EURO SECURITY

Das deutsche Fachmagazin für Sicherheit und Management in der DACH Region

- **Altenpflege**
  Über 21.000 Besucher! Leitmesse der Pflegebranche voller Erfolg
- **Anti-Terror**
  Hochsicherheitspoller: Sicherheit für Croisette und Strand in Cannes
- **IT-Sicherheit**
  Unternehmen wollen digitale Souveränität; Auch Politik ist gefragt

ISSN 09481249 • 4-2023 • ZKZ 16724 Postvertriebsstück bezahlt • 80383 BAY Germany ©SEC Global • euro-security.de

Inhalt

Inhalt

Titelbild: Pariser Zentrale von Canal+ nutzt 'Vernetzte Sicherheit'

Zutrittskontrolle für eine neue Pariser Medienzentrale nutzt eine Reihe von vernetzten ASSA ABLOY-Geräten: Für den neuen Hauptsitz in einem Pariser Vorort hat der Medienkonzern Canal+ ein vernetztes, intelligentes Gebäude gewählt, um effizientes und flexibles Arbeiten zu ermöglichen. Die Auswahl der richtigen vernetzbaren Zugangstechnologien kann eine zeitraubende Aufgabe sein, die allzu oft Kompro- misse im Namen der Kompatibilität erfordert.

>> www.assaabloy.com

Impressum *ISSN 09481249*

Redaktion *Euro Security Fachmedien; Dr Claudia Mrozek; 83083 Riedering, Tel: +49 (0)8036 3035071; Email: redaktion@euro-security.de*
Redaktionsteam *Dr. Claudia Mrozek (presserechtlich verantwortlich), Caroline Best, Angela Kloose, Dirk Lehmanski, Maria Lehmen, Anne Schneider, Heiko Scholz, Patricia Ovo, Markus Steben, Cathy Thomens, Sophie Mrozek, Alexander Mrozek, Mariam Nassreddin;*
Aboverkauf *DCMN Marketing Agentur, Email: abo@sec-global.org*
Anzeigenverwaltung/-vertretung *DCMN Marketing Agentur Oberbayern; Bestellungen und Druckvorlagen: anzeigen@euro-security.de*

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

Editorial

Data Privacy versus physkalischer Sicherheit?

Wenn man die aktuellen Entwicklungen bei Datenschutzregelungen betrachtet, erfüllen leider viele Sicherheitssysteme kaum die von Experten erarbeiteten Datenschutzanforderungen. Aber auch wenn Unternehmen sich im Datenschutzbereich über Bedrohungslage und Schwachstellen bewusst sind, sieht es bei Implementierung eines physischen Sicherheitssystem oft kritisch aus. Denn leider wird Datenschutz nicht von Anfang an integriert. Und im Bereich ‚Öffentliche Sicherheit' ergeben sich zudem besondere Anforderungen an den Schutz der Privatsphäre in überwachten Umgebungen. Dabei hat das Recht auf Privatsphäre einen wichtigen, immanenten Platz in Sicherheits- und Gesellschaftsmodellen.

Für ein hohes Maß an Sicherheit stellt Genetec in einem Whitepaper das Modell des ‚Privacy by Design' vor und zeigt Möglichkeiten auf, wie durch eine Wahrung der Privatsphäre in einem Sicherheitsbiotop - wie in einem Unternehmen - die Akzeptanz von not- wendigen Datenschutzrichtlinien und ggf. die Abgabe von persönlichen Daten, die für eine effiziente Sicherheitslösung hilfreich sind, durch Kunden / Mitarbeiter erfolgen kann. Genetec zeigt Bewertungskriterien einer aktuellen physischen Sicherheitsinfrastruktur auf und stellt Tools dar, die das Recht auf Privatsphäre trotz effizienter Sicherheitslösungen unterstützen.

Unter **https://tinyurl.com/355xddac** können Interessierte das Whitepaper herunterladen.

Dr Claudia Mrozek

Pariser Zentrale von Canal+ nutzt ‘Vernetzte Sicherheit’

Zutrittskontrolle für eine neue Pariser Medienzentrale nutzt eine Reihe von vernetzten ASSA ABLOY-Geräten: Für seinen neuen Hauptsitz in einem Pariser Vorort hat der Medienkonzern Canal+ ein vernetztes, intelligentes Gebäude gewählt, um effizientes und flexibles Arbeiten zu ermöglichen. Die Auswahl der richtigen vernetzbaren Zugangstechnologien kann eine zeitraubende Aufgabe sein, die allzu oft Kompromisse im Namen der Kompatibilität erfordert.

"Die schnell wachsende Nachfrage nach integrierten Gebäudesystemen macht es für Beschlaglieferanten unerlässlich, eine Reihe kompatibler Zutrittslösungen anzubieten", sagt Thomas Schulz, Product Marketing Director bei ASSA ABLOY Opening Solutions EMEIA.
"Die umfassende Kompetenz von ASSA ABLOY und die große Auswahl an anschlussfähigen Zutrittskontrolllösungen ermöglicht es uns, Geräte für viele Anwendungen, für fast jede Öffnung und für alle Bereiche eines Gebäudes zu finden."
Die neue Zutrittskontrolllösung für das Canal+-Gebäude filtert den Zugang zu und den Durchgang durch alle technischen Bereiche für 1.200 Mitarbeiter sowie Besucher und Auftragnehmer. Ein kompromissloser Schutz ist für mehrere Türtypen erforderlich, sowohl für interne Öffnungen als auch für externe oder Notausgänge.

Canal+ entschied sich für Zugangskontrollsysteme, die sowohl in Bezug auf die Sicherheit als auch auf Nachhaltigkeitskriterien eine hohe Leistung bieten. Besonderes Augenmerk wurde auf die Begrünung der Innen- und Außenbereiche sowie auf die Luftqualität in den Innenräumen und die Belichtung mit natürlichem Licht gelegt, um den Energieverbrauch des Gebäudes zu senken.

"Sobald wir über Zutrittssysteme sprechen, erzählen mir alle Dienstleister von ASSA ABLOY-Produkten", sagt Abdeljelil Saidi, Direktor für Sicherheit bei Vivendi/Canal+ Group.

Nahtlose Integration mit Genetec Synergis

Alle bei Canal+ installierten ASSA ABLOY-Geräte lassen sich nahtlos in die Genetec-Plattform integrieren. Diese Integration bietet den Mitarbeitern die Flexibilität und den Komfort eines einzigen Ausweises für mehrere Standorte. Über ein integriertes Genetec-Kontrollpanel können Administratoren den Zugang für einzelne Benutzer oder Räume erteilen, ändern oder entziehen.

Aperio- und ABLOY-Schlösser sind mit dem intelligenten Gebäudesystem verbunden, um unbefugtes Eindringen in sensible Bereiche zu verhindern.

Die Wahl des Aperio H100 Wireless Electronic Handle gegenüber kabelgebundenen Schlössern trug zur Verbesserung der Energieeffizienz bei. Wie jedes Aperio-Schloss wird auch das H100 ohne Verkabelung eingebaut, was bei der Installation Strom spart.
Der elektronische Griff funktioniert ohne Netzstrom und verbraucht viel weniger Energie als ein herkömmliches verkabeltes Türschloss.
Canal+ ist sehr zufrieden mit der Leistung der kombinierten Lösung von Genetec und ASSA ABLOY: "Wir planen, nicht nur den Hauptsitz von Canal+, sondern auch neue Standorte der Vivendi-Gruppe damit auszustatten", fügt M. Saidi hinzu.

Das richtige Gerät für jede Tür, innen und außen

Zur Sicherung von Innentüren kombiniert der mehrfach ausgezeichnete Aperio H100 Wireless Handle Sicherheit mit moderner Ästhetik. Sein robustes Design eignet sich perfekt für Türen mit hohem Publikumsverkehr; der H100 funktioniert mit Online- oder Offline-Zutrittskontrollsystemen. Die Batterie ist im Inneren des Griffs untergebracht, so dass nur ein minimaler, unauffälliger Platzbedarf entsteht.
Für ein noch höheres Maß an Sicherheit an Außentüren sind die elektromechanischen ABLOY-Schlösser auch vollständig in das Genetec-System des Gebäudes integriert. Diese in ihrer Klasse führenden Türvorrichtungen bieten einen hohen mechanischen Widerstand an gefährdeten Stellen wie Notausgängen. "Die elektromechanischen Schlösser von Abloy sind robust und effizient", bestätigt M. Saidi.

Mit drei Maßnahmen zum optimierten Rettungseinsatz

Einsatzkräfte müssen im Rettungswesen schnelle und richtige Entscheidungen treffen: bei der Sichtung in der Chaosphase, bei der Patientenversorgung und bei der Transportorganisation. VOMATEC, spezialisierter Anbieter für digitales Gefahrenmanagement und Leitstellentechnologie, nennt drei Ansatzpunkte für die Optimierung von Rettungseinsätzen. Im Rettungswesen zählt jede Sekunde, sei es bei Naturkatastrophen wie Erdbeben und Überschwemmungen oder bei Bränden und Unfällen. Die entscheidende Unterstützung für ein effizientes Rettungswesen bietet eine umfassende Digitalisierung. Sie beseitigt manuelle Arbeitsabläufe, automatisiert Prozesse und vernetzt Daten.

VOMATEC sieht dabei drei Kernmaßnahmen, die das Rettungswesen auf ein neues Level heben können:

1. Die Datenvernetzung

Vielfach nutzen Leitstellen und Einsatzkräfte vor Ort unterschiedliche Systeme. Die Verknüpfung dieser Systeme mit einer Weiterleitung relevanter Daten kann zu einer deutlichen Prozessoptimierung im Rettungswesen führen, etwa hinsichtlich einer verbesserten Koordination unterschiedlicher Hilfsorganisationen. Voraussetzung dafür ist die Digitalisierung der Infrastruktur mit der Vernetzung der Datenlandschaft und der Beseitigung von Medienbrüchen. Dadurch können Verantwortliche bei Vorfällen verschiedenster Art sehr schnell situationsgerechte Entscheidungen auf Basis aktueller Informationen treffen. Wichtig ist dabei, dass die Digitalisierung auch eine Automatisierung beinhaltet, das heißt zum Beispiel, dass vor Ort erhobene Daten automatisch in strukturierter Form weitergeleitet werden.

2. Die Eliminierung manueller Prozesse

Manuelle Prozesse gehen in Krisensituationen zulasten der Geschwindigkeit. Außerdem sind sie anfällig für menschliche Fehler. Solche Prozesse sollten weitestgehend eliminiert werden. Gerade mündliche Datenweitergaben oder papierbasierte Verfahren sind oft ein Grund für verzögerte Rettungsmaßnahmen. So statten Rettungskräfte Unfallopfer in der Regel mit Patientenanhängekarten oder Armbändern aus. Eine schnelle Kategorisierung und Priorisierung von Verletzten mit einer zielgerichteten Verteilung von Personen nach Verletzungsmustern auf bestimmte Kliniken wird damit erschwert. Als Alternative hierzu bieten sich digitale Lösungen in Form von vernetzten IoT-Geräten an, die Rettungskräfte Unfallopfern umhängen. Dadurch ist eine effiziente, reibungslose und automatische Weiterleitung von Informationen über einen Patienten – zum Beispiel hinsichtlich Triage, medizinischer Erstversorgung oder Verdachtsdiagnose – an Einsatzkräfte oder die Einsatzleitung möglich.

3. Die Nutzung von ausfallsicheren Systemen

Die Digitalisierung, Automatisierung und Vernetzung sind wichtige Maßnahmen für die Effizienzverbesserung im Rettungswesen. Dabei darf ein Aspekt aber nicht vergessen werden: Die genutzten Systeme müssen robust und vor allem ausfallsicher sein. Bei Vor-Ort-Einsätzen ist folglich die eventuell unzureichende Mobilfunkabdeckung zu beachten. Idealerweise unterstützen digitale Systeme deshalb verschiedene Übertragungskanäle, nach Möglichkeit auch eine autarke Kommunikation. Ein Beispiel hierfür wären Einsatzfahrzeuge, auf denen die notwendige Hardware für eine von Online-Services unabhängige Informationsübertragung installiert ist.

„Bei der Optimierung des Rettungswesens und der kommunalen Gefahrenabwehr wird, wie in anderen Bereichen auch, an der zunehmenden Digitalisierung und Vernetzung kein Weg vorbeiführen", erklärt Dr. Stephan Heuer, Geschäftsführer bei VOMATEC.

„Hierbei müssen allerdings noch einige Hindernisse überwunden werden, etwa hinsichtlich technischer Fragestellungen wie der Schnittstellenproblematik oder der heterogenen Strukturen im föderalen System in Deutschland. Durch die verschiedenen Naturkatastrophen der jüngsten Vergangenheit sind diese Themen aber auch auf die politische Agenda gerückt. Wir sollten folglich optimistisch in die Zukunft des Rettungswesens blicken können."

Sicherheit für Croisette und Strand in Cannes

Das italienische Unternehmen hat Hochsicherheits-Poller der Serie ONE EVO und feststehende Poller G6 EVO für die Zufahrten zur Croisette und für den Strandbereich von Boccacabana geliefert. Unter dem Motto Smart&Safe City stellt CAME den Schutz städtischer Umwelt und Personen in den Mittelpunkt der strategischen Vision des Unternehmens.

Cannes, eine äußerst faszinierende und renommierte Stadt, weltweit bekannt für das Film Festival und für die Promenade der la Croisette, hat CAME, führender Lieferant von integrierten technischen Lösungen für Wohnbereiche, Unternehmen sowie Städte und Kommunen, beauftragt, um die wichtigsten Zugangswege zur Croisette abzusichern. Diese bilden das sogenannte „Gold-Viereck" – die Croisette-Serbes, die Croisette-Cdt André, die Barrière Mace-Croisette - und die Boccacabana-Seeküste. Zur Entwicklung dieses wichtigen Projekts griff CAME auf die Erfahrung und das Know-how von CAME Urbaco zurück, einer Marke der Unternehmensgruppe. Diese ist spezialisiert auf die Planung und Produktion von technologischen Lösungen für die Zufahrtskontrolle und Absicherung in urbanen Bereichen und für den Schutz von sensiblen

Arealen, in denen die Sicherheit von Gebäuden und Menschen entscheidend ist. Das durch CAME entwickelte Projekt sichert die Fußgängerzonen und gewährleistet die Steuerung des Durchfahrtsflusses der Fahrzeuge in das „Goldenen-Viereck" zur Croisette im Laufe von Veranstaltungen. Die Zone wurde mit Hochsicherheits-Pollern der Serie ONE EVOausgerüstet, die in der Lage sind, Rammfahrzeugen zu widerstehen und den jüngsten internationalen Vorschriften entsprechen.
Zudem wurden eine Reihe feststehender Poller G6 EVO verbaut. Alle durch die versenkbaren Poller gesicherten Zugänge sind an die Software SYGMA 3 angeschlossen, einem Zufahrtskontrollsystem, das die allgemeine Verwaltung und Steuerung aller ange- schlossenen Geräte ermöglicht.
SYGMA 3 ist mit dem zentralisierten Technischen Management-System verbunden, das eine Übersicht der kontrollierten Bereiche bietet und das mit der lokalen Polizeidienststelle verbunden ist.

Mace-Croisette

Der Zufahrtspunkt zum Macé-Strand, nahe dem Festival-Palast, wurde mit 6 versenkbaren Hochsicherheits-Pollern ONE50 EVO gesichert, die eine kontrollierte Ein- und Ausfahrt ermöglichen. Zudem wurden 2 feststehende Poller ONE50 EVO installiert. Fahrzeuge erhalten Zugang über eine Gegensprechanlage, die in einer City6 EVO Standsäuleintegriert und mit der örtlichen Polizeidienststelle verbunden ist. Zudem enthält die Standsäule alle weiteren Bedienelemente, Signalanlagen und die Steuerung.
Mace-Croisette insbesondere während der Sommerzeit und während des Film Festivals im Mai ein von Touristen stark frequentierter Bereich. Daher steht Sicherheit an diesem Ort

an erster Stelle. Die größte Herausforderung bestand in der Aufgabe die Zufahrt der Fahrzeuge, die Ausrüstung im Filmpalast Be- und Entladen, zu regeln.
Das Modell ONE 50 EVO wurde entwickelt, um sensible Bereiche abzusichern und ein hohes Schutzniveau zu garantieren. Es ist in der Lage nacheinander 2 LKW von je 7,5 Tonnen bei einer Geschwindigkeit von 80 km/h aufzuhalten. Die Poller wurden mit dem Stadtwappen individualisiert und sind mit LED-Leuchtringen versehen, die sich harmonisch in die Stadtumgebung einfügen.

SICK

Prüflabor für International Data Spaces Association

Auf der Hannover Messe hat die SICK AG (SICK) und die International Data Spaces Association (IDSA) ei-nen Kooperationsvertrag zur Abwicklung von Prüf- und Testaufgaben im Rahmen der Zertifizierung von Daten-Gateways unterzeichnet. SICK wird zukünftig seine etablierte Infra- struktur für Prüf- und Testarbeiten zur Verfügung stellen, um die Sicherheit von Datenräumen zu gewährleisten.

SICK übernimmt zukünftig Prüf- und Testaufgaben, um einen vertrauensvollen Datenaustausch in Datenräumen zu gewährleisten. Darauf einigten sich heute auf der Hannover Messe Vertreter des IDSA und der SICK AG. Der Anbieter intelligenter Sensorlösungen ist das zweite Unternehmen, dass diese zertifizierten Prüf- und Testaufgaben für die IDSA weltweit anbietet.

SICK hat in den vergangenen Jahren eigene Produkte auf deren Cyber-Sicherheit getestet und sich einen umfangreichen Erfahrungsschatz aufgebaut. In Zukunft stellt das Unternehmen seine etablierte Infrastruktur für Prüf- und Testarbeiten zur Verfügung, testet auch Produkte anderer Marktteilnehmer hinsichtlich der IDSA-Zertifizierungskriterien und gibt diese für den die Nutzung in internationalen, branchenübergreifenden Datenräumen frei. Mit dieser Freigabe erhalten Unternehmen die Gewissheit, dass Daten wirklich souverän und vertrauensvoll ausgetauscht werden können.

„Den sicheren Datenaustausch über Unternehmensgrenzen hinaus zu ermöglichen, wird der digitalen Transformation in der Industrie zusätzlichen Rückenwind geben", meint Andreas Teuscher, Chief Industrial Security Officer bei der SICK AG. Wir erhoffen uns dadurch mehr Transparenz und Erkenntnisgewinn, um die Potenziale einer vernetzten Industrie nutzbar zu machen", so Teuscher weiter.

„SICK ist bereits seit langem Mitglied der IDSA. Daher freut es uns umso mehr, dass das Unternehmen nun das Ziel verfolgt, eine IDS Evaluation Facility zu werden," sagt Lars Nagel, CEO von IDSA. „Dadurch unterstreicht SICK sein außerordentliches Engagement für sichere und souveräne Data Spaces im industriellen Sektor. Es ist erfreulich zu sehen, dass immer mehr Organisationen aktive Schritte unternehmen, um sichere und transparente Daten-Sharing-Ökosysteme einzurichten."

Industrie 4.0, also die Vernetzung verschiedener Akteure für mehr Transparenz in industriellen Anwendungen, ist nur dann möglich, wenn einerseits sichere Datenräume einen vertrauensvollen Datenaustausch gewährleisten. Andererseits müssen auch die Akteure vertrauensvoll sein. Die IDSA hat ein Regelwerk entwikkelt, um diese Voraussetzungen sicherzustellen.

Dazu gehört auch die eingehende Prüfung von Gateways und anderen Produkten, um sicher zu gehen, dass sie vor Manipulation und unberechtigten Eingriffen geschützt sind. Als eines der Gründungsmitglieder des IDSA unterstützt die SICK AG nun auch deren Umsetzung.

Glutz Deutschland

Neue Geschäftsführung

Dietmar Vinke ist neuer Geschäftsführer der Glutz Deutschland GmbH. Seit Februar 2023 liegt die Gesamtverantwortung der Geschäftsführung für den deutschen Markt bei Dietmar Vinke. Er bringt profunde Erfahrung aus der Beschlags- und Baubranche mit. Bereits in der Vergangenheit hat der 48-jährige, gebürtige Bielefelder leitende Positionen, unter anderem bei der Deutsche Telekom AG und Franz Schneider Brakel GmbH & Co. KG, ausgeübt.
Glutz ist überzeugt, mit der neuen Leitung die Geschäftstätigkeit im deutschen Markt weiter auszubauen.

"Wir freuen uns, dass Dietmar Vinke unsere Kunden und Partner künftig mit dem Ziel der höchstmöglichen Zufriedenheit und Wertschätzung unterstützen wird, um damit nachhaltigen Wert und Erfolg für alle Beteiligten zu schaffen", erklärt Sascha Lauber, CSO der Glutz AG.

Dietmar Vinke folgt auf Robert Soda-Cotic, der nach drei erfolgreichen Jahren bei Glutz Deutschland GmbH, das Unternehmen auf eigenen Wunsch und aus persönlichen Gründen verlassen hat.

GISA

Vertrag von CEO Heino Feige vorzeitig bis Ende 2028 verlängert

Heino Feige bleibt bis Ende 2028 GISA-Geschäftsführer. Die Gesellschafter der GISA haben seinen Vertrag als CEO vorzeitig bis zum 31. Dezember 2028 verlängert. Feige ist seit Januar 2021 Geschäftsführer des IT-Dienstleisters.
„Mit Heino Feige als Geschäftsführer hat sich GISA in den vergangenen zwei Jahren positiv entwickelt. Das Unternehmen hat im letzten Geschäftsjahr einen Umsatz erwirtschaftet, der deutlich über dem Plan lag. Das macht uns als Hauptgesellschafter stolz", sagt Norbert Rotter, CEO der NTT DATA Business Solutions AG und Aufsichtsratsvorsitzender der GISA GmbH. „Wir sind davon überzeugt, mit unserer vorzeitigen Entscheidung die Weichen für eine erfolgreiche Zukunft gestellt zu haben."

„Heino Feige gibt sich nicht mit dem Status quo zufrieden, sondern hat als CEO wichtige Veränderungsprozesse im Unternehmen angestoßen", Sigrid Nagl, Personalvorständin des Gesellschafters envia Mitteldeutsche Energie AG. „Dazu zählen die paritätische Neuaufstellung des Managements, ein stärkerer Fokus auf nachhaltiges Agieren in allen Unternehmensbereichen sowie auf die Bedürfnisse der Mitarbeitenden."
Detlef Hillebrand, Geschäftsführer des Gesellschafters Kommunalwirtschaft Sachsen-Anhalt GmbH, ergänzt: „In der aktuellen Zeit mit vielen Einflussfaktoren braucht es für Mitarbeitende, Kunden und Partner ein Zeichen der Stabilität und Sicherheit. Mit Heino Feige ist diese Verlässlichkeit gegeben, daher sprechen wir ihm unser Vertrauen aus."
„Das ausgesprochene Vertrauen der Gesellschafter sehe ich als Ansporn, um den begonnenen Weg fortzusetzen. GISA gemeinsam mit den Mitarbeitenden in die Zukunft zu führen ist eine Aufgabe, der ich mich mit Freude annehme", kommentiert Heino Feige.

Heino Feige ist seit 2009 in verschiedenen Führungspositionen für GISA tätig. Zuvor war er für die Deutsche Telekom AG/T-Systems u. a. als General Manager im Bereich Public Sector und als Großkundenmanager im Segment Industrie beschäftigt. Neben dem Beruf engagiert er sich ehrenamtlich in regionalen und überregionalen IT-Netzwerken.

MOBOTIX

Kontinuität an der Spitze

Wiederbestellung des MOBOTIX CEO und CFO sowie Erweiterung des Vorstands um einen Chief Sales and Marketing Officer (CSMO).

Mit Wirkung vom 01. Mai 2023 bilden Thomas Lausten (CEO), Klaus Kiener (CFO) und Phil Antoniou (CSMO) zusammen mit dem kürzlich ernannten CTO, Christian Cabirol den neuen Vorstand der MOBOTIX AG. Der Vorstand wird sich, basierend auf einer beschleunigten Geschäfts- und Produktstrategie, auf die Weiterentwicklung und Innovation von MOBOTIX konzentrieren. So war bereits eine Umsatzsteigerung von 27% für das erste Halbjahr des Ende März abgeschlossenen Geschäftsjahres 2022/2023 möglich.

Thomas Lausten führt MOBOTIX auch in Zukunft

Am 20. April 2023 hat der Aufsichtsrat Thomas Lausten für weitere zwei Jahre zum Vorstandsvorsitzenden (CEO) der MOBOTIX AG bestellt. Thomas Lausten führt die MOBOTIX AG seit 15. Juni 2017 und hat die Transformation der MOBOTIX AG in den vergangenen Jahren vorangetrieben. Der Fokus lag dabei auf der Produktentwicklung und der Marktexpansion insbesondere in DACH, Europa und den USA, sowie der Stärkung der APAC-Märkte. Das Ziel für die kommenden Jahre wird es sein, vermehrt Produktinnovationen voranzutreiben und Investitionen zu tätigen, die eine stärkere globale Präsenz in ausgewählten geografischen und vertikalen Märkten sichern.

Klaus Kiener als CFO wiederbestellt

Ebenso hat der Aufsichtsrat in seiner Sitzung Klaus Kiener für weitere zwei Jahre zum Finanzvorstand (CFO) der MOBOTIX AG wiederbestellt. Klaus Kiener ist seit April 2016 für das Unternehmen tätig. Er ist zukünftig für die Bereiche Finanzen, Corporate Planning, Investor Relation, Recht/Compliance/Datenschutz, Organisation, Qualitätsmanagement, IT-Services, Logistik/Zoll verantwortlich.

Phil Antoniou Chief Sales and Marketing Officer (CSMO)

Mit Wirkung zum 1. Mai 2023 erweitert Phil Antoniou (Foto links) als viertes Mitglied den Vorstand der MOBOTIX AG in seiner neuen Position des Chief Sales and Marketing Officer (CSMO). Phil Antoniou hat in den vergangenen Jahren die EMEA-Märkte als auch APAC und zuletzt Nord- und Südamerika betreut, womit er eine breite Kenntnis über die weltweiten Kundenanforderungen besitzt und bestens mit allen Details der MOBOTIX Technologie vertraut ist.
In seiner neuen Funktion wird er sich auch auf das Unternehmensmarketing konzentrieren, um das Kundenfeedback verstärkt zu berücksichtigen und den Bekanntheitsgrad der MOBOTIX Lösungen und Produkte weiter zu steigern

Der neue Vorstand wird die technologische und vertriebliche Entwicklung von MOBOTIX, basierend auf der MOBOTIX DNA, vorantreiben. Zentrale Werte bleiben dabei die deutsche Qualität und beste Cybersicherheit. Im Zeitalter von künstlicher Intelligenz und Deep Learning bietet das Sammeln, Aggregieren und Analysieren von Daten eine Menge Wachstumschancen – und das nicht nur im Bereich der Sicherheit, sondern auch für Kundenanalysen und Produktionsprozesse, indem die Kombination von Hardware und KI-Lösungen Video- und Metadaten nicht nur aufzeichnen, sondern direkt analysieren.

PwC

Resilienz: Deutsche Unternehmen zu zögerlich

"Global Crisis and Resilience Survey 2023" sieht Lücke zwischen Bewusstsein und Umsetzung

Unternehmen versuchen sich zwar immer stärker gegen aktuelle und künftige Krisen zu wappnen, haben bei der Umsetzung von Programmen zur Resilienz aber Nachholbedarf. Zu dem Schluss kommt der "Global Crisis and Resilience Survey 2023" der Wirtschaftsprüfungs- und Beratungsgesellschaft PwC (https://pwc.de), für den weltweit über 1.800 Entscheider, darunter 132 in Deutschland, befragt worden sind

Deutsche müssen aufschließen

Laut der Umfrage ist beispielsweise das Business Continuity Management in nur 19 Prozent der deutschen Unternehmen Teil eines Resilienzprogramms. Der globale Schnitt liegt dagegen bei 40 Prozent. "Die Studie belegt, dass die Resilienz-Revolution auf globaler Ebene längst in vollem Gange ist. Für viele deutsche Unternehmen gilt es jetzt aufzuschließen", sagt Jane He, Director und Expertin für Resilienz bei PwC Deutschland.

Die Liste an Herausforderungen wird länger: In Deutschland sorgen sich Führungskräfte mit Blick auf die kommenden zwei Jahre am meisten über Cyber-Angriffe, Unterbrechungen der Lieferketten und Personalmangel. Fast zwei Drittel der Unternehmen haben als Gegenmaßnahme ein integriertes Resilienzprogramm entwickelt. Doch nur jedes fünfte davon ist bereits wirklich vollständig integriert, wie die Untersuchung ausweist.

CEOs nur halbherzig bei der Sache

Die Probleme der Widerstandsfähigkeit der Unternehmen gegen Krisen sind oft hausgemacht. In Deutschland werden laut PwC nur 22 Prozent der Programme von den CEOs unterstützt - elf Prozent weniger als im globalen Schnitt (33 Prozent). Fast jedes dritte Unternehmen hat zudem Probleme damit, ein Team mit den richtigen Fähigkeiten für den Bereich aufzubauen - nicht gut, um das Vertrauen der Stakeholder zu behalten und Wert sowie Ruf zu schützen.

Neben einem klaren Commitment der Führungsetage Zugleich für Resilienz ist die Bedeutung technologiegestützter Ansätze hervorzuheben: Fast 60 Prozent der weltweit Befragten verlassen sich bei der kurzfristigen Stärkung der Resilienz auf Technologie. Dennoch klafft laut der Studie in vielen Unternehmen eine Lücke zwischen Bewusstsein und Umsetzungsgrad.

Am stärksten sind der Befragung zufolge Unternehmen aus Technologie, Medien und Telekommunikation aufgestellt. Dort betreiben bereits 28 Prozent integrierte Resilienzprogramme. Es folgen Gesundheitswirtschaft (24 Prozent), Energie, Versorgungsunternehmen und Rohstoffwirtschaft (24 Prozent) sowie Finanzdienstleister (22 Prozent). Das Schlusslicht bilden mit 19 Prozent Regierung und öffentlicher Dienst, heißt es.

Fraunhofer AISEC

Deepfake-Total

Audio-Dateien auf Echtheit prüfen lassen

Das Fraunhofer AISEC hat »Deepfake-Total« gestartet: eine Plattform zur KI-gesteuerten Erkennung von Audio-Deepfakes. »Deepfake-Total« stellt den aktuellen Stand der automatisierten, KI-gesteuerten Audio-Deepfake-Erkennung vor und bietet Hilfestellung bei verdächtigen Audiodateien. Nutzende können einzelne Dateien und YouTube-Videos von unterschiedlichen Audio-Spoof- und Deepfake-Erkennungsmodellen auf ihre Authenzität untersuchen lassen.

[https://deepfake-total.com]

AI.BAY 2023

Manipulation und Absicherung von KI

Auf der AI.BAY – Bavarian International Conference on AI – am 23. und 24. Februar 2023 im Deutschen Museum in München sowie im virtuellen Stream informierten die Experten für Cognitive Security Technologies Dr. Nicolas Müller und Kilian Tscharke darüber, wie überzeugend sich eine Stimme mittels KI klonen lässt oder ein KI-System z. B. in einem autonomen Fahrzeug mit manipuliertem Material zu Fehlern verleitet werden kann.

Blog: Mit ‚Creation Attacks' KI-Systeme auf den Prüfstand stellen > tinyurl.com/mv4me5kz

Website zur Deepfake-Forschung: 'Mit KI-Systemen Audio- + Videomanipulationen verlässlich entlarven' > https://tinyurl.com/3tkaactj

Produktneuheiten

Teledyne FLIR

Kameras der G-Serie für die optische Bildgebung von Gasen

Sieben neue Modelle, mit denen Fachleute in der Öl-, Gas-, Fertigungs-, Stahlproduktions- und Versorgungsindustrie noch effektiver arbeiten können

Teledyne FLIR, ein Teil von Teledyne Technologies Incorporated, hat heute die neue G-Serie vorgestellt, eine Familie von Hightech-Kameras für die optische Bildgebung von Gasen (OGI) mit gekühltem Kern, mit denen Fachleute bei der Erkennung und Reparatur von Lecks (LDAR) schädliche Gasemissionen nahtlos lokalisieren und dokumentieren können. Die G-Serie wurde entwickelt, damit alltägliche Anwender in der Öl- und Gas-, Fertigungs-, Stahl- und Versorgungsindustrie mehr Zeit mit der Priorisierung von Leckreparaturen und weniger mit der Dokumentation verbringen und gleichzeitig bessere Einblicke in die Schwere der Emissionen erhalten können.

Die G-Serie umfasst sieben Kameramodelle. Alle Modelle sind mit drahtloser Konnektivität verfügbar, damit der Bediener gespeicherte Bilder und Videos automatisch hochladen und in der Software FLIR Ignite Cloud speichern kann, während er unterwegs ist. Die Kameras der G-Serie bieten eine einfache Kompatibilität mit Analysesoftware von Drittanbietern. So kann der Bediener die erfassten Inhalte zur Überprüfung an Kollegen auf der ganzen Welt drahtlos weiterleiten, damit weitere Analysen durchgeführt und die Aufnahmen verarbeitet werden können. Schnell austauschbare Objektive bieten dem Benutzer die nötige Flexibilität zur Inspektion aus verschiedenen Entfernungen. Teledyne FLIR hat die Modelle FLIR G620, Gx320 und Gx620 entwickelt, um Emissionen von Kohlenwasserstoffen, flüchtigen Gasen und anderen flüchtigen organischen Verbindungen (VOC) in der Öl- und Gasindustrie erkennen und genau quantifizieren zu können. Da die Quantifizierung jetzt in die Kamera integriert ist, ist es nicht mehr erforderlich, während der Inspektion ein zweites Begleitgerät mitzuführen. Teledyne FLIR hat außerdem die Bewertung nach ATEX, die Einhaltung der Empfindlichkeit nach OOOOa sowie einen ergonomischen, drehbaren Touchscreen hinzugefügt, damit die Fachleute ihre Arbeit sicherer und effizienter erledigen können.

Mit den Modellen G306 und G343 erhalten die Prüfer von Versorgungseinrichtungen eine überlegene Bildqualität und erweiterte Funktionen zur Erkennung von Schwefelhexafluorid bzw. Kohlendioxid zur Wartung elektrischer Geräte. Die Modelle G346 und G304 bieten eine wirksame Methode zur Erkennung von austretendem Kohlenmonoxid oder Kältemittel und von potenziellen Problemen, was die Sicherheit und Produktivität in der Anlagenumgebung erhöht.

„Die G-Serie von Teledyne FLIR bietet dem Benutzer erstmals eine unübertroffene Ergonomie bei den Modellen für Kohlenwasserstoffe mit der Quantifizierung in der Kamera, sowie nahtlose Emissionsmessungen bei der täglichen Leckerkennung und bei Reparaturen", so Craig O'Neill, Global OGI Business Development Director bei Teledyne FLIR. „Diese neuen Modelle stellen einen Durchbruch bei der OGI dar, mit modernsten Funktionen, den aktuellen Protokollen für die drahtlose Kommunikation und einem drehbaren LCD-Touchscreen, der die Effizienz für den Benutzer vor Ort maximiert."

Die G-Serie wird innerhalb des laufenden Quartals versandbereit sein.

DuPont

Kugelsichere Westen schützen noch besser

Das US-Unternehmen DuPont stellt mit "EXO" neue Kevlar-Faser vor, die noch widerstandsfähiger ist

Der US-Chemiekonzern DuPont (https://www.dupont.com) hat mit "EXO" eine neue Aramidfaser für Kleidungsstücke entwickelt, die laut eigenen Angaben die vor 50 Jahren auf den Markt gebrachte Kevlar-Faser in allen Eigenschaften übertrifft. Zum Einsatz kam die neue Hightech-Faser bei der "Best Ranger Competition 2023 (https://www.bestrangercompetition.com)", die vor wenigen Tagen im Militärstützpunkt Fort Benning zu Ende ging. 64 Teilnehmer trugen dabei Westen aus einem neuartigen Material.

Kugelsicher, feuerfest und flexibel

Kevlar wird unter anderem zur Herstellung von Schutzkleidung genutzt, die kugelsicher, feuerfest und flexibel ist. Ob Polizisten, Soldaten, private Sicherheitsdienste, Strafvollzugsbeamte oder Notfallhelfer: Sie alle tragen, wenn sie sich in Gefahr begeben müssen, derartige Westen. EXO absorbiert die Energie, wie sie etwa durch eine Pistolenkugel eingebracht wird, besser als das ursprüngliche Material, heißt es. Gleichzeitig passen sich Exo-Westen perfekt an den Körper an, weil sie deutlich flexibler sind. Das sorgt für mehr Beweglichkeit beim Träger und höheren Komfort, so DuPont.

Die Faser schmilzt erst bei einer Temperatur von mehr als 500 Grad Celsius und lässt sich nicht entflammen.

Zudem altert sie nicht. DuPont verspricht, dass sie nach fünfjährigem Gebrauch noch genauso viel Schutz bietet wie am ersten Tag. "Wir haben über ein Jahrzehnt damit verbracht, Kevlar EXO zu entwickeln, zu verfeinern und zu perfektionieren", sagt Steven LaGanke, Global Business Leader bei DuPont Life Protection, und ergänzt: "Das Ergebnis ist eine branchenverändernde Plattform, die die Schutzwirkung auf ein ganz neues Niveau katapultiert hat."

Kevlar schützt auch vor Meteoriten

Außer für Schutzkleidung wird Kevlar genutzt, um die Internationale Raumstation vor Mikrometeoriten zu schützen, Bootsrümpfe zu verstärken, zu Segeln verarbeitet und als Ersatz für Asbest sowie die Bespannung von Tennisschlägern verwendet. Weltweit werden von dieser Faser 55 Mio. Tonnen unter verschiedenen Namen hergestellt. Mit EXO hat DuPont nach eigener Einschätzung wieder ein Alleinstellungsmerkmal. Technisch gesehen sind Kevlar und EXO Aramidfasern, ein synthetisches Polymer, das aus aromatischen Ringen von sechs Kohlenstoffatomen besteht, die entlang der Faserachse angeordnet sind. Diese Ordnung hat DuPont jetzt modifiziert und so alle Eigenschaften des Materials verbessert.

Sprecher v.l.n.r..: Dr. Reinhard Brandl, MdB, CSU; Manuel Höferlin, MdB, FDP; Ralf Koenzen, CEO, LANCOM Systems; Peter Riedel COO, Rohde & Schwarz; Teresa Ritter, Moderatorin, GovTech Campus AlleFotos: ©LANCOM

Digitale Souveränität

Unternehmen wünschen sich digitale Souveränität, doch in der Praxis ist noch Luft nach oben – auch die Politik ist gefragt

Umfrage von LANCOM Systems, techconsult und Handelsblatt Research Institute

Digitale Souveränität ist im Bewusstsein der Unternehmen angekommen. Das ist das zentrale Ergebnis einer aktuellen Studie von LANCOM Systems, techconsult und Handelsblatt Research Institute. Etwa 70 Prozent der befragten Unternehmen messen dem Thema einen hohen Stellenwert bei. Dennoch wird das Ziel, digital souverän zu sein, größtenteils noch nicht erreicht: Bei einem Drittel der zu den Fokusfeldern Hardware & IT-Infrastruktur, Software & Anwendungen, Daten und IT-Sicherheit befragten Organisationen liegen etwa noch starke Abhängigkeiten von außereuropäischen Anbietern vor. Die Studienergebnisse präsentierte LANCOM am 20. April Digitalpolitikerinnen und -politikern des Deutschen Bundestags bei einem Parlamentarischen Dialog in Berlin – verbunden mit einem klaren Appell an die Politik: Eine aktive Industriepolitik und die Stärkung eu-

ropäischer Technologiekompetenz seien wichtig, um digitale Souveränität zu fördern.

Von Dezember 2022 bis Februar 2023 befragte LANCOM Systems, zusammen mit techconsult und Handelsblatt Research Institute mehr als 250 IT-Verantwortliche zum Status quo ihres Unternehmens hinsichtlich digitaler Souveränität, der Abhängigkeit von Nicht-EU-Anbietern sowie dem allgemeinen Stellenwert des Themas. Betrachtet wurden vier Fokusfelder: Hardware & IT-Infrastruktur, Software & Anwendungen, Daten sowie IT-Sicherheit.

70 Prozent sehen hohen Stellenwert

Erfreuliches Ergebnis der Befragung: Die Relevanz digitaler Souveränität ist bei den Unternehmen angekommen. Über 70 Prozent der Umfrageteilnehmenden messen ihr einen hohen Stellenwert bei. Die Umsetzung ist dabei im Fokusbereich Daten am weitesten fortgeschritten: Hier streben die Unternehmen nicht nur digitale Souveränität an, sondern sind diesem Ziel auch näher als in den anderen untersuchten Bereichen. Gut 36 Prozent geben an, dass eine Abhängigkeit gering oder nicht vorhanden ist.

Der Anteil der Unternehmen mit starker Abhängigkeit von nicht-europäischen Anbietern ist mit 27 Prozent gut zehn Prozentpunkte geringer als in den anderen Fokusfeldern.

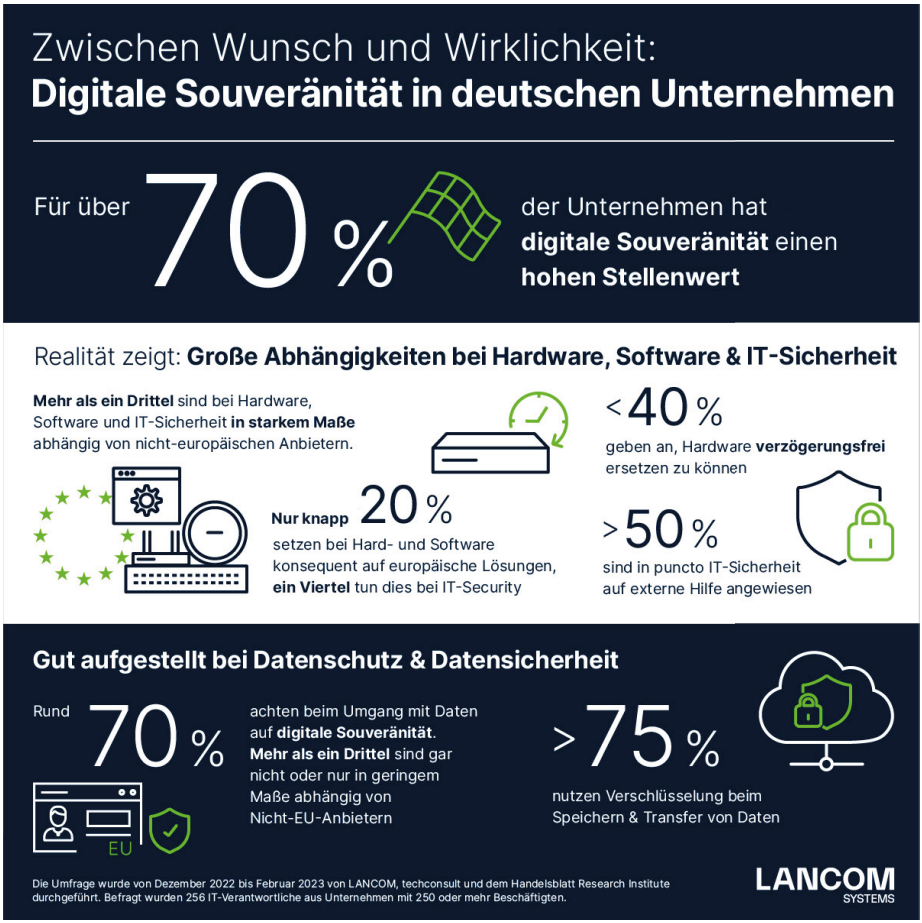


Foto links oben: Sprecher v.l.n.r..: Dr. Reinhard Brandl, MdB, CSU; Manuel Höferlin, MdB, FDP; Ralf Koenzen, CEO, LANCOM Systems
Foto links Mitte: Peter Riedel COO, Rohde & Schwarz
Foto links unten: Empfang

Gut aufgestellt bei Datenschutz und Datensicherheit

Das Thema Datenschutz (im Fokusbereich Daten) ist besonders im Blickfeld der Unternehmen: Mehr als 60 Prozent entscheiden bewusst und kontrollieren, wer auf welche Daten Zugriff hat. Auch im Bereich der Datensicherheit sieht sich der Großteil gut aufgestellt: Jeweils gut drei Viertel der Befragten geben an, dass sie Methoden und Tools zur Verschlüsselung sensibler Daten einsetzen und für eine sichere Verschlüsselung beim Datenaustausch sorgen.

Abhängigkeiten bei Hardware, Software und IT-Security

In den Fokusfeldern Hardware & IT-Infrastruktur, Software & Anwendungen sowie IT-Sicherheit zeigt sich, dass die befragten Unternehmen zwar überwiegend Aspekte der digitalen Souveränität bei der Auswahl von Komponenten und Anwendungen berücksichtigen. Dennoch liegen bei etwa einem Drittel starke Abhängigkeiten von nicht-europäischen Anbietern vor. Sie setzen Hardware, Software oder Security-Komponenten von Herstellern außerhalb der EU ein.

Auch die Politik ist gefragt

Am 20. April 2023 stellte LANCOM die Ergebnisse der Studie im Rahmen eines Parlamentarischen Dialogs Digitalpolitikerinnen und -politikern des

Deutschen Bundestags vor, verbunden mit einem klaren Appell:

Ralf Koenzen, Gründer und Geschäftsführer von LANCOM Systems: „Keine Frage – digitale Souveränität ist im Bewusstsein der Unternehmen angekommen, aber sie wird noch zu wenig umgesetzt. Hier sind sowohl Unternehmen als auch der Staat gefordert. Staatliche Vorgaben können helfen, kritische Abhängigkeiten und damit verbundene Risiken zu reduzieren. Dass solche Maßnahmen Wirkung haben, zeigt sich im Datenbereich, wo es mit der DSGVO bereits strenge Vorgaben gibt und zugleich – von allen vier Fokusfeldern – den höchsten Grad an digitaler Souveränität."

Peter Riedel, Geschäftsführer und COO der LANCOM Konzernmutter Rohde & Schwarz, ergänzt: „Digitale Souveränität ist eine Gemeinschaftsaufgabe. Wir müssen das Bewusstsein für europäische Technologiekompetenz stärken. Positive Beispiele dafür sind das europäische Chip-Gesetz und die Förderung einer eigenen Batterie-Produktion. Auch die Verbesserung von Standortbedingungen für Unternehmen sowie ein stärkerer Fokus auf die Förderung von MINT-Bereichen und die Qualifikation der Beschäftigten sind weitere Schlüssel für mehr digitale Souveränität."

Blick iauf Branchen: Banken & Versicherungen liegen vorne

Deutliche Unterschiede zeigen sich bei einer nach Branchen differenzierten Betrachtung der Studienergebnisse. Während mit etwa 90 Prozent besonders viele Unternehmen aus dem Banken- und Versicherungssektor den Stellenwert digitaler Souveränität als sehr oder eher hoch einschätzen, liegt der Anteil im Handel mit 50 Prozent unter dem Durchschnitt.

Bei Hardware & IT-Infrastruktur achten vor allem Industrieunternehmen auf die digitale Souveränität (79 %), während deren Berücksichtigung bei Dienstleistungsunternehmen deutlich geringer ausfällt (58 %). Allgemein wirkt sich die Tatsache, dass eingesetzte Hardware-Komponenten nicht ohne Verzögerung (nach-)geliefert werden können, negativ auf den digitalen Souveränitätsgrad aus. Nur bei 39 Prozent der Unternehmen ist dies gegeben. Damit ist ein sofortiger Ersatz etwa bei einem Ausfall bei einem Großteil nicht möglich

Bei Software & Anwendungen ist der Anteil der Unternehmen, die auf digitale Souveränität achten, in Handel, öffentlicher Verwaltung, Non-Profit-Bereich sowie Gesundheits- und Sozialwesen unterdurchschnittlich. Nicht einmal die Hälfte der befragten Unternehmen geben an, diese zu berücksichtigen.

Beim Fokusthema Daten sind es erneut Banken und Versicherungen, bei denen mit fast 82 Prozent überdurchschnittlich viele Organisationen auf digitale Souveränität achten.

Im Bereich IT-Sicherheit hat die digitale Souveränität besonders bei Unternehmen aus der Industrie (knapp 74 %) sowie abermals im Finanzbereich (knapp 70 %) einen hohen Stellenwert.

Service: Kostenloser Selbst-Check für Unternehmen

Um herauszufinden, wo ihr eigenes Unternehmen in puncto digitale Souveränität steht, bietet LANCOM Organisationen die Möglichkeit, ihren digitalen Souveränitätsgrad selbst zu bestimmen. Anhand eines Fragebogens können sie ihre individuelle Position im Vergleich zum Benchmark der in der Studie befragten Unternehmen ermitteln. Der Selbst-Check ist hier abrufbar.

Die Umfrage mit allen Ergebnissen ist zum Download erhältlich. https://tinyurl.com/295t3m2r

iDTRONIC

Neue Generation von RFID-Modulen für Industrie 4.0

iDTRONIC, Anbieter von Embedded-RFID-Modulen, hat eine neue Serie von leistungsstarken UHF-RFID-Lesemodulen (840 – 960 MHz) entwikkelt und auf den Markt gebracht. Diese Module basieren auf der neuen Generation der Leserchips IMPINJ E310 und E710 und wurden unter Berücksichtigung aktueller Industrie-4.0- und IoT-Trends entwikkelt. Unabhängig von der Anwendungsumgebung, sei es die Rückverfolgung von Assets in industriellen Prozessen oder die Identifikation von Waren im Einzelhandel, bieten diese drei Module eine enorme Flexibilität und Zuverlässigkeit. Das erweiterte "Herzstück" der iDTRONIC UHF-Module:

IMPINJ E310

- Gute Empfindlichkeit und bis zu 7 dB bessere Empfangsempfindlichkeit im Vergleich zu früheren Modellen für zuverlässige Leistung in der Nähe
- Bis zu 50 % geringerer Chip-Stromverbrauch und Unterstützung batteriebetriebener, energieeffizienter IoT-Geräte

IMPINJ E710

- Superior Empfindlichkeit und bis zu 4 dB besser empfangene Empfindlichkeit als frühere Modelle für zuverlässige Leistung in neuen und aufkommenden Anwendungen
- Bis zu 50 % geringerer Chip-Stromverbrauch und Unterstützung batteriebetriebener, energieeffizienter IoT-Geräte

Das kompakte Formdesign (inkl. SMD), hohe Leseraten von ≥900 Tags/s und leistungsstarke RF-Ausgänge von 30-33 dBm sind nur einige Gründe, warum sich diese Embedded-Module ideal für die industrielle Automatisierung eignen und nahtlos in Maschinen, Geräte oder Montagelinien integriert werden können. Darüber hinaus unterstützen sie EPC U HF Class 1 Gen 2 (ISO 18000-63) Protokoll-Tags sowie 98% der auf dem Markt erhältlichen UHF-Transponder.

Alle vier Ports in einem, ein Modul für alle (M650)

Unser UHF-Lesemodul M650 wurde speziell für eine hochgenaue Leistung entwickelt.
Mit vier Antennenanschlüssen bietet dieses Modul Flexibilität sowie einen stabilen Betrieb, auch in rauen Umgebungen. Das 4-Port-RFID-Modul basiert auf dem IMPINJ E710-Chip, ist kompakt in der Größe, niedrig im Stromverbrauch und hoch in der Stabilität. Auch ist es resistent gegen elektromagnetische Störungen und gut bei der Wärmeableitung. Das Modul eignet sich insbesondere für anspruchsvolle Branchen wie Lagerhaltung, Logistik, Bekleidung, Produktionslinien und dergleichen. Dieses leistungsstarke Lesemodul beschleunigt das Lesen mehrerer UHF-RFID-Tags in einer überfüllten Umgebung und stellt die Konsistenz beim Lesen von Tags sicher. Darüber hinaus erfüllt der M650 sowohl die europäischen als auch die US-amerikanischen regulatorischen Anforderungen und vereinfacht so den globalen Betrieb.

Dynamit-Design für Handheldgeräte, Drucker und Maschinen (M620)

Diese M620 RFID-Einheit bietet Ent-

wicklern eine einfache Steuerung über unser SDK, sodass komplexe Tag-Operationen mit einfachen, aber leistungsstarken vorkonfigurierten Befehlen ausgeführt werden können. Es eignet sich für Geräte, welche in verschiedenen Anwendungenwie RFID-Tag-Druckern, Geldautomaten, Fälschungsschutzgeräten und Lagerverwaltungs-Tools eingesetzt werden. Der M620 ist für RFID-Handlesegeräte oder Tag-Schreibgeräte konzipiert. Es verfügt über eine hohe Empfindlichkeit, einen Anti-Konflikt-Mechanismus, Multi-Tag-Lesung und MMCX-Antennenschnittstelle sowie andere Funktionen. Der schlanke Formfaktor des Geräts macht es ideal für die einfache Integration in leichte und mobile Geräte sowie andere OEM-Anwendungen. Das Lesemodul ist mit dem Leserchip IMPINJ E710 ausgestattet, der Leseraten von bis zu 900 Tags pro Sekunde ermöglicht.

Anwendungsbeispiel: SMD-Fertigung (M600)

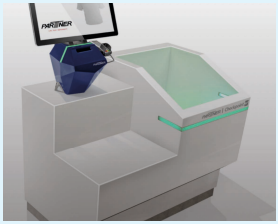
Das RFID-UHF-Modul M600 eignet sich besonders für SMD-Fertigungsprozesse. Auf Wunsch bieten wir auch das UHF-Modul auf Tape & Reel an. SMD-Bauelemente eignen sich für SMT-Bestückungssysteme (Surface Mount Technology). Diese Robotersysteme wurden speziell für SMD-Bauteile entwickelt. Sie werden für die präzise Platzierung von integrierten Schaltkreisen auf Leiterplatten verwendet. Diese wiederum werden in Computern sowie in Industrie-, Medizin-, Automobil-, Militär- und Telekommunikationsgeräten eingesetzt.

Ein Bestückkopf saugt in der Regel ein RFID-Modul aus dem Tape & Reel, prüft die Position mittels eines Kamerasystems, berechnet den Winkel und die Position und platziert das RFID-Modul auf der Leiterplatte. Anschließend wird das RFID-Modul auf die Leiterplatte gelötet.

Checkpoint Systems/ Tech Europe

Neue RFID-Lösung für den Self-Service-Checkout

Fashion RFID SCO heißt die neue Generation von Selbstbedienungskassen, die Checkpoint Systems und Partner Tech Europe, ein Hersteller von POS-Lösungen, gemeinsam entwickelt haben. Durch die Kombi- nation von RFID-Technologie und POS-Terminals verbessern die neuen Self-Service-Checkouts (SCOs) die Bestandsge- nauigkeit, die Warensicherheit und das Kundenerlebnis beim Einkauf.



Bei Fashion RFID SCO wird die Ware von Kunden und Kundinnen einfach auf dem Self-Service Checkout-Bereich ablegt, danach geschieht alles automatisch: Die Kasse identifiziert die RFID-Etiketten und deaktiviert sie, sobald die Zahlung verifiziert ist. Das beschleunigt den Bezahlvorgang und sorgt für ein angenehmes Einkaufserlebnis für den Kunden. Zudem wurden bei der Entwicklung von Fashion RFID SCO viele Problemstellungen gelöst, die es derzeit im Self-Service Checkout-Bereich zu bewältigen gilt. Dazu gehören die Identifizierung von Mehrfachpackungen, nicht barcodierten Artikeln und nicht lesbaren QR-Codes sowie Unannehmlichkeiten durch technische Probleme. Auch die Erkennung von Diebstahlversuchen und damit die Verlustprävention wurden optimiert.

Mehr Umsatz durch Bestandsgenauigkeit

Neben diesen Vorteilen liefert die neue RFID-basierte SCO-Lösung eine Fülle von genauen Daten über einzelne Einkäufe, die – in Kombination mit Bestandsinformationen – Geschäften dabei helfen können, ihren Warenbestand schneller aufzufüllen und die Zahl der Fehlbestände zu reduzieren. Studien haben gezeigt, dass die Einführung von RFID und die Erhöhung der Bestandsgenauigkeit auf über 93 % den Umsatz um 9 % steigern können

Das Fashion RFID SCO ist ab sofort und in verschiedenen Größen und Farben erhältlich, so dass Geschäfte die Lösung an das Design ihres Ladens anpassen können. Weitere Lösungen von Partner Tech sind Alfred, eine kompakte und modulare Self-Checkout-Kasse für verschiedene Einzelhandelssegmente mit einem integriertem "All-in-One"-Touch-POS, einem intelligenten Dreilichtsystem und einer Videokamera, Ace, eine Self-Checkout-Kasse für den Lebensmitteleinzelhandel und den allgemeinen Einzelhandel mit verbesserten Funktionen für Sicherheit und reibungsloses Einkaufen, sowie Bora Bora.
Der futuristische SCO wurde 2022 entwickelt und beinhaltet neben allen herkömmlichen Komponenten wie Scanner, Drucker und Zahlungsterminal auch einen holografischen Touch.

Kooperation

von Arvato Systems und Awesome Technologies

Arvato Systems und Awesome Technologies entwickeln Messenger-Dienst für das Gesundheitswesen

Zusammen mit dem Würzburger Unternehmen Awesome Technologies arbeitet Arvato Systems im Kontext der Telematikinfrastruktur (TI) an einem TI-Messenger für die deutsche Gesundheitsbranche. Der Messenger-Dienst „tim+" wird sowohl die Anforderungen der gematik erfüllen als auch über Features verfügen, die die fallbasierte Kommunikation zwischen den Leistungserbringern erleichtern.

Bei tim+ handelt es sich um einen Sofortnachrichtendienst (Instant Messaging), der die hohen sicherheitstechnischen und datenschutzrechtlichen Anforderungen des Gesundheitswesens erfüllt. Grundsätzlich ist die Einführung solcher TI-Messenger seitens der gematik in mehreren Ausbaustufen geplant: In der ersten Stufe soll zunächst die sektorübergreifende Ad-hoc-Kommunikation zwischen Ärzten, Psychotherapeuten, Mitarbeitenden in Apotheken und weiteren medizinischen Einrichtungen ermöglicht werden. Später soll der Messaging-Dienst dann auch Patienten zugänglich gemacht werden, um zum Beispiel in direkten Kontakt mit Hausarztpraxen oder Krankenkassen zu treten.

Dafür wird der tim+ Messaging-Dienst von Arvato Systems zum Beispiel den Austausch von Textnachrichten, Bildern, Dokumenten oder Sprachnachrichten bieten. Die Nutzung wird auf verschiedenen Wegen möglich sein: Ob per Web-Client, als mobile App auf dem Smartphone oder Tablet oder aber vollständig integriert in Primärsysteme. Zudem soll tim+ auch ohne Sicherheitsbedenken auf privaten Endgeräten genutzt werden können.
Das wird durch eine Ende-zu-Ende-Verschlüsselung und die Nutzung des HL7 FHIR-Standards ermöglicht, durch die Datenschutz sowie die Interoperabilität und der Datenaustausch zwischen unterschiedlichen Systemen sichergestellt werden können. Hinzu kommt, dass tim+ ein abgestuftes Berechtigungskonzept bieten wird, das die Kommunikation innerhalb und zwischen Arbeitsgruppen erleichtert.

Zusammengefasst ist es das Ziel der neuen Lösung, Versorgungsprozesse und Behandlungsabläufe zu unterstützen. Durch die zielgerichtete Integration von KI und Chatbot-Funktionen in tim+ können zukünftig sowohl die strukturierte Analyse von Daten als auch die weitere Verbesserung der Kommunikationsmöglichkeiten dazu beitragen.

„Mit Awesome Technologies haben wir einen starken Partner gefunden, der im Bereich Messaging und Telemedizin schon viele Erfolge feiern konnte", so Kai Ketzer, Senior Manager eHealth bei Arvato Systems. „Gemeinsam wollen wir dafür sorgen, mit tim+ als erster Anwendung der TI 2.0 die Kommunikation der Gesundheitsbranche auf ein neues Level zu heben."

Dr. Christoph Günther, CEO Awesome Technologies, ergänzt: „In mehreren Projekten und mit unseren bestehenden Produkten konnten wir zeigen, dass der organisatorische Aufwand für Patienten und betreuendes Pflegepersonal durch moderne Kommunikationstechnologie enorm reduziert werden kann. Zusammen mit Arvato Systems und seiner TI-Expertise können wir jetzt das wichtige Ziel erreichen, alle Beteiligten im Gesundheitswesen bestmöglich miteinander zu vernetzen."

Über Awesome Technologies

Awesome Technologies ist ein im Jahre 2017 gegründetes Softwareunternehmen aus Würzburg. Das Unternehmen ist u.a. spezialisiert auf Softwarelösungen im Bereich des Gesundheitswesens und verfügt über Expertise im Bereich sicheres Messaging, Telemedizin, Datasharing und FHIR. Die Softwarelösungen von Awesome Technologies unterstützen Kommunikation- und Prozessabläufe im medizinischen Alltag und leisten damit einen wichtigen Beitrag in der Patientenversorgung.

Fachkräftemangel an deutschen Flughäfen

In diesen Städten wird am dringendsten Personal im Sicherheitsbereich gesucht

- **Der Anbieter für Videomanagementsoftware Milestone Systems untersucht die zehn größten deutschen Flughäfen nach Stellenausschreibungen für Sicherheitspersonal**
- **Frankfurt am Main ist Spitzenreiter bei der Anzahl der Stellenausschreibungen**
- **Der am besten zahlende Arbeitgeber unter den Flughäfen ist Hannover**

An den Flughäfen in Deutschland herrscht ein großer Mangel an Fachkräften. Insbesondere Sicherheitspersonal wird nach der COVID-19-Pandemie dringend benötigt. Die Sicherheitskontrollen waren im Sommer 2022 oft unterbesetzt und überlastet. Das führte zu Chaos und dazu, dass viele Reisende ihre Flüge verpassten.

Foto: Fraport AG

Wenn modernste Videotechnologie verantwortungsvoll eingesetzt wird, kann das Sicherheitspersonal schnell und effektiv entlastet werden. Der Anbieter für Videomanagementsoftware Milestone Systems hat deshalb die zehn größten Flughäfen Deutschlands analysiert und herausgefunden, welche die meisten Stellenangebote im Bereich Sicherheit anbieten. Zusätzlich wurden entsprechende Gehälter und Arbeitsverhältnisse in die Recherche mit einbezogen.

Der größte Fachkräftemangel herrscht in Frankfurt am Main und Berlin

Besonders viele Reisende mussten im vergangenen Jahr unter dem fehlenden Sicherheitspersonal leiden. Mit insgesamt 171 Stellenausschreibungen wird schnell deutlich, wie dringend die Suche nach qualifizierten Sicherheitskräften ist. Frankfurt am Main ist dabei Spitzenreiter. Der Flughafen in der hessischen Hauptstadt verzeichnete gleich 40 Ausschreibungen für Sicherheitsfachkräfte. Dicht dahinter folgt Berlin mit 33 unbesetzten Jobangeboten im Sicherheitsbereich. Unter den Top fünf reihen sich anschließend München mit 27, sowie Stuttgart und Köln mit jeweils 14 Stellenanzeigen ein.

Hannover Flughafen bezahlt am besten

Die am besten bezahlten Sicherheitsfachkräfte arbeiten in Hannover. Dort können Arbeitnehmende im Sicherheitsbereich bei einer 40-Stunden-Woche bis zu 3414 Euro brutto im Monat verdienen. Damit zahlt der niedersächsische Flughafen über 500 Euro mehr aus als der Durchschnittsverdienst aller untersuchten Flughäfen. Dieser liegt bei 2846 Euro. Hamburg und Düsseldorf reihen sich mit 3414 und 3261 Euro auf Platz zwei und drei ein. Die Stellenausschreibungen beziehen sich hierbei zu über 80 Prozent auf Vollzeitstellen und zu fünf Prozent auf Ausbildungsplätze.

Foto: Fraport AG

Jos Beernink, VP EMEA von Milestone Systems, kommentiert die Analyse: "Die Zahl der fehlenden Sicherheitskräfte ist erschreckend hoch. An kaum einem anderen Arbeitsplatz ist Sicherheit so wichtig, um etwaige Risiken so weit wie möglich zu minimieren. Dabei kann Videotechnologie zur Hilfe hinzugezogen werden, um vor allem Fachkräfte so schnell wie möglich entlasten zu können. Moderne Videosoftware kann dem Personal dabei helfen, alles zu überwachen und proaktive oder reaktive Maßnahmen schnell in die Wege zu leiten. Dies ermöglicht zum einen, Videomaterial zu filtern und zum anderen durch die Trackingfunktion einen einfacheren virtuellen Überblick zu behalten. Zusätzlich kann das Fachpersonal im Sicherheitsbereich durch Videotechnologien unterstützt und entlastet werden. "

Über 21.000 Besucher!

Leitmesse der Pflegebranche voller Erfolg

Nach drei Tagen schloss die Leitmesse der Pflegebranchein in Nürnberg Ende April ihre Pforten.
Insgesamt kamen über 21.000 Besucher auf das Messegelände in Nürnberg, um sich bei 570 Ausstellern über neueste Produkte, Dienstleistungen und Trends aus den Bereichen Pflege & Therapie, Beruf & Bildung, IT & Management, Küche, Ernährung, Textil & Hygiene sowie Raum & Technik zu informieren. Zudem verfolgten rund 1500 Menschen das Forumsprogramm per Livestream im Internet.
Für die Veranstalter, das hannoversche Medienhaus Vincentz Network und die Deutsche Messe AG, ein mehr als gelungener Re-Start nachdem die ALTENPFLEGE 2021 pandemiebedingt in Nürnberg ausfallen musste und 2022 turnusmäßig in Essen stattfand.

Dr. Dominik Wagemann, Verlagsleiter bei Vincentz Network: „Wir konnten auf der ALTENPFLEGE erneut die wichtigsten Akteure der Pflegebranche zusammenbringen. Die Messe und der begleitende Kongress haben sich zum wiederholten Male als wichtigster Treffpunkt sowohl für das Management als auch für leitende Pflegefachkräfte in der Altenhilfe behauptet.“ Das belegen auch die Ergebnisse des unabhängigen Marktforschungsinstituts Gelszus aus Dortmund. Demnach gaben 92 Prozent der Besucher der ALTENPFLEGE die Bewertung gut bis sehr gut.

87 Prozent gaben an, die Messe auch in Zukunft besuchen zu wollen und 84 Prozent werden die Messe nach eigenen Angaben weiterempfehlen. Entsprechend hoch auch die Zufriedenheit unter den Ausstellern. Alexander Vögele, Vertriebscontroller der Firmengruppe Schneeweiss: „Wir sind erstmals seit 2010 wieder bei der ALTENPFLEGE dabei und sind mit dem Zuspruch und der Qualität der Besucher sowie den geknüpften Kontakten sehr zufrieden."

Maximilian Wischer Geschäftsleitungsassistent bei ille Papierservice: „Die Messe begeistert durch ein buntes, gemischtes Publikum, das aus Fachbesuchern und Entscheidungspersonal besteht. Das Besucheraufkommen war hoch und wir konnten gute Geschäftsabschlüsse und Marketingeffekte erzielen."
Und Julia Arndt, Marketing- und Eventmanagerin bei opta data: „Wir sind absolut zufrieden, speziell mit der Organisation der Messe. Die Qualität der Besucher hat uns sehr gut gefallen, genau wie die Location. Wir sind auf jeden Fall im nächsten Jahr wieder mit dabei." *)

Laut des Marktforschungsinstituts Gelszus gaben 84 Prozent der Aussteller an, mit der Messe vollkommen zufrieden bis zufrieden zu sein.

Zu den wichtigsten Themen der 33. Leitmesse und dem begleitenden Messekongress gehörten in diesem Jahr die Telematik Infrastruktur, die Digitalisierung der Pflege, der anhaltende Fachkräftemangel und die wirtschaftliche Stabilisierung der Pflegeeinrichtungen.
Dr. Dominik Wagemann: „Gemäß unserem diesjährigen Motto ‚Die Pflege gestalten. WIR. GEMEINSAM.' ist es uns gemeinsam mit allen Beteiligten gelungen, sowohl auf der Messe als auch im Kongress Lösungen für die großen Herausforderungen zu diskutieren und zu konkretisieren."

Ein besonderes Highlight der Messe stellte auch in diesem Jahr die Sonderpräsentation „AVENEO – Raum für Innovationen" dar. Über 50 Start-ups, Studierende, Forschungseinrichtungen und Hochschulen präsentierten ihre Ideen und zeigten Konzepte aus den Bereichen Pflege, Technologie, Internet der Dinge, Design, Architektur sowie Pflege- und Sozialwirtschaft. Die besten Ideen wurden im Rahmen der Start-Up-Challenge von einer hochkarätig besetzten Jury prämiert und mit attraktiven Marketingpaketen ausgezeichnet.

Die nächste ALTENPFLEGE findet 23. bis 25. April 2024 in Essen statt.

Legrand Care

Sicherheit für den Zugang in das CMP mit 2-Faktor-Authentifizierung

Ein Zugriff Unbefugter auf die Einstellungen im CMP kann große Auswirkungen für Hausnotrufdienst und Anwender haben. Es gilt daher sicherzustellen, dass niemand von außen Änderungen an den Geräten vornimmt oder diese anderweitig manipulieren kann. Um das Risiko, dass sich Unbefugte in das CMP unter Verwendung Ihrer Zugangsdaten einloggen, weiter zu verringern, aktiviert Legrand Care ab April die sogenannte Zwei-Faktor-Authentifizierung mit TOTP (Time-based One-Time Password) für alle CMP Benutzer. Vermutlich kennen Sie die Zwei-Faktor-Authentifizierung bereits von anderen Online-Diensten wie Ihrer Bank, PayPal, Google oder Microsoft Konten. Hier benötigt man neben einem Benutzernamen / E-Mail Adresse und Passwort ebenfalls eine zusätzliche Bestätigung Ihrer Identität. Diese Bestätigung erfolgt durch einen „Hardware-Token", der zeitbasierte „Einmal"- oder "Wegwerfpasswörter" generiert.

Varianten der Zwei-Faktor-Authentifizierung mit TOTP

In der Praxis kann auf verschiedene Möglichkeiten zurückgegriffen werden, um dieses Einmalpasswort zu erstellen. Falls schon eine Google, Microsoft oder andere Authenticator App auf den unternehmenseigenen Smartphones genutzt werden, kann auch für das CMP für einen weiteren Account hinzugefügt und verwendet werden. Neben der Möglichkeit, mit einem Smartphone oder Tablet zu arbeiten, besteht auch die Möglichkeit, den zweiten Faktor auf einem Computer zu generieren. Dies funktioniert ganz einfach mit kleinen Programmen oder Erweiterungen für gängige Browser.

Informationen zur Aktivierung

Ab April wird die Zwei-Faktor-Authentifizierung mit TOTP automatisch aktiviert. Sollten Anwender die Zwei-Faktor-Authentifizierung mit TOTP noch nicht aktiv genutzt haben, wird das gewohnte Login mit Benutzername und Passwort in einen Barcode umgewandelt. Mit diesem Barcode kann die neue Zwei-Faktor-Authentifizierung mit TOTP eingerichtet werdenn. Dieser Einrichtungs-Schritt kann nicht übersprungen werden.

Mutlifunktionaler PIR II

Bewegungsmelder und Türalarm in einem

Für eine effektive und gleichzeitig möglichst menschliche Betreuung von Demenz-Patienten braucht es ein gesundes Gleichgewicht zwischen Freiheit und Kontrolle. Mit der Demenz-Lösung rund um D-POS bietet NEAT hier schon seit Jahren ein zuverlässiges System. Jetzt gibt es dazu mit dem intelligenten Türalarm des Bewegungsmelder PIR II eine sinnvolle Ergänzung.Zur Überwachung der natürlichen Bewegungsfreiheit von Demenz-Patienten gibt es zwei verschiedene Ansätze:

Die personenbezogene und türbezogene Überwachung. Für die personenbezogene Überwachung von Demenz-Patienten bietet NEAT mit D-POS und dem dazugehörigen Funksender SMILE ID eine äußerst effektive Lösung.

Die betreuten Personen haben innerhalb der Ihnen zugänglichen Bereiche maximale Bewegungsfreiheit und genießen gleichzeitig das Gefühl größtmöglicher Sicherheit. Zur türbezogenen Überwachung gibt es neben dem bewährten Funk-Türalarm DOOR nun auch den Bewegungsmelder mit intelligentem Türalarm PIR II.

Bewegungsmelder PIR II erfüllt diverse Anforderungen

Das besondere an PIR II ist seine Flexibilität. So kann PIR II z. B. als Bewegungsmelder feststellen, ob eine fremde Person in einem Raum anwesend ist oder eine Inaktivität der darin lebenden Person registrieren. So lassen sich auch bettlägeriger Personen überwachen, die nachts aktiv sind oder Schwierigkeiten beim Aufstehen haben.

PIR II mit intelligentem Türalarm auch für Betreuung von Demenz-Patienten

Dank eines integrierten Türsensors eignet sich PIR II auch zur Überwachung von Türen, z. B. im Rahmen der Betreuung von Demenz-Patienten. PIR II kann z. B. unterscheiden, ob eine Person den Raum tatsächlich verlässt oder einfach nur die Tür öffnet und wieder schließt. Zudem lässt sich der Alarm auch zeitverzögert auslösen. Sowohl das Personal wie auch die Bewohner können den Raum dann z. B. innerhalb von 15 Sekunden verlassen oder betreten, ohne das ein Alarm ausgelöst wird.

Wesentliches Element zur Verbindung von Menschlichkeit und Effizienz

PIR II kann damit ein wesentlicher Schlüssel für eine erfolgreiche und für alle Beteiligten möglichst stressfreie Betreuung von Demenz-Patienten sein. Der Bewegungsmelder bietet eine Rund-um-die-Uhr Sicherheit und der Türalarm mit zeitlich programmierbarer Ein- und Ausgangsverzögerung größtmögliche Flexibilität

senvis Medical

Einfach unter eine Bettrolle - fertig!

Unter der Bettrolle platziert, analysiert AnnaCare mit Hilfe künstlicher Intelligenz Vibrationen im Bett. Wird eine potenzielle Gefahrensituation erkannt, z.B. das Verlassen des Bettes, werden Pflegekräfte umgehend alarmiert, damit rechtzeitig Hilfe geleistet werden kann.

Alarmierung innerhalb von Sekunden

Durch die hohe Erkennungsgenauigkeit und kontinuierliche Analyse der Vibrationen im Bett und Raum wird schnell und sicher Alarmiert. Im Gegensatz zu anderen Systemen verpasst AnnaCare aufgrund seiner Funktionsweise kein Aufstehen.
Der Abreißschutz an den beiden Kabelverbindungen zum Handgerät vermeidet Beschädigungen an den Kabeln, unserem AnnaCare-System und an Ihrer Rufanlage. Durch diese Schutzmaßnahme können zusätzlich einzelne Teilkomponenten werkzeugfrei getauscht werden. Bei Teildefekt werden so Kosten und Ressourcen gespart. Kundennutzen hat für uns höchste Priorität. AnnaCare wurde deshalb auf der Basis von Vibrationsanalyse entwickelt. Wir haben das Patienten-Monitoring neu gedacht und so ein einzigartiges Produkt geschaffen.

ActiGuard

Weglaufschutz

Das Sicherheitssystem, bei dem die pflegebedürftige Person keine Geräte mit sich tragen muss. Der MINI Wäschetransponder ist batterielos und kann z. B. an der Kleidung angebracht werden. Verlässt der Träger die sichere Zone, so wird das durch den Sensor an die Rufanlage signalisiert.

Mit ActiGuard kann einerseits der Bewegungsfreiraum der Personen im Gebäude eingegrenzt und kontrolliert werden, andererseits können Personen im Gebäude lokalisiert und geschützt werden. Das System besteht aus aktiven sowie passiven Transpondern und Lesegeräten, sogenannte Locator. Eine Person trägt den aktiven oder passiven Transponder bei sich, der von dem Locator in Reichweite erfasst wird. Locator können dabei nicht nur die Transponder erfassen, sondern auch Türen und Alarme steuern und so z. B. Bereiche abgrenzen oder öffnen. Die auf die jeweiligen Anwendungen konzipierte Managementsoftware bietet eine intuitive und leichte Bedienung und verfügt über Schnittstellen zur Anbindung an weitere Kommunikations- und Informationssysteme.
Bei der Verwendung des ActiGuard ist die amtsrichterliche Zustimmung für die betroffenen Personen zu beantragen. Bitte setzen sie sich vor dem Einsatz mit Ihrem Amtsgericht in Verbindung und lassen sich die betreuungsgerichtliche Genehmigung erteilen.

Systevo Call Smart

Pflegekommunikation der nächsten Generation

Zukunftsorientierte Krankenhausstrukturen setzen mit Systevo Call Ackermann auf smarte Arbeitsumgebungen und intelligenten Technologieeinsatz.

Durch die Integration von Kommunikationssystemen, Alarmmanagementsystemen und der Rufanlage werden Patientensicherheit und effiziente Arbeitsabläufe in Pflegeeinrichtungen zu Kernelemente unserer neuen Systemplattform. Durch die moderne Architektur ermöglicht das System, Prozessabläufe kundenorientiert und flexibel einzurichten und unterstützt die Pflegekräfte bei der täglichen Patientenversorgung. Ein wichtiger Vorteil ist, dass Systevo Call Ackermann eine flexible Integration in bestehende ITK-Systemlandschaften bietet. Systevo Call Smart Patientenhandgerät mit ergonomischem Design, für

die einfache Bedienung durch Patienten und Bewohner in Pflegeeinrichtungen.

Details im Einzelnen

- Benutzergeführte Sprachkommunikation mit dem Pflegepersonal im Freisprechmodus oder im diskreten Sprachmodus. Es ist mit großer Ruftaste mit leicht erkennbarem sowie fühlbarem Druckpunkt ist das Gerät für eine sichere Rufauslösung vorbereitet.
- Ergonomisches Design des Geräts für eine einfache Handhabung durch verschiedene Nutzergruppen und Altersstufen.
- Benutzerführung über das Touch-Display durch konfigurierbare Anzeigeelemente, Dienste und Visualisierung von Icons zur intuitiven Bedienung durch Benutzer in Pflegeeinrichtungen.
- Übertragung des TV-Tons über den integrierten Lautsprecher oder Kopfhörer.
- Überwachung/Synchronisation der Datenübertragung und der Audioverbindungen (Gespräche) durch den Master Room Controller, inkl. Verwaltung der Konfigurationsdaten.
- Aufrüstbar auf zukünftige System-Firmware dank fortschrittlicher Flash-Speichertechnologien. Inklusive der Möglichkeit zur automatischen Softwareaktualisierung im laufenden Betrieb. Erfüllung der Cybersicherheitsanforderungen moderner Datenbusinfrastrukturen.
- Lizenzpflichtige Systemfunktionen werden durch entsprechende Softwarelizenzen bereitgestellt.

Systevo

Touch IP mit 7" Display

Touch-Terminal IP, mit 7" Display und kapazitiver Bedienoberfläche ist zur Unterstützung der täglichen Pflegeabläufe in Pflegeeinrichtungen. Die anwender-konforme Anzeige, die Gestaltung laufzeitkritischer und relevanter Daten und die Unterstützung der Prozessabläufe für Anwendergruppen wie Pflegekräfte, ärztlichen Dienst sowie unterstützendes Personal (u.a. IT-Abteilung, techn. Dienst), zur Reduktion der Wegezeiten, Optimierung der Produktivität und effizientem Informationsfluss von Pflegeaufgaben umfassen das technische Aufgabenspektrum in der Pflege.

Die Nutzung der RFID-Technologi oder PIN-Code dient zur revisionssicheren Authentifizierung bzw. zeitgenauen Registrierung von Vorgängen und für die Zugriffssteuerung gemäß DSGVO-Vorgaben, in Abhängigkeit der Anforderung in Pflegeeinrichtungen. Eine IP-Kommunkationseinheit für den Full-Duplex Betrieb, im hochwertigen aP-Gehäuse für Bewohner-/Patientenzimmer/Dienstzimmern, sowie als Steuereinheit für Zusatzfunktionen im jeweiligen Zimmer und als Gateway zu mobilen Endgeräten gehört zur Lösung. Es ist eine intuitive Bedienung über das hintergrundbeleuchtete Touch-Display mit hoher Farbbrillanz und guter Ablesbarkeit in unterschiedlichen Umgebungsparametern (Helligkeit, Entfernung) möglich. Die Kommunikation im freien Gegensprechen (Full-Duplex) und die Durchsagefunktion (Senden/Empfangen) via IP-Kommunikation oder Bus-Technologie sowie Anbindung mit VoIP/SIP Schnittstelle (ETH, WIFI), zur Kommunikation ist über die Tk-Anlage or-

ganisiert. Es besteht außerdem eine optionale Erweiterung mit Telefonie-Client (SIP) für Dienstzimmer sowie Funktionsräume.

Die Anzeige von Systemmeldungen bei gesetzter Anwesenheit (Alarme, Rufe und Anwesenheiten etc.) mit der höchsten Priorität erfolgt in farblicher, priorisierter Reihenfolge sowie nach Uhrzeit und Datum. Eine akustische Rufnachsendung bei gesetzter Anwesenheit sowie besteht die Möglichkeit zur Auslösung weiterer Rufe. Eine Option zur Konfiguration des Nachmodus für die Abschaltung der Displayanzeige zur Erfüllung der Nachtruhe für Bewohner/Patienten ist ebenso inkludiert. Die Unterstützung Workflow-relevanter Prozesse durch eine Anzeige sowie das Auswählen bzw. Abwählen von Diensten (Zusammenschaltungen), zur erweiterten der Rufnachsendung in weitere Stationen runden die Zusatzfunktionen ab. Die RFID-Technik zur Legitimation am Touch-Terminal autorisiert den Zugriff auf die Patientendaten direkt im Patientenzimmer sowie eine Dokumentation von Pflegevorgänge.
Dadurch ergibt sich eine effiziente Gestaltung von Pflegeaufgaben und Tätigkeiten sowie der Dokumentation für den jeweiligen Patienten zur Entlastung bei Routinearbeiten sowie die Unterstützung der täglichen Pflegeprozesse in geeigneter Weise.

Pflegeleistungen werden unmittelbar nach der Bereitstellung dokumentiert: Eine Erfassung von Vitaldaten, pflegerischen Tätigkeiten, Medikation und anderen dokumentationspflichtigen Informationen, zur Reduktion fehlerbehafterer Aufzeichnungen. Energieeinsparung und optimierte domotische Kontrollfunk- tionen werden durch eine lokale Benutzeroberfläche bereitgestellt.
Die Überwachung und Synchronisation des gesamten Datenverkehrs, der Audioverbindungen (Gespräche, Durchsagen) zu anderen Zimmern innerhalb der Organisationseinheit, die Koordination der Kommunikation mit den Zentraleinheiten und weiteren IP-Teilnehmern erfolgt über IP-Schnittstelle (ETH-LAN, WIFI). Die Konfigurationsdaten eines Zimmers werden über den Management-Server verwaltet, durch die Nutzung standardisierter Web-Services bereitgestellt und lokal abgelegt.

Unterstützung der Cyber Security Anforderungen von modernen IT-Infrastrukturen. Aufrüstbar auf zukünftige System-Firmware dank zukunftsweisender Flash- und Speicher-Technologien, um einen automatisierten Software-Update im laufenden Betrieb zu gewährleisten. Mehrstufiges Sicherheitskonzept ermöglicht die lokale Rufsignalisierung bei fehlender Kommunikation mit der Zentraleinheit des Systems.

AUS DER PRAXIS

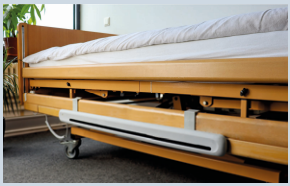
Zutrittskontrolle für Pflegeheim

Das Pflegeheim St. Elisabeth in Bettembourg, betreibt seit knapp zwei Jahren eine SCC 5.0 Software von Martin Care inklusive 130 LF-Ortungspunkte, mehr als 100 Bewohner-Transpondern und 115 gesichertenTüren mit der Zutrittskontrolle. Die errichtende Firma ist die Telkea Group in Luxembourg. Der Verwaltungsdirektor Robert Gindt erklärt die Beweggründe für den Einsatz des Systems und beschreibt die Erfahrungen des bisherigen Betriebs.

Das Ziel war es, dass alle Ein- bzw. Ausgangstüren von außen verschlossen sind und somit ein unberechtigter Zutritt außerhalb der Öffnungszeiten der Einrichtung unmöglich ist. Jedoch sollten Personal sowie BewohnerInnen mit ihren Transpondern jederzeit in die Einrichtung eintreten dürfen. Diese Maßnahme sollte die Einrichtung zum einen sicherer machen, insbesondere im Hinblick auf Diebstähle und zum anderen wird das Personal zeitlich entlastet. Denn für Personal und Bewohner entstand hiermit der Mehrwert, dass Bewohner jederzeit den Außenbereich, wie zum Beispiel die Terrasse betreten können und an-

schließend auch wieder selbstständig in das Haus zurückkehren können. Zuvor war es nötig gewesen, die Türen manuell durch das Personal zu öffnen. Insbesondere in der Coronapandemie wurde das ständige Türenöffnen durch das Personal aufwändig. Nun wird jedoch mit der Zutrittskontrolle der SCC 5.0 Zeit gespart und Arbeitsunterbrüche sind reduziert worden. Bewohner empfinden hierdurch außerdem ein größeres Gefühl von Selbstständigkeit.
Als weiteren Vorteil, der durch den Einsatz der SCC 5.0 entstanden ist, nannte Gindt die Alarmierungen der Transponder und Türen inklusive der Darstellung auf einer Karte: Die Wohnbereichsleiter haben nun eine bessere Möglichkeit, alle relevanten Vorgänge zu überwachen und durch die Anzeigeart sehen sie in dem System eine Qualitätsverbesserung für die Schwesternrufanlage.

Nach der Ersteinführung der Schutzengel-Systeme, hat sich die Einrichtungsleitung des Ste Elisabeth für eine Erweiterung entschieden: Das Nebengebäude – die Tagestätte der Einrichtung – ist nun ebenfalls in die SCC 5.0 eingebettet. Hier wird aktuell noch nicht mit einer Kartendarstellung gearbeitet, sondern ausschließlich mit Textnachrichten. Der Vorteil der Kartendarstellung überwiegt jedoch, sodass nach entsprechender PC-Hardware Anpassung seitens der Einrichtung, auch hier zukünftig die SCC 5.0 einschließlich der Kartendarstellung genutzt werden kann.



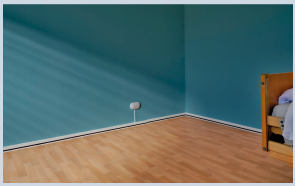
Neviscura

Bettsensor als Antwort auf Sensormatten

Der Bettsensor von nevisCura ist ein intelligenter Bettausstieg-Alarm, der Pflegekräften den Arbeitsalltag spurbar erleichtert. Einmal und mit nur wenigen Handgriffen am Bett angebracht, meldet der stille Wächter diskret, wenn ein Bewohner das Bett verlassen möchte – und das schon bevor er auch nur einen Fuß auf den Boden gesetzt hat. Und das Beste: Der Sensor ist kompatibel zu jeder gängigen Rufanlage.

Die Eigenschaften im Überblick:

- Weniger Fehlalarme: Die intelligente Technologie reduziert Fehlalarme auf ein Minimum.
- Flexible Alarmanbindung: Geeignet fur Telefonanlagen, Hausnotruf, Lichtrufanlage oder Funkgong
- Schnelle Installation: Einfach am Bett einhaken, mit der Rufanlage verbinden und schon kann das Gerät eingesetzt werden.
- Hoher Investitionsschutz: Durch regelmäßige Updates erhält das Gerät immer neue Funktionen und kann so lange eingesetzt werden.



Otiom A/S

Angst zu verschwinden

Otiom ist eine neue, in Dänemark entwickelte Ortungslösung, die Personen mit Demenz davor schützt zu verschwinden. Das System wurde in Zusammenarbeit mit Angehörigen, Pflegepersonal und Personen mit Demenz entwickelt. Otiom kann mit allen bekannten Rufanlagen oder Alarmserver-Lösungen integriert werden. Das System setzt geographische Geborgenheitsbereiche fest. Otiom überwacht nicht und ortet erst dann, wenn ein Bereich verlassen wird. Otiom benachrichtigt erst dann die vorher festgelegten Bezugspersonen per SMS oder über die App, wenn Gefahr im Verzug sein könnte. Deshalb kann man das Otiom nicht zur konstanten Überwachung verwenden. Dies verleiht dem Demenzerkrankten und den Angehörigen ein größeres Gefühl von Freiheit.

Dle Anwender legen selbst fest, in welchem Bereich sich der Demenzerkrankte sicher bewegen kann und persönliche Geborgenheitsbereiche werden individuell festgelegt. Geborgenheitsbereiche sind geographische Bereiche, in denen sich die Person mit Demenz frei bewegen kann, ohne überwacht zu werden. Verlässt die Person den Bereich, wird der Alarm aktiviert, und die vorher festgelegten Bezugspersonen werden benachrichtigt.

TEKTRONIK

Rufanlage mit Sprachfunktion

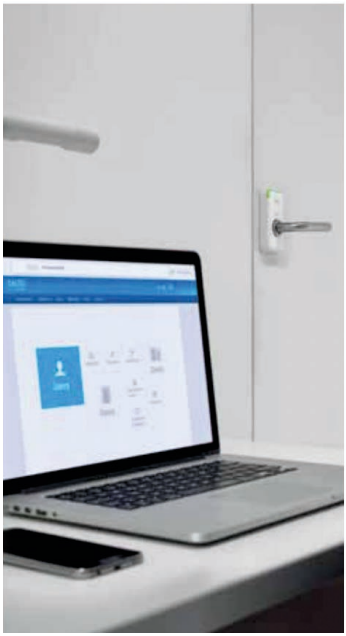
Mehrwert für das Personal durch direkte Kommunikation

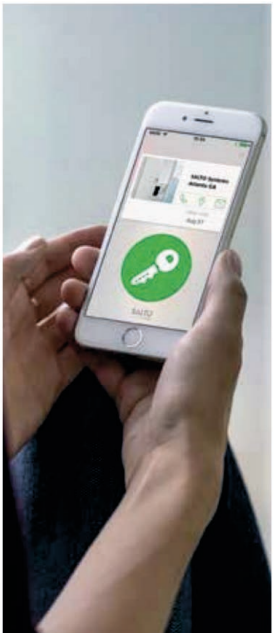
Die Optimierung interner Arbeitsabläufe im Gesundheitswesen spart Zeit und Geld. Unnötige Wege und lange Informationsketten können sich in Zeiten wachsenden Kostendrucks weder Kliniken noch Pflegeeinrichtungen leisten. Vor allem geht kostbare Zeit verloren, die Ihr Personal für die Betreuung von Patienten und Bewohnern dringend braucht. Rufanlagen helfen die Erreichbarkeit von Mitarbeitern erhöhen und damit wertvolle Zeit sparen. Moderne und innovative Rufanlagen verfügen über die Möglichkeit, dass Pflegekräfte direkt mit den zu pflegenden Personen in Kontakt treten können. Das betrifft gleichermaßen Senioren- bzw. Betreuungseinrichtungen als auch Krankenhäuser.

Die Sprache ermöglicht es dem Menschen seit jeher, umfassende Informationen zu erhalten. Bezogen auf eine Rufanlage kann es bedeuten, den Grund des Rufes zu erfragen, damit unmittelbar geeignete Maßnahme ergriffen bzw. organisiert werden können. Sprache hat aber auch eine beruhigende Wirkung, vor allem auf die Person, welche auf Unterstützung bzw. Hilfe angewiesen ist.
In Beratungsgesprächen kommt hin und wieder der Einwand, dass die Sprache zu unpersönlich sei, als störend empfunden wird und aus diesen Gründen auf generelle Ablehnung stößt. Ganz von der Hand zu weisen ist das nicht. In vielen Fällen zeigt sich allerdings, dass die Mitarbeitenden gar nicht wissen, dass die vorhandene Rufanlage über das Leistungsmerkmal der Sprache verfügt.
Ziel der Rufanlagen ist es auf gar keinen Fall, den persönlichen Kontakt zwischen Bewohnern / Patienten und dem Pflegepersonal zu reduzieren. Genau das Gegenteil ist der Fall, wenn diese Konzepte zielgerichtet und bedarfsorientiert eingesetzt werden So sind in den Einrichtungen tagsüber mehr Pflegekräfte auf einer Station bzw. einem Wohnbereich tätig als am Nachmittag oder in den Nachtstunden. Die Erfahrungen in der Praxis zeigen beispielsweise, dass die Sprachfunktion im Tagesverlauf deutlich seltener zur Anwendung kommt.Demgegenüber wird der Komfort einer Sprachverbindung zu dem Rufenden während der Nacht als außerordentlich entlastend vom Pflegepersonal wahrgenommen. Zurückgeführt wird das meist auf eine reduzierte Personalstärke, bei gleichbleibender Belegung der Betten.
Hinzu kommt, dass nicht jeder Ruf per se eine Notsituation darstellt. Und genau an dieser Stelle macht sich eine Rufanlage mit Sprachfunktion bezahlt. Ohne den Grund zu kennen, welcher zur Rufauslösung geführt hat, muss das Pflegepersonal nämlich den Ruf im jeweiligen Zimmer zurücksetzen.
Lässt sich dagegen der Ruf abfragen und die Dringlichkeit vom Pflegepersonal bewerten, dürfen abgefragte Rufe aus der Ferne abgestellt werden.
Auch die Corona-Pandemie war für Einrichtungen des Gesundheitswesens, Pflegekräfte und die zu pflegenden Personen eine außerordent- liche Herausforderung. Beispielsweise mussten Schutzanzüge beim Betreten eines Zimmers angelegt und nach dem Verlassen wieder abgelegt sowie entsorgt werden. Von unseren Kunden haben wir ein Feedback erhalten, dass mit den FN 6000 Sprachterminals ein schnelles und gezieltes Ansprechen möglich war, ohne das Zimmer betreten zu müssen. Zum Nachweis dokumentiert eine tetronik Rufanlage sämtliche abgefragten Rufe, welche via Fernabstellung bearbeitet wurden. Die Besonderheit des Sprachterminalsvon Tektronik ist zudem ein integrierter Sensor für die akustische Rufauslösung. Hierzu müssen zwei Bedingungen erfüllt sein. Dabei handelt es sich um einen definierten Lautstärkepegel welcher für eine definierte Zeit erkannt wird. Ist beides gegeben, kann das Sprachterminal vollautomatisch einen Ruf an das Pflegepersonal absetzen. Wenngleich Begriffe wie „Babyphone" die Funktion dem Grunde nach beschreiben, so steht die Zuverlässigkeit und Flexibilität unserer Produkte auf einem ganz anderen Level.

Fazit:

Rufanlagen mit Sprache kosten bei der Anschaffung zwar etwas mehr, umgerechnet auf die Laufzeit von 30 Jahren sollte der Mehrwert aber nicht außer Acht gelassen werden. Wenn bei Ihnen die Neubeschaffung ansteht, sehen Sie vielleicht eine Rufanlage mit Sprachfunktion in einem anderen Licht.





Durchgängige Zutrittslösung

in Senioren- und Pflegeheimen

SALTO präsentierte in Nürnberg seine SALTO Space Systemplattform und demonstriert live, wie Senioren- und Pflegeheime mit einer durchgängigen Zutrittslösung ihre Sicherheit verbessern sowie Betriebskosten senken können.

Mit den elektronischen Zutrittslösungen von SALTO lassen sich Gebäude, Bereiche und Räume klar strukturieren.
Auf diese Weise erhalten nur berechtigte Personen zeitlich begrenzten Zutritt zu z.B. Wohnungen, Gemeinschaftsräumen, Technikbereichen oder Büros. Das Zutrittsmanagement erfolgt über die Browser-basierte Software ProAccess Space, die sich funktional anpassen lässt, eine einfache Handhabung bietet und jederzeit einen Überblick über die aktuellen Zutrittsrechte aller Personengruppen wie Bewohner, Pflegepersonal, Verwaltungsmitarbeiter, Besucher und Dienstleister verschafft. Die SALTO Zutrittskontrolle bindet neben Türen bspw. auch Tore, Zufahrten und Möbel ein. Damit lassen sich u.a. Medikamente, medizinisches Gerät, Akten oder persönliche Wertgegenstände sicher verwahren und nachvollziehbar entnehmen, oder auch die Umkleiden der Mitarbeitenden und Schränke der Bewohner zentral verwalten.

Pflegeeinrichtungen ersetzen mit den Zutrittslösungen von SALTO mechanische Schließanlagen. Auf diese Weise sparen sie Zeit und Geld, weil sie bei Schlüsselverlusten keine Schlüssel oder Zylinder teuer nachbestellen und austauschen müssen – sie können Zutrittsrechte per Mausklick zuweisen oder entziehen. Sie gewinnen darüber hinaus an Flexibilität, da eine Umnutzung von Räumen oder Bereichen nur in der Software hinterlegt werden muss und keine Arbeiten an den Türen, z.B. durch Zylindertausch, entstehen. Das reduziert den Verwaltungsaufwand erheblich und gestaltet die Wartung effizienter.

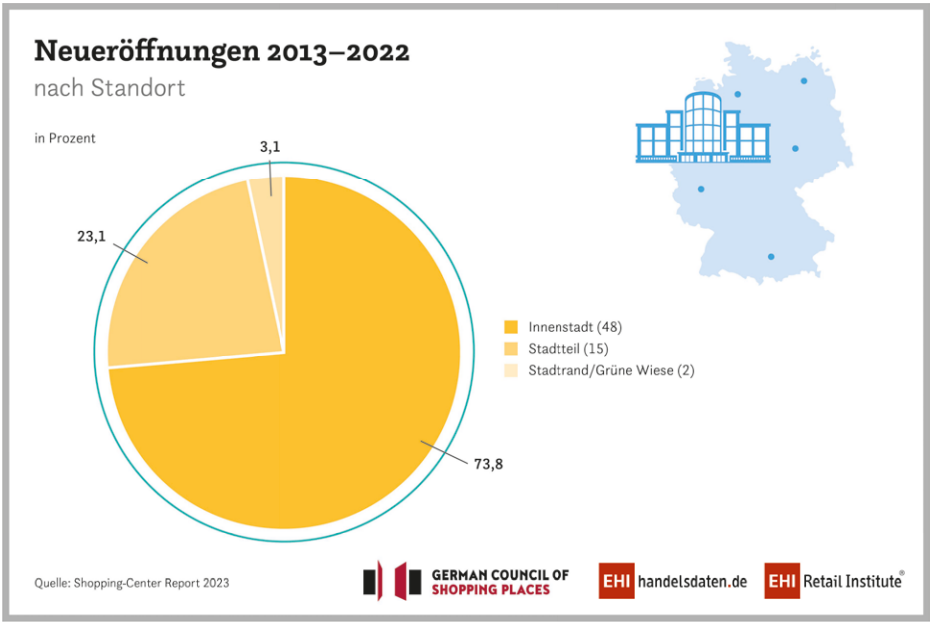
Darüber hinaus können Pflegedienstleister mit einer elektronischen Zutrittskontrolle Abläufe automatisieren, indem sie die SALTO Lösungen in Management- und IT-Systemen sowie Gebäudetechnik integrieren. Das schließt bspw. das ERP für den Stammdatenaustausch oder auch die Wäscherei für eine automatisierte Abgabe und Ausgabe der Dienstkleidung ein. Parallel trägt eine Verknüpfung mit der Licht-, Heizungs- und Jalousiensteuerung zur Senkung von Betriebskosten bei.

Infos: https://tinyurl.com/2p8btjvx

Einzelhandel

Über 500 Shopping-Center in Deutschland

EHI veröffentlicht Shopping-Center Report 2023



Entwicklung der Shopping-Center von 1965 bis 2023 in Deutschland

Jahr/Stand 01.01.	Zahl der Shopping-Center	Gesamtfläche in qm	durchschnittliche Fläche je Center in qm
1965	2	68.000	34.000
1970	14	458.800	32.800
1975	50	1.545.000	30.900
1980	65	1.956.500	30.100
1985	81	2.413.800	29.800
1990	93	2.780.700	29.900
1995	179	6.019.500	33.600
2000	279	9.212.200	33.000
2005	363	11.449.600	31.500
2010	428	13.512.000	31.600
2012	444	13.883.900	31.300
2013	453	14.266.600	31.500
2014	460	14.434.630	31.400
2015	463	14.849.090	32.100
2016	476	15.363.070	32.300
2017	479	15.446.350	32.200
2018	479	15.449.250	32.300
2019	483	15.651.000	32.400
2020	489	15.793.000	32.300
2021	493	15.916.700	32.300
2022	493	15.972.170	32.400
2023	509	16.374.584	32.200

Quelle: EHI Shopping-Center-Report 2023

GERMAN COUNCIL OF SHOPPING PLACES EHI handelsdaten.de EHI Retail Institute®

Der Markt für Handelsimmobilien durchläuft aktuell eine dynamische Phase, die von vielen notwendigen Veränderungen geprägt ist.
Seit einigen Jahren sind vermehrt Revitalisierungsmaßnahmen, Flächenumwand- lungen, Mixed-Use-Konzepte und Quartiersentwicklungen zu beobachten. „Ein Trend geht dahin, dass bisherige Handelsnutzungen durch andere Nutzungsformen ersetzt werden. Wenn großflächige Mieter ausziehen oder ihre Flächen verkleinern, ist die Suche nach geeigneten Nachmietern oft schwierig.

An vielen Standorten wird die bessere Lösung darin gesehen, solche überschüssigen Flächen beispielsweise für Fitnessstudios, medizinische Dienstleister oder Büromieter umzuwandeln", erklärt Studienautorin Lena Knopf aus dem Forschungsbereich Immobilien und Expansion.
Der EHI Shopping-Center Report 2023 zählt erstmals mehr als 500 großflächige Shopping-Center in Deutschland.

Vier Neueröffnungen in 2022

Anfang 2023 gibt es in Deutschland insgesamt 509 Shopping-Center mit einer Mindestgröße von 10.000 qm (Vorjahr: 493) – allerdings wurde die Statistik durch methodische Veränderungen bereinigt*. Alle Center zusammen verfügen über eine Gesamtfläche von 16,38 Mio. qm, was einer durchschnittlichen Fläche von 32.200 qm je Center entspricht. Im vergangenen Jahr kamen vier neueröffnete Shopping-Center hinzu: das Agnes in Göppingen, die Dreiländergalerie in Weil am Rhein, das Perlach Plaza in München sowie das Tegel-Quartier in Berlin.

Die meisten Shopping-Center befinden sich in Nordrhein-Westfalen, das mit 90 Centern 17,7 Prozent der Shopping-Center in Deutschland beheimatet. Die Top 3 der Bundesländer mit den meisten Centern komplettieren Bayern (58 Center) und Baden-Württemberg (52 Center).

Neueröffnungen meist in City-Lagen

Die meisten Shopping-Center (47,5 Prozent) liegen in Innenstädten, gefolgt von Stadtteilen (37,5 Prozent) und dem Stadtrand/Grüne Wiese (14,9 Prozent). Die Center auf der Grünen Wiese und in den Stadtteilen hatten ihre Blütezeit vor allem in den 90er Jahren, als nach der Wende in Ostdeutschland in kurzer Zeit viele große Center entstanden.

Seit den 2000er Jahren spielen diese Center jedoch kaum noch eine Rolle, da die Welle der Eröffnungen in die Innenstädte geschwappt ist. Diese hielt etwa bis zur Mitte der 2010er Jahre an und endete dann mit dem sich einstellenden Flächenüberangebot relativ abrupt. Seitdem wurden nur noch einzelne Neueröffnungen realisiert, die sich dann aber meist auf die Cities konzentrieren.

Entsprechend liegen die Neueröffnungen der letzten zehn Jahre zu rund drei Vierteln in der Innenstadt, nur 23,1 Prozent in Stadtteillagen. In diesem Zeitraum wurden nur noch zwei Center auf der Grünen Wiese bzw. in Stadtrandlage eröffnet – das LUV in Lübeck und das EEC Edingen-Neckarhäuser Einkauf Center.

*Die wichtigste Neuerung in der Definition ist, dass die Geschäfte eines Shopping-Centers nicht mehr mehrere verschiedene Branchen abdecken müssen. Nach der bisherigen Definition musste es sich bei den wichtigen Frequenzbringern in Shopping-Centern z.B. immer um Lebensmittelgeschäfte, Drogerien, große Modegeschäfte oder Elektronikmärkte handeln. Dies trifft zwar nach wie vor auf die meisten Einkaufszentren zu, ist aber per Definition keine Voraussetzung mehr. Durch die Überarbeitung der Methodik hat sich die Anzahl der Shopping-Center im EHI Shopping-Center Report verändert. So wurden zum einen bereits länger bestehende Center neu aufgenommen, zum anderen wurden Center aufgrund von Flächenreduzierungen oder Abrissen gestrichen.

Der Report ist ab Mitte Mai erhältlich und kostet 500 € (EHI-Mitglieder: 450 €) inklusive 12 Monate Zugang zur Online-Datenbank aller Shopping-Center. https://tinyurl.com/mr3x89mk

SALTO SYSTEMS

Spezialist für Gesichtserkennung übernommen

SALTO SYSTEMS hat das britische Unternehmen TouchByte, Anbieter einer Zutrittskontrolle mit Gesichtserkennung, übernommen. TouchByte ist ein Pionier auf dem Gebiet der reibungslosen Zutrittskontrolle mit fortschrittlichen Gesichtserkennungssystemen.

SALTO Systems, ein weltweit führender Anbieter innovativer intelligenter Zutrittskontrolllösungen, setzt auf den Einsatz biometrischer Technologie als die Zukunft der Zutrittskontrolle. In den letzten zwei Jahren hat das Unternehmen die Entwicklung von reibungslosen Zutrittskontrolllösungen durch verschiedene strategische Investitionen beschleunigt.
Die digitale Revolution hat die Gesellschaft verändert. Ganze Branchen haben sich neu erfunden, und unser Berufsleben, unsere Ausbildung und unsere Freizeit haben sich bis zur Unkenntlichkeit verändert. Digitale Ausweise, digitale Identitäten und Gesichtserkennung werden in allen Branchen zum Standard, wobei sich die automatische Gesichtserkennung als Schlüsseltechnologie zur Erfüllung der Marktbedürfnisse erweist.

Im Jahr 2022 übernahm SALTO Systems Cognitec, einen bedeutenden und wachsenden Akteur im Bereich der Gesichtserkennungssysteme. Dies war bereits ein bedeutender Schritt zur Verbesserung seiner Zugangskontrolllösungen durch Biometrie und die Nutzung der Gesichtserkennungstechnologie, um einen reibungslosen, intelligenten Zugang zu ermöglichen.

Durch die Integration des Flaggschiff-Algorithmus FaceVACS von Cognitec in die intelligenten Geräte von SALTO wird SALTO sein Produktportfolio um eine ganze Reihe neuer Möglichkeiten erweitern, um zusätzliche Anwendungsfälle in verschiedenen Branchen zu ermöglichen.
Jetzt ist dieser Moment näher denn je. Durch die kürzliche Übernahme von TouchByte, einem in Großbritannien ansässigen Technologie-Innovator mit Schwerpunkt auf Gesichtserkennung, beabsichtigt SALTO, die Entwicklung und Markteinführung der ersten und fortschrittlichsten Lösung für die Zutrittskontrolle mit Gesichtserkennung zu beschleunigen, indem das Potenzial des Cognitec-Algorithmus durch das Lösungsportfolio und die Gesichtsmanagement-Plattform von TouchByte realisiert wird.

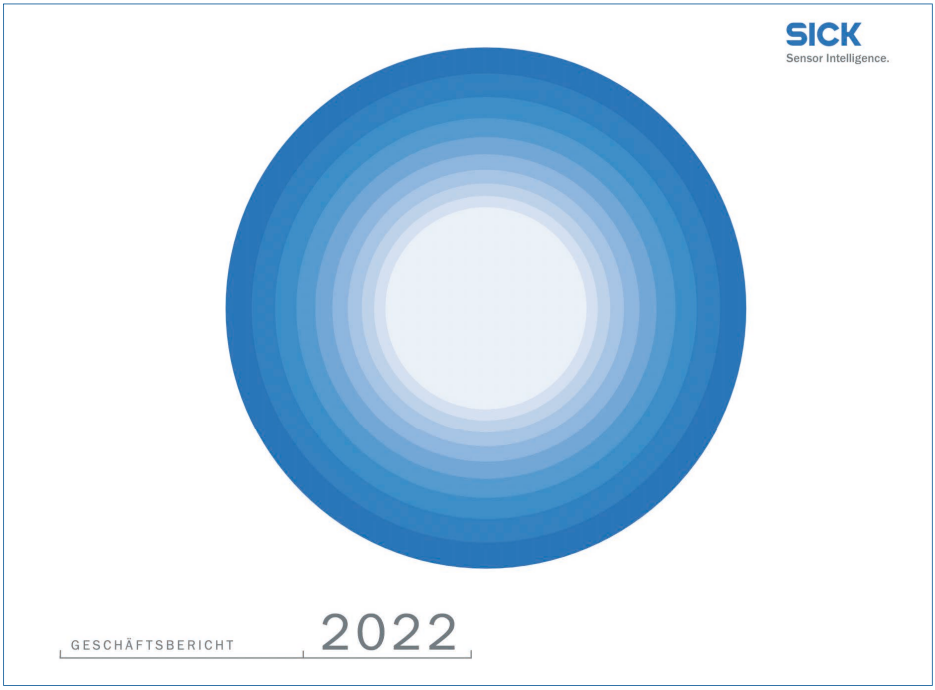
Die Aufnahme von TouchByte in die SALTO-Gruppe unterstreicht das Engagement von SALTO für Innovation und die Entwicklung neuer Technologien. "Unsere Übernahme von TouchByte ist ein natürlicher Schritt nach vorne in unserer Mission, innovative und hochmoderne Technologien auf den Zutrittskontrollmarkt zu bringen", sagte Marc Handels, Chief Technology & Innovation Officer bei SALTO Systems. "Mit unserer zukünftigen Gesichtserkennungslösung wollen wir unseren Kunden einen sicheren und reibungslosen Zugang zu ihren Gebäuden und Einrichtungen ermöglichen."

"SALTO Systems ist gespannt, was die Zukunft für die biometrische Technologie bereithält und wie sie seinen Kunden weiterhin von Nutzen sein kann."

TouchByte

Unternehmensprofil

TouchByte ist ein wachstumsstarkes Technologieunternehmen mit Sitz in Cornwall, Großbritannien, das sich auf die Entwicklung von Lösungen spezialisiert hat, die Gesichtserkennung zur Bewältigung geschäftlicher Herausforderungen nutzen. Das Unternehmen wird von einem erfahrenen Führungsteam geleitet und von einem jungen, enthusiastischen Team von Entwicklern und Support-Mitarbeitern unterstützt. Das neueste Produkt von TouchByte, Facentry, bietet eine schlüssellose Zugangskontrolle per Gesichtserkennung: "Betreten Sie einen Raum mit Ihrem Gesicht". Touchbyte glaubt an eine einfache, sichere und bequeme Zugangskontrolle, die einen effizienten Zugang zu Orten, Gebäuden und Räumen ermöglicht - ganz ohne Schlüssel, Codes, Anhänger, Karten, Armbänder oder Fingerabdruckscanner. Neben dem schlüssellosen Zugangskontrollsystem Facentry umfasst das Portfolio des Unternehmens eine webbasierte Face-Management-Plattform, eine Cloud-basierte Datenanalyse- und Sicherheitslösung sowie Benachrichtigungs- und Alarmierungssysteme.



GESCHÄFTSBERICHT

SICK AG verzeichnet Umsatzrekord und wirtschaftet solide

Umsatz erstmalig über 2 Milliarden Euro, Auftragseingang übersteigt 2,5 Milliarden Euro // Positives EBIT trotz herausfordernder Wirtschaftslage // Beschäftigtenzahl und Anzahl Patente weltweit gestiegen

Das Sensorunternehmen SICK mit Hauptsitz in Waldkirch konnte in einem herausfordernden Geschäftsjahr 2022 positive Ergebnisse verzeichnen. Mit einem Auftragseingang von 2.511 Millionen Euro sowie einem Umsatz von 2.190 Millionen Euro wurden neue Rekorde geschrieben und die hohe Nachfrage nach intelligenten Sensorlösungen für die industrielle Digitalisierung bestätigt. Das EBIT betrug 165 Millionen Euro und die gesamte Finanz- und Ertragslage zeigte sich solide. Der Umsatz wuchs in allen Regionen der Welt

ausgewogen und auch die Anzahl der Beschäftigten weltweit stieg um 8 Prozent auf 11.909. Das Unternehmen hat unverändert in seine Innovationskraft investiert und reichte 2022 erneut über 100 Patente ein, darunter mehr als 50 Prozent im Bereich Software- und KI-unterstützter Sensorlösungen.

Eine verunsicherte Weltwirtschaft in Folge des Ukrainekriegs, gestörte Lieferketten, Inflation und gestiegene Energie- und Rohstoffpreise sowie coronabedingte Einschränkungen v.a. in China bestimmten das herausfordernde Geschäftsjahr 2022. Die SICK AG erklärte die zuverlässige Lieferfähigkeit zur obersten Priorität und konnte damit die Geschäftsentwicklung positiv gestalten. Der Umsatz stieg um 11,5 Prozent auf 2.190 Millionen Euro (2021: 1.964 Millionen Euro) und überschritt somit nicht nur erstmalig die 2-Milliarden-Grenze, sondern übertraf auch die gesetzte Prognose. Zudem erhöhte sich der Auftragseingang um 8,2 Prozent auf 2.511 Millionen Euro (2021: 2.321 Millionen Euro).

Nach einem starken Geschäftsjahr 2021, das maßgeblich von Nachholeffekten nach der Corona-Pandemie bestimmt war, regulierte sich die EBIT-Marge 2022 auf einen soliden Wert von 7,5 Prozent vom Umsatz (2021: 10,3 Prozent). Das EBIT betrug somit 165 Millionen Euro und sank im Vorjahresvergleich um 18,6 Prozent, das Konzernergebnis lag bei 120 Millionen Euro (2021: 148 Millionen Euro). Die starke Erhöhung der Materialkosten (+17,3 Prozent) und sonstigen betrieblichen Aufwände (+32,2 Prozent), etwa durch Spotmarkt-Einkäufe, gestiegene Transportkosten und zusätzliche Entwicklungsaufwände, belasteten das EBIT.

Mats Gökstorp, Vorstandsvorsitzender der SICK AG

„Das Geschäftsjahr 2022 mit seinen angespannten Beschaffungsmärkten stellte die Wirtschaft und auch unser Unternehmen vor zahlreiche Herausforderungen, vor allem die hohen Kosten belasteten die Profitabilität. Im Namen des gesamten Vorstandes möchte ich mich bei allen SICK-Beschäftigten bedanken, die mit viel persönlichem Einsatz täglich neue Hürden genommen und im Sinne unserer Kunden flexible und kreative Lösungswege gefunden haben. Unser Fokus lag auf der Sicherstellung der Lieferfähigkeit und Aufrechterhaltung der Kundenbeziehung bei gleichzeitigem Kostenbewusstsein. Diesen Ansatz werden wir auch 2023 weiterverfolgen und die erfreuliche Nachfrage nach Sensoren und digitalen Lösungen mit unverändert hoher Innovationskraft bedienen“, sagte Dr. Mats Gökstorp, Vorstandsvorsitzender der SICK AG.

Rahmenbedingungen in der Sensorikindustrie

Die Entwicklung der Sensorikindustrie im Geschäftsjahr 2022 war nach Angaben des deutschen Branchenverbands der Sensorik und Messtechnik AMA e.V., positiv. Obwohl die wirtschaftlichen und politischen Unsicherheiten die Sensorikindustrie nicht

SICK

Vorstandswechsel - Finanzvorstand Markus Vatter gibt nach 17 Jahren Vorstandsamt ab

Die SICK AG, internationales Sensorunternehmen mit Hauptsitz in Waldkirch bei Freiburg, hat Veränderungen im Vorstand angekündigt: Markus Vatter, Vorstand Finance & IT bei der SICK AG, wird sein Vorstandsamt nach 17 Jahren spätestens zum Jahreswechsel niederlegen, um sich auf seine Aufgaben in verschiedenen Aufsichtsratsgremien zu konzentrieren. Zugleich teilte das Unternehmen mit, dass Jan-Helmut Eberhardt vom Aufsichtsrat in den Vorstand der SICK AG berufen wurde. Eberhardt wird die Vorstandsarbeit im Ressort Finance & IT nahtlos weiterführen.

Markus Vatter

Alle Fotos: ©SICK

Jan-Helmut Eberhardt

ausklammern, konnte der Umsatz im dritten Quartal 2022 im Vergleich zum Vorjahresquartal um 10 Prozent wachsen. Die hohe Nachfrage nach Sensorlösungen für industrielle Anwendungen schlägt sich auch in der SICK-Bilanz nieder. So war das Umsatzwachstum in allen drei Geschäftsbereichen Fabrikautomation (+12 Prozent), Logistikautomation (+12 Prozent) und Prozessautomation (+10 Prozent) ausgewogen. Die globalen Anstrengungen für eine bessere Nutzung begrenzter Ressourcen machen sich im steigenden Automatisierungsgrad in der Industrie bemerkbar, wofür SICK seit seiner Firmengründung 1946 technologische Lösungen entwickelt.

Gleichgewichtiges Wachstum auf allen globalen Märkten

In seinem Heimatmarkt Deutschland erreichte SICK mit einem Anstieg von 12 Prozent auf 365 Millionen Euro (2021: 326 Millionen Euro) einen neuen Umsatzrekord, konnte aufgrund der gestörten Lieferketten jedoch nicht den gesamten Auftragsbestand zum Jahresabschluss 2022 in Umsatz umwandeln. Die Anzahl der Beschäftigten wuchs an den deutschen Standorten auf insgesamt 6.750 (+ 7 Prozent). Insbesondere in den operativen Produktionsbereichen sowie in Forschung und Entwicklung, Vertrieb und Service wurden neue Mitarbeitende eingestellt.

In der Region Europa, Naher Osten und Afrika (EMEA) konnte der Umsatz um 8 Prozent auf 734 Millionen Euro gesteigert werden und übertraf die prognostizierten Werte. Diese positive Entwicklung spiegelt sich in vielen Ländern wider – besonders hervorzuheben sind große europäische Märkte wie Italien und die Niederlande. Die Beschäftigtenzahl wuchs um 6 Prozent auf 2.260 in der Region EMEA. Das Umsatzwachstum in Nord-, Mittel- und Südamerika (Americas) von 13 Prozent auf 509 Millionen Euro ergab sich insbesondere in den Geschäftsfeldern der Fabrik- und Prozessautomation und wurde durch die Währungseffekte positiv beeinflusst. Die Zahl der Mitarbeiterinnen und Mitarbeiter stieg um 10 Prozent auf 1.171. In der Region Asien-Pazifik verlief das Wachstum erneut dynamisch und betrug im Geschäftsjahr 2022 13,9 Prozent. Der Umsatz von 583 Millionen Euro wurde, insbesondere auf dem chinesischen Markt, durch die positiv wirkenden Wechselkurse unterstützt. 1.728 Beschäftigte sind für SICK in Asien-Pazifik tätig und somit 13 Prozent mehr als im Vorjahr. Die Währungseffekte hatten im Geschäftsjahr 2022 einen leicht positiven Einfluss auf die Entwicklung des Konzernumsatzes.

SICK-Lösungen für die industrielle Digitalisierung

SICK hat an seiner Innovationsstrate-

gie festgehalten und auch im Geschäftsjahr 2022 mit 241 Millionen Euro 11 Prozent des Umsatzes in Forschung und Entwicklung investiert. Das Unternehmen fokussiert sich auf die Möglichkeiten der Sensorintelligenz, mit dem SICK die Basis für die Steuerung digitaler und automatisierter industrieller Prozesse sowie den Schutz von Menschen und Umwelt mit Sensortechnologie legt. 2022 führte SICK dabei seine Entwicklung hin zum Anbieter von Komplettlösungen mit Sensorprodukten, Systemen, Software, künstlicher Intelligenz und Dienstleistungen weiter. SICK hat im vergangenen Geschäftsjahr 122 Patente angemeldet (+35 Prozent zum Vorjahr), wobei über die Hälfte den Bereichen Software und Künstliche Intelligenz zuzuordnen sind. Mit der Vernetzungsfähigkeit der Sensorik und Datensouveränität stets im Blick, ist SICK ein wichtiger Technologiepartner für die Digitalisierung der Industrie.

Eine herausragende Produktinnovation 2022 ist der kamerabasierte Codeleser Lector85x mit integrierter Software- und KI-Unterstützung. Dank 12,4 Megapixel-Bildchip und hoher Rechenleistung können Codes bei Geschwindigkeiten bis 3,5 m/s sicher identifiziert werden. Eingesetzt wird der Codeleser etwa in Logistikzentren oder in der Fluggepäcksortierung.

Die Möglichkeiten der Augmented Reality in der Fertigung setzt SICK bei seiner 2022 veröffentlichten SARA App ein: Der SICK Augmented Reality Assistant verbindet – als eine der ersten Lösungen dieser Art im industriellen Umfeld – Sensordaten und reale Umgebungen und visualisiert dadurch Prozess- und Diagnoseinformationen direkt auf dem Shopfloor. Die AR-App hilft dem Personal vor Ort bei der Parametrierung und der Diagnose von Sensoren. Auch im Bereich der Energiewende hat SICK 2022 diverse Produkte zur Marktreife geführt, darunter etwa den FLOWSIC500: Der Ultraschall-Gasdurchflusszähler ist nun in der Lage, auch Wasserstoffbeimischungen zuverlässig und sicher zu messen. Bestehende Anlagen können somit für den wichtigen Energieträger Wasserstoff aufgerüstet und zukunftssicher gemacht werden.
Wichtiger Teil der Innovationsstrategie von SICK sind die konzerninternen Start-ups, die 2022 nach einem „Business Idea Pitch" und Auswahlverfahren durch sechs weitere Start-ups ergänzt wurden. Die Start-ups erproben neue Marktchancen gezielt und mit schnellem Kundenfeedback. So sind Themen wie hyperspektrale Bildverarbeitung und Neuromorphing keine Zukunftsmusik, sondern wirken über die SICK Start-ups schon heute auf Produktentwicklungen ein.

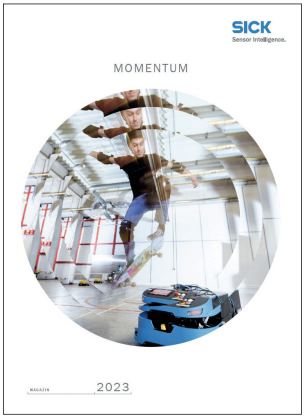
Nachhaltigkeit umfassend gedacht

SICK hat im Geschäftsjahr 2022 seine ganzheitliche Nachhaltigkeitsstrategie in den Handlungsfeldern „Environmental, Social & Governance (ESG)" konsequent weiterverfolgt und gesetzte Ziele erreicht. Das Nachhaltigkeitsverständnis von SICK umfasst die unternehmerische Verant- wortung für Mitarbeitende, die Umwelt, den wirtschaftlichen Erfolg und die Gesellschaft. Im Bereich Klima und Umwelt möchte SICK u.a. jährlich 0,5 Prozent des Vorjahresenergieverbrauchs reduzieren, was durch diverse Effizienzmaßnahmen 2022 gelungen ist. An seinen deutschen Standorten bezieht das Unternehmen bereits seit zehn Jahren ausschließlich Ökostrom und wird dies bis 2025 auch auf seine globalen Standorte ausweiten. Als Anbieter digitaler Sensorlösungen analysiert SICK zudem, welche Energieeinsparungspotenziale in seiner IT-Infrastruktur liegen und hat dazu 2022 ein Gesamtkonzept erstellt.

Der Schlüssel des unternehmerischen Erfolgs liegt bei seinen Beschäftigten, für die SICK ein attraktiver Arbeitsplatz für Heute und auch Morgen sein möchte. 2022 hat SICK die „Charta der Vielfalt" unterzeichnet und damit seinem Anliegen, Vielfalt und Wertschätzung in allen Bereichen zu fördern, ein sichtbares Zeichen gesetzt. Darüber hinaus wurde mit „MentalHealth@SICK" ein Projekt initiiert, um mentale Gesundheit nachhaltig in den Berufsalltag zu implementieren sowie das Thema „psychische Gesundheit" zu entstigmatisieren. Neben der Mitarbeitendengesundheit haben auch Ausbildung und lebenslanges Lernen seit Firmengründung einen hohen Stellenwert. Über 82.000 Schulungen wurden über die unternehmensinterne SICK Sensor Intelligence Academy (SIA) durchgeführt, 373 Auszubildende wurden im vergangenen Jahr für die industrielle Digitalisierung bei SICK qualifiziert.

2022 wurde SICK zum 20. Mal in Folge bei einer anonymen Befragung als „Great Place to Work"® Deutschland ausgezeichnet. „Alles in allem ist dies ein sehr guter Arbeitsplatz" – diese Aussage bestätigten 91 Prozent der befragten SICK-Mitarbeitenden.
Auch SICK-Gesellschaften in den USA,

Schweden und Indien wurden für ihre Arbeitsplatzkultur als „Great Place to Work" ® ausgezeichnet.
Im Bereich der unternehmerischen Governance hat SICK 2022 Vorkehrungen getroffen, um die im Lieferkettensorgfaltspflichtengesetz festgehaltenen Pflichten zu erfüllen. Dies beinhaltet insbesondere die Einrichtung eines Risikomanagements zur Einhaltung der menschenrechts- und umweltbezogenen Sorgfaltspflichten im Hinblick auf den eigenen Geschäftsbereich sowie die unmittelbaren und mittelbaren Zulieferer von SICK. Bereits 2021 wurde eine „Integrity Line" installiert, mit der Compliance-Verstöße anonym gemeldet werden können, um so das Unternehmen vor Schaden zu bewahren und das Vertrauen der Mitarbeiterinnen und Mitarbeiter sowie der Geschäftspartner in die Werte von SICK zu erhalten.



Detaillierte Bilanzinformationen sowie Angaben zu den Nachhaltigkeitszielen der SICK AG finden Sie im Geschäfts- und Nachhaltigkeitsbericht 2022:
www.sick.com/momentum

SICK

40.000 Asset Administration Shells

Standardisierte Informationen von über 40.000 SICK Sensoren stellt die SICK AG Kunden und Partnern kostenlos in Form von Verwaltungsschalen (Asset Administration Shells, AAS) zur Verfügung. Pünktlich zur Hannover Messe 2023 – dem Knotenpunkt für die Industrie – gab die SICK AG bekannt, dass sie über 40.000 AAS zur Verfügung stellt, die den Standard der Industrial Digital Twin Association (IDTA) erfüllen. Somit können wichtige Informationen von über 40.000 SICK Sensoren standardisiert und effizient von Kunden und Partnern integriert und weiterverwendet werden. Der Sensorhersteller unterstützt jetzt bereits das Submodell „Digital Nameplate" und arbeitet an weiteren Teilmodellen, um den Sensor entlang des gesamten Produktlebenszyklus digital abzubilden und dadurch die Digitalisierung in der Industrie voranzutreiben.
Als Anbieter für Sensorlösungen ist die SICK AG von der ersten Stunde Teil digitaler Ökosysteme und erkannte frühzeitig die Relevanz eines offenen Umgangs mit Sensorinformationen. SICK unterstützt daher die wesentlichen Komponenten industrieller digitaler Wertschöpfungsketten.

Dazu gehören u. a. Datenräume über die International Data Spaces Association (IDSA). Vor diesem Hintergrund unterstützt SICK nun auch Manufacturing-X, eine Initiative der vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) moderierten Plattform Industrie 4.0, um globale Akteure unternehmensübergreifend zu durchgängigen Wertschöpfungsketten zu vernetzen und einen standardisierten, globalen Datenaus- tausch zu ermöglichen. Die Verwaltungsschale mit sogenannten Sub- oder Teilmodellen stellt hierfür eine wichtige Grundlage dar. Sie hält relevante Informationen des Produktes im virtuellen Raum bereit und ermöglicht Anwendungen im Sinne der Industrie 4.0 sowie die Umsetzung des Digitalen Zwillings. Die Nutzer profitieren von geringeren Aufwänden bei der Bereitstellung, beim Design-In sowie bei Wartung und Dokumentation von Sensoren in ihren industriellen Anwendungen.

Der AssetHub ist ein digitales, webbasiertes Enterprise Asset Management (EAM) System, das eine interaktive Sicht sowohl auf einzelne Sensoren und Maschinen als auch auf Gesamtanlagen erzeugt. Zukünftig werden Verwaltungsschalen auch über die Website SICK.com bereitgestellt.

Umfrage

Cyberkriminelle schalten den Turbo ein und bringen Unternehmen an ihre Grenzen

Die Lage der Cybersicherheit in Unternehmen kann in einem Satz beschrieben werden: Während die Cyberkriminellen mit dem Supersportwagen unterwegs sind, versuchen Unternehmen oftmals, mit der der getunten Mittelklasselimousine mitzuhalten. Sprich: Die Angreifer werden immer schneller, und die angegriffenen Unternehmen können nicht mithalten.

Die aktuelle Studie "The State of Cybersecurity 2023: The Business Impact of Adversaries on Defenders" zeigt, dass die heutige Realität ein Cybersicherheitssystem der zwei Geschwindigkeiten ist, in dem sich Angreifer und Verteidiger mit unterschiedlichem Tempo bewegen. Die Angreifer beschleunigen und erweitern durch Maßnahmen wie Automatisierung, "as-a-Service"-Modelle für Cyberkriminalität, verdeckte Identitätswechsel und weitere Anpassungen stetig ihren Aktionsradius und können eine breite Palette ausgeklügelter Angriffe in großem Umfang durchführen.

Reaktionszeiten von bis zu 15 Stunden plus Fehlkonfigurationen sind Hauptrisiken

Auf der anderen Seite können die Verteidiger – gehandicapt durch einen Mangel an Fachwissen, eine überwältigende Anzahl von Warnungen und zu viel Zeit, die für die Reaktion auf Vorfälle aufgewendet werden muss – nicht mithalten.

Die meisten Unternehmen haben Schwierigkeiten bei der Erkennung von und Reaktion auf Bedrohungen. 93 % der Befragten bewerten die Durchführung grundlegender Sicherheitsaufgaben als schwierig. Die Aufarbeitung von Sicherheitswarnungen ist dabei ein weit verbreitetes Problem. Im Durchschnitt wird nur knapp die Hälfte (48 %) aller Warnmeldungen untersucht, um festzustellen, ob es sich um Anzeichen für bösartige Aktivitäten handelt.

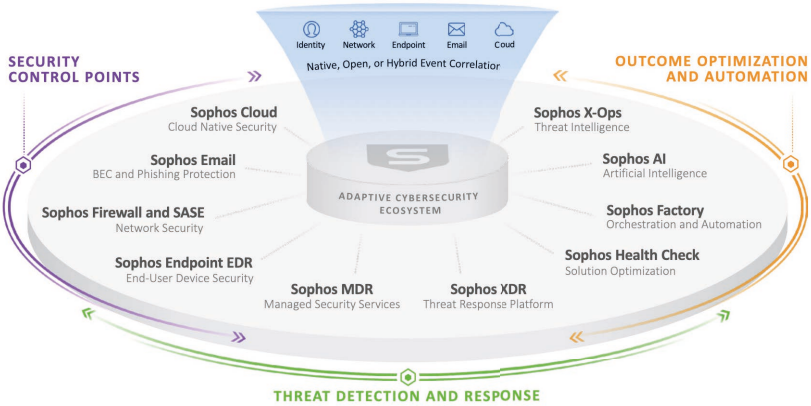
Die meisten Unternehmen tun sich außerdem schwer, die zu untersuchenden Warnmeldungen bzw. Ereignisse zu identifizieren und zu priorisieren (71 %).

Bei Unternehmen mit 100 bis 3.000 Mitarbeitern dauert der gesamte Erkennungs-, Untersuchungs- und Reaktionsprozess im Durchschnitt neun Stunden, bei Unternehmen mit 3.001 bis 5.000 Mitarbeitern sogar 15 Stunden.

In operativer Hinsicht fehlt es den Verteidigern an Vertrauen in ihre Prozesse, wobei die Fehlkonfiguration von Sicherheitstools als das am häufigsten benannte Sicherheitsrisiko im Jahr 2023 gilt.
Mehr als die Hälfte (52 %) der IT-Fachleute gibt an, dass Cyberbedrohungen für ihr Unternehmen inzwischen zu weit fortgeschritten sind, um sie allein bewältigen zu können. Bei kleinen Unternehmen (100-250 Mitarbeiter) sind es sogar 64 %.

The State of Cybersecurity 2023: The Business Impact of Adversaries

Achieve Optimal Cybersecurity Outcomes with Sophos



Schlaflose Nächte und zu viel Zeit für die Bewältigung von Bedrohungen

Diese Situation bedeutet für Firmen finanzielle, betriebliche und ressourcenbezogene Folgen, wobei die Auswirkungen des Systems der zwei Geschwindigkeiten erheblich sind und das gesamte Unternehmen betreffen. So sind die direkten finanziellen Auswirkungen eines Cybervorfalls enorm und bereits gut bekannt: Die durchschnittlichen Kosten für ein kleines oder mittelgroßes Unternehmen zur Behebung eines Ransomware-Angriffs belaufen sich auf 1,4 Millionen US-Dollar. Diese Kosten für die Beseitigung von Vorfällen sind jedoch nur ein Teil der gesamten Wahrheit.

Denn auch die Kapazität für die Bereitstellung anderer IT-Programme ist eingeschränkt: 55 % der Befragten gaben an, dass die Bewältigung von Cyberbedrohungen die Arbeit des IT-Teams an anderen Projekten beeinträchtigt hat.

Auch den geschäftsorientierten Bemühungen steht die Cybersicherheit durch ihre Dringlichkeit und Unvorhersehbarkeit im Weg: 64 % wünschen sich, dass das IT-Team mehr Zeit für strategische Fragen und weniger Zeit für die Bekämpfung von Vorfällen aufwenden könnte.

Die lange Zeit, die für die Erkennung, Untersuchung und Behebung von Sicherheitswarnungen aufgewendet wird, hat zudem beträchtliche finanzielle Auswirkungen in Bezug auf die Ressourcenkosten.

Und es zeigt sich, dass diese Situation auch für die Mitarbeiter eine große Belastung darstellt. 57 % der IT-Fachleute geben an, dass die Sorge, das Unternehmen könnte von einem Cyberangriff betroffen sein, sie manchmal nachts wachhält. Bei Unternehmen mit 3.001 bis 5.000 Mitarbeitern sind es sogar 65 %.

Angesichts der hohen Kosten für die Rekrutierung, Schulung und Bindung von Mitarbeitern in diesem Bereich stellen all diese Auswirkungen zusätzliche Herausforderungen und Kosten für das Unternehmen dar.

Autor: Joe Levy, President der Sophos Technology Group (STG)

Vollständiger Report Download: https://tinyurl.com/2j7zrjrk

8com

LockBit-Ransomware bereitet Angriffe auf Apple vor

Über Ransomware mussten sich die Nutzer von Apple-Geräten bislang weit weniger Gedanken machen als Windows-Nutzer. Mit einer neuen Variante von LockBit könnte sich das jetzt ändern.

Die Hintermänner der berüchtigten LockBit-Ransomware haben ihre Malware offenbar weiterentwickelt und eine neue Variante in Umlauf gebracht, die es auf Apple-Computer abgesehen hat. Dabei dürfte es sich um das erste Mal handeln, dass eine der bekannten Ransomware-Operationen ganz gezielt auf Macs ausgerichtet ist. Entdeckt wurde die Malware von den Sicherheitsforschern von MalwareHunterTeam, als sie ein ZIP-Archiv auf VirusTotal fanden, das offenbar die meisten der aktuell verfügbaren LockBit-Verschlüsselungen enthielt. Neben den bislang bekannten Versionen für Angriffe auf Windows-, Linux- und VMware ESXi-Server, fanden die Sicherheitsforscher auch bisher unbekannte Verschlüsselungsprogramme für macOS-, ARM-, FreeBSD-, MIPS- und SPARC-CPUs. Dabei sind nicht nur ältere Macs betroffen, sondern auch neuere, die bereits mit Apple Silicon laufen.
Eine weitergehende Untersuchung der gefundenen Daten ergab, dass einzelne Dateien bereits im Dezember 2022 bei VirusTotal hochgeladen wurden. Es ist also davon auszugehen, dass die Bedrohung schon seit einiger Zeit besteht, auch wenn es sich wohl derzeit nur um eine Testversion handelt. Auch das Magazin Blee-

Account Takeover: Wenn Identitätsdiebstahl richtig teuer wird

Für Cyberkriminelle sind Account-Takeover-Attacken (ATO) eine sehr effektive Methode, um Online-Unternehmen mit Kundenkontakt anzugreifen. Diese Angriffsformen sind skalierbar und versprechen den Kriminellen einen hohen finanziellen Gewinn. Eine aktuelle Studie des Researchunternehmens Aberdeen im Auftrag der auf sichere Login-Lösungen spezialisierten Nevis Security AG zeigt, dass die Folgen erfolgreicher Kontoübernahmen erschreckende Ausmaße angenommen haben. Die finanziellen Schäden gehen weit über die reinen Geschäftskosten hinaus und werden so zu einem existenziellen Risiko für betroffene Unternehmen.

Hauptursachen für erfolgreiche Kontoübernahmen sind, dass Menschen heute unzählige Onlinekonten benutzen und die Art, wie sie die dafür erforderlichen Credentials verwalten. So besitzt der durchschnittliche Nutzer bis zu 130 digitale Benutzerkonten, für die jeweils ein Passwort erforderlich ist. Bei dieser Anzahl ist es nicht verwunderlich, dass die User durchschnittlich zwölf Tage ihres Lebens damit verbringen, nach den richtigen Benutzernamen und Passwörtern zu suchen.
„Die daraus resultierende Frustration der Nutzer führt zu weiteren Sicherheitsproblemen, denn sie wollen es sich so einfach wie möglich machen", erklärt Stephan Schweizer, CEO von Nevis: „Die beliebtesten Passwörter sind nach wie vor „abc123", „password" und die Zahlenkombination „123456". Zudem haben die meisten Passwörter weniger als die empfohlene Mindestlänge von zehn Zeichen und mehr als die Hälfte der Nutzer verwendet das gleiche Passwort für mehrere Accounts."
Cyberkriminelle profitieren von diesem laxen Umgang mit Passwörtern. Er macht es ihnen leichter, in digitale Kundenkonten einzudringen und diese zu übernehmen. Nevis hat die

pingComputer analysierte das LockBit-Verschlüsselungsprogramm für Apple M1 und fand Zeichenfolgen, die in einem macOS-Verschlüsselungsprogramm eigentlich fehl am Platz sind. Beispielsweise gibt es zahlreiche Verweise auf VMware ESXi, das in einem Apple M1-Verschlüsselungsprogramm nichts zu suchen hätte, da VMware angekündigt hat, die CPU-Architektur nicht zu unterstützen. Das legt die Vermutung nahe, dass diese Version wahrscheinlich für einen Test erstellt wurde. Darüber hinaus ist eine Liste von 65 Dateierweiterungen und Dateinamen enthalten, die von der Verschlüsselung ausgeschlossen werden, wobei es sich bei allen um Windows- und nicht um Mac-Dateierweiterungen und -ordner handelt. Die gute Nachricht lautet daher: Allzu viel Angst vor unmittelbar bevorstehenden Angriffen mit LockBit auf Apple-Geräte müssen Nutzer noch nicht haben. Die gefundenen Daten deuten nicht darauf hin, dass die Mac-Version von LockBit bereits einsatzbereit ist. Doch es zeigt auch: Apple-Produkte sind ins Visier von Hackern geraten und es ist nur noch eine Frage der Zeit, bis es auch hier zu Angriffen kommt. Daher sollten sich alle Computerbenutzer, einschließlich Mac-Nutzer, grundlegende Verhaltensweisen angewöhnen, die das Risiko von Hacker- und Malware-Angriffen minimieren. Dazu gehört es, das Betriebssystem zu aktualisieren, das Öffnen unbekannter Anhänge und ausführbarer Dateien zu vermeiden und Offline-Back-ups zu erstellen. Die Verwendung sicherer und einzigartiger Passwörter für jeden verwendeten Online-Dienst sollte ohnehin selbstverständlich sein.

fünf erfolgreichsten Angriffsmethoden identifiziert, die im schlimmsten Fall zu einem Account Takeover führen können:

1. Phishing und Social Engineering: Mit über 17 Prozent ist dies die vierthäufigste Angriffsart. Die Hakker nutzen dabei das Vertrauen der User in die vermeintlichen Absender aus. Dabei setzen sie längst nicht mehr nur auf E-Mails und SMS, um an die Kontodaten zu gelangen, sondern manipulieren die Nutzer zunehmend auch über Telefonanrufe.

2 .Brute-Force-Angriffe: Mit über 18 Prozent Häufigkeit liegt diese Angriffsmethode auf Platz 3. Die Cyberkriminellen verwenden dafür Tools, mit denen sie Zugangsdaten automatisiert ausprobieren können. Diese Angriffsart ist erfolgversprechend, weil oft nicht so komplizierte und variable Passwörter zum Einsatz kommen, wie es Sicherheitsexperten empfehlen.

3. Keylogger-Angriffe: Bei dieser Methode verwenden Kriminelle Hard- oder Software, um Tastatureingaben nachzuvollziehen. Auf diese Weise können Buchstaben- und Zahlenkombinationen aufgezeichnet und Login-Daten rekonstruiert werden.

4 .Man-In-The-Middle-Angriff: Bei dieser Art von Attacke schaltet sich ein Mittelsmann zwischen die Übertragung zweier Kommunikationsnetze und kann so die Verschlüsselungen umgehen. Der Angreifer hat dann Zugriff auf verschiedene Daten, zum Beispiel Benutzername und Passwort.

5. Credential Stuffing: Die Cyberkriminellen greifen auf Zugangsdaten zurück, die nach einer Datenpanne öffentlich geworden sind oder im Dark Web gekauft wurden. Via Bots starten sie dann massenhafte Loginversuche bei anderen Online-Diensten. Da Nutzer oft dieselben Zugangsdaten für mehrere Konten verwenden, stehen die Chancen gut, dass es den Angreifern gelingt, einen anderen Account zu übernehmen. Angriffe über Credential Stuffing bleiben oft unentdeckt, da sich bei der Account-Übernahme ein „legitimer" Kunde einloggt.

Die Folgen einer erfolgreichen Kontoübernahme sind weitreichend: Betrügerische Einkäufe, der Diebstahl von Dienstleistungen oder auch die Registrierung neuer Konten durch kriminelle Nutzer, beispielsweise für Kreditanträge, gehören dazu.

„Um die Risiken beim Login und damit in puncto Account Takeover zu reduzieren, müssen Passwörter als Schwachstellen minimiert werden. Biometrische Verifikationsverfahren tragen nicht nur zu einer sicheren, sondern auch zu einer reibungslosen Kundenerfahrung bei.

Statt des ewigen Katz- und Maus-Spiels mit den Cyberkriminellen, ist es wichtig, dass Unternehmen vermehrt auf die passwortlose Authentifizierung setzen", so Schweizer abschließend.

Ransomware

ExtraHop-Bericht zeigt, dass 83 % der Unternehmen bei Ransomware-Angriffen gezahlt haben

Daten decken Zusammenhang zwischen Versäumnissen im Bereich Cybersecurity und Ransomware-Vorfällen auf

ExtraHop, Anbieter von cloudbasierter Networkdetection and Response (NDR), hat heute den Global Cyber Confidence Index 2023 veröffentlicht. Die Studie mit dem Titel „Versäumnisse bei Cybersecurity erhöhen Kosten und Ransomware-Risiken" zeigt einen Zusammenhang zwischen den Versäumnissen bei der Cybersecurity und erhöhter Anfälligkeit für Cybersecurity-Vorfälle, einschließlich Ransomware, bei Unternehmen auf der ganzen Welt.

Die Studie, die die Methoden von IT-Führungskräften hinsichtlich Cybersecurity mit der Realität der Angriffslandschaft vergleicht, ergab, dass Unternehmen einen erheblichen Anstieg von Ransomware erlebten - von durchschnittlich vier Angriffen innerhalb von fünf Jahren im Jahr 2021 zu vier Angriffen innerhalb eines Jahres im Jahr 2022. Von denjenigen, die Opfer von Ransomware wurden, gaben 83 % zu, mindestens einmal das Lösegeld bezahlt zu haben.
Da Unternehmen zunehmend angegriffen werden, haben die Daten ergeben, dass sie zunehmend unter ihren Versäumnissen bei der Cybersecurity leiden - nicht behobene Sicherheitsschwachstellen wie ungepatchte Software, nicht verwaltete Geräte, Schatten-IT und unsichere Netzwerkprotokolle, die als Zugangspunkte für bösartige Akteure dienen. Zu den wichtigsten Ergebnissen des Berichts gehören:

Veraltete Praktiken sind schuld

Mehr als drei Viertel (77 %) der IT-Entscheidungsträger geben an, dass veraltete Cybersicherheitspraktiken zu mindestens der Hälfte der Cybersicherheitsvorfälle in ihrem Unternehmen beigetragen haben. Trotz dieser besorgniserregenden Zahlen gaben weniger als ein Drittel der Befragten an, dass sie unmittelbare Pläne zur Behebung der veralteten Sicherheitspraktiken haben, die ihr Unternehmen gefährden.

Es mangelt an grundlegender Cyber-Hygiene

98 % der Befragten verwenden ein oder mehrere unsichere Netzwerkprotokolle, ein Anstieg von sechs Prozent im Vergleich zu 2021. Trotz der Aufforderung führender Technologieanbieter, SMBv1 aus dem Verkehr zu ziehen, das eine wichtige Rolle bei der Ausbreitung von WannaCry und NotPetya gespielt hat, verwenden 77 % dieses Protokoll noch immer in ihren Unternehmen.
Wenn es um nicht verwaltete Geräte geht, geben 53 % an, dass auf einige ihrer kritischen Geräte aus der Ferne zugegriffen werden kann und sie remote kontrolliert werden können. Weitere 47 % sagen, dass ihre kritischen Geräte dem öffentlichen Internet ausgesetzt sind.

Das Vertrauen in die Cloud-Sicherheit nimmt zu

In dem Maße, in dem Unternehmen geschäftskritische Anwendungen und sensible Daten in die Cloud verlagern, ist die Notwendigkeit, Cloud-Workloads zu überwachen, zunehmend relevant. Mit einem größeren Fokus auf ihre Cloud-Umgebungen gaben 72 % der Befragten an, dass sie vollständig oder größtenteils Vertrauen in die Sicherheit der Cloud-Workloads ihres Unternehmens haben.

"Es ist nicht verwunderlich, dass IT- und Sicherheitsteams angesichts von Personalknappheit und schrumpfenden Budgets einige der grundlegenden Cybersicherheitsanforderungen, die vielleicht etwas banaler oder ent-

behrlicher erscheinen, zurückstellen", so Mark Bowling, Chief Risk, Security und Information Security Officer bei ExtraHop.
"Die Wahrscheinlichkeit eines Ransomware-Angriffs verhält sich umgekehrt proportional zur Größe der nicht geschützten Angriffsfläche, was ein Beispiel für ein Versäumnis im Bereich der Cybersicherheit ist. Die Verbindlichkeiten und letztlich auch die finanziellen Schäden, die aus dieser mangelnden Priorisierung resultieren, verschlimmern die Cybersecurity auf Grund der bisherigen Versäumnisse und erhöhen die Risiken für Unternehmen. Ein besserer Einblick in das Netzwerk mit einer NDR-Lösung kann dazu beitragen, den wahren Ist-Zustand zu darzustellen und die dringendsten Schwachstellen zu beleuchten, so dass sie ihre bisherigen Versäumnisse in Sachen Cybersecurity besser in den Griff bekommen können."

Global Cyber Confidence Index 2023 herunter: Cybersecurity Debt Drives Up Costs and Ransomware Risk zum Download:

www.extrahop.com/resources/papers/cyber-confidence-index-2023/

State of Ransomware '23

- **Datenverschlüsselung durch Ransomware erreicht den höchsten Stand seit vier Jahren, so der jährliche Sophos State of Ransomware Report**
- **Die Zahlung des Lösegelds verdoppelt die Wiederherstellungskosten**
- **Die Zahl der Ransomware-Angriffe bleibt konstant: 66% der befragten Unternehmen gaben an, Opfer von Ransomware geworden zu sein**

Sophos, Anbieter von Innovationen und Cybersecurity-as-a-Service, hat heute seinen jährlichen "State of Ransomware 2023"-Report veröffentlicht, in dem festgestellt wird, dass es Angreifern in 76% der Ransomware-Angriffe auf befragte Unternehmen gelungen ist, Daten zu verschlüsseln. Dies ist die höchste Rate an Datenverschlüsselung durch Ransomware, seit Sophos den Report im Jahr 2020 veröffentlicht hat.

Die Studie zeigt auch, dass Unternehmen, die Lösegeld für die Entschlüsselung ihrer Daten zahlten, ihre Wiederherstellungskosten verdoppel-

ten (750.000 US-Dollar Wiederherstellungskosten im Vergleich zu 375.000 US-Dollar für Unternehmen, die Backups zur Datenwiederherstellung verwendeten). Außerdem bedeutete die Zahlung des Lösegelds in der Regel eine längere Wiederherstellungszeit: 45 % der Unternehmen, die Backups verwendeten, konnten die Daten innerhalb einer Woche wiederherstellen, verglichen mit 39 % der Unternehmen, die das Lösegeld zahlten.

Insgesamt wurden 66 % der befragten Unternehmen von Ransomware angegriffen - der gleiche Prozentsatz wie im Vorjahr. Dies deutet darauf hin, dass die Rate der Ransomware-Angriffe trotz eines vermeintlichen Rückgangs der Angriffe konstant geblieben ist.

"Die Verschlüsselungsraten sind nach einem vorübergehenden Einbruch während der Pandemie wieder auf ein sehr hohes Niveau angestiegen, was sicherlich besorgniserregend ist. Ransomware-Crews haben ihre Angriffsmethoden verfeinert und ihre Angriffe beschleunigt, um die Zeit zu verkürzen, in der die Verteidiger ihre Pläne durchkreuzen können", sagt Chester Wisniewski, Field CTO, Sophos.

"Die Kosten eines Vorfalls steigen erheblich, wenn Lösegeld gezahlt wird. Die meisten Opfer werden nicht in der Lage sein, alle ihre Dateien wiederherzustellen, indem sie einfach die Verschlüsselungsschlüssel kaufen; sie müssen auch ihre Backups wiederherstellen. Die Zahlung von Lösegeld bereichert nicht nur die Kriminellen, sondern verlangsamt auch die Reaktion auf den Vorfall und erhöht die Kosten in einer bereits verheerenden Situation", so Wisniewski.

Bei der Analyse der Ursachen von Ransomware-Angriffen war die häufigste Ursache eine ausgenutzte Sicherheitslücke (in 36 % der Fälle), gefolgt von kompromittierten Anmeldedaten (in 29 % der Fälle). Dies deckt sich mit den Ergebnissen des Sophos 2023 Active Adversary Report for Business Leaders, der sich mit der Reaktion auf Vorfälle vor Ort befasst.

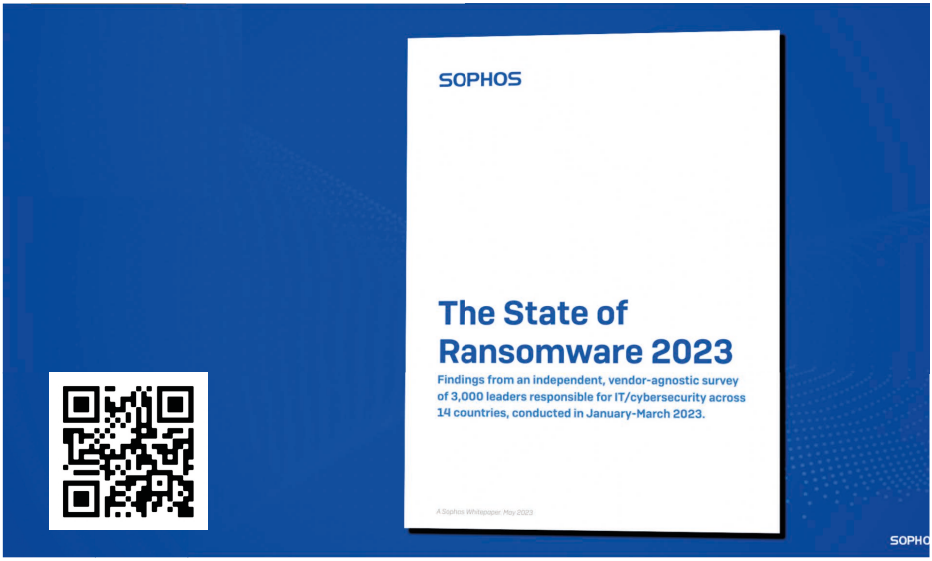
Weitere wichtige Erkenntnisse aus dem Report sind:

- In 30 % der Fälle, in denen Daten verschlüsselt wurden, wurden auch Daten gestohlen, was darauf hindeutet, dass diese "Double-Dip"-Methode (Datenverschlüsselung und Datenexfiltration) immer häufiger vorkommt.
- Der Bildungssektor meldete die meisten Ransomware-Angriffe: 79 % der befragten Organisationen im Hochschulbereich und 80 % der befragten Organisationen im unteren Bildungsbereich berichteten, dass sie Opfer von Ransomware waren.

Insgesamt zahlten 46 % der befragten Unternehmen, deren Daten verschlüsselt waren, das Lösegeld. Größere Unternehmen zahlten jedoch weitaus häufiger. Mehr als die Hälfte der Unternehmen mit einem Umsatz von 500 Millionen US-Dollar oder mehr zahlten das Lösegeld, wobei die höchste Rate bei Unternehmen mit einem Umsatz von über 5 Milliarden US-Dollar zu verzeichnen war. Dies könnte zum Teil darauf zurückzuführen sein, dass größere Unternehmen eher über eine eigenständige Cyber-Versicherungspolice verfügen, die Lösegeldzahlungen abdeckt

"Zwei Drittel der Unternehmen gaben an, im zweiten Jahr in Folge Opfer von Ransomware-Kriminellen geworden zu sein, und damit haben wir wahrscheinlich ein Plateau erreicht. Der Schlüssel zur Senkung dieser Zahl liegt darin, aggressiv daran zu arbeiten, sowohl die Zeit bis zur Entdeckung als auch die Zeit bis zur Reaktion zu verkürzen. Die von Menschen geleitete Bedrohungsjagd ist sehr effektiv, um diese Kriminellen zu stoppen, aber die Warnungen müssen untersucht und die Kriminellen innerhalb von Stunden und Tagen, nicht Wochen und Monaten, aus den Systemen entfernt werden. Erfahrene Analysten können die Muster eines aktiven Eindringens innerhalb von Minuten erkennen und sofort in Aktion treten. Dies ist wahrscheinlich der Unterschied zwischen dem Drittel, das sicher bleibt, und den zwei Dritteln, die nicht sicher sind. Unternehmen müssen rund um die Uhr in Alarmbereitschaft sein, um heutzutage eine effektive Verteidigung aufzubauen", sagt Wisniewski.

"Der jüngste Sophos Report macht deutlich, dass Ransomware nach wie vor eine große Bedrohung darstellt, sowohl was den Umfang als auch das Ausmaß betrifft. Dies gilt insbesondere für Unternehmen mit vielen Zielen und wenig Ressourcen, die nicht unbedingt über eigene interne Ressourcen für die Prävention, Reaktion und Wiederherstellung von Ransomware verfügen", sagt Megan Stifel, Executive Director der Ransomware Task Force und Chief Strategy Officer, Institute for Security and Technology. "Eine Möglichkeit, die Sicherheit zu erhöhen, die mit den Ergebnissen des Sophos Reports übereinstimmt, ist d$_{ie}$



Implementierung des Blueprint for Ransomware Defense der Ransomware Task Force, einem Rahmenwerk aus 48 Schutzmaßnahmen, das auf den CIS IG1 Controls basiert. Es ist höchste Zeit, dass sich der private und öffentliche Sektor zusammenschließt und Ransomware gemeinsam bekämpft. Deshalb freuen wir uns über die Zusammenarbeit mit Cybersecurity-Anbietern wie Sophos."

Sophos empfiehlt die folgenden Best Practices, um sich vor Ransomware und anderen Cyberattacken zu schützen:

- Sicherheits-Tools, die die häufigsten Angriffsvektoren abwehren, einschließlich Endpoint-Schutz mit starken Anti-Exploit-Funktionen, um die Ausnutzung von Schwachstellen zu verhindern, und Zero Trust Network Access (ZTNA), um den Missbrauch kompromittierter Anmeldedaten zu vereiteln
- Adaptive Technologien, die automatisch auf Angriffe reagieren, die Angreifer stören und den Verteidigern Zeit verschaffen, um zu reagieren
- 24/7-Bedrohungserkennung, -untersuchung und -reaktion, entweder intern oder durch einen spezialisierten Anbieter von Managed Detection and Response (MDR)
- Optimierung der Angriffsvorbereitung, einschließlich regelmäßiger Backups, Übungen zur Wiederherstellung von Daten aus Backups und Pflege eines aktuellen Reaktionsplans für Zwischenfälle
- Aufrechterhaltung einer guten Sicherheitshygiene, einschließlich rechtzeitiger Patches und regelmäßiger Überprüfung der Konfigurationen von Sicherheitstools

Die Daten für den Bericht "State of Ransomware 2023" stammen aus einer herstellerunabhängigen Umfrage unter 3.000 Führungskräften im Bereich Cybersicherheit/IT, die zwischen Januar und März 2023 durchgeführt wurde. Die Befragten stammten aus 14 Ländern in Nord- und Südamerika, EMEA und dem asiatisch-pazifischen Raum. Die befragten Unternehmen hatten zwischen 100 und 5.000 Mitarbeiter und einen Umsatz zwischen weniger als 10 Millionen und mehr als 5 Milliarden US-Dollar.

Bericht State of Ransomware 2023 mit globalen Ergebnissen und Daten nach Branchen: www.sophos.com/en-us/content/state-of-ransomware

MOBOTIX

Cybersicherheit und Datenschutz als Schlüsselelemente für Videosysteme

Die USA machte mit dem National Defense Authorization Act (NDAA) den Anfang. Der NDAA listet zum Schutz vor chinesischer Spionage bestimmte Bauteile und Firmen auf, die für Telekommunikationsausrüstungen (einschließlich Sicherheitsprodukte) oder Dienstleistungen nicht verwendet werden dürfen, um die Endprodukte an US-Bundesbehörden, ihren Auftragnehmern und Zuschuss- oder Darlehensempfängern und mit denen in Verbindung stehenden Einrichtungen zu verkaufen. Mit Großbritannien und Australien folgten weitere Länder diesem Beispiel, und auch die EU hat Ende letzten Jahres den Cyber Resilience Act (CRA) auf den Weg gebracht. Diese Unternehmen und Bauteile chinesischer Herkunft, die im NDAA aufgelistet sind, stehen im Verdacht, für die chinesische Regierung zur Ausspähung und Spionage eingesetzt werden zu können. Die MOBOTIX AG bestätigt, dass alle MOBOTIX Videosysteme den Anforderungen des NDAA entsprechen und zu 100 Prozent NDAA-konform sind. MOBOTIX verwendet keine SoC (System on Chip) oder andere Komponenten, die Software von chinesischen Unternehmen verarbeiten können. Darüber hinaus sind MOBOTIX-Produkte, die von OEM-Partnern (Original Equipment Manufacturers) bezogen werden, ebenfalls 100% NDAA-konform. MOBOTIX hat in einem definierten 3-stufigen Selbstzertifizierungsprozess eindeutig nachgewiesen, dass seine Videoüberwachungskameras keine chinesischen Komponenten enthalten. Die hohen Qualitäts-Standards werden auch vom renommierten australischen "Security Electronics & Networks Magazine (sen.news)" bestätigt.

Cybersicherheit und Datenschutz als Qualitätsmerkmale

Cybersicherheit ist fester Bestandteil der MOBOTIX DNA. Die MOBOTIX Videosysteme werden regelmäßigen Penetrationstests unterzogen, beispielsweise vom französischen Centre national de prévention et de protection (CNPP) und der SySS GmbH, dem führenden Institut für Penetrationstests in Deutschland. MOBOTIX bündelt das Sicherheitskonzept im Cactus Concept: **tinyurl.com/mtx8kw7b**
Ebenso sorgt die dezentrale Architektur der MOBOTIX Videosysteme für beste Sicherheit, da alle Bildverarbeitungs-Prozesse, wie beispielsweise die Verpixelung von Personen, direkt auf der Kamera passieren und keine Übermittlung von unverpixelten Daten erfolgt. Überhaupt stehen datenschutz- und DSGVO-konforme Anwendungen im Fokus von MOBOTIX.

So können Apps der MOBOTIX 7 Plattform Bilder sogar dynamisch verpixeln, indem sie Menschen erkennen und automatisch anonymisieren. Das kann bei der Überwachung sensibler Bereiche, von öffentlichen Plätzen oder Schulen wichtig sein. Auch Thermalanwendungen bieten beste Möglichkeiten für den DSGVO-konformen Perimeter- und Objektschutz, da Menschen im Thermalbild zwar zu sehen, aber nicht zu identifizieren sind. Die dezentrale Architektur erfordert zudem keinen dauerhaften Stream zu einem Server oder einer Zentrale, da Bilddaten nur bei einem Event übermittelt werden. Und dieser Dialog erfolgt stets verschlüsselt.

A10 Networks

Wachstumsprognosen führen zu Investitionen in Netzwerksicherheit

Die Mehrheit der Kommunikationsdienstleister in Deutschland rechnen in den nächsten zwei bis drei Jahren mit einem fortgesetzten Wachstum des Datenverkehrs, wobei 59 % von einem Wachstum von mindestens 50 % ausgehen. A10 Networks veröffentlicht eine Studie ‚Global Communication Service Providers: Market Growth Fuels Security Investments'

Die Studie wurde vom unabhängigen Marktforschungsunternehmen Opinion Matters durchgeführt. Befragt wurden 2.750 IT-Führungskräfte von unterschiedlichen Kommunikationsdienstleistern in elf Regionen weltweit, darunter 250 Umfrageteilnehmer aus Deutschland.*
Die Umfrage ergab, dass fast alle deutschen Dienstleister (99,6 %) in den nächsten zwei bis drei Jahren mit einem steigenden Volumen des Datenverkehrs rechnen. 59 % der Umfrageteilnehmer gehen von einem Wachstum von mind. 50 % aus, 12 % von 75 % oder mehr.

Vier Hauptthemen dominieren in der Umfrage von A10 Networks unter deutschen CSP:

- Fokus auf Investitionen
- Vorbereitung auf Wachstum
- Ausbau von Leistungen zur Abdeckung von unterversorgten Kommunen
- die Nutzung von Chancen, neue Märkte mit neuen Dienstleistungen zu erschließen.

Ernst Hillerkus, Country Manager DACH bei A10 Networks, kommentiert den positiven Wachstumstrend: „Diese Prognosen decken sich mit dem kontinuierlichen Wachstum des Datenverkehrs in den letzten Jahren. Zwar führte die Pandemie zu einem einmaligen Wachstumsschub, den unsere Umfrage von 2021 belegte. Aber auch langfristig läßt sich eine steile Wachstumskurve feststellen. Diese positive Entwicklung führt zu einem Investitionsdruck und zur Zuversicht, umfangreiche Investitionen zu tätigen." Strategien für Netzwerksicherheit werden deteilierter und vielseitiger. Die Umfrage ergab bei den deutschen Teilnehmern folgende Prioritäten für die Investitionen in Netzwerksicherheit:

- 28,4 %: Firewall-Upgrades
- 28 %: Vereinfachung und Integration von unzusammenhängenden, isolierten Sicherheitslösungen
- 27,6 %: DDoS-Cloud-Scrubbing
- 27,6 %: Schutz vor Ransomware und anderer Malware

Ernst Hillerkus: „Zwar wurde Firewall-Upgrades und anderen Sicherheitsanwendungen höchste Priorität zugeordnet, jedoch waren diese Themen nicht so dominant wie in der Umfrage vor zwei Jahren. Dies lässt darauf schließen, dass aktuelle Strategien für Netzwerksicherheit weiter gefasst und gut abgerundet sein müssen, damit sie das gesamte Spektrum möglicher Angriffsvektoren abdecken und einen hochwertigen, zuverlässigen und sicheren Kundenservice ermöglichen." Dienstleister arbeiten daran, die digitale Kluft zu überbrücken. Neben der Investition in Netzwerksicherheit planen deutsche CSP den Ausbau ihrer Netzwerke, um auch unter- und nicht versorgte Kommunen zu erreichen:

- 60 % der deutschen Umfrageteilnehmer geben an, ihre Netzwerke auf unter- und nicht versorgte Kommunen erweitern zu wollen.
- 46 % planen eine Erweiterung ihrer Kundenbasis um mehr als 10 %.
- 14 % wollen ihre Kundenbasis um mehr als 50 % erweitern.
- 40 % planen den Bau neuer Rechenzentren und wollen auch anderen Anbietern zusätzliche Kapazität bereitstellen.

Mit Blick auf diese Ergebnisse fügt Ernst Hillerkus hinzu: „Die Vernetzung von Kommunen ist entscheidend, um gleiche digitale Chancen für alle zu schaffen, weshalb dieser positive Trend sehr erfreulich ist. In Kombination mit robusten Sicherheitsstrategien führt dies dazu, dass mehr und mehr Menschen und Kommunen weltweit von sicheren und zuverlässigen digitalen Services profitieren werden." Enterprise-Cloud-Migration wirkt sich positiv aus Enterprise-Cloud-Migration war im letzten Jahrzehnt ein stabiler Trend, der durch die Pandemie weiter verstärkt wurde.
Die Umfrage ergab, dass deutsche CSP sich jetzt darauf konzentrieren, zur Unterstützung ihrer Zukunftspläne die richtige Kombination aus Cloud-Services zu finden:

- Insgesamt melden 68 % der deutschen Umfrageteilnehmer eine positive Bilanz ihres Umstiegs auf die Cloud.
- 24 % geben an, dass sie dadurch unmittelbar ihren Umsatz steigern konnten.
- 26 % haben ihr Angebot auf Public Cloud und verwaltete Rechenzentrumsservices ausgeweitet.
- 18 % bieten jetzt differenzierte Services an, die für ihre Kunden deutlich relevanter sind.

Ernst Hillerkus merkt an: „Es ist interessant, dass einer von vier CSP seinen Umsatz steigern konnte, weil Kunden ihre Arbeitslasten und Rechenzentrumsfunktionen zwischen Private und Public Cloud sowie lokalen Cloud-Servern verteilt haben. Der Umstieg auf die Cloud schlägt sich auch in den Beschaffungskriterien für Netzwerkausrüstung nieder: 32 % geben an, dass ein cloudnativer Formfaktor ein Muss ist." IPv6-Umstellung bleibt eine Herausfor- derung. Die weltweite Nachfrage mit immer mehr CSP-Kunden hat zu einem Engpass bei IPv4-Adressen geführt. Deshalb müssen Anbieter für die Umstellung auf IPv6 planen. Laut der Umfrage gehen

- 35 % der deutschen Befragten davon aus, dies innerhalb der nächsten 2–3 Jahre bewerkstelligen zu können.
- Über ein Viertel (28 %) folgt einer Strategie, die IPv4-Adressenpools gewissenhaft zu verwalten und nach und nach auf IPv6 umzustellen.
- 37 % setzen auf den Parallelbetrieb

Ernst Hillerkus fasst zusammen: „Dies zeigt, dass CSP beim Wechsel zu IPv6 zurückhaltender vorgehen, vorhandene Investitionen weiterhin nutzen und IPv4-Adressen sorgfältig verwalten bzw. beide Protokolle parallel einsetzen, statt auf einen harten Schnitt zu setzen.

Download des vollständigen Berichts unter herunter:
https://tinyurl.com/mpfsse7t

BRANCHENRADAR.com

Österreich: Nachfrage nach Schnelllauftoren wächst

Das Wachstum am österreichischen Markt für Garagen- und Industrietore war im Jahr 2022 preisgetrieben. Einzig bei Schnelllauftoren konnte auch die Nachfrage ausgeweitet werden, zeigen aktuelle Daten zweier Marktstudien des Marktforschungsinstituts BRANCHENRADAR.com Markta nalyse.

Der Markt für Garagen- und Industrietore verbuchte auch im vergangenen Jahr ein signifikantes Umsatzplus. Laut aktuellem BRANCHENRADAR Garagentore und Industrietore in Österreich erhöhten sich die Erlöse von Herstellern und Generalimporteuren im Jahr 2022 um rund sechs Prozent gegenüber Vorjahr auf insgesamt 149,2 Millionen Euro. Davon entfielen 65,6 Millionen Euro (+3,8% geg. VJ) auf Garagentore und 83,6 Millionen Euro (+7,7% geg. VJ) auf Industrietore. In beiden Märkten war das Wachstum jedoch ausschließlich preisgetrieben. Die Nachfrage sank im Jahresvergleich jeweils um rund 1,5 Prozent. Gegen den negativen Absatztrend entwickelten sich einzig Schnelllauftore, die zum überwiegenden Teil in Produktions- und Logistikgebäuden zum Einsatz kommen. Bereits 2021 stieg der Bedarf um neun Prozent gegenüber Vorjahr. Zuletzt lag das Plus bei knapp zehn Prozent. Der Trend zu Schnelllauftoren hat nicht zuletzt mit den steigenden Energiekosten zu tun, helfen die Produkte doch mit, den Energieverlust durch geöffnete Tore zu senken, ohne die Produktionsabläufe spürbar zu stören. Infolge wuchsen Schnelllauftore auch erlösseitig deutlich rascher als in den anderen Produktsegmenten. Der Umsatz mit Schnelllauftoren stieg um 16,0 Prozent, mit Sektionaltoren indessen insgesamt um 5,5 Prozent und mit anderen Tortypen (Falttoren, Rolltoren, Schwingtoren usw.) nur um 1,6 Prozent gegenüber Vorjahr.

GARAGENTORE & INDUSTRIETORE | Österreich

	2019	2020	2021	2022
Marktentwicklung Garagen. & Industrietore total | zu **Herstellerpr.**				
Umsatz | in Mio. Euro	**126,8**	**123,3**	**140,9**	**149,2**
Abw. geg. VJ in %	-	-2,8	14,3	5,9
davon ...				
Garagentore | in Mio. Euro	**62,2**	**58,3**	**63,2**	**65,6**
Abw. geg. VJ in %	-	-6,3	8,4	3,8
Industrietore | in Mio. Euro	**64,5**	**65,0**	**77,7**	**83,6**
Abw. geg. VJ in %	-	0,7	19,6	7,7

Quellen:

BRANCHENRADAR Garagentore in Österreich 2023

Phoenix Contact

Neuer Standard für die sichere Kommunikation bis zum letzten Meter

Die IO-Link-Safety-Technologie ermöglicht die sichere und durchgängige Datenübertragung von der Steuerungsebene bis zur Anbindung von sicherheitsgerichteten Sensoren und Aktoren im Feld. IO-Link hat sich als Kommunikationsstandard im Maschinen- und Anlagenbau etabliert. Durch die Weiterleitung zusätzlich bereitgestellter Daten der intelligenten Sensoren und Aktoren lassen sich im Rahmen der Digitalisierung Fertigungsprozesse optimieren. Von den Vorteilen der universellen Nutzung sowie der Datengenauigkeit und -verfügbarkeit profitiert auch der Bereich der funktionalen Sicherheit. Die sicherheitsgerichtete Systemerweiterung basiert auf der Verwendung von IO-Link Safety-Mastern und IO-Link Safety-Devices.

Die IO-Link Safety-I/O-Box von Phoenix Contact erlaubt die Einbindung

von sicheren Sensoren und Aktoren in IO-Link Safety-Systeme. Dafür stehen acht sichere digitale Ein-sowie vier sichere digitale Ausgänge zur Verfügung. Diese Anschlüsse ermöglichen die einfache Installation von Sensoren und Aktoren im Feld sowie den Zugriff auf erweiterte Diagnosedaten. Das Zusammenspiel von IO-Link und IO-Link Safety verspricht damit neue herstellerübergreifende Maschinen- und Anlagenkonzepte.

KRITIS-Studie

Cybersecurity-Bedrohung für Unternehmen wächst

Welchen Gefahren sind Unternehmen Kritischer Infrastrukturen (KRITIS) derzeit ausgesetzt? Wo liegen ihre größten Herausforderungen? Und welche Rolle spielen Systeme zur Angriffserkennung dabei? Um diese und weitere Fragen zu beantworten, hat das Research- und Beratungsunternehmen techconsult im Auftrag der secunet Security Networks AG mehr als 120 KRITIS-Unternehmen im Rahmen der Studie „Angriffserkennung in Unternehmen Kritischer Infrastrukturen – wie deutsche KRITIS-Unternehmen mit den steigenden IT- und OT-Risiken umgehen" befragt.

Die Ergebnisse zeigen, dass 79 Prozent der Unternehmen die aktuelle Bedrohungslage als wachsend bis stark wachsend einschätzen. Auch vor diesem Hintergrund hat die Bundesregierung 2021 das IT-Sicherheitsgesetz 2.0 auf den Weg gebracht, um die Bevölkerung vor Cyberangriffen und ihren Folgen zu schützen. Ab 1. Mai 2023 müssen betroffene Unternehmen den Einsatz von Systemen zur Angriffserkennung in ihrer IT-Infrastruktur, die zur Aufrechterhaltung der kritischen Versorgungsdienstleistungen unabdingbar ist, nachweisen. Obwohl solch ein System für andere Bereiche nicht verpflichtend ist, planen 71 Prozent der befragten KRITIS-Unternehmen, auch beispielsweise in der Büro-IT entsprechende Systeme zur Angriffserkennung zu etablieren. Bereits 21 Prozent haben ein derartiges System vollständig sowohl in den Pflichtbereichen als auch darüber hinaus eingeführt. 45 Prozent der Befragten planen die Einführung noch dieses Jahr und rund ein Drittel (33 Prozent) in den nächsten ein bis drei Jahren.

Prävention gegen Cyberrisiken scheitert häufig an fehlender Kompetenz

59 Prozent der befragten Unternehmen stufen sich als kompetent bis sehr kompetent beim verpflichtenden Melden von Sicherheitsvorfällen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) ein, 56 Prozent bei der Prävention gegen Cyberrisiken. Bei jeweils über 40 Prozent der Unternehmen besteht somit noch Verbesserungspotenzial hinsichtlich der Umsetzung der gesetzlichen Meldepflicht bei Sicherheitsvorfällen an das BSI. Dabei schätzt jedes zweite befragte Unternehmen (50 Prozent), dass IT-Sicherheitsvorfälle zu Kompromittierung sensibler und kritischer Daten führen würden. 45 Prozent befürchten bei einem Vorfall den Ausfall von für das Gemeinwesen relevanten Anlagen und 46 Prozent Umsatzeinbußen.

IT-Fachkräftemangel bleibt größte Herausforderung

Mehr als jedes zweite KRITIS-Unternehmen (59 Prozent) sieht den Mangel an IT-Fachpersonal als eine der größten Herausforderungen für die kommenden zwei Jahre. Dieses Fachpersonal fehlt, um die Anpassungen und die Umsetzung der Regularien und Vorgaben zu bewältigen. Ein weiterer Schmerzpunkt ist für 44 Prozent der Befragten die Schwachstellenanalyse im Netzwerk, die jedoch essenziell für weitere Maßnahmen zur Steigerung der Abwehr von Cyberangriffen ist.
Weitere Herausforderungen sind mit 30 Prozent die Absicherung von kritischen Komponenten im Internet of Things (IoT) oder Industry Control Systems (ICS), die Inbetriebnahme notwendiger Security-Lösungen (28 Prozent) sowie die Erbringung von Nachweisen zur Informationssicherheit (23 Prozent).

Über die Studie:
Die Studie „Angriffserkennung in Unternehmen Kritischer Infrastrukturen – wie deutsche KRITIS-Unternehmen mit den steigenden IT- und OT-Risiken umgehen" wurde im Januar 2023 von techconsult durchgeführt. Mit Hilfe eines strukturierten Fragebogens wurden branchenübergreifend 121 KRITIS-Unternehmen in Deutschland befragt.

Alle Ergebnisse der Studie unter dem folgenden Link: https://tinyurl.com/yc7868sx

Leuze

Einfach erfassen: Neue Simple Vision Sensoren

Die Sensoren der Simple Vision-Baureihe überzeugen mit flexibler Anwendbarkeit und einfacher Handhabung. Der neue IVS 108 eignet sich für die Anwesenheitserkennung von Objekten. Geräte der Reihe IVS1048i / DCR 1048i übernehmen zusätzlich Zähl- und Messaufgaben oder das Lesen von Codes.

Einfach bedienbare und leistungsstarke Sensoren – mit den Simple Vision-Sensoren von Leuze gehen Anlagenbetreiber auf Nummer sicher. Die kompakten Geräte lassen sich so komfortabel handhaben wie optoelektronische Sensoren, sind aber nahezu so leistungsfähig wie Kamerasysteme.

Der IVS 108 erkennt an- oder abwesende Objekte. Zum Beispiel Aufdrucke oder Labels auf Verpakkungen. Dank Autofokus-Einstellung und eines einfachen Teach-ins gelingt die Inbetriebnahme im Handumdrehen: ein Gut- und ein Schlecht-Teil werden vor dem Zielsystem positioniert. Der Anwender bestätigt jeweils per Teach-Taste. Fertig. Und zudem praktisch: Der Sensor speichert bis zu 32 unterschiedliche Aufgaben. Darüber hinaus können per Webbrowser Live-Bilder betrachtet und auf einer grafischen Bedienoberfläche weitere Parameter anwenderfreundlich eingestellt werden.

Der IVS 108 eignet sich optimal für Transport-, Sortier- und Förderanlagen. Und auch für die Qualitätskontrolle und bei der automatischen Montage mechanischer oder elektronischer Teile ist der Sensor die richtige Wahl.

Der IVS 1048i ist ein leistungsstarkes Allrounder-Modell: Anwender können aus sechs Varianten mit zwei unterschiedlichen Auflösungen wählen. Der Funktionsumfang des IVS 1048i reicht je nach Modell von der Objekterkennung über Messaufgaben bis hin zur integrierten Barcodelesung. Sollen ausschließlich Codes erfasst werden, bietet sich dafür alternativ der Sensor DCR 1048i an. Vorteil aller Sensoren der Baureihe IVS/DCR 1048i: Vier austauschbare S-Mount-Objektive mit variabler Fokuseinstellung und zwei Blenden ermöglichen hohe Flexibilität bei Leseabstand, Sichtfeld, Auflösung und Schärfentiefe. Zudem sind die digitalen Schnittstellen I/O, TCP/IP, PROFINET, FTP oder SFTP integriert.

GDP network solutions

Temperaturlogger für GDP-konforme Pharmalogistik

Für den GDP-konformen Transport von Pharma- und Medizinprodukten ist eine aktive Temperaturführung besonders wichtig. Wird die Temperatur nicht lückenlos kontrolliert und reguliert, können Qualitätseinbußen bei der transportierten Ware die Folge sein. Im Pharmalogistiknetzwerk von GDP network solutions müssen die Temperaturen nachweisbar zwischen + 15 C° und + 25 °C liegen und sowohl im Lager als auch beim Umschlag oder Transport konsequent erfasst werden.

„Bevor wir 2020 an unserem Hauptumschlagplatz in Kassel in den produktiven Betrieb gegangen sind, wurden im Rahmen eines Sommer- und Winter-Mappings Messpunkte festgelegt, um später die Temperatur im Routinebetrieb zu überwachen", erzählt Mathias Stolze, Qualitätsmanagementbeauftragter bei der GDP network solutions GmbH. „Nun sind Temperaturlogger an drei Positionen in unserem Lager 24/7 in Betrieb und an ein Alarmsystem gekoppelt, das uns entweder direkt per SMS oder über E-Mail benachrichtigt, sollten die gemessenen von den vorgegebenen Temperaturen abweichen."

Temperaturlogger für die zuverlässige Kontrolle

In der Pharmalogistik müssen Temperaturmess- und Überwachungssysteme mindestens einmal im Jahr verifiziert werden. Die Euroscan Parts & Services GmbH bietet dafür einen mobilen Kalibrierservice für Erst- und

Re-Kalibrierung sowie Reparaturen, Erweiterungen und die Montage in Lagerhallen oder Fahrzeugen, den auch GDP network solutions nutzt. „Die Sensoren werden vorab im Labor exakt auf die vorgegebenen Temperaturen kalibriert und dann vor Ort einfach ausgetauscht," so Stolze. Der Fehler wird auf drei Stellen nach dem Komma kontrolliert. Eine Toleranz von +/- 0,3 °C darf nicht überschritten werden. Jeder Datenlogger ist mit einem Barcode ausgestattet, wird über eine Seriennummer elektronisch erfasst und erhält sein eigenes Zertifikat. „In Verbindung mit einem Verifikationsdokument, inklusive Prüftemperatur ist dies ein gültiger Verifikationsnachweis nach höchsten aktuellen Standards." Ein USV-Batteriepack stellt außerdem sicher, dass die Sensoren auch bei einem Stromausfall weiter funktionieren.

Temperaturschreiber für die Datenerfassung

In den Hallen von GDP network solutions und vielen Fahrzeugen der Netzwerkpartner werden zudem die Temperaturschreiber von Euroscan verbaut, um Temperaturdaten aufzeichnen und sie entweder direkt über einen Drucker auszugeben, Echtzeit-Alarme auszulösen oder über eine Schnittstelle bzw. das Webportal ColdChainView von ORBCOMM an das Telematiksystem von GDP senden zu können. Dort werden die Temperaturdaten aller Netzwerkteilnehmer gebündelt und weiterverarbeitet.

„Das GAMP-5-zertifizierte und GDP-konforme Temperaturüberwachungssystem von Euroscan bietet insgesamt eine gute Performance, vielfältige Abfragemöglichkeiten und eine zuverlässige Verbindung," so Stolze abschließend.

„Außerdem haben wir dort einen festen Ansprechpartner, zu dem wir direkt Kontakt aufnehmen können, falls wir Fragen haben – und diese Sicherheit kommt auch unseren Auftraggebern zugute."

Flexibel und sicher

WALLIX führt SaaS Remote Access ein

- **WALLIX bringt SaaS Remote Access auf den Markt, die SaaS-Version der in die einheitliche Lösung WALLIX PAM4ALL integrierten Remote Access Management-Technologie. Diese SaaS-Version ist im WALLIX PAM4OT-Paket enthalten.**
- **Organisationen – in allen Sektoren und insbesondere in der Industrie – verlassen sich bei der Durchführung ihrer Aktivitäten oftmals auf externe Dienstleister, die zur Erfüllung ihrer Aufgaben eine Verbindung zu ihrer (traditionellen oder industriellen) IT-Infrastruktur benötigen.**
- **SaaS Remote Access richtet sich an alle Organisationen, die externen Dienstleistern einen digitalen Zugang zu ihrer IT-Infrastruktur gewähren.**

WALLIX, ein europäischer Anbieter von Cybersicherheitssoftware und Experte für Zugangs- und Identitätslösungen, bringt SaaS Remote Access auf den Markt, eine SaaS-Version (Software-as-a-Service) der in WALLIX PAM 4ALL integrierten Remote Access Management-Technologie. SaaS Remote Access wurde für Unternehmen aller Branchen und insbesondere der Industrie entwickelt, die externen Anbietern durch eine vereinfachte Verwaltung digitalen Zugang zu ihrer IT-Infrastruktur gewähren und gleichzeitig von der höchsten Cybersecurity eines von Gartner anerkannten PAM-Marktführers profitieren möchten.

Zur Ausübung ihrer Geschäftstätigkeit sind Unternehmen oftmals auf externe Dienstleister angewiesen, die sich mit deren IT-Infrastruktur (ob traditionell oder industriell) verbinden müssen. Dabei kann es sich um Fernwartungsunternehmen, Lieferanten der Lieferkette, Dienstleister, externe Berater usw. handeln.

Das Problem für Unternehmen besteht darin, dass diese externen Interessengruppen zahlreich sind und sich ständig ändern können. Darüber hinaus variieren die Häufigkeit und Dauer ihrer Zugriffe je nach den Bedürfnissen des Unternehmens und ihren Anforderungen. Aus diesem Grund bereitet die Visualisierung, Verwaltung und Sicherung dieser externen Zugriffs IT-Teams einiges Kopfzerbrechen. Für Unternehmen ist es in der Tat von entscheidender Bedeutung, die Zugriffsrechte zu verwalten und zu wissen, wer von wo aus auf was zugreifen kann und warum.

Nur so kann jeder Versuch eines Identitätsdiebstahls durch einen Hacker, interne Böswilligkeit oder Nachlässigkeit erkannt, gestoppt und Daten geschützt werden. Tatsache ist, dass die Kosten eines Cyberangriffs um durchschnittlich 370.000 Dollar steigen, wenn ein Dritter beteiligt ist.

Darüber hinaus stellen Unternehmen mit der Implementierung einer solchen Sicherheitslösung zur Rückverfolgbarkeit digitaler Zugriffe sicher, dass sie compliant sind und aktuelle Cybersicherheitsstandards einhalten.

Traditionell versuchen IT-Teams, den Zugriff externer Interessengruppen zu verwalten, indem sie VPN-Technologie einsetzen, also, einen sicheren „Tunnel" zwischen dem Gerät der externen Interessengruppe und der IT-Infrastruktur des Unternehmens aufbauen. Allerdings machen VPN-Schwachstellen in der Realität regelmäßig Schlagzeilen.

Andererseits ist die Implementierung von VPNs ein mühsamer und teurer Prozess: Jeder Akteur muss in der Active Directory verzeichnet werden, der jener

Microsoft-Software, die von fast allen Organisationen verwendet wird und die die Verwaltung von Berechtigungen und die Kontrolle der Zugriffe auf IT-Ressourcen (Daten, Server, Anwendungen, Software usw.) ermöglicht. Auch diese Technologie entspricht nicht den gesetzlichen Anforderungen.

Die Antwort: SaaS Remote Access

Um die Verwaltung des Zugriffs von externen Dienstleistern zu optimieren, sollten IT-Teams auf innovative Lösungen wie SaaS Remote Access zurückgreifen.

WALLIX PAM4ALL ist eine einheitliche Lösung zur Verwaltung von Berechtigungen. Sie kombiniert sämtliche WALLIX-Technologien: Multi-Faktor-Authentifizierung (MFA), Remote Access Management, Session Management, Passwortmanagement und Least Privilege Management.
Die Lösung sichert den gesamten Zugriff auf die IT-Infrastruktur und gewährleistet den Schutz der Daten, die Erkennung und den Schutz vor Cyberangriffen sowie die Geschäftskontinuität. Darüber hinaus gewährleistet sie die Einhaltung von Cybersi- cherheitsvorschriften.

SaaS Remote Access ist die "Remote Access Management"-Technologie von WALLIX PAM4ALL, die jetzt als Service verfügbar ist. Sie wurde speziell für das Zugriffsmanagement von externen Providern entwickelt. Diese SaaS-Version ist auch in WALLIX PAM4OT verfügbar, einem Paketangebot speziell entwickelt für Industrieunternehmen und Betreibern von Industrieanlagen (z.B. Krankenhäuser mit Scannern etc.).

Die Vorteile eines Abonnements dieser Funktionalität im SaaS-Modus sind:

- **Einfache Bereitstellung und Nutzung**
  Dank des SaaS-Modus muss keine neue Lösung installiert werden, um VPNs zu ersetzen; für den Zugriff auf SaaS Remote Access ist lediglich eine Internetverbindung erforderlich. Dies ermöglicht eine bessere Zugänglichkeit, Flexibilität und Kostenreduzierung.
  Darüber hinaus können Unternehmen dank der benutzerfreundlichen Schnittstelle ihre externen Dienstleister schnell und einfach registrieren und deren Zugriffsrechte auf autorisierte Ressourcen konfigurieren. Dadurch wird das IT-Team von diesen Aufgaben entlastet und kann sich auf wertschöpfungsintensivere Aufgaben konzentrieren.

- **End-to-End-Sicherheit**
  Die digitalen Identitäten und Passwörter externer Akteure sind nicht mehr in das Active Directory des Unternehmens integriert, sondern werden in SaaS Remote Access verwaltet und gesichert. Dadurch wird das Cyber-Risiko drastisch reduziert, denn je mehr digitale Identitäten im Active Directory vorhanden sind, desto größer ist die Wahrscheinlichkeit, dass ein Hakker sie stiehlt und dann auf alle Ressourcen der Person zugreift, deren Identität gestohlen wurde.

  Dies ermöglicht dem Unternehmen auch eine IT-Hygiene, die den Standards für Cybersicherheit und Rückverfolgbarkeit folgt und somit Cybersicherheit by Design ermöglicht.

- **Volle Sichtbarkeit des externen Fernzugriffs**
  Mit SaaS Remote Access gewinnen Unternehmen die Kontrolle über den externen Fernzugriff zurück. Unternehmen erstellen den Zugang für ihre externen Anbieter in Echtzeit für einen bestimmten Zeitraum und werden automatisch entfernt, sobald die Aufgabe abgeschlossen ist. Externe Anbieter stellen über das SaaS Remote Access-Webportal eine Verbindung zur IT-Infrastruktur des Unternehmens her und jede Aktion, die sie durchführen, wird überwacht, so dass volle Sichtbarkeit und Transparenz gewährleistet sind.

„Mit dieser Fernzugriffsverwaltung für Lieferanten stellen wir uns den Sicherheitsherausforderungen der IT-Teams und fördern gleichzeitig die digitale Transformation der Unternehmen. Außerdem geben wir den Business-Teams Autonomie und stellen die digitale Erfahrung in den Mittelpunkt unserer Lösung: Schnelligkeit bei der Erstellung von Zugängen, flüssige Interaktionen mit Lieferanten und operative Effizienz für alle Business- und IT-Teams.

Die Interaktion mit Lieferanten und die Aufrechterhaltung einer Verteidigungslinie für den digitalen Zugang wird mit unserer Lösung extrem einfach und kostengünstig. Die Einführung dieses Dienstes zur Sicherung des externen Zugriffs auf IT- und Industrieinfrastrukturen ist nur die erste Phase unserer SaaS-Strategie“, erklärt Edwige Brossard, Product Director bei WALLIX.

Für Notrufe und Gipfel-Selfies

Mobilfunk in den Alpen: Vodafone vollendet Ausbauoffensive schneller als geplant

121 Baumaßnahmen in nur neun Monaten realisiert • 22 LTE-Funklöcher beseitigt • Mobiler Datenverkehr steigt um mehr als 35 Prozent

Vodafone hat seine aktuelle Ausbau-Offensive für die deutsche Alpenregion schneller vollendet als geplant. Im Juli 2022 hatte Vodafone auf der Aueralm in Bad Wiessee angekündigt, in den acht Landkreisen der Alpen 115 Bauprojekte zu realisieren, um das Netz in der Fläche auszubauen und zu verstärken. Nur neun Monate nach dem Start sind alle diese Bauprojekte bereits geschafft. Mehr noch: Es wurden 121 Baumaßnahmen umgesetzt, um Notrufe zu erleichtern und schnelleres Senden von Gipfel-Selfies zu ermöglichen. Hintergrund: Mobilfunk bringt ein Stück mehr Sicherheit in die Alpenregion. Zudem steigt der mobile Datenverkehr um über 35 Prozent, weil die Einheimischen und die Gäste immer stärker zum Smartphone greifen.

99,7% **der besiedelten Alpenregionen sind an das Vodafone-Netz angeschlossen Starke Nachfrage der Bevölkerung**

Im Rahmen der aktuellen Ausbauoffensive hat Vodafone 22 LTE-Funklöcher beseitigt – vor allem durch Neubauten von Stationen. Zudem wurden 78 neue 5G-Stationen in Betrieb genommen, indem bestehende Standorte zu 5G-Stationen aufgewertet wurden. Insgesamt betreibt Vodafone in der Alpenregion nunmehr 416 Mobilfunk-Stationen. Dadurch sind 99,7 Prozent der besiedelten Gebiete in der Alpenregion – das sind die Landkreise Oberallgäu, Ostallgäu, Garmisch-Partenkirchen, Bad Tölz-Wolfratshausen, Miesbach, Rosenheim, Traunstein und

Berchtesgadener Land – an das Vodafone-Mobil- funknetz angebunden. Mit seinem mobilen Breitbandnetz LTE erreicht Vodafone mehr als 99 Prozent der Haushalte und Ferienwohnungen in den Alpen.

Netzausbau: Ein Mast als Mobilfunk-Basisstation auf dem Land in der Region am Tegernsee.

Mit seinen Investitionen in den Ausbau des LTE-Netzes und dem Aufbau des 5G-Netzes trägt Vodafone der starken Nachfrage der Bevölkerung Rechnung: Der mobile Datenverkehr in der Alpenregion wächst rasant - mit einer jährlichen Steigerungsrate von aktuell mehr als 35 Prozent. Die Menschen surfen also immer stärker im mobilen Internet - etwa aus beruflichen Gründen oder um ihre Urlaubseindrücke in sozialen Medien zu teilen, Videos in HD-Qualität anzuschauen, Events aus Kultur und Sport (z.B. Fußball-Bundesliga, 2. Liga und Champions League) und TV-Sendungen im Live-Stream zu verfolgen oder sich in Nachrichtenportalen von Medienhäusern zu informieren.

Regionaler Netzausbau

Netzempfang bringt in den Alpen aber auch ein Stück mehr Sicherheit: Früher war es häufig unmöglich, inmitten der Berge einen Anruf an die Notfallzentrale abzusetzen oder auf dem Handy die Wetterlage, die Streckenplanung oder Wander-Karten aufzurufen. Aus diesem Grund hat Vodafone in Kooperation mit dem Deutschen Alpenverein bereits vor mehr als 30 Jahren den Ausbau seines Mobilfunk-Netzes in den Alpen gestartet. Die erste Mobilfunk-Station in den Alpen wurde im Juni 1992 in Betrieb genommen. Ein Ziel war – und ist es weiterhin – mehr Sicherheit für die Wanderer und Bergsteiger durch die Einführung des Handy-Notrufes zu schaffen. Inzwischen ist das Netz in den Alpen auch in abseits gelegenen Rad- und Wanderwegen schon ganz gut ausgebaut. Mehr noch: Vodafone hat inzwischen in allen 416 Mobilfunkstationen in den Alpen die Notruf-Technologie AML (Advanced Mobile Location) eingebaut. Bei einem Notruf an die '112' wird der genaue Standort eines Anrufers via AML automatisch an die Rettungsleitstelle übertragen. So können die Retter schnellstmöglich an einen Unglücksort gelangen und Hilfe leisten.

Darüber hinaus wurde ganz aktuell im Februar 2023 das neue Katastrophen-Warnsystem Cell Broadcast in allen 416 Mobilfunk-Stationen der Alpenregion in Betrieb genommen. Mit Cell Broadcast kann die Bevölkerung in der Alpenregion seitdem gezielt und schnell per Textnachricht auf mobilen Endgeräten vor Katastrophen gewarnt werden - etwa vor Unwettern, Bränden, Erdbeben, akuten Lawinengefahren oder Überflutungen. Das gilt für kommende sowie bereits eingetretene Katastrophen. Vodafone sieht in Cell Broadcast eine sinnvolle Ergänzung zu vorhandenen Warnsystemen wie Sirenen, Rundfunk und Warn-Apps.

Der Ausbau geht weiter

Der Mobilfunk-Ausbau in den Alpen geht auch nach Vollendung der aktuellen Ausbau-Offensive weiter, denn ein Netz ist nie fertig. Allein bis Ende 2023 baut Vodafone 15 weitere mobile Datenautobahnen. Von Mobilfunk-Neubauten profitieren beispielsweise die Einwohner und Touristen in Tittmoning (LK Traunstein), Marktschellenberg und Teisendorf (LK Berchtesgadener Land) sowie Pforzen (LK Ostallgäu). Allerdings ist der Ausbau des Netzes gerade in den Alpen eine besondere Herausforderung. Denn das Gebiet ist aufgrund der Topographie viel schwerer zu versorgen als etwa das flache Land. Zudem muss immer zwischen Naturschutz und Mobilfunk-Versorgung abgewogen werden. Ebenso sollen sich die Stationen möglichst harmonisch in das Landschaftsbild einfügen. Bei der Suche nach neuen Standorten freut sich unser Dienstleister, die Funkturm-Gesellschaft Vantage Towers, über die Unterstützung von Gemeinden, Vermietern und Verpächtern.

EIKONA

Zeitfenstermanagement: Neue Funktionen auf der LogiMAT 2023

Mit seinem verbesserten Zeitfenstermanagement, das auch wesentliche Funktionen aus dem Yard Management beinhaltet, zeigt EIKONA Logistics auf der LogiMAT, wie Spediteure mit seinem benutzerfreundlichen Zeitfenstermanagement noch schneller und effizienter arbeiten können.
Auf der diesjährigen LogiMAT vom 25. bis 27. April zeigt EIKONA Logistics in Halle 8, Stand 8C55, sein optimiertes Zeitfenstermanagement. Das System hat bereits in der Praxis bewiesen, dass es auch bei hochvolumigen Stückgutnetzen gut funktioniert. Die Verbesserungen in der aktuellen Version sind direkt aus der Praxis entstanden.

So ermöglicht das Tool beispielsweise die Planung von Zeitfenstern unter Berücksichtigung der Entladezeitfenster im Direktverkehr. Dazu berechnet die Anwendung die Fahrzeit und die Entfernung und ermittelt, wann eine Sendung abgefertigt werden muss, damit das vorgegebene Entladezeitfenster am Zielort eingehalten werden kann. Für mehr Übersichtlichkeit sorgt auch die überarbeitete grafische Darstellung der Benutzeroberfläche. Alle wesentlichen Informationen sind nun für alle Prozessbeteiligten noch schneller zu erkennen. Neu in der Kalenderansicht sind auch die Spuren "Ungebucht" und "Ungeplant": Für ungebuchte Aufträge wurde noch kein Zeitfenster bestätigt, außerplanmäßige Touren kommen im Laufe des Tages ohne gebuchtes Zeitfenster an. Dank eindeutiger farblicher Kennzeichnung bleiben auch diese immer im Blick und können zwischen geplanten Ladevorgängen eingefügt werden. Darüber hinaus können jedem Standort beliebig viele Bereiche zugeordnet werden: Weiß der Anwender bereits von der Ware, dass sie z.B. ins Außenlager muss, kann er dies auf der Tour vorgeben und muss später nur noch den Ladeort auswählen. Darüber hinaus gibt eine Ressourcenübersicht, ähnlich einer Heatmap, jederzeit genaue Auskunft über die aktuelle Auslastung.

Klare Kommunikation dank Zeitfenster-Management

Sobald ein Zeitfenster buchbar ist, sendet das System eine E-Mail an den jeweiligen Spediteur mit der entsprechenden Anfrage. Die Aufforderung zur Buchung von Zeitfenstern kann nach granularen Regeln konfiguriert werden und wird über ein angeschlossenes Online-Portal oder einen direkten Link per E-Mail versendet. Um dem Spediteur oder Subunternehmer die Buchung von Zeitfenstern so einfach wie möglich zu machen, werden alle Kommunikationsarten, von E-Mail bis SMS, abgedeckt. Über das Yard-Management kann jedes authentifizierte Fahrzeug an der Verladestelle über die Zuweisung von Stellplätzen - deren Belegung ebenfalls im System ablesbar ist - bis hin zum Check-in an der vorgesehenen Rampe und schließlich der Abfahrt gesteuert werden. Der Fahrer erhält vom System per SMS die gewünschten Informationen. Zeitstempel protokollieren jeden Schritt, so dass Abweichungen von der geplanten Ankunfts- oder Abfahrtszeit eindeutig nachvollzogen werden können. Um jederzeit die aktuelle Position der Lkw zu kennen, kann das Zeitfenstermanagementsystem mit gängigen Fahrer-Apps verknüpft werden. Auf diese Weise kann schnell auf Abweichungen reagiert und lange Wartezeiten vermieden werden.

[Bastian Späth]

Dallmeier Partnertage 2023

Steigende Nachfrage nach Videotechnik „Made in Germany“

Auch in diesem Jahr veranstaltet Dallmeier wieder seine beliebten Partnertage – diese finden an insgesamt fünf verschiedenen Terminen im „Dallmeier Experience Centre“ in Regensburg statt. Errichter und Channel Partner aus der Sicherheitsbranche können sich dort über die aktuellen Produkte und Lösungen des deutschen Videosicherheitstechnik-Herstellers informieren.

Der Markt für Videosicherheitstechnik verzeichnet weiterhin ein solides Wachstum. Gleichzeitig steigen die Anforderungen der Endkunden – nicht zuletzt vor dem Hintergrund der aktuellen geopolitischen Veränderungen und den damit verbundenen Herausforderungen rund um Cybersicherheit, Datenschutz und ethische Verantwortung bei Investitionsentscheidungen. Dallmeier zeigt auf seinen Partnertagen, wie Partner diese Anforderungen bestmöglich erfüllen und mit hochwertigen Produkten „Made in Germany“ vom Wachstum der Branche profitieren können.

KRITIS im Fokus

Die Agenda bietet an den eineinhalb Tagen ein breites Themenspektrum. So stehen neben den neuesten Produkten die Themen Datenschutz, Datensicherheit sowie ethische und sicherheitspolitische Fragen rund um die Investitionsentscheidung „Videosicherheit“ im Mittelpunkt. Auch rechtliche und gesetzgeberische sowie datenschutzrechtliche Aspekte wie das IT-Sicherheitsgesetz 2.0 bzw. das BSI-Gesetz, die EU-Richtlinie NIS2 oder die Auswirkungen der NDAA-Compliance auf den deutschen Markt werden erläutert, insbesondere auch im Kontext kritischer Infrastrukturen (KRITIS).

Wettbewerbsfähig mit Produkten aus dem Hochlohnland

Neben einer Führung durch das Unternehmen mit eigener Fertigung am Rande der Regensburger Altstadt und dem „Experience Centre“ lernen die Besucher auch das brandneue, intuitive 3D-Planungstool „planD“ kennen. Darüber hinaus erfahren interessierte Partner, wie sie mit Produkten aus dem Hochlohnland Deutschland Lösungen beim Endkunden realisieren, die sich dennoch durch niedrige Gesamtbetriebskosten vom Wettbewerb abheben.

Breite Einsatzmöglichkeiten

Der Plattformgedanke ist aus der Videobranche nicht mehr wegzudenken. Die Kameras von Dallmeier sind daher in eine ganze Reihe von Drittsystemen wie Milestone, Genetec oder Advancis integriert. Auch diese Integrationen werden von den Dallmeier-Experten ausführlich erläutert. Die ersten Dallmeier Partnertage im Jahr 2023 waren komplett ausgebucht.
Unter www.dallmeier.com/de/dallmeier-partner-tage können sich Errichter und Reseller die vollständige Agenda ansehen und sich zu den Terminen für das Jahr 2023 anmelden:

- **26. + 27. April 2023**
- **24. + 25. Mai 2023**
- **5. + 6. September 2023**
- **10. + 11. Oktober 2023**

PMRExpo

Unter Regie der Koelnmesse

Die europäische Leitmesse für sichere Kommunikation und Professionellen Mobilfunk findet vom 28. bis 30. November 2023 wieder in Köln statt. Auf dem Event treffen sich die wichtigsten Akteure der Branche, um sich über neue Trends zu informieren, Know-how auszutauschen und wichtige Kontakte zu knüpfen.

Ab diesem Jahr organisiert die Koelnmesse als neuer Veranstaltungspartner die PMRExpo, ideeller Träger ist der PMeV – Netzwerk sichere Kommunikation. Wenn Sie im Vorfeld der PMRExpo über alle News auf dem Laufenden bleiben möchten, melden Sie sich bitte für unseren neuen Newsletter an.

Fünf Gründe für Ihre Teilnahme:

- Die PMRExpo ist die europäische Leitmesse für sichere Kommunikation.
- Seit über 20 Jahren ist die PMRExpo eine fest etablierte Branchenveranstaltung und im nationalen und internationalen Markt hervorragend positioniert.
- Die führenden Key Accounts der Branche sind vertreten.
- Es erwartet Sie ein vielfältiges und hochwertiges Konferenzprogramm mit relevanten und aktuellen Themen rund um sicherheits- und geschäftskritische Kommunikation, Professionellen Mobilfunk und Leitstellen.
- Mit dem PMeV haben wir den führenden deutschen Branchenverband im Umfeld sicherer Kommunikationslösungen als ideellen Träger an unserer Seite.

Resilienz als Zielbild für globale Wertschöpfungsketten

Resilienz ist in vielen Bereichen des täglichen Lebens derzeit allgegenwärtig. Aber auch verschiedenste Industrien oder die Politik rücken das Thema immer mehr in den Fokus. Mit ein Grund, warum es im Konferenzprogramm der transport logistic, die von 9. bis 12. Mai 2023 auf dem Messegelände in München stattfindet, weit oben auf der Agenda steht. Die Bundesvereinigung Logistik (BVL) wird dazu ein Fachforum veranstalten und hat im Vorfeld für die transport logistic ein Whitepaper veröffentlicht, das ab sofort kostenfrei zum Download zur Verfügung steht.

Resilientere Wertschöpfungsketten sind gefragt

Die Logistikbranche steht vor der herausfordernden Aufgabe, resilientere Wertschöpfungsketten zu schaffen, die den Rahmenbedingungen der VUCA- (volatil, unsicher, komplex und mehrdeutig) und BANI- (brüchig, ängstlich, nicht-linear, unbegreiflich) Welt gerecht werden. Noch bis vor wenigen Jahren stand bei der Planung von Wertschöpfungsketten das Lean-Konzept im Mittelpunkt.

Heute muss neben der Kostenminimierung die Lieferfähigkeit stärker in die Planung einbezogen werden, bei gleichzeitiger Kalkulation von Risiken entlang der Wertschöpfungsketten. Dies macht die Planung komplexer und damit auch die dabei eingesetzten Methoden und Instrumente.

Studie zeigt Möglichkeiten zur Optimierung auf

Die Autoren Dr. Martin Schwemmer, Geschäftsführer der BVL, und Saskia Sardesai, stellvertretende Abteilungsleiterin Supply Chain Engineering Fraunhofer IML, ordnen die Situation und die jüngsten Entwicklungen ein. Darauf aufbauend nennen sie mögliche Strategien, wie Unternehmen ihre Wertschöpfungsketten resilienter machen können. Möglichkeiten bieten demnach vor allem die Bereiche Kostenrechnung, Beschaffung, IT und digitale Infrastruktur sowie die Zusammenarbeit über die Unternehmensgrenzen hinaus.

Konferenzprogramm mit Fokus auf Resilienz

Die Session der BVL während der transport logistic „Der Einfluss der Geopolitik auf ihre Supply Chain - Aktuelle Einordnung und Ausblick" (9. Mai, 13:00 Uhr bis 14:00 Uhr, Forum Halle B2) beleuchtet diese und weitere Aspekte. Die Moderation übernimmt Dr. Tilo Bobel, Global Head of Continuous Improvement, Lean and Automation bei A.P. Moeller Maersk. Als Referenten dabei sind Dr. Udo Lange, President und CEO von FedEx Logistics Memphis, Andreas Schulz, Head of Main Department bei TRUMPF Werkzeugmaschinen, Thomas Heck, Partner und Leiter China Business Group in Deutschland & Europa bei PwC, sowie Wolfram Senger-Weiss, Vorsitzender der Geschäftsleitung bei Gebrüder Weiss.

Das Paper zum Download unter: www.bvl.de/resilienz

Messe Stuttgart

LogiMAT 2023 erzielt bestes Ergebnis seit Bestehen der Messe

Stabile Ausstellerzahl, erneut volle Flächenauslastung und stärkster Besucheransturm seit 20 Jahren: Die LogiMAT 2023 knüpft an den Vorjahreserfolg an und setzt ihren Wachstumskurs weiter fort. Das ist in Summe das beste Ergebnis seit Bestehen der Intralogistikmesse. Mit einem Anteil von 35 Prozent unter den Ausstellern unterstreichen Unternehmen aus 39 Nationen die Internationalität der Messe.

Mit einem deutlichen Besucherzuwachs gegenüber dem Vorjahresergebnis schloss die LogiMAT 2023 am heutigen Donnerstag ihre Tore. Während der drei Messetage kamen insgesamt 62.343 Fachbesucher (+25 %) auf das Stuttgarter Messegelände. Damit übertrifft die aktuelle Veranstaltung sogar das Vor-Pandemieergebnis von 2019. „Eine LogiMAT der Rekorde", konstatiert Messeleiter Michael Ruchty vom Messeveranstalter EUROEXPO GmbH, München. „Die LogiMAT 2023 erzielte den höchsten Besucherzuspruch seit Bestehen der Messe. Zusammen mit dem Zuwachs bei den internationalen Ausstellern belegt, dass die Marke LogiMAT als weltweit führende Messe und feste Größe für zukunftsfähige Auslegung effizienter Intralogistik-Prozesse fest etabliert ist."

In den komplett ausgebuchten zehn Messehallen des Stuttgarter Messegeländes präsentierten 1.563 Aussteller aus 39 Nationen ihre jüngsten Entwicklungen und Innovationen für optimale Materialflüsse und effizientes Prozessmanagement. 125.000 Quadratmeter genutzte Bruttoausstellungsfläche des Messegeländes boten den internationalen Ausstellern eine Nettoausstellungsfläche von 65.503 Quadratmeter (+8 %). Bereits im Vorfeld meldeten die Aussteller der LogiMAT 2023 mehr als 100 exklusive Produktpremieren. Darunter Weltneuheiten und weltweit einmalige Innovationen wie etwa der als „Bestes Produkt" in der Kategorie „Kommissionier-, Förder-, Hebe-, La-

gertechnik" ausgezeichnete 3D-Ultraschallsensor Toposens Echo One", den die Meysens GmbH für akustische Erfassung entwickelt hat.

Mit den Exponaten der Aussteller und dem bewährten Rahmenprogramm deckte die LogiMAT 2023 den Informations- und Wissenstransfer für zukunftsfähige Investitionen. Diese zielen auf Automatisierung, die digitale Transformation und die Einbindung moderner Technologien wie Robotik, Sensorik und Künstliche Intelligenz (KI) zur Optimierung der innerbetrieblichen Prozesse. Zudem standen Lösungen rund um die Themen Nachhaltigkeit und Energieeffizienz im Fokus der Aussteller und Fachbesucher. Das Fachpublikum nutzte die Präsenzmesse für Geschäftsanbahnungen und die Marktsondierung unter Wettbewerbern. Die Besucher gaben an, auf der LogiMAT gezielt etwa nach Automatisierungslösungen zu suchen, sich von neuen Technologien inspirieren zu lassen und potenzielle Kooperationspartner zu evaluieren. Die Aussteller verzeichneten entsprechend qualifizierte Kundenkontakte mit vielversprechenden Projektanfragen und Kooperationsvereinbarungen. Der Besucheranalyse vom unabhängigen Baseler Marktforschungsinstitut Wissler & Partner zufolge, kam ein hoher Prozentsatz der Fachbesucher mit konkreten Investitionsabsichten zur LogiMAT. Das bestätigen die zahlreichen gemeldeten Vertragsabschlüsse, die auf der LogiMAT 2023 getätigt wurden.

So gaben etwa das französische Technologieunternehmen Exotec und Generalunternehmer Unitechnik eine Kooperationsvereinbarung bekannt. Das türkische Robotikunternehmen Bottobo Robotics und Wiferion unterzeichneten einen Vertragsabschluss über die Lieferung induktiver Ladesysteme im vierstelligen Bereich. Der Hard- und Softwareanbieter Ecovium vereinbarte mit der Lux CT Transportlogistik die Installation einer Software für Transport- und Speditionsmanagement. Die Vertragsunterzeichnungen unterstreichen den Stellenwert der LogiMAT als Arbeitsmesse. Insgesamt erteilten mehr als 40 Prozent der Fachbesucher einen Zuschlag oder beabsichtigen, dies unmittelbar nach der Veranstaltung zu tun. Dabei übernehmen 84,2 Prozent der Messebesucher in ihrem Unternehmen Entscheiderfunktionen. Erneut hat die LogiMAT in diesem Jahr den Grad ihrer Internationalisierung weiter gesteigert. Bei fast jedem zweiten Fachbesucher war der Anreiseweg länger als 300 Kilometer. Jeder vierte reiste aus dem Ausland an. Gut zehn Prozent der Messesucher kamen aus Übersee. Unter den Ausstellern der LogiMAT 2023 ist der Anteil internationaler Unternehmen in diesem Jahr auf mehr als ein Drittel angewachsen. Weiteres Indiz für die Internationalität: Unter den rund 200 Neuausstellern, die dieses Jahr erstmals nach Stuttgart kamen, lag der Anteil internationaler Unternehmen bei fast 70 Prozent. „Das insgesamt hervorragende Ergebnis der LogiMAT 2023 übertrifft alle Erwartungen", resümiert Messeleiter Ruchty. „Netzwerken und direkter Informations- und Wissenstransfer zwischen allen namhaften Entwicklern, Herstellern und Lösungsanbietern mit einem Fachpublikum auf Rekordniveau. Zudem Vertragsunterzeichnungen im internationalen Rahmen. Das untermauert erneut die Position der LogiMAT als maßgebliche Branchenplattform der Intralogistik und Arbeitsmesse für Entscheider."

Die nächste LogiMAT ist die „LogiMAT China", die bereits vom 14.-16.06 in Shanghai veranstaltet wird. Vom 25.-27.10 öffnet die „LogiMAT Intelligent Warehouse" in Bangkok ihre Tore. Die kommende LogiMAT in Stuttgart findet vom 19.-21.03.2024 statt.

Preisgekrönte „BESTE PRODUKTE“ für mehr Effizienz in der Intralogistik

Ein innovativer Ultraschallsensor, der die Echoortung nutzt, wie sie von der Fledermaus bekannt ist, ein Ladungs-System für die autonome Lkw-Verladung und ein innovativer Algorithmus zur effizienten Routen- und Tourenplanung – das sind die innovativen Spitzenleistungen, die auf der diesjährigen LogiMAT 2023 mit dem renommierten Preis „BESTES PRODUKT“ ausgezeichnet wurden.

Die unabhängige Jury aus Wissenschaftlern und Journalisten wählte aus mehr als einhundert eingegangenen Bewerbungen drei würdige Preisträger aus, die dem Namen „BESTES PRODUKT“ alle Ehre machen. Sie erfüllen in herausragender Weise die Wettbewerbsbedingungen: Produktivitätssteigerung, Kostenersparnis und Rationalisierung. Die ausgezeichneten Unternehmen leisten mit ihren Produkten einen Beitrag zu sicheren Prozessen, zur flexiblen Anpassung bei Veränderungen sowie zur Effizienzverbesserung und somit letztlich zur Steigerung der Produktivität in der Logistik. Vergeben wurde der Preis „BESTES PRODUKT“ im Rahmen der feierlichen Eröffnung in der LogiMAT Arena am Vormittag des ersten Messetages. Die Laudatio hielt Prof. Dr.-Ing. Johannes Fottner, Ordinarius des Lehrstuhls für Fördertechnik Materialfluss Logistik der Technischen Universität München.

In der Kategorie **„Kommissionier-, Förder-, Hebe-, Lagertechnik“** ging der Preis an die MEYSENS GmbH (Eingang Ost, Stand EO91A, Gemeinschaftsstand „Innovation made in Germany“) für den 3D Ultraschallsensor Toposens ECHO ONE:
Der 3D Ultraschallsensor ECHO ONE ermöglicht es mobilen Robotern wie AGVs und AMRs, Kollisionen mit allen Arten von Hindernissen zu vermeiden. Im Gegensatz zu bestehenden Sensortechnologien, die durch Lichtverhältnisse oder Feuchtigkeit negativ beeinflusst werden können, nutzt der Sensor die Echoortung wie sie von der Fledermaus bekannt ist, um robuste 3D-Echoortungsdaten in Echtzeit zu erzeugen. Und das unabhängig von den jeweiligen Bedingungen vor Ort.
Die Sensorik unterscheidet sich dabei grundlegend von gängigen Sensor-Systemen, die meistens auf optischer Basis funktionieren und aufgrund dessen Schwachstellen in der Objektekennung verzeichnen, wenn die optischen Umgebungsverhältnisse nicht optimal sind. Dies kann zu vermeidbaren Kollisionen führen, wobei ein akustisch-basierender Sensor wie der ECHO ONE Abhilfe leisten kann. Er bietet eine 3D-Multi-Objekt-Erkennung von komplexen und transparenten Objekten im Ultranahbereich von 10 cm bis zu 3 m sowie ein sehr weites Sichtfeld von bis zu 160° im Ultranahbereich und bis zu 110° bei 3 m. Dies ist besonders wichtig für die Erkennung von Gabelstaplerzinken, welche in der sensorbasierten Objekterkennung zu den komplexen Objekten zählen und speziell in der Intralogistik und dort vor allem im Mischbetrieb Gefahrenpotential haben, wenn sie nicht zuverlässig erkannt werden.
Der Sensor kompensiert die Nachteile optischer Sensoren, die Probleme in der Erkennung von Glas oder spiegelnden Oberflächen haben können, durch schallbasierte Triangulation in Kombination mit hochentwickelter Rauschfilter-Software. So erzeugt er robuste 3D-Daten in Echtzeit für jedes erkannte Hindernis innerhalb der voll einstellbaren, dynamischen Warn- und Stoppzonen. Das System bietet digitale Ein- und Ausgänge sowie Ethernet als Hardware-Schnittstelle. Durch die Erkennung selbst der komplexesten Objekte in der Umgebung mit einer kleinen Blindzone werden kostspielige Unfälle reduziert und gleichzeitig höchste Sicherheit in jedem Anwendungsbereich gewährleistet. Daher ist er die ideale Lösung für eine sichere und zuverlässige Navigation von mobilen Robotern in der innerbetrieblichen Logistik.

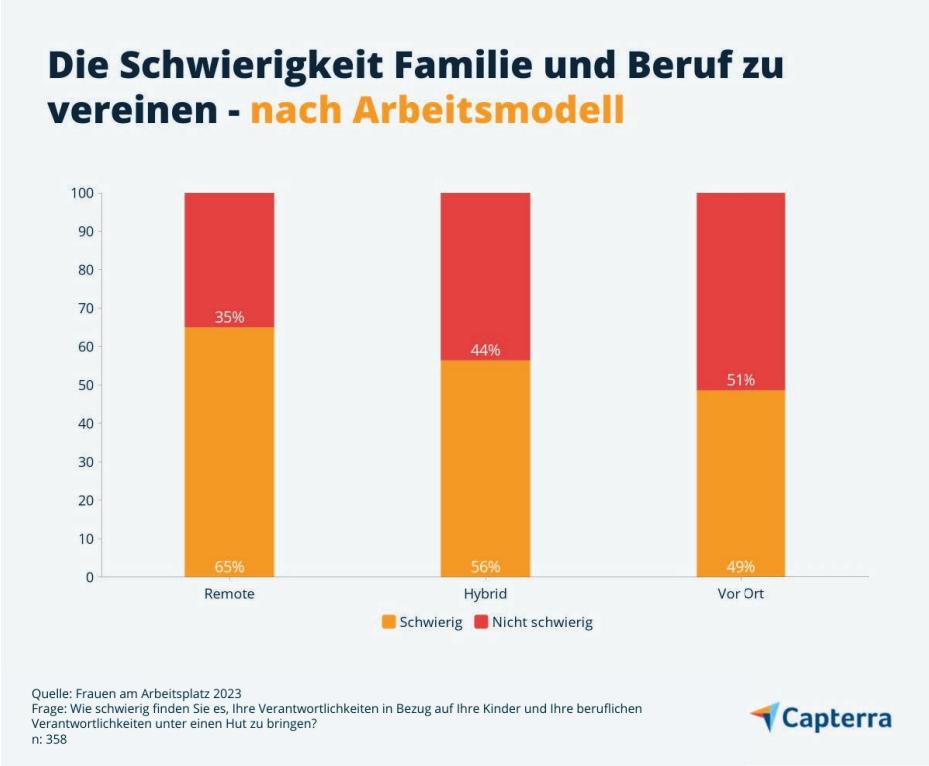
In der Kategorie **„Identifikation, Verpackungs- und Verladetechnik, Ladungssicherung“** wurde der Preis der TRAPO GmbH verliehen (Halle 5, Stand 5D53). Ausgezeichnet wurde

das Be- und Entladesystem TLS 3600, das Palettenladung autonom vom Lager bis in den Lkw hinein verlädt.
Das TLS 3600 schließt die Sicherheitslücke in der Ladezone. Es kann in Kombination mit Fahrerlosen Transportsystemen die üblichen Gabelstapler-Transporte von Palettenware zwischen Produktion, Lager und Verladezone durch einen vollautomatisierten Prozess ersetzen und schafft so Personen- und Warensicherheit beim Be- und Entladen.
Flüsterleise ist es in der Ladezone, wo üblicherweise emsiger Staplerverkehr herrscht. Nach Ankunft meldet sich der Lkw-Fahrer aus der Wartezone heraus über die Bedienfläche eines Monitors an. Dies löst das automatisierte Be- oder Entladen aus. Das TLS realisiert den Warenumschlag im Sinne einer effektiven Gesamtlogistik sicher, automatisiert mit kurzen Wegen und bei Bedarf 24/7. Seinen Namen erhielt das TLS 3600 von einem besonderen Feature: Es verlädt in einem Arbeitsgang parallel jeweils drei Paletten à 1.200 kg, entsprechend 3.600 kg.
Die Anlieferung der Paletten erfolgt wahlweise durch konventionelle Technik, einen Shuttle-Schwarm oder ein XXL-Shuttle, letzteres liefert jeweils drei Paletten gleichzeitig an. Verladen in drei Schritten: Zunächst werden bis zu drei Paletten auf der Fördertechnik nebeneinander in Reihe platziert (Schritt 1) und ausgerichtet. Es folgen die Aufnahme (Schritt 2) und das Verladen der Reihe (Schritt 3). Während des Verladevorgangs wird die nachfolgende Palettenreihe gebildet und bereitgestellt. Ein kontinuierlicher Ablauf, der Zeit und Wegstrecke spart.
Wettbewerber bieten vor allem One-Shot-Systeme an. Sie stellen die gesamte Lkw-Ladung in der Ladezone bereit, bevor sie in einem Zug verladen wird. Vor allem aber wird in der ohnedies knapp bemessenen Fläche viel Raum unnötig durch Stellplätze von etwa 20 Metern Länge blockiert. Das TLS 3600 beweist Flexibilität: Optimal eingebunden in die Lagerlogistik, agiert das TLS autonom, denn es ist sowohl als starres System als auch zwischen Ladeluken verfahrbar und korrigiert bei Einfahrt in den Lkw per Hinterradlenkung selbsttätig seine Position an der Rampe.

In der Kategorie **„Software, Kommunikation, IT“** ging der Preis an die Greenplan GmbH – Member of EPG (Halle 8, Stand 8A71) für den Greenplan-Algorithmus zur Routenplanung. Greenplan ist ein SaaS-Anbieter zur Planung dynamischer Routen, die sowohl effizient, als auch nachhaltig sind. Die Routenplanung basiert auf einem mathematischen Algorithmus, der Effizienzsteigerungen von bis zu 20 % ermöglicht. Zwei weitere Besonderheiten: die dynamische Planung und das Konzept der Overlapping Districts. Volldynamische Routen lösen feste Lieferdistrikte vollständig auf. Dadurch kommt es zur Optimierung der gesamten Liefergebiete und verbesserten Ausbalancierung der Volumina über alle Touren hinweg. Gleichzeitig werden die Fahrzeiten optimiert, was in Kosteneffizienzen resultiert. Die täglichen Touren variieren, da diese auf den tatsächlichen Sendungsmengen basieren und nicht auf Durchschnittswerten. Somit kann die Anzahl der Touren signifikant reduziert werden (ein europäisches Postunternehmen konnte anstatt mit 63 Vehikeln mit 32 Vehikeln pro Woche planen), sodass letztendlich auch weniger CO2 -Emissionen entstehen. Overlapping Districts bieten den Kompromiss zwischen volldynamischen Routen und festen Lieferdistrikten. Sie lösen die unausgewogenen Routen, die beispielsweise durch Postleitzahlgebiete entstehen, auf. Sie überlappen an ihren Grenzen um einige Kilometer, so dass Fahrer auch Adressen anfahren können, die in der Nähe ihrer eigentlichen Ziele liegen z. B. naheliegende Parkplätze gezielt eingeplant werden können.
Eine weitere Herausforderung in der Routenplanung: Trotz einer vermeintlich optimalen Planung kommt es oft zu Ineffizienzen und Problemen, denn die tatsächliche Verkehrslage wird bei den meisten Routenplanern nicht berücksichtigt. Greenplan hingegen arbeitet mit historischen Geschwindigkeitsprofilen. Diese geben Auskunft darüber, zu welcher Uhrzeit auf welchem Straßenabschnitt welche durchschnittlichen Geschwindigkeiten gefahren werden. So entstehen tageszeitabhängige Fahrzeiten, die die optimale Planung von Stopps und das Einhalten von Zeitfenstern ermöglichen. Da die Fahrtzeiten auf derselben Straße im Laufe des Tages erheblich variieren, wirkt sich dies natürlich auch auf die Stoppplanung aus. Der Algorithmus identifiziert die optimalen Routen aus realen, straßenspezifischen Fließgeschwindigkeiten des Verkehrs und erkennt so, wann es wirklich Sinn macht ein Vehikel beispielsweise in eine Hauptstraße fahren zu lassen. So werden Staus vermieden, Fahrer verbringen weniger Zeit im Verkehr und eine zusätzliche Verstopfung der Innenstädte bleibt aus.

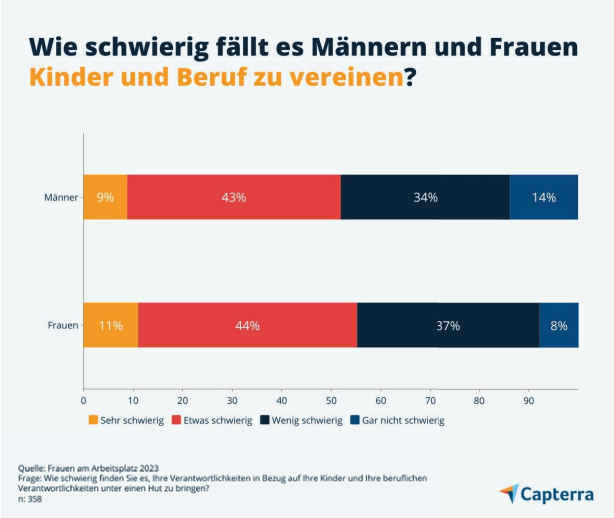
Vereinbarkeit von Familie und Beruf

Studie stellt fest: 68 % der Eltern erhalten nicht genug oder gar keine Unterstützung vom Arbeitgeber



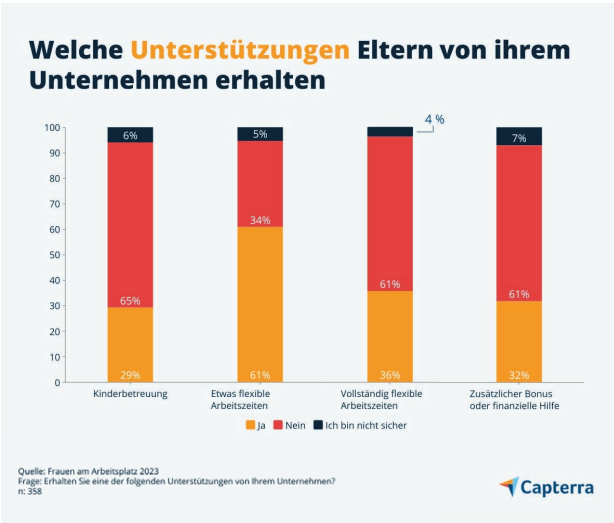
Eltern im Homeoffice nach Arbeitsmodell

Berufstätige Frauen streben heute eine gleichberechtigte Karriere an. Doch wie schwierig ist es heutzutage, Familie und Beruf unter einen Hut zu bringen? Und welche Herausforderungen erleben Frauen anders als Männer? Die Software-Bewertungsplattform Capterra befragte 994 Teilnehmer zur Vereinbarkeit von Familie und Beruf, darunter 515 Frauen und 479 Männer. Die Studie zeigt, wie Eltern damit umgehen und was Unternehmen tun können, um ihre Mitarbeiter besser zu unterstützen.



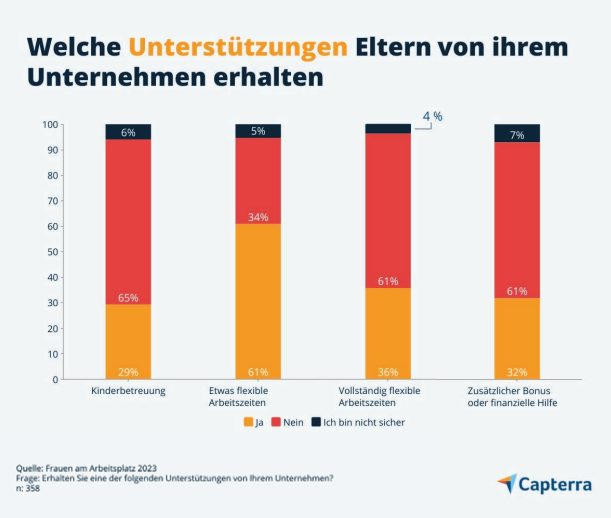
Highlights der Studie:

- 68 % der Eltern erhalten nicht genug oder gar keine Unterstützung vom Arbeitgeber, um Arbeit und Privatleben in Einklang zu bringen
- 77 % der Eltern haben Schwierigkeiten Privat- und Arbeitsleben im Home-Office zu balancieren
- Mütter in der Arbeitswelt sind besonderen Schwierigkeiten ausgesetzt: 36 % der Frauen mit Kindern erfahren mehr Vorurteile bei Beförderungen, im Gegensatz zu 19 % ohne Kinder. Bei Gehaltserhöhungen sind es sogar 40 % im Gegensatz zu 27 %.



Lückenhafte Unterstützung der Eltern seitens der Unternehmen

Für erwerbstätige Eltern werden Unterstützungsleistungen wie Kinderbetreuung, flexible Arbeitszeiten oder finanzielle Unterstützung bei der Gesundheitsvorsorge wichtig, um mit der Kinderbetreuung verbundene Belastungen zu reduzieren. Dass sie von ihrem Unternehmen Unterstützung erhalten und damit zufrieden sind, geben jedoch nur 32 % der befragten Eltern an. 48 % erhalten nicht genügend Unterstützung, um Beruf und



Familie miteinander zu vereinbaren. 20 % erhalten überhaupt keine Unterstützung (davon 18 % Männer und 23 % Frauen).
In den meisten Unternehmen werden Mitarbeitende mit Kindern durch (teilweise) flexible Arbeitszeiten unterstützt, in 36 % der Unternehmen sogar durch vollständig flexible Arbeitszeiten. Knapp ein Drittel der Unternehmen bietet zudem einen zusätzlichen Bonus und Kinderbetreuung an.

Im Home-Office ist die Vereinbarkeit von Familie und Beruf schwerer

„Entgegen unserer Erwartungen und der vielen Vorteile, die Eltern im Home-Office haben, ist die Vereinbarkeit von Familie und Beruf bei der Arbeit von zu Hause schwieriger. 65 % der Remote-Mitarbeiter geben an, dass es sehr oder etwas schwierig ist, Verantwortlichkeiten in Bezug auf ihre Kinder und ihre beruflichen Verantwortlichkeiten unter einen Hut zu bringen. Dagegen finden es ‚nur' 49 % der vor Ort arbeitenden Angestellten schwierig", kommentiert Ines Bahr, Senior Analystin bei Capterra.
Schaut man sich die Antworten der Remote-Eltern genauer an, so haben 77 % Schwierigkeiten damit, Arbeits- und Privatleben zu Hause zu balancieren. Lediglich 23 % der befragten Eltern geben an, keine Schwierigkeiten damit zu haben. Zwischen Männern und Frauen gibt es hierbei keine signifikanten Unterschiede.

Frauen sind jedoch mehr als Männer von Work-Life-Blending betroffen. 31 % der Mütter geben an, dass es für sie schwierig ist, Arbeits- und Privatleben zu trennen, wenn sie von zu Hause aus arbeiten und nennen u.a. folgende Probleme:

- Ich habe nach der Arbeit nie wirklich Feierabend (38 %)
- Die Qualität meiner Arbeit leidet manchmal, weil ich mich um Familie, Haustiere, Hausarbeit usw. kümmern muss (38 %)
- Ich mache Überstunden (29 %)
- Ich bin mir nicht sicher, ob ich meine vertraglich vereinbarte Wochenarbeitszeit erreiche (29 %)

Mütter in der Arbeitswelt stehen vor besonderen Herausforderungen

27 % der Mütter, die zum Zeitpunkt der Schwangerschaft in einem Unternehmen beschäftigt waren, gaben an, dass sie keine Unterstützung erhalten haben, nachdem sie ihren Arbeitgeber über ihre Schwangerschaft informiert haben. 46 % der Frauen gaben sogar an, sich Sorgen um ihre Arbeitsstelle gemacht zu haben, als sie von der Schwangerschaft erfuhren. Die Studie zeigt, dass Frauen mit Kindern in höherem Maße mit Vorurteilen oder Diskriminierung zu kämpfen haben, wenn es um eine Beförderung oder um eine Gehaltserhöhung geht. 36 % der Frauen mit Kindern bestätigen, dass sie im Hinblick auf eine Beförderung mit mehr Vorurteilen zu kämpfen haben, im Vergleich zu 19 % der Frauen ohne Kinder. Bei Gehaltserhöhungen sind es sogar 40 % gegenüber 27 %.

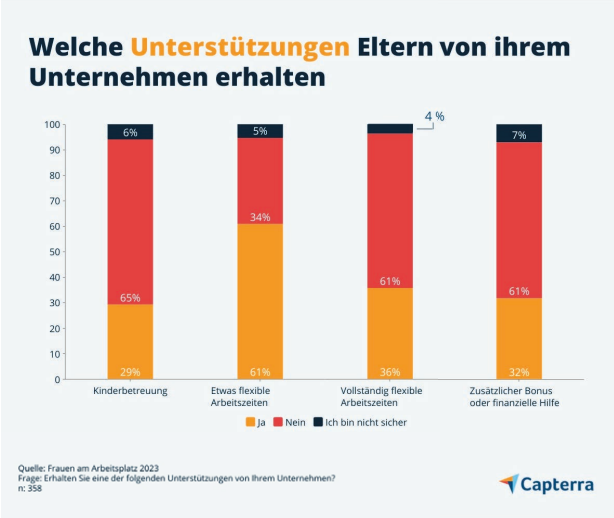
Darüber hinaus sagen 40 % der Frauen mit Kindern, dass sie bei Projekten häufiger übergangen werden, weil die anderen Teammitglieder der Meinung sind, dass sie bereits zu beschäftigt sind. Dies könnte einer der Gründe dafür sein, dass Frauen schlechter abschneiden, wenn es darum geht, ihr Gehalt zu erhöhen

oder eine Beförderung zu erhalten.

Tipps für Unternehmen zur Unterstützung von Familien

Es ist wichtig, dass Unternehmen erwerbstätige Eltern unterstützen und die Vereinbarkeit von Beruf und Familie fördern. Beispielsweise könnten sie ihre Zielvereinbarungen auf monatlicher statt auf täglicher oder wöchentlicher Basis überprüfen, um den potenziellen Stress zu verringern, der mit täglichen Höchstleistungen verbunden ist. Hier sind 6 Tipps, wie die Personalabteilung im Unternehmen unterstützen kann:

- Die Mitarbeiter sollten regelmäßig befragt werden, um herauszufinden, welche Unterstützungen den Eltern im Unternehmen wirklich dienen. Mitarbeiterbefragungen helfen, die angebotenen Leistungen an individuelle Bedürfnisse anzupassen.
- Allen Mitarbeitern durch Weiterbildungs-, Schulungs- und Mentoringprogramme berufliche Entwicklungsmöglichkeiten bieten. Diese können auch während der Elternzeit angeboten werden, damit der Kontakt zum Unternehmen bestehen bleibt.
- Ein elternfreundliches Umfeld schaffen, das die Unterstützung berufstätiger Eltern zum zentralen Unternehmenswert macht. Wirksame Maßnahmen sind z. B. die Bereitstellung von Ressourcen, die ihnen helfen, ihre Doppelrolle als Eltern und Mitarbeiter zu bewältigen, Selbsthilfegruppen einzurichten und Familientage mit Kinderveranstaltungen zu organisieren.
- Ein weiterer Tipp ist, die Unterstützung für werdende und neue Mütter im Unternehmen transparent und offen zu gestalten. Dazu gehören Unterstützungsmöglichkeiten, die Eltern helfen, Beruf und Familie zu vereinbaren, sei es durch flexible Arbeitszeiten, Kinderbetreuungsangebote oder andere Leistungen.
- Die Arbeit von zu Hause aus kann den Stress für berufstätige Mütter und Väter erhöhen, da ihre Verpflichtungen in Bezug auf die Kinderbetreuung mit ihrer Arbeit kollidieren können. Hier kann die Bereitstellung von Zeiterfassungstools für projektbezogene Arbeitszeiten, Projektmanagement-Tools oder Home-Office-Software den Arbeitsalltag erleichtern.
- Für Beschäftigte, die sich in einer veränderten Familiensituation befinden, ist ein Mitarbeiterhilfeprogramm (EAP) hilfreich. Durch eine möglichst integrative und transparente Gestaltung des Arbeitsplatzes können sich schwangere Arbeitnehmerinnen unterstützt und einbezogen fühlen.



Methodik:
Capterra führte im Januar 2023 eine Online-Umfrage unter 994 Beschäftigten durch, darunter 515 Frauen (wovon 154 Kinder unter 18 Jahren haben, mit denen Sie zusammenleben) und 479 Männer (204 mit Kindern im Haushalt).

Teilnehmer wurden anhand folgender Kriterien ausgewählt:
> wohnen in Deutschland
> sind zwischen 18 und 65 Jahre alt vollzeit- und teilzeitbeschäftigt oder in Elternzeit arbeiten in einem Unternehmen mit mehr als einem Beschäftigten sind nicht als Praktikant/in tätig.

Brandschutz ist Umweltschutz

Auch in der Logistik

WAGNER adressiert das Thema auf der LogiMAT 2023 und erläutert, wie neben dem Schutz von Leben und Werten sowie der Erhaltung der Lieferfähigkeit auch Nachhaltigkeitsziele durch Brandschutz erreicht werden können

Nachhaltigkeit ist auch in der Logistik ein zentrales Thema. Denn der Schutz von Luft- und Wasserqualität sowie die Reduzierung von Emissionen sind eine gesamtgesellschaftliche Aufgabe, und Nachhaltigkeit ist mittlerweile zum zentralen Wirtschaftsfaktor geworden. Auf der LogiMAT 2023 in Stuttgart stellt die WAGNER

Group GmbH als einer der Technologieführer in den Bereichen Branderkennung und Brandvermeidung vom 25. bis 27. April in Halle 7 am Stand C15 vor, wie Logistikunternehmen durch ganzheitlichen Brandschutz ihren Beitrag zum Klima- und Umweltschutz leisten – und wie entsprechende Brandschutzlösungen sie bei der Umsetzung und Erreichung ihrer Nachhaltigkeitsziele unterstützen.

Ökologische Schäden durch Brandereignisse

„Wenn es um die Planung und die vielfältige Nutzung von Lagerimmobilien geht, sollte im Zuge einer Risiko-, Wirtschaftlichkeits- und Schutzzielbetrachtung immer auch das Thema Brandschutz in die Überlegungen einbezogen werden", so Steffen Springer, Geschäftsführer der WAGNER Group GmbH. Stichwort: Lagerlogistik mit hoher Wertekonzentration. Brandereignisse vernichten Sachwerte der Immobilie und des Lagerguts und können die Lieferfähigkeit gefährden. Darüber hinaus sind die ökologischen Folgen oft fatal: Rauchgase, Rauch- und Rußpartikel und andere, potenziell toxische Stoffe und Verbindungen werden freigesetzt, abhängig auch von der Lagerware. Bei jeder Verbrennung kommt es zudem zum Ausstoß großer Mengen an CO_2. Brandrückstände sowie nicht-zerstörungsfreie Löschmittel, die im Zuge einer Brandbekämpfung eingesetzt werden, können teilweise katastrophale Folgeschäden verursachen, kontaminiertes Löschwasser kann die Sauberkeit des Grundwassers gefährden.

„Jeder Brand, der vermieden werden kann, ist die beste Lösung, um die Gefährdung von Menschen auszuschließen sowie Prozesse und die Umwelt zu schützen. Aktive Brandvermeidung, die mit dem Prinzip der Sauerstoffreduktion in den zu schützenden Bereichen arbeitet, ist dafür eine der effektivsten Möglichkeiten", stellt Steffen Springer fest. „Zu diesem Zweck haben wir unser OxyReduct® -System entwickelt."

Sonderfall Lithium-Ionen-Batterien

Die Nachfrage nach neuen Lagerflächen ist ungebrochen, und zunehmend geht es dabei um die Lagerung von Lithium-Ionen-Batterien. Einer der Treiber ist die Automobilindustrie mit ihren steigenden Volumina im Bereich E-Mobility. In Deutschland wird dies gerade besonders augenscheinlich an der neuen Tesla-„Gigafactory" in Brandenburg – und an den Plänen der Bundesregierung, mindestens 15 Millionen E-Autos bis 2030 auf Deutschlands Straßen zu bringen.* Aber auch in anderen Branchen werden Lagerlösungen für diese Energiespeicher benötigt, die beispielsweise auch in Laptops und Smartphones sowie in E-Bikes zum Einsatz kommen.

Kuno Neumeier, CEO der Logivest und Sprecher des Themenkreises Logistikimmobilien der Bundesvereinigung Logistik (BVL), prognostiziert die Größe der benötigten Lagerfläche für Lithium-Ionen-Batterien auf ca. 7 Millionen Quadratmeter bis zum Jahr 2030.**

In puncto Lagerung stellen diese Energieträger besondere Anforderungen an den Brandschutz, denn sie bergen die Gefahr einer Selbstentzündung durch einen Thermal Runaway – teilweise mit fatalen wirtschaftlichen sowie umweltgefährdenden Folgen. Bei einem Thermal Runaway lässt sich der Brandprozess nicht durch Löschen unterbrechen, Schadstoffe werden freigesetzt, und ein Überspringen auf anderes Lagergut führt häufig zu einer schnellen Brandausbreitung.

Um insbesondere bei der Lagerung des Gefahrgutes Lithium-Ionen-Batterie die Ware vor Schäden durch Feuer zu schützen, Betriebsunterbrechungen und ihre Folgeschäden zu verhindern, die Lieferfähigkeit zu erhalten und eine Umweltgefährdung zu vermeiden, sind ganzheitliche Brandschutzlösungen unverzichtbar. Diese bestehen aus frühestmöglicher Branderkennung in Kombination mit aktiver Brandvermeidung und Maßnahmen des organisatorischen Brandschutzes. Auf der LogiMAT präsentiert WAGNER am Beispiel des Referenzprojektes für die KETTLER Alu-Rad GmbH wie eine solche ganzheitliche und individuell für den Kunden konzipierte Lösung aussehen kann.

Weitere Informationen zur Messepräsenz von WAGNER unter: bit.ly/3KAWPes

Thema 'Brandschutz ist Umweltschutz':: bit.ly/3KA9NsR

Quellen:
***https://www.bundesregierung.de/breg-de/themen/klimaschutz/eenergie-und-mobilitaet/nachhaltige-mobilitaet-2044132**
**** https://www.logivest.de/news/lithium-ionen-batterien-fordern-deutschen-logistikimmobilienmarkt**

STÖBICH BRANDSCHUTZ

Förderanlagenabschlüsse

Vielfältige Produktions- und Logistikprozesse erfordern unterschiedlichste Bauarten von Förderanlagen. Wenn diese Förderstrecken durch feuerhemmende bzw. feuerbeständige Wände oder Decken führen, müssen die hierfür notwendigen Öffnungen mit Feuerschutzabschlüssen versehen werden, um eine Ausbreitung des Feuers über die Fördertechnik oder das Fördergut zu verhindern.

Im Brandfall müssen Förderanlagenabschlüsse (kurz FAA) diese Öffnungen unverzüglich und automatisch verschließen. Dabei kommt es auf einen nach DIN EN 13501-2 klassifizierten Feuerwiderstand ebenso an, wie auf das reibungslose Freiräumen der Schließbereiche im Auslösungsfall.

Optische Branderkennung

Je eher ein Feuer erkannt wird, desto effizienter kann es bekämpft werden. Mithilfe von optischen Sensoren erkennt der FireMultiDetector frühzeitig, wenn ein Brand entsteht – und kann so eine schnelle Ausbreitung von Flammen und toxischen Brandgasen verhindern. Via App alarmiert das smarte System mit der patentierten Erkennungssoftware zuverlässig im Brandfall. Eingesetzt wird es z. B. auf Recyclinghöfen und in Tiefkühllagern.

Der Kern der Lösung zur Vermeidung – insbesondere von großen Bränden – ist die Reduzierung der Zeit zwischen Brandentstehung und Branderkennung durch den Einsatz von optisch-thermischen Detektoren in Verbindung mit der patentierten Erkennungssoftware.

Möglich macht dies die Erkennung von Rauch, Temperaturen und natürlichen Flammen mit nur einem Detektor. Störgrößen wie Wolken, Sonne, Nebel, Staub oder wärmeabgebende Fahrzeuge führen nicht zu Fehlalarmen. Somit ist diese Lösung hervorragend geeignet für den Innen- und Außenbereich, besonders bei großen Überwachungsflächen. Die 24/7-Verfügbarkeit sorgt für große Sicherheit in Verbindung mit der intelligenten Informationsverarbeitung und dafür, dass alle notwendigen Stellen sofort informiert, alarmiert und mit wichtigen Zusatzinformationen versorgt werden. Mit dieser Lösung gehören große Brände mit all ihren einschneidenden Folgen für Mensch, Betrieb und Umwelt der Vergangenheit an.

Löschmethoden

Es gibt energie- und umweltschonende Alternativen zu herkömmlichen Löschmethoden. Niederdruckwassernebelanlagen (NDWN) zum Beispiel: Sie erzeugen im Nieder-

GCC
Schlanker, platzsparender Förderanlagenabschluss in Elementbauweise

ECCLOS®-S
Förderanlagenabschluss für Vertikalheber (universeller Deckenabschluss)

ECCLOS®-Q
Förderanlagenabschluss als platzsparende, robuste Klappe in Blechpaneelbauweise

ECCLOS®-K
Förderanlagenabschluss in robuster Schieberbauweise für obenliegende Fördertechnik

ECCLOS®-D
Förderanlagenabschluss als ökonomische Kombination von Manschette und Tor

ECCLOS®-FLEX-I
Einteiliger, vertikal schließender Feuerschutzabschluss im Zuge bahngebundener Förderanlagen

druckbereich einen feinen Wassernebel und damit eine größere Oberfläche aus winzigen Wassertröpfchen. Mit weniger Wasser wird so ein höherer Kühleffekt erzielt. In Kombination mit einer Brandfrüherkennung und einer Brandmeldezentrale wird die NDWN-Anlage zu einer effizienten und wirtschaftlichen Systemlösung.

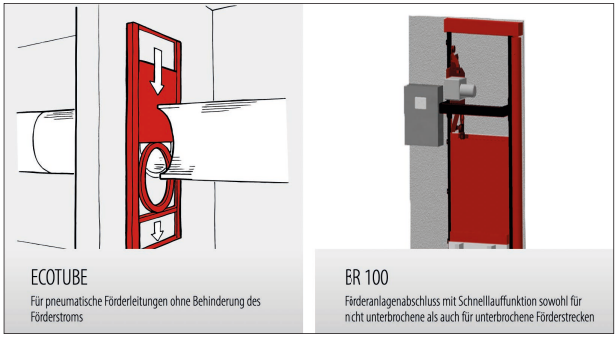
Die Niederdruckwassernebelanlage (NDWN) stellt eine umweltschonende Alternative zu vielen herkömmlichen Löschmethoden dar und findet in vielen unterschiedlichen Bereichen Anwendung. Durch den geringeren Verbrauch an Wasser und Strom arbeitet sie sehr effizient. Der durch Druck und spezielle Düsen erzeugte Wassernebel bekämpft Brände durch seine hohe Kühlleistung und den Effekt der Sauerstoffverdrängung besonders gut und schnell.

Die kompakte Bauweise führt dazu, dass die Niederdruckwassernebelanlage auch in Bereichen mit wenig Platz installiert werden kann, wie z. B. an Teststänten oder Trafostationen. Geringe Betriebs- und Wartungsaufwände ermöglichen einen preisgünstigen Betrieb. Diese Anlage kann auf Kundenwunsch in Kombination mit einer Brandfrüherkennung zu einer Systemlösung konzipiert werden.

STÖBICH Brandschutz: Lagerung / Transport

Für die sichere Lagerung und den ADR-konformen Transport von Energiespeichern gibt passgenaue Lösungen in verschiedenen Größen. Ha- variert eine Lithium-Ionen-Batterie im Inneren, können keine giftigen Flüssigkeiten, Feststoffe und Flammen nach außen dringen. Ein ausgeklügeltes Zusammenspiel von Gasfiltersystem, Thermomanagement, druckfester Konstruktion und standhafter Verriegelung macht es möglich.Die StrainBox xs bis XL ermöglichen es, kritische und defekte Lithium-Ionen-Batterien ADR-konform zu befördern und sicher zu lagern. Größe und Bauweise wurden speziell für die Lagerung und den Transport von Batterien und Modulen, wie sie zum Beispiel in batterieelektrischen Fahrzeugen verbaut werden, konzipiert. Alle Verpackungen der StrainBox Serie verfügen über ein integriertes Filtersystem, das die toxischen Gase zu einem großen Teil herausfiltert. Gesundheitsschädliche Stäube und Partikel werden zurückgehalten und der Austritt von Feststoffen, Flüssigkeiten und Flammen wird verhindert. Durch das integrierte

Thermomanagement kommt es zu keiner kritischen Temperaturerhöhung der Außenwände. Sollten die Batterien im Inneren havarieren, so wird eine Kontamination im Umfeld der Verpackung verhindert. Zum Schutz von Personen und Sachgütern verfügt auch die StrainBox XL über die typischen Sicherheitsmerkmale, die so nur die Produkte der Stöbich Brandschutz GmbH bieten. Dazu zählen das Filtersystem, die mechanisch standhafte Bauweise und das



ECOTUBE

Für pneumatische Förderleitungen ohne Behinderung des Förderstroms

ER 100

Förderanlagenabschluss mit Schnelllauffunktion sowohl für nicht unterbrochene als auch für unterbrochene Förderstrecken

integrierte Thermomanagement. Lithium-Ionen-Batterien erzeugen bei einer Havarie Druckstöße, die von Explosionen begleitet werden können. Die dabei entstehenden Gase sind hochgiftig. Das Gefährdungsszenario hat sich im Vergleich zu den klassischen Gefahrgutschränken dadurch grundlegend verändert. Die Feuergefahr wirkt nicht meh von außen auf den Schrank, sie wirkt von innen und ist von Flammen, Explosionen und giftigen Gasen begleitet. Der StrainLock ist die Lösung zur sicheren Lagerung von Lithium-Ionen-Batterien. Die Neuentwicklung für dieses spezielle Gefahrenszenario besitzt ein Filtersystem, das toxische Gase und Stäube genauso wie Funken und Flammen zurückhält. Durch das integrierte Thermomanagement wird eine kritische Temperatur der Außenwände verhindert. Sollte eine Batterie im Inneren des StrainLock havarieren, dann verhindern die Sicherheitsmerkmale eine Brandausbreitung und die Kontamination des Umfelds.

Flut- und Lagercontainer

Die Flut- und Lagercontainer dienen zur sicheren Aufnahme von defekten und nicht defekten Batteriespeichern. Jeder der stationären Container ist so ausgelegt, dass dort Batterien mit einer Gesamtnennenergie von 125 kWh gelagert werden können. Über die integrierte Branddetektion wird im Havariefall eine schnelle Flutung des jeweiligen Lagerplatzes veranlasst. So werden die Batterien frühzeitig gekühlt und ein Thermal Runaway bestmöglich verhindert. In dem zentralen Wasserspeicher mit Frostschutz und Wasseraufbereitung steht Wasser für die Flutung beider Container bereit. Um einen ausreichenden Umweltschutz zu gewährleisten verfügt das System über Schadgasfilter. Das System kann neben der optisch-akustischen Alarmierung vor Ort auch in eine bestehende Brandmeldeanlage integriert werden. Zusätzlich ist eine Status- und Alarmmeldung über die SMC-App auf mobilen Endgeräten möglich.

Nürnberg, Germany
21.–22.6.2023

FeuerTrutz 2023

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

FeuerTrutz
Eine Marke von
RM Rudolf Müller Medien

feuertrutz-messe.de

NÜRNBERG MESSE