Focus on Security

Ausgabe 10, Oktober 2016

SECURITAS

Inhalt

Arbeitsschutz

Für vorbildlichen Arbeitsschutz wurde die **Securitas Power & Service GmbH & Co.KG** in Biblis mit dem VBG-Arbeitsschutzpreis 2016 in Gold ausgezeichnet, meldet der DSD in der Ausgabe 3-2016, S. 73. Sie erhielt die Auszeichnung für ihr „betriebliches Gesundheitsmanagement im Objekt Biblis". Sie habe zielstrebig an der Einführung neuer Präventionsmaßnahmen gearbeitet und diese auch erfolgreich umgesetzt.

Anforderungen und normengerechte **Persönliche Schutzausrüstung** (PSA) sei Sache der Hersteller, des Handels und der Arbeitgeber, betont Werner Münnich, Wirtschaftsverband Textilservice WIRTEX e. V., in der Zeitschrift GIT, Ausgabe 4-2016, S. 196–198. Die PSA solle den Träger bei seiner täglichen Arbeit schützen. Dabei handele es sich bei PSA meist um Schutzkleidung, doch auch Hand- und Fußschutz sowie Atem- und Kopfschutz zählten als Schutzausrüstung. Alle Produkte unterlägen dabei den Normen der EU-Kommission. Im April sei die neue EU-Verordnung zu PSA 2016/425 in Kraft getreten. Sie unterscheide sich deutlich von der PSA-Richtlinie 89/686 EWG und schaffe mehr Sicherheit für Beschäftigte und verantwortliche Arbeitgeber. Hersteller und Handel würden stärker in die Pflicht genommen. Dass die PSA während der gesamten Nutzungsdauer funktionieren und sich in einem hygienisch einwandfreien Zustand befinden müsse, sei zudem der PSA-Benutzerverordnung sowie den technischen Regeln zu entnehmen. Mietservice-Anbieter von Berufskleidung sorgten für stets gereinigte und nach der aktuellen Norm zertifizierte Kleidung. So müssten sich Unternehmen auch bei der neuen Gesetzeslage um nichts kümmern.

Bahnsicherheit

Hans-Hilmar Rischke geht in einem Interview mit GIT SICHERHEIT auf die Sicherheitsstrategie der Deutschen Bahn ein (GIT-SICHERHEIT.de vom 23. September). Sie habe mehrere Säulen. An erster Stelle stehe die ganz enge Abstimmung mit den Sicherheitsbehörden. Die zweite Säule seien hochqualifizierte und motivierte Mitarbeiter. Die dritte Säule sei die Technik, mit der die Mitarbeiter unterstützt würden. Der DB-Vorstand habe den Auftrag erteilt, die Security-Organisation des Konzerns weiterzuentwickeln. Für die DB Sicherheit bedeute das, nicht wie bisher als Dienstleister Sicherheitsstunden nach Auftrag zu erbringen, sondern die vollständige operative Verantwortung für die Sicherheit von Kunden und Mitarbeitern zu übernehmen. Die DB Sicherheit sei in der Fläche präsent, fokussiere sich aber zunehmend auf Schwerpunkte: stark frequentierte Stationen ebenso wie Stationen, die nur am Wochenende oder bei Veranstaltungen und Volksfesten genutzt werden. Sie bekämpfe gezielt Phänomene wie etwa den Metalldiebstahl. Nach mehr als 3.000 Fällen 2012 seien 2015 nur noch gut 1.000 Fälle registriert worden. Gezielte Bestreifung, enge Zusammenarbeit mit der Bundespolizei, künstliche DNA zur Markierung von Metallteilen und die enge Zusammenarbeit mit Metallhändlern im In- und Ausland hätten das Risiko für Täter massiv erhöht. Videoüberwachung, Gepäck- und Personenkontrollen oder Personalpräsenz und sogar „Train-Marshalls" könnten einen fanatischen Einzeltäter nicht abhalten, das **offene System Bahn** und seine Nutzer anzugreifen. In der Praxis hieße das für die Mitarbeiter und Kunden, auffällige Personen, Bewegungen und Gepäckstücke zu erkennen. Bundesweit seien über 5.000 Kameras an 700 Bahnhöfen im Einsatz. Damit würden bereits über 80 Prozent der Reisendenströme erfasst. Kürzlich sei die Aufzeichnungsfunktion von 600 Kameras an 70 Berliner S-Bahnhöfen in Betrieb genommen worden. Rund

27.000 Kameras seien in Nahverkehrs- und S-Bahnzügen eingebaut. Den Zugriff auf alle Aufzeichnungen habe nur die Bundespolizei.

Bausicherheit

Verbände warnen vor Sicherheitslücken beim Bauen, titelt die FAZ am 5. September. Kristallisationspunkt des Verbände-Ärgers sei die **EU-Bauproduktenverordnung** – oder besser die Art und Weise, wie sie in Deutschland umgesetzt werde. Einige der Bauprodukte, die auf Basis der EU-Verordnung auf dem Markt sind, erfüllten nach Meinung der Bauwirtschaft nicht die deutschen Anforderungen an Sicherheit und Umweltverträglichkeit. Zum Beispiel fehlten Aussagen zum Brandverhalten von Wärmedämmstoffen. Für völlig verfehlt hielten die Verbände den Plan der Regierung, dass Produkthersteller künftig freiwillig Nachweise in puncto Sicherheit einführen sollen, die wiederum Bauherren, Architekten, Ingenieure und Handwerker dann klaglos akzeptieren sollen. Dass die bislang staatlich geregelte Sicherheit von Bauprodukten nun auf die Unternehmen verlagert werden soll, stelle „einen Paradigmenwechsel" mit weitreichenden Folgen dar. Das derzeitige Niveau der Sicherheit und Umweltverträglichkeit von Bauwerken in Deutschland werde mit dem europäischen CE-Zeichen für Bauprodukte allein jedenfalls nicht mehr zu halten sein.

Betrug

Betrügereien in Telekom-Filialen, titelt die FAZ am 8. September. Mitarbeiter der Deutschen Telekom hätten sich beim Abschluss von Handyverträgen jahrelang Payback-Punkte auf eigene Karten gutschreiben lassen. Nach Angaben des Konzerns seien quer durch Deutschland rund 120 Mitarbeiter in die Betrügereien verwickelt. In den Jahren 2014 und 2015 sei es zu mehreren tausend Falschbuchungen gekommen. Den Gesamtschaden habe die Telekom auf 400.000 Euro beziffert. Im Zuge der Vertragsverlängerung zwischen der Telekom und Payback Mitte 2016 hätten beide Seiten Vorkehrungen getroffen, um derartige Machenschaften in Zukunft zu verhindern. Außerdem müsse jeder Telekom-Mitarbeiter eine Erklärung unterschreiben, dass von Kunden ungenutzte Vergünstigungen nicht auf eigene Kartenkonten gebucht werden dürften.

Inkerman Fraud Weekly weist in der Ausgabe 177 darauf hin, dass einer neuen Studie zufolge **Social-Media-Betrugsdelikte** einen neuen Höchststand erreicht hätten. Die Studie stelle fest, dass 20 Prozent der mit zehn großen weltweiten Marken verbundenen Social-Media-Konten gefälscht gewesen seien. Die zwischen April und Juni 2016 durchgeführte Studie habe sich auf allgemein bekannte Plattformen wie Facebook, Twitter, YouTube und Instagram konzentriert. 30 Prozent der als gefälscht identifizierten Konten enthielten Angebote für gefälschte Waren und Dienstleistungen, während weitere vier Prozent mit Phishing, Schädlingen und Protesten verknüpft gewesen seien. Phishing sei die am schnellsten zunehmende Bedrohung in den sozialen Medien (Anstieg von 150 Prozent von 2015 bis 2016).

Weltweit sei eine starke **Zunahme von Finanzbetrugsdelikten** gemeldet worden, wobei zwischen Januar und Juni 2016 mehr als eine Million Vorfälle erfasst worden seien, die zu Geldverlusten geführt hätten, meldet Inkerman Fraud Weekly in der Ausgabe 178. Gegenüber der ersten Jahreshälfte von 2015 stelle dies einen Anstieg von 53 Prozent dar. Die Vorfälle bezögen sich auf Zahlungskarten-, Scheck-, Online-Banking- und Telebanking-Betrug.

Brandschutz

Dipl.-Ing. Paul Frey, Basellandschaftliche Gebäudeversicherung, stellt in der Ausgabe 4-2016 der Zeitschrift Sicherheitsforum, S. 61–63, **ingenieurwissenschaftliche Methoden** im Brandschutz vor. Das von seiner Versicherung herausgegebene **Handbuch** „Brandschutzplanung mit ingenieurwissenschaftlichen Methoden" sei aus dem Studium einer umfangreichen Sammlung von Publikationen hervorgegangen, die vornehmlich ausländische Normen, Richtlinien, Forschungsarbeiten, Fachbücher und Fachzeitschriften umfasse. Der Autor listet die Themen der leistungsorientierten Brandschutzplanung auf, die im Handbuch behandelt werden und geht auf gesetzliche Grundlagen, auf Prozessschritte der leistungsorientierten Brandschutzplanung, auf drei Stufen brandschutztechnischer Berechnungen (Berechnungen mithilfe tabellarischer Werte, Berechnungen mithilfe vereinfachter Rechenverfahren und Berechnungen mithilfe allgemeiner Rechenverfahren), auf Schutz- und Planungsziele, Brand- und Personensicherheitsberechnungen sowie Brand- und Personenstrommodelle ein.

Mit der **Abschaltung von Brandmeldeanlagen** (BMA) befasst sich GIT in der Ausgabe 9-2016, S. 100/101. Abschaltungen gehörten bei BMA zum täglichen Geschäft. Sie müssten immer korrekt ausgeführt und wieder rückgängig gemacht werden. Darüber hinaus empfehle es sich, den gesamten Vorgang zu dokumentieren. Für das Management solcher Abschaltungen stünden den Verantwortlichen in der Sicherheitsleitstelle bislang nur unzureichende Konzepte zur Verfügung. Abhilfe schaffe ein neues Konzept, das ein solches Abschaltungsmanagement parallel zum normalen Meldungsbetrieb ermögliche, sich aber nicht ausschließlich auf die Bedürfnisse bei der Abschaltung von BMA beschränke. Mit Hilfe eines Moduls zum Management von Schaltvorgängen ließen sich Zeiträume einzeln oder zyklisch festlegen, in denen bestimmte angeschlossene Sensoren und Aktoren in einen definierten Zielzustand versetzt werden sollten. Neben der Planung und Automatisierung von Schaltzeiten übernehme ein solches Modul auch deren Verwaltung und Dokumentation.

Nach wie vor würden bei den meisten Feststellanlagen die **Rauchschalter** nur selten oder gar nicht ausgetauscht, berichtet die Zeitschrift GIT in der Ausgabe 9-2016, S. 158/159. Dabei sei in der DIN 14677 ein eindeutiger Tauschzyklus festgelegt. Diese 2011 herausgegebene Norm beschreibe die allgemein anerkannten Regeln der Technik. Wer nicht nach ihr handelt, habe ein erhöhtes Haftungsrisiko. Demnach müssten Rauchschalter ohne Verschmutzungskompensation nach fünf Jahren ausgetauscht werden, für Rauchschalter mit Verschmutzungskompensation gelte eine Austauschfrist von acht Jahren. Der „Instandhalter" sollte den Betreiber nachdrücklich auf die Austauschpflicht und die mit ihrer Missachtung verbundenen Risiken hinweisen. Dass der Instandhalter seiner Informationspflicht nachgekommen ist, sollte er auch nachweisbar dokumentieren.

Peter Holzamer, Prymos GmbH, verteidigt in der Zeitschrift GIT, Ausgabe 9-2016, S. 162–165, den Vertrieb des **Feuerlöscher-Sprays und der wartungsfreien Feuerlöscher** gegen die fachliche Kritik des Fachingenieurs für Brandschutz, Peter Gundermann. Durch das neue Konzept werde die alte Ordnung der angenehm engmaschigen Wartungsintervalle und des blühenden Ersatzteilgeschäfts kräftig aufgemischt. Die kombinierte Brandschutzlösung sei so einfach wie stimmig: Feuerlöscher-Sprays am Arbeitsplatz, kombiniert mit leichtgewichtigen und wartungsfreien Composite-Kevlar-Feuerlöschern neuester Generation, folglich eine individuell am Arbeitsplatz orientierte Absicherung. Dazu wartungsfrei, denn nach fünf bzw. zehn Jahren würden die Löschgeräte kundenfreundlich einfach ausgetauscht. Der Wartungsaufwand könne entfallen.

Der Sicherheits-Berater direkt weist am 22. September auf die neueste Innovation der **TITANUS**-Familie hin: Das Ansaugrauchmeldesystem analysiere mittels 4-D-Detektionsverfahren Rauchpartikel auf Muster- und Stofferkennung. Der neuartige Ansaugrauchmelder erkenne, was brennt und was täuscht. Dies ermögliche vollkommen neue Schutzkonzepte. Beispielsweise könne zwischen Theaternebel als Täuschungsgröße und Rauchpartikeln von Kabelbränden unterschieden werden. Erstmalig könnten täuschende Partikel wie Staub oder Tabakrauch, die häufig zu Falschalarmen führen, dem neuen Ansaugrauchmelder TITANUS MULTI SENS kundenspezifisch angelernt werden, um Betriebsausfälle und Feuerwehreinsätze zu vermeiden.

Dr. Günther Roßmann, GDV, befasst sich in der Ausgabe 3-2016 der Zeitschrift s+s report S. 13–17, mit der GDV-Publikation zur Schadenverhütung „**Umgang mit Magnesium** – Gefahren und Schutzkonzepte" (VdS 3537), die die Brand- und Explosionsgefahren bei der Be- und Verarbeitung sowie bei der Lagerung von Magnesium beschreibt. Im Vordergrund der Richtlinie stünden der Sachwertschutz sowie die Vermeidung von Betriebsunterbrechungsschäden. Magnesium besitze deutlich kritischere Brand- und Explosionskenngrößen als Aluminium. Der Autor beschreibt das Anwendungsspektrum von Magnesium, Brand- und Explosionsgefahren aufgrund der Reaktionsfähigkeit (Reaktion mit Wasser/Luftfeuchtigkeit, Reaktion mit anderen Stoffen und Staubexplosionsgefahr), Löschmittel für Magnesium, Brand- und Explosionsschutzmaßnahmen, Lagerung und Bearbeitung von Magnesium (spanende und spanlose Verfahren).

Brandschutzanforderungen bei älteren Gebäuden behandelt Rechtsanwalt Stefan Koch in der Ausgabe 3-2016 der Fachzeitschrift s+s report, S. 18–21. Er zeigt den rechtlichen Rahmen und das Verhältnis der Rechtsinstitute „Bestandschutz", „Verkehrssicherungspflicht" und „Strafbarkeit" auf. Der Bestandsschutz finde seine Grenzen dort, wo Leib und Leben durch unzureichende Brandschutzmaßnahmen gefährdet werden. Für das Entstehen einer Verkehrspflicht seien verschiedene Grundlagen anerkannt. Der Verkehrssicherungspflichtige sei jedoch nicht verpflichtet, das Gebäude als Gefahrenquelle gegen alle denkbaren Schadensfälle abzusichern. Seine Pflicht beschränke sich vielmehr darauf, Vorkehrungen gegen Gefahren zu treffen, welche durch eine gewöhnliche Benutzung eintreten können und vorhersehbar sind. So stelle die Sicherung des zweiten Rettungsweges z. B. der Regelung in § 17 Abs. 3 BauO NRW eine nach objektiven Maßstäben zumutbare und erforderliche Verkehrspflicht dar, ebenso die gesetzlich geforderte Installation von Rauchmeldern. Die Fälle, in denen trotz objektiver Verletzung einer Verkehrspflicht die Haftung am Verschulden scheitert, seien selten. Die Verkehrssicherungspflicht könne umfassender sein als die von der „Baupolizei" gestellten Anforderungen. Die Gefahrenschwelle des öffentlichen Baurechts kennzeichne in der Regel zugleich die Schwelle für eine zivil- und strafrechtliche Pflicht zum Tätigwerden.

Dipl.-Ing. Heike Siefkes, VdS Schadenverhütung, skizziert in s+s report, Ausgabe 3-2016, S. 24/25, die Überarbeitung der VdS-Richtlinien 2380, 2381, 2093 und 3518 für Planung und Einbau von **Gaslöschanlagen**. Die Autorin behandelt die Aussetzung des Klassifizierungssystems, aktuelle Änderungen der Richtlinien, Richtlinienänderungen bei der Ansteuerung und Auslösung der Löschanlagen und bei der Betriebsmittelabschaltung. Auch das Regelwerk VdS 2093 (Planung und Einbau von CO_2 -Feuerlöschanlagen) befinde sich in Überarbeitung.

Dipl.-Ing. Frank Schäfer, VdS Schadenverhütung, erläutert in der Ausgabe 3-2016 der Zeitschrift s+s report, S. 26/27, die **VdS-Anerkennung für Produkte und Systeme**. Sie könne über die Verfahrensrichtlinie VdS

2344 beantragt werden. Der Autor behandelt die Funktionsprüfung und Umweltprüfungen (Temperatur, hohe Luftfeuchtigkeit, Korrosion, mechanische Festigkeit, elektromagnetische Verträglichkeit und IP-Schutz) und Besonderheiten softwaregesteuerter Geräte. Da es praktisch unmöglich sei, alle verschiedenen Kombinationen eines Systems zu prüfen, sei ein spezielles Verfahren entwickelt worden, das in DIN EN 54-13 festgelegt sei. Am Anfang stehe die theoretische Analyse des gesamten Systems. Mit den einzelnen Systemsegmenten würden Prüfungen unter Worst-Case-Bedingungen durchgeführt.

Compliance

In Deutschland fehlen Richtlinien für Compliance, heißt es in der FAZ am 14. September. Ernsthafte Risiken für Manager entstünden dann, wenn das Unternehmen in maßgeblicher Weise gegen Strafvorschriften verstößt. Das Management brauche nicht selbst am Verstoß beteiligt zu sein; es reiche aus, wenn fahrlässiger Weise nicht genug oder nicht richtig in Prävention investiert wurde, insbesondere in ein Compliance-Managementsystem, kurz CMS. Wie ein solches CMS aussehen muss, sage der deutsche Gesetzgeber nicht. Insbesondere in den USA und Großbritannien würden die zu erwartenden rechtlichen Konsequenzen das in Deutschland mögliche Ausmaß übersteigen. Zum Beispiel soll in den USA die Verantwortung für die Implementierung eines effektiven CMS einem Führungsgremium übertragen werden, die Mitarbeiter sollen geschult und das CMS solle regelmäßig überprüft werden. International wachse der Konsens über Bedeutung und Inhalte von Leitlinien zu Compliance-Maßnahmen. Der gesetzliche Arbeitsschutz für Managementrisiken stecke in Deutschland also weiterhin im Entwicklungsstadium.

Datenschutz

Rechtsanwältin Petra Menge behandelt in der Ausgabe 3-2016 von s+s report, S. 28–32, die Datenschutzproblematik bei Verwendung einer **Schnittstelle zu anderen Beteiligten einer Sicherungskette** (Sicherheitsdienstleister, Notruf- und Serviceleitstelle, Interventionsstelle, Polizei, Feuerwehr). Kernpunkte seien: Sicherstellung von Zweckbindung, Datenvermeidung und Datensparsamkeit bei der Verarbeitung personenbezogener Daten; Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherheit (§ 9 BDSG); Verpflichtung der Mitarbeiter auf das Datengeheimnis und Sensibilisierung durch entsprechende Schulungen (§ 5 BDSG); Führen eines Verfahrensverzeichnisses; bei Bedarf jederzeitige Auskunft an Betroffene über gespeicherte Daten (§ 19 BDSG). Für die Beteiligten der Sicherungskette gebe es zwei wichtige Lösungsmöglichkeiten: erstens das Erstellen eines Datenschutzkonzepts und zweitens sparsamer Umgang mit der Datenerhebung. Zusätzliche Absicherung biete die Einführung eines Datenschutzmanagementsystems.

Datensicherheit

Heise.de weist am 2. September darauf hin, dass Opfer von **Identitätsdiebstahl im Internet** sich bei der Schufa ab sofort gegen weiteren Missbrauch ihrer persönlichen Daten schützen könnten. Die Auskunftei habe dazu eine Datenbank eingeführt, in der entsprechende Merkmale gespeichert werden. Zudem werde die persönliche Schufa-Auskunft um das Verbrauchermerkmal „Identitätsopfer" erweitert. Betroffene sollten damit vor Wiederholungsfällen geschützt werden. Grund für diesen Schritt bilde nach einem Bericht der WirtschaftsWoche die stark steigende Zahl solcher Fälle: Vier von fünf Online-Händler hätten es demzu-

folge schon mit Betrügern zu tun gehabt. In mehr als der Hälfte der Fälle nutzten die Kriminellen dafür eine fremde oder falsche Identität. Opfer von Identitätsmissbrauch sollten zunächst eine Anzeige bei der Polizei erstatten. Eine Kopie dieser Anzeige könne dann zusammen mit den Kopien der Ausweise und einem entsprechenden Formular, das auf der Schufa-Homepage heruntergeladen werden kann, eingereicht werden.

Drohnen

Knapp fünf Mio. Drohnen sollen bis 2020 von Hobbysportlern geflogen und in Unternehmen eingesetzt werden, berichtet die FAZ am 14. September. Damit rechne die Allianz Global Corporate & Specialty nach einer Studie, welche die Industrieversichertensparte veröffentlicht habe. Der globale Markt für „**Drohnenversicherungen**" werde in zehn Jahren ein Volumen von einer Milliarde Dollar erreichen. Neben einer Pilotenausbildung empfiehlt die Allianz der Politik, auch eine Pflicht zur Registrierung von Drohnen einzuführen. Bundesverkehrsminister Dobrindt habe schon angekündigt, dass die Kennzeichnungspflicht für Drohnen kommen werde. In Deutschland müssen Drohnen sowohl für den privaten als auch für den gewerblichen Einsatz bereits versichert werden. In der Wirtschaft würden Drohnen noch überwiegend im Baugewerbe für Inspektionen, in der Agrarwirtschaft zur Kontrolle des Anbaus und im Tourismussektor zu Marketingzwecken eingesetzt. In Kriegsgebieten könnten Drohnen bald schon eingeschlossene Zivilisten mit Medizin und Blutkonserven versorgen. Mit Gesichtserkennungssoftware könnten sie entlang den Grenzen von Hoheitsgebieten nach Schmugglern und Terrorverdächtigen fahnden.

Der Gesetzgeber müsse eine Grundsatzentscheidung zum Drohneneinsatz fällen, betont Professor Dr. Martin Maslaton, Fachanwalt, in der September-Ausgabe des Behörden Spiegel. Marktforscher prognostizierten für das Jahr 2021 einen weltweiten Markt allein für die Hardware der Drohnen von zwölf Milliarden US-Dollar. Nach geltendem Luftfahrtrecht müsste jeder einzelne Flug von der Behörde genehmigt werden. Hier drohe eine Überregulierung, die den Markt und die technische Entwicklung in Deutschland frühzeitig abschnüren könnte. Das BMVI habe neue Regelungen für Drohnenflüge angekündigt. Erlaubt seien in Deutschland heute eigentlich nur Flüge mit Sichtkontrolle. Das BMVI wolle ermöglichen, dass gewerbliche Drohnen künftig auch außerhalb der Sichtweite ihres Piloten operieren dürfen. Voraussetzung soll dann der Nachweis eines sicheren Betriebs und einer automatischen Landung sein. Auch die Führerscheinpflicht, die Versicherung und die Kennzeichnung von Drohnen sollten geregelt werden. Nur wenn der Einsatz von Drohnen einfach und unbürokratisch erfolgen kann, habe die Weiterentwicklung der Hardware und der Dienstleistungen in Deutschland eine Chance.

Einbruchmeldeanlagen

Wolfgang Wüst, BSG-Wüst GmbH, stellt in Ausgabe 3-2016 des DSD, S. 3–5, die Frage nach einem Anstieg bei den Überwindungsversuchen von **Passiv-Infrarot-Bewegungsmeldern** (PIR-BWM). Diskutiert werde das Phänomen der Überwindung solcher Melder durch ganz unterschiedliche Vorgehensweisen der Täter. Es gebe sogar aktuelle Warnhinweise aus der Versicherungswirtschaft, dass sich ganze Tätergruppen darauf spezialisiert hätten. Um einen funktionsfähigen Bewegungsmelder zu konstruieren, werde dem pyroelektrischen Element des Sensors, der Wärmestrahlung misst, ein mehr oder weniger komplexes, infrarot durchlässiges Spiegelsystem vorgebaut, das den Überwachungsbereich fächerförmig in Sektoren einteile. Um beispielsweise durch den Betrieb von Heizungen, die sich allmählich

erwärmen, keine unerwünschten Auslösungen zu bekommen, sei zur sicheren Detektion eine Mindestgeschwindigkeit der sich bewegenden Personen erforderlich. Durch sehr langsames Bewegen könne ein Täter sich der Detektion entziehen. Die Physik der PIR-BWM sei nicht neu. Eine EMA, die ausschließlich auf diese Melder setze, sei mit Vorsicht zu genießen. Juristisch von nicht zu unterschätzender Bedeutung sei die in der EN 50131 geforderte Risiko-Analyse des Schutzobjektes durch den Facherrichter. Setzt der Errichter ausschließlich auf relativ wenige PIR-BWM und verzichtet auf andere Sensorik, gehe er ein schwer kalkulierbares Risiko für sich selbst und für seinen Kunden ein. Durch den Einsatz ganz unterschiedlicher Sensoren und/oder durch Bewegungsmelder, die sich gegenseitig überwachen, könne dieses Risiko bereits nachhaltig reduziert werden.

Dipl.-Ing. Güner Grundmann thematisiert in der Ausgabe 3-2016 der Zeitschrift s+s report, S. 40–42, die **Nutzung von IT-Netzen in Einbruchmeldeanlagen** (EMA). Ausgehend von EMA mit konventioneller oder busbasierter Technik ergäben sich grundlegende Anforderungen an die Weiterleitung von Meldungen: Es dürften keine Meldungen verloren gehen und Meldungen dürften nicht länger als zehn Sekunden zur Weiterleitung und Verarbeitung benötigen. Der Autor erläutert notwendige Anforderungen, die sowohl für die Planung und Errichtung als auch für die entsprechenden Produkte gelten: strukturierte Verkabelung; Sabotagesicherheit der Verteilerräume; überwachte und messbare Verfügbarkeit; Vertraulichkeit und Authentizität; eigene Produktkategorie als gerätetechnische Umsetzung; Notstromkonzept. Mit dem Entwurf entsprechender Richtlinien (VdS 3147 und 3106) schaffe VdS die Basis für deren Integration.

Einzelhandelssicherheit

Dipl.-Phys. Bertrand Völckers, FLIR Commercial Vision Systems, und Frank Liebelt, Journalist, stellen in der Ausgabe 9-2016 der Zeitschrift GIT, S. 122/122, Wärmebildkameras von Flir als neue Waffe im Kampf gegen Ladendiebstahl vor. Die **Diebstahlschutzlösung xPredator** verwende eine Wärmebildkamera von FLIR und die intelligente visuelle Wärmebildverfolgungssoftware Thermal Visual Tracking, die zum gezielten Aufspüren von Waren entwickelt worden sei, die mit Diebstahlsabsicht unter der Kleidung versteckt wurden. Mit dem berührungsfreien Modus von xPredator lasse sich sofort erkennen, was sich unter der Kleidung verbirgt. Der Anwender könne alle Bereiche kontrollieren, die seine nähere Aufmerksamkeit erfordern, die jeweilige Situation komplett überwachen und gegebenenfalls sofort geeignete Maßnahmen einleiten. Nach Angaben des italienischen Entwicklungsunternehmens Sefitalia könne die Diebstahlsquote bis zu 60 Prozent reduziert werden.

Das niederländische Unternehmen Hikvision präsentiert in der Ausgabe 9-2016 der Zeitschrift GIT, S. 146/147 eine **anwenderfreundliche Videomanagement-Lösung** für den Einzelhandel. Das System Blazer Express sei für kleine bis mittlere Einzelhandelsanwendungen konzipiert und unterstütze eine nahtlose Integration mit vorhandenen POS-Systemen. POS-Transaktionsdaten würden mit den relevanten Videoaufnahmen assoziiert, was die Identifizierung und Prüfung verdächtiger Transaktionen unterstütze und Beweismaterial für Streitfälle mit Kunden liefere. Blazer Express IVMS-Stationen könnten an diversen Standorten installiert werden. Der Kaskadenmodus ermögliche zentralisiertes Videomanagement. Im Multi-Standort-Modus gestattet Blazer Express den Zugriff auf Video- und Alarminformationen aus Filialen an anderen Standorten. Das System könne problemlos erweitert werden. Selbst die Integration von Fremdsystemen sei möglich.

Endgerätesicherheit

Roland Hunkeler, Siemens Building Technologies, behandelt in der Fachzeitschrift Sicherheitsforum, Ausgabe 4-2016, S. 32/33, Vorteile der Verwendung mobiler Endgeräte, auch im professionellen Umfeld. Die hohe Gebrauchstauglichkeit von Tablets und Smartphones im privaten Umfeld werde im professionellen Umfeld zunehmend eingefordert. Usability sei in der Sicherheitsbranche zu einem wichtigen Differenzierungsmerkmal geworden. Eine optimale Ergonomie und die damit einhergehende intuitive Bedienung spielten gerade im Sicherheitsbereich eine wichtige Rolle. Denn dann seien auch in komplexen Einsatzlagen eine stressfreie Bedienung und schnelle Reaktionszeiten möglich. Durch die intuitive Bedienung verkürzten sich die Schulungsdauer und Einarbeitungszeiten der Operatoren.

Erdbebensicherheit

Mit Ideen zur Erdbebensicherheit von Gebäuden – von „einfach aber clever" bis „Hightech" – befasst sich die WirtschaftsWoche vom 2. September. Weltweit seien allein zwischen 2000 und 2012 mehr als 800.000 Menschen bei Erdstößen gestorben. Dass allzu oft selbst als sicher eingestufte Häuser zu Todesfallen werden, liege an einer schlampig umgesetzten Erdbebensicherung oder tödlichen Konstruktionsfehlern. Als Sicherungsmöglichkeiten werden beschrieben: Metallkugel als Schwingungstilger, stabile Pfeiler, Karbonseile, Leichtbau, Strohwände, verstärkte Wände, Kunststoffnetze, kleine Fenster, Luftkissen, starre Rahmen und Stahlrahmen als Stoßdämpfer.

Evakuierung

Ein Arbeitskreis des ZVEI-Fachverbands Sicherheit hat das **Merkblatt „Adaptive Fluchtweglenkung"** fertiggestellt, meldet GIT in der Ausgabe 9-2016, S. 138. Die 58-seitige Broschüre erläutere ausführlich den erreichten Stand auf dem Gebiet der dynamischen Fluchtweglenkung. Kern der adaptiven Fluchtweglenkung sei eine kontinuierliche Gefahrenerkennung in Fluchtwegen und damit das permanente Umsteuern der dynamischen Rettungszeichenleuchten. Das Merkblatt solle über grundsätzliche technische Möglichkeiten informieren und Handlungsbedarf in Technologie, Forschung, Normung und Anwendung aufzeigen. Dynamische Fluchtwegleitsysteme seien bereits seit längerer Zeit erfolgreich im Einsatz. Sie seien mit einer BMA gekoppelt und würden deren Informationen auswerten. Das Merkblatt könne kostenlos heruntergeladen oder als gedruckte Broschüre bestellt werden.

Extremismus

Eine neue Broschüre des Bundesamtes für Verfassungsschutz (BfV) für Personen und Organisationen, die sich in der Flüchtlingshilfe professionell engagieren, macht auf potenzielle Berührungspunkte zu extremistischen und geheimdienstlichen Aktivitäten aufmerksam. Werbungsversuche in oder im Umfeld von Flüchtlingsunterkünften seien zu beobachten. Die Broschüre, die als PDF-Datei heruntergeladen werden kann, behandelt islamistische, ausländerextremistische, rechts- und linksextremistische sowie geheimdienstliche Aktivitäten fremder Staaten mit Flüchtlingsbezug.

Das BKA berichtet in der Wochenlage am 17. September, dass Unbekannte am 8. August sieben Dienstfahrzeuge der Bundespolizei und mindestens **zehn Fahrzeuge der Deutschen Bahn** bzw. Privatfahrzeuge

in Brand gesetzt haben. Die Pkw seien auf einem nicht videoüberwachten Parkplatz am Hauptbahnhof Magdeburg abgestellt gewesen. 750.000 Euro Sachschaden sei entstanden. Auf der linksgerichteten Internetseite „linksunten" hätten Unbekannte tags darauf ein Selbstbezichtigungsschreiben zur Tat veröffentlicht und dabei hauptsächlich die Polizei Magdeburg kritisiert.

Gefahrenmeldeanlagen

Martin Häußler, ITENOS GmbH, zeigt in der Ausgabe 3-2016 der Zeitschrift s+s report, S. 36/37, wie sich der **Umstieg auf All-IP** für Unternehmen der Sicherheitsbranche meistern lässt. Die Ablösung sei Teil eines Prozesses, an dessen Ende die Regentschaft eines einzigen Netzes, nämlich des IP-basierten „Next Generation Networks" (NGN) stehe. Für die verschiedenen Übertragungsklassen würden künftig feste Rahmenvorgaben bezüglich Verfügbarkeit, Laufzeit und anderer Betriebsparameter definiert. ITENOS habe sich auf sichere Übertragungswege spezialisiert und stehe Security-Dienstleistern beim Umstieg von Datex-P auf IP-Technik bei Bedarf zur Seite. Sie biete komplette Servicepakete an. Basis sei stets die eigenentwickelte Plattform „ProtectService", auf der alle Kundenlösungen aufgebaut seien.

Geldautomatensicherheit

Carsten Roll, GDV, äußert sich in s+s report, Ausgabe 3-2016, S. 44/45, zur Neuauflage der Richtlinien zur Sicherung von GA (VdS 5052). Im Ergebnis seien die Inhalte der Richtlinie an neue Tätermethoden und -techniken angepasst worden. In der Richtlinie würden die Risiken durch Angriffe auf GA beschrieben sowie Empfehlungen zur Absicherung gegeben. Nur die Kombination verschiedener technischer, organisatorischer und baulicher Maßnahmen könne die Gefährdung signifikant reduzieren und den Angriff mit unterschiedlicher Tatbegehungsweise erheblich erschweren. Neben der aktuellen Empfehlung, dass die Sicherheitsstufe der in GA eingesetzten Wertbehältnisse mindestens dem Widerstandsgrad IV gemäß VdS 2450 bzw. EN 1143-1 mit dem Zusatz „EX GAS" entsprechen sollte, gehörten Standortauswahl, die Einbausituation und die bauliche und technische Ausstattung vor Ort zu den wesentlichen Sicherheitsfaktoren.

Hagelschutzsystem

Chefredakteur Roger Strässle thematisiert in Ausgabe 4-2016 der Zeitschrift Sicherheitsforum (S. 19–21) das Hagelschutzsystem. Rund 200.000 Schadensfälle der letzten zehn Jahre habe die Assekuranz rund 640 Mio. Franken gekostet. Praktisch die Hälfte (320 Mio. Franken) sei auf Hagelereignisse entfallen. Die Kantonalen Gebäudeversicherungen hätten deshalb zusammen mit Partnern das System „Hagelschutz – einfach automatisch" entwickelt. Drohe akutes Hagelgewitter in einer bestimmten Region, sende SFR Meteo ein Signal an die gefährdeten und mit dem Hagelschutzsystem ausgestatten Liegenschaften. Zum Zug komme das Hagelschutzsystem vorwiegend in Gebäuden mit elektrischen Storen und insbesondere auch dort, wo übers Wochenende niemand anwesend sei. Das reiche von Schulhäusern über größere Geschäfts- und Bürogebäude bis hin zum Industriebau.

Hochwasser und Starkregen

Risikovorsorge gegen Starkregen und Hochwasser thematisiert Alexander Küsel, GDV, in s+s report, Ausgabe 3-2016, S. 58/59. Allein die Starkregenereignisse im Mai/Juni

2016 hätten versicherte Schäden von rund 1,2 Mrd. Euro verursacht. Noch nie hätten Unwetter mit heftigen Regenfällen innerhalb so kurzer Zeit so hohe Schäden verursacht. Bundesweit schützten sich derzeit nur rund 40 Prozent der Hausbesitzer gegen Elementarschäden, obwohl mehr als 99 Prozent aller Gebäude problemlos gegen Hochwasser oder Starkregen versicherbar seien. Der Autor erläutert, was die **Elementarschadenversicherung** leistet und dass man mit „ZÜRS Geo" Überschwemmungsrisiken richtig kalkulieren könne. Schutz böten Sicherungssysteme und wasserresistente Baumaterialien. Außerdem sollte ein eventuell vorhandener Öltank besonders geschützt werden. In stark gefährdeten Gebieten könnten Schutzmaßnahmen wie die Ausstattung von Kellerfenstern, Türen und Lichtschächten mit Sicherungssystemen, das Fliesen gefährdeter Räume und die Aufbewahrung von Wertgegenständen und elektrischen Geräten in oberen Stockwerken das Schadeneintrittsrisiko und das Schadensausmaß vermindern.

Hotelsicherheit

Am Beispiel des Maritim in Dresden befasst sich VdS Schadensverhütung mit dem Brandschutz im Hotel (GIT, Ausgabe 9-2016, S. 50–54). In dem Hotel seien in jedem Zimmer mindestens zwei Melder installiert, einer im Raum selbst und einer im Flur. Beide Melder seien mit einer direkten Verbindung zu der an der Rezeption installierten BMA ausgestattet. Außerdem verfügten sie über eine Voralarmierung. **Der gesamte Hotelbereich sei „gesprinklert**". Die Garderobe sei eine Gefahrenquelle, die oft übersehen werde. Bei Veranstaltungen von mehreren tausend Leuten sammle sich dort eine enorme Brandlast an. Wasserdampf sei eine besondere Herausforderung für Rauchmelder, da der wie Brandrauch aus großen, gut sichtbaren Partikeln besteht. Moderne BMA könnten aufgrund der Auswertung der Signale verschiedener Streulichtwinkel mittlerweile zwischen den sehr großen Wasserdampfpartikeln und den etwas kleineren Brandrauchaerosolen unterscheiden. Löse ein Rauchmelder in einem der 328 Zimmer aus, so könne die Ursache innerhalb von maximal 180 Sekunden durch die Hotel-Mitarbeiter erkundet werden. Werde der Feueralarm allerdings nicht innerhalb der ersten 30 Sekunden quittiert, dann werde automatisch die im System hinterlegte Brandfallsteuerung abgespult. Die Sprinkler-und Sprühwasseranlage besitze eine eigene Wasserversorgung (WV) mit zwei unabhängigen Systemen (WV der dritten Art), die auch beim Ausfall eines Systems sofort mit der Brandbekämpfung beginnen könnten. Zusätzlich zu Sprinklern seien BMA vor allem bei Schwelbränden, also Bränden mit niedriger Temperatur, wie sie gerade durch Elektrogeräte häufig ausgelöst würden, sinnvoll. Da reagierten Sprinkler naturgemäß erst einmal nicht, weil sie offenes Feuer brauchen. Der maximale Fluchtweg bis zu einem sicheren Treppenhaus bzw. ins Freie betrage 15 Meter, unabhängig davon, wo Gäste und Angestellte sich befinden. Sehr hilfreich sei die automatische Sprachalarmierung. Alles an Sicherheitstechnik im Hotel sei automatisiert, auch die Evakuierung. Die Küche werde mit Sprinklern geschützt. Die Friteuse und der Herdbereich dagegen verfügten natürlich über eine automatische Fettbrand-Löschanlage, die in der Abzugshaube integriert ist und bei Bedarf auch manuell ausgelöst werden könne. Einen Fettbrand dürfe man keinesfalls mit Wasser löschen.

Internet der Dinge (IoT)

Silikon.de weist am 19. September auf eine Studie von Vodafone hin, nach deren Ergebnis immer mehr Anwender überzeugt davon sind, mit vernetzten Geräten und dem IoT wirtschaftliche Erfolge feiern zu können. Die Ausgabe für vernetzte Technologien liege noch vor Cloud und Hosting, Analytics und Mobility auf dem ersten Rang. 63 Prozent der

Unternehmen weltweit sähen die Investitionen in IoT als lohnend an und meldeten einen signifikanten Return on Investment. 53 Prozent der Unternehmen in Deutschland seien dabei, IoT-Projekte umzusetzen oder zu planen. Der Schwerpunkt scheine in der Auswertung der Daten zu liegen. Auf diese Weise würden Unternehmen in Echtzeit Handlungsempfehlungen bekommen, könnten System- und Materialfehler vorhersagen und den Verschleiß von Bauteilen berechnen. 67 Prozent der befragten deutschen Unternehmen hätten angegeben, dass auch die Mitarbeiter dem Thema aufgeschlossen gegenüberstehen. 87 Prozent der deutschen Unternehmen legten auch großen Wert darauf, IoT-Securityprozesse selbst zu managen. Weltweit liege der Wert bei 69 Prozent.

IT-Sicherheit

<kes>info fasst am 8. September die Antworten von 15 Experten zur aktuellen Lage sowie zu den weiteren Aussichten bei einer Befragung des BSI, von Beratern, Verbänden und Anbietern zusammen. Die häufigste Antwort auf die Frage nach der derzeit größten Bedrohung in Sachen Malware lautete: **Ransomware**. In einer **Umfrage der Allianz für Cybersicherheit** im Frühjahr 2016 hätte rund ein Drittel aller befragten Institutionen angegeben, in den letzten sechs Monaten von Ransomware betroffen gewesen zu sein. Hätten ursprünglich Privat- und Einzelanwender den größten Teil der Infektionen ausgemacht, seien zunehmend Unternehmen zum Ziel geworden – häufig KMU, bei denen Schutzverfahren nicht oder nicht stark genug implementiert gewesen seien. Für neue Viren-Varianten müssten neue heuristische Erkennungen erstellt werden, da reine Dateisignaturen nutzlos seien. Und auch Unternehmen müssten ihr Sicherheitskonzept erweitern. In Unternehmen sehe man sich bedroht von Spionageangriffen und ferngesteuerter Manipulation von Anlagen.

Nach Überzeugung von Holger Suhl, Kaspersky Lab, steige die Bedrohung durch Malware, weil im Zuge des Internets der Dinge beziehungsweise der Industrie 4.0 immer mehr Angriffsflächen entstünden. Alles werde vernetzt und smart und daher angreifbar. Eine große Bedrohung bildeten zudem weiterhin die Advanced Persistant Threats (ATP). APT-Angriffe zeichneten sich durch großen personellen, finanziellen und technischen Aufwand aus. Erstaunlicherweise würden die IT-Abteilung und vor allem IT-Sicherheit noch immer oft negativ wahrgenommen – als Kostenträger und Prozessbremse. Die IT bilde jedoch das Rückgrat fast aller Unternehmen. Bei einem Ausfall könnten ganze Produktionen zum Erliegen kommen. Malware werde inzwischen oft individuell entwickelt, erzeugt oder automatisch so häufig variiert, dass Antiviren-Lösungen keine Signaturen für die neuen Objekte haben und der Kunde somit nicht mehr geschützt sei. Stefan Strobel, cirosec, sieht den derzeit größten Handlungsbedarf in der Erstellung eines neuen Malwareschutzkonzepts. Olaf Niemeitz, Crocodial, zeigt sich überzeugt, dass viele Unternehmen keine echte Security-Strategie hätten, weil sie zu stark auf ihr operatives Geschäft fokussiert seien. Ihnen fehle ein zuverlässiges Information-Security-Management, ein Gesamtkonzept, das Regeln, Verfahren und Verantwortlichkeiten für den Ernstfall definiere. Thomas Hemker, Symantec, lege Wert auf ein integriertes Risikomanagement als Grundlage eines systematischen Schutzes. Für das BSI gehöre zum Gesamtkonzept IT-Sicherheit auch, dass Cybersicherheit als Managementthema begriffen wird. Sehr häufig würden in Unternehmen bewusst Security-Basics vernachlässigt, weil diese angeblich das Arbeiten der Anwender beeinträchtigen. Dazu zähle beispielsweise, dass Mitarbeiter sichere Passwörter verwenden und Sticks anschließen dürfen und generell nur auf diejenigen Programme und Daten zugreifen können, die sie für die Erfüllung ihrer Aufgaben benötigen. Bei den Techniken zur Abwehr finde ein grundlegender Technologiewandel statt.

Moderne Isolationsverfahren würden die Prävention stark verbessern und neue Produkte zur Verhaltenserkennung auf dem Endgerät werden die Erkennung von bisher unbekannter Malware auf ein neues Niveau bringen. Alexander Vuksevic, Avira, sehe neben einem Echtzeitschutz gegen Malware auf Cloud-Basis vor allem Chancen in der künstlichen Intelligenz. Immer wichtiger werde Security by Design. Über das Web verbundene Geräte sollten auch selbst in der Lage sein, Anomalien zu entdecken und dementsprechend zu reagieren. Professionalität und Intensität von Attacken würden weiter zunehmen. Einer der Gründe dafür sei das Auftauchen von Nationalstaaten als Cyberangreifer. Bestrebungen von Regierungen, Sicherheitsmechanismen wie Verschlüsselung für ihre Überwachungsbemühungen zu schwächen, verschlimmerten die Lage weiter. Aus Sicht des BSI sei es eine wichtige Entwicklung, dass Cybersicherheit immer mehr in den Köpfen der Menschen verankert wird. In den Vorstandsetagen werde Cybersicherheit nicht mehr als Fachthema verstanden, sondern zunehmend als Chefsache. Auf die Frage nach den besten Tipps zur Abwehr von Ransomware seien folgende drei „Top-Tipps" von jeweils rund zwei Dritteln der Experten genannt: Backup, Backup, Backup; Schulung und Sensibilisierung, Patches und Updates. Mehrere Experten rieten zu einer Verringerung der Angriffsfläche durch Vermeiden riskanter Software wie Flash oder Java, der Deaktivierung von Office-Makros und Skriptdateien, einer möglichst weitgehenden Beschränkung von Nutzerrechten sowie eventuell der Installation eines Ad-Blockers im Browser.

Die FAZ berichtet am 16. September über ein EuGH-Urteil, nach dem derjenige, der öffentliche **Funknetze** zugänglich macht, die Nutzer identifizieren muss. Man könne zwar Dritten einen WLAN-Zugang eröffnen, ohne Abmahnungen durch Anwälte zu befürchten. Allerdings habe sich das Gericht auch für Passwortschutz und die Identifizierung der Nutzer ausgesprochen. Demnach haftet, wer einen Internetanschluss über WLAN anbietet, zwar nicht auf Schadensersatz und müsse auch keine Anwaltskosten begleichen, wenn etwa die Musikindustrie klagt. Allerdings könne der Betreiber nach Ansicht der Richter verpflichtet werden, die Identität der Nutzer abzufragen und den Zugang durch ein Passwort zu schützen.

Heise.de meldet am 14. September, Microsoft warne vor einer Sicherheitslücke in seinem quelloffenen **Web-Application-Framework ASP.NET Core**. Entwickler, die bestimmte Module in ihren Projekten einsetzen, machten diese angreifbar, da der Software ein falscher Nutzer vorgespielt werde, was dazu führe, dass der Angreifer Nutzerrechte unter Umständen dramatisch auszuweiten vermag. In einer Sicherheitsmeldung erkläre Microsoft das Problem und zeige, wie Entwickler die Lücke schließen können. Microsoft empfehle, das Update „Microsoft.NET Core 1.0.1 – VS 2015 Tooling Preview 2" einzuspielen, um verwundbare Versionen der Modelle loszuwerden.

Frank Cerminara, InfoGuard AG, befasst sich in der Ausgabe 4-2016 der Zeitschrift Sicherheitsforum, S. 23–25, mit Cyberangriffen als Service aus dem Darknet. Das Internet sei zu einem digitalen Schlachtfeld geworden, auf dem immer professioneller Daten gestohlen werden. Dazu trage sicher auch das Darknet mit seinen Shops für Cyberangriffe bei. Um dieser steigenden Bedrohung zu begegnen, müsse ein Umdenken in der IT-Sicherheit stattfinden. Man müsse wie ein Angreifer denken. Beim gezielten und komplexen Angriff (Advanced Persistent Threat, APT) würden systematisch Daten über aufkeimende Bedrohungen und Trends gesammelt, gefiltert, analysiert und korreliert, um daraus nützliche Informationen abzuleiten und mit den Angreifern stets Schritt zu halten. Denn nur wer seine Gegner im Detail kenne, könne aus einer fundierten Informationsposition heraus agieren. **Cyber Threat Intelligence** sei ein anspruchsvolles Aufgabenfeld und

bleibe leider bei vielen Unternehmen durch den Businessalltag auf der Strecke. Abhilfe schafften da professionelle Services.

Das betriebseigene Fertigungssystem **Slat Production System** (SPS) stellt Frauke Petzold, Slat GmbH, in der Ausgabe 9-2016 der Fachzeitschrift GIT, S. 172/173, vor. Seit einigen Jahren arbeite man bei Slat nach der japanischen Kaizen-Methode, welche Führungskräfte und Mitarbeiter in das innerbetriebliche Managementsystem einbeziehe und sich einem kontinuierlichen Optimierungsprozess verschrieben habe.
Eine speicherprogrammierte Steuerung und die Bereitstellung interner Programme zur Betriebskontinuität im Störfall gewährleisteten optimale Produktivität und fristgerechte Lieferungen. Darüber hinaus würden die Produkte regelmäßigen Kontrollen unterzogen. Anfang 2016 sei das Unternehmen mit einer neuen Produktgeneration auf den Markt gekommen: Safe DC. Es diene der Sicherung der verteilten Intelligenz innerhalb des Gebäudes. Es handele sich um Mikro-Energiequellen, die in unmittelbarer Nähe von anwendungsbezogenen Steuer- und Messgeräten installiert würden. Ihre Aufgabe sei es, die gesamte Steuerungs- und Kommunikationskette abzusichern, ohne die ein störungsfreier Betrieb des intelligenten Gebäudes nicht möglich sei.

Mit Wirkung zum 15. Juni 2016 sei in Straßburg die **European Cyber Security Organisation** (ECSO) gegründet worden. Ziel sei es, Unternehmen im EU-Binnenmarkt besser vor Cyberangriffen zu schützen, den europäischen IT-Sicherheitsmarkt sowie eine konkurrenzfähige, leistungsstarke IKT-Industrie weiter auszubauen, den Einsatz vertrauensvoller und innovativer EU-Lösungen zum Schutz wettbewerbsfähiger und kritischer Infrastrukturen zu fördern, die Forschung zu fördern und eine europäische „Cybersecurity Industrial Policy" zu entwickeln und zu implementieren.

Der Behörden Spiegel plädiert in der September-Ausgabe für die **Funktion Passwortmanager**. Dies sei eine Möglichkeit, sämtliche Accounts, die man nutzt, mit einzigartigen und sicheren Passwörtern auszustatten.
Die Basis eines Kennwort-Managers sei das sogenannte Hauptpasswort. Die meisten Passwortmanager arbeiteten mit starken Verschlüsselungsalgorithmen und verschlüsselten nicht nur die zu verwaltenden Kennwörter, sondern auch die jeweiligen Datenbanken, zu denen die einzelnen Kennwörter den Zugriff ermöglichen. Gegenüber einem offline genutzten Passwortmanagement, was z. B. mittels handschriftlichen Listen praktiziert wird, habe eine sich auf dem Desktop befindende Datei mehrere Vorteile. Die verwalteten Kennwörter könnten bequem per Copy and Paste eingegeben werden und müssten nicht jedesmal manuell eingetippt werden.

IuK-Kriminalität

Zeit-online berichtet am 6. September, das BSI warne vor einer hohen Zahl an Cyberangriffen auf deutsche Behörden und Unternehmen. Allein der VW-Konzern gebe die Zahl der Cyberattacken auf sein IT-Netz mit 6.000 Fällen pro Tag an. BSI-Präsident Schönbohm plädiere für eine konsequente Abwehr. Die Cyberattacken hätten sich im Laufe der Zeit stark verändert. Bis vor wenigen Jahren hätten Cyberangriffe einem elektronischen Flächen-Bombardement geglichen. Dadurch hätten Angreifer große Streuverluste gehabt. Heute seien **Cyberattacken sehr viel präziser** und auf einzelne Ziele angelegt.

Swift ergreift Maßnahmen gegen **Hackerangriffe auf Banken**, titelt die FAZ am 21. September. Das Zahlungsverkehrssystem Swift, dem 11.000 Banken aus 200 Ländern angeschlossen sind und das für internationale Überweisungen eine Monopolstellung einnehme, werde den Banken über einen unabhängigen Kanal tägliche Berichte über

ihre Swift-Aktivitäten bereitstellen. Damit solle sichergestellt werden, dass den Instituten ungewöhnliche Zahlungsvorgänge sofort auffallen und sie rechtzeitig dagegen steuern können. Aber auch die Zentralbanken seien alarmiert. Ein Fachausschuss der Bank der Zentralbanken (Bank für Internationalen Zahlungsausgleich – BIZ) habe eine Spezialeinheit gegründet, um die großen Zahlungsverkehrssysteme zu überprüfen. Täglich würden über Swift 25 Mio. Meldungen zwischen den Banken verschickt, auf denen dann die internationalen Überweisungen beruhen. Sollte irgendwann das Vertrauen in Swift verloren gehen, fiele für die Banken das wichtigste und bislang einzige Zahlungsverkehrsnetzwerk weg. Swift werde den Banken erstmals die Tagesberichte zur Verfügung stellen. Diese würden aus einem Aktivitätenprotokoll und einem Risikoprotokoll bestehen. Das Risikoprotokoll solle auf ungewöhnliche und große Transaktionen aufmerksam machen, damit Betrugsfälle schneller erkannt werden könnten.

Der Behörden Spiegel weist in der September-Ausgabe darauf hin, dass das BSI seit 2012 alle zwei Jahre ein Dokument mit dem Titel „**Industrial Control System Security**" herausgibt, in dem auf die zehn größten IT-Bedrohungen für industrielle IT-Systeme eingegangen wird. Um sich vor Angriffen durch Phishing und Social Engineering zu schützen, halte es das BSI für ratsam, zielgerichtete Awareness-Kampagnen durchzuführen, Datenträger und auch Papier sicher zu entsorgen sowie ein Datensicherungskonzept zu erarbeiten. Im Industrieumfeld vorhandene IT-Standardkomponenten wie Betriebssysteme, Application Server oder Datenbanken würden häufig Fehler und Schwachstellen enthalten, die von Angreifern ausgenutzt werden könnten. Bei Angriffen auf Authentisierungsmechanismen würden automatisiert tausende Kombinationen eingegeben, um Kennwörter zu knacken. Auch Netzwerkkomponenten wie Router oder Firewalls könnten nach einer ersten erfolgreichen Attacke durch Angreifer manipuliert werden, um Sicherheitsmechanismen außer Kraft zu setzen oder den Datenverkehr umzuleiten. Das BSI appelliere an die Unternehmen, die Verantwortlichkeit für IT-Sicherheit auf Vorstandsebene anzusiedeln. Desweiteren rate das BSI dazu, die jeweiligen Industrial Control Systeme in ein umfassendes Informationssicherheits-Managementsystem (ISMS) einzubringen, durch das die gesamte IT im jeweiligen Unternehmen erfasst werden könne. Das Dokument „Industrial Control System Security" könne auf der Homepage des BSI heruntergeladen werden.

Bislang habe es keinen größeren Hackerangriff gegeben, dem terroristische Motive zugrunde gelegen haben, stellt der Behörden Spiegel in der September-Ausgabe fest. Dies habe vielfältige Ursachen. Die wichtigste sei, dass global agierende terroristische Gruppierungen wie der sogenannte Islamische Staat (IS) dazu schlichtweg nicht in der Lage seien. Außer für professionelle Propaganda nutze der IS das Internet mangels vorhandener Hacker-Fertigkeiten nicht. Die Bundesregierung verwende eine sehr weite Definition des Begriffs **Cyber-Terrorismus**. Laut BMI fielen sämtliche Angriffe auf kritische Infrastrukturen hierunter. Auch Cyberangriffe, mit denen die Wirtschaft nachhaltig geschwächt werden soll, seien für das BMI Cyber-Terrorismus.

Der Cyberabwehr des Bundesamtes für Verfassungsschutz (BfV) liegen nach einer Warnmeldung vom 22. September Erkenntnisse zu einem versuchten Cyberangriff der **Angreifergruppierung APT 28** auf ein deutsches Medienunternehmen vor. Der Angriff sei über eine Spear-Phishing-Mail mit einem darin enthaltenen Link zu einer mit Schadcode infizierten Seite erfolgt. Der gefälschte Absender lautete heinrich.krammer@hg.nato.int. Bei einem der Angriffe sei statt eines schadhaften Links ein „maliziöses" Office-Dokument als Anlage verwendet worden. Viele der von den Akteuren der APT-28-Kampagne versandten Spear-Phishing-Mails nähmen Bezug auf ein aktuelles tagespolitisches Ereignis. Das Opfer werde in diesen E-Mails

aufgefordert, für weiterführende Informationen einen maliziösen Link anzuklicken oder ein schadhaftes Office-Dokument zu öffnen. Klickt das Opfer auf den Link, werde es auf eine legitime Nachrichtenseite weitergeleitet, während sich im Hintergrund die Schadsoftware automatisch auf seinem Rechner installiert. Es werde empfohlen, eine Überprüfung der E-Mail-Postfächer nach der oben genannten Absenderadresse vorzunehmen. Die Kampagne APT 28 stelle derzeit eine der aktivsten und aggressivsten Cyberspionageoperationen im virtuellen Raum dar. Bei dieser Kampagne bestünden Indizien für eine Steuerung durch staatliche Stellen Russlands.

Kommunikationssicherheit

Die Ära der herkömmlichen Festnetztelefonie, sprich analog und ISDN, gehe zu Ende, betont Roger Strässle, Chefredakteur der Zeitschrift Sicherheitsforum in der Ausgabe 4-2016, S. 45–47. Sie werde durch das Internet Protokoll abgelöst. Dass der erste digitale Standard ISDN Ende 2017 abgeschaltet wird, habe die Telekombranche schon vor einiger Zeit bekannt gegeben. Von der neuen IP-Technologie seien auch die Alarmierung und der Liftnotruf betroffen. Das einheitliche Transportprotokoll IP bilde die neue Basis der digitalen Kommunikation, sei es für Machine-to-Machine (M2M), für das Internet of Things, Cloud-Lösungen oder andere zukünftige Anwendungen. Für den Betrieb von Sonderanwendungen über das herkömmliche Festnetz hinaus böten sich laut Telekomunternehmen folgende Lösungen an: Weiterverwendung über die analoge Schnittstelle des IP-Routers, Arbeit mit Konverter oder IP-Umstellung auf ein IP-fähiges Gerät. Auch im Aufzugsbereich böte die IP-Technologie Vorteile. Die Verfügbarkeit der Anlagen steige. Durch die digitale Anbindung könnte man permanent Ferndiagnosen durchführen und wesentlich schneller reagieren, wenn die Aufzugsanlage Probleme verursache.

Krisenregionen

Security insight berichtet in der Ausgabe 5-2016, S. 6/7, über eine **Sicherheitspartnerschaft von fünf Dax-Konzernen mit Mexiko**. Gemeinsam mit Vertretern aus Politik und Behörden initiierten Siemens, VW, BASF, Daimler und Bayer eine gemeinsame Plattform. Im Rahmen dieser Public Private Partnership im Bereich der Unternehmenssicherheit solle an Themen wie z. B. der Sicherheit der Standorte, der Mitarbeiter der Supply Chain sowie Frühwarnung und Krisenmanagement gemeinsam gearbeitet werden. In das Programm seien neben den mexikanischen Behörden auch die deutschen Sicherheitsbehörden und die deutsche Botschaft eingebunden. Im Ergebnis sei ein Maßnahmenpaket vereinbart worden, das auf professioneller Basis einen regelmäßigen Austausch und eine enge Zusammenarbeit bei verschiedenen Sicherheitsthemen gewährleistet.

Kritische Infrastrukturen

Akuten Handlungsdruck für Betreiber kritischer Infrastrukturen sieht Dr. Timo Neumann, Bundesdruckerei, in der Ausgabe 5-2016 der Zeitschrift Security insight, S. 28/29. Um einen angemessenen Schutz von Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit erfüllen zu können, empfehle es sich für die Betreiber, ein **Informationssicherheits-Managementsystem (ISMS)** aufzubauen. Vor einer Zertifizierung sollten die Unternehmen das ISMS erfahrungsgemäß mindestens sechs Monate betrieben haben, um für eine mögliche Zertifizierungsprüfung ausreichende Nachweise der Effektivität und Wirksamkeit erbringen zu können. Die sogenannte „Reifegradfeststellung nach ISO 27001" verschaffe dem Unternehmen einen ersten Überblick über anstehende Herausforderungen bei der Implementierung des ISMS. Innerhalb weniger Tage würden

sämtliche Unternehmensbereiche untersucht, die von den Anforderungen betroffen sind. Die Ergebnisse fließen in ein von der Bundesdruckerei entwickeltes Reifegrad-Modell ein, das sich auf die Standards ISO/IEC 27001, ISO/IEC 27002 und die branchenspezifische ISO/IEC TR 27019 stützt. Gleichzeitig zum Aufbau des ISMS sollten gezielt Technologien ergänzt werden, die Unternehmen zukunftssicher machen. Dabei spielten Konzepte für sichere Identitäten die entscheidende Rolle.

Franziska Hain, PricewaterhouseCoopers (PwC), und Manuel Weller, ebenfalls PwC, sehen **Energieversorger im Fokus des IT-Sicherheitsgesetzes** (Security insight, Ausgabe 4-2016, S. 36/37). Ein sicherer Netzbetrieb sei gewährleistet, wenn der von der Bundesnetzagentur entwickelte IT-Sicherheitskatalog eingehalten werde. Dieser fordere die Implementierung eines ISMS nach DIN ISO 27001 und umfasse alle zentralen und dezentralen Anwendungen, Systeme und Komponenten, die für einen sicheren Betrieb des Energieversorgungsnetzes notwendig sind. Die Verantwortung für die Einhaltung des Katalogs liege ausschließlich beim Netzbetreiber, selbst dann, wenn die betreffenden Einrichtungen durch Dritte betrieben werden. Um die organisationale Widerstandsfähigkeit und so die Wirtschaftsfähigkeit nachhaltig zu erhöhen, sei die Integration weiter Managementansätze erforderlich. Die Implementierung eines ganzheitlichen Business Continuity Management Systems (BCMS) biete hierbei eine zielführende Ergänzung des gesetzlich geforderten ISMS. Adressatengerechte Notfallpläne greifen die ausgewählten Strategien auf. Wie eine im Jahr 2012 veröffentlichte Studie von PwC zeige, bestehe jedoch insbesondere im Bereich der Notfallkonzeption dringender Nachholbedarf. Um der steigenden Gefahr von Cyberangriffen angemessen zu begegnen, sei dabei die Integration eines IT Service Continuity Managements (ITSCM) ratsam. Schließlich bildeten BCMS und ITSCM die Grundlage für ein ganzheitliches Krisenmanagement.

Kunstdiebstahl

Das BKA berichtet am 17. September, dass am 13. September neun vermisste sakrale Figuren an die Diözesen Aachen und Münster zurückgegeben werden konnten.
Am 29. Februar hatte ein Benediktinerbruder zwei Reisegepäckstücke aufgefunden, die von Unbekannten über die Mauern des Klosters Maria Laach geworfen worden seien. Gestohlene Kunstgegenstände würden häufig erst nach Jahren und mehrmaligen Besitzerwechseln auf Kunstmessen oder über Aktionshäuser angeboten. Erst ein Vergleich spezifischer Merkmale habe die Feststellung der Identität ermöglicht.

Logistik

Mit einer **Weitbereichslösung bei der Zufahrtskontrolle** eines Logistikunternehmens befasst sich Security insight in der Ausgabe 5-2016, S. 26/27. Nur freigegebene Zugmaschinen, Kleintransporter, Wechselbrücken oder Trailer sollten in das Speditionsgelände einfahren oder es verlassen können. Das System solle die Zu- und Abfahrten überwachen und bei Manipulationsversuchen oder unberechtigtem Zugang Alarm auslösen. Ganze Wertschöpfungsketten hingen oft an der Termintreue. Für die Montage der Leser mussten Masten errichtet und Verkehrsschilder an strategischen Positionen aufgestellt werden. Die Fahrzeuge seien mit sogenannten Scheibentranspondern ausgerüstet worden. Die visitenkartenähnlichen Aufkleber mit integriertem Chip seien im Führerhaus jeweils an derselben Position aufgebracht worden, um die Kommunikation zwischen Leser und dem Fahrzeug störungsfrei zu gewährleisten. Die Transponder auf den Wechselbrücken und Trailern übermittelten bei der Durchfahrt dem Leser notwendige Informationen, welcher Ladungsträger wo ist. Der Import-/Export-Generator sorge durch

eine Schnittstelle zur Kennzeichenerkennung mittels Videoüberwachung für den notwendigen Abgleich zwischen den Transponderdaten und dem hinterlegten Kennzeichen. Das sorge für zusätzliche Sicherheit.

Luftverkehrssicherheit

Rechtsanwältin Juliane Holtz behandelt im DSD, Ausgabe 3-2016, S. 54/55, **Sicherheitsforschung im Bereich Aviation**. Das BMFT habe in den letzten zehn Jahren im Rahmen des Programms „Forschung für die zivile Sicherheit" über 470 Mio. Euro investiert. Im Projekt Trans4Goods (Sicherheit im Güterlandtransport mittels sicherer Informationsmuster an der Fracht) sei ein IT-Konzept entwickelt worden. Damit solle die Sicherheit von Gütertransporten in komplexen Lieferketten durch eine verbesserte Rückverfolgbarkeit der Warenbewegungen erreicht werden. Als Orientierung diene hier schon das hohe Niveau an Sicherheit im Luftfrachtverkehr. Eine ähnliche Herangehensweise verfolge das Verbundprojekt SiLuFra (Konzepte, Strategien und Technologien für sichere und effiziente Luftfracht-Transportketten). Als Nachfolgeprojekt beschäftige sich das Projekt Soft Parts (Soziale Bestimmungsgründe der Sicherheit am Flughafen) nicht mehr mit innovativen Technologielösungen, sondern lediglich mit der sozialwissenschaftlichen Perspektive bei der Herstellung von Sicherheit. Der mit Abschluss dieses Projektes Soft Parts entwickelte Leitfaden enthalte konkrete Handlungsempfehlungen zur Verbesserung der Kommunikation und Kooperation der beteiligten Akteure.

Maschinensicherheit

GIT stellt in der Ausgabe 9-2016, S. 180–182, Funkschaltgeräte der Firma steute an den Auslegern von Teleskopkranen vor. Funk statt Kabel: Nach diesem Motto rüste Paus die **Kranbaureihe Sky Worker PTK 27** mit speziellen Sicherheitseinrichtungen aus. Funkschaltgeräte übermittelten die Position des Kranhakens und den Ausschubzustand der Teleskope. Damit hätten die Konstrukteure eine ebenso zuverlässige wie kostengünstige Lösung entwickelt. Thematisiert werden in dem Beitrag: Funk statt Federkabeltrommel; zuverlässige Übertragung auch unter ungünstigen Bedingungen; energieautarker Betrieb; Erfassung des Ausschubzustands des Teleskopmastes durch Funksensoren; innovatives Krankonzept.

Matthias Wimmer, Pilz GmbH & Co., erläutert in der Ausgabe 9-2016, S. 186/187, wie der **Safety Calculator PAScal** den Umgang mit Normen und Richtlinien erleichtert. Er unterstütze bei der Berechnung des erreichbaren Performance Level und Safety integrity Level von Sicherheitsfunktionen in Maschinen und Anlagen. Thematisiert werden in dem Beitrag: das Einheitsblatt des VDMA, das den Datenaustausch erleichtere; die Minimierung des Aufwands durch Berechnungstools und die Modellierung per „Drag and Drop". Für die Modellierung der einzelnen Sicherheitsfunktionen könnten Komponenten mittels „Drag and Drop" aus den Bibliotheken in das Editor-Fenster gezogen werden.

Mit **Safety-Modulen für Servoantriebe** befasst sich die Zeitschrift GIT in der Ausgabe 9-2016, S. 190/191. Varimotion werde hauptsächlich in Automatisierungsanlagen eingesetzt, die hohe Ansprüche an Schnelligkeit und Präzision von koordinierten Bewegungen stellen. Da insbesondere bei schnellen Bewegungen beachtliche Anforderungen hinsichtlich der funktionalen Sicherheit zu erfüllen seien, habe man sich bei Promicon entschlossen, eine Lösung zu schaffen, die diesem Kriterium gerecht wird. Nicht selten werde eine Geschwindigkeit von 1m/s in weniger als 20 Millisekunden erreicht. Um derartige Situationen beherrschen zu können, seien die Safety-Module so ausgelegt, dass

eine unzulässige Bewegung in gerade einmal zwei Millisekunden erkannt werden kann. Die Servoregler und die Safety-Module seien so aufeinander abgestimmt, dass lediglich eine RJ45- Verbindung zwischen den Geräten erforderlich ist. Das gesamte Sicherheitskonzept sei vom TÜV zertifiziert und entspreche den gültigen Normen und Vorschriften.

Jonas Urlaub, Kübler Group, behandelt in der Ausgabe 9-2016 der Zeitschrift GIT, S. 192–194, modulare Sicherheit für die unterbrechungsfreie Zusammenarbeit von Mensch und Maschine. Vor mehr als einem Jahr habe das Unternehmen mit **Safety-M compact und Safety-M modular** seine zweite Generation an Sicherheitsmodulen präsentiert. Flexibel, passgenau und ganz unabhängig von der Antriebsart ließen sich nun modulare Sicherheitslösungen realisieren. Nun lege Kübler nach und baue die modulare Serie mit einem analogen Eingangsmodul aus. Das Ziel sei ein effizienter, kostenoptimierter Weg zu noch sicherer und unterbrechungsfreier Zusammenarbeit von Mensch und Maschine. Mit der Familie Safety-M lasse sich mit geringem Aufwand eine Vielzahl von Sicherheitseinrichtungen an Maschinen und Anlagen überwachen, seien es Drehmomentbegrenzer, Luftmessgeräte, Last oder Temperatursensoren. Das analoge Safety-Modul mache eine Überwachung einzelner Sensoren über Sicherheitsrelais überflüssig. Mit der großen Anzahl vordefinierter Sicherheitsmodule könnten besonders einfach passgenaue Sicherheitskonzepte realisiert werden.

Mindestlohn

Rechtsanwältin Cornelia Okpara weist in der Ausgabe 3-2016 des DSD, S. 65, auf ein Urteil des BAG vom 29. Juni hin, nach dem der gesetzliche Mindestlohn für jede geleistete Arbeitsstunde zu zahlen ist. Zur vergütungspflichtigen Arbeit zählten auch Bereitschaftszeiten, während derer sich der Arbeitnehmer an einem vom Arbeitgeber bestimmten Ort innerhalb oder außerhalb des Betriebs bereithalten muss, um bei Bedarf die Arbeit aufzunehmen.

Security insight zeigt in der Ausgabe 5-2016, S. 42/43, wie sich Sicherheitsdienstleister auf die Schwarzarbeit- und Mindestlohn-Kontrolle vorbereiten, siehe auch **Schwarzarbeit.**

Notfallmanagement

Erstmals könne eine hochverfügbare Notruf- und Informations-App für Smartphones in ein ganzheitliches Sicherheitskonzept eingebunden werden, berichtet Security insight in der Ausgabe 5-2016, S. 52/53. Die von Schneider Intercom entwickelte Notfall-App mit dem Namen **„SaveME"** schließe im Bereich der mobilen Alarmierung eine gravierende Sicherheitslücke. Bislang konnten rein auf Mobilfunktechnik basierende Applikationen aufgrund ihrer Abhängigkeit vom Funknetz keine professionellen Sicherheitsanforderungen erfüllen. Schneider Intercom biete nun eine innovative Lösung: Durch die Verbindung der neuen Smartphone-App mit dem Command Intercom-Server könne eine ständige Verfügbarkeit sichergestellt werden. Die Anwendungsszenarien seien vielfältig. In der Nutzung werde zwischen zwei verfügbaren Angriffen von außen oder Chemieunfällen unterschieden. Im zweiten Fall handele es sich um den „Persönlichen Hilferuf", der etwa bei einer Bedrohung oder einer Verletzung zum Tragen komme. Die Alarmauslösung erfolge dabei immer direkt am Smartphone oder mit Hilfe eines externen Bluetooth-Tasters, der versteckt am Arbeitsplatz angebracht sei oder am Körper getragen werde. Der Command Intercom-Server überwache ständig die Verfügbarkeit der Smartphones, verwalte die User, visualisiere deren Status, nehme die Notrufe auf und verarbeite sie.

Notruf

Sicherheit.info weist am 12. September darauf hin, dass am 1. Juli eine **neue technische Norm für Notruf- und Gefahren-Reaktionssysteme** in öffentlichen Gebäuden wie Schulen und Kitas, aber auch Krankenhäusern und Banken, veröffentlicht wurde. Die Richtlinie beschreibe ganz konkret die Anforderungen, die neue Kommunikationsanlagen in Not- und Gefahrenfällen künftig erfüllen sollten. Die neue deutsche Norm VDE 0827 sei darauf ausgerichtet, die organisatorischen Prozesse innerhalb einer Schule, einer Behörde oder einer Institution bestmöglich zu unterstützen. Sie gebe aber keine Verhaltensvorgaben zu spezifischen Vorfällen wie etwa einem Amokalarm. Es gelte, die zumeist bestehenden Konzepte mit Hilfe von Notfall- und Gefahrenreaktionssystemen umzusetzen. Neu sei die Position des technischen Risikomanagers, der innerhalb einer Organisation bestimmt, welcher Sicherheitsgrad umgesetzt werden müsse. Er sei es auch, der entscheiden könne, ob eventuell von den Vorgaben der Norm abgewichen werden kann. Zentrale Aufgabe des Risikomanagers sei außerdem die Risikoanalyse und die Risikobewertung. Damit die relevanten Schutzziele erreicht werden, ist die direkte Kommunikation zwischen dem Hilfesuchenden und einem Sicherheitsdienstleister von besonderer Bedeutung. Eine direkte Verbindung sei deshalb so wichtig, weil sich nur auf diese Weise die angemessene Reaktion auf einen Alarm bestimmen lasse. Egal sei, ob der Hilfesuchende sich in einem Flur, dem Lehrerzimmer oder in einem Unterrichtsraum aufhält. Auch wenn der Absender des Notrufs nicht antwortet, könne die Leitstelle die Situation vor Ort akustisch über ein Mikrofon mitverfolgen und passende Maßnahmen einleiten.

Objektsicherheit

Die Zertifizierung nach VdS-Richtlinie 3406 „Sicherheitsmanagement für bauliche Objekte" erläutern Dipl.-Ing. Klaus Behling, VZM GmbH, und Dipl.-Wirtschaftsjurist Sebastian Brose, VdS, in s+s report, Ausgabe 3-2016, S. 33–35. Sie beschreiben die Inhalte der VdS 3406 (Festlegung der Verantwortung; Ermittlung der Assets; Beschreibung der Gefährdungen; Definition der Maßnahmen; Prüfung der Wirksamkeit) und das VdS-Zertifizierungsverfahren (Vorbereitung gemeinsam mit dem Kunden; Reifegradprüfung; Audit vor Ort; VdS-Zertifikat). Zudem plädieren sie für neutrale Sicherheitsberatungen.

Perimeterschutz

Airportsicherheit aus Sicht des Perimeterschutzes behandelt die Zeitschrift GIT in der Ausgabe 9-2016, S. 126/127. Es müssten Bereiche mit niedrigeren Sicherheitsanforderungen und solche mit höheren Sicherheitsanforderungen definiert und entsprechend ausgestaltet werden. Dabei sei zu entscheiden, was passiert, wenn eine Störung des Sicherheitsbereichs entdeckt wird und wie lange eine Alarmierung und eine wirkungsvolle Reaktion dauern darf und aussehen muss. Sind diese Entscheidungen einmal getroffen, gehe es um die jeweils beste Kombination aus technischen Lösungen und Prozessen.

Sie müssten für die einzelnen Sektionen des Perimeters definiert und umgesetzt werden. Als „Mittel der Wahl" hätten sich intelligente Zäune und Barrieren in Kombination mit Videoüberwachung herauskristallisiert. Dort, wo keine Überwachung möglich oder erwünscht ist, aber dennoch ein hoher Sicherheitsbedarf besteht und nur geringste Fehlalarmquoten tolerabel sind, würden sich Spanndrahtsysteme anbieten. Das seien hybride Systeme, bei denen Sensoren und Spann- oder Stachel-

draht bereits in einem einzigen System kombiniert sind und damit zugleich eine physische Barriere mit hohem Überwindungswert und Detektion erreicht werde. Eine besonders schwer zu überwindende Sicherung bestehe im Einsatz von Mikrowellen oder Bodenmeldesystemen. Sie bildeten einen unsichtbaren und virtuellen Zaun. Solche Systeme sollten deshalb hinter einem mechanischen Zaun als zweite Alarmierungslinie platziert werden. Bodensysteme seien sehr zuverlässig und praktisch unüberwindbare Perimetersysteme für Hochsicherheitsbereiche. Sie seien in Planung, Anschaffung und Installation als langfristige Sicherheitsinvestitionen zu verstehen. Die allermeisten hochwertigen Sensorsysteme könnten über Schnittstellen miteinander verbunden und betrieben werden und eigneten sich somit perfekt abgestimmt für jeden Einsatzzweck.

Mit Sicherheitslösungen für eine effektive Geländeabsicherung befasst sich die Zeitschrift GIT in der Ausgabe 9-2016, S. 132/133. Mit 80.000 installierten Systemen sei **Southwest Microwafe** in mehr als hundert Ländern einer der wichtigsten Anbieter im wachsenden Markt für elektronische Perimeter-Sicherungssysteme. Der Hersteller legt hohen Wert auf höchste Detektionsfähigkeit und niedrigste Fehlalarmraten. Mit zum Angebot gehörten technische Dienstleistungen und eine Produktgarantie von fünf Jahren, flexible Anpassung an die Sicherheitsbedürfnisse des jeweiligen Kunden, nahtlose Verbindungsfähigkeit zwischen den Sensoren und dem sicherheitsspezifischen „Rahmenprogramm" sowie eine Produktqualität, die für langjährigen Betrieb auch unter harten Witterungsbedingungen sorge. Der Hersteller behandelt in dem Fachbeitrag das Zaundetektionssystem, erdverlegte Kabeldetektion, digitale Mikrowellenbarriere, Alarmüberwachungs- und Kontrollsysteme sowie technischen Support.

Perimeterschutz kritischer Infrastrukturen thematisiert Martin Vogler, Senstar GmbH, in der Ausgabe 5-2016 von Security insight, S. 24/25. Weil immer mehr Objekte kritischer Infrastrukturen miteinander vernetzt und voneinander abhängig sind, rückt auch die wirkungsvolle Absicherung von Einrichtungen der Energieversorgung immer wieder in den Mittelpunkt der Überlegungen. Im Bereich der Zaunmeldesysteme könne unterschieden werden zwischen herkömmlichen Technologien oder faseroptischen Systemen, die gänzlich unabhängig sind von elektronischer Beeinflussung und Störung. Beide Technologien hätten ihre spezifischen Vorteile und sollten im Vorfeld der Planung mit den entsprechenden Fachleuten besprochen werden, um das beste System für die jeweilige Anwendung zu finden. Allen Systemen sei gemein, dass Störungen des gesicherten Perimeters metergenau lokalisiert und in Kombination mit einer Videoüberwachung und einem Alarmmanagementsystem die Ursache in Sekundenschnelle ermittelt und beurteilt werden können. Elektronische Sicherheit sei nicht umsonst zu haben, sei aber unermesslich wertvoll in ihrer Funktion und äußerst billig in Relation zu den möglichen Auswirkungen und Schäden im Bereich der Energieversorgung.

Photovoltaikanlagensicherheit

Dipl.-Ing. Lutz Erbe, VGH Versicherungen, befasst sich mit fehlerhaft dimensionierten Kabelanlagen bei Photovoltaikanlagen in s+s report, Ausgabe 3-2016, S. 52–56: Der Autor listet gravierende Fehler bei der Planung und Errichtung solcher Anlagen auf. Er geht insbesondere ein auf normative Vorgaben bei der Kabeldimensionierung, auf Faktoren, die wesentlichen Einfluss auf die Strombelastbarkeit von Kabel und Leitungen haben, auf die Dimensionierung nach vereinbarten Leitungsverlusten, nach Tabellen für Energieversorgungsnetze mit Belastungsgrad 0,7, auf die unrealistische Annahme von Umgebungsbedingungen, auf den Erdbodenwärmewiderstand und auf

typische Ausführungsfehler (direkte Sonneneinstrahlung, mangelhafte Befestigung und auf Kabelführung über Brandwände).

Piraterie

Über einem neuen Schwerpunkt der Piraterie im Golf von Guinea berichtet Peter Niggl in Security insight (Ausgabe 5-2016, S. 22/23). Weltweit seien die Fallzahlen im ersten Quartal 2016 gegenüber dem ersten Quartal 2015 deutlich zurückgegangen. Im Brennpunkt Golf von Guinea seien die Fallzahlen dagegen angestiegen. Die Überfälle fänden zum größten Teil in einem Korridor von 50 bis 100 Seemeilen (ca. 90 bis 180 km) vor der Küste statt. Dabei sei speziell vor Westafrika von einer hohen Dunkelziffer auszugehen.

Rechenzentrumssicherheit

Als Spezialist für Systemarmaturen habe die MIT Moderne Industrietechnik GmbH & Co. KG einen Aluminium-Löschtank entwickelt, der im **OneU-Aktivlöschsystem von Minimax** zum Einsatz komme, berichtet die Zeitschrift GIT in der Ausgabe 9-2016, S. 166/167. OneU sorge für Brandschutz in Rechenzentren und brauche nur 44 mm Bauhöhe im IT-Rack. Der extrem kompakte Tank verlange hohes Entwicklungs- und Fertigungs-Know-how. Beim Auslösen öffne – ähnlich wie beim Pkw-Airbag – eine Treibgaspatrone einen Schieber, der das unter Druck stehende Löschmittel Novec 1230 freisetzt. Das Löschmittel verteile sich sofort im Rack und verhindere damit die Ausbreitung des Brandes auf die umgebende IT-Infrastruktur. Treibgaspatrone, Schieber und Löschdüse seien in einer separaten, ebenfalls aus Aluminium gefertigten Baugruppe untergebracht, die mit dem Tank verschweißt werde.

Reisesicherheit

Michael Pülmann, SmartRiskSolutions GmbH, schildert im Newsletter des ASW vom 17. September die Situation in **Venezuela** aus Sicht von Geschäftsreisenden. Jeden Monat würden Flughafenmitarbeiter wegen krimineller Aktivitäten verhaftet. Geschäftsreisende würden bereits bei der Ankunft am Flughafen von Caracas gezielt von kriminellen Banden ausgewählt. Einem Deutschen, der am Flughafen durch seine Luxusuhr aufgefallen sei, wären die Täter bis zu seinem Hotel gefolgt. Beim Betreten des Eurobuilding Hotels hätten ihn die drei Täter mit Maschinenpistolen angegriffen. Auch ein Ägypter, der sich beim Überfall am Flughafen wehrte, sei von einem Täter erschossen worden.
Bei Dunkelheit sei die Fahrt vom Flughafen Maiquetia nach Caracas äußerst gefährlich und erfordere besondere Aufmerksamkeit. Dann gebe es nur noch eine geringe Polizeipräsenz, und Fahrzeuge würden regelmäßig überfallen. Für solche Fahrten sei ein sondergeschütztes Fahrzeug angeraten.
Bei allen Fahrten sei es unabdingbar, einen vertrauenswürdigen und bekannten Fahrer zu haben. Wegen des mangelnden Vertrauens in die Sicherheitsbehörden schätze man, dass rund 90 Prozent der Entführungen nicht angezeigt würden. Offiziell sei die Zahlung von Lösegeld verboten. Die Korruption stelle ein sehr großes Problem dar. Insbesondere bei Polizeikontrollen nach Sonnenuntergang sei Vorsicht geboten. Die Regierung habe eingeräumt, dass ca. 300 Ermittlungsverfahren gegen Staatsbedienstete wegen einer möglichen Beteiligung an Entführungen anhängig sind. Bei Überlandfahrten sei zu bedenken, dass Tankstellen bisweilen auch während der offiziellen Öffnungszeiten geschlossen seien oder keinen Treibstoff mehr haben. Bei Verkehrsunfällen müsse offiziell die Polizei gerufen werden – die teilweise erst nach Stunden eintreffe.

Schadenverhütung

Die Präventionsarbeit des GDV beschreibt Alexander Küsel, GDV, in der Ausgabe 3-2016 von s+s report, S. 50/51. Er skizziert praktische Musterschutzkonzepte für verschiedene Branchen, die Aufgabenstellung der Kommission Sach-Schadenverhütung (KSSV) im GDV, das von VdS Schadenverhütung betriebene Informationsportal, die Ergebnisse der GDV Schadenverhütungsarbeit in Form unverbindlicher Leitlinien unter sss.vds-industrial.de zum kostenlosen Download und die periodisch erscheinende Bericht der GDV-Schadenverhütung **(www.gdv.de/2016/06/schaeden-verhindern-bevor-sie-entstehen).**

Schließsysteme

Manuela Engel-Dahan, Lock Your World GmbH & Co. KG, befasst sich in s+s report, Ausgabe 3-2016, S. 46–48, mit dem neuen **Schließsystem „pylocx"** für Hochsicherheitsbereiche. Neben der klaren Forderung „Die Batterie muss raus aus dem Schloss" sei ein Katalog mit Eigenschaften zusammengestellt worden, die pylocx auszeichnen sollten: vor allem Vandalismus-Sicherheit und die Einsatzfähigkeit sowohl im Indoor- als auch im Outdoor-Bereich. Schwerpunkte des Beitrags sind: individuelles Code-System zur Öffnungsberechtigung; Einmal-Codevergabe durch den Operator oder automatisiert. Individuelle Branchenlösungen wie „pylocx banking", „pylocx mobile" (für Telekommunikation und für Behörden), „pylocx logistics" und „pylocx retail" (für Handel und Tankstellen) würden gemeinsam mit den Kooperationspartnern ausgearbeitet. Bei einem Verlust der mobilen Bedieneinheit seien keine Änderungen vor Ort an Schließkomponenten notwendig. Der verlustige pyKey werde in der Datenbank gelöscht und dem Nutzer ein neuer ausgehändigt.

Schwarzarbeit

Security insight zeigt in der Ausgabe 5-2016, S. 42/43, wie sich Sicherheitsdienstleister auf die Schwarzarbeit- und Mindestlohn-Kontrolle vorbereiten. Es handelt sich insbesondere um folgende Vorbereitungen: Bereithalten eines Schichtplans; Anweisung an Mitarbeiter, immer ein Ausweisdokument mitzuführen; Arbeitsstundenübersicht bereithalten; Auskünfte erteilen und Dokumente aushändigen; Anweisung an die Mitarbeiter, sich kooperativ dem Zoll gegenüber zu verhalten; Begleitung der Beamten durch den verantwortlichen Schichtleiter; keine Aushilfen unangemeldet arbeiten lassen; bei Bedarf Anwalt oder Steuerberater zu Rate ziehen.

Sicherheitsgefühl

Die Ergebnisse einer **Umfrage von Axis Communication in den Niederlanden** skizziert Epko van Nisselrooj in der Zeitschrift GIT, Ausgabe 9-2016, S. 116–118. Von den rund tausend befragten Niederländern zwischen 18 bis 64 Jahren gaben 60 Prozent an, sich im öffentlichen Raum unsicher zu fühlen, 46 Prozent sorgten sich über die Kriminalität in ihrer Gemeinschaft, 43 Prozent sogar auch tagsüber. Trotzdem hätten nur 19 Prozent im Jahr 2015 auf eine Aktivität wie Kinobesuch oder Spaziergang deswegen verzichtet. 13 Prozent hätten auf eine Fahrt mit öffentlichen Verkehrsmitteln verzichtet. 55 Prozent gaben an, keine Schutzmaßnahmen unternommen zu haben. 24 Prozent hätten eine Versicherung abgeschlossen, 21 Prozent hätten sich mit den Nachbarn abgestimmt, 14 Prozent hätten eine Alarmanlage zu Hause. 57 Prozent forderten mehr Polizeipersonal, 49 Prozent eine bessere Beleuchtung von öffentlichen Plätzen und Straßen, 35 Prozent mehr Videoüberwachung.

Sicherheitsmarkt

Die Fachzeitschrift DSD enthält in der Ausgabe 3-2016, S. 46, eine Aufzählung von Zahlen, Daten und **Fakten zum Sicherheitsmarkt in Deutschland**. Insgesamt habe sich im Zweijahresvergleich von 2013 bis 2015 ein Umsatzwachstum von 17 Prozent auf 14,5 Mrd. Euro ergeben. Die Wachstumsrate des Umsatzes von Sicherheitsdienstleistungen habe 21 Prozent betragen. Im Einzelnen sei der Umsatz in den verschiedenen Branchen wie folgt angestiegen (in Mrd. Euro): bei Bewachungen inklusive Dienstleistungszentren auf 6,9; bei der elektronischen Sicherheitstechnik 3,7; bei sonstigen Sicherheitsanlagen auf 0,9; bei stationären Löschanlagen auf 0,4; bei Schlössern und Beschlägen auf 1,0; bei Geldschränken und Tresoren auf 0,2; bei mechanischer Außenhautsicherung auf 0,7; bei sonstiger Sicherheitstechnik auf 0,7. Die Aufwärtsentwicklung werde auch weiterhin vor allem von der positiven Entwicklung der Brandmeldeanlagen (+ 24 Prozent) getragen, die aus der beachtlichen Nachfrage nach Rauchwarnmeldern resultiere. Der Umsatz der Sicherheitsdienstleister sei von 2014 auf 2015 von 6,01 auf 6,90 Mrd. Euro gestiegen. Im gleichen Zeitraum sei die Zahl der Beschäftigten im Sicherheitsgewerbe von 214.000 auf rund 233.000 angewachsen.

Dr. Harald Olschok, BDSW, behandelt in Ausgabe 3-2016 des DSD, S. 48/49, die **Forschung für die zivile Sicherheit**. Das BMBF fördere seit 2007 umfassende Sicherheitslösungen. Gegenstand der Förderung seien unter anderem neue wirtschaftliche Zusammenhänge, Wertschöpfungsmuster und innovative Ansätze für Geschäftsmodelle einer modernen Sicherheitswirtschaft in einem konkreten Anwendungsszenario. Der BDSW habe sich entschlossen, gemeinsam mit Partnern aus der Wissenschaft unter Federführung des Brandenburgischen Instituts für Sicherheit und Gesellschaft die „Ordnung des Sicherheitsmarktes" (OSiMa) zu analysieren. Dabei gehe es insbesondere darum, darzulegen, welchen Beitrag aus ordnungspolitischer Sicht die private Sicherheitswirtschaft leisten könne, sowie den Rahmen zu beschreiben, innerhalb dessen neue Dienstleistungen und Organisationsformen von Schutz und Sicherheit durch die Sicherheitswirtschaft entstehen könnten. In dem Projekt OSiMa gehe es zusammenfassend darum, welche Formen von Schutz und Sicherheit durch den Staat und welche auch durch Private bereit- und herzustellen sind.

Horst Schärges, freier Journalist, entwickelt in der Zeitschrift Sicherheitsforum (Ausgabe 4-2016, S. 50–53) eine Prognose der **Entwicklung der Sicherheitswirtschaft bis 2020**. Das Marktvolumen weltweit werde in den nächsten vier Jahren auf 500 Mrd. US-Dollar anwachsen. Es sei absehbar, dass sich die Sicherheitskonjunktur aus vielfältigen Gründen zunehmend unabhängig von der Baukonjunktur entwickeln werde. Hinzu kämen gesellschaftlich erwünschte technologische Entwicklungen, die sich ohne eine Anhebung des Sicherheitsniveaus kaum umsetzen ließen (Internet of Things, Smart Buildings, Industrie 4.0). Branchenbezogen sähen die Wachstumsraten wie folgt aus: Im umsatzstärksten Teilsegment der Sicherheitswirtschaft, der Cyber-Security, erwarteten die Analysten bis 2020 ein Wachstum von jährlich 9,8 Prozent auf weltweit 170 Mrd. US-Dollar. Die klassische elektronische Sicherheit werde bis 2020 weltweit um durchschnittlich acht Prozent wachsen. Für den Brandschutzmarkt werde mit einem durchschnittlichen jährlichen Wachstum von 11,5 Prozent gerechnet. Auch wenn die internetbasierte IP-Technik aufgrund der zusätzlichen Möglichkeiten einen zunehmend höheren Marktanteil bei der Videoüberwachung aufweisen dürfte (jährliches Wachstum 39,2 Prozent), sähen die Analysten auch für die alte analoge Technik noch Potenzial. Bei den Umsätzen für Speicherlösungen werde bis 2020 mit einem jährlichen Plus von 22,4 Prozent gerechnet. Der Active-Pixel-Sensorik

werde im Vergleich zu CCD-Lösungen aufgrund geringerer Einbaugrößen, niedrigerem Energiebedarf, höheren Frameraten und günstigeren Herstellungskosten ein höheres Wachstum zugeschrieben. Für die meist cloudbasierte Video Surveillance as a Service werde bis 2020 ein jährliches Wachstum von 28,2 Prozent weltweit prognostiziert. Für die Thermo-Kameras, die insbesondere im militärischen Bereich und bei der Zaun- oder Geländeüberwachung Verwendung finden, werde aktuell ein jährlicher Zuwachs von 14,3 Prozent prognostiziert. Die Marktanteile im Videobereich verteilten sich 2016 etwa so: 84,4 Prozent für die professionelle Überwachung; 9,8 Prozent für Videoüberwachung von Privathaushalten; 4,4 Pro-zent für Video Surveillance as a Service.

Sicherheitstechnik

Die Komplexität sei eine große Herausforderung für moderne Sicherheitstechnik, betont Horst Schärges, freier Fachjournalist, in der Ausgabe 3-2016 des DSD, S. 6–8. Komplexität erleichtere nicht nur redundante Lösungen, sie erhöhe auch die Fehlerwahrscheinlichkeit. Auch auf der security-Messe in Essen werde sich immer wieder die grundlegende Frage stellen, in welchem Umfang es sinnvoll sei, Sicherheitslösungen in die Betriebs- oder Gebäudesysteme zu integrieren, oder ob manche Überwachungsaufgaben nicht besser in getrennten Systemen untergebracht werden sollten. Bei der Organisation von Sicherheitsdienstleistungen, bei der Überprüfung und Wartung von Sicherheitstechnik, bei der Live-Überwachung oder bei der Reaktion auf Sicherheitsvorfälle unterstütze die Kombination aus Sprachkommunikation, mobiler Rechenkapazität und Online-Datenverbindung Entscheidungen, beschleunige Prozesse und spare so Kosten. Bei mobil zu erbringenden Sicherheitsdienstleistungen, etwa bei Kontrollgängen und bei der Live-Dokumentation von Vorgängen würden die Lösungen gezielt auf die mobile Nutzung ausgerichtet. Die perfekte Ergänzung seien dabei Service-Konzepte per Cloud. Video Surveillance as a service oder Acces Control as a Service seien im Kern allerdings keine neuen Angebote. Die Entwicklungen in der Sensorik, die Verfügbarkeit immer leistungsfähigerer Algorithmen und Prozessoren für die Datenauswertung und bezahlbare Speicherkapazitäten ermöglichten der Sicherheitstechnik derzeit einen großen Schritt nach vorn.

„Neuronale Kommunikation" lautet der Titel eines Beitrags zum Thema „Gebäudebezogene und **sicherheitstechnische Sprach- und Kommunikationssysteme**" in der Ausgabe 9-2016 der Zeitschrift GIT, S. 114/115. „Neurokom IP" – so heiße die jüngste Innovation des Unternehmens Gehrke Sales GmbH. Die Endgeräteserie basiere auf server- und zentralenloser Intercom-Technologie und intelligenten neuronalen Terminals. Das neuronale System arbeite komplett ohne Zentrale oder Server – einfach im Netzwerk mit intelligenten Endgeräten. Bis zu 9.000 eigenständige NeuroUnit-Module könnten direkt untereinander kommunizieren und müssten nicht durch eine zentrale Instanz gesteuert werden. Die Sicherheit der Systeme sei extrem hoch, da es keine zentrale Instanz, keinen Kommunikationsserver oder -rechner gebe – also keinen „single point of failure". Einige Aufgabenbeispiele für die intelligenten Netzwerk-Komponenten: Tür-, Tor- und Schrankenkommunikation einschließlich deren Steuerung, Aufzugnotruf, Leitstandsysteme mit oder ohne Funkansteuerung, Informations- und Notrufsprechanlagen, Reaktionssysteme bei Amok-, Alarm- und Notfall-Gefahren, Schulsprechanlagen, Industriesprechgeräte für unterschiedliche Umgebungsbedingungen, OP-Sprechstellen, Zutrittsberechtigungskonzepte, Beschallungssysteme. Die bestehenden zentralengesteuerten Sprechanlagen und eventuell vorhandene ELA-, ENS- oder Sprachalarmierungssysteme könnten in die neuronalen Sicherheitskommunikationslösungen integriert werden.

Sicherheitswirtschaft

Das „neue Sicherheitsunternehmen" wird in Ausgabe 3-2016 der Fachzeitschrift DSD, S. 10–14, vorgestellt. Die Sicherheitsbedürfnisse von Kunden aus der Wirtschaft sowie von Staat und Kommunen unterlägen einem ständigen Wandel. Die Ursachen dafür seien vielschichtig. Für das „neue Sicherheitsunternehmen" komme es entscheidend darauf an, sich auf die wechselnden Kundenbedürfnisse einzustellen und eine kundenspezifische Gesamtlösung zu entwickeln. Dies setze eine Sicherheitskonzeption der gesamten „Sicherheitskette" voraus. Derzeit stehe das Sicherheitsgewerbe in einem sich flächenartig entwickelnden „Business Change", einem Paradigmenwechsel. Ohne eine fundierte Kenntnis der jeweiligen Technik könne der Sicherheitsdienstleister weder ein seriöses Angebot einer bestimmten Technologie unterbreiten, noch einzelne Systeme in ihrer konkreten Anwendbarkeit und Effizienz beurteilen und die Sicherheitstechnik in eine kundenspezifische Gesamtlösung integrieren. Expertenwissen sowie das Wissen der Geschäftsführung reichten jedoch allein nicht aus. Damit die moderne Dienstleistung auf dem Markt erfolgreich verkauft werden kann, müssten auch die Sicherheitsmitarbeiterinnen und -mitarbeiter vor Ort wichtige Grundkenntnisse der Sicherheitstechnik haben. Dringend erforderlich sei eine grundlegende Novellierung der rechtlichen Rahmenbedingungen. Der Staat müsse seinen Beitrag dazu leisten, damit sich künftig qualifizierte Sicherheitsdienstleister auf dem Markt erfolgreich behaupten könnten.

Mit **Weichenstellungen und Positionsbestimmungen für die zukünftige Sicherheitsarchitektur** befasst sich Dr. Berthold Stoppelkamp, BDSW, in der Ausgabe 3-2016 des DSD, S. 67/68. Nach der seit 1992 von der R + V Versicherung durchgeführten repräsentativen „Ängste-Studie" sei im Jahr 2016 die Angst der Deutschen vor terroristischen Angriffen mit 73 Prozent (Vorjahr 52 Prozent) am größten. Auf Platz zwei rangiere die Angst vor „politischem Extremismus" mit 68 Prozent (Vorjahr 49 Prozent), auf Platz drei die Angst vor Spannungen durch Zuzug von Ausländern mit 67 Prozent (Vorjahr 49 Prozent). In der aktuellen Diskussion würden von der Politik in der Regel Ansätze eines vernetzten Sicherheitsansatzes von Staat, Wirtschaft und Sicherheitswirtschaft nicht erwähnt. Zum Ausbau der deutschen Sicherheitsarchitektur durch nachhaltige Stärkung der privaten Sicherheitssäule in der Kooperation mit der Polizei beim Schutz von Großveranstaltungen, Schutz des ÖPV, Schutz von Flüchtlingsunterkünften und dem Schutz kritischer Infrastrukturen bedürfe es allerdings eines sektorspezifischen Regulierungsansatzes außerhalb der Gewerbeordnung.

Thomas Ball, Lünendonk GmbH, unternimmt in Ausgabe 3-2016 der Fachzeitschrift DSD, S. 50/51, eine Bestandsaufnahme der „komplizierten Beziehung" privater Sicherheitsdienstleistungen für die öffentliche Hand. Erst langsam wandle sich die Interpretation des **Wirtschaftlichkeitsbegriffs der Vergabeordnung** für Leistungen (VOL) von günstigst hin zum besten Preis-/Leistungsverhältnis. Es sei Zeit für eine stärkere Regulierung, um die negativen Begleiterscheinungen des liberalisierten Marktes einzugrenzen. Die Liberalisierung habe ihren Zweck, für günstige Preise zu sorgen, bereits lange erreicht. Im Rahmen der Lünendonkstudie 2015 entwickelte Grafiken zeigen, dass die Öffentliche Hand nach Umsatzvolumen mit 24,1 Prozent im Jahr 2014 nach der Industrie (41,4 Prozent) der zweitwichtigste Kunde des Sicherheitsgewerbes war. Die höchste Zustimmung bekam bei einer Befragung mit 1,6 (von -2 bis + 2) die These: „Gut ausgebildete Mitarbeiter werden ein Wettbewerbsvorteil sein", gefolgt von der These „Das öffentliche Bild der Sicherheitsdienstleister wird sich zukünftig verbessern".

„Sicherheitsbranche wächst in unsicheren Zeiten" titelt die FAZ am 20. September.

Sie suche infolge der Flüchtlingskrise und vermehrter terroristischer Übergriffe händeringend Mitarbeiter. Derzeit seien nach einer Mitteilung des BDSW **rund 13.000 Stellen offen**. In der „Boombranche", die ihren Aufschwung einem abnehmenden Sicherheitsempfinden in der Bevölkerung verdanke, herrsche nach Einschätzung der Gewerkschaft Verdi ein Preiskampf, der auch die Löhne unter Druck setze. Während in der Branche meist einfachste Bewachungstätigkeiten ausgeschrieben seien, müssten die Beschäftigten in Flüchtlingsunterkünften häufig zusätzlich Aufgaben, etwa von Psychologen oder Sozialarbeitern übernehmen. Der BDSW wünsche sich eine bessere Ausbildung des Personals. Ein Problem für viele Auftraggeber seien die deutlich höheren Kosten für das qualifizierte Personal. Wer eine dreijährige Ausbildung zur Fachkraft für Schutz und Sicherheit absolviert habe, sei mit einem Stundenlohn von 15,43 Euro für den Auftraggeber deutlich teurer als ein Wachmann, der lediglich an einer Unterweisung durch die IHK teilgenommen habe. Letztendlich sei meist der niedrigste Preis ausschlaggebend. Deutlich verstärkt habe sich etwa die Nachfrage nach allem, was mit der Sicherheit bei Großveranstaltungen zusammenhänge. Zu den "Schwergewichten" der Branche zählten Securitas und die Essener Familienfirma Kötter. Während Securitas 2015 als „Branchenprimus" mit 19.500 Beschäftigten einen Umsatz von rund 720 Mio. Euro erwirtschaftet habe, habe der Umsatz bei Kötter mit 18.100 Beschäftigten bei rund 502 Mio. Euro gelegen. Bundesweit gebe es nach Schätzungen zwischen 4.000 und 5.000 Sicherheitsunternehmen.

Die Wochenzeitung DAS PARLAMENT vom 26. September weist darauf hin, dass der Bundestag ein **Gesetz zur Änderung bewachungsrechtlicher Vorschriften** (18/8558, 18/9707) beschlossen hat, mit dem auf Vorfälle bei der Bewachung von Flüchtlingsheimen reagiert werde. Bewachungsunternehmer und deren leitendes Personal müssten künftig eine Prüfung über ihre Sachkunde ablegen und würden regelmäßig überprüft werden.

Stadionsicherheit

Sicherheit bei Großveranstaltungen im Zeichen von Terrorwarnungen behandelt der BDSW in der Zeitschrift Security insight (Ausgabe 5-2016, S. 69). Die Gewährleistung von Sicherheit und Ordnung bei Großveranstaltungen sei ein bedeutendes Aufgabengebiet für das Sicherheitsgewerbe geworden. Der Gesetzgeber verlange zwar in der Muster-Versammlungsstättenverordnung den Einsatz von Ordnungsdiensten, habe diese aber nicht ausreichend definiert. In der Praxis würden die Begriffe „Ordnung" und „Sicherheit" häufig synonym verwendet. Hier sei eine Vereinheitlichung mit dem gewerberechtlichen Ansatz erforderlich. Bis zu 12.000 private Sicherheitskräfte seien pro Spieltag in den drei Bundesligen im Einsatz. Bei gleichzeitig stattfindenden „Risikospielen" könne die Zahl noch deutlich höher sein. Eine Umfrage unter 1.000 Dauerkartenbesitzern habe ergeben, dass 94 Prozent Verständnis für schärfere Überprüfungen äußerten. Für den Einsatz von Sicherheits- und Ordnungskräften in Fußballstadien fordert der BDSW eine tätigkeitsspezifische Qualifizierung, die speziell auf die Situation im Stadion abgestimmt sein müsse. Der BDSW fordere eine über die derzeit geltenden gewerberechtlichen Regelungen hinausgehende, unbürokratische und schnelle Zuverlässigkeitsüberprüfung durch die Polizeibehörden.

„USBV-Inspektor"

Der Behörden Spiegel berichtet in der September-Ausgabe über die Entwicklung eines Detektions- und Analysesystems zur Abklärung, ob es sich bei einem aufgefundenen verdächtigen Gegenstand um eine

„unkonventionelle Spreng- und Brandvorrichtung (USBV)" handelt. Bei dem zu entwickelnden intelligenten Einsatzhelfer handele es sich um eine multimodale Sensor-Suite. Sie bestehe aus einem Millimeterwellenscanner, einer hochauflösenden digitalen Kamera und einer dreidimensionalen Umgebungserfassung. Die Bestandteile seien in einem Gehäuse integriert und auf einer Roboterplattform montiert. Der Roboter werde von den Entschärfern aus sicherer Entfernung ferngesteuert. Der Millimeterwellensensor durchleuchte die Gefahrenquelle und bilde das Innere dreidimensional ab. Ein in den Roboter integrierter Industriecomputer sammle die Daten und sende sie an den Rechner, wo sie per Sensordatenfusion zusammengeführt werden.

Videoüberwachung

Das Sicherheitsforum (Ausgabe 4-2016, S. 6) weist auf eine neue EN-Nummer (62676-4) statt der bisherigen Norm EN 50132-7 für Video Security hin. Dahinter stecke, dass die europäische CENELEC-Norm nun als IEC-Norm global zur Verfügung steht.

Die Zeitschrift Security insight stellt in der Ausgabe 5-2016, S. 30 die Frage: **Sind Kameras das schwächste Glied im Videoüberwachungsnetzwerk?** Moderne, intelligente Videoüberwachungssysteme bestünden heute fast ausschließlich aus „Internet of Things" (IoT)-Geräten wie z. B. Kameras, Server und Zutrittskontrollgeräte. Diese Systeme seien effizient, dynamisch, teilweise sogar Cloud-basiert und böten vielerlei Vorteile gegenüber analogen CCTV-Systemen. Entgegen allen Vermutungen sei nicht die Sicherheit der Cloud das größte Problem, sondern die mangelnde Sicherheit der angeschlossenen Geräte selbst. Die Kameras stünden an der Spitze dieser Liste. Die Standardpasswörter Hunderter Kameramodelle ließen sich über eine einfache Suchmaschinenabfrage ausfindet machen. Neue Passwörter für alle Komponenten des Sicherheitssystems zu vergeben, sei ein wichtiger Schritt. Genauso wichtig seien regelmäßige Firmware und Software-Updates. Zentrales Cloud-Management mache es nicht nur einfacher, Firmware-Updates mit nur einem einfachen Mausklick auf Hunderte von Kameras zu verteilen. Sie könnten auch den Systemzustand aller Kameras überwachen.

Wächterkontrollsystem

Den Smartphone-Eintrag ins virtuelle Wachbuch behandelt Security insight in der Ausgabe 5-2016, S. 40. Wenn es um die Vereinfachung, Strukturierung und Beschleunigung täglicher Prozesse und Aufgaben bei Sicherheitsdienstleistern geht, sei heute meist Software am Werk. Sie sei insbesondere bei der Dienst- und Personalplanung eine große Hilfe. Bei Anwendung der NFC-Technologie würden für das Wachpersonal am zu bewachenden Objekt gut sichtbare Kontrollpunkte in Form von NFC-Chips angebracht. Mit einem handelsüblichen Smartphone könne der Mitarbeiter während seines Kontrollgangs die Kontrollstellen (NFC-Tags) scannen. Das erzeuge automatisch einen Eintrag ins virtuelle Wachbuch, der sich um weitere Informationen, beispielsweise eine Vorfallsbeschreibung, mit Text und Bild ergänzen lasse.

Windows 10

Sicherheit stehe bei Windows 10 weiterhin im Fokus, berichtet <kes> am 8. September. Auch das Anniversary-Update liefere neue Security-Funktionen. Überdies bleibe das Microsoft-Betriebssystem mit häufigeren „großen" Updates ein bewegliches Ziel, das Angreifern weniger Zeit lasse, um tiefer liegende Verwundbarkeiten auszunutzen. 350 Mio. Anwender hätten sich

bisher dafür entschieden, die neue Betriebssystemversion zu nutzen und somit auch die aktuellsten Sicherheitsfunktionen zum Einsatz zu bringen. Gleichzeitig vollziehe sich weiterhin etwas, das wohl als Revolution der Cyberbedrohungen gelten müsse: Gut ausgebildete und ausgestattete Angreifer erwiesen sich als überaus erfolgreich, auch gegenüber gut geschützten Umgebungen. Gegenwehr müsse weiterhin auf allen Ebenen erfolgen, und so sei es auch notwendig, die Technik weiterzuentwickeln und neue Ansätze zur Verteidigung so bald wie möglich auch wirksam zum Einsatz zu bringen.

Wirtschaftsspionage

Ein umfassendes Konzept zur Abwehr von Wirtschaftsspionage dürfe nicht auf Sensibilisierung beschränkt bleiben, betont der Behörden Spiegel in seiner September-Ausgabe. Klassische Schutzmaßnahmen wie Virenschutzprogramme und Firewalls reichten nicht mehr aus. Eine effektive Security-Strategie stelle sich den Herausforderungen des digitalen Marktes, indem sie klassische unabhängige Systeme in einer einzigen Architektur mit fünf kritischen und voneinander abhängigen Faktoren vereine: Skalierbarkeit, Sichtbarkeit, Sicherheit, Proaktivität und Offenheit.

Wohnungseinbruch

Mit der Begrenzung staatlicher **Fördermittel für den Einbruchschutz** befasst sich die FAZ am 21. September. 440,8 Mio. Euro – so hoch sei der finanzielle Schaden gewesen, der dem BMI zufolge bei insgesamt 167.000 Einbrüchen im Jahr 2015 entstanden ist. Seit Jahren werde in Deutschland immer häufiger eingebrochen. Schon zum neunten Mal in Folge sei die Zahl der gemeldeten Fälle 2015 gestiegen. In den vergangenen fünf Jahren erhöhte sich die Zahl um mehr als 30 Prozent. Im Rahmen eines KfW-Förderprogramms unterstütze das Bundesbauministerium jeden Eigentümer oder Mieter, der seinen Haushalt besser gegen Einbrecher sichern möchte. 20 Mio. Euro habe der Bund bisher zur Verfügung gestellt. Doch der Topf für 2016 sei mittlerweile leer. Der staatliche Zuschuss könne zwar 2016 noch beantragt werden. Das Geld werde dann allerdings erst 2017 ausgezahlt. Für 2017 plane die große Koalition, die Mittel auf 50 Mio. im Jahr aufzustocken. 10 Prozent ihrer Umbaukosten und maximal 1.500 Euro könnten sich Eigentümer und Mieter im Rahmen der Kfw-Förderung erstatten lassen, vorausgesetzt, sie stellen den Antrag vorher und lassen die Arbeiten von einem Fachunternehmen ausführen. Gefördert würden vor allem Maßnahmen wie der Einbau einbruchsicherer Türen und Fenster, aber auch die Installation von Alarmanlagen oder spezieller Beleuchtung. Nach einer Studie des Kriminologischen Forschungsinstituts Niedersachsen seien in mehr als 40 Prozent der Versuche die Einbrecher an vorhandenen Sicherheitseinrichtungen gescheitert und hätten aufgegeben.

„Zugelassener Wirtschaftsbeteiligter"

Die Pflichten „zugelassener Wirtschaftsbeteiligter" (Authorized Economic Operator – AEO) behandelt GIT in der Ausgabe 9-2016, S. 108/109. Exportierende Unternehmen müssten kontrollieren, ob gegen Geschäftspartner Sanktionen verhängt wurden. Dies geschehe unter anderem durch den Abgleich mit sogenannten Sanktionslisten. Gerade Unternehmen, die vom Zoll als AEO geprüft und zertifiziert wurden, um innerhalb der EU in einem vereinfachten Verfahren ihren Handel betreiben zu können, betreffe diese notwendige Überprüfung ihrer Handelskontakte. Treffer müssten dokumentiert und unverzüglich gemeldet werden.

Zutrittskontrolle

Fabian Lange, Vertreter der Interessengemeinschaft **Offline Standard iGOS**, fordert in der Zeitschrift Sicherheitsforum (Ausgabe 4-2016, S. 10–13) einen herstellerneutralen Standard im Bereich des Offline-Zutrittsmanagements. Im Bereich der Online-Zutrittskontrollsysteme habe sich auf RFID-Medien seit Längerem ein herstellerneutraler Standard etabliert (Standard Access). Eine Interessengemeinschaft von Endanwendern habe diesen realen Standard nun im Segment der „Open Security Standards (OSS)" gefunden. Der Standard OSS sei aus zwei Gründen der bislang erfolgreichste Versuch, einen herstellerneutralen Standard für das Zutrittsmanagement im Bereich Offline-RFID zu erarbeiten. Einerseits hätten sich einige renommierte Hersteller zusammengesetzt und ein Produkt entwickelt, das „Hand und Fuß" habe. Andererseits böten die Endanwender mit einigen geplanten Projekten für die Produzenten den nötigen finanziellen Anreiz, dieses Produkt auch tatsächlich zu entwickeln.

Eine direkt im SAP-System integrierte Zutrittslösung wird in der Zeitschrift Security insight, Ausgabe 5-2016, S. 48/49, vorgestellt. Mit Kaba EACM erfolge das komplette Online-Zutrittsmanagement direkt über das SAP-Modul Organisationsmanagement von SAP HCM. Damit werde keine zusätzliche Middleware benötigt und alle Zutrittskomponenten kommunizierten ohne Umwege direkt mit dem SAP System. Diese Lösung sorge für höchste Unternehmenssicherheit bei gleichzeitig minimiertem Verwaltungsaufwand.

Mobile-Access-Lösungen thematisiert Security insight in der Ausgabe 5-2016, S. 76/77. Viele Zugangskontrollsysteme seien völlig veraltet. Mobile-Access-Lösungen seien heute State of the Art und basierten auf den modernsten und sichersten Technologiestandards. Oft könnten bisher genutzte Komponenten wie Lesegeräte, Panels oder auch die Verkabelung bestehen bleiben. Auch bisher im Unternehmen eingesetzte Smartphones könnten einfach für die Mobile-Access-Nutzung vorbereitet werden. Es seien weder spezielle mobile Geräte erforderlich noch der Einsatz einer neuen microSD (Speicherkarte). Die Nutzung von Mobile-IDs sei sicherer als die Verwendung von Ausweiskarten. Alle Identitätsdaten seien verschlüsselt und manipulationssicher gespeichert, und zwar als kryptographisch geschützte Datenobjekte im Gerätespeicher des Smartphones. Zudem seien alle mobilen IDs auch an ein spezifisches Gerät gekoppelt und nicht übertragbar.

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

focus.securitas.de

Kontakt
Securitas Holding GmbH
Redaktion Focus on Security
Potsdamer Str. 88
D-10785 Berlin

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

E-Mail: info@securitas.de