FOCUS ON SECURITY

AUSGABE 12, DEZEMBER 2017

SECURITAS

Inhaltsverzeichnis

Alarmkonzept

Rainer Dietsche, Marquart Sicherheit und Security AG, zeigt in der Ausgabe 5-2017 der Zeitschrift Sicherheitsforum, S. 18–21, den Weg zu wirkungsvollen Alarmierungskonzepten. Sie bestünden nicht nur aus raffinierter Technik. Ebenso wichtig seien eine sorgfältige Planung der Alarmierung und die organisatorischen Maßnahmen rund um die Technik. Der Autor behandelt den Stellenwert der Alarmierung, das Alarmierungskonzept, Planung, Umsetzung und Inbetriebnahme, die Systemevaluation und den Betrieb. **Building Information Modeling** (BIM) stehe noch am Anfang. Wer aber in Zukunft diese neuen Möglichkeiten nutzt, sei auf dem richtigen Weg, wirkungsvolle Alarmierungskonzepte zu erstellen.

Anschläge

Zeit.online berichtet am 6. November unter Berufung auf das BKA, dass trotz einer rückläufigen Tendenz in Deutschland im Durchschnitt noch immer fast jeden Tag ein Anschlag auf eine Asylbewerberunterkunft verübt werde. In den ersten neun Monaten 2017 seien es 211 gewesen. Bei der überwiegenden Mehrheit sei ein rechtsradikaler Hintergrund ermittelt worden. 2015 seien 1.031, 2016 rund 1.000 Anschläge registriert worden.

Baustellenüberwachung

Baustellenüberwachung wird in der Ausgabe 11-2017 der Zeitschrift PROTECTOR, S. 28, thematisiert. Um einen größtmöglichen Detektionserfolg sicherzustellen, müsse die Technik exakt auf die Anforderungen des harten Baustellenalltags und die jeweiligen örtlichen Gegebenheiten ausgerichtet sein. Bei Baustellen im innerstädtischen Bereich sollten angrenzende Wohnhäuser und ihre Bewohner nicht erfasst werden. Vorgestellt wird das System **„Video Guard Professional"** der International Security Group GmbH und der Maibach Verkehrssicherheits- und Straßenausrüstungsprodukte GmbH. Das System setze auf drei Kameras mit unterschiedlichem Öffnungswinkel. So werde der Erfassungsbereich maximiert und auf die verschiedenen Anforderungen im Nah- und Fernbereich eingegangen. Zeitgleich werde durch die Addition der Sichtfelder ein Bereich von 170 Grad erfasst. Die Kameras verfügten über einen hochauflösenden Bildsensor und im Nachtbetrieb zusätzlich über einen motorischen NIR-Filter.

Betrug

Betrüger erbeuten Millionen von der Post, titelt die FAZ am 20. November. Durch großangelegte Betrügereien soll ein Netz von Kriminellen die **Deutsche Post** um Millionenbeträge geschädigt haben. Offenbar hätten sie sich von der Post massenhaft Rabatte für fingierte Briefe auszahlen lassen. Vorwiegend sollen Mitarbeiter von privaten Briefdiensten beteiligt gewesen sein, die mit der Post um die Briefe von Großversendern konkurrieren. Für die eingelieferten Briefe stellt die Post den als „Konsolidierer" bezeichneten Briefdiensten zunächst das übliche Porto in Rechnung. Anschließend überweist sie für den Transport und die Versandvorbereitung einen mengenabhängigen Rabatt zurück. Den Betrügern sei es offenbar gelungen, „virtuelle Mengen" in das System einzuspeisen und dafür Rückerstattungen zu ergaunern, ohne dass ihnen die Post vorher eine Rechnung geschrieben hat. Den Schaden bezifferten Insider auf 50 bis 100 Mio. Euro. Nach Angaben der Staatsanwaltschaft machten sich die Betrüger Lücken im Kontrollsystem der Post zunutze. Pikant sei, dass eine Spur sogar zu einem „Konsolidierer" führe, an dem die Post selbst beteiligt ist: dem Zustelldienst Compador.

Am 23. November berichtet die FAZ vom „größten Betrugsfall aller Zeiten in der **Online-Werbung**". Adform, selbst eine Einkaufsplattform für Werbeanzeigen im Internet, habe den Fall aufgedeckt und schätze, dass Werbekunden jeden Tag zwischen 262.000 und 1,3 Mio. Euro praktisch umsonst zahlten, weil ihre Anzeigen nicht von Menschen, sondern von Bots, also Computerprogrammen angeklickt worden seien. Der Betrug sei global: Betroffen seien neben den internationalen Werbern hauptsächlich Internetnutzer in den USA, deren Rechenzeit und Strom dafür gestohlen worden seien, Werbeanzeigen anzuklicken. 34.000 Internetadressen hätten die Betrüger gefälscht und mehr als 1,5 Mio. Aufrufe am Tag erzeugt.

Biometrie

Heise.de weist am 17. November darauf hin, dass BKA-Präsident Münch angekündigt habe, dass Deutschland als erstes europäisches Land seine **Fingerabdruck-Datenbank AFIS** an das Schengener Informationssystem SIS II anschließt. Die Fahndung allein mittels Fingerabdruck müsse dringend modernisiert werden. Unter Frankreichs Federführung arbeite Deutschland an einem neuen Abfragesystem mit, das den Abruf von Fingerabdrücken und weiteren Biometrie-Daten nach dem Prümer Vertrag über ganz Europa hinweg vereinfache.

PCS Systemtechnik GmbH stellt in der Ausgabe 11-2017 der Zeitschrift GIT, S. 46/47, eine biometrische **Handvenenerkennung für ein Logistikzentrum** vor. Sie nutze die Absorption von Infrarotstrahlen in venösem Blut. Der Sensor sende Nah-Infrarotstrahlung in Richtung der Handflächen aus. Das sauerstoffreduzierte Blut in den Venen absorbiere die Infrarotstrahlung. Die Kamera des Sensors erstelle ein Bild des Venenmusters und wandele das Bild in ein Template um, das auf dem Mitarbeiterausweis gespeichert werden kann. Die Handvenenerkennung sei ein hochsicheres Zutrittssystem und nicht zu manipulieren.

Brandmeldeanlage

Carsten Meißner, Siemens AG Building Technologies, und Mark Egbers, Pfannenberg, befassen sich in der Ausgabe 11-2017 der Zeitschrift GIT, S. 70–72, mit dem **Brandschutz nach VDE 0833-2**. Mit Veröffentlichung der Überarbeitung der Planungs- und Projektierungsregeln der DIN VDE 0833-2 seien die Anforderungen der Produktnorm EN 54-23 implementiert, und es werde eindeutig beschrieben, wie und in welcher Menge optische Signalgeber zu projektieren sind. Nach wie vor lege die DIN VDE 0833-2 eindeutig fest, dass der Betreiber einer Anlage für das Brandmelde- und Alarmierungskonzept verantwortlich ist. Die umgehende und eindeutige Alarmierung geschehe in der Regel durch ein gebäudeübergreifendes System aus akustischen und/oder optischen Signalgebern. Die Autoren behandeln verbindliche Vorgaben für optische Signalgeber, die erstmalige Definition konkreter Signalisierungsbereiche, die Bedeutung der Alarmierungsfarbe und die richtige Auswahl. Industrielle Gebäude hätten meist hohe Decken und große Flächen, die den Signalisierungsbereich entscheidend definieren. Hier empfehle sich der Einsatz von Signalgebern der Kategorie „O", also mit flexibler Montage. Auch die Auswahl der Lichttechnologie könne entscheidend sein. Signalgeber mit XENON-Technologie deckten in der Regel größere Signalisierungsbereiche ab als vergleichbare Produkte mit anderen Technologien. Jede Alarmierungslösung müsse individuell geplant werden.

Brandschutz

Annika Westphal, Erwin Frick und Frederic Scharnhorst, Minimax GmbH, befassen sich in Ausgabe 5-2017 der Zeitschrift Sicherheitsforum, S. 22–24, mit der **Brennstoffzellentechnologie** zur gleichzeitigen Energieversorgung und Brandvermeidung. Brennstoffzellen erzeugten, ähnlich wie motorische Blockheizkraftwerke, gleichzeitig Strom und Wärme. Der erzeugte Strom könne den konventionellen Elektrizitätsbezug deutlich reduzieren oder für eine Notstromversorgung eingesetzt werden. Durch die erhöhte Effizienz würden nicht nur die Betriebskosten sinken, sondern es werde auch eine kontinuierliche Energieversorgung sichergestellt, und das System sei umweltschonender als eine herkömmliche Brandvermeidungsanlage. Die Autoren behandeln das Redundanzkonzept für unerwartete Störungen, die Brandgefahr im Tiefkühllager, das Funktionsprinzip einer Sauerstoffreduzierungsanlage und die Kombination mit einer Brennstoffzelle.

Die **Brandfrüherkennung** mittels Infrarotmesstechnik **in der Abfallwirtschaft** behandelt PROTECTOR, Ausgabe 11-2017, S. 44/45. Die vielfältigen Brandursachen erforderten ein flexibles System zur Erfassung sowohl von einer Initialzündung als auch einer Temperaturerhöhung des gesamten Lagergutes. Mit einer Infrarotkamera sei es möglich, die Oberflächentemperatur von Materialien genau zu bestimmen. Durch die hohe Auflösung von 384 mal 288 Pixel könnten auch kleine Glutnester zuverlässig erkannt werden. Beim Brandfrüherkennungssystem von Dias werde die IR-Kamera auf einen Schwenk/Neige-Kopf montiert, wodurch die Änderung des Blickwinkels ermöglicht werde. Wird eine Überschreitung der Temperaturschwellen in einem Sektor detektiert, so erfolge eine optische und akustische Alarmierung des Bedieners. In einem Ringspeicher würden alle Sektoraufnahmen und Alarmbilder radiometrisch gespeichert. Damit sei es möglich, im Nachgang die IR-Aufnahmen temperaturbezogen

auszuwerten. Durch die Nutzung eines speziellen Detektionsalgorithmus könnten Täuschungsalarme durch Fahrzeuge oder Reflexionen verhindert werden. Jeder IR-Kamera sei ein Referenzstrahler zugeordnet. In einem vorgegebenen Intervall werde die Kamera in Richtung Referenzstrahler ausgerichtet und es erfolge die Überprüfung der gemessenen Temperatur.

PROTECTOR weist in der Ausgabe 11-2017, S. 48, darauf hin, dass der Brandschutzcontainer des Typs „BLS F 90 F-SAFE" die Zulassung vom Deutschen Institut für Bautechnik (DIBt) bekommen hat. Gewährleistet werde damit die maximale Sicherheit bei der Lagerung von entzündlichen brandfördernden und giftigen Stoffen, sowie organischen Peroxiden in Kleingebinden, Fässern oder IBC.

Cloud Computing

Florian Benne, Microsoft Deutschland GmbH, und Hendrik Schulte im Walde, Schille Informationssysteme GmbH, stellen in der Zeitschrift PROTECTOR, Ausgabe 11-2017, S. 26/27, ein **cloudbasiertes Videoüberwachungssystem für Hochsicherheitsanwendungen** vor. Cloud-Technologien würden dank ihrer Möglichkeiten mit Blick auf Skalierbarkeit, Flexibilität, nutzungsabhängiger Abrechnung und vor allem der stets aktuellen Dienste als Innovationstreiber gelten. In der Sicherheitsbranche stehe diese Entwicklung noch am Anfang. Das von Schille entwickelte cloudbasierte Videoüberwachungssystem für Hochsicherheitsanwendungen sei für den professionellen Einsatz in privaten und öffentlichen Einrichtungen und für hoheitliche Aufgaben mit höchsten Anforderungen an den Datenschutz entwickelt worden. Die Kameras und Arbeitsplätze nutzten SSL/TLS-Leitungen mit AES256-Verschlüsselung und Zertifikatsprüfung sowie Authentifizierungen.

Die FAZ weist am 29. November darauf hin, dass Ransomware-Schadprogramme alle Dateien infizieren, derer sie habhaft werden können, sodass auch die eigenen Inhalte in der Cloud betroffen sind, selbst wenn sie auf externen Servern liegen. Nun seien zusätzliche Vorkehrungen gefragt: Wichtige Daten müssten regelmäßig auf externen Medien gesichert und physisch vom Rechner getrennt werden. Der Autor untersucht mehrere Alternativen und Produkte: so eine Speicherkarte fürs Handy, SSD-Laufwerke und das Western Digital My Cloud Home für zwei 3,5 Zoll-Festplatten. An erster Stelle stünden externe Festplatten mit USB-Anschluss. Besonders gefallen habe die **My Passport** von Western Digital. Das Produkt **„My Cloud Home"** sei eine Art persönliche Cloud, ein Netzwerkspeicher fürs Heim, der aber auch über das Internet erreichbar sei. Der Vorteil liege in der einfachen Bedienung. Ein Nachteil bestehe darin, dass es keine Funktionen eines erheblich komplexeren Network Attached Storage biete.

Datenschutz

Arne Vodegel, IPG AG, befasst sich in der Ausgabe 11-2017 der Zeitschrift PROTECTOR, S. 50/51, mit der neuen **DSGVO**, die am 25. Mai 2018 in Kraft tritt. Auf die IT habe sie verschiedene Auswirkungen, die vom Autor beschrieben werden: im Bereich Haftung, Marktortprinzip, Verlust-Folgenabschätzung und Datenschutz-Managementsystem. Rechte müssten durchgängig in einer Identity-Management- und Identity-Governance-Lösung dynamisch verwaltbar und protokollierbar sein. Identity & Access Management (IAM) unterstütze in der Einhaltung der DSGVO überall dort, wo ein Risiko-Inventar erstellt wird und Schutzniveaus eine Rolle spielen (Art. 35/36) und dort, wo Zugriff und Verarbeitung auf schützenswerte Daten gesteuert und belegt werden müssen (Art. 5/32); ferner dort, wo Verarbeitungstätigkeiten geschützt und nachvollzogen werden müssen (Art. 30) und wo Auftragsverarbeiter ihnen anvertraute Daten DSGVO-konform beherrschen und dies auch belegen müssen (Art. 28). Um IAM als solide Basis für die DSGVO/GDPR (General Data Protection Regulation) zu nutzen, unterstütze die IPG AG mit verschiedenen Leistungen in den Bereichen Advisory, Integration, Operation und Education.

Die FAZ weist am 27. November darauf hin, dass in 180 Tagen die europäische Datenschutz-Grundverordnung in Kraft tritt. Viele Unternehmen würden in diesen Tagen allmählich auf das Mammutprojekt aufmerksam. Andere, zumal die großen Konzerne, seien längst vorbereitet und andere hätten schon bekanntgegeben, den Mai 2018 mit Rechtsbrüchen zu begehen. Sie würden schlicht nicht fertig, wie Studien sowohl in Deutschland als auch in Europa zeigten. Jetzt hole sich jeder Zweite Hilfe, habe Bitkom verkündet. 48 Prozent aller Unternehmen mit mehr als 20 Beschäftigten zögen demnach externe Fachleute hinzu. Nur rund jedes achte Unternehmen werde nach eigener Einschätzung bis zum Stichtag die Vorgaben der DS-GVO vollständig umgesetzt haben. Zur Umsetzung müssten viele Sachverhalte im Unternehmen neu

bewertet und neue Abläufe eingeführt werden. Das **größte Problem für Unternehmen** sei die **Beweislast**. Sie müssten künftig nachweisen, dass sie beim Datenschutz alles richtig gemacht haben. Das sei in der Praxis enorm schwer.

Datensicherheit

Andreas Bechter, Veritas, rät in der Ausgabe 5-2017 der Zeitschrift Sicherheitsforum, S. 35, dazu, Daten erst „auszusieben" und dann in die Cloud zu verschieben. Deutsche IT-Verantwortliche würden nur 15 **Prozent** ihrer Informationen als geschäftskritisch einschätzen. Den Rest müssten die Unternehmen genauer untersuchen. Rund 19 **Prozent** seien sogenannte „ROT-Daten" (redundant, obsolet, trivial). Die verbleibenden 66 Prozent der Informationen seien „dark data" und könnten nicht genau eingeordnet werden. Infolge des immensen Datenwachstums müssten die **„Aufräumaktionen" kontinuierlich** erfolgen.

Einzelhandelssicherheit

Hans Günter Lemke, Lemke Beratung UG, gibt in der Ausgabe 5-2017 der Zeitschrift Sicherheitsforum, S. 82–84, Antwort auf die Frage: Welche Warensicherung eignet sich wo? Er behandelt **drei Technologien der elektronischen Artikelsicherung**: Radio-Frequenztechnik, elektromagnetische Technik und akustomagnetische Technik. Als Kriterien für die Auswahl eines geeigneten EAS-Systems kämen in Betracht: Schleusenbreite, Detektionsrate und Fehlalarmhäufigkeit. Mehr als 95 **Prozent** aller Signale würden durch vergessene oder nicht korrekt entwertete Etiketten ausgelöst werden. Sicherheitsetiketten müssten so angebracht werden, dass sie nicht zu leicht entfernt werden können.

Evakuierung

Dr. Stephan Gundel, Gruner Gruppe, beschreibt in der Zeitschrift Sicherheitsforum, Ausgabe 5-2017, S. 46–49, **Herausforderungen für die Evakuierungsplanung**. Der Komplexitätsgrad bei Evakuierungsplanungen nehme zu. Grundlage sei zunächst die detaillierte Analyse der möglichen und hinreichend wahrscheinlichen Szenarien, die zu einer Evakuierung führen können. Die notwendigen baulichen und technischen Hilfsmittel für eine Evakuierung müssten ermittelt und dokumentiert werden. Für die Evakuierung selbst müsse ein klarer, lückenloser und jederzeit funktionsfähiger Ablauf bei in Frage kommenden Szenarien ausgearbeitet und dargestellt werden. Ergänzend müsste die notwendige Aufbauorganisation mit entsprechender personeller Besetzung und persönlichen Hilfsmitteln definiert, geschult und vorgehalten werden.

Explosionsschutz

Zum Thema **vorbeugender und organisatorischer Explosionsschutz** äußert sich im Sicherheitsforum, Ausgabe 5-2017, S. 86–89, Sicherheitsingenieur Rolf Oster, Sicherheitsberatung. Er hänge im Wesentlichen von der Zündquellenanalyse und der Umsetzung der technischen und organisatorischen Maßnahmen ab. Der Autor behandelt die Zündquellenerkennung und -analyse, Arten von Zündquellen, technische Ableitungen an den Objekten, organisatorische Erdung und Ableitungen, Aufrechterhaltung sicherer Arbeitsmethoden, Bildung und Anhäufung elektrostatischer Ladungen, Konformität und Messprotokoll bei der Umsetzung in der Praxis und Verbesserungspotenzial. Die größte Herausforderung bei den Lösungen im Zusammenhang mit elektrischer Ableitung sei die Instandhaltung der Arbeits- und Hilfsmittel.

Geldwäsche

Rechtsanwalt Stephan Müller, Oppenhoff & Partner, befasst sich in der FAZ vom 29. November mit der Anwendbarkeit der Regeln zur Geldwäscheprävention auf die sogenannten **Güterhändler**. Damit werde die Geldwäscheprävention ein weiterer Standard für die Compliance-Organisation von Unternehmen. Für Unternehmen, die mit Waren jeder Art Handel treiben, bedeute dies vor allem, dass sie Maßnahmen im Unternehmen treffen müssen, die die Geldwäscherisiken erkennen lassen. Ein vertieftes Risikomanagement einschließlich einer Risikoanalyse müssten Güterhändler nur dann etablieren, wenn sie im Rahmen einer geschäftlichen Transaktion Barzahlungen

von mindestens 10.000 Euro vornehmen oder erhalten. Behörden könnten die Bestellung eines Geldwäschebeauftragten anordnen. Ein solches Vorgehen sei insbesondere dann vorstellbar, wenn die gehandelten Güter erfahrungsgemäß zur Geldwäsche genutzt werden können, also vor allem bei Händlern von Luxusgütern. Die allgemeine Sorgfaltspflicht, die im Grundsatz die Identifizierung des jeweiligen Vertragspartners verlange, greife für Güterhändler ebenfalls nur bei Überschreiten der 10.000 Euro-Schwelle. Es bestehe aber auch eine vom Geldwert der Transaktion unabhängige Sorgfaltspflicht. Danach seien die Händler verpflichtet, auf Anhaltspunkte für Geldwäscheaktivitäten zu achten. Bei einem Verdacht bestehe die Pflicht, die Transaktion an die Zentralstelle für Finanztransaktionsuntersuchungen zu melden. Dabei habe die Generalzolldirektion als für die Entgegennahme von Meldungen zuständige Behörde das BKA abgelöst. Zudem sei eine Hotline eingerichtet worden, über die Meldungen abgegeben werden können. Zu den Compliance-Maßnahmen gehöre vor allem die regelmäßige Schulung der Mitarbeiter, damit diese die Indikatoren für ein Geldwäscherisiko kennen und wissen, was im Verdachtsfall konkret zu tun ist.

IoT

Den **Fernzugriff auf Industrial-IT-Systeme** (IoT) thematisiert Rainer Rehm, ISC-Chapter Germany, in der Ausgabe 5-2017 der Zeitschrift <kes>, S. 80–84. Eine Strategie für einen entsprechend sicheren Remote-Zugriff sollte die folgenden Komponenten berücksichtigen: vertrauenswürdiger Authentifizierungsprozess; klare Definition eines Rechte- und Rollenkonzepts; zeitliche Beschränkung des Zugriffs; Möglichkeiten für Kontrolle und Audits müssten zu allen Zeiten gegeben sein. Eine Umsetzung mit Einbindung der Prinzipien von „Security by Design" und „Security by Default" ermögliche den sicheren Betrieb von langlaufenden Systemen wie sie in der Industrie und Produktion häufig anzutreffen seien. Gleichlautende Prinzipien seien in der ab Mai 2018 gültigen DSGVO als „Privacy by Design" und „Privacy by Default" gefordert.

Trends, neue Herausforderungen und neue Lösungen in Sachen Identifikation thematisiert HID Global in der Ausgabe 11-2017 der Zeitschrift GIT, S. 63–65. Die **Nutzung von vertrauenswürdigen Identitätslösungen** steige auf breiter Front. Faktoren, die diese Entwicklung beflügeln, seien der zunehmende Einsatz von mobilen Geräten und neuen Smartcard-Technologien, die erhöhte Bedeutung des IoT und das boomende Smart Building. Bei der Sicherung von IoT-Anwendungen zeichneten sich mehrere neue Entwicklungen ab: Echtzeit-Lokalisierungssysteme, Präsenz- und Proximity-basierte Lokalisierungsfunktionen sowie Zustandsüberwachungslösungen, die verstärkt zum Einsatz kommen, Bluetooth-Low-Energy-basierte Lösungen, die sichere Proof-of-Presence-Möglichkeiten um Vorhersagbarkeit erweitern, und RFID-Technologien, die auf BLE, NFC und RAIN UHF basieren und Supply-Chain-Managementprozesse automatisieren. In einer Studie von Ifsec Global mit einer Befragung von Facility Managern und Sicherheitsverantwortlichen in mehr als 50 Ländern hätten 65 Prozent verbesserte Sicherheit, 46 Prozent Multifaktor-Authentifizierung und 41 Prozent die Unterstützung unterschiedlichster ID-Formfaktoren als zentrale Treiber für Upgrades der Zutrittskontrollsysteme genannt.

IT-Sicherheit

In der Ausgabe 5-2017 der Fachzeitschrift <kes>, S. 6–10, behandelt Martin Huber, Corporate Trust, Business Risk & Crisis Management GmbH, das Aufspüren bekannter **„Indicators of Compromise"** (IoC). Darunter verstehe man eine Art Signatur von Angriffen beziehungsweise die Beschreibung konkreter Spuren, die sie in der IT hinterlassen. Einen Angreifer anhand bekannter Merkmale gezielt in der eigenen Infrastruktur zu finden, erfolge im Wesentlichen in vier Schritten: IoC identifizieren, Verwendung planen, Infrastruktur vorbereiten; Datengrundlage für die IoC in der Infrastruktur sammeln; IoC in den gesammelten Daten suchen; Suche automatisieren und dokumentieren. Die wichtigste Ressource bei der Suche nach IoC sei der Mensch: Threat-Hunting erforderte einen technisch versierten Mitarbeiter mit ausreichend Zeit und tiefgehender Kenntnis der lokalen IT-Infrastruktur. Die Datenerhebung sei so zu gestalten, dass die Clients sie selbstständig ausführen und die Ergebnisse bei nächster Gelegenheit an einen zentralen Sammelpunkt übermitteln, Außerdem müsse es eine Möglichkeit geben, den Status und den aktuellen Abdeckungsgrad einer Suche zu erkennen. Ergibt die IoC-Suche einen Treffer, deute dies auf einen ernst zu nehmenden, von den etablierten Präventionsmaßnahmen nicht verhinderten Angriff auf die IT hin. Die Allianz für Cybersicherheit habe für solche Fälle einen Leitfaden herausgegeben.

Anna Riske, Volkswagen AG, berichtet in der Ausgabe 5-2017 der Fachzeitschrift <kes>, S. 12–16, von ihren Erfahrungen bei Aufbau und Betrieb eines Informationssicherheits-Managementsystems (**ISMS) bei der Volkswagen AG**. Das Hauptziel des Sicherheits-Managements sei es, ein angemessen hohes Sicherheitsniveau zu schaffen und somit letzten Endes Kosten zu sparen. Aus dem Ansatz einer Risikobewertung heraus dränge sich ein ISMS als zentrales Steuerungselement geradezu auf. Der Einsatz eines ISMS bedeute aber noch nicht gleichzeitig, dass ein Unternehmen in puncto Informationssicherheit perfekt aufgestellt ist und es keine Risiken mehr hat. Ein ISMS mache jedoch die Definition und Überwachung von Schutzzielen und -maßnahmen wesentlich transparenter. Dabei sei ein ISMS jedoch keinesfalls ein fertiges Produkt, sondern müsse sehr stark den individuellen Gegebenheiten des nutzenden Unternehmens Rechnung tragen. Das Unternehmen müsse das Rahmenwerk der ISO 27001 auf ihre eigenen Strukturen anwenden, das heiße: vor allem die Prozesse betrachten, auf welche die Informationssicherheit große Auswirkungen habe. Ein ISMS setze sich formal aus Prozessen zur Planung, Umsetzung, Überprüfung und Verbesserung (PDCA) von Informationssicherheit sowie deren Maßnahmen-Dokumentation zusammen. Ein wesentlicher Teil der ISMS-Toolbox seien die Werkzeuge zur Entwicklung eines aussagekräftigen Kennzahlensystems. Schließlich müsse ein ISMS mit den darin manifestierten Schutzmaßnahmen regelmäßig auf seine Wirksamkeit hin geprüft werden. Die ISMS-Toolbox verwende dazu ein Security-Dashboard, das Kennzahlen und Metriken zusammenführe: Dieses zentrale Überwachungs- und Steuerungsinstrument bilde die wichtigsten Key-Performance-Indicators für die Informationssicherheit des Unternehmens ab.

Karsten U. Bartels LL.M., Bundesverband IT-Sicherheit e. V. (TeleTrust), beleuchtet in der Fachzeitschrift <kes>, Ausgabe 5-2017, S. 35–37, zulässige Handlungsoptionen und Rechtsfolgen von **Fehlentscheidungen im Zusammenhang mit der EU Datenschutz-Grundverordnung** (DSGVO), der europäischen Netzwerk- und Informationssicherheits-(NIS-) Richtlinie sowie dem deutschen IT-Sicherheitsgesetz. Das zentrale Tatbestandsmerkmal für die IT-Sicherheit dieser Normen sei der „Stand der Technik". Damit dieser objekttechnische Begriff durch die Verpflichteten in der Praxis umgesetzt werden kann, enthielten die jeweiligen Normen zusätzlich subjektive Einschränkungen. Dies ermögliche es Unternehmen, den Stand der Technik rechtskonform zu unterschreiten. Eine solche Unterschreitung sei nur ratsam, wenn neben einer gewissenhaften Bewertung eingesetzter und einsetzbarer Maßnahmen eine umfangreiche Dokumentation erfolgt. Eine rechtskonforme Unterschreitung könne dann aber zu erheblichen Einsparungen und organisatorischen Minderaufwand führen. Es empfehle sich daher, im Rahmen der gesetzlich notwendigen Umsetzung der IT-Sicherheitsmaßnahmen technische und rechtliche Expertise einzuholen.

Das BSI Forum thematisiert in der Ausgabe 5-2017 der Fachzeitschrift <kes>, S. 44–46, die **Allianz für Cybersicherheit**. Das Interesse an Cybersicherheitsthemen sei gerade bei kleinen und mittelständischen Unternehmen hoch. Nicht zuletzt aufgrund immer neuer Angriffe werde die Allianz für Cybersicherheit voraussichtlich auch in den nächsten Jahren weiter wachsen. Gleichzeitig ließen sich mit einer derart großen Teilnehmerbasis auch verschiedene Vorhaben realisieren: So führe die Allianz jährlich die Cybersicherheitsumfrage durch, in der deutsche Institutionen zu ihrer Betroffenheit durch Cyberangriffe befragt werden. Außerdem sei auf der Allianz-Website eine Meldestelle eingerichtet worden. Hier könnten deutsche Unternehmen freiwillig und anonym über IT-Sicherheitsvorfälle berichten. Die regelmäßig eingehenden Hinweise gingen in den BSI-Lagebericht ein.

Bettina Weßelmann, Beraterin, und Dr. Johannes Wiele, Managing Security-Consultant, plädieren in der Fachzeitschrift <kes>, Ausgabe 5-2017, S. 18–22, für das **Etablieren einer Sicherheitskultur**. Die stehe aus Sicht der Informationssicherheit für den Wunsch, das Thema Security und ein entsprechendes Verhalten so fest im Alltag einer Organisation zu verankern, dass es dort zu einem der zentralen Leitmotive des Handelns wird. Allerdings lasse sich eine „Kultur" nicht einfach aus dem Boden stampfen. Und überdies mangele es häufig noch an der Erkenntnis, dass eine Informationssicherheitskultur vor allem eine **Fehlerkultur** sein muss. Erfolgversprechend seien folgende Ansätze: die Einführung obligatorischer Sicherheitsbetrachtungen oder Risikoassessments für alle neu eingeführten Systeme oder Prozesse; Aufnahme des Themas „Sicherheit" in Jahresgespräche und reguläre Statusmeetings; Einrichtung eines Security-Helpdesks; Gestaltung der Sicherheitskultur als Fehlerkultur. Die Sensibilität, Bedenken vorzubeugen, sei für eine positive Sicherheitskultur in einer Organisation ein kritischer Erfolgsfaktor.

Sebastian Klipper, CycleSEC, befasst sich in <kes>, Ausgabe 5-2017, S. 68–78, mit dem **Härten von Content-Management-Systemen** (CMS). Auch wenn CMS-Entwickler Security-Aspekte durchaus ernst nähmen, gebe es an Standardinstallationen doch einiges zu verbessern. Die eigentliche Härtung umfasse verschiedene Maßnahmen,

die der Autor im Einzelnen erläutert: Konfigurationsdatei absichern; Maßnahmen in der .htaccess-Datei, Admin-Bereich absichern; Anmeldung via HTRTPS; Benutzerverwaltung einschränken; Tabellenpräfix ändern; Header-Output einschränken; PHP-Fehlermeldungen deaktivieren; Updates und Sicherheitspatches; Installation von Security-Plugins.

Stephan Schweizer, AdNovum Informatik AG, stellt in <kes>, Ausgabe 5-2017, S. 86–88, Lösungen zum Customer-/Consumer-Identity- und -Access-Management (CIAM) vor, die gleichzeitig der Sicherheit, der Usability und dem Marketing dienen würden. Er behandelt die moderne Authentifizierung und gibt **Tipps für CIAM-Projekte**.

Sebastian Krüsmann und Tobias Goldschmidt, HiSolutions AG, schildern die Herausforderungen für bestehende IT-Grundschutzkonzepte durch die neue Version für drei BSI-Standards (IT-Grundschutz 2.0) in der Ausgabe 5-2017 der Zeitschrift <kes>, S. 89–94. Die Autoren stellen die wesentlichen **Änderungen der BSI-Standards** detailliert dar: Ziele, Adressaten und Definitionen der Managementsysteme, den Prozess zum Aufbau eines ISMS, die Vorgehensweisen, das IT-Grundschutz-Kompendium und den IT-Grundschutzcheck, die Risikoanalyse für 46 elementare Gefährdungen und das Vorgehensmodell, die Migration des bestehenden IT-Sicherheitskonzepts in den modernisierten IT-Grundschutz, wobei Migrationen immer in gewissen Szenarien verlaufen würden, die im ersten Schritt definiert werden müssten. Die Aktualisierung der BSI-Standards ermögliche es Institutionen aller Arten und Größen, ein angemessenes ISMS aufzubauen. Dazu trügen die neuen Vorgehensweisen „Basis-Absicherung" und „Kern-Absicherung" bei, in deren Rahmen Informationsverbände zunächst grundlegend abgesichert oder zentrale Aspekte vorrangig betrachtet werden.

Mit der Neufassung der Methodik des vom BSI entwickelten IT-Grundschutzes solle die Erhöhung der IT- und Informationssicherheit in Unternehmen flexibler und handhabbarer werden, heißt es auch in der November-Ausgabe des Behörden Spiegel. Der 1994 eingeführte IT-Grundschutz habe sich zum weit verbreiteten Standard in Deutschland für die Einführung eines ISMS entwickelt. Die zugrundeliegende Dokumentation sei nun neu strukturiert und verschlankt worden. Bestandteile des überarbeiteten Grundschutzes seien das IT-Grundschutz-Kompendium, die BSI-Standards 200-1, 200-2 und 200-3 sowie der **„Leitfaden zur Basisabsicherung".** Das Kompendium ersetze die früheren IT-Grundschutzkataloge. Neben einer Einführung enthalte es 80 Bausteine, die jeweils auf etwa zehn Seiten grundlegende Anforderungen entsprechend des jeweiligen Schutzbedarfs für einzelne Teilaspekte einer IT-Systemlandschaft umreißen. Die neuen Standards definierten Anforderungen an ein IT-Sicherheits- bzw. Risikomanagement. Der BSI-Standard 200-2 stelle die eigentliche IT-Grundschutzmethodik dar und diene als Anleitung für den Aufbau eines soliden ISMS. Es sei möglich, die neuen Bausteine mit jenen aus den alten Grundschutzkatalogen zu kombinieren und so ein bestehendes ISMS Schritt für Schritt auf den aktuellen Standard zu heben. Alle Dokumente zum IT-Grundschutz stünden auf der Webseite des BSI zum Download bereit. Weil auch in der modernisierten Form aus Sicht des VdS der IT-Grundschutz in seinem Gesamtumfang zu komplex für kleine Unternehmen sei, sollten es die seit 2015 vorliegenden VdS-Richtlinien 3473 kleinen Organisationen ermöglichen, mit vergleichsweise überschaubarem organisatorischem und finanziellem Aufwand ein angemessenes Schutzniveau zu etablieren.

Die FAZ weist am 9. November auf den neuesten **Lagebericht des BSI** für das Berichtsjahr Juli 2016 bis Juni 2017 hin. Danach sei die Gefährdungslage in der digitalen Welt weiterhin auf hohem Niveau angespannt. Das Bedrohungspotenzial steige deutlich an, da sich die Anzahl möglicher Angriffspunkte erhöhe und die zu verarbeitenden Datenmengen sich vervielfachen. Der Lagebericht verweise vor allem auf das Internet der Dinge. Es entwickele sich den Angaben zufolge immer mehr zu einer Gefahrenquelle für die IT-Sicherheit. IoT-Geräte seien einfach angreifbar, weil deren IT-Sicherheit derzeit weder bei der Produktion noch bei der Kaufentscheidung des Kunden eine ausreichende Rolle spiele.

In einem Kommentar in der FAZ am 13. November zeigen Constanze Kurz und Stefan Kölbl, „wie unsere Computerverschlüsselungen" zustande kommen. In wenigen öffentlichen Wettbewerben brächten Kryptografen ihre Ideen ein. Im besten Fall entstehe dann in einem jahrelangen Prozess ein neuer weltweiter kryptografischer Standard. Standards wie AES oder SHA-3 würden in Milliarden von Computersystemen eingebaut. In starkem Kontrast zu diesen öffentlichen Wettbewerben stünden die Prozesse bei der Internationalen Organisation für Normung (ISO), die großenteils hinter verschlossenen Türen stattfänden. Traditionell mischten die formidabel ausgestatteten Geheimdienste in solchen Arbeitsgruppen mit und hätten einen bedeutenden Einfluss auf die Standardisierungsprozesse. 2013 habe die NSA **zwei neue Verschlüsselungsverfahren** mit den Namen Simon und Speck veröffentlicht. Sie befänden sich nun seit

etwa drei Jahren im Standardisierungsprozess der ISO. Die mangelnde Bereitschaft der NASA, die den Verschlüsselungsverfahren zugrundeliegenden Konzepte zu erläutern, sei nicht geeignet, Vertrauen in die Verfahren zu gewinnen. Ohne die Offenlegung aller Details sollten in Zukunft keine kryptografischen Verfahren mehr etabliert werden.

„Proaktiv statt reaktiv" titelt Michael Kleist, CyberArk, in der November-Ausgabe des Behörden Spiegel. Standard-Sicherheitsvorkehrungen mit Firewall, Antivirenschutz oder Webfilter-Techniken zu ergreifen sei heute Status quo. Allerdings reichten sie bei Weitem nicht mehr aus. Die Verwaltung und Überwachung privilegierter Benutzerkonten und Aktivitäten sollte deshalb im Zentrum jeder Sicherheitsinitiative stehen. Die Softwarelösung **Privileged Account Security von CyberArk** sei gezielt für den Schutz privilegierter Benutzerkonten konzipiert. Sie lege die Passwörter der Konten an einem zentralen und besonders geschützten Ort ab, einem sogenannten **Vault**, und stelle durch spezielle Authentifizierungs- und Zugriffs-Kontrollmethoden sicher, dass sie nur von berechtigten Personen benutzt werden können. Das größte Risiko sei der Kontrollverlust im Bereich des Active Directory. Somit müssten im ersten Schritt Sicherungsmaßnahmen für den Schutz privilegierter Zugangsdaten der Windows-Domäne ergriffen werden. Auch Application Accounts oder Software Accounts seien eine Sicherheitslücke. Mit der CyberArk-Lösung könnten die eingebetteten statischen Passwörter eliminiert werden, das heißt, sie würden zentral abgelegt, automatisch verwaltet und in Abhängigkeit zu den Systemkonten mitgeändert. Ein innovativer Ansatz bei der Applikationsüberwachung sei das Greylisting von Anwendungen. Damit könnten zum einen die Ausführung bekannter Malware auf Blacklists verhindert und zum andern die Berechtigungen für alle Anwendungen begrenzt werden.

Eine der häufigsten **Ursachen für Infektionen mit Schadsoftware** sei der Besuch von Webseiten und der Klick auf schadhafte Links, betont Dr. Norbert Schirmer, Rohde & Schwarz Cybersecurity, in der November-Ausgabe des Behörden Spiegel. Problematisch seien vor allem aktive Inhalte wie Flash oder Java. Dabei werde fremder, externer Code auf dem PC, auf dem eigenen Betriebssystem und damit in der Dateninfrastruktur ausgeführt. Enthält dieser Programmcode Schadsoftware, so gelange diese ebenfalls zur Ausführung. Die bisherigen Ansätze in der Bedrohungsabwehr seien vielfach noch von rein reaktiver Natur. Zero Day-Exploits, die bisher unbekannte Sicherheitslücken ausnutzen, oder Advanced Persistent Threats würden von Antivirenprogrammen nicht herausgefiltert. Exemplarisch an dem Beispiel der Internetnutzung in Unternehmen sei ein Paradigmenwechsel von rein reaktiven Systemen hin zu proaktiven Lösungen. Der Aspekt der proaktiven Sicherheit werde besonders durch die Sicherheitslösung **Browser in the Box** von Rohde & Schwarz Cybersecurity deutlich. Sie sei in Unternehmen erfolgreich im Einsatz. Die Sicherheitsarchitektur von Browser in the Box beruhe zunächst auf der Trennung von Internet und Intranet. Auf dem PC bestehe Browser in the Box aus einer virtuellen Maschine, auf der Linux als Betriebssystem installiert ist. Zum Einsatz komme eine Vollvirtualisierung. Sie trenne im ersten Schritt den Browser vom restlichen PC. Für ein noch höheres Sicherheitsniveau trenne Browser in the Box das Internet vom internen Unternehmensnetzwerk oder Intranet. Jeglicher Zugriff auf das Internet erfolge durch einen VPN-Tunnel und werde somit vom Netzwerk ferngehalten.

IT-Sicherheit von Industrial Automation and Control Systems gemäß IEC 62443 behandelt Thorsten Vogel, Phoenix Contact Cyber Security, in der Ausgabe 11-2017 der Zeitschrift GIT, S. 78–80. Die aus den Erfahrungen mit der Malware Stuxnet entstandene Normenfamilie IEC 62443 betrachte vier Konzepte: die grundlegenden Anforderungen, die Zonen und Conduits, die Security Level sowie den Security-Lebenszyklus. Die Konzepte spiegelten sich in den vier Teilen wieder, aus denen sich die Norm zusammensetzt: General Information, Policies & Procedures, System und Component. Der Autor beschreibt die Sammelstelle für Security-relevante Ereignisse, die Absicherung ausgewählter Kommunikationskanäle und Lösungen zur Erhöhung der Sicherheit.

GIT weist in der Ausgabe 11-2017, S. 101, auf eine weltweit durchgeführte Studie von Kaspersky Lab unter Verantwortlichen für **Cybersicherheit im ICS-Bereich** hin, die zeige, dass mehr als die Hälfte der befragten Industrieunternehmen in den vergangenen zwölf Monaten mindestens einen Cybersicherheitsvorfall zu beklagen hatten – auch wenn 83 **Prozent** der Befragten davon ausgehen, dass ihre Industriesysteme gut gegen Cybersicherheitsvorfälle gerüstet sind. Laut Studie beliefen sich die Kosten für industrielle Organisationen aufgrund ineffektiver Cybersicherheit durchschnittlich auf 497.000 Dollar pro Jahr.

Nach dem von CA Veracode veröffentlichten Bericht **„State of Software" 2017** enthalten, wie Peter Marwan am 21. November auf silicon.de schreibt, 88 **Prozent** der Java-Anwendungen mindestens eine angreifbare Komponente. 53 **Prozent** der Java-Anwendungen bauten sogar auf einer Komponente auf, die über eine Lücke mit CVE-Kennung angreifbar ist.

Wie die FAZ am 27. November berichtet, fordere der deutsche Branchenverband für IT-Sicherheit, Teletrust, von der künftigen Bundesregierung, dass sie mindestens **eine Milliarde Euro im Jahr für Cybersicherheit** ausgibt und dieses Ziel auch im Koalitionsvertrag festschreibt. Angesichts der jährlichen Schäden für die Wirtschaft in Höhe von 55 Mrd. Euro sei eine Förderung von einer Milliarde keine übertriebene Forderung. Konkrete Ziele zu Cybersicherheitsstrategien gebe es noch kaum.

Am 30. November weist die FAZ auf eine **Sicherheitslücke im neuen Betriebssystem High Sierra** für Macintosh-Computer hin, die dazu führe, dass Unbefugte sich auf simple Weise und ganz ohne ausgefeiltes Hacking Kontrolle über die Rechner verschaffen könnten. Sie müssten dazu offenbar nur einen bestimmten Nutzernamen eingeben und bekämen ganz ohne Passwort Zugriff auf den Computer. Apple arbeite an einem Software-Update. Als Zwischenlösung rate er Mac-Nutzern, selbst ein „Root"-Passwort zu setzen, um unerwünschten Zugriff von Dritten zu verhindern.

IuK-Kriminalität

Nach einer Meldung von golem.de hat der US-Pharmahersteller Merck Sharp und Dome durch den **NotPetya-Malwareangriff** rund 375 Mio. Dollar verloren. Auch die Logistikkonzerne Maersk und TNT hätten jeweils große Schäden durch NotPetya hinnehmen müssen. Maersk habe einen Verlust von 200 bis 300 Mio. Dollar angegeben, TNT ebenfalls rund 300 Mio.

Banking-Trojaner Qakbot und Emotet greifen zunehmend Firmennetzwerke an, schreibt Stefan Beiersmann am 8. November auf silicon.de. Microsoft weise darauf hin, dass sich die eigentlich auf Verbraucher ausgerichteten Bank-Trojaner Qakbot und Emotet immer häufiger auch in Unternehmen verbreiten. Neuere Varianten verfügten offenbar über Techniken, die von der Ransomware WannaCry benutzt wurden, um sich in Firmennetzwerken zu verbreiten. In der Regel würden beide Trojaner als Dateianhang auf einen Rechner gelangen. Würden sie ausgeführt, richteten sie sich als Windows-Dienst oder über die Registry als Autostart-Programm ein. Mit ihren Befehlsservern kommunizierten sie über verschlüsselte HTTP- oder FTP-Verbindungen. Einige neuere Emotet-Varianten würden über ihre Befehlsserver sogar zusätzliche Malware-Module herunterladen. Unabhängig davon könnten beide Schadprogramme Tastatureingaben aufzeichnen sowie Browser- oder Netzwerk-APIs kapern, um Informationen zu stehlen. Sie würden aber auch Cookies auslesen. In einem Blogeintrag gebe Microsoft Tipps, wie sich die Verbreitung von Qakbot und Emotet eindämmen sowie vorhandene Infektionen erkennen ließen.

Im Newsletter des Bundesverbands ASW am 17. November weist die Kanzlei für Wirtschaftsschutz ONC auf die **Ransomware „Ordinypt"** hin, die derzeit hauptsächlich Benutzer aus Deutschland befalle. Unter der Haube habe sie einige Merkmale, die herausstechen. Auffällig sei zunächst einmal, dass Ordinypt in einer für Ransomware unüblichen Programmiersprache verfasst ist (Delphi). Die Daten würden wie bei jeder Ransomware verschlüsselt, die Dateinamen scheinbar zufällig gewählt. Auffällig sei auch, dass in der Erpressernachricht ein Stück Programmcode versteckt ist, der jedes Mal eine neue Bitcoin-Adresse generiert, an die eine Lösegeldzahlung gesendet werden soll. Bisher konnte dieses Verhalten noch bei keiner anderen Ransomware entdeckt werden. Zweck dieser Vorgehensweise ist möglicherweise, die Verfolgung von Zahlungsströmen durch Strafverfolgungsbehörden zu erschweren.

Auf silicon.de weist Stefan Beiersmann am 17. November auf die **Malware Terdot** hin. Sie spähe neben Bankdaten auch die Anmeldedaten für soziale Netzwerke wie Facebook und Twitter aus. Außerdem könne die Malware auch den E-Mail-Verkehr abhören. In den E-Mails sei in der Regel ein Button enthalten, der angeblich zu einer PDF-Datei führt, stattdessen aber JavaScript-Code zum Download der Malware ausführt. Wie andere Zeus-Ableger auch richte sich Terdot ausschließlich gegen Windows-Systeme. Gefährdet seien derzeit vor allem Nutzer in den USA, Kanada, Großbritannien, Australien und Deutschland. Nach seiner Installation kapere Terdot Browserprozesse, um den Traffic zu überwachen. Mithilfe einer Spionagesoftware würden Daten ausgelesen und anschließend an einen Befehlsserver übermittelt. Bitdefender stufe Terdot als eine erhebliche Bedrohung ein. Es gebe zwar Trojaner mit einer deutlich höheren Verbreitung, die Kombination aus Banking-Malware und Spyware mache Terdot jedoch zu einer gefährlichen Weiterentwicklung im Bereich Cybercrime.

Die Wachstumsrate für den **Handel mit Erpressungstrojanern im Darknet** liege bei über 2.500 **Prozent**. Das sei das Ergebnis einer Studie von Experten des IT-Sicherheitsanbieters Carbon Black, meldet der Behörden Spiegel in der November-Ausgabe. Demnach gebe es derzeit mehr als 6.300 Marktplätze im Darknet. Je nach Umfang von Paketen

schwankten die Preise für Ransomware zwischen 50 Cent und 3.000 Dollar. Bei teureren Angeboten würden sogar Server zur Verbreitung der Schadsoftwarfe mitgeliefert.

Uber vertuscht die Hacking-Attacke, titelt die FAZ am 23. November. Wie Uber jetzt zugegeben habe, hatten Hacker schon vor mehr als einem Jahr persönliche Daten von 57 Mio. Passagieren und Fahrern des Unternehmens gestohlen. Uber habe aber weder die Kunden noch die Fahrer benachrichtigt, sondern sich alle Mühe gegeben, den Vorfall zu vertuschen. Das Unternehmen habe den Angreifern eine Art Lösegeld von 100.000 Dollar gezahlt und sich damit von ihnen nicht nur das Versprechen erkauft, die erbeuteten Daten wieder zu löschen, sondern auch die Zusage, die Attacke geheim zu halten. Nach § 42a BDSG müssten Unternehmen der Aufsichtsbehörde und den Betroffenen zügig melden, wenn personenbezogene Daten „unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind". Dabei müssten die Unternehmen die Art des Datenlecks benennen und den Opfern Empfehlungen geben, wie weitere negative Auswirkungen vermieden werden könnten. Allerdings müssten nach dem Gesetz die Betroffenen durch das Leck „schwerwiegend beeinträchtigt" sein. Die Meldepflicht gelte bei Internetdiensten für alle Bestands- und Nutzungsdaten. Außerhalb des Internets würden noch einige Monate lang weniger strenge Regeln gelten. Dort greife die Meldepflicht nur für besonders sensible Daten – etwa solche über die Gesundheit, Berufsgeheimnisse etwa von Ärzten oder Anwälten und Kreditkartendaten. Bei Verstößen könnten Geldbußen bis zu 300.000 Euro verhängt werden. Nach der von Mai kommenden Jahres an geltenden Datenschutz-Grundverordnung würden viel strengere Regeln greifen. Sämtliche Datenpannen seien dann meldepflichtig. Die Bußen könnten 10 Mio. Euro betragen oder zwei Prozent des Jahresumsatzes.

Peter Marwan weist am 23. November auf silicon.de darauf hin, dass 2017 die Kosten, die Unternehmen durch Cyberangriffe entstehen, erneut stark gestiegen seien. Im Durchschnitt weise die vom Ponemon Institute im Auftrag von Accenture durchgeführte Erhebung „Cost of Cybercrime" gegenüber dem Vorjahr eine Steigerung von 23 Prozent auf. In den vergangenen fünf Jahren seien die Kosten demnach um 62 Prozent angestiegen. Besonders hoch fielen die Kosten bei Finanzdienstleistern und Energieunternehmen aus. Die höchsten Kosten seien mit durchschnittlich 17,4 Mio. Dollar US-Unternehmen entstanden. Deutsche Unternehmen hätten der Umfrage nach einen besonders starken Anstieg verzeichnet. Die **Kosten durch Cyberangriffe** in Deutschland seien um 42 Prozent auf nun durchschnittlich 11,2 Mio. Dollar pro Jahr gestiegen. Sie umfassten die Ausgaben für das Aufdecken, die Wiederherstellung und Untersuchung sowie Reaktionen auf Sicherheitsvorfälle. Außerdem seien die finanziellen Auswirkungen der dadurch bedingten Betriebsunterbrechungen einbezogen worden. Die starke Zunahme der Kosten führe Accenture insbesondere auf die Malware-Attacken WannaCry und Petya zurück, die bei Unternehmen wie Honda, LG Electronics, Merck, Reckitt-Benckiser oder TNT Express für Umsatzausfälle in Höhe von mehreren hundert Millionen gesorgt hätten. Die Erhebung zeige zudem von Jahr zu Jahr steigende Angriffszahlen. 2017 habe jedes der befragten Unternehmen jährlich 130 ernsthafte Sicherheitsverletzungen verzeichnet. Das entspreche im Vergleich zu 2016 einem Anstieg um 27 Prozent und einer Verdoppelung in fünf Jahren. Gleichzeitig habe die Zeit zugenommen, die benötigt wird, um die Folgen der Angriffe zu beseitigen. Bei Vorfällen mit Insidern dauere die Schadensbehebung durchschnittlich 50 Tage, bei Ransomware-Angriffen 23 Tage.

Gelddiebe haben kaum Chancen, titelt die FAZ am 25. November. 2016 habe es 62,8 Mio. Online-Konten gegeben. Dabei sei es nur zu 2.175 Phishing-Fällen gekommen. Rein statistisch gesehen seien lediglich 0,003 Prozent aller Online-Konten angegriffen und leer geräumt worden. Schützen vor solchen Angriffen könne man sich schon mit einfachen Mitteln: mit einem aktuellen Virenscanner auf dem Rechner. Außerdem sollte man bei Mails von unbekannten Absendern vorsichtig sein und nicht die Anhänge sofort öffnen. Ähnliches gelte für unbekannte Internetseiten. Die Sicherheitslücke im mTAN-Verfahren könne nur ausgenutzt werden, wenn TAN-Programm und Banking-App auf demselben Telefon installiert sind. Die TAN sollte nicht auf demselben Gerät erzeugt werden wie die Überweisung. Bei „Chiptan Comfort" gebe es einen Generator, der Zufalls-TANs produziert und nur mit der eigenen Chipkarte funktioniert. Das sei zumindest aktuell die sicherste Variante.

Wie die FAZ am 29. November berichtet, hat das US-Justizministerium **drei Chinesen** wegen Hacking-Angriffen auf Unternehmen **angeklagt**. Zu den Betroffenen gehöre auch der Siemens Konzern. Den Angeklagten werde vorgeworden, sich 2014 Zugang zu den Computernetzwerken der amerikanischen Tochtergesellschaft von Siemens verschafft und dann im Jahr darauf mehr als 400 Gigabyte an Daten gestohlen zu haben. Die Anklage erhebe nicht direkt den Vorwurf, die Regierung Chinas stehe hinter dem Angriff, und gehe auch nicht im Detail auf das mögliche

Motiv der Hacker ein. Die Ermittler mutmaßten allerdings, dass finanzielle Anreize eine Rolle gespielt haben dürften. Neben den eher banalen Angriffen über E-Mails mit versuchten Anhängen an Siemens-Mitarbeiter sollen auch die Server angegriffen und Daten abgegriffen worden sein.

Kennzeichenerkennung

Die Zeitschrift PROTECTOR enthält in der Ausgabe 11-2017, S. 36/37, eine **Marktübersicht** über 56 Kennzeichenerkennungssystemen von 28 Anbietern. Zu den 29 abgefragten Kriterien gehören neben allgemeinen Angaben Kriterien zum Funktionsumfang, unter anderen Fahrzeugtypen, Kennzeichentypen, Kennzeichenermittlung im Videobild, Auswertungsmöglichkeiten, Auswertesicherheit, Auswertegeschwindigkeit und Auswertebereiche.

Kommunale Sicherheit

Wie der Behörden Spiegel in seiner November-Ausgabe berichtet, führe Nürnberg einen qualifizierten **Kommunalen Außendienst** ein. Er solle zwölf Mitarbeiter umfassen. Sie könnten zum Vorgehen gegen Ordnungsstörungen aller Art eingesetzt werden. Und das sowohl präventiv als auch repressiv. Des Weiteren könnten die Beschäftigten die Polizei und andere Behörden dabei unterstützen, Sicherheitsstörungen sowie das Anbahnen krimineller Handlungen frühzeitig zu erkennen und an die zuständigen Stellen zu melden. Die Arbeitszeiten sollten derart gestaltet werden, dass auch Einsätze in den Abend- und Nachtstunden sowie am Wochenende möglich wären.

„Proaktive Stadtsicherheit" titelt GIT in der Ausgabe 11-2017, S. 50–52. Es bestehe dringender Bedarf an einem intelligenten, integrierten System für urbane Sicherheit. Die „Deep Learning"-fähige Videoüberwachung ermögliche eine zeitnahe und effektive Risikoerkennung. Die einheitliche Plattform erlaube eine schnellere Reaktion im Notfall, und das leistungsfähige Data-Mining trage dazu bei, aus den von Front End-Systemen erfassten Daten mehr Erkenntnisse zu gewinnen. Deep Learning ermögliche sogar die sofortige Klassifizierung von Menschen und Fahrzeugen, die in Videos erscheinen, und erfasse extrahierte Merkmale wie zum Beispiel Farbe der Kleidung, Geschlecht, Kopfbedeckung sowie Nummernschild, Farbe, Größe, Marke und Modell des Fahrzeugs. Die Dahua Smart City Solution lasse sich in vier Arbeitsstufen einteilen: Prävention, Erkennung, Reaktion und Untersuchung. Die integrierte Plattform ermögliche einheitliche Befehle und die zentralisierte Datenspeicherung sowie einen abteilungsübergreifenden Informationsaustausch. Die Untersuchungsstufe erlaube eine schnelle Analyse aller von unterschiedlichen Systemen erfassten Daten. Eine große Auswahl an Data Mining-Methoden wie zum Beispiel die Analyse der aktiven Bereiche, der aktiven Ziele und der Trajektorie stehe ebenfalls zur Verfügung.

Krankenhaussicherheit

Dormakaba Deutschland GmbH stellt in der Zeitschrift GIT, Ausgabe 11-2017, S. 44/45, ein elektronisches Zutrittssystem für ein Krankenhaus vor. Nach dem Prinzip **„Access on Card"** seien die jeweiligen Berechtigungen der Mitarbeiter auf ihrem Ausweismedium gespeichert. Um zu verhindern, dass unberechtigtes Personal oder Patienten Zugriff auf Medikamente in der Notaufnahme haben, seien an den Medikamentenschränken Online-Leser installiert worden. Beschläge sicherten die Zugänge zu Untersuchungsräumen und zu Einzelbüros. An zwei Aufladestationen könnten sich die Mitarbeiter regelmäßig ihre jeweiligen Zutrittsberechtigungen holen.

Logistiksicherheit

Eine Sicherheitsstrategie für Autohöfe und **Lkw-Rastplätze** wird in der Ausgabe 11-2017 der Zeitschrift GIT, S. 62, thematisiert. Durchschnittlich eine Million Euro pro Arbeitstag bezahlten deutsche Versicherer allein für verschwundene Fracht. Das Unternehmen Euro Rastpark biete für Lkw an mittlerweile sieben Autohöfen nach VEDA-Standards abgeschirmte und überwachte Premium-Parkplätze an. Das Unternehmen setze auf pragmatische, kurzfristig wirkende Aufklärungs- und Abschreckungsmaßnahmen wie beschränkte Zufahrten, Beleuchtung und lückenlose Dokumentation aller Fahrzeug- und Personenbewegungen. So seien auf dem Euro Rastpark Theeßen beispielsweise hochauflösende Infrarotkameras vom Typ DE5200HD-DN/IR zur Sicherung der Ein- und Ausfahrten zu den gesonderten Lkw-Stellplätzen im Einsatz.

Maschinensicherheit

In der Ausgabe 11-2017 der Zeitschrift GIT, S. 88–90, stellt die Bihl+Wiedemann GmbH die **„Safety Software Suite"** für AS-i (Actuator/Sensor-Interface) vor. Am Anfang jeder Projektierung eines AS-i-Netzwerks stehe die Zusammenstellung der sicheren Hardware sowie die Erstellung und Inbetriebnahme der sicherheitsgerichteten Gesamtkonfiguration. Die aufeinander abgestimmten Bausteine der „Safety Software Suite" gewährleisteten den schnellen und einfachen Aufbau von Safety-Applikationen sowie deren sichere Inbetriebnahme und die umfassende Dokumentation der mit AS-i Safety at Work realisierten Maschinenabsicherung. Der Beitrag behandelt die Diagnosesoftware, einen Konfigurationstest ohne Hardware, die Hardware-Adressierung und Live-Diagnose sowie das Programmmodul „Konfigurationsübersetzer".

Die Fiessler Elektronik GmbH & Co. KG präsentiert in GIT, Ausgabe 11-2017, S. 92/93, die Sicherheitssteuerung „**Fiessler Modular Safety Controller**". Mit ihrem modularen Konzept könne das Steuerungskonzept flexibel und effizient an die steuerungstechnische Aufgabe angepasst werden. Mit der Variante FMSC Profi könne der maximale Systemausbau von bis zu 16 Erweiterungsmodulen erreicht werden. Dies entspreche einer maximalen Systemkonfiguration von 204 Eingängen, 68 sicheren Ausgängen und 85 Standardausgängen.

Michael Sanchez zeigt in der Ausgabe 11-2017 der Zeitschrift GIT, S. 98–100, wie mit Hilfe von Sicherheitslaserscannern (Produktfamilie MicroScan3) sowie einer Sicherheitssteuerung (Flexi Soft) an einer Spritzgießmaschine der **sichere Betrieb eines Roboters** gewährleistet wird. Die berührungslos wirkenden Schutzeinrichtungen ermöglichten einen ergonomischen Zugang an die Maschine zur prozessgerechten Materialbereitstellung und -entnahme. Der Roboter nehme das bereitgestellte Rohmaterial automatisch auf, sobald der Sicherheitsbereich frei ist und gebe die bearbeiteten Silikon- und Gummiteile aus. Der Beitrag befasst sich mit der Mensch-Roboter-Kooperation (MRK) zur automatischen Materialzufuhr und -entnahme, mit der horizontalen und vertikalen Absicherung mit Sicherheitslaserscannern MicroScan3, den stabilen Messwerten, mit der Vermeidung gegenseitiger Beeinflussung durch kodierte Pulse, der verbesserten Immunität gegen Blendung, Staub und Belagbildung sowie umfassender Expertise bei der Auslegung sicherer Roboterapplikationen. Mit der Produktfamilie MicroScan3 habe ein Technologiewechsel im Markt der aktiv tastenden **Sicherheitslaserscanner** stattgefunden.

Notfall- und Krisenmanagement

Almut Eger und Walter Rüegg, 4m2s – 4 Management 2 Security GmbH, plädieren in der Ausgabe 5-2017 der Zeitschrift Sicherheitsforum, S. 50–53, für „glasklare" Entscheidungen im Notfall- und Krisenmanagement und einen Plan B. Sie beschreiben die wesentlichen Merkmale einer Krise, die überraschende oder schleichende Entstehung einer Krise, Vorbeugungsmöglichkeiten, den BCM-Ansatz als Grundlage, konkrete Maßnahmen für Prävention, Sensibilisierung für frühe Warnsignale, Information und Kommunikation in der Krise, klare Rollenaufteilung und die Umsetzung des Notfall- und Krisenmanagements. Mit Vorbereitung geeigneter Maßnahmen könne die Resilienz des Unternehmens gesteigert und gezielt bearbeitet werden. Mit Schulung und regelmäßigen Übungen könne zusätzlich Sicherheit in die Abläufe gebracht werden.

Dipl.-Entrepreneur FH Uwe Müller-Gauss, Müller-Gauss Consulting, beschreibt im Sicherheitsforum, Ausgabe 5-2017, S. 75–78, vier verschiedene Notfallpläne, die helfen, das Restrisiko zu managen und das Überleben einer Organisation im Fall eines Desasters zu überleben: automatische Evakuierung, angeordnete Evakuierung, Teilevakuierung und Verbleiben im Gebäude. In der Praxis hätten sich folgende **Notfall- und Evakuierungsorganisations(NEO)-Module** bewährt: Die Basislösung, eine „Mini"-Lösung, die „Midi"-Lösung und die „Maxi"-Lösung, die der Autor näher erläutert. Der konkrete Gewinn einer NEO liege nicht allein im verbesserten Schutz von Menschenleben und Sachwerten, sondern auch in einem durch periodisches Üben erhöhten Risikobewusstsein der Mitarbeiter und der damit verbundenen verbesserten Sicherheitskultur.

Öffentliche Sicherheit

Innere und äußere Sicherheit verschmelzen zunehmend, titelt der Behörden Spiegel in seiner November-Ausgabe. Die Globalisierung und die Entwicklungen im digitalen Raum führten dazu, dass sich Sphären, die früher klar voneinander zu unterscheiden waren, immer mehr vermischen. Das spürten auch die deutschen Nachrichtendienste, die heutzutage viel stärker bereits im Bereich der Vorfeldaufklärung und Gefahreneinschätzung tätig würden. Es käme zwischen den Nachrichtendiensten des Bundes darauf an, untereinander Synergien zu nutzen,

Erkenntnisse zu teilen und gemeinsame Datenbanken zu verwenden. Letzteres sei bisher nur mit europäischen Nachrichtendiensten gestattet. BND und BfV dürften hingegen derzeit noch keine gemeinsamen Projektdateien errichten.

Rechenzentrumssicherheit

Das BSI empfiehlt in der Zeitschrift <kes>, Ausgabe 5-2017, S. 42/43, folgende **neue, zeitgemäße Rechenzentrumsdefinition**: „Hat eine IT-nutzende Organisation nur einen zentralen IT-Betriebsbereich, ist dieser gemeinsam mit den erforderlichen Supportbereichen grundsätzlich immer wie ein RZ entsprechend dem Schutzbedarf zu behandeln. Unter ‚IT-Betriebsbereich' sind Räume zu verstehen, in denen die Hardware aufgebaut ist und betrieben wird, die der Bereitstellung von Diensten und Daten dient. Das RZ umfasst neben dem IT-Betriebsbereich alle weiteren technischen Supportbereiche (Stromversorgung, Kälteversorgung, Löschtechnik, Sicherheitstechnik usw.), die dem bestimmungsgemäßen Betrieb und der Sicherheit des IT-Betriebsbereichs dienen." Es folgen Definitionsabweichungen: wenn die IT innerhalb eines Gebäudes/einer Liegenschaft verteilt betrieben wird; wenn die IT-nutzende Organisation an mehreren, räumlich voneinander getrennten Standorten angesiedelt ist; für kritische Geschäftsprozesse; und für IT-Betriebsbereiche, aus denen heraus Dienste für Dritte erbracht werden.

Schließsysteme

Die **Kombination elektronischer und mechanischer Schließsysteme** thematisiert in der Zeitschrift PROTECTOR, Ausgabe 11-2017, S. 40/41, Gerd Reime, PICOSENS GmbH. Beide hätten ihre Vorteile, aber leider auch ihre Nachteile. PICOSENS habe sich vorgenommen, die Vorteile beider Systeme in einem System zu vereinen und eine komplett neuartige Variante von Schlüssel und Leseeinheit entwickelt, die auf Basis von quantenphysikalischer sogenannter Festkörperkryptografie beruht. Erreicht werde diese Verschlüsselung durch einen komplexen Vorgang, bei dem durch lokale Veränderungen der Kristallgitterstruktur des Materials, der unverwechselbare, eindeutige Code in das Metall unauslöschlich „geschrieben" wird. In einem kleinen, acht Zentimeter langen Metallschlüssel könnten so über 900 Mrd. eindeutig unterscheidbare Codes untergebracht werden. Die Leseeinheit des Quantenkeys könne mit jeder beliebigen Schließeinheit über verschlüsselte Daten kommunizieren und biete zahlreiche Anwendungen. Das System sei voll integrierbar in bereits bestehende Systeme.

ASSA ABLOY präsentiert in der Ausgabe 11-2017 der Zeitschrift GIT, S. 37, das Schließsystem **Keso 8000Omega2**. Nach einer Studie des LKA Berlin wird ein Einbruch über den Zylinder in 23 Prozent der Fälle mit nichtdestruktiven Methoden geöffnet, durch illegale Schlüsselkopien oder Picking, und in rund 77 Prozent über destruktive Methoden wie Bohren, Ziehen oder Abbrechen. Daher sei es wichtig, dass ein Schließsystem beiden Manipulationsarten standhalten kann. Keso sei die neueste Generation mechanischer und mechatronischer Schließanlagen. Das patentierte System sei modular aufgebaut, voll mechatronisch erweiterbar und mit einem aktiven Kopierschutz Omega2 gegen Picking und illegale Schlüsselkopien geschützt. Durch das Wendeschlüsselsystem seien sowohl komplexe als auch einfache Schließanlagen realisierbar. Der Aktivkopierschutz Omega2 bestehe aus integrierten beweglichen Elementen im Schlüssel, welche durch gleich mehrere Trennlinien im Zylinder abgefragt werden. Diese patentierte Technologie biete maximalen Schutz bei Picking-Versuchen.

Schmuggel und Fälschungskriminalität

Deutschland sei ein großes **Ziel des Zigarettenschmuggels,** heißt es in einem Bericht in der November-Ausgabe des Behörden Spiegel. Die Polizei kümmere sich kaum um den Zigarettenschmuggel. In Berlin verkauften vietnamesische Händler die Zigaretten mittlerweile aus Plastiktüten heraus stangenweise. Sie hätten auch nicht mehr größere Vorräte an Zigaretten direkt an ihren Verkaufsplätzen. Der Nachschub werde vielmehr aus sogenannten „Bunkern" heraus geliefert. Dabei handele es sich in der Regel um Wohnungen sozial schwächerer deutscher Staatsbürger. Bei den in Polen startenden Nachschubfahrten seien mindestens zwei, teilweise auch drei Fahrzeuge mit gefälschten Kennzeichen unterwegs. Bei einem von ihnen handele es sich um den sogenannten „Piloten". Dessen Lenker fahre vorweg und prüfe die Strecke mit seinem hochmotorisierten Fahrzeug auf Kontrollpunkte. Stelle er solche fest, informiere er den

Fahrer des eigentlichen Lieferfahrzeugs und fordere diesen sogar auf, nach Polen zurückzukehren. Produktfälscher seien in jenen Feldern aktiv, in denen die Gewinne hoch und die Kontrolldichten gering seien. Im Kampf gegen Plagiate sei eine bessere Zusammenarbeit von Industrie, Handel und Behörden erforderlich. Nur durch Interoperabilität könnten alle Glieder einer Lieferkette effektiv geschützt werden.

Sicherheitsgewerbe

In der Ausgabe 11-2017 stellt PROTECTOR ein **Wächterkontrollsystem mit digitalem Wachbuch** vor (S. 70/71). Wenn es um die Vereinfachung, Strukturierung und Beschleunigung täglicher Prozesse und Aufgaben in Sicherheitsunternehmen geht, biete das Programm Disponic der Bite AG eine komfortable Komplettlösung. Insbesondere bei der Personaleinsatzplanung sei das Programm eine große Hilfe, da beispielsweise Doppelbelegungen verhindert und die Planung zahlreicher Mitarbeiter inklusive der jeweiligen Qualifikationen optimal übernommen würden. Nun gebe es einen weiteren Baustein: Ein Wächterkontrollsystem mit integriertem Wachbuch. Neben der dokumentensicheren Protokollierung aller Vorfälle am Objekt speichere das Logbuch per App automatisch und elektronisch auch Arbeitsstunden und Pausenzeiten der Mitarbeiter. An einem zu bewachenden Objekt würden kostengünstige und wetterbeständige Kontrollpunkte in Form von „Near Field Communication" (NFC)-Chips angebracht. Mit einem handelsüblichen Smartphone könne der Mitarbeiter während seinem Kontrollgang die Kontrollstellen scannen. Dadurch werde automatisch und elektronisch ein Eintrag im Wachbuch erzeugt. Dieser könne mit zusätzlichen Informationen – wie Text und Bildern – ergänzt werden. Das Unternehmen sehe aufgrund des Wächterkontrollsystems rechtzeitig, ob ein Mitarbeiter zum Dienst vor Ort erschienen ist.

Walter Rijk, SequriX B.V., thematisiert in der Ausgabe 11-2017 der Zeitschrift PROTECTOR, S. 72, die **Verwaltung von Unternehmensdaten**. Noch interessanter als Smartphones, Videosysteme und Sensoren als Informationsquellen sei die Verbindung dieser Quellen, auch das „Internet der Dinge" genannt. Innerhalb der Software von Sequrix würden Daten aus mehreren Informationsquellen verknüpft. Damit wolle man nicht nur Sicherheitsdienste automatisieren und Wachleute besser kommunizieren lassen, sondern dem Sicherheitsunternehmen auch wertvolle Informationen bieten. SequriX sei nach ISO 27001 und SOC2 zertifiziert und arbeite mit Zwei-Faktor-Authentifizierung.

Neue DIN 77200 ermöglicht die Zertifizierung von Wach- und Sicherheitsdienstleistungen, titelt SecuPedia am 11. November (secupedia.info). Der BDSW weise darauf hin, dass das DIN im November die Teile eins und drei der Reihe veröffentlicht habe. Der Normteil DIN 77200-1 enthalte Mindestanforderungen an Sicherheitsdienstleister und deren Niederlassungen in Bezug auf Organisation, Prozesse und Personal. So müssten sie belegen, dass Mitarbeiter erfolgreich die Sachkundeprüfung nach § 34a GewO abgelegt haben und dass sie über ein schriftlich dokumentiertes Verfahren verfügen, um die Aus- und Weiterbildung der Mitarbeiter sicherzustellen. Normteil DIN 77200-3 beschreibe die Anforderungen an Zertifizierungsstellen und den Ablauf des Verfahrens, mit dem sich prüfen lasse, ob die in Teil 1 beschriebenen Kriterien eingehalten werden. Der Normteil DIN 77200-2 enthalte weitere Anforderungen für besondere Leistungsbereiche, beispielsweise öffentliche Veranstaltungen und den Personenverkehr. Er sei in Bearbeitung und werde voraussichtlich im Sommer 2018 veröffentlicht.

Sicherheitstechnik

Thomas Streit, Bouygues Energies & Services Schweiz AG, beleuchtet in der Ausgabe 5-2017 der Zeitschrift Sicherheitsforum, S. 92–95, Wartung und Unterhalt von Sicherheitsgewerken mit Fokus auf den baulich-technischen Teil im Sinne des **technischen Facility Managements**. Er behandelt die Disposition von Störungen und sonstigen Meldungen, die Ereignisvorsorge, Arbeitssicherheit und Gesundheitsschutz, Informationssicherheit und Datenschutz, Brandschutz und Evakuierungsplanung.

Smart Home Security

Ein interaktives, funkbasiertes Smart Home-System stellt UTC Fire & Security Deutschland in der Ausgabe 11-2017 der Zeitschrift GIT, S. 45/55, vor. Die Konfiguration dieses Systems (**ZeroWire**) sei einfach. Sie basiere auf dem Konzept der „Szenen", die bis zu 16 Aktionen auslösen könnten,

um ein automatisiertes Ereignis zu erstellen. Eine Szene könne entweder manuell, über einen Zeitplan oder über ein Systemereignis ausgelöst werden, zum Beispiel über einen Sensor. Eine „Gute Nacht"-Szene könne dazu führen, dass die Türen verschlossen sind und die Lichter abgeschaltet werden, wenn das Sicherheitssystem scharf geschaltet ist.

Umweltschutz

Wie Wertschöpfungsketten durch **Chinas Umsetzung von Umweltrichtlinien** leiden, beschreibt Julia Coym, Control Risks, im ASW-Newsletter vom 24. November. Mit Berichten über Schließungen von nicht weniger als 30.000 vorwiegend chinesischen Unternehmen allein in einem Industriezentrum in Shandong habe die Zahl der permanenten und zeitweiligen Stilllegungen während der letzten beiden Runden der Regierungskampagne für die Umsetzung von Umweltschutzmaßnahmen ein beispielloses Niveau erreicht. Ein strengeres Umweltschutzgesetz, in Kraft seit 2015, habe die Strafen erheblich erhöht und ein rechtliches Vorgehen durch Staatsbedienstete und Umweltschutzorganisationen gegen Unternehmen ermöglicht, die gegen Umweltgesetze verstoßen. Die Behörden könnten die Einhaltung von Umweltschutzbestimmungen häufiger und in größerem Umfang überprüfen. Die Autorin rät Unternehmen, die treibenden Kräfte und den Zeitplan hinter diesen breit angelegten Umsetzungsmaßnahmen verstehen zu lernen, ihre Kommunikation mit allen Aufsichtsbehörden im Hinblick auf Umweltfragen neu auszurichten und zu intensivieren, und ihre gesamte Lieferkette kennenzulernen, um sicherstellen zu können, dass alle Beteiligten sich ebenfalls an die Vorgaben zum Umweltschutz halten.

Veranstaltungssicherheit

Ein Zaunsystem, das temporären Schutz bei Veranstaltungen biete, stellt der Behörden Spiegel in der November-Ausgabe vor. Mit dem **Mobilen Sicherheitszaun Publifor** biete Betafence ein massives, bewegliches Zaunsystem für die temporäre Absicherung von Veranstaltungen und Objekten an. Die rund 2,4 Tonnen schweren Zaunelemente bestünden aus einem robusten Rahmenprofil mit beidseitig montierten Gittermatten und einem massiven, mit Beton gefüllten Stahlsockel. Die äußerst widerstandsfähigen Elemente seien für den Transport mit einem Gabelstapler konzipiert und ließen sich in kurzer Zeit als temporäre Sicherung aufbauen, die größere Menschenansammlungen kontrolliere. Die Grundkonstruktion der 2,50 m hohen Zaunelemente bestehe aus sehr robusten waagerechten und senkrechten Stahlpfosten und 80 x 60 mm Profil. Das Publifor-System verbinde Mobilitätmit enormer Widerstandskraft und ermögliche mit geringem Montageaufwand eine hohe temporäre Sicherheit.

Die FAZ berichtet am 29. November, dass nach einer Eilentscheidung des Berliner Verwaltungsgerichts vom 28. November für den **Schutz von Weihnachtsmärkten** vor Terroranschlägen nicht die Veranstalter zuständig sind. Maßnahmen wie der Schutz des Geländes etwa in Form von Betonquadern oder die Bereitstellung „eines beweglichen schweren Fahrzeugs als mobile Komponente" könnten nicht den Betreibern auferlegt werden.

Videoüberwachung

„Video Surveillance as a Service" (VSaaS) behandelt Marco Pompili, Axis Communications GmbH, in der Zeitschrift Sicherheitsforum, Ausgabe 5-2017, S. 42/43. Unternehmen, insbesondere KMU, könnten Videoüberwachung als einen Service abonnieren, der über die Cloud aus der Ferne verwaltet wird. Der Service bringe eine Reihe an Vorteilen gegenüber einem eigenen Videoüberwachungssystem mit sich. Einer davon sei finanzieller Natur: Statt eines großen Betrags zahle das Unternehmen eine feste monatliche Gebühr. Ein weiterer Vorteil: der Dienstleister übernehme die Administration des Betriebssystems und der Anwendungssoftware. Unternehmen könnten den Service mit einer Notrufserviceleitstelle kombinieren. Vor allem KMU seien mit dem VSaaS-Modell gut bedient, denn es koste sie keinerlei technische Investitionen oder Wartungsaufwand.

Einen **Digital Video Manager**, EVM R620, stellt Honeywell Building Solutions, in der Ausgabe 11-2017 von GIT, S. 18/19, vor. Auf Basis einer hochverfügbaren dezentralen Architektur ermögliche das System die Wiedergabe von Aufzeichnungen direkt von der Kamera aus (Edge Recording Playback). Das Video werde dabei zunächst auf einer Kameraspeicherkarte erfasst und erst dann mittels Backfill-Funktion auf den Hauptserver des Systems übertragen und dort abgespeichert. Diese

Funktionen machten das System widerstandsfähiger gegenüber Unterbrechungen. Neben der verbesserten Verfügbarkeit, der Benutzerfreundlichkeit und der Interoperabilität befähige DVM R620 Unternehmen zur durchgehenden Authentifizierung von Videomaterial, zur sicheren Aufbewahrung und zu effizienterer Nutzung von Netzwerk- und Hardwareressourcen.

Sensitive Kameras, Thermaltechnologie und Drohnen erweitern die Möglichkeiten der Videoüberwachung, betont Hikvision Europe in GIT, Ausgabe 11-2017, S. 38–40. Für Aufnahmen bei schwachem Licht sei die **Darkfighter-Technologie** entwickelt worden: Hochauflösende CMOS-Sensoren gepaart mit Wider Dynamic Range-Funktionen und der 3D DNR (Dynamic Noise Reduction)-Technologie, die Bildrauschen in schwierigen Lichtsituationen unterdrückt. Thermalkameras arbeiteten mit einem selbstentwickelten Chip und zeichneten sich durch attraktive Gesamtbetriebskosten, Flexibilität sowie leistungsstarke Smart-Funktionen aus. Der Einsatz der Kameras könne bei der Überwachung großer Flächen und im Perimeterschutz empfohlen werden. Die Darkfighter PTZ-Kamera mit Infrarotbeleuchtung bis 500 Meter und optischem 36x-Zoom sei speziell für scharfe Farb- und monochrome Bilder unter schwierigsten Lichtverhältnissen entwickelt worden.

Wirtschaftsschutz

Volker Wagner, ASW, weist in PROTECTOR (Ausgabe 11-2017, S. 58/59) darauf hin, dass der ASW Bundesverband die Verankerung von Wirtschaftsschutzbeauftragten in Unternehmen und staatlichen Stellen fordere. Der ASW Bundesverband habe ferner zusammen mit dem BfV und dem BSI am 16. Oktober 2017 einen neuen Baustein für das **Wirtschaftsgrundschutz-Handbuch** veröffentlicht. Er befasse sich mit dem Thema Krisenkommunikation.

Impressum

Focus on Security enthält Informationen zum Unternehmensschutz und wird monatlich herausgegeben. Der Focus on Security erscheint per elektronischem Newsletter, der an 1.800 Abonnenten verteilt wird.

Hinweis der Redaktion
Sämtliche Personenbezeichnungen im Plural gelten auch ohne ausdrückliche Nennung gleichermaßen für männliche und weibliche Personen.

Herausgeber
Manfred Buhl, Vorsitzender der Geschäftsführung, Düsseldorf

Verantwortlicher Redakteur
Bernd Weiler, Leiter Kommunikation und Marketing

Beratender Redakteur
Reinhard Rupprecht, Bonn

www.securitas.de/focus

Kontakt

Securitas Holding GmbH
Redaktion Focus on Security
Potsdamer Straße 88
10785 Berlin

Sitz: Düsseldorf, Amtsgericht Düsseldorf HRB 33348
Geschäftsführer: Manfred Buhl (Vors.), Jens Müller, Gabriele Biesing, Dr. Heiko Kroll
Vorsitzender des Aufsichtsrates: Dr. Carl A. Schade

E-Mail: info@securitas.de