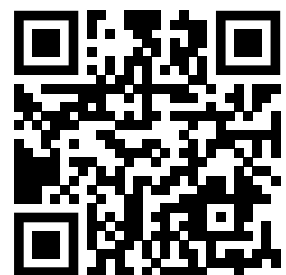


M73 und S74 mit drei bzw. vier Sensormodulen pro Kamera. Künstliche Intelligenz und Deep-Learning-Prozesse sind Treiber der Video-Lösungsplattform. Mit den vielen speziellen Video-

Elektronische Schließanlagen sicher & komfortabel verwalten.



Perfekt geeignet für **KMUs, Konzerne und Hotels.**



<https://easyAccess.wilka.de>

WILKA
SCHLIESSTECHNIK



Salto Wandleser im Innenbereich des Hauptsitzes von MBG

PRAXISBERICHT INDUSTRIE

Einfach und filigran

Virtuell und funkvernetzte Zutrittslösung für MBG Group

Eine stabile Funktion sowie ein differenziertes und übersichtliches Rechtemanagement waren die zentralen Anforderungen der MBG Group an die neue elektronische Zutrittskontrolle. Erreicht haben die Verantwortlichen das mit einer Lösung von Salto, die spürbar die Sicherheit des Unternehmens verbessert und zugleich eine einfache Handhabung bietet.

Die MBG Group ist ein international agierender Lieferant von nicht-alkoholischen, alkoholischen und Mix-Getränken, der Gastronomie, Einzelhändler, Tankstellen und Getränkehändler zu seinen Kunden zählt. Für den Hauptsitz in Paderborn suchte das Unternehmen eine neue Zutrittskontrolle. „Denn unser bisheriges elektronisches Schließsystem hat nicht zuverlässig funktioniert. Es kam vor, dass Mitarbeiter Türen nicht öffnen konnten, obwohl sie dafür berechtigt waren. Das hat uns veranlasst, die Reißleine zu ziehen und ein neues System zu suchen“, beschreibt Jörg Loh, der IT-Leiter der MBG Group und

verantwortlich für die Zutrittskontrolle, die Ausgangssituation.

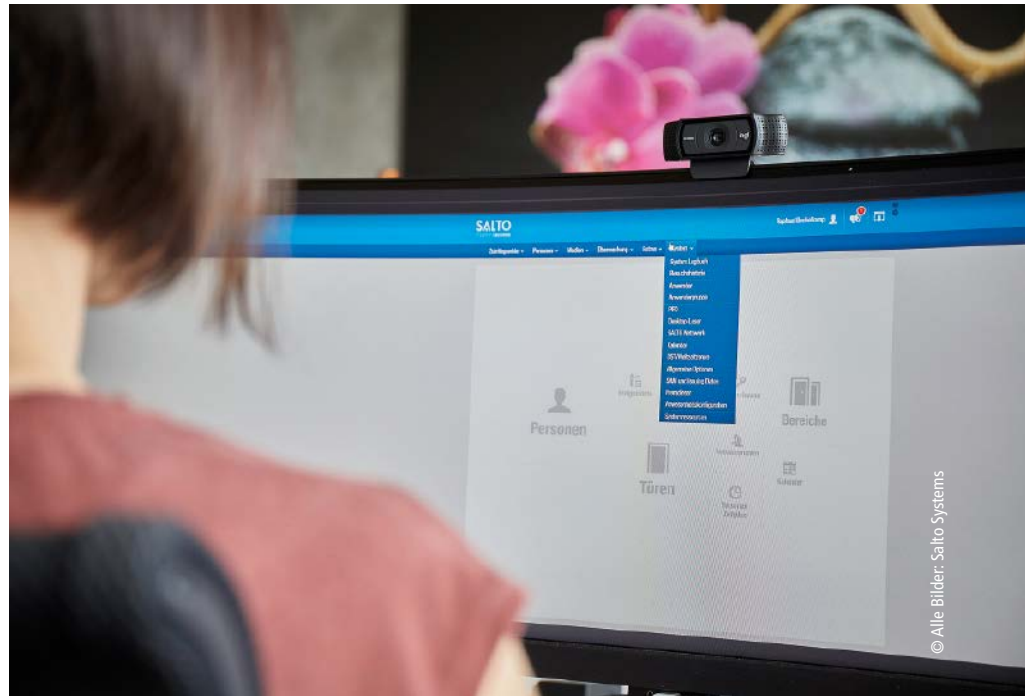
Stabile Funktion, Multiapplikation und Skalierbarkeit

„Unser neues System sollte in erster Linie funktionieren“, formuliert Loh seinen grundsätzlichen Wunsch an die neue Zutrittskontrolle. Im Detail war ihm eine zentrale Verwaltung mit individuellen Profilen und zeitlichen Berechtigungen sowie die Option, Transponder aus der Ferne zu sperren, wichtig. „Wir wollten überdies künftig nur noch ein Medium mit Multiapplikation für die Einbindung der Alarmanlage und der Zeiterfassung

im Lager. In der Zukunft können wir uns vorstellen, zusätzlich die Nutzung unseres Fitnessstudios, das bargeldlose Bezahlen und den PC-Login mit dem Medium umzusetzen“, ergänzt der IT-Leiter. Ein weiterer Aspekt für die Auswahl war für ihn die Skalierbarkeit, auch über Ländergrenzen hinweg: „Das hat vor allem zwei Gründe. Einerseits statten wir unseren Stammsitz nicht in einem Zuge komplett aus, sondern erweitern die Anlage permanent in kleinen Schritten. Andererseits sind wir ein international agierendes Unternehmen, bei dem durchaus vorstellbar ist, dass wir das System auf unsere Niederlassungen ausdehnen“.



Elektronischer XS4 One Beschlag von Salto im Innenbereich



Komfortable Zutrittsrechteverwaltung bei MBG mit der Managementsoftware

Testinstallation überzeugt

Um sich mit den Möglichkeiten aktueller Zutrittslösungen vertraut zu machen, recherchierte Jörg Loh im Vorfeld und schaute sich ferner etliche Anlagen in anderen Unternehmen an. Mit den gewonnenen Erkenntnissen und seinen Anforderungen wandte er sich an den Facherrichter Adverbis Security aus Schloss Holte-Stukenbrock. „Wir haben MBG die Salto Space Systemplattform empfohlen, weil sie aus unserer Sicht für das Projekt mit seinen Anforderungen ideal geeignet ist.

Damit die Verantwortlichen den Funktionsumfang prüfen und analysieren konnten, haben wir an einigen Türen eine Testinstallation eingerichtet. Zusammen haben wir außerdem die technischen Voraussetzungen geklärt, insbesondere für die Serverinstallation“, erinnert sich Dirk Humpert, Geschäftsführer des Salto Premium Plus Partners.

Die Testinstallation hat Jörg Loh und seine Mitarbeiter überzeugt: „Uns haben vor allem die Zuverlässigkeit und Schnelligkeit der Hardware und Datenübertragung sowie die

komfortable Verwaltung in der Managementsoftware beeindruckt. Im Vergleich mit unserer bisherigen Anlage sehen wir das Berechtigungsmanagement mit Salto in einer ganz anderen Liga, weil einfacher und filigranter“.

Die Installation begann mit der Installation und Konfiguration der Software und dem Stammdatenimport. Dank der Web-basierten Architektur des Managementsystems ging das rasch, da nur ein Server eingerichtet werden muss, auf den die Administratoren per Webbrowser zugreifen. Die ersten Türen

Bitte umblättern ▶

Upgrade von Audio-Management-Software

Axis Communications kündigt mit dem Audio-Manager-Edge ein Upgrade für das eingebettete Software-Management-System der eigenen Netzwerk-Lautsprecher an. Die Edge-basierte Software, die für die Verwaltung von bis zu 200 Lautspre-

chern in bis zu 20 Zonen entwickelt wurde, eignet sich für kleine bis mittlere Unternehmen mit vergleichsweise unkomplizierten Anforderungen. Audio-Manager-Edge ermöglicht ein All-in-one-Audiosystem, das einfach einzurichten, zu verwalten und anzuwenden ist.

Netzwerk-Lautsprecher sind ein wichtiger Bestandteil vieler Sicherheits- bzw. Gebäudekonzepte. Sie eignen sich insbesondere, um Personen von unerwünschten Aktivitäten abzuhalten sowie Live- oder aufgezeichnete Durchsagen auszuspielen. Die eingebettete Software Audio-Manager-Edge bietet eine

einfache Inhaltsverwaltung, mit der Benutzer Durchsagen, Audiowerbung und Hintergrundmusik je nach Bedarf in bis zu 20 Zonen aufteilen können. Die Software ist mit vorkonfigurierten Regeln für eine einfache Einrichtung und Bedienung ausgestattet und ermöglicht so eine unkomplizierte Planung von Inhalten. Separate Zugriffsrechte für Administratoren, Content-Manager und andere erlauben es dem Nutzer, Einzelpersonen nur jene Berechtigungen zuzuweisen, die sie auch benötigten. Dies verringert das Risiko von Fehlern und Systemausfällen. Eine integrierte Systemüberwa-

chung und ein Dashboard, das den Systemstatus anzeigt, sorgen dafür, dass Nutzer schnell auf Probleme hingewiesen werden, die eventuell ein Eingreifen ihrerseits notwendig machen.

Die Software sei direkt im Lautsprecher integriert und könne von dort aus konfiguriert und verwaltet werden. Sie benötige also keine zusätzliche Hardware, so Marco Pompili von Axis. Mithilfe der Software und der Funktionen können die passenden Audioinhalte zur richtigen Zeit am richtigen Ort ausgespielt werden.

www.axis.com ■



Wiley Industry Days
WIN  **DAYS**
 www.WileyIndustryDays.com
7.-9. Juni 2021



Jörg Wüllner
 Tel.: +49 6201 606 749
 joerg.wuellner@wiley.com

Virtuelle Show mit Konferenz, Ausstellung und Networking für Automatisierung, Machine Vision, Photonics, Healthcare und Sicherheit.

www.WileyIndustryDays.com

wurden innerhalb von zwei Tagen ausgestattet. „Die Zusammenarbeit mit Adverbis verläuft sehr gut. Wir erhalten zeitnahe Informationen, Lösungen und Angebote. Mit dem Support sind wir sehr zufrieden. Und durch die regionale Nähe kann schnell mal ein Techniker vorbeikommen, wenn wir spontane Unterstützung benötigen“, lobt Loh. Dirk Humpert fügt hierzu an: „Für uns ist Partnerschaft nicht nur ein Wort. Wir legen großen Wert auf eine gute Betreuung!“

Virtuell und per Funk vernetzt

Die Systemarchitektur bei MBG ist ein Mix aus Funkvernetzung und virtuellem Netzwerk, ergänzt um Mobile Access. Die Salto BLUenet Wireless-Technologie eignet sich vor allem für Anwendungen, in denen eine Echtzeitüberwachung von Türen erforderlich oder gewünscht ist. Salto BLUenet verbindet über Bluetooth die batteriebetriebenen elektronischen Beschläge mit Gateways, die wiederum per Ethernet oder WLAN mit dem Server kommunizieren. Bei einer Unterbrechung oder Störung der Funkverbindung arbeitet das Zutrittssystem weiterhin, da die virtuelle Vernetzung der Türhardware über das Salto Virtual Network (SVN) als Basistechnologie immer aktiv bleibt.

Im SVN mit patentierter Schreib-Lese-Funktionalität und verschlüsselter Datenübertragung werden die Schließberechtigungen auf dem Identmedium gespeichert, wodurch die elektronischen Beschläge kabel- und netzunabhängig funktionieren. Gleichzeitig schreiben die Türkomponenten Informationen über gesperrte Identmedien oder beispielsweise Batteriestände auf die Identmedien und geben sie somit weiter. Die Update-Punkte übertragen die ausgelesenen Daten an den zentralen Server und übermitteln zugleich die aktuellen Zutrittsrechte auf die Identmedien.

An einigen Türen hat Loh zudem die mobile Zutrittstechnologie JustIN Mobile ausprobiert. JustIN Mobile erlaubt das Öffnen von Türen mit dem Smartphone und verwendet dafür BLE (Bluetooth Low Energy) oder NFC (Near Field Communication). Der mobile Schlüssel wird aus der Managementsoftware „Over the Air“ (OTA) an die in einem verifizierten Smartphone installierte JustIN Mobile App verschickt. Der Mitarbeiter erhält eine Nachricht, dass er einen neuen mobilen Schlüssel erhalten hat und für welche Türen er berechtigt ist. Er muss dann nur noch das Smartphone vor den elektronischen Beschlag, Zylinder oder Wandleser halten und via App

die Kommunikation starten. „Wir sehen Mobile Access definitiv als Option für die Zukunft“, resümiert Loh.

Einfach zu administrieren

Für die Berechtigungsverwaltung der über 170 Nutzer setzt MBG die Web-basierte Managementsoftware ProAccess SPACE von Salto ein. Durch das Anlegen von passenden Bereichen und Personengruppen lassen sich neue Mitarbeiter schnell und einfach hinzufügen. „Ausgewählte Türen haben wir mit einer zeitlichen Beschränkung versehen, ansonsten verwendet MBG unterschiedliche Öffnungsmodi, passend zu den jeweiligen Türen“, erklärt Dirk Humpert. Die Einarbeitung erfolgte über eine Einweisung durch Adverbis. „Das Zuweisen und Entfernen von Zutrittsrechten ist aber selbsterklärend. Wir haben uns schnell zurechtgefunden. Darüber hinaus ist es sehr wertvoll, dass wir den Batteriestand

sowie den Status der Türen und Nutzer zentral einsehen können. Dadurch ist das System wirklich einfach zu administrieren“, freut sich Jörg Loh und zieht ein positives Fazit zur Einführung der neuen Zutrittskontrolle: „Schlüsselverluste stellen für uns kein Problem mehr dar, weil wir Transponder aus der Ferne am Haupteingang sperren

können. Das System funktioniert zuverlässig, wodurch wir nicht nur die Sicherheit unseres Unternehmens gewährleisten, sondern zugleich eine deutlich angenehmere Nutzererfahrung für die Mitarbeiter erreichen. Das wiederum wirkt sich entscheidend auf die Akzeptanz der Zutrittskontrolle aus. Und wir spüren eine deutliche Verbesserung beim Zutrittsmanagement – flexiblere Rechtevergabe, bessere Übersicht und weniger Aufwand für die Wartung des Systems.“ ■



„Uns haben vor allem die Zuverlässigkeit und Schnelligkeit der Datenübertragung sowie die komfortable Managementsoftware beeindruckt.“

Jörg Loh, IT-Leiter MBG

Kontakt

Salto Systems GmbH
 Wuppertal
 Tel.: +49 202 769579 0
 info.de@saltosystems.com
 www.saltosystems.de

MBG International Premium Brands GmbH
 Paderborn
 www.mbgglobal.net

Adverbis security GmbH
 Schloss Holte-Stukenbrock
 Tel.: +49 5207 9573652
 info@adverbis-security.de
 www.adverbis-security.de



Office-Monitore ▲

Durch ihre gute Konnektivität und die daraus resultierenden unzähligen Clean-Desk-Optionen lassen die Eizo Flexscan-Monitore EV2495 und EV2795 den Arbeitsplatz flexibel und zukunftssicher werden. Egal, ob Dockingfunktion, Mehrbildschirm Lösungen, Thin-Client-Halterungen oder die praktische Kabelführung: Alle Optionen sorgen dafür, dass nichts auf dem Schreibtisch ist, was dort nicht auch wirklich gebraucht wird. Beide Monitore haben eine hohe Bildqualität mit einer Auflösung von 1.920 x 1.200 (EV2495,

24,1") bzw. 2.560 x 1.440 Bildpunkten (EV2795, 27"). So geben die Monitore gestochen scharfe Bilder wider mit präzisen Farb- und Grautönen sowie einer sehr guten Blickwinkelstabilität. Das Unternehmen setzt außerdem auf eine sorgfältige Werksjustage jedes einzelnen Monitors. Für eine einfache Verkettung zwischen mehreren Monitoren sorgt die USB-C-Daisy-Chain-Funktion. Damit ist nur eine Verbindung zwischen Rechner und dem ersten Monitor notwendig.

www.eizo.de ■

Geräuscharmer Türöffner für Fluchttüren

Für den Einsatz in Fluchttüren bietet Assa Abloy Sicherheitstechnik einen geräuscharmen Türöffner an. Der Effeff Sicherheitstüröffner 352M verursacht dank seiner speziellen Konstruktion nur besonders leise Betriebsgeräusche. Er lässt sich leicht montieren und ist gut für den Einbau in Anschlag- und Pendeltüren geeignet. Sicherheitssensible Türen im Objektbereich erfordern geprüfte Schließsysteme, die den gesetzlichen Anforderungen entsprechen. Das gilt auch für solche Fluchttüren, die von außen gegen unbefugten Zutritt gesichert sein müssen. Als elektrische Zusatzverriegelungen kommen hier Türöffner zum Einsatz, die trotz der Verriegelungsfunktion die Sicherheit in den Flucht- und Rettungswegen gewährleisten. Mit einer Haltekraft unter Vorlast

von bis zu 5.000 Newton ist der 352M der stärkste Türöffner im Portfolio. Seine neuartige Konstruktion verbessert zudem den Schutz vor Manipulationen an der Tür und erschwert damit einen unbefugten Zutritt. Der Ruhestromtüröffner zeichnet sich durch besonders leise Betriebsgeräusche und eine klare, ansprechende Optik aus. Die elegante Fluchttürverriegelung reduziert die sichtbare Mechanik an der Tür auf ein Minimum und sorgt für einen nahezu geräuschlosen Schließvorgang. Sowohl das Verriegeln als auch das Entriegeln sind außerordentlich leise, so der Hersteller. Der Betrieb bei Dauerfreigabe ist praktisch geräuschlos. www.assaabloyopeningsolutions.de ■



© FOTOHINWEIS: Wilka, Gira Mediadatenban

Neue Generation elektronischer Schließsystemlösungen ▲

Mit easyAccess bringt Wilka Schließtechnik aus Velbert eine neue Generation elektronischer Schließsystemlösungen auf den Markt. Die Lösung umfasst einen neu entwickelten Beschlag, einen designtechnisch überarbeiteten Wandler sowie eine neue Version der Softwareplattform. Diese basiert auf der Mifare Desfire (EV2) Technologie, einem der zurzeit sichersten Transpondersysteme. Die Transponder (2K bis 8K) können je nach Kundenanforderungen konfiguriert werden und bieten zudem ausreichend Platz für die Nutzung zusätzlicher Anwendungen, wie z. B. Arbeitszeiterfassung oder Kantinenabrechnung. – Dabei lassen sich auch bereits bewährte Wilka-Produkte, wie der modulare elektronische easy Schließzylinder, in die neue easyAccess Lösung integrieren. Ob als reines Offline-System oder in einer teilvernetzten Version mit Online-Geräten, die via IP-Netzwerk oder via Internet mit dem Server verknüpft sind, kann das System vielfach erweitert werden.

Mit easyAccess können, vom kleinen Handwerksbetrieb über mittel-

ständige Unternehmen bis hin zum großen Konzern mit mehreren Standorten, elektronische Schließanlagen komfortabel verwaltet werden. Je nach Anforderung zentral von einer Stelle aus oder lokal von jedem Standort individuell. Auch ein eigenes Modul für die zielgerichtete Verwendung in Hotels und Seminarhäusern mit Gästeverwaltung steht zur Verfügung.

Die mehrplatz- und serverfähige Software kann dabei eine Vielzahl von Anwenderwünschen erfüllen. Übersichtlich und einfach können Zutrittsberechtigungen vergeben und entzogen werden. Die einfache Schließplanmatrix erlaubt dem Anwender einen schnellen Zugriff auf alle Funktionen der einzelnen Geräte. Zeitliche Schließberechtigungen, je nach Ausbaustufe 30 bis 128, können ebenso vergeben werden wie Zutrittsberechtigungen für bestimmte Datumsbereiche (temporärer Zutritt). Durch die konsequente Verwendung von Gruppen bei Nutzern und Türen wird eine übersichtliche und strukturierte Darstellung erzielt. ■

Feststellbare Türdrücker

FSB hat die Verriegelungsfunktion von Türbeschlägen neu konzipiert und sie in die Türdrücker-Rosette integriert. Mit dem feststellbaren Türdrücker verzichtet der Hersteller auf eine zusätzliche Rosette für den Riegel. Bequem mit einer Hand bedienbar, liefert das Rosetten-Design mit integrierter Feststellfunktion eine technische Optimierung bei reduziertem Erscheinungsbild. Die Feststellfunktion befindet sich auf



der Türinnenseite. Mit einmaliger Betätigung des verbauten Druckknopfes wird die Verriegelung eingerastet und die Schlossbetätigung gesperrt.

www.fsb.de ■

PRAXISBERICHT KLINIK

Infektionsschutz am Entrée

Zutrittschleuse im Klinikum Herford knüpft Gebäudezutritt an Kontrolle der Körpertemperatur und die Einhaltung der Maskenpflicht

Systemrelevant und sensible Zone – dem Krankenhaus als medizinische Versorgungszentrale kommt während der anhaltenden Corona-Pandemie eine Schlüsselrolle zu. Infektions- und Gesundheitsschutz müssen hier allerhöchste Priorität besitzen. Daher hat sich das Klinikum Herford bei Bielefeld zur Umsetzung präventiver Schutzmaßnahmen während der Pandemie für eine smarte Lösung entschieden: Seit kurzem sorgt im Foyer ein Galaxyport Protect von Wanzl für eine automatische Zutrittskontrolle mit Infektionsschutz.

„Die Regierung formuliert gerade für uns als Klinik klare Anforderungen an den Infektionsschutz, weil er nirgendwo sonst so existentiell ist wie hier“, so Marco Kauling, Notarzt und Mitglied des Krisenstabes im Klinikum Herford. „Wir versorgen Risikogruppen, die für das Virus besonders anfällig sind. Außerdem

können wir auf keinen Mitarbeiter verzichten. Insgesamt haben wir im Haus 800 Betten, von denen derzeit 70 % belegt sind. Den Gebäudezutritt an die Kontrolle von Körpertemperatur und das Tragen des Mund-Nasen-Schutzes zu knüpfen, war daher schlichtweg notwendig.“

Für die Erstellung eines Konzepts zum Besuchermanagement orientierte sich das Klinikum Herford an den Empfehlungen des RKI und den ministerialen Vorgaben im Bundesland Nordrhein-Westfalen. „Seit Covid-19 sind wir zu einem standardisierten Besuchermanagement verpflichtet. Wir koppeln die Besuchserlaubnis an den laufenden 7-Tage-Inzidenzwert. Ist er zu hoch, gilt ein allgemeines Betretungsverbot. Währenddessen erteilen wir für Besuche nur Ausnahme Genehmigungen“, erklärt Marco Kauling weiter.

Temperatur und Maske im Check

Bewegt sich der Wert im akzeptablen Bereich, frequentieren täglich etwa 150 Besucher das Klinikum, dazu kommen 70 bis 100 ambulante Patienten. Sie alle dürfen erst passieren, wenn sichergestellt wurde, dass sie kein Fieber haben und die Maskenpflicht einhalten. Dank dem Galaxyport Protect von Wanzl kann das Klinikum diese Kontrollprozesse nun automatisieren und standardisieren. Es überprüft jeden Besucher mittels DSGVO-konformer Wärmebildkamera.

Ist seine Körpertemperatur im Normalbereich und trägt er einen Mund-Nasen-Schutz, öffnet sich blitzschnell die automatische Schwenktür aus transparentem ESG-Glas. Sollte erhöhte Temperatur festgestellt werden, misst ein Pförtner nach. Bei einer tatsächlichen Fieberprognose wird der Zutritt verweigert – zum Schutze der Patienten und auch der Mitarbeiter. Kauling äußert sich zufrieden: „Durch die automatische Zutrittslösung mit der integrierten Kamera vereinfachen wir die Kontrolle maßgeblich. Das Galaxyport Protect war rasch installiert und erleichtert unkompliziert unsere täglichen Abläufe. Lange Warteschlangen werden vermieden und auch für unsere Besucher wird die Kontrolle so komfortabler.“

Mit ihrer modularen Ausstattung ist die Zutrittsanlage zudem individuell konfigurierbar und auch die Durchgangsbreiten sind anpassbar – je nach Kundenbedürfnis und architektonischen Voraussetzungen im Gebäude.



Ist die Körpertemperatur im Normalbereich und trägt der Eintretende einen Mund-Nasen-Schutz, öffnet sich blitzschnell die automatische Schwenktür aus transparentem ESG-Glas. Sollte erhöhte Temperatur festgestellt werden, misst ein Pförtner nach



Ein Galaxyport Protect von Wanzl sorgt im Foyer des Klinikums Herford für eine automatische Zutrittskontrolle mit Infektionsschutz

Rückverfolgbarkeit im Krisenfall

Neben Kontrolle ist auch Datendokumentation Teil des Besuchermanagements – jeder Besucher ist verpflichtet, vorab einen Fragebogen auszufüllen, um im Krisenfall Infektionsketten rasch rückverfolgen zu können. Nach Abgabe des Fragebogens an der Pforte erfolgt schließlich die Kontrolle der Zutrittsberechtigung. Lediglich die Mitarbeiter erhalten separaten Zugang zum Gebäude. Das hat laut Kauling einen einfachen Grund: „Wir verlassen uns bei unseren Mitarbeitern darauf, dass sie eigenverantwortlich die Regeln einhalten und Selbstmonitoring über ihren Gesundheitszustand betreiben. Sie sind entsprechend geschult und sensibilisiert, daher ist ein tägliches Screening am Galaxyport Protect nicht notwendig. Die Zutrittskontrolle ist ausschließlich für externe Personen gedacht.“

Für Kauling hat diese Kontrolle auch einen ideellen Wert: „Wir schaffen Klarheit darüber, dass man sich hier im Klinikum in einer sensiblen Zone befindet. Ein Virus, das eingeschleppt wird und sich verbreitet, kann für unsere Patienten fatale Folgen haben. Hier stehen wir und unsere Mitarbeiter in der Verantwortung, bestmöglich vorzusorgen.“

Der gesamte Gebäudekomplex des Klinikums umfasst 18 Stationen auf neun Ebenen. Für alle Personen, die das Hauptgebäude betreten, führt der Weg durch das Foyer zu den Aufzügen in die verschiedenen Stockwerke. Direkt vor ihnen ist das Galaxyport Protect als Zugang zentral in der Halle positioniert. Seitlich an der Anlage angebracht, unterstützen Raumtrenner aus Edelstahl und ESG-Glas zusätzlich die Wegführung. Sämtliche übrigen Zugänge wurden zur Optimierung des Besuchermanagements im Zuge der Pandemie geschlossen – die Zutrittschleuse regelt den Gebäudezutritt am Haupteingang. Dabei ist sie zugleich barrierefreier Zugang und dient

als sicherer Fluchtweg, denn im Brandfall öffnen sich die ESG-Schwenkarme automatisch.

Flexibel konzipiert

Das Konzept des Zutrittssystems im Klinikum wurde von der Abteilung Bau und Technik gemeinsam mit Wanzl erarbeitet und stets modifiziert. Ralf Klemme, Leiter Bau und Technik im Klinikum Herford, erinnert sich: „Wir hatten durch Covid-19 ständig wechselnde Anforderungen an das System. Im letzten halben Jahr haben wir über die Art und den Verlauf der Krankheit viel dazu gelernt und daher Prozesse, wie etwa die Wegführung, immer wieder revidiert – hier waren wir begeistert von der Flexibilität von Wanzl, unseren Wünschen laufend nachzukommen. Dank diesem konsequenten Feintuning haben wir das Projekt mit einem hervorragenden Ergebnis realisiert.“

Ob die Technologie auch nach Covid-19 beibehalten wird? Kauling prognostiziert: „Sicherlich wird sich die Krankenhauswelt durch die Pandemie verändern, gerade was das Besuchermanagement betrifft. Die Häuser werden sich im Umgang mit externen Personen an neue, verbesserte Hygienekonzepte anpassen. Das Tragen einer Maske und ein Temperaturscan leisten nun mal einen wichtigen Beitrag zum Infektionsschutz, der in jedem Krankenhaus höchste Priorität hat. Das Galaxyport Protect vereinfacht nicht nur unsere Abläufe, sondern trägt auch zu mehr Verantwortungsbewusstsein bei – zum Wohle der eigenen Gesundheit und natürlich die der anderen.“ ■

Kontakt

Wanzl GmbH & Co. KGaA
Leipheim
Tel.: +49 8221 729 0
info@wanzl.de
www.wanzl.com



Immer für Sie aktiv

Special Nachhaltigkeit

Preise und Margen der Lebensmittelindustrie sind unter Druck. Neben der Marktmacht des Handels steigen Energie-, Wasser-, Rohstoff- und Personalkosten.

LVT LEBENSMITTEL Industrie berichtet über gangbare Lösungswege in Specials wie Nachhaltigkeit, Energieeffizienz und Qualitätssicherung.

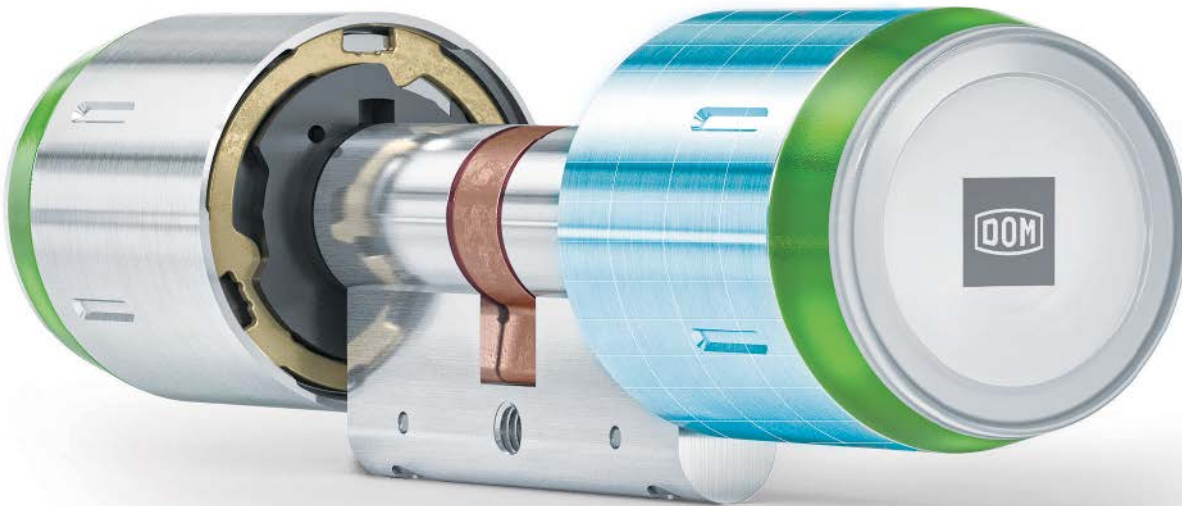
Dr. Jürgen Kreuzig
Chefredaktion
Tel.: +49 (0) 6201 606 729
juergen.kreuzig@wiley.com

Stefan Schwartze
Mediaberatung
Tel.: +49 (0) 6201 606 491
stefan.schwartze@wiley.com

Marion Schulz
Mediaberatung
Tel.: +49 (0) 6201 606 565
marion.schulz@wiley.com

ENTSCHEIDER KNOW-HOW FÜR FOOD & BEVERAGE
LVT LEBENSMITTEL
Industrie

www.LVT-WEB.de



Beschichtung genau auf den Flächen, die ein Anwender mit der Hand berührt

SCHLIESSYSTEME

Drei Mal Silber für die Sicherheit

Antimikrobielle Oberflächen für Beschläge, Zylinder und Panikstangen

Dom Security hat antimikrobielle Oberflächen für digitale Beschläge, digitale Zylinder und Panikstangen eingeführt. Dazu hat Dom mit zwei Unternehmen in Deutschland und Italien zusammengearbeitet: GB Neuhaus und Inver. Beide arbeiten mit Industrielacken und innovativen Beschichtungslösungen, insbesondere Lösungen mit Nanosilber bzw. Silberionen als Hauptbestandteil. GIT SICHERHEIT sprach darüber mit Thomas Schiffer, Produktmanager Elektronik bei Dom Sicherheitstechnik.



Thomas Schiffer, Product Manager Electronics – Dom Security

GIT SICHERHEIT: Herr Schiffer, Sie setzen bei Dom Sicherheitstechnik bei einigen Produkten Silberbeschichtungen ein – geben Sie uns einen Überblick?

Thomas Schiffer: Wir alle wissen inzwischen, wie oft wir uns am Tag unterbewusst mit den Händen ins Gesicht fassen und dabei Bakterien und Viren in unseren Mund-, Nasen- und Augenbereich übertragen. Dabei gehören Türdrücker und Türkäufe zu den Stellen, die von uns allen häufig am Tag angefasst werden. Mit den Anti-bakteriellen und antiviralen Beschichtungen auf den Knäufen des digitalen Zylinders Pro und auf den Drückern des digitalen Beschlags Guard

reduzieren wir massiv das Risiko, dass Bakterien und Viren von einem Anwender zum nächsten übertragen werden.

Dazu haben Sie sich mit Partnern zusammengetan?

Thomas Schiffer: Wir arbeiten hier mit GB Neuhaus zusammen – dieses Unternehmen ist auf solche anti-bakteriellen und anti-viralen Beschichtungen spezialisiert. Unsere Zusammenarbeit, unsere jeweiligen Erfahrungen und unser Know-how ermöglichten es, dass die antibakterielle und -virale Oberflächenbeschichtung, die wir einsetzen, langlebig auf Metall aufgebracht werden kann.



Dom setzt Nano-Silberbeschichtungen auf den Knäufen des digitalen Zylinders Pro und den Drückern des digitalen Beschlages Guard ein

Bei welchen Branchen und Kunden rechnen Sie mit der größten Nachfrage?

Thomas Schiffer: Viele Unternehmen versuchen ihren Mitarbeitern das Home-Office zu ermöglichen. Aber nicht immer ist das möglich – zum Beispiel, wenn die Grundvoraussetzungen wie etwa ein schnelles Internet beim Mitarbeiter zuhause nicht gegeben sind. Gerade im produzierenden Gewerbe ist es außerdem nahezu unmöglich, die Produktion nach Hause zu verlegen. Im medizinischen Bereich, bei Ärzten beispielsweise, ist es aufgrund des benötigten Equipments kaum möglich, alle Untersuchungen durch Hausbesuche stattfinden zu lassen. Sie müssen in den Räumen einer Arztpraxis durchgeführt werden. In Krankenhäusern ist es gar nicht möglich, weil Patienten meist stationär behandelt werden müssen und Patienten und Mitarbeiter permanent der Gefahr ausgesetzt sind, sich mit Bakterien und Viren anderer zu infizieren. Brandaktuell sehen wir, wie immens schwierig die Organisation ist, die Betreuung und Lehre von Kindern, Schülern und Studenten, ohne die Präsenz vor Ort in Kindergärten, Schulen und Universitäten durchzuführen. In diesen Branchen und Bereichen sehen wir im Moment das größte Nachfragepotential. Generell sehen wir aber eine Nachfrage bei allen Arbeitgebern, die ihre Kosten durch Krankheitsausfall von Mitarbeitern reduzieren wollen und müssen. Jedes Jahr fallen Mitarbeiter einige Tage bis Wochen durch saisonale Erkrankungen, wie z. B. die Grippe aus. Dies verursacht immense Kosten für die Arbeitgeber. Das Ansteckungsrisiko

Wirksam gegen schädliche Mikroorganismen

Zahlreiche Forschungsarbeiten zeigen, dass Silber das einzige chemische Element ist, das Schimmel, Bakterien, Viren und Pilze bekämpft. Nach 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 der menschlichen Haut in Kontakt kommt, reagieren die Silberionen mit der DNS der Bakterien und töten die Bakterien schließlich ab. Ein ähnlicher Effekt tritt bei Pilzen und Viren auf. Daher werden Silberionen oder Nanosilber als aktive Komponente in antimikrobiellen Beschichtungen und Farben eingesetzt.

Die Nanosilberbeschichtung wird auf den Metallelementen der Türgriffe der Dom Guard-Familie, den Metallknäufen des digitalen Schließzylinders Pro, sowie auf den Griffflächen der Panikstangen verwendet.

am Arbeitsplatz kann schnell durch entsprechende Schutzmaßnahmen, wie z. B. durch eine digitale Dom-Zutrittskontrollanlage mit entsprechenden antibakteriellen und antiviralen Oberflächen auf unseren Türverschlussgeräten Pro und Guard minimiert werden. ■

Kontakt

Dom Sicherheitstechnik GmbH & Co. KG
Brühl/Köln
Tel.: +49 2232 704 823
dom@dom-group.de
www.dom-security.com



Türdrücker FSB 1287 mit Anti-Infection-Coating

▲ Ergonomische Türdrücker mit Hygieneschutz

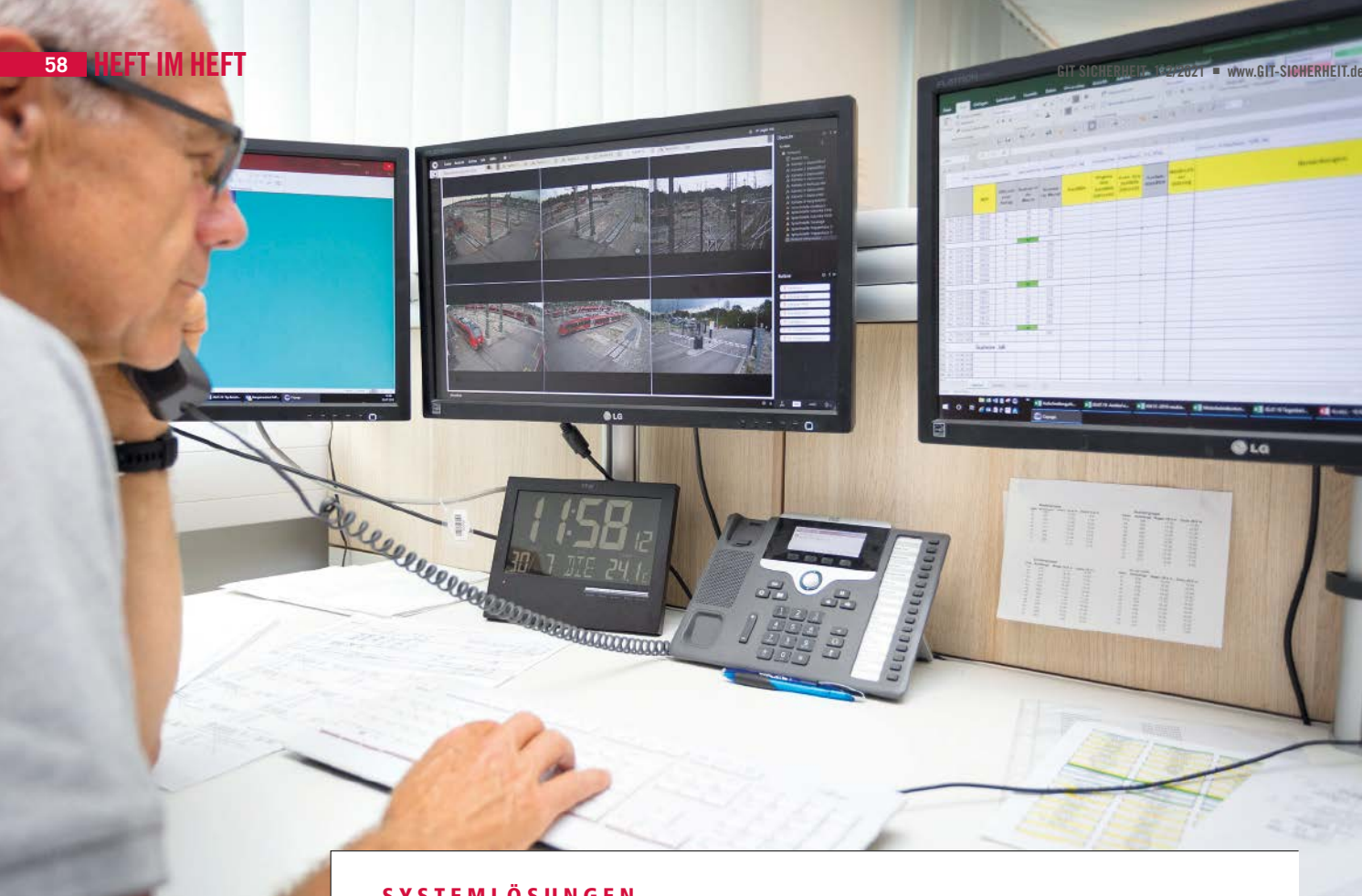
Der Türdrücker 1287 von FSB eliminiert den Kontakt der Hand zum Türdrücker und sorgt für erhöhten Infektionsschutz sowie eine neu gewonnene Freiheit der Hände. Zur Betätigung liegt der Unterarm auf dem abgewinkelten Ende des Drückers – dem Return – auf und bildet mit der nach oben gebogenen Handhabe einen Abschluss. Auf Grundlage statistischer Daten zu durchschnittlichen Körpermaßen wurde die Positionierung für den Return in einer Höhe von 111 cm identifiziert. Hier lässt sich der Arm besonders bequem auf den Türdrücker auflegen. Die Bedienung des objekttauglichen Entwurfs ist unabhängig von der Zugangsrichtung (links- oder rechtskommend) möglich. Neben einer sicheren Betätigung bleiben die Hände frei für den Transport medizinischen Equipments, das Tragen eines Tablett oder sonstiger Arbeitsgeräte. Der Drücker ist serienmäßig mit dem antibakteriellen Anti-Infection-Coating (AIC) beschichtet.

www.fsb.de ■

De Jong verlagert Produktion von Irm-Guard nach Holland

Aufgrund enorm gestiegener Nachfrage haben die Firmen de Jong Sicherheit & IT und Bravilor Bonamat eine enge Zusammenarbeit bei der Produktion der intelligenten Hygiene säule Irm-Guard vereinbart. Auch vertriebllich wird zukünftig intensiv zusammengearbeitet. Die weltweite Situation um Covid-19 stellt sehr viele Unternehmen vor besondere Herausforderungen. Mit so einer Nachfrage habe das Unternehmen nicht gerechnet, so Paul André de Jong, CEO von de Jong Sicherheit & IT. Die Produktionskapazitäten seien am Limit, die Kunden müssten derzeit schon Lieferzeiten von bis zu vier Wochen in Kauf nehmen. Durch die Verlagerung auf die vorhandenen Montagelinien von Bravilor Bonamat, die mit einem passenden Maschinenpark ausgestattet ist, könne de Jong die Produktion hochskalieren und nochmals die Effizienz und Qualität steigern, so Paul André de Jong.

www.dejong.gmbh ■



- ▲ Für eine schnelle Nachverfolgung unberechtigter Zutrittsversuche gibt es mehrere Alarmierungsoptionen

SYSTEMLÖSUNGEN

Bereit fürs Neue

Zukunftsorientierte Planung lässt die Zutrittskontrolle mit den Anforderungen an die Gebäudesicherheit mitwachsen

Eine elektronische Zutrittskontrolle dient dem Schutz von Gebäude und Gelände – das ist klar. Aber kann ein Zutrittssystem so geplant werden, dass es für andere Aufgaben gerüstet ist? Für Zutritts- und Gebäudesicherheitsspezialist PCS ist die Antwort eindeutig: es ist ein großer Vorteil, wenn auch weitergehende Anforderungen rund um die Gebäudesicherheit umgesetzt werden können.

Gerade in den letzten Monaten konnten wir erleben, dass neben der physischen Sicherheit plötzlich auch Maßnahmen für den Gesundheitsschutz im Unternehmen gefragt waren, zum Beispiel Personenzählsysteme oder ein Körpertemperaturscreening an der Vereinzelungsanlage. Um solche neuen Funktionen umzusetzen, empfiehlt PCS eine leistungsfähige Zutrittskontroll-Software mit flexiblen Schnittstellen zu anderen Gewerken. So können präventive Schutzmaßnahmen sehr gut mit der Zutrittskontrolle verbunden werden.

Verlässliche Sicherheit und komfortable Anwendung bilden den Spannungsbogen für alle Aufgaben der Gebäudesicherheit. Das System soll sich bestmöglich in die Abläufe integrieren

und keinen Hemmschuh im Arbeitsalltag darstellen, sonst leidet die Akzeptanz.

Die Grundprinzipien der Unternehmenssicherheit bestehen aus den vier Eckpunkten:

- Absicherung von unterschiedlich risikorelevanten Zonen
- Überwachung von Eintrittszonen
- Einlass nur nach positiver Kontrolle
- Benachrichtigung im Falle eines Ereignisses und Alarmierung

Neue Aufgaben in Ausnahmesituationen

RFID-Zutrittsleser sind heute der aktuelle Stand der Sicherheitstechnik. Mit verschlüsselter Datenübertragung ist ein hoher Sicherheitsstandard gegeben. Wichtig dabei ist eine



▲ Gibt es an einem Sammelplatz einen Notfall-Leser, können die geretteten Mitarbeiter ihre Anwesenheit buchen und müssen nicht einzeln gezählt werden



▲ RFID-Leser übernehmen neue Aufgaben in Ausnahmesituationen

Auswahlmöglichkeit für die unterschiedlichsten Montagebedingungen, z. B. für Auf- oder Unterputz, Einbau in Norm-Schalterprogramme, Montage auf Zargen, auf Metall oder als wetterfester Leser für den Außenbereich. Neben der Zutrittssteuerung eignen sich die RFID-Leser auch für Positiv-Buchungen verschiedenster Art: sie können z. B. in Zeiten einer Pandemie zur Personenzählung für eine Raumzone genutzt werden. Dafür erhält ein Bereich jeweils einen Eintritts- und Austrittsleser, den jede Person nutzt. Ist der Raum vollzählig besetzt, ist kein weiterer Zutritt mehr möglich.

Diese sogenannte Bilanzierung ist auch für andere Fälle geeignet, etwa für eine Evakuierung im Notfall: Gibt es an einem offiziellen Sammelplatz einen Notfall-Leser, so können die geretteten Mitarbeiterinnen und Mitarbeiter ihre Anwesenheit buchen und müssen nicht einzeln gezählt werden. Auch Hygienemaßnahmen lassen sich umsetzen: Die DI/DOs können zur Aktivierung einer Motorsteuerung genutzt werden, so dass sich Türen nach Anmeldung am Leser ohne direkten Kontakt öffnen.

Management der Gebäudesicherheit

Damit ein Sicherheitssystem so flexibel reagiert, ist eine konfigurierbare Software Voraussetzung. Als lösungsorientiertes Managementsystem agiert zum Beispiel die PCS-Software Dexicon Enterprise. Sie verwaltet alle beteiligten Komponenten, sowohl die Personen als auch die physischen Zutrittskomponenten wie Zutrittsleser und übergeordnete Steuereinheiten. Funktionen wie Türoffenzeitüberwachung, Anti-Passback

oder Aufenthaltsdauerüberwachung sind intelligente Sicherheitsmaßnahmen, um die Gebäudesicherheit zu gewährleisten.

Verknüpfung von Video oder Einbruchmeldeanlage

Besonders hilfreich ist die Lösung bei der Kombination mit anderen Gewerken, z. B. einer Videoüberwachung oder der Ansteuerung der Einbruchmeldeanlage. So fordern Ereignisse in der Zutrittskontrolle Videobilder an, die direkt beim Zutrittsereignis gespeichert werden. Komfortabel ist das Bedienen der Einbruchmeldeanlage: ein Mitarbeiter schaltet abends die EMA scharf durch Karten-Buchung oder Eingabe eines PINs am Zutrittsleser. Dexicon ermöglicht diese kombinierten Funktionen durch die Vielzahl von Schnittstellen, z. B. Webservice-Interface, zertifizierte SAP-Schnittstelle, Interface zur Kennzeichenerkennung.

Will man als Unternehmen noch weitere Gewerke der Sicherheitstechnik integrieren, so bietet sich ein Gefahrenmanagementsystem (GMS) an. Dexicon kann über seinen OPC-Server mit einem solchen integriert werden.

Alarmierungsoptionen für schnelle Nachverfolgung

Gibt es Auffälligkeiten in der Zutrittskontrolle, ist eine schnelle Alarmierung sinnvoll. Für die Benachrichtigung des Wachdienstes gibt es bei Dexicon mehrere Möglichkeiten, zuständiges Personal zu verständigen: so kann eine Email-Benachrichtigung abgesetzt werden, z. B. auf ein Smartphone, das ein Wachdienst immer bei sich hat. Eine Trigger-Option

sorgt für Abschreckung und das Auslösen einer Alarmierung z. B. durch Signale eines Weißlichtscheinwerfers oder durch eine Lautsprecher-Ansage.

Zufahrtskontrolle per Kennzeichenerkennung

Die Zutrittskontrolle zum Gebäude kann auf Parkplätze und Tiefgaragen ausgedehnt werden. Mehr und mehr setzt sich die Kennzeichenerkennung via Kamera und Kennzeichenerkennungssoftware durch. Sie eignet sich besonders gut, wenn regelmäßig auch Besucher in die Tiefgaragen oder Lieferantens ins Werksgelände einfahren. Kfz-Kennzeichen werden bei der Besuchsanmeldung registriert und ermöglichen ein bequemes Einfahren in die Garage bzw. aufs Gelände.

Vorangemeldete Besucher können sich anschließend am Self-Service-Terminal selbstständig registrieren und einen Besucherausweis oder eine Sicherheitsunterweisung absolvieren. Mit solch einem Netz an umfassenden Schutzmaßnahmen für Gebäude und Gelände ist man bestens vorbereitet auf die Zukunft, was immer auf uns wartet: Die Unternehmenssicherheit wächst mit ihren Aufgaben. ■

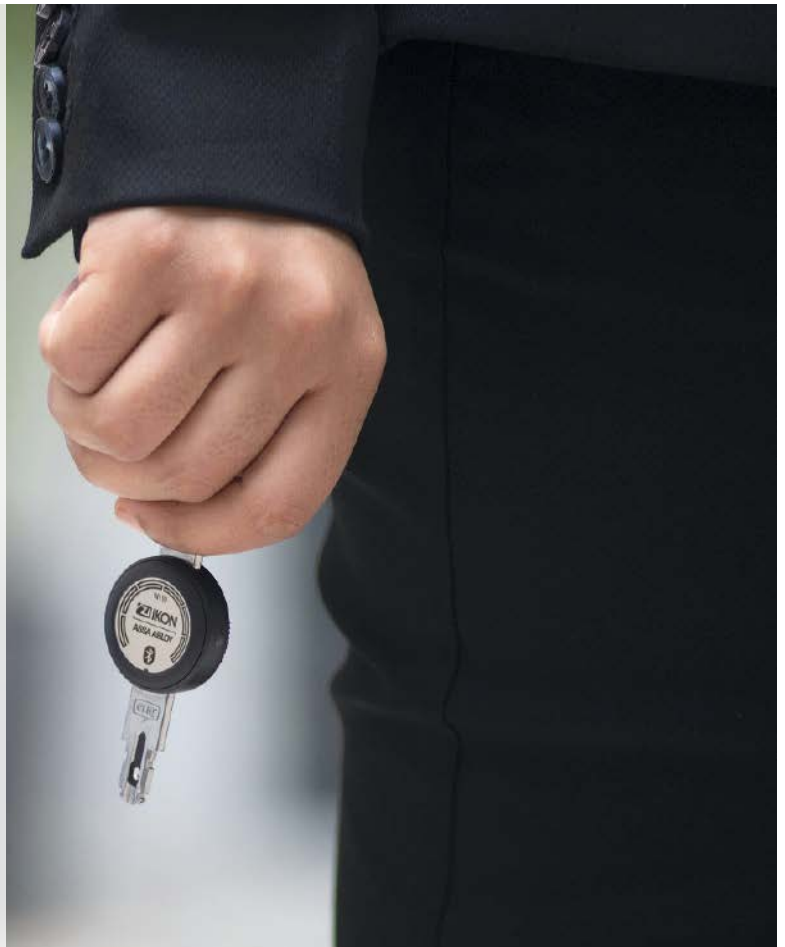
Kontakt

PCS Systemtechnik GmbH
München
Tel.: +49 89 68004 253
splank@pcs.com
www.pcs.com

KRITISCHE INFRASTRUKTUREN

KRITIS: Kriterien für ganz- heitliche Sicherheit

Mechanische und elektronische Schließanlagen im Wandel der Sicherheitstechnik



Betreiber Kritischer Infrastrukturen (KRITIS) sollten ein ganzheitliches Sicherheitskonzept verfolgen, das neben der IT-Sicherheit und dem Datenschutz auch die physische Sicherheit berücksichtigt. Assa Abloy Sicherheitstechnik stellt im folgenden Beitrag für GIT SICHERHEIT eine Planungsgrundlage für elektronische Schließanlagen vor und erläutert, worauf KRITIS-Institutionen bei der Auswahl eines geeigneten Systems achten sollten.

Auf 205,7 Milliarden Euro beläuft sich aktuellen Schätzungen zufolge der Gesamtschaden, der deutschen Unternehmen allein durch digitale Angriffe oder andere IT-Sicherheitsprobleme in den Jahren 2018 und 2019 entstanden ist. Und die meisten Unternehmen rechnen sogar fest mit einer weiteren Zunahme von Security-Vorfällen in den nächsten Jahren. Betreiber Kritischer Infrastrukturen (KRITIS) sind mindestens genauso lukrative Angriffsziele für Cyber-Attacks oder Vandalismus, besitzen jedoch ein besonders hohes Schadenspotenzial in Bezug auf ihre hohe Relevanz für die Gesellschaft.

Technische Leiter Kritischer Infrastrukturen (KRITIS) sehen sich heute mit stark veränderten Sicherheitsanforderungen konfrontiert. Die verpflichtende Umsetzung definierter Mindeststandards für IT-Sicherheit ist nur ein Beispiel dafür. Zum Schutz gegen

Cyberattacken oder Vandalismus müssen die Sicherheitsverantwortlichen diese Veränderungen und immer neue gesetzliche Vorschriften berücksichtigen und jederzeit adäquat darauf reagieren. Keine einfache Aufgabe, wenn man bedenkt, dass die Institutionen allein personell kaum mit der rasanten Entwicklung und den zunehmenden Verantwortlichkeiten Schritt halten können.

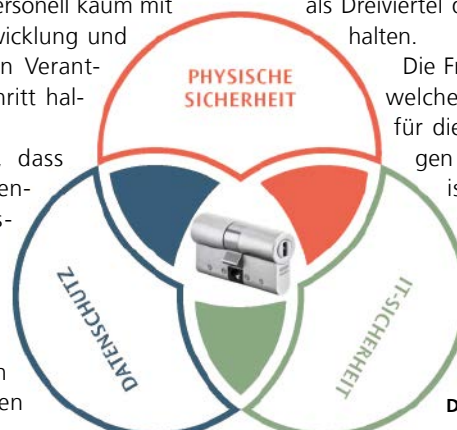
Hinzu kommt, dass auch die bestehende Sicherheitstechnik an sich laufend auf dem neuesten Stand gehalten werden muss. Im Bereich von Schließanlagen

bieten elektronische und vernetzte Schließsystemlösungen für Rettungswege und Brandschutz inzwischen deutliche Vorteile gegenüber rein mechanischen Systemen. Sie ermöglichen darüber hinaus eine einfache und ressourcenschonende Schließanlagenverwaltung für das Facilitymanagement.

Spezialanbieter für Schließlösungen

Aufgrund der steigenden Nachfrage nach modernen Schließanlagen mit möglichst komfortabler Schließanlagenverwaltung ist auch die Anzahl der Anbieter und Systeme in den letzten Jahren deutlich gewachsen. Der deutsche Markt fokussiert sich aber auf fünf nennenswerte Unternehmen, die mehr als Dreiviertel der begehrten Marktanteile halten.

Die Frage, welcher Anbieter und welche Systeme die passendsten für die individuellen Anforderungen von KRITIS-Betreibern sind, ist dennoch nicht spontan zu beantworten. Auch



◀ KRITIS-Betreiber sollten bei der Planung einer Schließanlage auf den Dreiklang aus physischer Sicherheit, IT-Sicherheit und Datenschutz achten

◀ **KRITIS sind wegen ihrer hohen Relevanz für die Gesellschaft lukrative Ziele für Cyber-Attacks oder Vandalismus. Im Sicherheitskonzept sind innovative, zukunftssichere Schließsystemlösungen deshalb unerlässlich**

wenn erfahrungsgemäß das Budget nicht immer die wichtigste Rolle spielt, so berichten doch viele Sicherheitsverantwortliche von nicht nachvollziehbaren Kostenexplosionen und teilweise ärgerlichen Terminverzögerungen in der Zusammenarbeit mit verschiedenen Dienstleistern. Das ist einer der Gründe dafür, weshalb der Bedarf nach objektiven und fundierten Entscheidungshilfen für die Auswahl des passenden Schließsystems und Anbieters größer wird.

Mechanische und elektronische Schließanlagen im Vergleich

Tatsächlich gibt es die „beste“ Schließanlage nicht. Allerdings sind mechatronische und elektronische Schließsysteme heute wesentlich flexibler als rein mechanische Systeme. Das gilt sowohl für ihre vielseitigen Einsatzmöglichkeiten als auch die zeitgemäße Bedienbarkeit und komfortable Verwaltung. Da bei elektronischen Systemen die mechanische Freigabe des Schließzylinders durch eine

elektronische Variante ergänzt oder ersetzt wird, kommen heute Chipkarten (Badges), Transponder, elektronische Schlüssel oder auch das Smartphone als Ersatz für mechanische Schlüssel in Betracht. Erst diese digitale Ebene erlaubt die außergewöhnlich leichte und einfache Vergabe und Änderungen von individuellen Zutrittsberechtigungen, die auch zeitlich oder räumlich in einem Gebäude begrenzt werden können.

Kriterien für die Planung

Allen KRITIS ist ihre elementare Bedeutung für die Gesellschaft gemein, dennoch ist die Auswahl eines geeigneten Schließsystems für eine Institution zunächst von ganz individuellen Anforderungen abhängig, die sich in den Bereichen Energie, Gesundheit, Wasser oder Ernährung durchaus unterscheiden können. Die zusätzlichen Herausforderungen durch sich ändernde gesetzliche Bestimmungen machen die Planung insgesamt sehr komplex. Vereinfachend lassen sich aber ein paar allgemeine Kriterien definieren, an denen sich die erste Bedarfsabfrage und danach die detaillierte Planung orientieren kann.

Eines dieser Kriterien sind beispielsweise die Schließzylinder und die Frage, welche Eigenschaften sie haben sollen und müssen. Es geht weiter mit Software und Vernetzung und

Einfacher und schneller Einbau der Zylinder ohne Verkabelung

Neue, zukunftssichere CLIQ® Chip-Generation mit AES-Verschlüsselung und schneller Verarbeitungsgeschwindigkeit bei einem effizienten Energiemanagement.

Der elektronische Kontakt zwischen Schlüsseln und Schließzylindern dient der sicheren Strom- und Datenübertragung

Rotor
Feder mit Massekontakt
Motor

Schlüssel und Zylinder können mit flexiblen Schließberechtigungen und Zeitplänen programmiert werden

Wasser- und staubdichte Schlüsselreide mit Batterie und Elektronikboard
Schneller Wechsel der Standardbatterie im Schlüssel – ohne Werkzeugeinsatz

VdS
PIVCERT
DIN certified
Ex
SKG

Mechatronische und elektronische Schließsysteme sind heute wesentlich flexibler als rein mechanische Systeme. Das gilt sowohl für ihre vielseitigen Einsatzmöglichkeiten als auch die zeitgemäße Bedienbarkeit und komfortable Verwaltung

Jetzt LESER werden!

Lesen Sie die inspect oder messtec drives Automation jederzeit und überall.

Registrieren Sie sich auf:
www.wileyindustrynews.com



der Frage, ob eher eine kabelgebundene oder funkvernetzte Online-, bzw. Offline-Schließanlage geeignet sein könnte. Abschließend sind auch die erforderlichen Spezifikationen der Beschlagsysteme ein wichtiges Kriterium der Bedarfsanalyse.

Dass letztere sich ebenfalls in moderne Schließanlagen integrieren lassen, ist zwar bekannt und gerade in der Hotelbranche wegen des schlüssellosen Nutzerkomforts weit verbreitet. Sie erfordern aber auch einen etwas höheren Planungs- und Montageaufwand, da sie auf eventuell bereits vorhandene Türen angepasst werden müssen und die entsprechenden Zulassungen benötigen. Allerdings spielen mechatronische und elektronische Beschlagsysteme inzwischen auch im Sicherheitskonzept von KRITIS in Deutschland eine immer größere Rolle.

Die Qual der (Aus)Wahl

Ist die Bedarfsabfrage Schritt für Schritt klar geworden, stehen vor der endgültigen Auswahl eines passenden mechatronischen oder elektronischen Schließsystems noch verschiedene weitere Einflussfaktoren, die ebenfalls berücksichtigt werden müssen. Dazu gehören grundlegende Überlegungen zu den anfallenden Investitionskosten genauso wie ein klarer Überblick über die unzähligen Anbieter und verschiedenen Systeme – inklusive ihrer jeweiligen Vor- und Nachteile.

Die umfassende Bedarfsanalyse und systematische Auflistung der individuellen Anforderungen hilft bei der Entscheidung und kann wertvolle Hinweise liefern, mit denen sich eine unternehmerisch tragfähige Investitionsrechnung aufstellen lässt. Vor der Entscheidung für eine konkrete Schließanlage sollte es dann beispielsweise eindeutige Antworten auf folgende Fragen geben:

- Wie hoch sind die Investitionskosten (CAPEX) sowie die geschätzten Folgekosten, Betriebs- und Verwaltungskosten (OPEX)?
- Wie lang ist die voraussichtliche Nutzungsdauer?
- Wie hoch ist die Investitionssicherheit?
- Werden die unternehmensspezifisch zwingenden Muss-Anforderungen erfüllt?
- In welcher Güte werden die unternehmenseigenen Soll-Anforderungen erfüllt?

IT-Sicherheit mit etabliertem Schwachstellenmanagement

Bei allem Bestreben nach Kosteneffizienz sollte der Hersteller dennoch so ausgewählt werden, dass die Anlage inklusive der Software auch nach vielen Jahren noch auf dem Stand der Technik und der IT-Sicherheit ist. Dann rentiert sich auch eine hohe Investition, sowohl für die Betreiber als auch für die

Nutzer des Systems. Dem liegt die Tatsache zugrunde, dass sich im Laufe des Lebenszyklus einer Anlage die Software mehrfach technisch überholen wird.

Seriöse Hersteller stellen deren Nachhaltigkeit sicher, in dem sie bereits bei der Software-Entwicklung auf einen ISO-27001-konformen Prozess setzen. Dieser beinhaltet unter anderem bestimmte Informations- und Zugangssteuerungsrichtlinien oder auch Maßnahmen zur Personalsicherheit sowie umfangreiche Dokumentationsmöglichkeiten.

Der Hersteller sollte zudem ein Schwachstellenmanagement in der Software implementiert haben, das Penetrationstests erlaubt, um Schwachstellen des Systems vorausschauend zu identifizieren, zu eskalieren, zu beheben und zu verteilen. Software-Updates und -Upgrades sollten darüber hinaus über ein Supportverfahren geregelt sein, bei dem ein fachlicher Ansprechpartner zeitnah helfen kann.

Entscheidungshilfe für die passende Schließsystemlösung

Mit dem Whitepaper „Entscheidungsgrundlagen für elektronische Schließanlagen“ bietet Assa Abloy eine Planungshilfe an, die die wichtigsten Fragen gleichzeitig mit einer Bewertungsmatrix mit gewichtetem Punkteverwertungsverfahren und definierten Muss- und Sollenanforderungen verknüpft.

Des Weiteren beinhaltet die Planungsgrundlage viele nützliche Checklisten für die oben bereits erwähnte Bedarfsermittlung zur Auswahl und Planung der geeigneten Schließanlage. Enthalten sind außerdem Informationen über die wichtigsten Hersteller und Spezialanbieter sowie ausführliche Portraits und Erklärungen zu den unterschiedlichen Mechaniken, Sicherheitsniveaus und Komponenten elektronischer Schließanlagen. ■

Das Whitepaper „Entscheidungsgrundlage für elektronische Schließanlagen“ zum kostenlosen Download



<https://bit.ly/2XJtMlY>

Kontakt

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

WEBSEMINAR

Bevor die Hacker kommen

Cyber-Angriffe auf Krankenhäuser werden häufiger und zerstörerischer – was tun? Ein Webseminar von Wiley und Veeam am 23. Februar gibt Aufschluss

Tatort Krankenhaus: immer wieder werden Gesundheitseinrichtungen zum Ziel von Cybergangstern. Haben Hacker noch nicht zugeschlagen, bleibt Kliniken Zeit für die Vorbereitung auf den Ernstfall. So können diese sensible Daten schützen und den Betrieb aufrechterhalten.

Mit der zunehmenden Digitalisierung und Vernetzung im Gesundheitswesen steigen auch die Komplexität und die Gefahr von IT-Schwachstellen, die Hacker als Einfallstor nutzen könnten. Angriffe sind nicht vermeidbar, aber Schadensbegrenzung extrem wichtig.

Im Idealfall kann mit Prävention eine Attacke unterbrochen werden - zumindest aber läuft bei entsprechenden Vorkehrungen der Betrieb schnell wieder an und es wird verhindert, dass Daten gestohlen werden oder verloren gehen. Der Maßnahmenkatalog dafür umfasst:

- ein zuverlässiges Datensicherungskonzept
- einen „unlöschen“ Backup-Speicher



© Goradenkoff Productions QJ / AdobeStock.com

- ein Backup ohne Viren
- einen detaillierten Plan für die richtige Abfolge beim Restart
- sowie ein komplettes Notfallsystem, das offline bereit steht.

Kontinuierliche Datensicherung ist die Basis – für den Tagesbetrieb ebenso wie den Disaster-Fall. Dafür empfiehlt Veeam die „3-2-1-1-0-Strategie“: drei Backup-Kopien gespeichert auf zwei unterschiedlichen Medien, davon ein Voll-Backup extern gelagert

und ein weiteres offline, „air-gapped“: Auf dieses Backup sollte kein Online-Zugriff möglich sein und es sollte nicht löschar sein. Werden Backups automatisch auf Wiederherstellbarkeit und Viren getestet, erspart das böse Überraschungen bei der Wiederherstellung.

Manuelle Prozesse bedeuten Stress und potenzielle Fehler im Ernstfall. Werden Restart-Prozesse im Vorfeld geplant, getestet und verifiziert – und mit einer Orchestrierungssoftware automatisiert – kann der Betrieb schnellstmöglich wiederanlaufen.

Vorbereitung ist die beste Abwehrstrategie. Planen, automatisieren, testen und trainieren. So steigern Kliniken - aber auch anderen Institutionen und Branchen - ihre Wiederanlaufbarkeit, ihre Resilienz und ihre Verfügbarkeit.

Weitere Infos zu den Experten von Veeam unter: www.veeam.com/de

© Foto: Veeam Software



André Walsleben, Director Public,
Veeam Software Germany

In Zusammenarbeit mit der Fachzeitschrift Management & Krankenhaus laden wir Sie ein zur kostenfreien Teilnahme am Webseminar von **Veeam und Wiley am 23. Februar 2021** von 14 bis 15 Uhr. André Walsleben, Director Public bei Veeam Software Germany, spricht zum Thema „Ransomware in KRITIS-Infrastrukturen: Seien Sie vorbereitet!“

Dieses Webseminar richtet sich an Führungskräfte und IT-Verantwortliche (nicht nur) in Kliniken, Krankenhäusern und Gesundheitseinrichtungen.

Es liefert praktische Tipps sowohl für Einsteiger als auch für fortgeschrittene Simulationsanwender.

Link zu Infos und Anmeldung:

<https://bit.ly/35Gnkvi>



QR zur Information und Anmeldung ►

CYBER SECURITY

Cybersicherheit und Resilienz

Wie mobiles Arbeiten und Arbeiten im Homeoffice sicher gelingt

Die meisten modernen Bürojobs lassen sich völlig standortunabhängig durchführen. Wie gut das funktionieren kann, haben uns die vergangenen Monate gezeigt. Daher wird mobiles Arbeiten vermutlich auch nach Ende der Pandemie weiterhin ein wichtiger Teil der Wirtschaft sein. Das hat allerdings auch Implikationen auf die Cybersicherheit und somit die Resilienz von Unternehmen, wie Tiago Dias, Cyber Security Consultant bei FM Global, darlegt.

COVID-19 hat den meisten Unternehmen erst die Vorteile der Online-Kommunikation und die Effektivität des mobilen Arbeitens im sogenannten Homeoffice vor Augen geführt. Diese Arbeitsmethode ist auch wesentlich kostengünstiger als das Anmieten herkömmlicher Büroräume – daher werden wohl viele Unternehmen zögern, zum alten Präsenzsystem zurückzukehren, da sie Büros als veraltet und unnötig teuer empfinden könnten.

Resilienz in verteilten Infrastrukturen

Dieser revolutionäre Wandel in der Arbeitswelt löst jedoch auch Bedenken in Bezug auf die Cyberresilienz aus, denn diese „verteilte Arbeit“ auf unterschiedlichste Standorte bringt gewisse Risiken mit sich. Viele Unternehmen sind aktuell verwundbarer denn je, da sie eine große Zahl an Geräten managen müssen, die sich außerhalb traditioneller Sicherheitssysteme befinden. IT-Sicherheitsexperten sollten sich daher der größeren Gefahr für ihr Unternehmen bewusst sein und dabei helfen, die Cyberresilienz gegenüber den aktuellen Bedrohungen zu stärken.

Durch die neue verteilte Arbeitsweise wird der digitale Fußabdruck von Organisationen größer denn je. Außerdem gibt es viel weniger Standardisierung, wenn jeder Mitarbeiter sein eigenes WLAN-Netzwerk nutzt, oder womöglich auch eigene Geräte. Durch diesen größeren Fußabdruck ergeben sich auch ganz neue Angriffspunkte, die Hacker nutzen können. Das kann sogar zu physischen Schäden an Immobilien führen, indem sich Kriminelle Zugang zu Gebäudemanagement- oder Notfallsystemen verschaffen.

Eine weitere Herausforderung, die durch die Zunahme des mobilen Arbeitens entsteht, ist die Überforderung von internen Systemen und VPNs durch die erhöhte Anzahl von Nutzern, die sich gleichzeitig von externen Systemen aus verbinden. Diese Belastung der bestehenden digitalen Infrastruktur kann erhebliche Schwachstellen für Unternehmen mit sich bringen und gleichzeitig die Produktivität und Effizienz beeinträchtigen. Systeme, die für den Zugriff einer begrenzten Anzahl von Personen konzipiert wurden, müssen jetzt und in Zukunft viel mehr Traffic verarbeiten. In diesem Fall muss nicht nur die

Bandbreite größer sein, sondern es müssen auch Sicherheitswerkzeuge wie Firewalls geprüft werden, um festzustellen, ob sie dem größeren Datenaufkommen gewachsen sind. Im Zusammenhang mit den Problemen, die durch einen Mangel an Standardisierung verursacht werden, kann es sein, dass verschiedene Mitarbeiter unterschiedliche Firewalls verwenden, die nicht alle gleich gut mit dem erhöhten Zugriff von außen zurechtkommen.

Unternehmen, die diese Probleme ernsthaft angehen und sich auf die neue Realität des mobilen Arbeitens einstellen, können sowohl während der COVID-19-Krise, als auch in einer Welt nach der Pandemie die größtmögliche Sicherheit im Cyberspace schaffen.

Neue Sicherheitsmaßnahmen für eine neue Realität

Ein erster Schritt für Unternehmen, die ihre Resilienz erhöhen wollen: Zusätzliche Sicherheitsüberprüfungen innerhalb der IT-Systeme initiieren und so eine weitere Sicherheitsebene schaffen. Organisationen sollten über digitale Kontrollpunkte verfügen, um die richtigen Personen zu autorisieren und Cyberkriminelle

am Zugriff auf sensible Systeme zu hindern. Dies kann zum Beispiel mit Firmen-Laptops erreicht werden, die spezifische Kontrollen oder eine Multifaktor-Authentifizierung für den VPN-fähigen Fernzugriff verwenden – jede Methode fügt eine weitere Abwehrschicht hinzu, um sicherzustellen, dass die Personen mit entsprechendem Zugriff eine geschützte Verbindung herstellen können.

Ein weiterer Aspekt, den Unternehmen in Bezug auf die Cyberresilienz berücksichtigen müssen, ist die Bedeutung eines aktuellen Krisenplans. Die Pandemie hat deutlich gemacht, wie unvorhersehbare Ereignisse, die scheinbar nichts mit der Cybersicherheit zu tun haben, in Zukunft angemessen berücksichtigt werden müssen. Als Grundvoraussetzung muss man die Gefährdung durch Cyberrisiken verstehen und wissen, welche Bereiche möglicherweise mehr Aufmerksamkeit benötigen. Verfügt das eigene Unternehmen über die richtigen Richtlinien und Verfahrensweisen? Und wird der Krisenplan regelmäßig aktualisiert, um neuen

potenziellen Schwachstellen Rechnung zu tragen? Diese Fragen müssen mit ausreichend Verständnis dafür beantwortet werden, welches die geschäftskritischen Prozesse sind und wie diese angemessen geschützt werden können.

Wichtig bei der Bewertung von Cyberrisiken ist es auch, die Versicherer ins Boot zu holen. Methoden wie das Cyber Risk Assessment von FM Global können dabei helfen, Cyberrisiken in den eigenen Geschäftsmodellen besser zu verstehen. Diese Informationen als Grundlage für einen belastbaren Krisenplan zu nutzen, ist von entscheidender Bedeutung – denn Corona hat gezeigt, dass die Widerstandsfähigkeit des Cyberspace auch durch Ereignisse, die nicht direkt mit der digitalen Technologie zusammenhängen, beeinträchtigt werden kann.

Fazit

Es ist jetzt klar, dass die COVID-19-Pandemie einen großen Einfluss auf die Cyberresilienz haben wird, selbst wenn der Höhepunkt der

Pandemie überstanden ist. Obwohl Änderungen der Betriebsstrukturen aus der Notwendigkeit heraus und oft sehr schnell vorgenommen wurden, ist es wahrscheinlich, dass mobiles Arbeiten noch lange eine gängige Praxis bleiben wird. Cyber-Risk-Experten müssen diesen Trend ernst nehmen: Sie tragen die Verantwortung dafür, dass es im Homeoffice zu keinen digitalen Gefahren kommt. Vor ihnen steht die große Aufgabe, die Sicherheitsmaßnahmen des Firmennetzwerks für jeden Mitarbeiter an seinem heimischen Arbeitsplatz zu replizieren. Das ist eine beachtliche Herausforderung. Aber andernfalls riskieren Unternehmen, dass sie unter der neuen Realität leiden. ■

Kontakt

FM Global
Frankfurt
Tel: +49 69 1540 60
www.fmglobal.de

Gute Bewertung für Firewall

Die Web Application Firewall von Rohde & Schwarz Cybersecurity ist im Gartner Peer Insights „Voice of the Customer“: Web Application Firewalls Report mit 4,6 von 5 Punkten bewertet worden. Laut dem Bericht gaben 92 % der Kunden eine „Bereitschaft zur Weiteremp-

fehlung“ an. Die Web Application Firewall schützt geschäftskritische Webanwendungen – einschließlich bestehender Legacy-Anwendungen und kundenspezifischer APIs – vor bekannten und unbekanntem Angriffen und ist eine Sicherheitslösung für Unternehmen und Behörden. Sie erfüllt sowohl spezifische Entwicklungsanforderungen als auch die Anforderungen von Infrastrukturmöglichkeiten und Sicherheitsrichtlinien. Die hochskalierbare Lösung kann vor Ort, in der öffentlichen Cloud und in Hybrid-/Multi-Cloud-Umgebungen eingesetzt werden.

www.rohde-schwarz.com/cybersecurity ■



Erhöhtes Risiko von Cyberangriffen

Trend Micro veröffentlicht Studienergebnisse, wonach 75 Prozent der Unternehmen in Deutschland in den vergangenen zwölf Monaten Cyberangriffe erlebten, die ihre Netzwerke oder Systeme infiltrieren. Die Mehrheit (64 Prozent) der befragten Unternehmen in Deutschland erwartet, dass solche Angriffe in den nächsten zwölf Monaten „etwas“ bis „sehr“

wahrscheinlich erneut vorkommen werden. Die Erkenntnisse stammen aus der neuesten Version des Cyber Risk Index (CRI). Dieser Index wird vom unabhängigen Ponemon Institute berechnet und beschreibt die Differenz zwischen dem aktuellen Sicherheitsniveau von Unternehmen und der Wahrscheinlichkeit eines Angriffs. www.trendmicro.com ■

Hochleistungs-Rugged-Edge-Computer

Die Edge-Computer der MC-1220-Serie von Moxa sind mit einem leistungsstarken Intel Core i7/i5/i3-Prozessor und mehreren Erweiterungsschnittstellen ausgestattet. Die Erweiterungsschnittstellen können Hardwarebeschleuniger wie VPUs enthalten und unterstützen das Intel OpenVIN-Toolkit für die Entwicklung von AIoT-Anwendungen. Die lüfterlosen Computer können in einem breiten Betriebstemperaturbereich betrieben werden und sind „C1D2/ATEX Zone 2“-zertifiziert für Einsätze im Freien und in gefährlichen Umgebungen. Durch ihre geringe Größe können sie leicht in kleine Schaltschränke vor Ort eingebaut werden. Die Computer der MC-1220 Serie unter-



stützen mehrere Wi-Fi/Mobilfunk-Konnektivitätsoptionen. Dadurch entfällt die Notwendigkeit eines zusätzlichen drahtlosen Gateways. Die Computerplattform ist mit der TPM 2.0-Technologie für verbesserte Hardwaresicherheit ausgestattet. www.moxa.com ■

Mehr Angriffe auf das Gesundheitswesen

Bedingt durch die Corona-Pandemie hat das Thema IT im Gesundheitswesen an Brisanz gewonnen, wie Kaspersky mitteilt. Das Unternehmen geht davon aus, dass es im kommenden Jahr zu Leaks von Patientendaten in der Cloud kommen werde und Gesundheitsorganisationen sowie Impfstoff- und Arzneimittelhersteller zunehmend Cyber-Angriffen ausgesetzt sein

werden. Vor allem die Entwicklung eines Corona-Impfstoffs stehen im Fokus Cyberkrimineller für zielgerichtete Angriffe: So hatte schon dieses Jahr die Wellmess-Kampagne verschiedene Einrichtungen in Kanada, Großbritannien und den USA im Visier, die in die Forschung für einen Covid-19-Impfstoff involviert sind. www.kaspersky.de ■

VERHALTEN IM BRANDFALL

Nicht jeder weiß Bescheid!

Richtiges Verhalten im Brandfall: Zehn Fragen an den Experten

Deutschland gilt als vorbildlich, wenn es um Brandschutz geht. Kaum ein anderes Land hat so viele Feuerwehrleute pro Einwohner. Aber wie steht es um die Brandschutzaufklärung der Bevölkerung? Dazu befragten wir Frieder Kircher. Er ist Leitender Branddirektor i. R. der Berliner Feuerwehr sowie Vorsitzender des Gemeinsamen Ausschusses für Brandschutzerziehung und Brandschutzaufklärung des Deutschen Feuerwehrverbandes (DFV) und der Vereinigung zur Förderung des Deutschen Brandschutzes (vfdb).



Frieder Kircher, Leitender Branddirektor i. R. der Berliner Feuerwehr und Vorsitzender des Gemeinsamen Ausschusses für Brandschutzerziehung und Brandschutzaufklärung des Deutschen Feuerwehrverbandes (DFV) und der Vereinigung zur Förderung des Deutschen Brandschutzes (vfdb)

GIT SICHERHEIT: Herr Kircher, geben Sie uns zum Einstieg einmal einen Überblick, wie Brandschutzerziehung und -aufklärung in Deutschland geregelt sind?

Frieder Kircher: Die Verantwortung für Brandschutzerziehung und Brandschutzaufklärung ist in fast allen Feuerwegesetzen der Bundesrepublik als Zuständigkeit der Kommunen geregelt. Nur in Berlin und Bayern gibt es keine derartige Zuständigkeit. Durchgeführt wird die Brandschutzerziehung in den meisten Fällen von ehrenamtlichen Mitarbeitern der Freiwilligen Feuerwehr. Die Landesfeuerwehrverbände und die Landesfeuerwehrschulen bieten für die Brandschutzerzieher Seminare und Schulungen an. Der gemeinsame Ausschuss für Brandschutzerziehung und Brandschutzaufklärung von DFV und vfdb bietet als Fachgremium Arbeitshilfen und bemüht sich um die Koordinierung und Erfahrungsaustausch.

Sind solche Vorschriften wirklich notwendig? Wie sind Ihre Erfahrungen aus Ihrer langjährigen Arbeit?

Frieder Kircher: Die Kenntnis über das richtige Verhalten im Brandfall ist leider nicht so weit verbreitet, wie wir uns das als Fachleute gerne wünschen würden. Jeder glaubt zwar, wenn man aber detailliert nachfragt, kommen oft erhebliche Lücken zum Vorschein.

Brand in der eigenen Wohnung im Mehrfamilienhaus

Kurzempfehlung für das gebäudeorientierte brandschutzgerechte Verhalten

Die Fachempfehlung von DFV und vfdb unterscheidet insgesamt vier Fälle: Brand in einem Mehrfamilienhaus in der eigenen Wohnung und in der Nachbarwohnung, Brand im Einfamilienhaus und Brand oder verqualmtes Treppenhaus im Mehrfamilienhaus.

- Ruhe bewahren!
- Besteht die Möglichkeit, mit einfachen Mitteln das Feuer zu löschen? (Deckel auf den brennenden Topf, Anwendung eines vorhandenen Kleinlöschgerätes, Gefäß mit Wasser usw.?)
- Kann die Tür zum brennenden Raum geschlossen werden?
- Sind noch weitere Personen in der Wohnung? Wenn ja, wissen diese Personen von dem Brand und sind sie in der Lage, die Wohnung selbständig zu verlassen?
- Ist der Fluchtweg zum Wohnungsausgang frei?
- Liegen Mobiltelefon und Wohnungsschlüssel griffbereit?
- Kann ich / können wir die Wohnung über die Eingangstür verlassen? Welche anderen Fluchtwege stehen zur Verfügung?
- Habe ich beim Verlassen der Wohnung die Tür zum Treppenhaus zugezogen?
- Habe ich aus einem sicheren Bereich die Feuerwehr über die Telefonnummer 112 alarmiert?
- Habe ich die Nachbarn gewarnt?
- Ist vor dem Gebäude ausreichend Platz für die Feuerwehr oder kann ich Anwohner bitten, ihre Autos wegzufahren? Kann ich der Feuerwehr wichtige Informationen geben, zum Beispiel ob und wo noch Personen im Gebäude sind?

Mit anderen Worten: Es gibt Informationsbedarf auf breiter Ebene. Aber wie kann sichergestellt werden, dass diejenigen, die schon Kindern richtiges Verhalten vermitteln sollen, genügend vorbereitet sind und auch einheitliche Regeln vermitteln?

Frieder Kircher: Wir haben für diesen Fall als bundesweit tätiges Gremium eine neue Strategie zur Brandschutzaufklärung entwickelt. Ein Kernpunkt davon ist die Fachempfehlung zum Verhalten im Brandfall, die insbesondere natürlich für die Menschen, die in der Brandschutzerziehung und -aufklärung tätig sind, ein wichtiger Leitfaden ist, aber auch von jedem anderen selbst gelesen werden kann.

Lassen sich denn überhaupt feste Regeln formulieren? Immerhin ist ja jeder Brand anders.

Frieder Kircher: Das ist richtig, und bisher ist eines wenig beachtet worden: Es ist ein Unterschied, ob ein Brandfall in einer Wohnung in einem Mehrfamilienhaus auftritt oder im Obergeschoss eines Einfamilienhauses. Für diese unterschiedlichen Fälle haben wir abgeänderte Verhaltensregeln entworfen, die auf die jeweiligen Verhältnisse angepasst sind

Welche sind die Kernpunkte der Empfehlung?

Frieder Kircher: Einer der wichtigsten Punkte der Fachempfehlung ist der Ratschlag: Schließ' die Tür. Wenn ein Brand ausbricht, breitet sich insbesondere Rauch sehr schnell

auf alle Räume aus. Durch das Schließen der Tür, möglichst natürlich mit einem freien Weg zur Fluchttür, kann die weitere Rauchausbreitung erst einmal bis zum Abschluss der Flucht verzögert werden.

Was wird bei Ausbruch eines Feuers im privaten Bereich am häufigsten falsch gemacht?

Frieder Kircher: Das größte Übel ist, dass sich die Menschen keine Gedanken darüber gemacht haben, was sie im Brandfall tun, wo ihr nächster Fluchtweg ist und was sie unbedingt beachten müssen. Dann reagieren sie oft falsch, laufen zum Fenster und schreien um Hilfe und hinter ihnen breitet sich das Feuer weiter aus. Dann bleibt oft nur noch der Sprung aus dem Fenster, der leider in vielen Fällen tödlich endet.

Können Sie dafür ein Beispiel aus dem Einsatzgeschehen geben?

Frieder Kircher: Es gibt zahlreiche Beispiele aus dem Einsatzalltag der Feuerwehren. Mir ist eines aus meiner Berufstätigkeit bekannt. Eine Frau bemerkt einen Brand in ihrer Einzimmerwohnung im vierten Obergeschoss. Sie erinnert sich an die Bilder aus den Kinderbüchern, wo die Menschen am Fenster stehen und laut um Hilfe rufen und dann der Feuerwehrmann mit der Leiter zu Rettung kommt – das funktioniert leider nicht in einem Altbau auf dem Hinterhof – da reichen

**BRANDGEFÄHRLICH:
LAGERN UND LADEN
VON LITHIUM AKKUS**

Die Lösung: **ION-LINE
Sicherheitschränke!**



**Günstige
Mietkonditionen:**

**360^o
Miete**

Mehr Infos unter:
www.asecos.com



Frieder Kircher: „Jeder glaubt zwar, zu wissen, was er im Brandfall machen soll, wenn man aber detailliert nachfragt, kommen oft erhebliche Lücken zum Vorschein“

die Leitern nicht. Sie hätte schnellstens versuchen müssen, die Wohnung zu verlassen. In dem Fall konnte sie nur springen. Die Feuerwehr kam gerade an, als das Feuer schon ihre Kleidung entzündete.

Wie geht es weiter – was erhoffen Sie von dem Papier?

Frieder Kircher: Wir sehen einen langfristigen Prozess, um die Informationen über die vielen Aktiven in der Brandschutzerziehung

unter die Menschen zu bringen. Dazu gibt es auch Informationsseiten wie z. B. www.rauchmelder-lebensretter.de/120sek, wo wir den Inhalt auch schon grafisch aufbereitet haben. Darüber hinaus werden wir immer wieder Aktionen starten, um bei Tagen der offenen Tür der Feuerwehren, aber auch mit Verantwortungsträgern wie z. B. Wohnungsbau- oder Immobilienverwaltungen eine Sensibilität für dieses Thema zu schaffen.

Gibt es schon Beispiele, wie so etwas umgesetzt wird?

Frieder Kircher: Ein schönes Beispiel haben wir von der ersten Wohnungsbaugesellschaft Berlin-Marzahn, die unsere Fachempfehlung in eine ansprechende Broschüre umgesetzt hat, die an alle Mieter verteilt wird.

Mit der Fachempfehlung allein ist es sicher nicht getan. Es gibt noch verschiedene Projekte und Kampagnen, um das Brandschutz-Bewusstsein in der Bevölkerung zu stärken. Welches sind Ihrer Meinung nach die wichtigsten Aktionen?

Frieder Kircher: Die Aktion „Rauchmelder retten Leben“ auf der Website www.rauchmelder-lebensretter.de ist für uns und die Verbreitung von Rauchmeldern sehr wichtig. Auch Aktionen wie z. B. von Paulinchen e.V. auf der Website www.paulinchen.de helfen, für das Thema „Verhalten im Brandfall“ mehr Verständnis zu finden. ■

Fachempfehlung
von DFV und vfdb
zum Verhalten
im Brandfall
<https://bit.ly/39ZAF5m>



Kontakt

Vereinigung zur Förderung
des Deutschen Brandschutzes e.V. (vfdb)
Pinneberg
Tel.: +49 4101 46 203
duvneck@vfdb.de
www.vfdb.de
www.brandschutzaufklaerung.de

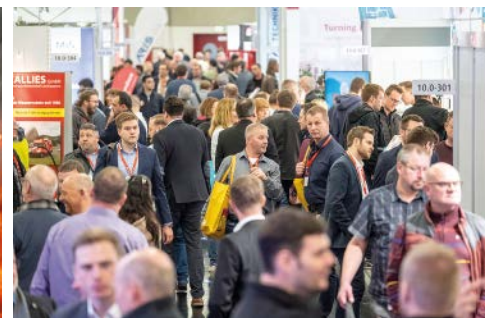
Feuertrutz: Zweigleisiges Konzept

Die Veranstalter Nürnberg Messe und Feuertrutz Network setzen für die Durchführung der Internationalen Fachmesse für vorbeugenden Brandschutz mit Kongress auf ein zweigleisiges Konzept. Am 23. und 24. Juni 2021 soll sich die Brandschutz-Community sowohl vor Ort in Nürnberg als auch online im Rahmen einer digitalen Plattform treffen. Mit diesem Konzept werde frühzeitig Planungssicherheit für alle Beteiligten geschaffen. In zahlreichen Gesprächen mit Kunden sei der Wunsch deutlich geworden, dass sich die Brandschutzbranche wieder persönlich treffen wolle. Das sei auch der größte Wunsch der Veranstalter. Trotzdem wisse zum aktuellen Zeitpunkt keiner, wie die Situation rund um Corona Ende Juni aussehen werde, so Stefan Dittrich, Leiter der Feuertrutz, Nürnberg Messe. Um den Kunden frühzeitig Planungssicherheit zu geben, habe man sich entschlossen, eine digitale Plattform parallel zur Messe vor Ort aufzubauen.



en. Dieses Vorgehen gewährleiste Ausstellern, Besuchern und Veranstaltern die notwendige Flexibilität im kommenden Jahr.

Auch der parallel stattfindende Brandschutzkongress, organisiert von Feuertrutz Network, wird ergänzend zum Kongress vor Ort online im Livestream übertragen. Es sollen zwei spannende Tage mit zahlreichen aktuellen Themen und neuen Lösungen rund um den vorbeugenden



Brandschutz aus erster Hand von erfahrenen Experten werden – vor Ort und digital, so André Gesellchen, Leitung Programm Brandschutz, Feuertrutz Network. Ein Kongressschwerpunkt sind 2021 „Lösungen für Sonderbauten“. Erfahrene Praktiker werden unter anderem moderne Problemlösungen und vermeidbare Fehler für verschiedene Sonderbautypen schildern.

www.feuertrutz-messe.de ■



Brandschutz

15./16. April 2021

Kongresszentrum Hotel Esperanto, Fulda



- | | | |
|------------------------------|---|---------------------------------|
| Brandmeldetechnik | ◆ | Sicherheitsbeleuchtung |
| Rauch- und Wärmeabzug | ◆ | Flucht- und Rettungswege |
| Sprachalarmierung | ◆ | Rauch-/Feuerschutztüren |

Wissen, Ideen + Networking für

- **Errichter, Planer- und Ingenieurbüros sowie Hersteller**
- **Sicherheitsbeauftragte von Anwendern und Betreiber von Leitstellen**
- **Behörden, Ministerien und Versicherer**

Anmeldung und Programm beim BHE (Telefon 0 63 86 / 92 14-34)

... oder unter www.bhe.de



©5second - stock.adobe.com

Puderzucker, brauner Zucker, Kandis, Zucker in Tütchen und Döschen: Süßes ist allgegenwärtig in den Fabriken des Zuckerherstellers Pfeifer & Langen. Das Unternehmen stellt seit 150 Jahren süße Produkte aus Rübe und Rohr für die Lebensmittelindustrie und den Endverbraucher her und vertreibt sie unter dem Namen Diamant Zucker. Mit mehreren Standorten in Europa gehört das in Köln gegründete Unternehmen zu den größten Zuckerherstellern. Für einen der Produktionsstandorte in Polen ist Mitte 2020 ein neu gebautes Hochregallager in Betrieb gegangen – mit passendem Brandschutz von Wagner Polen.

NAHRUNG UND GENUSSMITTEL

Süßes gut geschützt

Diamant Zucker: Brandschutzlösung mit Sauerstoffreduzierung

Am Produktionsstandort Sroda Wiełkopolska bei Poznan hat Pfeifer & Langen Polska S.A. ein neues Hochregallager errichtet. Hier werden Zuckerspezialitäten wie Zimtzucker oder Sirup gelagert. Bis zu 24.000 Palettenstellplätze sind in dem 35 Meter hohen und 140.000 Kubikmeter umfassenden Warenlager vorgesehen. Per Schleuse ist es direkt an die Zuckerfabrik angeschlossen. Ein- und Auslagerung der Ware sowie deren Kommissionierung erfolgen vollautomatisiert.

Doch nicht nur das neu gebaute Lager an sich – und die damit verbundenen Neuinvestitionen – brauchen speziellen Schutz. „Das Wichtigste ist in diesem Fall der Schutz des gelagerten Zuckers“, sagt Andrzej Biedulski, Projektleiter bei Pfeifer & Langen Polska. Damit entschied sich das Unternehmen von

vornherein gegen eine wasser- oder schaum-basierte Lösung.

Beim Einsatz solcher Systeme sind Schäden durch Löschmittel in der Regel nicht vermeidbar. Eine alternative Brandschutzlösung musste her. So stieß das Unternehmen auf die Wagner Group und ihre Expertise in der aktiven Brandvermeidung.

Zucker optimal schützen, Warenverfügbarkeit erhalten

Gemeinsam mit dem Team von Ireneusz Bruski, Geschäftsführer von Wagner Polen, haben Pfeifer & Langen Polska im Vorfeld ihre Schutzziele genau definiert. Neben dem Personenschutz sind es folgende Schutzziele, die es zu berücksichtigen galt: Im Ernstfall darf kein Stück Zucker in Rauch oder Ruß aufgehen oder durch Löschwasser zerstört werden.

Betriebsabläufe sowie der Warenfluss und weitere logistische Prozesse müssen auch im Ernstfall aufrechterhalten werden und die Ware muss ständig für Kunden verfügbar bleiben.

Das neu erbaute Hochregallager von Pfeifer & Langen Polska S.A. ist mittels einer Schleuse mit der Produktionshalle des Standortes verbunden. Die dort entstehenden Zuckerprodukte und Spezialitäten werden verpackt und auf Palette verladen, bevor sie in das Lager zum Weitertransport kommen. Diese Schritte sind den heutigen Standards angepasst vollkommen automatisiert. Dazu werden Regalbediengeräte und Fördertechnik eingesetzt. Diese bergen ebenso wie die Verpackung der Ware Brandrisiken, die es zu ermitteln gilt. Nur auf Grundlage dieser Risikoanalyse kann eine passende, auf den

Schutzbereich individuell angepasste Brandschutzlösung gefunden werden.

Im Hochregallager sind unterschiedlichste Brandrisiken zu berücksichtigen. Ein hoher Grad an Automatisierung in den Produktionshallen als auch im Lager selbst und damit auch ein hoher Anteil an elektrischen Komponenten stellt ein hohes Brandrisiko dar. Mit einer Lagerhöhe von rund 35 Meter und aufgrund enger Bauweise wird im Brandfall der Kamineffekt im Lager begünstigt. Ebenso wirkt sich eine hohe Packungsdichte der Waren sowie das Verpackungsmaterial Pappe und die Lagerung auf Paletten auf die Brandausbreitung aus. Einbezogen werden mussten zudem die komplexen Produktionsprozesse durch Anschluss an die Produktionshalle mittels einer Schleuse sowie die hohe



Ein Großteil der Brandschutztechnik wie Stickstoff-erzeuger und Schaltschränke wurden in einem Container neben dem Hochregallager untergebracht

Empfindlichkeit der Waren gegenüber Rauch und Feuchtigkeit. Werden diese Brandrisiken berücksichtigt, kann die passende Lösung erstellt werden. Dabei hat immer äußerste Priorität: Ein Feuer im Lager ist unter allen Umständen zu vermeiden.

Lösung im Container

Vier Oxyreduct V-Line-Anlagen bilden zusammen mit einer Brandfrüherkennung die Grundlage der Brandschutzlösung. Die V-Line-Anlagen produzieren aus der Umgebungsluft Stickstoff und leiten diesen in den zuvor definierten Schutzbereich ein. So wird dort die Sauerstoffkonzentration unter die spezifische Entzündungsgrenze der dort hauptsächlich gelagerten Materialien gesenkt. In dieser Schutzatmosphäre kann sich ein Feuer nicht weiter entwickeln, ebenso wenig weiter ausbreiten. Da es trotz der Sauerstoffreduzierung aber noch zu einem Schwelbrand kommen kann, gehört zu dieser Lösung auch ein System zur Brandfrüherkennung mit Ansaugrauchmeldern.

Die Titanus-Ansaugpunkte hängen über den Gassen des Hochregallagers und entnehmen dort der Umgebungsluft permanent Proben. Feinste Pyrolysepartikel werden so frühestmöglich erkannt. Damit sind die Geräte bis zu 2000 Mal sensibler als herkömmliche Punktmelder.

Das Besondere an der Lösung bei Pfeifer & Langen ist, dass ein Großteil der Brandschutztechnik wie Stickstoff-erzeuger und Schaltschränke nicht in einem separaten Betriebsraum, sondern in einem Container neben dem Hochregallager verbaut wurde. „Für die Wartung und den Service ist so ein externer Betriebsraum optimal, da er einfach zugänglich ist. Außerdem konnten Baukosten gespart werden, da kein separater Technikraum im Lager für die Brandschutzanlage geschaffen werden musste“, nennt Ireneusz Bruski, Geschäftsführer Wagner Polen, die Gründe für die Containerlösung.

Mitte des Jahres ging das Hochregallager in Betrieb. Seitdem werden die verschiedenen



Die gesamte Brandschutztechnik ist platzsparend in einem Container verbaut



Auf Paletten gepackt, werden die Zuckerprodukte im 35 m hohen, automatisierten Hochregallager zum Weiterversand verstaub

Zuckersorten sicher in die einzelnen Länder Europas vertrieben. ■

Kontakt

Wagner Group GmbH
Langenhagen
Tel: +49 511 97383 0
info@wagnergroup.com
www.wagnergroup.com

Neuer Termin für die Interschutz im Juni 2022

Die Interschutz wird neu terminiert und findet nun vom 20. bis 25.06.2022 auf dem Messegelände Hannover statt. Die Entscheidung für die Neuterminierung der Weltleitmesse für Feuerwehr, Rettungswesen, Bevölkerungsschutz und Sicherheit wurde nach gründlichen Überlegungen und intensiven Gesprächen mit dem Markt seitens der Deutschen Messe getroffen. Wie bei zahlreichen anderen Messen und Veranstaltungen liegen die Gründe für diese Entscheidung auch bei der Interschutz in den aktuellen Entwicklungen des weltweiten Infektionsgeschehens im Zuge der Covid-19-Pandemie. Gerade Weltleitmessens wie die Interschutz hätten einen langfristigen Planungshorizont und benötigten eine Vorlaufzeit von mehreren Monaten. Zudem seien die Branchen, die an der Messe als Aussteller oder Besucher teilnehmen, maximal in das aktuelle Infektionsgeschehen auf der ganzen Welt involviert, so Andreas Gruchow, Mitglied des Vorstands der Deutschen Messe.

Die Interschutz findet in einem Messeturnus von fünf Jahren statt. Die Community, bestehend aus Feuerwehr- und Rettungswesen sowie dem Bevölkerungsschutz, fiebere der nächsten Ausgabe mehr als entgegen. Gerade vor diesem Hintergrund sei der Deutschen Messe die Entscheidung für die Neuterminierung sehr schwergefallen, so Andreas Gruchow. Intensive

Gespräche mit Partnern, Ausstellern und Vertretern wesentlicher Besucherzielgruppen hätten jedoch bestätigt, dass dieser Schritt unumgänglich ist. Eine Durchführung im Sommer 2022 werde von allen Seiten begrüßt. Denn nur so könne allen Beteiligten die notwendige Planungssicherheit für ihre Messevorbereitungen geboten werden. Zudem lebe eine Weltleitmesse auch von zahlreichen internationalen Besuchern sowie im Besonderen der persönlichen Begegnung. Mit Blick auf weltweite Reisebe- und -einschränkungen lasse sich eine Messe mit dieser globalen Strahlkraft aktuell nicht seriös auf Kundenseite vorbereiten.

Bereits für die ursprünglich im Juni 2020 geplante Ausgabe konnte eine Rekordbeteiligung verzeichnet werden. Man sei zuversichtlich, dass die Aussteller gemeinsam mit der Deutschen Messe die Interschutz 2022 gestalten werden, dann erstmalig als hybride Veranstaltung. Die Pandemie habe uns allen vor Augen geführt, wie wichtig die Bereiche Feuerwehr, Rettungswesen und Bevölkerungsschutz sind. Zudem erwarte man überall auf der Welt deutliche Investitionssteigerungen in diesen Branchen, so Martin Folkerts, Global Director Interschutz bei der Deutschen Messe.

www.interschutz.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 Klases, 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.-Betw. 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

Elke Palzer

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: DE5501108006161517443

Zurzeit gilt Anzeigenpreisliste vom 1.10.2020. Die namentlich gekennzeichneten Beiträge stehen in der Verantwortung des Autors.

2021 erscheinen 10 Ausgaben

„GIT SICHERHEIT“

Druckauflage: 30.000

inkl. GIT Sonderausgabe PRO-4-PRO



Abonnement 2021: 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

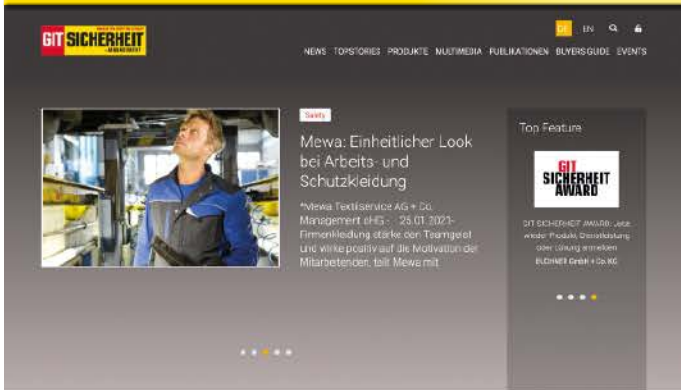
Die namentlich gekennzeichneten Beiträge stehen in der Verantwortung des Autors. Nachdruck, auch auszugsweise, nur mit Genehmigung der Redaktion und mit Quellenangabe gestattet. Für unaufgefordert eingesandte Manuskripte und Abbildungen übernimmt der Verlag keine Haftung.

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



News

Zutrittskontrolle bis in die Unendlichkeit gedacht!
30.01.2021 - Alle der Infobit-Leser: Ihre Infobit Reader von Infobit electronic ist die modernste Technik für maximaler Flexibilität und Sicherheit für Unternehmen verfügbar.

Kritische Infrastrukturen KRITIS: Kriterien für ganzheitliche Sicherheit
26.01.2021 - Betreiber Kritischer Infrastrukturen (KRITIS) sollten ein ganzheitliches Sicherheitskonzept verfolgen, das neben IT-Maßnahmen und dem Datenschutz auch die...

BVSW-Veranstaltungen erhalten ISO-9001-Zertifizierung
25.01.2021 - Die Betriebswirtschaftliche Sicherheit in der Wirtschaft (BVSW) hat eine weitere ISO-9001-Zertifizierung erhalten.

GIT SICHERHEIT AWARD: Jetzt wieder Produkt, Dienstleistung oder Lösung anmelden
22.01.2021 - Wenn Sie Arbeiten in diesem Bereich sind, dann stellen Sie Ihre Lösung jetzt an. Oder erheben Sie als Nutzer ein Produkt - Anmeldefrist: 31. März 2021

WEBSIMINAR
Ransomware in KRITIS-Infrastrukturen: Seien Sie vorbereitet!
31. Feb. 2021
WEBSIMINAR

Topstories

Pfaffenberg: Und das Kranlicht leuchtet ihm ...
11.01.2021 - Zahlreiche Arbeitstationen, viele Menschen, viele Maschinen – stauwachen schweren Lasten, die perpendikular und schräg transportiert werden müssen.

B&R: Wie eine schützende Hülle - Safety Tür mobile Maschinen
11.01.2021 - Die Ausmahlung mobiler Arbeitsmaschinen bedingt, dass sich deren Hersteller weiterhin mit der europäischer Maschinenrichtlinie und dem Thema Sicherheitsdruck...

Sick: In perfekter Harmonie
11.01.2021 - In zahlreichen Einsatzgebieten sind die unterschiedlichsten Arbeitsschritte werden Menschen vor Risiken unterstut.

WEBSIMINAR
Ransomware in KRITIS-Infrastrukturen: Seien Sie vorbereitet!
31. Feb. 2021
WEBSIMINAR

Publikationen

Baro-Switche schützen Sicherheitsnetzwerke und Geräte von Dritten vor Ransomware Cyberangriffen
21.01.2021 - Ransomware stellt eine Reihe von 19 Schwachstellen in einer Local- und TFTP-Softwarebibliothek. Dies stellt eine unmittelbare Bedrohung für viele Produkte dar. Die...

WEBSIMINAR
Ransomware in KRITIS-Infrastrukturen: Seien Sie vorbereitet!
31. Feb. 2021
WEBSIMINAR

Multimedia

WIN-DAYS im Video: Lisa Holland zeigt die virtuelle Wiley Industry Days
04.01.2021 - Willkommen bei den WIN-DAYS im Video! Lisa Holland zeigt die virtuelle Wiley Industry Days. Wie geht es auf der virtuellen Bühne? Die Antworten finden Sie in den Aufzeichnungen...

WIN-DAYS Konferenz 2020 On Demand
21.11.2020 - JEZT AKTIVIEREN Sie Ihre On-Demand-Konferenz! Die Konferenzunterlagen sind online verfügbar. Sie werden bei der nächsten Konferenz zur Verfügung gestellt werden.

Drei Gründe für die Umstellung auf ein reibendes Zutrittskontrollsystem
26.01.2020 - Ein reibendes Zutrittskontrollsystem ist ein entscheidender Schritt für die Sicherheit der Ihre Unternehmensdaten. Die effiziente Verwaltung von Geschäften und...

WEBSIMINAR
Ransomware in KRITIS-Infrastrukturen: Seien Sie vorbereitet!
31. Feb. 2021
WEBSIMINAR

ALLE NEWS

ALLE TOPSTORIES

ALLE PUBLIKATIONEN

ALLE MEDIEN

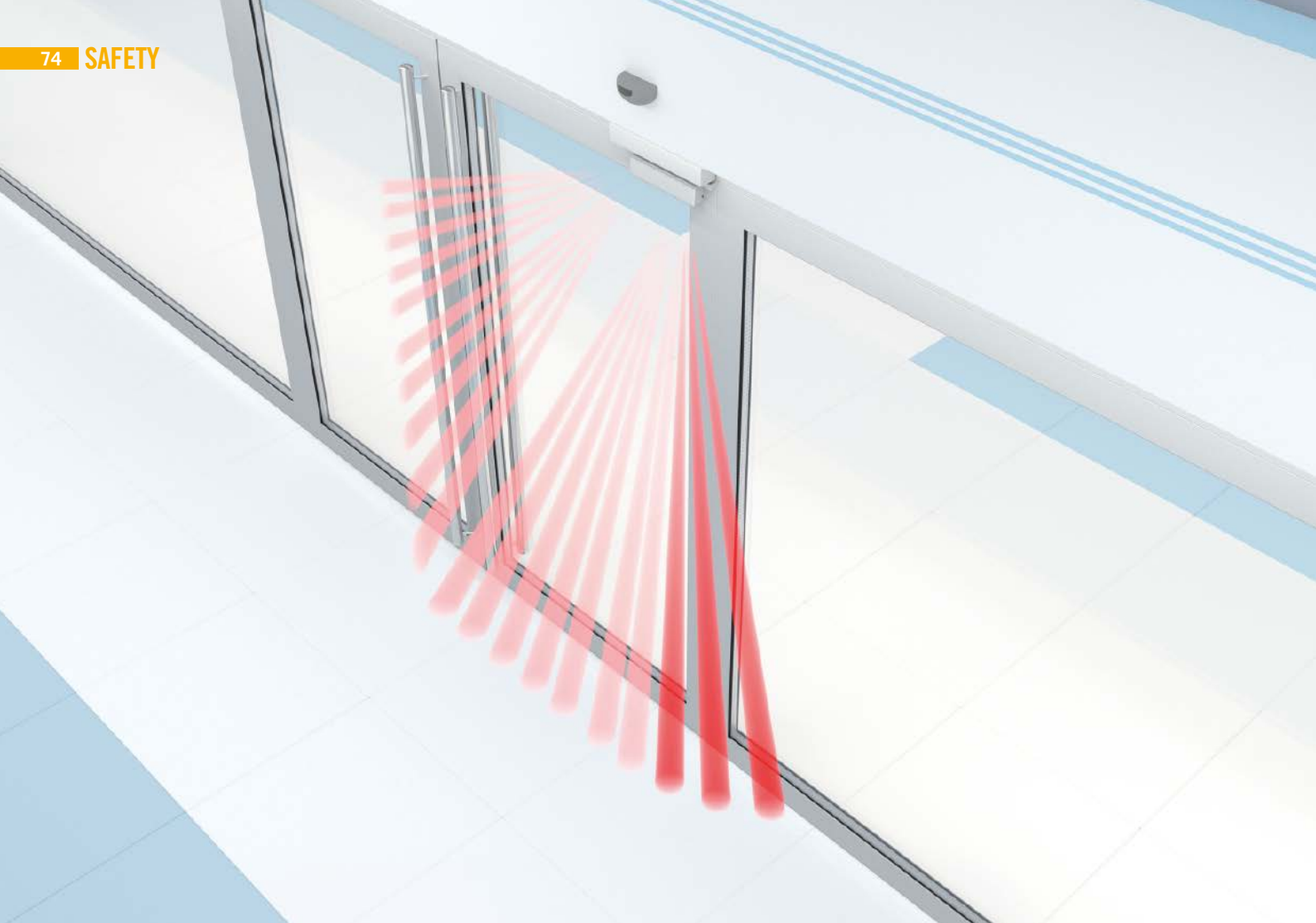


GIT

SAFETY

INNENTITEL

Diesen Monat
Schwerpunkt:
Solid-State-Scanner
ab Seite 74



▲ Zur Absicherung der Nebenschließkante sind die Strahlen derart angeordnet, dass die Gefahrenzone durch ein gekrümmtes Schutzfeld quasi umbettet wird

SENSOREN

Lautlos nach dem Lauf des Lichts

Solid-State-Scanner zum Überwachen automatischer Drehflügel- und Karusselltüren

Mit dem ShieldScan hat Pepperl+Fuchs einen robusten Sicherheitssensor entwickelt, der mit der Erfassung der Lichtlaufzeit von Objekten arbeitet (Time-of-Flight-Technologie, ToF). Das geräuschlos arbeitende System dient in erster Linie zur Absicherung automatischer Drehflügel- und Karusselltüren, eignet sich aber auch für alle Anwendungen, die eine „Berührungslos Wirkende Schutzeinrichtung“ gemäß Sicherheitsintegritätslevel SIL 2 sowie Performance Level PL d Kategorie 2 benötigen.

Der Türsensor ist in einem kompakten, formschönen Gehäuse untergebracht, das sich unauffällig in der Türecke unterbringen lässt ▼



Von automatischen Drehflügeltüren und Karusselltüren geht ein typisches Gefährdungspotenzial aus, von dem grundsätzlich jeder Passant betroffen ist. Zur Absicherung dienen entsprechende Türsensoren, die zusammen mit dem Türantrieb eine „Berührungslos Wirkende Schutzeinrichtung“ bilden. Der Sicherheits-Türsensor ShieldScan von Sensorik- und Sicherheitsspezialist Pepperl+Fuchs arbeitet mit der fortschrittlichen Lichtlaufzeitmessung und kommt ohne rotierendes Innenleben aus (Solid-State-Scanner). Selbst unter schwierigen Licht- und Beleuchtungssituationen, Bodenbeschaffenheiten oder spiegelnden Oberflächen zeichnet sich das System durch eine außergewöhnliche Zuverlässigkeit aus.

Auch automatische Türsysteme sind letztendlich Maschinen, die – ebenso wie Industrieanlagen – über bewegliche Teile, Antriebe und Steuerungen verfügen. Sicherheitstechnisch unterliegen Automatiktüren der Maschinenrichtlinie und es besteht in gewisser Hinsicht sogar eine erhöhte Gefährdungssituation. Denn während in Fabriken nur begrenzte Personenkreise mit den Maschinen in Kontakt kommen, z. B. geschultes oder angelerntes Personal, gibt es bei vielen Automatiktüren keinerlei Beschränkung. Zu öffentlichen Drehflügel- und Karusselltüren haben prinzipiell alle denkbaren Personen Zugang, einschließlich Kinder sowie alte und behinderte Menschen.

Automatiktüren erfordern Sicherheitstechnik

Welche sicherheitstechnischen Anforderungen zum Personenschutz sich im Detail an automatische Türsysteme stellen, ist in EN 16005 bzw. DIN 18650 beschrieben. Die Risikoanalyse an einer automatischen Drehflügel- oder Karusselltür wird stets zu dem Ergebnis kommen, dass man sich dort verletzen und zu Schaden kommen kann. Folglich ist sie mit zertifizierten Sicherheitssensoren abzusichern.

Beim neuen ShieldScan handelt es sich um einen Sicherheits-Türsensor zum Errichten von „Berührungslos Wirkenden Schutzeinrichtungen“ (BWS) gemäß Sicherheitsintegritätslevel SIL 2 sowie Performance Level PL d, Kategorie 2. Das System arbeitet mit der neuesten ToF-Technologie (Time-of-Flight), die die Zielobjekte über die Lichtlaufzeit erfasst. Das Verfahren ist ausgesprochen robust bei Anwendungen in schwierigen Umgebungsbedingungen und zeichnet sich durch eine sehr hohe Kontrast- und Fremdlichtunabhängigkeit aus. So meistert der ShieldScan auch problemlos Erkennungsaufgaben, bei denen andere Systeme an ihre Grenzen stoßen, etwa bei spiegelnden Böden und Wänden oder ungünstigen Beleuchtungssituationen.

Nur noch ein Sensor für große und kleine Türen

Der Türsensor spannt ein Schutzfeld aus 20 Einzelstrahlen auf und benötigt kein rotierendes Spiegelsystem zur Strahlervielfältigung. Anders als bei einem rotierenden System, bei dem alle Strahlen stets in derselben Ebene liegen, lassen sich die Einzelstrahlen des Solid-State-Sensors beliebig ausrichten und optimal an die Applikation anpassen. Zur Absicherung der Nebenschließkante hat Pepperl+Fuchs die Strahlen derart angeordnet, dass die Gefahrenzone durch ein gekrümmtes Schutzfeld quasi umbettet und ein bestmöglicher Umgreif- oder Hintergreifschutz realisiert wird.

Insgesamt sichern zehn Strahlen die Hauptschließkante, sieben die Schließkante unten am Türblatt sowie drei die Nebenschließkante an der Türaufhängung. Da sich alle Strahlen in einem kleinen Winkel von der Tür entfernen, schauen sie unter anderem problemlos am Handlauf der Hauptschließkante vorbei. So lässt sich mit einem einzigen System eine komplette Drehflügeltürseite mit bis zu 1800 mm Breite und 3500 mm Höhe überwachen.



Statische Time-of-Flight-Technologie bietet höchste Präzision und Zuverlässigkeit.“

Virtuelle Wand sorgt für stabilen Betrieb

Montage und Inbetriebnahme gestalten sich zügig und unkompliziert. Ein Novum stellt die sogenannte Virtuelle Wand dar. Der Sensor verfügt über eine dynamische, winkelabhängige Anpassung seines Schutzfelds. Damit ist ein explizites Einlernen einer Wand hinter der geöffneten Tür nicht notwendig. Beim Öffnen der Tür blendet das System die einzelnen Strahlen des Schutzfelds nacheinander aus, bis der maximale Türöffnungswinkel erreicht

ist. Durch einen integrierten Gyrosensors kennt die Tür zu jedem Zeitpunkt ihre aktuelle Position.

Eine einmalige Lernfahrt reicht aus, um den maximalen Öffnungswinkel zu definieren. Anschließend ignoriert der Sensor jegliche Veränderungen hinter der geöffneten Tür und der Virtuellen Wand. So ist ein stabiler Betrieb gewährleistet, der sich etwa durch das Verschieben von Blumenkübeln oder anderen Objekten nicht beeinträchtigen lässt. Auch beim Verstellen des Neigungswinkels über das dafür vorgesehene Stellrädchen ist kein neuer Einlernvorgang notwendig. Der Sensor erfasst diese Änderung und berechnet automatisch die erforderlichen Parameter neu.

Vollkommen geräuschloser Betrieb

Der Verzicht auf einen rotierenden Antrieb mit empfindlichen beweglichen Teilen macht das System nicht nur robust gegenüber mechanischen Einflüssen wie Schlag- und Stoßbelastungen, sondern erlaubt auch einen vollkommen geräuschlosen Betrieb. Dem Einsatz in OP-Sälen, Ruheräumen, Bibliotheken, Konzert-Sälen usw. steht nichts entgegen. Mit der Schutzart IP65 ist der Türsensor auch ideal gegen Feuchtigkeit und Regen geschützt, so dass er sich auch im Außenbereich einsetzen lässt. Der Türsensor ist in einem kompakten, formschönen Gehäuse untergebracht, das sich unauffällig in der Türecke unterbringen lässt. Der Deckel ist in verschiedenen Farben erhältlich und kann bei Bedarf umgespritzt werden.

Der ShieldScan erfüllt alle einschlägigen Sicherheitskriterien und -Normen. Wie bei Sicherheitsprodukten üblich, wird er mit der entsprechenden Baumusterprüfung ausgeliefert. In der Typprüfung beweist das System, dass es den in der EN 16005 definierten Prüfkörper CA zuverlässig erkennt und allen weiteren Anforderungen, wie EMV-, Temperaturfestigkeit usw., gerecht wird. ■

Kontakt

Pepperl+Fuchs, Mannheim
Tel.: +49 621 776-1111
fa-info@de.pepperl-fuchs.com
www.pepperl-fuchs.com

**Wir bringen Ihre Medien sicher auf Temperatur!
Informieren Sie sich jetzt über die Funktionsweise
unserer Wärmekammern!**



<https://www.bauer-suedlohn.de/waermekammer>



MASCHINEN- UND ANLAGENSICHERHEIT

„Hot and Spicy“

Kleinsteuerung PNOZmulti 2 sorgt für optimierte Sicherheit und Effizienz

Bereits 2017 hatte sich der zur Paulig Group gehörende Snack Food-Hersteller Poco Loco entschlossen, seine Produktionslinien und Prozesse auf den Prüfstand zu stellen. Optimierung als Ziel. Im Mittelpunkt des Konzepts: Die Effizienz, aber auch die Sicherheit der Linien. Seit dem Retrofit sorgt beim belgischen Hersteller hochwertiger Tex Mex-Produkte die konfigurierbare Kleinsteuerung PNOZmulti 2 als zentrale Sicherheitsinstanz für eine gleichbleibend gute und auch sichere Produktion der leckeren Knabberprodukte.



© vitals - stock.adobe.com

Das Portfolio von Poco Loco aus Roelare liest sich wie die Speisekarte beim Mexikaner. Das Unternehmen bietet seinen weltweiten Kunden vom Chip bis zum Dip praktisch alles: Unterschiedliche Arten von Tortilla-Wraps, dazu Tortilla-Chips in verschiedensten Geschmacksvariationen, ganze Mahlzeit-Kits sowie Gewürzmischungen und Salsas. Auch in vielen Eigenmarken „steckt“ Poco Loco. Z. B. in Tortilla-Chips für Kunden in ganz Europa. Mit seinem Sortiment gehört der Snack-Food-Hersteller hier zu den Marktführern im Bereich Tex Mex-Produkte.

Backe, backe – Tortilla

Der Herstellungsprozess für Tortilla Chips ist dann auch fast so umfassend wie das Portfolio: Am Anfang steht die Bereitstellung und Dosierung der wichtigsten Zutaten wie Wasser und Maismehl, die anschließend zu einem Teig vermischt werden. Die Maisteig-Mischung gelangt danach in eine Strangpresse, die für eine gute Textur sorgt. Weiter geht es mit der Bearbeitung in einer Ausrollmaschine, die anders als das heimische Nudelholz gleich aus zwei riesigen Walzen besteht, die sich mit geringem Abstand zueinander drehen und

so den Teig passgenau auf die gewünschte Dicke ausrollen. Gleichzeitig werden bei diesem Schritt des Fertigungsprozesses die Chips auch ausgeschnitten.

Hierauf folgt ein Trocknungsprozess und das Bad im heißen Öl einer Fritteuse, durch das die Chips ihre goldgelbe Farbe. Nach einer Qualitäts-Zwischenkontrolle werden die jeweils vom Kunden gewünschten Gewürze zugegeben. Und erst danach geht's für die Tortilla Chips ab in die Tüte.

Also ein umfassender Produktionsablauf mit präzise definierten Prozessschritten, die

◀ Die konfigurierbare sichere Kleinsteuerung PNOZmulti 2 von Pilz wacht heute als zentrale Sicherheitsinstanz über die Tortilla-Chips-Produktionslinie

die verkettete Anlage aufeinander abgestimmt und präzise abarbeiten muss. „Genau dies, also dass die Anlage dezentral gesteuert wurde, hat in der Vergangenheit zu Schwierigkeiten geführt,“ berichtet SPS-Programmierer Jeroom Verstraete von Poco Loco. „Weil die verkettete Produktionslinie von verschiedenen Maschinenbauern installiert wurde und auch die Steuerung der Anlage eine Kombination verschiedener SPSen und Not-Halt-Relais war.“

Besser im Zusammenhang steuern

Die Maschinen als separate Einheiten gedacht – ein nicht nur auf Steuerungsebene umständliches Handling. „Lästige Nebeneffekte“, wie Poco Loco diese nannte, waren die Folge. So hatte beispielsweise jede Teilanlage einen eigenen Notabschaltstromkreis, was dazu führte, dass die Not-Halte teilweise getrennt voneinander Sicherheitszonen abschalteten.

Eine typische Schwierigkeit beim Verketteten mehrerer Maschinen, weiß Francky Maveau, Leiter der Abteilung Elektro bei Poco Loco. Auch einen weiteren großen Nachteil beschreibt er: „In der technischen Abteilung wurden im Fall einer Fehlersuche alle Hände gebraucht. Wenn bei einer Sicherheitssteuerung alle Not-Halte in Reihe geschaltet sind, ist es bei Ausfällen oft schwierig, das Problem



▲ Die Kleinsteuerung PNOZmulti 2 steuert alle Sicherheitsfunktionen

genau zu lokalisieren. Oft mussten wir eine Menge Anschlusskästen und Notstecker öffnen und buchstäblich jedes einzelne Kabel überprüfen. Dies führte häufig zu langen Stillstandszeiten.“

Damit war für den Snackhersteller klar: Nicht nur eine sicherere Produktionslinie, sondern auch ein effizienterer Betrieb sollte das Ziel sein. Jeroom Verstraete erläutert, welche Aspekte ganz oben auf der „Wunschliste“

standen: „Wir wollten die dezentrale Steuerung durch eine zentrale SPS mit dezentraler E/A für die einzelnen Maschinen umwandeln. Die Not-Halte sollten in ein übergeordnetes System integriert werden. Auch eine Visualisierung der Anlage, um einen

sofortigen klaren Überblick über die Produktionslinie zu erhalten, sollte umgesetzt werden.“

Produktion stets sicher im Blick

Die Visualisierung der gesamten Anlage ist heute so geregelt, dass Probleme frühzeitig erkannt werden und keine größeren Auswirkungen auf den Gesamtprozess haben können. Wenn ein Problem auftritt, wird den Technikern auf ihrem Bediengerät sofort angezeigt, an welcher Stelle der verketteten Anlage welche Sicherheitsfunktion – welcher Not-Halt oder welche Tür – betroffen ist. Dies beschleunigt die Fehlersuche enorm.

Technisch löst dies die Kleinsteuerung, indem über die Software jede Sicherheitskomponente eine eindeutige DIAG-Adresse (Dynamic Information and Action Gateway-Adresse) zugewiesen bekommt. So lassen sich Informationen mittels virtueller Bits über ein Feldbussystem an die übergeordnete Steuerung übermitteln, damit sie von dieser für die Diagnose aufbereitet werden.

Zusätzlich lassen sich über das Display der Kleinsteuerung die Statusmeldungen anzeigen. Bis zu 20 verschiedene Meldungen kann diese unabhängig von der übergeordneten Anlagen-Steuerung direkt übermitteln. Die Techniker sind somit in der Lage, die

▼ Durch die Lösung von Pilz wurde der Zeitaufwand sowohl für das Engineering als auch für die Fehlersuche stark reduziert





▲ Das Softwaretool PNOZmulti Configurator sorgt für schnelles und einfaches Engineering

Diagnose sofort durchzuführen, ohne zwingend einen Laptop für eine weitergehende Diagnose anzuschließen.

Und es gibt noch einen weiteren Pluspunkt für die Sicherheit: Nach Fertigstellung und Validierung wird das Sicherheitsprogramm mit einer CRC-Summe versehen und diese dokumentiert. Jede zwischenzeitlich erfolgte Änderung lässt sich somit schnell erkennen. Das erhöht die Sicherheit vor Manipulationen und im Haftungsfall ist die Möglichkeit zur Nachverfolgung gegeben.

Besser bewegt, besser produziert

Auch das Bewegungsmanagement für die Anlage wurde durch den Einsatz der Kleinsteuerung mit Blick auf die Sicherheit und Diagnose optimiert: Dazu erfolgte die Umstellung der Produktionslinie auf Antriebe mit Frequenzumrichter, die mit der STO-Funktion (Safe Torque Off = sicher abgeschaltetes Moment) ausgestattet sind.

Zuvor erfolgte die Abschaltung eines Sicherheitsbereichs in der Regel dadurch, dass der Stromfluss zum Antrieb mithilfe von Leistungsschützen blockiert wurde. Eine nachträgliche Fehler-Diagnose war somit nicht möglich. Mit der Kopplung über PNOZmulti 2 jedoch wird dafür Sorge getragen, dass bei Aulösung eines Not-Halts, der Antrieb über die STO-Funktion kontrolliert stoppt.

In Zonen denken

An der verketteten Produktionsanlage für Tortilla Chips sind neben fünfzehn Not-Halte zusätzlich zahlreiche Sicherheitsschalter verbaut. Die Produktionslinie selbst ist in Zonen

unterteilt, damit ein Abschalten in einer Zone keine Auswirkungen auf eine andere Zone haben kann. Heute lassen sich nicht nur die Not-Halte einfach – und bei Bedarf – immer wieder anhand einer Sicherheitsmatrix über das zur Kleinsteuerung PNOZmulti 2 gehörige Softwaretool PNOZmulti Configurator neu konfigurieren. Vielmehr kann beispielsweise die Fritteuse weiterarbeiten, auch wenn eine Störung am Anfang der Produktionslinie auftritt. Ursprünglich hatte man bei Poco Loco nur drei getrennte Zonen präferiert. Die Praxis hat jedoch gezeigt, dass eine Umstellung auf insgesamt neun Zonen Vorteile bereithält.

Funktionen intuitiv und flexibel handhaben

Mit dem Konfigurationstool PNOZmulti Configurator können bei Poco Loco nicht nur die für die Programmierung der SPS zuständigen Techniker, sondern auch andere technische Mitarbeiter ein PNOZmulti-Programm erstellen und bei entsprechender Berechtigung auch modifizieren. Gleichzeitig kann dieses Tool bei der Fehlersuche von den Technikern für die einfache Diagnose einer Störung genutzt werden.

Maarten Dedeurwaerder, Projektingenieur bei Poco Loco, betont im Zusammenhang mit dieser Software-Ausstattung auch das rundum einfache Handling: „Dass wir uns für PNOZmulti 2 als eigenständige Steuerung für die Sicherheit entschieden haben, die wir zusätzlich zu der übergeordneten Maschinensteuerung einsetzen, hat seine Gründe auch im einfach zu bedienenden Konfigurationstool.“

Unterschiedliche Benutzerebenen in der Software des Tools verhindern zudem, dass das Sicherheitsprogramm während einer Wartungsmaßnahme manipuliert werden kann. „Um das Tool korrekt zur Fehlerbehebung einsetzen zu können, wurde unsere gesamte technische Abteilung einen halben Tag lang in die Einrichtung und Bedienung des PNOZmulti Systems eingewiesen,“ ergänzt Dedeurwaerder. Die so geschulten Techniker wurden auf diese Art in die Lage versetzt, die dynamische Programmanzeige, in der das gesamte Sicherheitsprogramm verfolgbar ist, problemlos zu starten. Dabei führt eine „grüne Linie“ direkt durch die Analyse. Eine sehr benutzerfreundliche Art der Anwendung, „weil sie stark visuell ausgerichtet ist und eine intuitive Arbeitsweise ermöglicht“, wie auch der Projektingenieur von Poco Loco bestätigt.

Wie erkenntlich wird, führte die Modernisierung der Anlage somit nicht nur zu einer nachhaltigen Optimierung der Sicherheit, sondern zu einer Optimierung des gesamten Produktionsablaufs. Denn die zentrale Steuerungsinstanz sorgt dafür, dass ein Fehler nicht zu einem umfassenden Stillstand und damit zu weniger Produktionseffizienz führen kann. ■

Autor

Kwinten Cantraine

Business Development Manager

Pilz Belgien

Kontakt

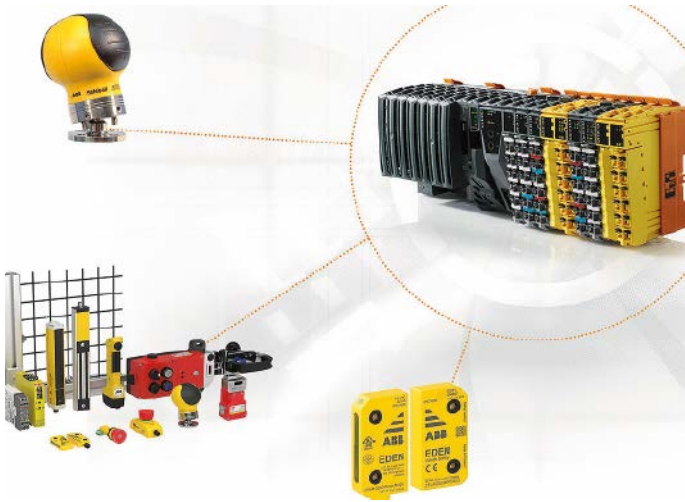
Pilz GmbH & co. KG

Ostfildern

Tel.: +49 711 3409 0

info@pilz.de

www.pilz.de



Breites Portfolio vereinfacht Aufbau von Sicherheitssystemen ▲

Die Sicherheitssensoren von ABB Jokab können nun direkt mit der integrierten Sicherheitstechnik von B&R verwendet werden. Das Portfolio von ABB Jokab umfasst ein vollständiges Set an Türzuhaltungen, Lichtgittern und Schutzmaten. Durch die breite Auswahl lassen sich Sicherheitskonzepte in Zukunft einfacher umsetzen. Safety-Produkte von ABB Jokab werden einfach mit den sicheren B&R-I/Os verdrahtet. Beide Hersteller erfüllen mit ihren Produkten die Anforderungen der Norm ISO 13849-1 bis

zur höchsten Sicherheitsstufe PL/Kat. 4. Die sicheren Sensoren von ABB Jokab unterstützen die Verkabelung einer Sicherheitsfunktion mit mehreren unterschiedlichen Sensoren, die in Reihe geschaltet sind. So kann beispielsweise eine Reihenschaltung mehrerer Sicherheitstüren umgesetzt werden. Diese Möglichkeit reduziert Kabel und damit auch die Anzahl der notwendigen sicheren Eingangskanäle. Trotz der Reihenschaltung bleibt die maximale Sicherheit gegeben.

www.br-automation.com ■



Überspannungsschutz für die Windenergie ▲

Die kombinierten Blitzstrom- und Überspannungs-Ableiter der Geräteserie Blitzductorconnect von Dehn schützen MSR-Technik einer Windenergieanlage sowie deren informationstechnische Schnittstellen und Bussysteme. Es gibt die Schutzgeräte der Geräte-Familie kompakt oder modular aufgebaut und dabei haben beide Varianten nur eine Baubreite von 6 mm. Funktionen wie die secR-Entriegelungstasten und die Push-in-Technik helfen, den Installationsaufwand zu minimieren.

Statusanzeige und passende FM-Einheit melden Ausfälle bei Überlast sofort. Pitchsysteme, zur Steuerung der Rotorblätter von Windenergieanlagen beispielsweise, müssen auch als Sicherheitssysteme jederzeit funktionsfähig bleiben. Denn mit ihnen wird nicht nur die Rotordrehzahl dem Windangebot angepasst. Sie sind auch Teil des Bremsystems (aerodynamische Bremse) und dienen daher als Notfallbremse.

www.dehn.de ■

Kompakter Not-Aus-Schalter

APEM hat einen kompakten Not-Aus-Schalter mit 22 mm Frontplattenausschnitt auf den Markt gebracht, der durch einen zusätzlichen Sicherungsring beide Teile zusammenhält und so ein „Schwimmen“ der Halterung vermeidet. Zwei Pole und ein Sicherungsring: Diese Kombination habe es bei Not-Aus-Schaltern für Leiterplatten bisher noch nicht gegeben, so das Unternehmen. Die Serie EC für Leiterplatten bietet daher eine außergewöhnliche Bedien- und



Montagesicherheit. Sie ist zudem kabellos und damit zeitsparend zu installieren und dank ihrer extrem kompakten Abmessungen insbesondere gut geeignet für mobile Anwendungen wie Automatisierte Transportfahrzeuge (AGV), Bellybox-Steuerungen oder Fernbedienungen. Als zusätzlicher Sicherheitsfaktor zeigt ein grüner optischer Indikator deutlich erkennbar den Schalterstatus an. Der Durchmesser des Betätigers beträgt 30 mm.

www.apem.de ■

Cyberdiode unterstützt Industrie-4.0-Protokoll

Genua hat seine Datendiode „Cyberdiode“ für das Industrie 4.0-Protokoll OPC UA erweitert. Das Securityprodukt ermöglicht damit den hochsicheren Datenexport beim Industrial Monitoring von Maschinen und Anlagen. OT- und IT-Infrastrukturen schützt die Cyberdiode vor Cyberangriffen, Manipulation und Produktionsausfällen. Die IT-Security-Lösung lässt ausschließlich One-Way-Datentransfers zu – in Gegenrichtung blockt sie jeden Informationsfluss ab. Ein Transport von Schadcode oder andere Cyberrisiken sind damit ausgeschlossen. Dies ermöglicht eine rückwirkungsfreie Ausleitung von Maschinen- und Anlagendaten in unsichere Netze, etwa



in die Cloud zur Datenanalyse. Die besondere Hardware-Separierung auf Mikrokernel-Ebene basiert auf BSI-zertifizierten Produkten. Das gewährleistet den Integritätsschutz hochsicherer industrieller Netzwerke.

www.genua.de ■

Phasenwächter schützt vor Beschädigung

Mit dem multifunktionalen Phasenwächter BD 9080/003 der Varimeter-Pro-Serie bietet Dold mehrere Überwachungsmöglichkeiten, um Maschinenausfälle, Stillstandszeiten und Reparaturen zu vermeiden. Ohne separate Hilfsspannung überwacht der Phasenwächter beim dreiphasigen Netz die Unter-/Überspannung bis max. 3 AC 1000 V, die Spannungssymmetrie der Phasen, den Phasenausfall und die Phasenfolge. Die Ansprechverzögerung kann von 0,1 bis 30 Sekunden eingestellt werden. Die Anlaufüberbrückungszeit ist auf 30 Sekunden fest eingestellt und wirkt einmalig nach Anlegen der Betriebsspannung. Durch eine be-



dienerefreundliche Gerätekonfiguration kann der Phasenwächter optimal an die Applikation angepasst werden. Der Phasenwächter ist vielseitig einsetzbar und schützt z.B. vor Motorschäden bei Phasenasymmetrie oder Phasenausfall.

www.dold.com ■



MASCHINEN- UND ANLAGENSICHERHEIT

So könnte vorgegangen werden

Prüfung und Messung an Maschinen

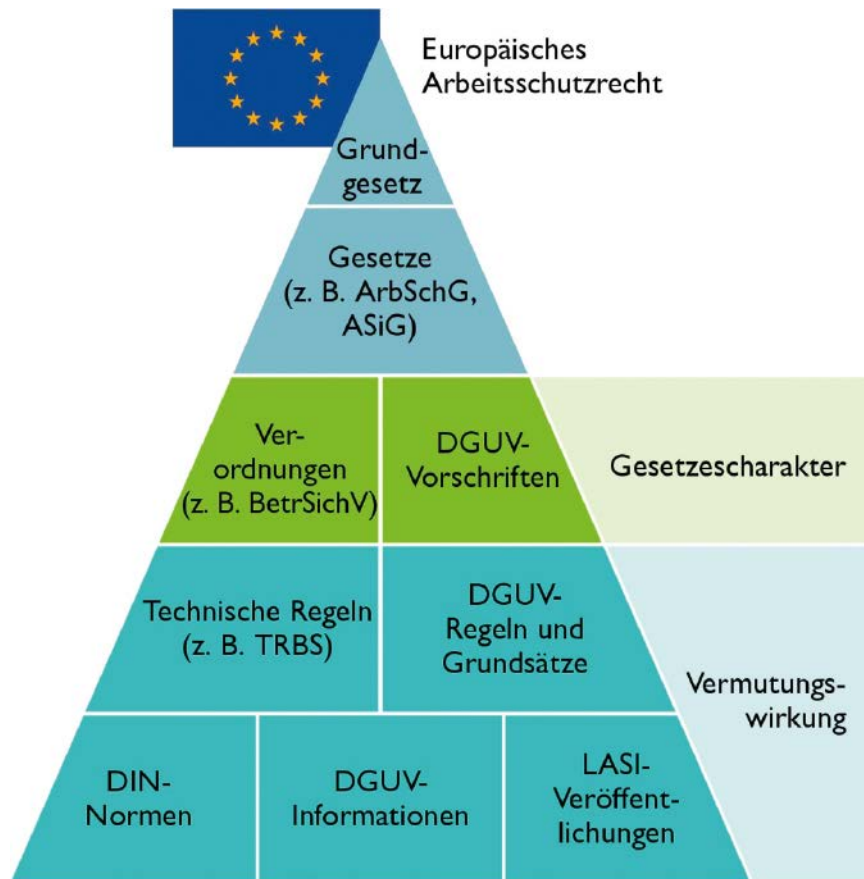
Die Betreiber von Maschinen und Anlagen wissen zumeist, dass sie regelmäßige Prüfungen und Messungen durchführen müssen. Am bekanntesten ist hier sicher die Prüfung nach DGUV-Vorschrift 3 für elektrische Anlagen und Betriebsmittel. Sollen Umgebungen und Arbeitsbedingungen so gestaltet werden, dass die Gesundheit der Mitarbeiter nicht negativ beeinflusst wird, geht das Thema jedoch weit über die DGUV-Richtlinie hinaus.

Vereinfacht ausgedrückt darf die Arbeit nicht zu Krankheiten führen. Aus dieser Maßgabe leiten sich schnell die weiteren notwendigen Prüfungen und Messungen ab. Dabei kann es sich beispielsweise um eine Lärmmessung oder die Überprüfung der Beleuchtungsstärke respektive der Konzentration von Gefahrstoffen und Gasen handeln. Welche Untersuchungen im Einzelnen erforderlich sind, wird im Rahmen der Gefährdungsbeurteilung ermittelt.

Das Prüfen und Messen an Maschinen erweist sich als elementar, um die Pflichten des Arbeitgebers zu erfüllen. Konkret ist dies in §3 „Gefährdungsbeurteilung“ und §14 „Prüfung von Arbeitsmitteln“ der Betriebs-sicherheitsverordnung (BetrSichV) beschrieben. Bei der BetrSichV handelt es sich um die Konkretisierung der Anforderungen aus dem Arbeitsschutzgesetz. Eine Ergänzung dazu stellen die Technischen Regeln für Betriebs-sicherheit (TRBS) dar. In der TRBS 1201 wird das Thema Prüfungen und Kontrollen

von Arbeitsmitteln [...] weiter ausgeführt. Die Pyramide Arbeitsrecht verdeutlicht die Abstufung zwischen Gesetzen, Verordnungen und anderen Vorschriften.

Zur Herleitung der konkreten Herangehensweise sind zunächst verschiedene Begrifflichkeiten zu klären. Die Prüfung von Arbeitsmitteln umfasst die Feststellung des Istzustands, den Vergleich des Ist- mit dem Sollzustand sowie die Bewertung der Abweichungen zwischen den Zuständen. Bei den Prüfungen wird grundsätzlich zwischen



▲ Rechtliche Zusammenhänge im Arbeitsschutz

Ordnungs- und technischen Prüfungen unterschieden. Insbesondere bei den technischen Prüfungen spielt die Kontrolle mit Mess- und Prüfmitteln eine wesentliche Rolle.

Erst nachmessen, dann beurteilen

Wie sieht nun das Vorgehen in der Praxis aus? Bevor das Arbeitsmittel durch den Arbeitgeber bereitgestellt wird, ist eine Gefährdungsbeurteilung durchzuführen. Einen Bestandteil dieser Beurteilung bildet die Definition der notwendigen Prüfungen sowie der Intervalle, in denen Wiederholungsprüfungen stattfinden müssen. Zudem wird evaluiert, welche Gefährdungen von einem Arbeitsmittel ausgehen und wie sich diese mindern lassen. Letztendlich kann es allerdings Gefährdungen geben, die im ersten Schritt nachzumessen und zu beurteilen sind, um die Notwendigkeit von Maßnahmen zu ermitteln. Als Beispiel sei das Thema Lärm angeführt. Der Maschinenhersteller gibt in seiner Dokumentation bereits an, welche Geräuschemissionen von seinem Produkt ausgehen. Er kann jedoch nicht bewerten, wie sich diese in der Arbeitsstätte des Arbeitgebers verhalten und ob Lärmschutzmaßnahmen umgesetzt werden müssen.

Des Weiteren betrachtet ein Maschinenhersteller die Geschwindigkeit von Antrieben explizit, wenn die Antriebe durch berührungslos wirkende Schutzeinrichtungen

abgesichert sind. Hinter dem Begriff dieser Schutzvorrichtung verbergen sich zum Beispiel die häufig verwendeten Lichtvorhänge und Lichtgitter. Sie schützen den Maschinenbediener nur insofern, als dass der sichere Zustand eingeleitet wird, wenn die Lichtstrahlen unterbrochen sind. Allerdings greifen Personen mit einer gewissen Geschwindigkeit in die Maschine, die normativ für die Berechnung definiert ist. Ein typischer Wert beim Eingreifen mit den Armen oder der Hand beträgt 2000 Millimeter pro Sekunde. Daraus lässt sich dann bestimmen, wie lange ein Antrieb nachlaufen darf, bis der sichere Zustand erreicht sein muss.

Maßgeblich ist der aktuelle Stand der Technik

Wie können die erforderlichen Prüfungen also festgelegt werden? Erst einmal lässt sich dazu die Dokumentation des Arbeitsmittelherstellers heranziehen. Insbesondere er verfügt über das fachliche Know-how, um Vorgaben und Vorschläge für die zu realisierenden Prüfungen zu definieren. Die Untersuchungen werden anschließend im Rahmen der Betriebsanleitung dokumentiert.

Darüber hinaus lassen sich die notwendigen Prüfungen durch den Betreiber anhand der vorhandenen Komponenten feststellen. Die Komponenten unterliegen typischerweise

einem Verschleiß und erweisen sich somit als relevant. Es empfiehlt sich, mögliche Prüfungen in allgemeinen Listen aufzuarbeiten, sodass im Rahmen der Gefährdungsbeurteilung eine Auswahl stattfinden kann. Für diese Kontrollen ist der generelle Stand der Technik zur sicheren Nutzung zu berücksichtigen.

Wie wird das bei der Nachlaufzeit gemacht

Aus der Betriebssicherungsverordnung geht hervor, dass Arbeitsmittel – in diesem Fall Maschinen und Anlagen – in regelmäßigen Abständen überprüft werden müssen. Hier lässt die BetrSichV eine gewisse Freiheit zu und gibt nicht vor, wie oft etwas kontrolliert werden soll. Wie schon erwähnt, sind die zeitlichen Angaben in der Gefährdungsbeurteilung festgeschrieben. Informationen dazu finden sich teilweise in den Dokumentationen der jeweiligen Hersteller.

Einleitend wurde die Nachlaufzeitmessung bereits aufgeführt. Sie wird an berührungslos wirkenden Schutzeinrichtungen ebenso wie an beweglich trennenden Schutzeinrichtungen – auch als Schutztüren bekannt – durchgeführt. Bei der Nachlaufzeitmessung lösen das Messgerät und ein zugehöriger Akteur ein Stoppsignal aus. Danach erfolgt eine Auswertung, wie lange es dauert, bis eine gefährbringende Bewegung zum Stillstand kommt.



▲ Abgleich zwischen dem Soll- und Ist-Zustand

Auf Basis der erfassten Nachlaufzeit lässt sich mit Hilfe einer Formel aus der DIN EN ISO 13855 der Sicherheitsabstand bestimmen. In der Regel nimmt das Messgerät diese Berechnungen selbst vor und zeigt sofort den normativen Mindestabstand an. Dieser sagt aus, in welcher Entfernung die berührungslos wirkende Schutzeinrichtung von der gefahrbringenden Bewegung angebracht sein muss.

Am besten alles dokumentieren

In der Praxis wird die Nachlaufzeitmessung wie folgt realisiert: Zu Beginn muss sich der Verantwortliche einen Überblick über die Situation verschaffen. In diesem Zusammenhang legt er fest, wo und wie das Nachlaufzeitmessgerät angebracht werden kann. Dabei ist zu beachten, dass das Messgerät ebenso wie die gefahrbringende Bewegung nicht beeinträchtigt, geschweige denn beschädigt wird. Es muss überhaupt möglich sein, Antriebe im manuellen oder automatischen Betrieb

zu aktivieren und noch unter den definierten Geschwindigkeiten bewegen zu lassen.

In der Dokumentation wird aufgenommen, wie die Maschine beschrieben ist. Um im Nachhinein den Überblick zu behalten sowie eine eindeutige Identifizierung umsetzen zu können, empfiehlt es sich, die Daten zur Maschine, der überprüften Schutzeinrichtung und dem eingesetzten Messgerät schriftlich festzuhalten.

Im Anschluss werden das Messgerät und der gewählte Sensor in Stellung gebracht. Hierbei kann es sich um optische Sensoren als auch Seilzuggeber oder vergleichbare Geräte handeln. Ist der Sensor an der gefahrbringenden Bewegung installiert, steht der Personenschutz im Fokus. Zum Starten der Messung müssen sich die Mitarbeiter aus dem Gefahrenbereich entfernen. Anschließend geschieht die Einstellung des Messgeräts. Als nächstes wird die zehnmals zu wiederholende Messung durchgeführt. Unter Umständen

hat eine vorab vorgenommene Geschwindigkeitsmessung Einfluss auf den Zeitpunkt der Messung. Die Auslösung mit handelsüblichen Geräten passiert dann automatisch.

Mit früheren Werten vergleichen

Während der Messung sollte unbedingt ein maschinenkundiger Mitarbeiter vor Ort sein. Dieser kennt normalerweise die Bewegungen und Abläufe der Maschine, weshalb er sie beim Messen in die Ausgangsposition bringen kann, um die zehn Messungen auszuführen. Ist dies erledigt und sind die Ergebnisse ausgewertet, wird der Prüfbericht generiert. Aus ihm lässt sich ableiten, ob die erfassten Werte in Ordnung sind. Ein Vergleich mit vorab stattgefundenen Messungen zeigt auf, ob es im Laufe der Zeit Veränderungen gibt. In Punkt D.4 der DIN EN ISO 13855 sind Empfehlungen aufgelistet, wie ein Prüfprotokoll aussehen kann. ■

Autoren



Stefan Seibel



Henrik Vandieken

Competence Center Services,
Phoenix Contact Deutschland GmbH

Kontakt

Phoenix Contact
Blomberg
Tel.: +495235 3 12000
info@phoenixcontact.de
www.phoenixcontact.de

Die Maschine vom Profi inspizieren lassen

Damit Maschinen sicher betrieben werden können, empfiehlt es sich, ergänzend zur Gefährdungsbeurteilung eine Maschineninspektion durchzuführen. Im Rahmen einer solchen Inspektion werden die Umsetzung der Sicherheitsfunktionen, der Stand der Technik der Schutzeinrichtungen sowie deren korrekte Installation inklusive der Sicherheitsabstände überprüft. Ferner erfolgt eine Kontrolle der elektrischen, pneumatischen, hydraulischen und weiteren Ausrüstung. Einen zusätzlichen Bestandteil der Maschineninspektion bilden die in der Gefährdungsbeurteilung ermittelten und zu realisierenden Messungen.

Aus dem Gesamtergebnis lässt sich ableiten, welche Maschinen mit welcher Priorität bearbeitet werden müssen, welche Maßnahmen erforderlich sind und mit welchen Kosten kalkuliert werden muss. Das Team des Competence Center Services unterstützt gerne bei der konkreten Umsetzung der detektierten und festgelegten Schritte. Als weiterführende Lektüre bietet sich das Buch „Betreiberpflichten für Alt- und Gebrauchsmaschinen“ aus dem Reguvis Verlag (ISBN 978-3-8462-1017-8) an.



Fachbuch zu Betreiberpflichten für Alt- und Gebrauchsmaschinen ▶

Umrücker für Profinet IRT zertifiziert

Mit dem offenen Ethernet-Standard Profinet setzt Baumüller auf eine flexible, sichere und durchgängige Kommunikationstopologie. Das Unternehmen hat seine Servoantriebe B Maxx 5000 nach dem aktuellsten Standard für Profinet IRT zertifiziert. Neben dem echtzeitfähigen EtherCAT-Feldbus bietet das Unternehmen für das Servosystem B Maxx 5500 verschiedene Bussysteme wie CANopen, Varan, Modbus TCP, Profinet IRT, Ethernet/IP oder Powerlink. Die Antriebstechnik des Unternehmens ist dadurch besonders flexibel und ermöglicht die Kombination mit Systemkomponenten verschiedener Hersteller. Die B-Maxx-5000-Familie umfasst sowohl anreihbare Geräte als auch leistungsstarke Monoein-



heiten. Die kompakten Einspeise-, Rückspeise- und Achseinheiten lassen sich durch ein integriertes Drive-Connect-System schnell und einfach kombinieren und sind in den Kühlarten Luft, Wasser und Öl verfügbar.

www.baumueller.de ■

Mehrfarbige LED-Leuchte für Ex-Bereich

Pfannenberg ergänzt mit der Quadro LED-RGB-3G/3D sein Produktportfolio für den Ex-Bereich. Ausgestattet mit moderner LED-Technologie bietet die RGB-Leuchte flexible und vielfältige Signaloptionen und Betriebsmodi für Industrieanwendungen im Bereich Informieren und Warnen. Der entscheidende Vorteil der Leuchte ist, dass aus einer Vielzahl von RGB-Farben gewählt werden und so über nur eine Leuchte der gewünschte Status visualisiert werden kann. Die Leuchte kann überall dort zur Anwendung kommen, wo mit Gasen und Feinstäuben sowie anderen explosiven Materialien gearbeitet wird. Die Anwendungen sind dabei vielfältig, so ist die RGB-Leuchte sowohl für den



Innen- als auch den Außenbereich geeignet und kommt beispielsweise in Maschinen- und Anlagenbetrieben, in Raffinerien, der pharmazeutischen und chemischen Industrie, in der Holzverarbeitenden Industrie, in Lackierbereichen oder auch in industriellen Bäckereien zum Einsatz.

www.pfannenberg.com/de ■

Forschungsexperimente unter Weltraumbedingungen

Der ADV200-Frequenzumrichter von Gefran ist im Einsatz, um physikalische und produktionstechnische Versuche für Anwendungen im Weltraum, auf dem Mond oder sogar auf dem Mars zu simulieren. Dafür finden Forschungsexperimente statt, die das Institut für Transport- und Automatisierungstechnik (ITA) mit dem Institut für Quantenoptik der Leibniz Universität Hannover auf die Beine gestellt. Während die Wiederholrate bei anderen Falltürmen bei etwa zwei bis drei Versu-

chen am Tag liegt, kann im Einstein-Elevator alle vier Minuten ein neuer Durchlauf stattfinden. Anstelle von großen Vakuumkammern und freiem Fall, saust hier eine an Schienen geführte Versuchskammer in hoher Geschwindigkeit auf und ab. Bei einem Abschuss der Gondel wird eine große Menge an Energie durch die Gefran-Umrücker aus einem Supercap-Energiespeicher entnommen und an die Statoren weitergegeben.

www.gefran.com ■

Funktionale Gehäuselinie Proboxx

Flexibel, funktional und formschön – diese Eigenschaften zeichnen die Gehäusereihe Proboxx von Schlegel aus. Mit der Produktlinie ergänzt der Hersteller sein Gehäuse-Portfolio um eine edle und zugleich praktische Variante, die das tägliche Arbeiten erleichtert. Die Proboxx kann vielfältig eingesetzt werden. Die Konzeption erlaubt eine einfache Integration in bestehende Strukturen und berücksichtigt aktuelle technische Standards. Sie kann sowohl mit konventioneller Verdrahtung als auch mit modernen Kommunikationssysteme-



men genutzt werden. Der Hersteller bietet die Proboxx als Leergehäuse oder als bestücktes Gehäuse an. Die bestückten Gehäuse gibt es für vier verschiedene Systeme mit jeweils bis zu vier Befehlsstellen: konventionelle Verdrahtung, IO-Link, AS-Interface und Funk. Alle Systeme sind mit einer M12-Schnittstelle ausgestattet.

www.schlegel.biz ■

Not-Halt-Schalter

Mit dem Smart-Safety-System von Bernstein können auch die Not-Halt-Geräte SEU (Safety Emergency Unit) in ein und demselben Sicherheitskreis verdrahtet werden. Klassischerweise werden die Schutztür-Überwachung sowie die Not-Halt-Funktion in Reihe verdrahtet, aber immer noch getrennt voneinander, sodass mehrere Sicherheitsrelais benötigt werden. Neben den Sicherheitssensoren SRF (Safety RFID) zur Überwachung der Schutztüren, können auch die Not-Halt-Geräte SEU in ein und demselben Sicherheitskreis verdrahtet werden. Dank des patentierten Daisy-Chain-Diagnosesystems (DCD) können mit den dazugehörigen Sicherheitsauswertungen umfangreiche Diagnose-daten jedes angeschlossenen Geräts



zum Beispiel über Ethernet ausgewertet werden. Mit dem beleuchteten Not-Halt SEU können diese Daten nicht mehr nur an einem HMI (Human-Machine-Interface) visualisiert werden, sondern sind dank der großen LED-Statusanzeige auch direkt am Gerät schnell sichtbar.

www.bernstein.eu ■




MASCHINEN- UND ANLAGENSICHERHEIT

Intralogistik im Outdoor-Bereich auf einem neuen Level

Der Sicherheitslaserscanner outdoorScan3 im Stresstest bei Basf

Mit fahrerlosen Transportsystemen (FTS) entwickelt Basf Prozesse in der Intralogistik über die Hallengrenzen hinaus weiter. Das global agierende Chemieunternehmen hat dabei eine Steigerung der Produktivität und Flexibilisierung der Logistikprozesse an seinen Standorten im Fokus. Mit interdisziplinärer Kompetenz arbeiten Basf, Sick und namhafte FTS-Hersteller gemeinsam an einem Konzept für eine autonome und lückenlose Logistikkette im Außenbereich.



Stresstest für den outdoorScan3: Bei Basf beweist der Sicherheitslaserscanner zurzeit seine outdoor-Fähigkeiten



Michael Badeja,
Product Manager bei
der Sick AG



Marco Burkhart,
Intralogistic Design,
BASF SE



Tobias Gaschnitz,
Intralogistic Design,
BASF SE

Bei einem Besuch auf der SPS IPC Drives 2018 in Nürnberg nehmen Marco Burkhart und Tobias Gaschnitz, beide als Automatisierungstechniker bei Basf für Intralogistic Design zuständig, am Sick Messestand den outdoorScan3 genau unter die Lupe. Der Sicherheitslaserscanner kommt für die Anforderungen an eine sichere und verfügbare Mensch-Maschinen-Kollaboration für den Außenbereich bei Basf in die engere Wahl. Die Logistikexperten der Basf haben viel Erfahrung mit fahrerlosen Transportsystemen im Indoor-Bereich gesammelt. Nun wagen sie den nächsten Schritt für die Zukunft mit automatisierter Logistik im Außenbereich: „Wir wollen ein Outdoor-Fahrzeug zum Einsatz bringen, das auch bei schwierigen Umweltbedingungen autonom ist und ohne menschliche Überwachung funktioniert“, bringt Marco Burkhart das Ziel des Entwicklungsprojektes auf den Punkt.

Sichere Interaktion zwischen Mensch und Maschine

Das Wichtigste dabei ist, so Tobias Gaschnitz, „dass Menschen und natürlich auch Waren vor Kollisionen mit den oft schnellen und teils auch schwer beladenen Fahrzeugen zu hundert Prozent geschützt sind.“ Gleichzeitig darf die Sicherheitstechnik nicht zu einer Verfügbarkeitsbremse werden. Für die sichere Interaktion zwischen Menschen und Maschinen will man zukünftig auf taktile Lösungen mit Sicherheits-Schaltleiste verzichten und dafür eine kontaktlose smarte Sensorlösung einsetzen. Hierzu wird der outdoorScan3 als mögliche Lösung getestet.

Eine Vielzahl von Herausforderungen ist für diese Zukunftsvision der autonomen Logistik zu bewältigen. Dafür hat sich Basf kompetente Partner ins Boot geholt – darunter mehrere namhafte FTS-Hersteller und Sick für die Sicherheitssensorik. Denn mit verschiedenster Sick Sensorik zur kontur- oder reflektorbasierten Lokalisierung, zur Grob- und Feinpositionierung, zum Messen und Identifizieren sowie zur optischen Datenübertragung hat Basf bereits an vielen Standorten weltweit gute Erfahrungen gesammelt. „Wir sind von der Kompetenz von Sick bei

smarten Sensorlösungen für die Intralogistik überzeugt. Idealerweise verbindet Sick auch noch eine langjährige Zusammenarbeit mit den FTS-Herstellern“, erläutert Marco Burkhart die Entscheidung für den Test-Partner.

Mit der Entwicklung des Sicherheitslaserscanners outdoorScan3 ist jetzt eine Technologie verfügbar, die sich ausgesprochen unempfindlich gegenüber Sonnenlicht, Regen, Schnee oder Nebel zeigt. Dank der outdoor-safeHDDM-Scantechnologie arbeitet der Laserscanner bei einer Sonneneinstrahlung mit einer Beleuchtungsstärke bis zu 40.000 lux fehlerfrei. Zudem erkennt der intelligente Software-Algorithmus des Laserscanners Regen und Schnee und filtert diese Umwelteinflüsse problemlos aus – Regen beispielsweise bis zu einer Niederschlagsstärke von 10 mm/h. Selbst bei Nebel bis zu einer meteorologischen Sichtweite von 50 Metern detektiert der outdoorScan3 alle Hindernisse gewissenhaft.

Applikationsentwicklung im Spannungsfeld von Produktivität und Sicherheit

Seit Herbst 2019 erprobt Basf sukzessive die zentralen Features des outdoorScan3 an mehreren Produktionsstandorten mit individuell konfigurierten Teststationen, um die Tauglichkeit des outdoorScan3 weltweit zu bewerten. Sick begleitet mit dieser Art Teststationen die Applikationsentwicklung seiner Kunden vor Ort und von Beginn an. Dabei setzt Sick auf praxisorientierte Diagnostik, die über Fernzugriff und Cloud-Dienste für die jeweils bestmögliche Automatisierungslösung im Sinne von Industrie 4.0 sorgt. Michael Badeja, Produkt Manager bei Sick, erläutert die Vorgehensweise: „Produktivität und Sicherheit sind zwei Aspekte, die in dieser gemeinsamen Applikationsentwicklung mit Basf und den FTS-Herstellern stets gleichberechtigt bewertet werden. Unsere Herangehensweise erfolgt auf zwei Ebenen: Wir betrachten zum einen die grundsätzliche Verfügbarkeit sowie die Arbeitsweise des outdoorScan3 und zum anderen die Integration auf Systemebene im Fahrzeug. Wir suchen so bei diesen Aspekten gemeinsam nach der

Wiley Industry Days
WIN DAYS
www.WileyIndustryDays.com
7.-9. Juni 2021



Jörg Wüllner
 Tel.: +49 6201 606 749
joerg.wuellner@wiley.com

Virtuelle Show mit Konferenz, Ausstellung und Networking für Automatisierung, Machine Vision, Photonics, Healthcare und Sicherheit.



Sichere Interaktion zwischen Menschen und Maschinen: So könnte eine kontaktlose Sensorlösung im Außenbereich aussehen

jeweils optimalen Lösung und kommen über Synergien zu strukturellen Verbesserungen und neuen Ansätzen, die wir marktbegleitend umsetzen.“

Verfügbarkeit: vielversprechend

Die bisherigen Ergebnisse aus dem TestszENARIO stimmen die Logistikexperten positiv, denn die grundsätzliche Verfügbarkeit des outdoorScan3 ist vielversprechend. Über den Fernzugriff erhalten die Anwender Einblick in standortspezifische Gegebenheiten. So wird zum Beispiel das Verhalten des outdoorScan3 bei Regen und die daraus resultierende Dauer der kumulierten Feldverletzungen pro Tag diskutiert. Ziel der interdisziplinären Teamarbeit ist es, die unerwünschten Feldverletzungen bei Regen auf ein Minimum zu reduzieren.

Dabei kommt den Synergieeffekten ein erhöhtes Augenmerk zu. Denn erst durch die Verbindung von Installation des outdoorScan3 im Fahrzeug, der Einsatz eines geeigneten Wetterschutzes und organisatorische Maßnahmen wird eine zufriedenstellende Lösung entwickelt.

Condition Monitoring – Basis für Lösungsansätze

Möglich wird diese umfangreiche Diagnose als Basis für die erfolgreiche Lösungsfindung mit dem Einsatz der Systeme für Fernzugriff von Sick. Durch neue digitale Services, wie Condition Monitoring und Datenanalyse, werden Live-Daten aus der Applikation und ihre Historie visualisiert, ausgewertet und interpretiert. Vierteljährlich erfolgt in einem Basf-spezifischen Bericht eine Analyse der Daten. Ergänzende Wetterdaten erlauben mit Anomalie- und Mustererkennung die Bewertung von Einflüssen auf die Verfügbarkeit des outdoorScan3. So lassen sich große Datenmengen auf die wesentlichen Aussagen reduzieren und nutzen. Zugleich können Schutzfeldeinstellungen frühzeitig angepasst und Serviceeinsätze bedarfsorientiert durchgeführt werden. Das erhöht die Verfügbarkeit und minimiert langfristig die Downtime.

Limitierungen auflösen

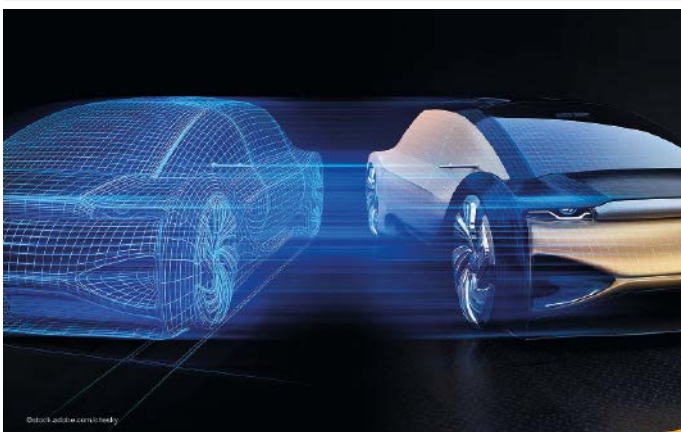
Doch warum schaltet der Sicherheitslaserscanner überhaupt ab? Hier kommt die Anforderung für funktionale Sicherheitssensoren

zum Tragen. Über Selbstdiagnose im Gerät und smarte Algorithmen muss der Sicherheitslaserscanner kontinuierlich die Umgebungsbedingungen sowie den zuverlässigen Betriebszustand überwachen, um den hohen Sicherheitslevel Pl d (ISO 13849-1) auch für den Außenbereich zu gewährleisten. Dies kann dazu führen, dass bei bestimmten Umgebungsbedingungen die Verfügbarkeit limitiert wird, da sich die Messdatengüte nicht sichergestellt lässt. Diese Limitierungen können durch zusätzliches Equipment an Scanner und Fahrzeug, z. B. über Schutzhauben aufgelöst werden.

Nach den vielversprechenden statischen Tests an den Sensor-Stationen geht der Stress-Test für den outdoorScan3 bei Basf nun in die nächste Phase: Zeitnah beginnt der Aufbau an den fahrerlosen Transportfahrzeugen, um weiter applikationsnah zu testen und das System auf den produktiven Betrieb vorzubereiten. Für alle Beteiligten wird dies ein mit Spannung erwarteter nächster Schritt auf dem Weg in die Zukunft der autonomen Outdoor-Logistik. ■

Kontakt

Sick AG
Waldkirch
Tel.: +49 7681 202 4183
info@sick.de
www.sick.de



Smarte Sensoren für KI-Anwendungen ▲

Ob Predictive Maintenance, Smart Shipping oder Digitaler Zwilling: Intelligente Sensoren liefern Daten für viele wegweisende Anwendungen der Zukunft. Smarte Sensoren sind in der Lage, ungeheure Datenmengen eigenständig zu verarbeiten. Sie übernehmen nicht nur das Pre-Processing wie z. B. die A/D-Wandlung und Filterung, sondern können die vorverarbeiteten Daten dank der integrierten Rechentechnik auch

aus- und bewerten. Die smarten Sensoren übermitteln deshalb keine Rohdaten mehr an Peripherie-Geräte, sondern nur noch Statusinformationen. Eine aufwendige externe Datenerfassung und -verarbeitung ist somit nicht mehr erforderlich. Smarte Sensoren übertragen ihre Signale zudem drahtlos, sodass eine zeitintensive Verkabelung entfällt.

www.asc-sensors.de ■



Wie Steigtechnik korrekt geprüft und eingesetzt wird ▲

Wie Hymer-Leichtmetallbau mitteilt, haben Unternehmen, die Leitern, Tritte, Arbeits- oder Schutzgerüste einsetzen, im Sinne der Arbeitssicherheit einige Pflichten zu erfüllen: Die Steighilfen müssen regelmäßig auf ihren ordnungsgemäßen Zustand überprüft und die Mitarbeiter im Umgang geschult werden. Wie das vorschriftsgemäß umgesetzt wird, vermittelt Diplom-Ingenieurin (FH) Petra Liebsch – Expertin mit

über zwanzigjähriger Erfahrung in den Bereichen Leitern, Tritte, Fahrgerüste, Arbeitssicherheit und Qualität – im VDSI-anerkannten „Seminar für befähigte Personen für Leitern, Tritte und Fahrgerüste“ auf Basis der BetrSichV, der TRBS 2121-1 bzw. -2 sowie der DGUV-Informationen 208-016 und 201-011 am Firmensitz von Hymer-Leichtmetallbau in Wangen im Allgäu.

www.hymer-alu.de ■

Schutzanzug gegen Hochdruckwasserstrahlen

Der Schutzanzug Dehncare WJP Advanced gegen Hochdruckwasserstrahlen von Dehn bietet zusammen mit Handschuhen, Helm, Visier, Strümpfen und Kapselgehörschutz umfassende Arbeitssicherheit für



den Anwender. Bereiche, die dem Strahlwasser besonders ausgesetzt sind – vor allem die Arme und unteren Beine – werden beim WJP Advanced durch zusätzliche Protektoren verstärkt geschützt. Entsprechend dem Prüfgrundsatz des Instituts für Arbeitsschutz der DGUV ist der Anzug mit 1.000 bar (Flachstrahldüse) zertifiziert. Geprüft wurde er mit 1.200 bar. Mit nur noch 1,6 kg (Größe M) gibt es eine Basic-Variante des WJP Schutzanzugs. Dieser bietet bei Hochdruckwasser einen Schutz bis 750 bar (geprüft mit Flachstrahldüse in Anlehnung an Prüfgrundsatz). Verwendet wird das gleiche Material wie beim Dehncare WJP Advanced, das abrieb-, reißfest und wasserdicht ist.

www.dehn.de ■

Montagearbeitsplätze mit Cobot-Anbindung

Mit seinen nach ergonomischen Gesichtspunkten gestalteten, anforderungsspezifischen Montagearbeitsplätzen bietet RK Rose+Krieger eine richtungsweisende Lösung für die wirtschaftliche Fertigung komplexer Produkte in kleinen Stückzahlen mit einer hohen Variabilität. Kombiniert mit kollaborierenden Robotern und (teil)automatisierten Entnahme- und Beladevorrichtungen von Mitsubishi Electric sowie lineartechnischen Zuführungen aus dem Portfolio von RK Rose+Krieger entlasten sie die Mitarbeiter von körperlich belastenden oder monotonen Tätigkeiten und sichern gleichzeitig die prozesssichere, fehlerfreie Fertigung. Bei der Montage an modernen Arbeitsplätzen können kollaborierende Roboter dem Werker Material anreichen oder fertige Teile an den dafür vorgesehenen Stellen



abgeben. Sie bieten sich auch für bahngesteuerte oder in Position haltende Tätigkeiten, die ein Mensch entweder nicht so präzise, dauerhaft oder schnell und sicher ausführen kann wie eine Maschine, an.

www.rk-rose-krieger.com ■

Alarmweiterleitung für Sicherheitsschrankmodelle

Asecos bringt zwei Module zur Alarmweiterleitung für Ion-Line-Sicherheitsschrankmodelle auf den Markt. Sie geben im Ernstfall verschiedene Warn- und Alarmzustände an eine Rufnummer bzw. eine Leitstelle weiter. So lassen sich umgehend individuelle Maßnahmen



ergreifen. Zu jeder Tages- und Nachtzeit muss ein Lithium-Ionen-Sicherheitsschrank sicher beaufsichtigt werden, um einen umfassenden Schutz zu gewährleisten. Schließlich lagern Batterien oder Akkus in ihm oder werden dort aufgeladen. Die beiden Alarmweiterleitungsmodule gewährleisten diesen

Schutz. Das Fernmeldemodul bietet Nutzern die Möglichkeit, einen Alarm über das Mobilfunknetz per SMS mit frei konfigurierbaren Nachrichtentexten oder per Anruf an bis zu fünf programmierbare Rufnummern weiterzuleiten. Insbesondere für kleine und mittelständische Unternehmen ohne eine zentrale Gebäudeleittechnik ist dies eine gute Option.

Das Fernmeldemodul ist für die drei Modelle „Battery Charge“, „Battery Charge Pro“ und „Battery Store Pro“ der Ion-Line-Reihe entwickelt und lässt sich vom Schranknutzer selbstständig nachrüsten. Sobald Veränderungen im Schrank eintreten, informiert das Fernmeldemodul die Nutzer – zu jeder Tages- und Nachtzeit und an jedem Ort, an dem sich der Empfänger aufhält. Wird eine Temperaturerhöhung oder eine Rauchentwicklung detektiert, wird bei den Pro-Modellen der Ion-Line ein Anruf oder eine SMS getätigt. Sollte sich im Schrank Rauch bilden, werden beim Modell Battery Charge die Nutzer ebenfalls per SMS oder Anruf informiert. Das Relaismodul unterscheidet vier verschiedene Warn- und Alarmstufen



für die beiden Modelle Battery Charge Pro und Battery Store Pro und leitet sie über separate, potentialfreie Kontakte an eine Leitstelle. Durch die Differenzierung der verschiedenen Warn- und Alarmzustände lassen sich jeweils umgehend individuelle Maßnahmen einleiten. Somit kann ein optimaler Schutz für Personen und Gebäude gewährleistet werden.

Asecos bietet ein Whitepaper als Nachschlagewerk zur schnellen Information über Lithium-Ionen-

Akkus. Auf 20 Seiten hat Dr. Friedhelm Kring – freier Fachjournalist mit Schwerpunkt Umweltschutz und Sicherheit am Arbeitsplatz – wichtige Fachinformationen zu Lithium-Ionen-Akkus verständlich dargestellt. Tipps, Praxisbeispiele und Checklisten für den Umgang mit dem modernen Gefahrstoff Lithium-Ionen-Akku runden das Nachschlagewerk ab. Über www.asecos.com/whitepaper kann das Whitepaper angefordert werden.

www.asecos.com ■

GEFAHRSTOFFE

Training ist alles

Bei Gefahrstoff-Leckagen zählen Know-how und der richtige Handgriff

Im Umgang mit flüssigen Gefahrstoffen kann es bei der täglichen Arbeit auch zu Leckagen oder anderen Zwischenfällen kommen. Dann ist ein schnelles und routiniertes Handeln erforderlich, bei dem jede Sekunde zählt, um Sach-, Personen- und Umweltschäden einzudämmen und um die Anforderungen des Gesetzgebers oder von Versicherungen einzuhalten.

Damit es erst gar nicht zu unerwünschten Schäden kommt, können Unternehmen präventiv viele Maßnahmen im Leckagemanagement treffen, um gesetzeskonform zu agieren. Doch für „Nichtfachleute“ kann es schnell schwierig und zeitaufwändig werden, sich bei der Vielzahl an gesetzlichen Rahmenbedingungen zurecht zu finden und die geeigneten Maßnahmen für den eigenen Betrieb auszuwählen. Um sich einen leichteren Überblick zu verschaffen, steht Gefahrstoffexperte Tobias Authmann, Fachreferent für Gefahrstofflagerung und Arbeitssicherheit bei Denios im Interview rund um das Thema Leckagemanagement mit GIT SICHERHEIT Rede und Antwort.

GIT SICHERHEIT: Herr Authmann Sie führen seit Jahren regelmäßig das „Leckage-Notfall-Training“ in der Denios Academy für die unterschiedlichsten Unternehmen und deren Mitarbeiter durch. Wo liegen aus Ihrer Sicht die Hauptursachen für Gefahrstoffleckagen?

Tobias Authmann: Die Ursachen für Leckagen sind vielfältig und schwer auf eine Hauptursache einzugrenzen. Man kann aber eine Unterscheidung nach quantitativen Aspekten vornehmen: Bei händisch durchgeführten Arbeiten mit kleineren Gefäßen sowie Umfüllvorgängen kommt es im Normalfall zu kleineren, meist gut beherrschbaren Leckagen. Anders ist es dagegen bei der Anlieferung und Entsorgung, im innerbetrieblichen Transport sowie bei der Einspeisung großer Mengen von Gefahrstoffen in Anlagen, also dort, wo große Behältnisse im Spiel sind. Wenn es an diesen Stellen zu einer Leckage kommt, kann die Schadensbegrenzung zu einer ernstlichen Herausforderung werden und die daraus resultierenden Schäden können erheblich sein.

In welchem Bereich im Umgang mit Gefahrstoffleckagen herrscht die größte Unsicherheit? Wo liegen die typischen Gefahrenpotentiale im Unternehmen?

Tobias Authmann: Sobald der Normalbetrieb aufgrund unvorhergesehener Ereignisse wie Leckagen verlassen wird, entstehen Unsicherheiten. Je nach ausgetretener Menge, Gefährlichkeit der Substanz sowie Örtlichkeit, an dem sich die Leckage ereignet hat, kann bei vielen Mitarbeitern schnell Nervosität und Überforderung eintreten. Um dem entgegenzuwirken ist es grundsätzlich notwendig, dass sich die Unternehmen bereits vor dem Eintritt des Ernstfalls Notfallpläne erarbeiten, in denen unter anderem auch klare Handlungsanweisungen für diese Situationen festgelegt werden.

Gibt es im Leckagemanagement von Gefahrstoffen Unterschiede für Gefahrenpotentiale durch die Unternehmensgröße?

Tobias Authmann: Gefahrenpotentiale sind einmal quantitativ, nach der Menge der vorhandenen Betriebsstoffe zu bewerten. Hier lässt sich in vielen Fällen ein Zusammenhang zwischen der Unternehmensgröße und dem Gefahrenpotential herstellen.

Hingegen ist die rein qualitative Gefahr vorrangig von den Stoffeigenschaften abhängig. In Bezug darauf lässt die Unternehmensgröße nicht zwangsläufig einen Rückschluss auf das Gefahrenpotential zu. Werden sehr viele unterschiedliche Chemikalien auf dem Betriebsgelände vorgehalten, stellen sich bereits an eine sichere gesetzeskonforme Lagerung hohe Ansprüche. Für den Leckagefall ergeben sich so mehr Szenarien, die im



Tobias Authmann,
Fachspezialist für
Gefahrstoffleckagen
bei Denios



Notfallplan bedacht werden und auf welche die Mitarbeiter vorbereitet werden müssen.

Können Sie grundsätzlich aufzeigen, wie man im Falle einer Leckage mit den jeweiligen Gefahrstoffen vorgeht? Bei einer Leckage mit Öl muss sicherlich anders vorgegangen werden als bei einer Leckage mit Säuren oder Laugen. Worin genau liegen hier die Unterschiede?

Tobias Authmann: Bei der Eindämmung und Aufnahme von Leckagen gibt es keine großen Unterschiede. Wichtig sind vor allem die Wahl eines für den jeweiligen Fall geeigneten Bindemittels sowie die adäquate Persönlicher Schutzausrüstung (PSA). Der Selbstschutz der Mitarbeiter sollte bei jeglicher Aktivität immer die höchste Priorität genießen! Insofern sind die Fragen nach der adäquaten Schutzausrüstung und ob man die Leckage selbst bereinigen kann oder doch besser die Feuerwehr zur Hilfe ruft, im wahrsten Sinne des Wortes von existenzieller Bedeutung.

Wie können Unternehmen in Bezug auf Gefahrstoffleckagen aktiv Vorsorge betreiben?

Tobias Authmann: Der §5 Arbeitsschutzgesetz (ArbSchG) schreibt Gefährdungsbeurteilungen vor. Daraus leiten sich Schutzmaßnahmen, Betriebsanweisungen und Notfallpläne ab. Werden in diesen Zuständigkeiten, Vorgehensweisen im Unternehmen klar definiert, und eine den Stoffen und Mengen entsprechende Notfallausrüstung vorgehalten und deren Verwendung trainiert, ist ein Unternehmen gut vorbereitet!

Wie wichtig sind aus Ihrer Sicht Mitarbeiterschulungen für das Leckagemanagement bei Gefahrstoffen?

Tobias Authmann: Die Mitarbeiterschulung ist ein unverzichtbarer Baustein der Betriebssicherheit. Der beste Notfallplan kann nur funktionieren, wenn er unter Einbeziehung der Mitarbeiter auf Praxistauglichkeit getestet wurde. Daher beinhaltet das Leckage Notfall-Training der Denios Academy auch den aktiven Trainingsteil. Entsprechend geschulte Mitarbeiter beachten den Eigenschutz, kennen die verfügbaren technischen Hilfsmittel, deren Aufbewahrungsort und wissen, wie sie diese verwenden müssen. So ist es ihnen möglich, im Ernstfall souveräner und routinierter zu reagieren. Verkürzte Reaktionszeiten tragen wesentlich zum besseren Schutz der Umwelt und des Unternehmens bei.

Aus welchen Bestandteilen sollte sich die persönliche Schutzausrüstung für die Beschäftigten zusammensetzen, wenn sie sich in einem Leckagefall mit Gefahrstoffen befinden?

Tobias Authmann: Als minimale Schutzausrüstung sollten ausnahmslos geschlossene Sicherheitsschuhe, eine dicht schließende Schutzbrille sowie medienbeständige Schutzhandschuhe getragen werden! In manchen Fällen kann auch Atemschutz erforderlich sein. Sobald die Verwendung von Vollschutz notwendig ist, muss man sich fragen, ob die Feuerwehr verständigt werden sollte. Wurden die Voraussetzungen hierfür bereits im Notfallplan definiert, so schafft das für alle Beteiligten zusätzlich Sicherheit und spart ggf. Zeit! In Ex-Zonen muss zudem auf eine ATEX-konforme Ausrüstung geachtet werden.

Welche technischen Schutzmaßnahmen sollten am Arbeitsplatz für den Leckagefall mit Gefahrstoffen zur Verfügung stehen?

Tobias Authmann: Am Arbeitsplatz sind die geeignete PSA und sonstige Schutzmaßnahmen bereits für die reguläre tägliche Arbeit essentiell. Darüber hinaus sollten erweiterte technische Schutzmaßnahmen wie geeignete Bindemittel, Gullyabdeckungen, Faltrwannen etc. bereitgehalten werden. Am besten nahe an den Orten platziert, an denen nach der Gefährdungsbeurteilung am ehesten mit Leckagen zu rechnen ist.

Welche Maßnahmen schreibt der Gesetzgeber vor, um Umweltgefährdungen im Leckagefall mit Gefahrstoffen zu vermeiden?

Tobias Authmann: Es gibt zwei elementare Ansätze bei der Vermeidung von Umweltbeeinträchtigungen: Zum einen gibt es die präventiven Maßnahmen, zu denen das gesetzeskonforme Lagern von Gefahrstoffen in speziellen Gefahrstofflagern zählt. Dazu zählt auch die passende Auffangwanne für den jeweiligen Gefahrstoff, um bei der Lagerung kein Risiko einzugehen. Zum anderen sollten die Maßnahmen, die nach dem Notfallplan aufgestellt, berücksichtigt werden, um die bestmögliche Minimierung der Auswirkungen im Schadensfall zu bewirken. ■

Kontakt

Denios AG
Bad Oeynhausen
Tel.: +49 5731 753 0
info@denios.de
www.denios.de

Berufsbekleidung steuerlich anerkannt



Wie Mewa mitteilt, gewinnt ein Unternehmer doppelt, wenn er die Anschaffung der Schutzkleidung sowie Arbeits- oder Berufsbeklei-

dung für sein Personal selbst in die Hand nimmt. Einerseits kann er sicherstellen, dass seine Mitarbeiter mit einem professionellen und zum Unternehmen passenden Outfit ausgestattet sind. Andererseits kann er die Ausgaben für die Anschaffung sowie für die kontinuierliche Pflege und Instandhaltung als Betriebsausgaben steuermindernd geltend machen. Das Gleiche gilt, wenn er diese Aufgaben teilweise oder ganz einem Textildienstleister überlässt. Entscheidende Voraussetzung: Es muss sich um klassische Berufsbekleidung handeln. Das sind für das Finanzamt Kleidungsstücke, die die Berufsbeziehung der Kleidung äußerlich sichtbar zum Ausdruck kommen lassen.

www.mewa.de ■



Warnschutzkollektion in neuer Farbe ▲

Gute Sichtbarkeit bei Tag und Nacht gewährleistet Kübler Reflectiq mit der Kombination aus segmentierten und durchgehenden Reflexstreifen und deren Anordnung im Body-Language-Design. Darüber hinaus hat die nach EN ISO 20471 zertifizierte Warnschutzkleidung einen modernen Schnitt. Mit Warngelb-Dunkelblau als siebte Farbstellung – neben Warnorange, Warngelb, Warnrot sowie Warnorange-Moosgrün, Warngelb-Anthraxit und Warnrot-Schwarz – hat sich die

Auswahl nun noch vergrößert. Kübler entspricht damit dem Wunsch von Kommunen und Unternehmen, ihre Mitarbeiter hochwertig und passend zur Corporate Identity einzukleiden. Eine breite Modellauswahl macht die Warnschutzkleidung zur Ganzjahreskollektion. Bund- und Latzhose werden durch eine leichte Sommerhose und Shorts ergänzt. Die Auswahl an Jacken reicht von der Arbeitsjacke über Wetter-, Softshell- und Fleecejacke bis zur Weste.

www.kuebler.eu ■



Die GIT SICHERHEIT ist für mich wichtig, weil sie kompetent über die (lebens-)wichtigen Funktionen von Schutzkleidung berichtet.“



Astrid Rechel, Referentin Arbeitsgremien, Wirtschaftsverband Textil Service - WIRTEX e.V.



Luftreiniger sorgt für saubere Luft

Denios hat einen mobilen Luftreiniger entwickelt, mit dem sich Sars-CoV-2-Viren mit einer Effizienz von 99,995 % zurückhalten lassen. Das Gerät lässt sich anschlussfertig ohne Fachpersonal in Betrieb nehmen. Es eignet sich für Innenräume mit unzureichenden Lüftungsmöglichkeiten in öffentlichen sowie gewerblichen Gebäuden bzw. als Ergänzung zu bestehenden Hygienekonzepten. Der Luftreiniger ist mit einem Hochleistungsvolumenstrom von 1.180 m³/h ausgestattet und bei einem empfohlenen 10-fachen Luftwechsel pro Stunde für 120 m³ Raumvolumen (das entspricht einer Fläche von 40 m² bei einer Raumhöhe von 3 Me-



tern) geeignet. Dank dieser hohen Luftwechselrate und einer 5-stufigen Filtertechnik inkl. verbautem Hepa-Filter H14 gemäß EN 1822 werden Gerüche, Schadstoffe und Aerosole zuverlässig und sicher reduziert.

www.denios.de ■

FFP-Masken werden für Kunden eingelagert

Um im Pandemiefall sowohl den Regelbedarf der Industrie zu decken als auch dem besonderen Bedarf von Krankenhäusern und Gesundheitseinrichtungen nachkommen zu können, hat Draeger ein neues Bevorratungskonzept für FFP-Masken entwickelt. Dieses richtet sich an jeden, der im Bedarfsfall vorbereitet sein möchte – vom großen internationalen Industriekonzern oder mittelständischen Unternehmen, über das Gesundheitswesen bis hin zu Feuerwehren und Behörden. Mo-

natliche FFP2- und FFP3-Maskenkontingente können beim Medizin- und Sicherheitstechnikhersteller vorbestellt werden. Diese können dann abhängig vom Bestelldatum voraussichtlich ab dem zweiten Quartal 2021 zur Verfügung gestellt werden. Die FFP-Masken werden in den Fertigungen in Frankreich, Schweden oder Großbritannien produziert und anschließend in einem deutschen Lager bereitgestellt.

www.draeger.com ■

Footwear-Kollektion für Herbst & Winter

Helly Hansen hat die Footwear-Kollektion für Herbst/Winter ausgeweitet und kommt mit einem Upgrade der Chelsea-Evolution-Linie. Der Chelsea Evolution Boa Wide Mid erhielt mit dem Boa-Fit-System ein Upgrade, das einen guten Sitz und Funktionalität bietet. Die wasserfeste und atmungsaktive Helly-Tech-Performance-Membran, eine Schuhkappe aus leichtgewichtigen Material sowie eine nicht durchdringbare Zwischensohle, runden das Design des Schuhs ab. Die Magni Winter Sock bietet maximalen Schutz mit einer nylon-geschützten Ferse, einem Nanoglide geschützten Fersen- und Zehenbereich und Primaloft-Fasern. Die Chelsea Evolution Winter Sock vereint das Design der Kollektion mit Lifa-Fasern im Fersen- und Ze-



Chelsea Evolution Boa Wide Mid von Helly Hansen

henbereich und Mesh-Belüftung für mehr Atmungsfähigkeit. Das letzte Modell der Wintersocken ist die Oxford Winter Sock, die sich durch ein wärmendes Vollfrottee am Bein und durch Polyamidfasern an der Ferse und an den Zehen für eine höhere Beständigkeit auszeichnet.

www.hhworkwear.com ■

In jeder Ausgabe erklären Sicherheitsexperten Begriffe, Methoden und Technologien.

WAS IST EIGENTLICH...

... EIN INNOVATIVER SICHERHEITSSCHUH?



VON ANDREAS HIMMELREICH

IN DIESER AUSGABE UNTERSTÜTZT VON DER HAIX GMBH

ANZEIGE

Die zentrale Funktion von Sicherheitsschuhen besteht natürlich darin, die Füße des Trägers vor Verletzungen zu schützen. Doch wo genau setzt dieser Schutz an? Quetschungen oder Schnitte sind sicherlich die bekanntesten Risiken in rauen Arbeitsumgebungen vor denen Sicherheitsschuhe zuverlässig schützen sollen. Doch ein innovativer Sicherheitsschuh, geht noch einen „ganzen Schritt weiter“.

Komfort und Gesundheitsaspekte spielen heute eine genauso wichtige Rolle wie der bloße Safety-Aspekt. Dabei gehen Sicherheit und Tragekomfort bei genauer Betrachtung Hand in Hand. Schließlich verbringen hunderttausende von Beschäftigten täglich ihren Arbeitstag auf den Beinen. Sie gehen viele Kilometer oder stehen sich die Beine in den Bauch – und klagen häufig über

Schmerzen in Füßen, Beinen und Rücken, was die Leistungsfähigkeit und das Wohlbefinden erheblich einschränkt. Dabei spielen insbesondere die sogenannten Faszien eine zentrale Rolle.

Faszientraining im Schuh

Faszien sind ein Bindegewebe, das Muskeln, Organe sowie Knochen umhüllt und dem Körper seine Form gibt. Ohne die Faszien würden Muskeln kaum Spannung besitzen. Außerdem haben die Faszien großen Anteil an den Bewegungen, indem sie Bewegungsenergie speichern und wieder entladen. Werden die Faszien jedoch geschädigt, kann das unangenehme Folgen haben. Sie können z. B. durch mangelnde Bewegung oder falsche Belastung verkleben, was häufig zu Verspannungen und Schmerzen führt. Das gilt natürlich auch für die Füße.

Hier setzt Connexis Safety von Haix an. Durch den Schuh verläuft ein speziell entwickeltes Tape, das die Fußwurzel umfasst und Druck auf die verschiedenen Muskel-Faszienzüge ausübt, die hier zusammentreffen. So werden über die gesamte Tragezeit hinweg die Faszien leicht stimuliert. Wie im Sport auf einer Faszienrolle werden dabei verklebte

Faszien gelöst, spannungsbedingte Schmerzen gelindert und die Muskulatur stimuliert.

Zusätzlich zum Faszien-Tape hat Haix einen neuen Leisten entwickelt. Im Gegensatz zu herkömmlichen Sicherheitsschuhen ist der Leisten bei Connexis Safety nicht nach unten gebogen, sondern gerade. Dadurch hängt der Fußballen nicht durch und die Zehen haben mehr Platz, um dem Fuß Stabilität zu geben. Ein sicherer Stand bei weniger Energieverbrauch ist die Folge. Beide Entwicklungen dienen also dazu negative Auswirkungen auf den Bewegungsapparat zu reduzieren, die Leistungsfähigkeit des Schuhträgers zu erhalten und dabei zugleich ein neues Maß an Tragekomfort und Wohlbefinden zu schaffen.

Connexis Safety ist als S1-, S1P- und S3-Sicherheitsschuh erhältlich und wurde speziell für den Einsatz im Innenbereich entwickelt. Er eignet sich für alle, die im Job viel auf den Beinen sind, z. B. in Produktion und Lagerlogistik, in vielen Handwerksberufen oder im Lebensmitteleinzelhandel. ■



Der Connexis Safety zeichnet sich zusätzlich durch sein ansprechendes Design aus

Kontakt

Haix Schuhe Produktions & Vertriebs GmbH
Mainburg
Tel.: +49 8751 8625 0
info@haix.com
www.haix.com

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 Privat-anwendern 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.

Ihr Eintrag in der Rubrik



Schicken Sie einfach eine E-Mail an miryam.reubold@wiley.com
Wir beraten Sie gerne!

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
Höfgeshofweg 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



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

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



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.

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, Komplettelösungen für Industrie, Handel, Finanzdienstleister, Behörden und Tankstellen

GEBÄUDE SICHERHEIT

Gebäudesicherheit



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



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

Gebäudesicherheit



Dictator Technik GmbH
Gutenbergstr. 9 · 86356 Neusäß
Tel. 0821/24673-0 · Fax +49 2232 704-375
info@dictator.de · www.dictator.de
Antriebstechnik, Sicherheitstechnik, Tür- und Tor-technik

Gebäudesicherheit



DOM Sicherheitstechnik GmbH & Co. KG
Wesseling 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



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
Schnelllaufstore, Rollstore, Falttore, Industrietore, Hallentore, Sicherheitstore.

Gebäudesicherheit



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

Gebäudesicherheit



SimonsVoss Technologies GmbH
Feringastr. 4 · 85774 Unterföhring
Tel. 089 992280
marketing-simonsvoss@allegion.com
www.simons-voss.com
Digitale Schließanlagen mit Zutrittskontrolle, kabellose und bohrungsfreie Montage, batteriebetrieben, keine Probleme bei Schlüsselverlust.
Digital Schließen ist neu für Sie? Rufen Sie an: 089 99228-555

Ihr Eintrag in der Rubrik



Schicken Sie einfach eine E-Mail
an miryam.reubold@wiley.com
Wir beraten Sie gerne!

Gebäudesicherheit



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

Gebäudesicherheit



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

Gebäudesicherheit



Walter Wurster GmbH
Heckenrosenstr. 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 beschuss-hemmend bis FB7, Durchreichen für Geld, Wertsachen und Dokumente, Hochsicherheits-Durchreichen, Bankschalter, Nachtschalter, Tankstellenschalter, Apothekenschalter, Ticketschalter für Sport- und Kulturstätten

PERIMETER SCHUTZ

Perimeterschutz



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, Drehflügelstore, Zaun-, Zugangs- und Detektionssysteme haben Sie mit INOVA auf alle Fragen des Perimeterschutzes die passende Antwort.

Perimeterschutz



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 Videoanalyseysteme, Zutrittskontrolle

VIDEO ÜBERWACHUNG

Videoüberwachung



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



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



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 Privat- anwendern spezialisiert.

Videoüberwachung



Axis Communications GmbH
 Adalperstraße 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



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



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



VIDEO SECURITY & NETWORK GMBH

Ihr zuverlässiger Partner für professionelle Videoüberwachung

DEKOM Video Security & Network GmbH
 Hohlfluchtchausee 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



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



EIZO Europe GmbH
 Belgrader Straße 2
 41069 Mönchengladbach
 Tel.: +49 2161 8210 0
 info@eizo.de · www.eizo.de
 Professionelle Monitore für den 24/7-Einsatz in der Videoüberwachung, IP-Decoder-Monitore für den computerlosen Anschluss an IP-Kameras.

Videoüberwachung



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

Hanwha Techwin Europe Limited
 Kölner Strasse 10
 65760 Eschborn
 Tel: +49 (0)6196 7700 490
 hte.dach@hanwha.com · www.hanwha-security.eu/de
 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



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



www.luna-hd.de

Videoüberwachung



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



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-Angriffen im Einklang mit DSGVO, VMS: Video Insight

Videoüberwachung



Santec BW AG
 Womgermühle 1, 58540 Meinerzhagen
 Tel. +49 2358/905 450 · Fax +49 2358/905 499
 santec_info@burg.biz · www.santec-video.com
 Videoüberwachung · Netzwerktechnik
 IR-Freilandsensoren · Dienstleistungen

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.

Videoüberwachung



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



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



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



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
ZEUS® Workforce Management von ISGUS: Zeiterfassung, Personaleinsatzplanung, Betriebsdatenerfassung, Zutrittskontrolle

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



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

Ihr Eintrag in der Rubrik



Schicken Sie einfach eine E-Mail
an miryam.reubold@wiley.com
Wir beraten Sie gerne!

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

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



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.

Zeit + Zutritt



FEIG ELECTRONIC GMBH
Lange Straße 4 · 35781 Weilburg
Tel. 06471/3109-0 · Fax 06471/3109-99
sales@feig.de · www.feig.de
RFID-Leser (LF, HF, UHF) für Zutritts- und Zufahrtskontrolle, Geländeabsicherung, Bezahlsysteme u.v.m.

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

Notruf- und Service-Leitstelle



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

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



phg
Peter Hengstler GmbH + Co. KG
D-78652 Deißlingen · Tel. +49(0)7420/89-0
datentechnik@phg.de · www.phg.de
RFID und Mobile Access: Leser für Zutrittskontrolle, Zeiterfassung, BDE, Türkommunikation, Besuchermanagement, Parksysteme, Zufahrtskontrolle, Vending, ... Terminals, Einbaumodule, Kartenspende, Tischlesegeräte, Leser für Markenschalterprogramme, Modbus-Module, Identifikationsmedien, ... einfach und komfortabel zu integrieren.

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.

BRANDSCHUTZ

Brandschutz



DENIOS AG
Dehmer Straße 58-66
32549 Bad Oeynhausen
Fachberatung: 0800 753-000-2
Gefahrstoffflagersysteme, Gefahrstoffmanagement, Raumsysteme, Thermotechnik, Auffangwannen, Arbeitsschutz, Industriebedarf, Gefahrstoff Leakage-Warnsystem

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 Vertriebs GmbH
Brühlmatten 9 · 79295 Sulzburg
Tel. 07634/500-0 · Fax 07634/6419
info@hekatron.de · www.hekatron.de
Brandmeldesysteme, Rauchschaltanlagen, Rauchwärmelder, 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, Löscheinrichtungen und Notbeleuchtung

Brandschutz



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

Brandschutz



Securitas Electronic Security Deutschland GmbH
SeTec Sicherheitstechnik
Hauptstr. 40 a · 82229 Seefeld
Tel. +49(0)8152/9913-0 · Fax +49(0)8152/9913-20
info@setec-gmbh.net · www.setec-gmbh.net
Handfeuermelder, Lineare Wärmemelder, Feuerwehrlösungen, Schlüsseldepos, Feuerwehrlösungen, Schlüsselmanager, Feuerwehrlösungen, Feststellanlagen, Störmeldezentralen

Brandschutz

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

Brandschutz

ARBEITSSICHERHEIT

Arbeitssicherheit



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.

MASCHINENANLAGENSICHERHEIT

Maschinen + Anlagen



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



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 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 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

Maschinen + Anlagen



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, Zustimmungstaster uvm.

GEFAHRSTOFF MANAGEMENT

Gefahrstoffmanagement



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 Umluft-
schränke, Druckgasflaschenschränke, Gefahrstoffar-
beitsplätze, Absauganlagen, Raumluftreiniger uvm.

Gefahrstoffmanagement



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

Gefahrstoffmanagement



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, Brand-
schutz- Schränke + Container, Gasflaschenlagerung

UNTER BRECHUNGSFREIE STROMVERSORGUNG

Unterbrechungsfreie Stromversorgung



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 hoch-
wertige Produkte für Videoüberwachungssysteme im
Außenbereich. Mikroklima-Komponenten für Außengehäuse:
Heizgerät, Kühlen, Thermostate. Industrielle PoE-Switches,
Ethernet-Extenders und Überspannungsschutzgeräte.

Unterbrechungsfreie Stromversorgung



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.

DIE VIP COUCH



© VDSI

Prof. Dr. Arno Weber

Professor für Arbeits- und Gesundheitsschutz an der Hochschule Furtwangen & Vorstandsvorsitzender des VDSI – Verband für Sicherheit, Gesundheit und Umweltschutz bei der Arbeit e.V.

- Jahrgang 1965
- 1984-1994 Studium der Chemie (Diplom + Promotion) an der Universität Erlangen-Nürnberg
- 1995-1996 Weiterbildung zum „Europäischen Sicherheits- und Qualitätsmanager“ in Saarbrücken
- Seit 1995 diverse Lehraufträge an verschiedenen Hochschulen
- Seit 2004 Mitglied des geschäftsführenden Vorstands des VDSI, seit 2019 Vorsitzender
- 2014 Berufung an die Hochschule Furtwangen für den Studiengang Security & Safety Engineering
- 2019 stellvertretendes Mitglied im Ausschuss für Betriebssicherheit

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:

Chemiker – das habe ich zu dem Zeitpunkt auch schon studiert.

Was hat Sie dazu bewogen, eine Aufgabe im Bereich Sicherheit zu übernehmen?

Während der Promotion kam mein damaliger Doktorvater auf mich zu, ob ich mich nicht um die Umsetzung der Gefahrstoffverordnung an unserem Institut kümmern könnte. Arbeitsschutzvorschriften waren damals für Universitäten noch weitgehend Neuland. Ich fand damals die Kombination aus Chemie und (Labor-)Sicherheit ein unwahrscheinlich spannendes Feld, bei dem man auch etwas „Gutes“ für die Beteiligten tun konnte. Deshalb habe ich meine Weiterbildung entsprechend ausgerichtet.

Welche sicherheitspolitische Entscheidung oder welches Projekt sollte Ihrer Meinung nach schon längst umgesetzt sein?

Führungskräfte und Unternehmer sollten auf verschiedenen Ebenen noch besser geschult und sensibilisiert werden. Es muss ein größeres Bewusstsein dafür geschaffen werden, dass sie die Verantwortung für Mitarbeiter tragen und Fachexperten, wie z. B. Fachkräfte für Arbeitssicherheit, ihnen dabei zur Seite stehen.

Ein Erfolg, den Sie kürzlich errungen haben, war:

Ich bin seit März letzten Jahres in den hochschulinternen Corona-Leitungstab mit eingebunden. Ich glaube, was wir dort gemeinschaftlich und interdisziplinär erarbeitet und geleistet haben, kann sich durchaus sehen lassen. Meine Bewunderung gilt hier unserem Rektor und unserer Kanzlerin, die beide sehr offen für die Anregungen und Vorschläge des gesamten Stabs waren. Ich betrachte daher nicht nur die Ergebnisse als Erfolg, sondern auch die Art des miteinander Zusammenwirkens.

Welche Reform bewundern Sie am meisten?

Die Einführung der Sozialversicherung im Allgemeinen und der gesetzlichen Unfall-

versicherung mit der Haftungsablösung ist sicher eine der größten und weitsichtigsten Errungenschaften, die es bei uns gesamtgesellschaftlich gab. Ich glaube, dass sich viele Unternehmer und auch Versicherte gar nicht mehr bewusst sind, in welchem Luxus wir hier leben.

Worüber können Sie sich freuen?

Dass ich jetzt gleich mit meiner Lebenspartnerin einen schönen Schneespaziergang machen werde.

Wobei entspannen Sie?

Beim Wandern, Spazieren, Zeitunglesen und manchmal auch mit der Modellbahn.

Welchen Urlaubsort können Sie empfehlen?

Das könnte ich ja jetzt für mich behalten, sonst ist es mit der Ruhe vorbei ... aber Spaß beiseite: Das Allgäu ist traumhaft schön, insbesondere die Ecke um den Grünen.

Welche Zeitschriften lesen Sie regelmäßig?

GIT SICHERHEIT, Sicherheitsingenieur, Sicher ist Sicher, VDSI aktuell, Zeitschriften der Unfallversicherungsträger, Nachrichten aus der Chemie, Süddeutsche Zeitung, Märklin Magazin, ... (bestimmt habe ich jetzt was vergessen)

Welches Buch haben Sie zuletzt gelesen?

Beruflich: die neuen Veröffentlichungen und Urteilsbesprechungen von Thomas Wilrich rund um das Thema Arbeitsschutzverantwortung.
Privat, bitte nicht lachen: „Latte Igel und der Wasserstein“ (ist eigentlich ein Buch aus meiner Kindheit)

Die beste Erfindung im Bereich Sicherheit ist Ihrer Meinung nach:

Die Erkenntnis, dass man aktiv etwas gegen Unfälle und arbeitsbedingte Erkrankungen tun und darüber hinaus auch immer besser werden kann.

Ihre gegenwärtige Geistesverfassung ist: Hoffnungsvoll.

Wiley Industry Days

WIN DAYS

7-9 June 2021

www.WileyIndustryDays.com



**JETZT KOSTENFREI
ALS BESUCHER
REGISTRIEREN
REGISTER NOW
FOR FREE VISIT**

Virtuelle Show mit Konferenz, Ausstellung und Networking für Automatisierung, Machine Vision, Photonics, Healthcare und Sicherheit.

Virtual show with conference, exhibition and networking for automation, machine vision, photonics, healthcare and safety & security.

Standbuchungen:



Jörg Wüllner
Tel.: +49 6201 606 749
joerg.wuellner@wiley.com



Miryam Reubold
Tel. +49 6201 606 127
miryam.reubold@wiley.com



Dr. Michael Leising
Tel. +49 3603 89 42 800
leising@leising-marketing.de



Anne Anders
Tel. +49 6201 606 552
aanders@wiley.com



Mehtap Yildiz
Tel. +49 6201 606 225
myildiz@wiley.com



Martin Fettig
Tel. +49 721 145080 44
m.fettig@dasmedienquartier.de



Manfred Böhler
Tel. +49 6201 606 705
mboehler@wiley.com



Claudia Müssigbrodt
Tel. +49 89 43749678
claudia.muessigbrodt@tonline.de



Dr. Timo Gimbel
Tel. +49 6201 606 049
timo.gimbel@wiley.com



Asi-5

**AUTOMATISIERUNG
NEU GEDACHT.**

**IHR WEG IN
DIE DIGITALE
ZUKUNFT.**



Automatisierungstreff
IT & AUTOMATION 2021
27. - 29. April 2021 | Kongresshalle Boblingen



IO-Link

**Bihl
+ Wiedemann**

www.bihl-wiedemann.de