Focus on Security

Ausgabe 05, Mai 2017

SECURITAS

Inhalt

Alarmübertragung

Dipl.-Ing. Stephan Holzem, TAS Telefonbau Arthur Schwabe GmbH & Co. KG, behandelt in der Ausgabe 1-2017 der Zeitschrift s+s report, S. 46–49, die **IP-basierte Übertragungstechnik**. Eine zukunftsweisende Adressierung gehe nur noch über IP-Adressen. In der europäischen Working-Group 5 von CENELEC werde bereits an einem Anhang EN 50136-a/A1 gearbeitet, der deutlich mache, in welche Richtung die Alarmübertragung sich weiterentwickelt. Mit dem neuen Begriff „Secure Location" gehe es schnell in die Nähe von zukünftigen Cloud-Lösungen für den Alarmempfang. Eine „Secure Location" könne nach dem Normentwurf entweder eine AES (Monitoring Alarm Receiving Center) oder ein Rechenzentrum nach einem Standard wie TIER 3 oder EN 50600 sein. In der AES gebe es dem Entwurf folgend nur noch ein „IRCT" – das Interface zum RDT, dem Alarmempfänger. Nach der Norm sei der ATSP (Alarm Transmission Service Provider) zukünftig in den höheren Übertragungsklassen immer erforderlich. Der ATSP behalte immer die Gesamtverantwortung für die gesamte Übertragungsstrecke. Über diese Definition würden der Betrieb und die Verantwortung der Komponenten in der Cloud verbindlich definiert. Der Autor beschreibt die neue Cloud-Lösung „Hosted ATS". Die Nutzung von Sicherheitsnetzen biete gegenüber öffentlichen Netzen generell einige Vorteile, die sich im Wesentlichen auf die höhere Verfügbarkeit des Übertragungssystems bezögen. Die Anbindung von Einbruch- oder Brandmeldesystemen über ein Übertragungsgerät an eine IP-basierte Netzstruktur eröffne neue Möglichkeiten in Bezug auf Fernservicedienstleistungen. Dabei sei es unerheblich, ob ein Sicherheitsnetz oder eine internetbasierende Cloudlösung verwendet wird.

Biogasanlagen

Schadenverhütung in Biogasanlagen thematisiert Dipl.-Ing. Karsten Callondann, VdS Schadenverhütung, in der Ausgabe 1-2017 von s+s report, S. 58/59. Im GDV sei eine Projektgruppe gegründet worden, die die Ursachen von Schäden in Biogasanlagen analysieren sollte. Die Analyse habe gezeigt, dass eine Vielzahl von Brandschäden ihren Ursprung im Blockheizkraftwerk (BHKW) hatte. Außerdem seien defekte BHKW-Motoren, Rührwerke, Rohrleitungen und Fermenter-Folien sowie Schäden an der elektrischen Anlage zahlreich vertreten gewesen. Danach sei eine eigene Publikation im VdS-Verlag erstellt worden, die alle versicherungsrelevanten Themen abdecke. Die versicherungsrelevanten Inhalte würden sich aus den verschiedenen Möglichkeiten ergeben, wie eine Biogasanlage versichert werden kann. Der Leitfaden zu Biogasanlagen (VdS 3470) solle Betreiber, Planer und Errichter sensibilisieren. Es gehe darum, die Risiken für die Versicherungen mit entsprechenden Hinweisen zu reduzieren. Der Autor behandelt Auswahl, Planung und Errichtung von Biogasanlagen, Organisation, Qualifikation sowie Betrieb und Instandhaltung.

Brandschutz

Dr. Florian Meinhard, VdS Schadenverhütung, befasst sich in der Ausgabe 1-2017 von s+s report, S. 16–18, mit **druckgeregelten Inertgas-Löschanlagen**. Es gäbe zur ursprünglichen Bauweise eine Alternative: Anstatt mittels einer Blende den Druckanstieg im Verteilerrohrnetz auf einen Maximaldruck zu begrenzen, werde mechanische Druckregeltechnik eingesetzt, um den Rohrnetzdruck für längere Zeit in einem möglichst hohen Bereich zu halten, unterhalb des Maximaldrucks der Rohrleitung. Der Autor behandelt die Regelung auf Eingangs- oder Ausgangs-

druck, den „idealen" Druckregler, das Ziel schlanker Rohrleitungen und das Ziel einer Minimierung der Vorratsmenge. Druckgeregelte Systeme seien großartige Erfindungen. Gerade bei langen Flutungszeiten könnten sie ihre Vorteile im Vergleich mit ungeregelten Systemen voll ausspielen. Würden sie jedoch knapp ausgelegt oder bei sehr hohen Gasflüssen betrieben, so könnten sie einen Großteil ihrer Vorzüge gegenüber konventionellen Anlagen verlieren.

Ingenieurmäßige Kennzahlen zum Brandschutz in **Behinderteneinrichtungen** stellt Dipl.-Ing. M. Eng. Johannes Göbell, göbell kallinowsky ingenieure, in der Ausgabe 1-2017 von s+s report, S. 19–23, vor. Sie sollten die subjektive Einschätzung notwendiger Brandschutzmaßnahmen durch ein ingenieurmäßiges und belastbares Verfahren ersetzen. Der Autor behandelt zunächst eine brandschutztechnische Einordnung von Behinderten. Neben der Mobilität müssten auch noch Parameter zur sensitiven und kognitiven Beeinträchtigung beachtet werden. Aus der Anzahl der Personen je Einstufung von Nutzern bezüglich der Fähigkeit zur Selbstrettung für die horizontale Flucht in sechs Stufen und dem dazugehörigen Einstufungsfaktor lasse sich die Anzahl der notwendigen Betreuer für die Bemessungsgruppe berechnen. Aus der Kombination der gesetzlich vorgegebenen Anzahl von Pflegekräften pro Hilfsbedürftigem einer bestimmten Pflegestufe und der Zuordnung der Pflegestufen zu den Einstufungen ließen sich die Helferquoten für Einrichtungen der Altenpflege ermitteln. Der Berechnung der Helferquote für vergleichbare geregelte Sonderbauten ergebe Werte zwischen 0,17 in einer Station eines Pflegeheims mit geringer Pflegeintensität und 0,33 in der Intensivstation eines Krankenhauses. Mit der Möglichkeit, über die Helferquote und den Räumungsschlüssel die Betreuungssituation numerisch einschätzen zu können, ließen sich Art und Umfang von Brandschutzmaßnahmen nutzergruppenbezogen individuell abstimmen. Die Ergebnisse der kennzahlenorientierten Brandschutzanalyse ermöglichten Aussagen zu den Themen Personenstrom, Räumungssituation, Möglichkeit der Nutzung vertikaler Rettungswege, Helfersituation und Organisation.

Neuerungen in den Anforderungen der Normen **VDE 0100-420 und VdS 2033** behandelt Dipl.-Ing. Lutz Erbe, VGH Versicherungen, in der Ausgabe 1-2017 von s+s report, S. 24–28. Er beschreibt typische Mängel in feuergefährdeten Betriebsstätten und Einstufungen feuergefährdeter Betriebsstätten. Allein das Vorhandensein brennbaren Materials und leicht entzündlicher Stoffe in gefahrdrohender Menge führe zu einer Einstufung als „feuergefährdete Betriebsstätte". Verantwortlich für diese Einstufung und für den ordnungsgemäßen Zustand der elektrischen Anlage sei der Betreiber. Der Autor stellt neue normative Anforderungen und Einrichtungen zur Lichtbogenerkennung und -abschaltung und Störlichtbogenschutzeinrichtungen vor und behandelt das Laden von Elektrofahrzeugen. Bei der Begutachtung von elektrischen Anlagen würde sich die Qualität der elektrischen Installation in Lagern und Produktionsbereichen oft als unzureichend herausstellen. Dies führe zu einer Erhöhung des Brandrisikos für das gesamte Gebäude.

Dipl.-Ing. Heike Siefkes, VdS Schadenverhütung, geht in der Zeitschrift s+s report, Ausgabe 1-2017, S. 29–32, auf **Aerosol-Feuerlöschanlagen** ein. Sie beschreibt zunächst das Löschmittel und seine Wirkungsweise. Aerosol sei die Verteilung feiner flüssiger oder fester Stoffe in einem Gas oder in der Luft. Die primäre Löschwirkung beruhe auf dem Prinzip der Unterbrechung der Kettenreaktion, die bei einer Verbrennung abläuft. Die Autorin vergleicht Aerosolgeneratoren mit konventionellen Anlagen, beschreibt den Löschgenerator und schildert gängige Anwendungsfälle. Generell sei eine Aerosol-Feuerlöschanlage für den Raumschutz von unbesetzten Räumen geeignet, da durch die Auslösung der Anlage eine Personen-

gefährdung bestehe. Nicht geeignet seien die Anlagen dagegen für Bereiche, in denen Chemikalien gelagert werden, die ihre eigene Sauerstoffversorgung enthalten. Behandelt werden ferner die Planung und Auslegung der Anlage, die Abdichtung und Druckentlastung, Maßnahmen nach dem Auslösen, das Brandmeldesystem und die Steuerzentrale sowie das Prüf- und Anerkennungsverfahren bei VdS Schadenverhütung.

veko online berichtet in der April-Ausgabe über einen Vortrag von Peter Ohmberger, Hekatron, zum Thema „**Brandschutz 4.0** oder Das sichere Gebäude der Zukunft" in dem er drei Hauptbotschaften und Strategien für die Zukunft im Kontext von Sicherheit 4.0 und Brandschutz 4.0 verkündet:
1. „Wir müssen unseren Kunden ‚Security as a service' bieten und Schnittstellen zu anderen Lebensbereichen wie Finanzen, Energieeffizienz, Entertainment und Gesundheit schaffen". 2. „Wer in der Sicherheitsbranche im Spiel bleiben will, muss sich zum Anbieter von Komplettlösungen, Dienstleistungen und Wissensverkauf entwickeln." 3. Es gelte das Thema „Kooperation und Kollaboration" neu zu denken. „Wir müssen uns insbesondere gegenüber den Anbietern – beispielsweise von Gas, Wasser, Strom und Medien – öffnen, die schon Zutritt ins Gebäude besitzen."

Dr. Sebastian Festag, ZVEI, stellt in der Ausgabe 4-2017 der Zeitschrift GIT, S. 70/71, Ergebnisse eines ZVEI-Projekts zur Erforschung der frühen Brandphase vor. Ein deutlicher Mehrwert für die Personensicherheit durch eine **Brandfrühesterkennung** liege vor allem darin, dass toxische Gase erfasst werden können, die insbesondere bei Entstehungs- und Schwelbränden wesentlich eher auftreten als beispielsweise hohe Wärmestrahlungen einer flammenden Verbrennung. Bisher habe der Fokus hauptsächlich auf Kohlenmonoxid als Leitkomponente für Rauchgasvergiftungen gelegen. Daneben hätten sich vor allem Chlorwasserstoff und Cyanwasserstoff als geeignete Detektorgase für alle untersuchten Proben gezeigt. Sie seien vor allem deshalb relevant, weil ihre toxikologischen Grenzwerte je nach Gas etwa um den Faktor zehn niedriger sind als bei CO und sie dadurch eine hohe Gefährdung für Personen im Brandfall darstellen. Ein weiteres Ergebnis des Projekts sei die Aufzeichnung von Daten, die das Reaktionsverhalten der Brandstoffe charakterisieren und daher als Grundlage für die Entwicklung von Verbrennungsmodellen genutzt werden können. Die gewonnenen Daten stellten einen ersten Schritt in der Erforschung von zukünftigen Sensortechnologien dar. Als nächstes sei ein Augenmerk auf die Charakterisierung des Ausbreitungsverhaltens der identifizierten Brandgase in Gebäuden zu legen.

GIT weist in der Ausgabe 4-2017, S. 106, auf das **„Gore Parallon System"** hin, das auf der Messe INTERSCHUTZ vorgestellt worden ist. Es sei speziell für die mit Feuchtigkeit verbundenen thermischen Gefahren wie Wärmedurchschlag, Verbrühungen und Hitzestress entwickelt und ermögliche Feuerwehrschutzkleidung, die nicht nur zuverlässig vor Hitze und Flammen schützt, sondern auch die Wärmeabgabe des Körpers nachhaltig unterstützt. Feuerwehrleute sollten damit von konstantem thermischen Schutz und zugleich hohem Tragekomfort profitieren.

Rudolf Vennemann, Siemens AG, befasst sich in der Ausgabe 4-2017 der Zeitschrift PROTECTOR, S. 44/45, mit **Brandschutzschaltern** in Schulen. Während Leitungsschutzschalter Schutz bei Kurzschluss und bei Überlast bieten, erfassten Fehlerstromschutzeinrichtungen Fehlerströme gegen Erde. Neben parallelen Fehlerlichtbögen gebe es jedoch auch serielle, wie sie etwa bei der Unterbrechung eines Leiters oder in Folge von losen Kontakten entstehen können. Diese ließen sich mit den gängigen Schutzgeräten nicht erkennen. Diese Schutzlücke würden Brandschutzschalter wie der 5SM6 aus dem Sentron-Portfolio von Siemens schließen. Allein in Deutschland sei rund ein

Drittel aller Brände auf Elektrizität als Brandursache zurückzuführen. Im Detektionsfall schalte das Gerät den Stromkreis über den LS- beziehungsweise FI/LS-Schalter sicher ab. Brandgefahren von der elektrischen Leitung bis zum Endgerät könnten so frühzeitig erkannt und unterbunden werden. Die Norm VDE 0100-420 fordere verpflichtend die Installation des Brandschutzschalters für einphasige Endstromkreise bis 16 A in definierten Anwendungsbereichen. Darunter fielen insbesondere Betriebe, in denen potenziell brennbare Materialien vorhanden sind, öffentliche Gebäude wie Bahnhöfe, Flughäfen und Museen sowie Schlaf- und Aufenthaltsräume von Heimen und Tageseinrichtungen für Kinder, behinderte oder alte Menschen.

Die **Brandschutzverglasung** in der Deutschen Nationalbibliothek in Leipzig wird in Ausgabe 4-2017 von PROTECTOR, S. 46/47, beschrieben. Zum Einsatz komme Pyranova Spezialglas von Schott, ein klares Mehrscheibenverbundglas für Brandschutzverglasungen der Feuerwiderstandsklasse F beziehungsweise EL, das Feuer, Rauch und Wärmestrahlung abhalte. Es werde abhängig von der Feuerwiderstandsklasse aus mindestens zwei Floatglasscheiben hergestellt, zwischen die eine transparente Brandschutzschicht eingelagert ist. Im Brandfall zerspringe die dem Brandherd zugewandte Scheibe, die Schicht schäume auf und bilde einen Hitzeschild.

Wassernebel-Löschanlagen behandelt Olaf Schilloks, Tyco Fire & Security Holding Germany GmbH, in der Ausgabe 4-2017 von PROTECTOR, S. 48. Bei vielen herkömmlichen Löschtechniken würden nur fünf Prozent des Wassers aktiv brandbekämpfend wirken. 95 Prozent blieben ungenutzt und verursachten oft hohe Sekundärschäden. Allerdings stoße auch das Prinzip der möglichst starken Zerstäubung an seine Grenzen: Sehr feine Tropfen seien für die Bekämpfung von Glutnestern weniger geeignet. Aufsteigende heiße Brandgase würden sie davontragen, ehe sie ihr Ziel erreichen. Der Planer einer Wassernebel-Lösch- oder Brandunterdrückungsanlage müsse daher die Art des Schutzobjektes ebenso berücksichtigen wie Brandlast, Brandgut, die potenzielle Brandausbreitungsgeschwindigkeit und Umgebungsbedingungen. Beachtet werden müssten die Tropfengröße, Dichte, Geschwindigkeit der Tropfen und die Gestalt des erzeugten Tropfenschwarms. Wassernebel-Löschanlagen müssten also sehr flexibel konfigurierbar sein, damit sie in jedem Fall die maximale Wirkung erzielen.

Compliance

Jeder zehnte Angehörige des mittleren Managements in Deutschland würde eine Regulierungsbehörde täuschen, wenn er sich dadurch einen persönlichen Vorteil verschaffen könnte. Das sei – nach einem Bericht in der FAZ am 6. April – das überraschendste Ergebnis einer Studie zur Wirtschaftskriminalität, die das Beratungsunternehmen EY alle zwei Jahre durchführt. Der Durchschnitt in Westeuropa liege bei fünf Prozent. Wirtschaftskriminalität und unmoralisches Verhalten in Unternehmen wird nach den Worten von Stefan Heißner, EY, stark von der Wahrnehmung beeinflusst. Wer glaubt, dass alle so etwas tun, der tue es auch. Unternehmen sollten seiner Ansicht nach viel mehr auf Menschen achten, die „einen Hang zur Grenzmoral" zeigten, also immer am Rande der Moral oder der Legalität arbeiten, alles ausloten, was gerade noch möglich ist. Die wenigsten Wirtschaftskriminellen seien von Gier oder krimineller Energie geprägt. Die meisten testeten Grenzen des Möglichen aus. In der täglichen Arbeit gerieten einzelne Mitarbeiter immer wieder in Konfliktsituationen, in solche mit Vorgesetzten, in solche um die eigene Karriere oder in Konflikte zwischen Privatsphäre und Beruf, die sie glaubten nur dadurch entschärfen zu können, dass sie Grenzen überschreiten. In Deutschland werde

Moral und gute Unternehmensführung zu juristisch betrachtet und zu stark in starren Prozessen organisiert. Dabei sei Kriminalitätsbekämpfung in Unternehmen nicht in erster Linie eine Frage der fixierten Regeln, sondern der Kultur, der offenen Kommunikation und des Verhaltens der Führung.

Mit der Überwachung der **Accounting Compliance** durch den Aufsichtsrat und die Deutsche Prüfstelle für Rechnungslegung (DPR) befasst sich Prof. Dr. Sonja Wüstemann in Ausgabe 1-2017 der Zeitschrift comply, S. 48–50. Die Ausübung unternehmerischen Ermessens spiele bei der Anwendung der International Financial Reporting Standards (IFRS) wegen des Zukunftsbezugs der zu vermittelnden Informationen eine zentrale Rolle. Die Beurteilung der Ordnungsmäßigkeit der Ermessensausübung durch den Aufsichtsrat setze eingehende Kenntnisse der IFRS-Rechnungslegung, aber auch Vertrautheit mit dem Geschäftssektor des Unternehmens voraus, was nunmehr sogar in § 100 Abs. 5 AktG gesetzlich gefordert werde. Die über zehnjährige Erfahrung seit Einrichtung der DPR zeige, dass diese bei der Überprüfung von Ermessensentscheidungen strengere Maßstäbe anlegt als Aufsichtsräte und Abschlussprüfer. Es empfehle sich aus Sicht der Aufsichtsräte, auf eine gute Dokumentation und Substantiierung der ermessensbezogenen Entscheidungsprozesse zu achten, sich über die Aktivitäten und vergangenen Fehlerfeststellungen der DPR regelmäßig zu informieren und kritische Ermessensfragen eingehend mit dem Abschlussprüfer zu diskutieren.

Datenschutz

Martin Schindler weist am 4. April in silicon.de darauf hin, dass die Umsetzungsfrist für die EU-DSGVO am 25. Mai 2018 endet. Im Mai 2017 solle das deutsche Umsetzungsgesetz zur DSGVO veröffentlicht werden. Es zeichne sich ab, dass durch die Neuregelung Bußgeldhöhen für Unternehmen stark angehoben werden. So biete der Art. 83 Abs. 5 der DSGVO den Aufsichtsbehörden die Möglichkeit, Bußgelder bis zu 20 Mio. Euro beziehungsweise bei Konzernen bis zu vier Prozent des weltweiten Umsatzes des Vorjahres zu verhängen.

Diebstahl

Mit **Diebstahl auf Bestellung** befasst sich Peter Niggl, Redaktion Security insight in der Ausgabe 2-2017, S. 13–17. Hochwertige Einzel- und Ersatzteile würden an Attraktivität gewinnen. Es gebe inzwischen logistische Spezialisten, die wissen, wo hochwertige Autoteile gerade gefragt sind. Hochwertige Fahrzeuge seien ein besonderes Ziel. Niggl rät: „Seien Sie misstrauisch, wenn Ihr Fahrzeug von fremden Personen lange beobachtet wird, wenn diese Fotos machen oder wenn ein Auto mit ausländischem Kennzeichen auffällig häufig und mehrmals an Ihrem Auto vorbeifährt." Der Ecclesia Versicherungsdienst habe zwischen Februar 2014 und Juli 2016 bundesweit 55 Fälle verzeichnet, in denen teure Untersuchungsgeräte aus Kliniken gestohlen worden sind. Dem Handel mache besonders der professionell organisierte Ladendiebstahl von Banden und Tätern zu schaffen, die bestimmte Waren in großen Mengen auf Bestellung stehlen.

Drohnen

Eike Kühl weist in zeit.online am 12. April auf die Geltung der neuen **Drohnenverordnung** hin. Bei mehr als 250 Gramm Gewicht müssten die Quadrokopter mit Name und Anschrift gekennzeichnet werden. Ab zwei Kilogramm Startgewicht benötigten die Flugbesitzer einen sogenannten Kenntnis- oder Flugkundenachweis. Ab fünf Kilo Startgewicht

sei eine Aufstiegsgenehmigung der jeweiligen Landesluftbehörde erforderlich. Eine Ausnahmeerlaubnis sei darüber hinaus für Flüge in einer Höhe von mehr als 100 Meter notwendig. Außerhalb der Sichtweite ihrer Piloten dürften Drohnen nur mit Genehmigung geflogen werden. Der Einsatz über und in der Nähe von Bundes- und Landesbehörden, Verfassungsorganen, Flugplätzen, Industrieanlagen inklusive Umspannwerken, Gefängnissen und Naturschutzgebieten bleibe verboten. Bei Menschenansammlungen, Einsatzorten von Rettungskräften sowie Fernstraßen und Bahnanlagen müsse ein Abstand von 100 Metern eingehalten werden.

Drohnenalarm über Deutschland, titelt die FAZ am 24. April. Die Gefahr von Terroranschlägen mit ferngesteuerten Flugrobotern, die mittlerweile Lasten von mehr als 15 kg tragen können, werde nach Meinung von Sicherheitsexperten in Deutschland unterschätzt. Weil bisher noch nicht viel passiert sei, werde auch wenig in konkrete Abwehrtechnologien investiert. Dabei gebe es gute technische Lösungen von hochqualifizierten Anbietern. Dazu gehöre die Deutsche Telekom mit ihrem „Drohnenschutzschild" und Dedrone, das sich mit seinen Abwehrsystemen als weltweit marktführend sieht. Gefährdet seien große Rechenzentren, in denen die Server ständig gekühlt werden müssen. Wenn Drohnen die Luftansaugung auf den Gebäudedächern durch das Versprühen von Stoffen lahmlegten, könne das zum Stillstand des gesamten Rechenzentrums führen. Terroristen könnten es darauf anlegen, Drohnen in der Einflugschneise via GPS zu positionieren, um Triebwerke von Flugzeugen zu zerstören. Gefährlich sei, dass die Drohnen inzwischen über das Internet gesteuert werden können. Der Pilot könne nicht nur Tausende Kilometer von der Drohne entfernt sein. Er könne sie auch programmieren und mit einem Timer versehen. Sie starte dann zum vorgegebenen Zeitpunkt automatisch und fliege die einprogrammierte Route eigenständig ab. Die Abwehrtechnik ziele darauf, fremde Drohnen mit Hilfe verschiedener Sensoren (Videokameras, Mikrofone, Infrarotscanner, Frequenzscanner) zu orten, um dann über Funk auf der entsprechenden Frequenz in die Steuerung einzudringen. Eine Lokalisierung des Piloten wäre so möglich. Prophylaktisch eine Mauer mit Störsendern aufzubauen sei nicht erlaubt, weil so auch Mobilfunknetze außer Betrieb gerieten. Die Deutsche Flugsicherung (DFS) habe 2016 64 Drohnensichtungen gemeldet. Eine DFS-Sprecherin habe betont, dass die kleinen Flugobjekte auf dem Radarschirm der Lotsen nicht sichtbar seien. Derzeit laufe zusammen mit der Telekom ein Forschungsvorhaben, Drohnen über das Mobilfunknetz zu orten und so im Luftlagebild für Lotsen sichtbar zu machen. Neue Modelle verfügten über GPS-Chips, in denen Flugverbotszonen programmiert sind.

Einbruch

Einbruchdiebstähle in **Gewerbeobjekten** thematisiert Dr. Frank Kawelovski in der Ausgabe 1-2017 von s+s report, S. 37–39. Eine Untersuchung von 400 staatsanwaltschaftlichen Akten in NRW habe gezeigt, dass mit zwölf Prozent nur ein relativ geringer Teil polizeilich geklärt werden konnte. In 46 Prozent der Fälle sei es beim Tatversuch geblieben, teilweise weil die Täter den Einbruch, aber nicht den Diebstahl vollendet hatten. Am stärksten betroffen seien Kioske (10,8 Prozent), gefolgt von Schankwirtschaften (6,5 Prozent), Arztpraxen (6,0 Prozent), Frisiersalons (3,8 Prozent) und Lebensmittelgeschäften (3,5 Prozent). Die Beute bestand in 31 Prozent der Fälle aus Bargeld. Unter entwendeten Waren dominierten Zigaretten (bei 8,0 Prozent der Einbrüche). Der durchschnittliche Beuteschaden habe sich mit 2.800 Euro deutlich unter den Erwartungen herausgestellt. Sachschäden seien häufig höher gewesen als die Beuteschäden. In fast 65 Prozent aller Fälle sei es den Tätern

gelungen, die Zugänge der Firmen zu überwinden. Angegangen worden seien in 65 Prozent aller Fälle Außentüren, in knapp 30 Prozent Fenster und in rund elf Prozent Türen in Treppenhäusern. Waren Videoüberwachungsanlagen vorhanden, so bekam die Polizei nur in jedem zehnten Fall brauchbare Bilder mit Aufnahmen der Täter. In fast der Hälfte der Fälle seien die Aufnahmen unbrauchbar gewesen, weil die Kameras entweder gar nicht oder mit zu schwachen Lichtquellen gekoppelt waren. Bei den Taten, in denen die betroffenen Unternehmen zu einem Wachdienst aufgeschaltet waren, habe in keinem einzigen Fall ein Täter auf frischer Tat gefasst werden können. Ursächlich hierfür schien in allen Fällen eine umständliche Alarmierungskette zu sein. In knapp 18 Prozent aller Fälle, in denen es Alarmanlagen gab, hätten diese aus unterschiedlichen Gründen keinen Alarm abgegeben.

Die Zeitschrift s+s report weist in der Ausgabe 1-2017, S. 62, auf die **VdS-Fachtagung** „Einbruchdiebstahlschutz" am 27./28. Juni 2017 hin. Themen seien u. a. die Neuerungen an der Richtlinie VdS 2311, das Normungsvorhaben der EU für die Fernwartung und -prüfung von Sicherheitssystemen, die Möglichkeiten für NSL, per Videoüberwachung im Ernstfall direkt die Polizei alarmieren zu können, ganzheitliches Sicherheitsmanagement für umfassenden Risikoschutz und branchenspezifische Aspekte der Industrie 4.0, Cybersecurity speziell für EMA und Neuigkeiten aus der Regulierung zu Smart-Home-Systemen.

Einzelhandelssicherheit

Jan Seitz und Felix Polla, TH Wildau, befassen sich in der April-Ausgabe des Behörden Spiegel mit der **Sicherheit in der Lebensmittelkette**. In Sicherungssysteme, Redundanzen und ähnliches werde kaum investiert, da Prozesssicherheit auf dem heiß umkämpften, aber stabilen deutschen Markt „nur" Kosten verursache. Die gesteigerte Gesamtproduktivität werde voraussichtlich auf Kosten der Sicherheit erreicht. Bereits jetzt gebe es zu wenige realistische Krisenplanungen, zu wenig Kapazitäten zum Ausgleich unvorhergesehener Ereignisse und erhebliche Probleme in der IT-Sicherheit.

Diebesbanden plündern den Einzelhandel, titelt die FAZ am 27. April. „Eigentumsdelikte dürfen nicht als Bagatellen betrachtet werden. Staatsanwaltschaften und Gerichte sollten bei Ladendiebstählen auf die Möglichkeit der Verfahrenseinstellung nur in Ausnahmefällen zurückgreifen und Taten stattdessen konsequent strafrechtlich sanktionieren", habe der Hauptgeschäftsführer des Handelsverbandes HDE, Stefan Genth, erklärt. Gert Pieper, Chef der größten inhabergeführten Parfümeriekette Deutschlands, berichte von mehr als 300 Ladendiebstählen täglich in seinen 150 Geschäften. Laut EHI Retail Institute liegt die Dunkelziffer beim einfachen Ladendiebstahl bei 98 Prozent, womit zuletzt jährlich mehr als 26 Mio. Fälle im Wert von rund 86 Euro je Diebstahl unentdeckt blieben. Der durch Ladendiebstähle verursachte wirtschaftliche Schaden betrage jährlich über zwei Mrd. Euro. Am 28. April meldet die FAZ, dass der bayerische Justizminister, Winfried Bausback, mit Nachdruck fordere, zur Abschreckung Tätern den **Führerschein** zu **entziehen**. Ladendiebstahl dürfe keinesfalls als bloße Bagatelle abgetan werden. Laut FAZ stellt sich aber die Frage, ob man den überwiegenden Teil der Diebesbanden mit einem Fahrverbot erreicht. Zielführender wären verschärfte Auflagen der Gerichte an die Meldepflichten dieser Personen.

Endgerätesicherheit

GIT weist in der Ausgabe 4-2017, S. 66, auf die von Rohde & Schwarz Cybersecurity entwickelte **sichere Plattform für Smartphones**

und Tablets Bizz Trust hin. Basierend auf einem gehärteten Sicherheitskern für das meistgenutzte Smartphone-Betriebssystem Android werde sie in zwei isolierte Sicherheitsbereiche unterteilt: einen privaten Bereich und einen Unternehmensbereich. Anwendungen und Daten in diesen jeweiligen Sicherheitsdomänen würden streng voneinander getrennt. Die Personal-Domäne stehe zu einem gewissen Grad unter Kontrolle der Anwender. Im Gegensatz dazu stehe die Business-Domäne unter vollständiger Kontrolle eines zentralen Managements. Der zugrunde liegende Turaya-Sicherheitskern verhindere einen unerlaubten Abfluss von Informationen aus der Business-Domäne, indem er durch eingefügte Zugriffskontrollmechanismen beide Domänen streng voneinander isoliere. Zudem schütze er die Unternehmensdaten mittels kryptografischer Maßnahmen sowohl bei der lokalen Speicherung als auch bei der Übertragung. Anwendungen aus dem Business-Bereich könnten über einen sicheren VPN-Tunnel auf E-Mails, Kontakte, Kalender und Intranet zugreifen und untereinander Daten austauschen. Der Zugriff auf externe Webseiten erfolge im Business-Bereich über die Unternehmensfirewall.

Fingerspurenscanner

Die Fachzeitschrift PROTECTOR berichtet in der Ausgabe 4-2017, S. 71, dass dank der 10-jährigen Entwicklungsarbeit von Jürgen Marx, Scanovis, das Einpinseln der Fingerspuren am Tatort bald durch einen Hightech-Laser ersetzt werden könne. Durch den schnellen und unkomplizierten Einsatz des Lasers könne die Untersuchungszeit von bis zu 36 Stunden für einen Tatort auf unter eine Minute reduziert werden. Die kleinste Laborversion des Scanners soll in einen Koffer verpackt auch transportabel sein. In einem zweiten Entwicklungsschritt werde der Scanner modifiziert, um weitere Substanzen scannen zu können. Dazu könnten unter anderem Blut, Drogen oder Sperma gehören. Die dritte Entwicklungsstufe sehe die Fertigstellung des Handscanners vor, der direkt am Tatort scannt, auswertet und die Spur per WLAN mit dem Datennetz der Polizei abgleicht.

Gefahrenmeldeanlagen

Markus Schroth, ATS Elektronik GmbH, behandelt in s+s report, Ausgabe 1-2017, S. 40–42, die Richtlinie VdS 2465 Version 2. Die komplette Überarbeitung der Norm sei unter anderem deshalb notwendig gewesen, da mit der ersten Version die Erfüllung der Anforderungen aus der europäischen Norm EN 501365 nur mit sehr hohem Aufwand auf Seiten der Errichter und der Leitstelle erreicht werden konnte. Der Autor gibt eine kurze Übersicht über die wichtigsten Neuerungen von VdS 2465-2 und 2465-3. Und er geht auf die Richtlinie VdS 2471 ein, die Anforderungen und Prüfmethoden für Übertragungswege in Alarmübertragungsanlagen beschreibt. Er behandelt die Überwachung der Übertragungsdauer, die Einweg-Übertragung (analog zu SP4 gemäß DIN EN 50136-1) und die Zweiweg-Übertragung (analog zu DP4 gemäß DIN EN 50136-1).

Gefahrstoffe

Im März 2017 ist die 2. Auflage des Buches **„Sicheres Arbeiten mit Gefahrstoffen“** von Dr. Birgit Stöffler im Verlag ecomed erschienen. Es will schnell und gleichzeitig grundlegend über alle wichtigen Aspekte des sicheren Arbeitens mit Gefahrstoffen informieren. Es enthält Merksätze, die Angaben aus den Vorschriften in verständlicheren Worten zusammenfassen. Praxistipps sollen die Umsetzung der Anforderungen aus den Vorschriften in die betriebliche Praxis

erleichtern. Zusätzlich enthalten viele Kapitel Übungsaufgaben, mit denen die Beschäftigten ihr eigenes Wissen direkt selber überprüfen können. Die Autorin behandelt: Arbeitsplatzgrenzwerte (AGW)/Luftgrenzwerte, Arbeitsplatzmessungen, Betriebsanweisungen, Biologische Grenzwerte (BGW), CLP-Verordnung/GHS, Einstufung und Kennzeichnung, Fachkunde und Sachkunde, Gefährdungsbeurteilung, Gefährdungszahl bei Flüssigkeiten, Gefahrenermittlung, Gefahrenpiktogramme, Gefahrstoffbeauftragte, Gefahrstoffe, Gefahrstoffverordnung, TGS, BekGS u. a., Gefahrstoffverzeichnis, Gefahrzahlen für Gefahrstoffe, Geruch, H-Sätze (Gefahrenhinweise), Hautresorption, Kennzeichnungselemente nach CLP-Verordnung, Labor, Mengen, Mutterschutz, organisatorische Schutzmaßnahmen, P-Sätze (Sicherheitshinweise), personenbezogene Schutzmaßnahmen (SA), Rangfolgeregelungen bei Kennzeichnungselementen, REACH-Verordnung, Schutzmaßnahmen, Sicherheitsdatenblatt, Signalwort, Substitution, technische Schutzmaßnahmen, Unterweisung, Wirksamkeitskontrolle, Wirkungen.

Geldautomatensicherheit

Die Zeitschrift s+s report weist in der Ausgabe 1-2017, S. 60, auf die VdS 5052 hin. Die Richtlinie beinhalte praxisnahe Tipps gegen alle bekannten Angriffsvarianten mit thermisch oder mechanisch wirkenden Werkzeugen und natürlich auch mit Explosivstoffen, dazu außerdem gegen Manipulationen im und am Automaten oder an den Geräteprozessen. In der Neuauflage finde sich auch eine kompakte Matrix zur Gefährdungsbestimmung für die Automaten anhand von Kernfaktoren wie Standortauswahl, Einbausituation, baulicher und technischer Ausstattung.

Geldwäsche

Das Bundesfinanzministerium verstärkt den Kampf gegen Geldwäsche und Terror-Finanzierung, meldet die FAZ am 5. April. Die „Zentralstelle für Finanztransaktionsuntersuchungen" (Financial Intelligence Unit – FIU) werde unter dem Dach des Zolls neu aufgestellt. Die von 25 auf 165 Beamte aufgestockte Einheit solle zum 1. Juli vom BKA zum Zoll umziehen. Ihre Aufgabe sei es, Hinweise auf Geldwäsche und Terror-Finanzierung entgegenzunehmen und auszuwerten, um die Strafverfolgungsbehörden zu entlasten. Nach der Jahresbilanz des Zolls für 2016 seien mehr als 40.000 Arbeitgeber überprüft und 1.651 Ermittlungsverfahren eingeleitet worden, weil weniger als der gesetzliche Mindestlohn gezahlt worden sei. Der Zoll habe gefälschte Waren im Wert von 180 Mio. Euro aus dem Verkehr gezogen. Darüber hinaus seien 120 Mio. Zigaretten einkassiert worden. Alles in allem weise die Zollbilanz für 2016 mehr als 17.000 Ermittlungsfälle gegen rund 22.000 Tatverdächtige aus.

Industrie 4.0

Security-Aspekte der Digitalisierung thematisiert Dipl.-Ing. Franz Köbinger, Siemens AG, in der Ausgabe 4-2017 der Zeitschrift GIT, S. 88–90. Netzwerke seien die Einfallstore für Hacker und Malware. Wenn alles miteinander vernetzt sei, könne auch alles über das Netzwerk erreicht werden. Die Manipulation von Daten habe vor allem im industriellen Umfeld ein hohes Schadenspotenzial. Die Netzwerke würden zudem „konvergenter". Zunehmende Standardisierung erleichtere zugleich Hackern oder Malware einen Angriff, da sie sich auf weniger Technologie konzentrieren müssten. Bei der Sicherung der Datenübertragung müssten Sender und Empfänger eindeutig identifiziert bzw. authentifiziert werden, die Integrität der

Datenübertragung müsse gesichert und bei Bedarf gegen Spionage und Manipulation durch Verschlüsselung geschützt werden. Ein anderer Aspekt betreffe den Zugriffsschutz von Automatisierung und Netzwerkkomponenten. Insgesamt sei eine mehrschichtige Verteidigung erforderlich (Defense-in-Depth-Strategie). Die Zugänge zu einem Netzwerk würden von Firewalls wie den industrietauglichen Security Appliances der Scalance-S-Produktfamilie kontrolliert. Als zweite Schicht biete sich insbesondere bei größeren Netzwerken die sicherheitstechnische Netz-Segmentierung an. Die nächste Hürde seien die Automatisierungskomponenten selber. Zusätzlich zu Netzwerken und Komponenten müsse die Kommunikation geschützt werden. Die Datenverschlüsselung sei unabdingbar. Eine bewährte Möglichkeit sei die Verwendung von „virtual private network", da hier Sender und Empfänger authentifiziert und die Datenübertragung durch Verschlüsselung gegen Manipulationen geschützt sei. „Security by Design" müsse von Anfang an berücksichtigt werden.

IT-Sicherheit

Stefan Girschner, silicon.de, weist am 28. März auf eine **Cloud-basierte Signaturlösung** für sicheren Datenaustausch hin. Mit einer webbasierten Signaturlösung könnten gerade KMU die Unterzeichnung und den Versand vertrauenswürdiger Dokumente digitalisieren, unabhängig vom jeweiligen Standort der Mitarbeiter. Eine solche webbasierte Lösung habe FP-Mentana-Claimsoft entwickelt. Die Vorteile für den Anwender lägen im Zeitgewinn und dem einfacheren Prozess, Dokumente digital zu signieren. Die webbasierte Lösung nutze für die sichere Datenverarbeitung ausschließlich deutsche Rechenzentren, die vom BSI zertifiziert sind. Alternativ lasse sich die „Software as a service"-Lösung auch über ein Portal ansteuern. Diese Variante sei besonders für KMU attraktiv, weil keine Implementierung erforderlich sei.

Die Zeitschrift s+s report weist in der Ausgabe 1-2017, S. 6/7, darauf hin, dass der GDV bereits 2015 damit begonnen habe, ein unverbindliches Musterbedingungswerk zur **Cyberrisiko-Versicherung** zu entwickeln. Es ermögliche Versicherungsunternehmen, den Versicherungsumfang für ihre Kunden möglichst eindeutig zu beschreiben.

Stefan Bange, Trustwave Deutschland, gibt in der Ausgabe 4-2017 der Zeitschrift GIT, S. 64/65, **fünf goldene Sicherheitsregeln** zum Schutz vor Cyberattacken: Schutz der Sicherheitsinfrastruktur maximieren; regelmäßig Sicherheitstests durchführen; 24 x 7 Security Monitoring installieren; Jagd auf Bedrohungen machen; auf Sicherheitsvorfälle angemessen reagieren. Das Angebot von Trustwave beinhalte vor allem drei Lösungen: Trustwave Secure Web Gateway, eine cloud-basierte Sicherheitslösung; Trustwave WebDefend Web Application Firewall schütze jede Art von Web-Anwendung vor Angriffen, Datenverlusten und DoS-Attacken; Trustwave Network Access Control biete einen kontinuierlichen Schutz des Unternehmensnetzwerks und eine kontinuierliche Überwachung aller Endgeräte.

Nach einem Bericht in der April-Ausgabe des Behörden Spiegel fordern Innenminister EU-Regelungen zum **Umgang mit verschlüsselter Kommunikation**. Internetbasierte Messenger-Dienste fielen gemeinsam mit Webshops, Suchmaschinen und anderen Angeboten unter das Telemediengesetz und unterlägen damit nicht den Vorgaben des TKG hinsichtlich der Pflichten klassischer Telekommunikationsdienstleister gegenüber den Sicherheitsbehörden. Es müsse Ansprechpartner für Ermittlungsbehörden und klare Grundlagen für die Herausgabe von Daten und die Überwachung von Kommunikation geben. Es müssten Lösungen gefunden werden, mit denen verschlüsselte

Kommunikation berücksichtigt und zugleich die Erhältlichkeit starker und zuverlässiger Kryptografie-Systeme gewährleistet werden kann. Künftig sei mit vermehrtem Einsatz staatlicher Trojaner-Softwarfe zu rechnen, die es Ermittlungsbehörden ermögliche, Nachrichten unbemerkt direkt von Geräten abzuschöpfen und mitzulesen, noch bevor sie von der Messenger-Software verschlüsselt und versendet werden. Diese Quellen-TKÜ sei in Deutschland bereits möglich. Technische Möglichkeiten für die Entschlüsselung verschlüsselter Nachrichten zu schaffen, sei Aufgabe der neuen Zentralen Stelle für Informationstechnik im Sicherheitsbereich.

Das Magazin Focus weist am 22. April darauf hin, dass nach einer Studie der Credit Suisse die beiden Bereiche Netzwerksicherheit und Schwachstellenmanagement zu den am schnellsten wachsenden Segmenten gehörten und die Ausgaben für IT-Sicherheit schneller wachsen würden als die für IT-Dienstleistungen. Sie hätten 2016 bei weltweit knapp 82 Mrd. US-Dollar gelegen – Prognose: + acht Prozent pro Jahr.

Der Sicherheitsexperte Marco Rogge plädiert in der Ausgabe 2-2017 von Security insight, S. 52, für **Passwortsicherheit am mobilen Arbeitsplatz.** Eine Möglichkeit zur Verwaltung und Absicherung von Passwörtern seien sogenannte Hardware- oder OTP-Token. Hardware-Token generierten Einmalpasswörter und böten eine Zwei-Faktor-Authentifizierung an. Als Beispiele für Hardware-Token benennt der Autor den RSA SecurID-Token und den Yubikey von Yubico. Im Geschäftsumfeld finde Yubikey immer mehr Anwendung aufgrund seines hohen Sicherheitsstandards und der geringen Anschaffungskosten. Ein Beispielsszenarium sei die Verwendung von Yubikey bei Homeoffice-Arbeitsplätzen. Mit einem OTP-Token würden Passwörter für Hardware, Applikationen und Dienste rund um den mobilen Arbeitsplatz abgesichert.

Die FAZ weist am 28. April auf einen Leitfaden des Bankenverbandes hin, mit dessen Hilfe sich Unternehmen besser gegen die Angriffe aus dem Netz schützen können. Vor allem die Betrugsmethoden, die im Fachjargon **„CEO-Fraud"** heißen, nähmen zu. Unternehmen sollten in jedem Fall ihre Systeme ausreichend schützen, indem sie Firewalls einziehen, Antivirensoftware installierten und alle Programme regelmäßig auf den neuesten Stand brächten. Ganz wichtig sei aber auch, dass die Mitarbeiter entsprechend über die Gefahren informiert würden. „Appellieren Sie an die Aufmerksamkeit Ihrer Mitarbeiter: Jeder ungewöhnliche Sachverhalt sollte mit gesundem Menschenverstand betrachtet werden", schreibt der Verband in der Mitteilung an die Unternehmen.

Zehn aktuelle Problemfelder der Cyber Security beschreibt Prof. Dr. Norbert Pohlmann in der Zeitschrift comply, Ausgabe 1-2017, S. 24–27: zu viele Schwachstellen in Software; ungenügender Schutz vor Malware; keine internationalen Lösungen für Identifikation und Authentifikation; unsichere Webseiten im Internet; neue Gefahren durch die Nutzung mobiler Geräte; eine E-Mail ist wie eine Postkarte; Geschäftsmodell: Bezahlen mit persönlichen Daten; Internetnutzer haben zu wenig Internetkompetenz; manipulierte IT und IT-Sicherheitstechnologien und problematische Rahmenbedingungen: Es gebe noch zu viele Länder, in denen keine Strafverfolgung möglich ist. Und wir haben durch neue Betriebssysteme, neue IT-Konzepte, neue Angriffsstrategien und neue Player im OIT-Markt neue Gegebenheiten und Randbedingungen, auf die wir uns immer wieder sehr schnell einstellen müssen.

IuK-Kriminalität

ControlRisk stellt in einem Hintergrundbericht im ASW-Newsletter am 7. April **Prognosen für die Bedrohung im Cyberspace 2017** auf. 2016 sei ein besonders ereignisreiches

Jahr im Hinblick auf die Bedrohungslage im Cyberspace gewesen. Die Zahl der Einbrüche in Datenbanken sei kontinuierlich gewachsen und die Taktiken der Cyberkriminellen seien immer kreativer geworden. Mit großer Wahrscheinlichkeit würden 2017 Cyberstraftäter ihre kriminellen Aktivitäten zunehmend auf mobile Geräte ausrichten, was teilweise der wachsenden Vernetzung und Funktionalität dieser Plattform geschuldet sei. Die Nachfrage im cyberkriminellen Untergrund, in dem sich in jüngster Zeit das kommerzielle Modell „Crimeware as a Service" etabliert habe, werde die Entwicklung innovativer Malware weiter ankurbeln. Voraussichtlich werde ein besonderer Schwerpunkt auf der Entwicklung von Trojanern im Bereich Online-Banking und mobiler Malware mit einer Bandbreite an Funktionen liegen. So würden Straftäter auch in der Lage sein, die Zwei-Faktor-Authentifizierung über Textnachrichten zu umgehen, was Finanzinstitute dazu zwingen werde, Gegenmaßnahmen zu entwickeln. Ein weiterer Weg für Cyberkriminelle, die wachsende Nutzung von mobilen Geräten finanziell auszubeuten, sei die Manipulation von Technologie für die Near Field Communication. Als Folge der zunehmend sicheren Standards für die Zahlung mit einer physischen Kreditkarte würden Straftäter aller Voraussicht nach ihre eigenen kontaktlosen Bezahlsysteme entwickeln, um aus gestohlenen Kreditkartendaten Kapital zu schlagen. Darüber hinaus werde die poröse Beschaffenheit von App-Stores auf der Android-Plattform dafür sorgen, dass Cyberkriminelle auch weiter versuchen werden, ihre eigenen Apps als Infektionsvektor zu entwickeln, um Geräte zu manipulieren und damit Zahlungen auf ihre eigenen Konten zu tätigen.

Stefan Beiersmann weist in silicon.de am 10. April darauf hin, dass McAfee und FireEye vor einer **Zero-Day-Lücke in Microsoft Word** gewarnt hätten, die bereits für zielgerichtete Angriffe genutzt werde. Angreifer könnten unter Umständen Schadcodes einschleusen und auch auf vollständig gepatchten Systemen ausführen. Von der Schwachstelle betroffen seien alle Office-Versionen bis hin zu Office 2016 unter Windows 10. Exploits seien offenbar schon seit Ende Januar im Umlauf. Die Schwachstelle sei besonders gefährlich, weil sie nicht auf die Aktivierung von Makros angewiesen ist. Die Anfälligkeit stecke in der Funktion Windows Object Linking and Embedding (Windows OLE). Ein speziell präpariertes Dokument im Rich Text Format (RTF) mit doc-Dateiendung könne die Anfälligkeit ausnutzen.

Die FAZ erinnert am 21. April an die Hackerattacke auf die Stadtwerke in Ettlingen 2013. Und sie verweist auf eine Schätzung von Wirtschaftswissenschaftlern, nach der sich der jährliche ökonomische Schaden durch Cyberkriminelle weltweit auf 400 Mrd. Dollar belaufe. In Deutschland habe die Schadensumme 2015 und 2016 mindestens 100 Mrd. Euro betragen. Unter diese Schäden fielen zum Beispiel Plagiate, die Störung von Betriebsabläufen, Patentrechtsverletzungen oder auch Lösegelderpressungen mit gestohlenen Daten. Um sich zu schützen müssten Kommunen, Firmen und Landesregierungen für Beratung und Schutzsoftware immer mehr Geld ausgeben. Es gebe auch einige Probleme, die politisch noch ungelöst seien: So könnten Softwarenutzer die Hersteller für Fehler immer noch nicht zur Verantwortung ziehen, weil das Produkthaftungsgesetz für Computerprogramme nicht gilt. Viele Stadtwerke seien gegen Blackouts nicht versichert, der Grund ist aus Sicht der Versicherungsunternehmen die bisherige „Katastrophenarmut". Das Bewusstsein für die Hackerangriffe sei immer noch unterentwickelt. Mit der Energiewende komme auf die deutschen Städte mit ihren Stadtwerken noch ein Problem zu, das wahrscheinlich größer sei als die derzeitige Gefährdungslage: Es heiße **„Smart metering"**. Die Energiewende führe zur dezentralen Energieerzeugung, aus fünf Produzenten seien mehrere hundert geworden. Jedes Gerät, mit dem an einem Windrad

Daten gemessen und übermittelt werden, sei aber ein neues Scheunentor für die Cyberverbrecher.

Korruption

Der ASW veröffentlicht in seinem Newsletter am 21. April eine Umfrage des Moskauer Meinungsforschungsinstituts Lewada-Zentrum vom März 2017 zum Thema Korruption unter 1.600 Personen in 46 Regionen Russlands. 65 Prozent hätten die Frage nach Korruption in Behörden mit der Aussage beantwortet, dass sie völlig inakzeptabel sei, 24 Prozent hätten gemeint, dass Korruption nicht toleriert werden könne. Auf die Frage, in welchem Maß die Machtorgane korrupt sind, hätten 47 Prozent geantwortet, dass sie in hohem Maße korrupt sind, 32 Prozent festgestellt, dass sie „von oben nach unten" von der Korruption erfasst sind. Für 13 Prozent seien die Machtorgane nur in geringem Maß korrupt. Für 43 Prozent bestünden seit dem Jahr 2000 (Wahl von Putin zum Präsidenten) in der Führung des Landes Diebstahl und Korruption unverändert weiter, 31 Prozent hätten sogar gemeint, dass sie zugenommen haben.

Praktische Auswirkungen des Korruptionsbekämpfungsgesetzes 2015 beschreibt Staatsanwalt Michael Loer in comply, Ausgabe 1-2017, S. 28–31. Die Strafbarkeit nach § 299 ff. StGB sei auf Gegenleistungen für die Vornahme oder eine Handlung des Angestellten oder Beauftragten ausgeweitet worden, durch die dieser seine Pflichten gegenüber dem Arbeit- oder Auftraggeber verletzt. Und der Begriff der „gewerblichen Leistung" sei durch den weiteren Begriff der „Dienstleistung" ersetzt worden. Eine Auslandsbestechung/-bestechlichkeit im geschäftlichen Verkehr sei weiterhin nur dann strafbar, wenn sie eine unlautere Bevorzugung im geschäftlichen Verkehr zum Gegenstand hat und wenn der konkrete Sachverhalt auch im jeweiligen Auslandsstaat einen Straftatbestand erfüllt. EU-Amtsträger seien deutschen Amtsträgern gleichgestellt. Der Vortatenkatalog des § 261 StGB sei erweitert.

Krankenhaussicherheit

Informationssicherheit gemäß VdS 3473 in Krankenhäusern thematisiert Markus Edel, VdS Schadenverhütung, in s+s report, Ausgabe 1-2017, S. 44/45. Das Regelwerk VdS 3473 könne aufgrund seines konsequent generischen Aufbaus auf die meisten Wirtschaftsbranchen angewendet werden. Der Autor behandelt die Themen Zuverlässigkeit und Funktionssicherheit im Gesundheitswesen, besondere Anforderungen an Vertraulichkeit in Krankenhäusern, Komplikationen bei der Systemverwaltung und Sicherheitsupdates und räumliche Anforderungen für Serverräume. Die Vorgaben der Richtlinien VdS 3473 seien dazu geeignet, auch im Krankenhausumfeld ein robustes Schutzniveau für Informationsmanagement zu definieren. Da die Anforderungen der VdS 3473 aufwärtskompatibel mit denen der ISO/IEC 27001 seien, sei die Implementierung eines ISMS gemäß VdS 3473 ein legitimer Schritt auf dem Weg zur Erfüllung der KRITIS-Anforderungen.

Kreditkartensicherheit

Mastercard teste seit längerem Kreditkarten, die die **Authentifizierung durch Fingerabdruck** anbieten, berichtet die FAZ am 22. April. Es sei eigentlich ein Wunder, dass es so lange gedauert hat, bis der Fingerabdruck an der Ladentheke angelangt ist. Man halte die Karte auf das Terminal oder führe sie in das Lesegerät ein und bestätige mit dem Fingerabdruck seine Identität. In Zeiten, in denen an der Supermarktkasse nicht mehr die Zeit besteht, jede Feinheit der Unterschrift

zu überprüfen, sei die eigene Handschrift kein Sicherheitsmerkmal mehr. Der Markt glaube an den Erfolg der neuen Technologie. In Deutschland sei die Deutsche Bank Vorreiter. Sie lasse den Fingerabdruck für Überweisungen via Handy bereits heute schon zu.

Krisenregionen

Eva Nolle, Falkensteyn GmbH, befasst sich in der Ausgabe 2-2017 von Security insight, S. 45/46, mit ethnischen Konflikten in Äthiopien. Ausländische Firmen seien 2016 zum Ziel der Auseinandersetzungen in Äthiopien geworden. Die seit 2015 andauernde Protestwelle der Oromos in Äthiopien habe nicht nur zum Ausruf eines Notstandes geführt, sondern auch zu bürgerkriegsähnlichen Unruhen, sodass viele ausländische Unternehmen immer noch unter Polizeischutz stünden. Gerade das postsozialistische Äthiopien unterhalte einen Überwachungsapparat mit ausgeprägtem Spitzelsystem. Da in Äthiopien nur wenige deutsche Unternehmen seien, sollten sie sich mit anderen internationalen Unternehmen zusammenschließen, um einen Informationsaustausch zu initiieren.

Lebensmittelfälschung

Das Magazin Focus befasst sich am 15. April mit der Lebensmittelfälschung. Längst sei die Mafia in das Geschäft eingestiegen. Das Bundesamt für Verbraucherschutz spreche von Gewinnen wie im Drogenhandel. Im besten Fall seien die Plagiate minderwertig und überteuert. Schlimmer sei es, wenn sie die Gesundheit gefährden. Verbraucher könnten die Gefahr kaum erkennen. Jetzt wollten die Kontrolleure Betrüger mit einer neuen Strategie entlarven. Ihr Mittel sei ein Nachweis für echte Lebensmittel, eine Art Fingerabdruck, der die Zusammensetzung der Inhaltsstoffe umfassend, genau und unverwechselbar darlegt. Damit hätten die Behörden erstmals einen technologischen Vorsprung. Seit 2013 arbeite das Bundesministerium für Ernährung und Landwirtschaft an einer nationalen Strategie gegen Lebensmittelbetrug. Daran beteiligt seien die Überwachungsbehörden der Bundesländer, Euro- und Interpol sowie der Zoll. Zwei Mio. Euro gebe das Ministerium aus, um eine Datenbank mit Fingerabdrücken aufzubauen. Der Laborgerätehersteller Bruker sei vor drei Jahren in das Geschäft eingestiegen. Eine eigene Abteilung lege seither Signaturen für Tausende Varianten von Wein, Saft und Honig an. Mittlerweise habe das Unternehmen die Daten von mehr als 30.000 Fruchtsäften, 19.000 Weinen und 10.000 Honigen. Zu Brukers Kunden zählten Überwachungsbehörden, Lebensmittelkonzerne sowie kleine und mittlere Unternehmen. Besonders viel betrogen werde mit Honig. Er werde oft mit Zuckersirup aller Art gestreckt. Für die 15-minütige Messung würden die Labormitarbeiter die Kernmagnetresonanz-Spektroskopie nutzen. Allerdings könne jedes chemische Analyseverfahren ein unverwechselbares Profil liefern. Mit Hilfe eines DNA-Fingerabdrucks beispielsweise hätten Forscher des Leibniz-Instituts für Zoo- und Wildtierforschung in Berlin vor zwei Jahren einen systematischen Kaviarschwindel aufgedeckt. Die Methode, unverwechselbare Abschnitte herauszupicken, nenne sich DNA-Barcoding. Damit hätten Wissenschaftler des Senckenberg Forschungsinstituts in Wilhelmshaven entdeckt, dass jeder zehnte Fisch nicht dem entspricht, was auf dem Etikett steht. Die Methode eines regionalen Fingerabdrucks beruhe auf einem faszinierenden Prinzip: Etliche Atome in den Inhaltsstoffen der Nahrung gebe es in zwei Varianten, einer schweren und einer leichteren. Und da sich die Erde dreht, sammeln sich die schwereren Moleküle wie bei einer Zentrifuge eher am Äquator. Darauf entstehe eine Karte der Verteilung schwerer und leichter Atome, abhängig von Ort und Klima. Diese Karte offenbare, wenn der Spargel nicht aus Griechenland kommt oder der Wein nicht aus Frankreich.

Lithium-Batterien

Zu den **Gefahren von Lithium-Batterien** und Schutzmöglichkeiten nimmt Dr. Michael Buser, Risk Experts, in der Ausgabe 1-2017 von s+s report, S. 10–13, im Interview Stellung. Die größte Gefahr sei sicherlich der sogenannte „Thermal Runaway". Dabei werde die gesamte Energie einer Batterie nicht kontrolliert als elektrische Energie, sondern unkontrolliert in Form von thermischer Energie abgegeben (explosionsartiges Abbrennen der Batteriezelle). Eine Lithium-Ionen-Batterie könne im Falle des Versagens das ca. Sieben- bis Elffache der elektrisch gespeicherten Energie in Form von thermischer Energie freisetzen. Hinzu komme, dass einige der eingesetzten Kathodenmaterialien aus Übergangsmetall-Oxiden bestehen, die bei hohen Temperaturen zerfallen könnten und somit den chemisch gebundenen Sauerstoff der Oxide freisetzen. Mit konventionellen Löschmethoden seien solche Brände nur schwer beherrschbar. Außerdem könne bei einem Brandereignis die hermetische Kapselung der Batterie beschädigt werden, wodurch brennbare Inhaltsstoffe, aber auch unterschiedliche ätzende, giftige und kanzerogene Stoffe als Brandfolgeprodukte austreten könnten. Zudem bestehe für Rettungskräfte und Wartungspersonal eine Gefahr durch elektrische Spannung und Strom. Auch was die Stromstärke angeht seien die HV-Systeme äußerst gefährlich, da sie kurzzeitig Ströme in der Größenordnung von mehreren hundert Ampere liefern. Weiterhin könnten bei Kurzschlüssen Lichtbögen entstehen, die zu Bränden führen können. Gefährliche Situationen resultierten insbesondere aus fehlerhafter Handhabung und unsachgemäßem Umgang. Neben externen Fehlerquellen könnten auch Fertigungsfehler zu internen Kurzschlüssen führen. Als bauliche Brandschutzvorkehrung habe sich die räumliche und bauliche Abtrennung bei der Lagerung und Handhabung von Lithium-Batterien bewährt. Trotz des offenkundigen Gefahrenpotenzials habe sich bisher kein Löschanlagenkonzept als etablierter Standard durchsetzen können. Eine flächendeckende Brandfrüherkennung sei ein absolutes Muss. Bei Geräten wie Smartphones, Laptops etc. solle unbedingt darauf geachtet werden, sie nicht in der Sonne liegen zu lassen. E-Bikes sollten nicht in Reichweite brennbarer Materialien geparkt oder geladen werden. Der Ladevorgang sollte überwacht werden. Die neuen Hochleistungsbatterien verlangten mit der Zunahme an Energiedichte und Kapazität innovative und wirksame Sicherheitskonzepte.

Logistiksicherheit

Frachtdiebstähle behandelt Thomas Schuster in der Ausgabe 2-2017 von Security insight, S. 18/19. Der Transportsicherheitsvereinigung Tapa seien 2016 insgesamt 2.611 Frachtdiebstähle in 34 Ländern der Regionen Europa, Naher Osten und Afrika bekannt geworden. 86,5 Prozent der Delikte seien auf nur vier Länder entfallen: Großbritannien, Niederlande, Deutschland und Schweden. Frachtenbörsen würden immer häufiger benutzt, um auf kriminelle Weise an wertvolle Ladung zu kommen. Vorsicht sei dann geboten, wenn ein Auftrag über eine Online-Frachtenbörse vergeben werden soll und sich die Partner nicht persönlich kennen. Ladungsunterschlagungen über Frachtenbörsen bedürften einer strategischen Vorbereitung und trügen die Handschrift gut organisierter Tätergruppen. Der jährliche Schaden werde mit über 8,5 Mrd. Euro beziffert. Erfolge die Kontaktaufnahme über eine Mobilfunknummer, sollte dies ein erstes Warnsignal sein. Der zweite Indikator seien E-Mail-Adressen von kostenlosen Anbietern. Professionelle Transportunternehmen hätten eine eigene Domain. Mittels Google-Earth könne man erkennen, ob unter der angegebenen Anschrift eine Transportfirma über ein entsprechendes Gelände verfügt, oder ob es sich um ein Wohngebiet handelt. Ein absolut notwendiger Teil der Auftragsver-

gabe bestehe darin, dass der Disponent sich alle notwendigen Papiere vorlegen lässt. Ein weiterer Sicherheitsschritt sei die Prüfung von Qualität und Layout der Dokumente. Schlechte Qualität der Dokumente sei meist das Ergebnis einer Fälschung. Vorsicht geboten sei bei Dumpingangeboten und wenn der Subunternehmer seine Tour auf einen Zeitraum direkt vor ein verlängertes Wochenende legt.

Gernot Dähne, DeDeNet GmbH, erläutert in Ausgabe 2-2017 von Security insight, S. 25/26, **GPS-Tracking** als Schutz für Fuhrpark und Fahrer. 2015 seien in Deutschland 1.605 Lkw entwendet worden. Es belege europaweit den zweiten Platz hinsichtlich gestohlener Ladung. Die Schadenssumme habe zuletzt 1,5 Mrd. Euro betragen. Die Transportmanagement-Software DeDeFleet der DeDeNet GmbH biete zum Beispiel Funktionen wie Diebstahlschutz, Echtzeitortung und die Kontrolle der Lenk- und Ruhezeiten. Erfahrungen machten deutlich, dass der Einsatz eines Ortungsgerätes der effektivste Diebstahlschutz sei. DeDeFleet werde per Schnittstelle in die meist schon vorhandene Standard-Transportmanagementlösung integriert. Die Telematiklösung ermögliche eine detaillierte Streckenansicht und eine Live-Verfolgung des Fahrzeugs. Das unbefugte Starten des Lkw und das Verlassen des Abstellortes seien an ein Alarmsystem gekoppelt, das den Spediteur benachrichtige und ihm via GPS-Daten ein schnelles Orten des gestohlenen Lkw ermögliche.

Luftverkehrssicherheit

Wie der Mannheimer Morgen am 1. April meldet, haben Terrororganisationen nach Erkenntnissen von US-Ermittlern Methoden entwickelt, um Sprengsätze in Laptops und anderen elektronischen Geräten zu verbergen. Der Sprengstoff werde möglicherweise von den Scannern bei der Sicherheitskontrolle an Flughäfen nicht entdeckt.

Maschinensicherheit

Den **Weg zur sicheren Mensch-Roboter-Kollaboration** (MRK) schildert Jochen Vetter, Pilz GmbH & Co. KG, in GIT, Ausgabe 4-2017, S. 92–95. Wesentliches Unterscheidungsmerkmal zwischen „klassischen" umhausten Roboterapplikationen und MRK sei, dass Kollisionen zwischen Maschine und Mensch ein reales Szenario sein können. Sie dürften ausdrücklich jedoch zu keinen Verletzungen führen. Voraussetzungen für ein sicheres Miteinander seien zum einen zuverlässigere Steuerungen und intelligente, dynamische Sensoren am Roboter selbst. Mit der Technischen Spezifikation ISO/TS 15066 könnten nach entsprechender Validierung sichere MRK umgesetzt werden. In ihr seien vier Kollaborationsarten als Schutzprinzipien genauer beschrieben: sicherheitsbewerteter überwachter Stillstand; Handführung; Geschwindigkeits- und Abstandsüberwachung sowie Leistungs- und Kraftbegrenzung. Die Herausforderung bei schutzzaunlosen Roboterapplikationen bestehe darin, dass sich die Grenzen der beiden Arbeitsbereiche von Mensch und Maschine auflösen. Der Autor beschreibt die zentrale Rolle der Validierung. Im Anhang A der ISO/TS 15066 werde ein Körpermodell mit 29 spezifischen, in zwölf Körperregionen eingeteilte Körperbereiche, aufgeführt. Das Modell mache zu jedem Körperteil eine Angabe zu den jeweiligen Belastungsgrenzwerten mit Blick auf Kraft und Druck. Letztlich sei die sichere MRK-Applikation das Ergebnis des Zusammenspiels normativer Rahmenbedingungen, einer darauf aufbauenden komplexen Risikoanalyse, der Auswahl eines Roboters mit den entsprechenden Sicherheitsfunktionen, der Auswahl der passenden, zusätzlichen Sicherheitskomponenten und schließlich der Validierung.

Andreas Schenk, steute Schaltgeräte GmbH & Co. KG, befasst sich in GIT, Ausgabe 4-2017, S. 96/97, mit der **Sicherheit an**

Umformanlagen. Zustimmschalter gehörten zu den typischen Mensch/Maschine-Schnittstellen an Gesenkbiegepressen, Schwenkbiegeanlagen und anderen Anlagen der Umformtechnik. Neuerdings könnten die Hersteller und Anwender von Pressen für diese Aufgabe kabellose Fußschalter einsetzen, die dem Bediener verbesserte Ergonomie und größere Bewegungsfreiheit ermöglichten.

Die **Sicherheit der Schweißzelle** behandelt die Zeitschrift GIT in der Ausgabe 4-2017, S. 98–100. Die von der Firma Guttroff produzierte mobile Schweißroboterzelle bilde eine vollständig abgeschlossene und abgesicherte Einheit. Die optoelektronischen Sicherheitssysteme der Serie SLC420 des Unternehmens Schmersal seien sehr robust, da Sender und Empfänger in zwei geschlossenen Sensorprofilen integriert sind. Zugänglich sei die Schweißzelle nur über eine Tür, die während des Betriebs mit der Sicherheitszuhaltung AZM300 von Schmersal verriegelt ist. Zu den besonderen Merkmalen des AZM300 gehöre das neuartige, patentierte Wirkprinzip mit Drehwelle und Drehkreuz.

Museumssicherheit

PROTECTOR stellt in der Ausgabe 4-2017, S. 25, die „Museumslösung" Sedor Art vor, eine Analyse-Applikation für die Software DVS Analysis Server, für die Überwachung von Kunstwerken in Ausstellungsräumen konzipiert. Neben der Video-Komplettlösung aus Außen- und Gemäldeabsicherung, automatischer Aufschaltung auf eine Wachzentrale und einem intuitiven Videomanagementsystem mit integrierten Lageplänen seien auch zahlreiche Anbindungen möglich. So könnten beispielsweise Drittsysteme zur Berührungsdetektion und Alarmierung über Onvif und andere Integrationsprotokolle mit Videobeobachtungsanlagen verbunden werden. Die Analyseform „unzulässige Annäherung/Berührungsschutz" sei unempfindlich gegenüber Schattenwurf und normalen, tagesablaufbedingten Lichtschwankungen. Angezeigt würden zum Beispiel auch unbeaufsichtigte Gepäckstücke in den Ausstellungsräumen.

Notausgangssicherheit

Mit alarmgesicherten Türen befasst sich PROTECTOR in der Ausgabe 4-2017, S. 49. Viele Betreiber, die Notausgänge in sensiblen Bereichen gegen unbefugtes Begehen absichern möchten, würden sich für technische Lösungen mit akustischer Alarmierung entscheiden. Exitalarm eigne sich insbesondere für die Absicherung von Einzeltüren, die sich im näheren Umfeld von Personal befinden. Es handele sich um ein Gerät mit Überwachungshebel, das mit deutlichen akustischen Signalen über eine Aktivierung informiert; zunächst über einen Voralarm, der bei unberechtigter Betätigung davon abhalten soll, den Drücker komplett durchzudrücken. Über Fluchtwegterminals könne die verriegelte Tür von innen problemlos mit dem Schlüssel am Terminal und von außen am Schlüsselschalter freigegeben werden, ohne dass ein akustischer Alarm ausgelöst wird.

Panik

Professor Michael Schreckenberg, Universität Duisburg-Essen, behandelt in s+s report, Ausgabe 1-2017, S. 50–54, das Phänomen Panik. Er befasst sich zunächst mit dem Panik-Begriff und der Entstehung einer Panik. Untersuchungen hätten ergeben, dass unterhalb einer Durchgangsbreite von 70 cm der Durchfluss unter Druck deutlich geringer werde als bei kooperativem Verhalten. Eine testweise und mehrmalige Durchführung einer Evakuierung einer Massenveranstaltung sei praktisch nicht möglich. Der Autor geht dann auf Zuständigkeiten und Kommunikation ein. Von ganz entscheidender Bedeutung sei,

wer die Situation beurteilt, welche Informationen dieser Person vorliegen, wie schnell diese übermittelt werden können, welche Handlungsmöglichkeiten überhaupt zur Verfügung stehen. Aus den bekannten Katastrophen könne man auch lernen, dass auf die Kommunikation kein Verlass ist. Ein wichtiges Maß zum Erkennen potenzieller Problemsituationen seien zu erwartende hohe Personendichten (über zwei Personen/qm) über einen längeren Zeitraum (ca. 15 Sekunden) bei zugleich eingeschränkter Geometrie und/oder Wahrnehmung möglicher Fluchtwege. Prof. Schreckenberg stellt fünf Möglichkeiten vor, um sich nach heutigem Verständnis optimaler Sicherheit zumindest zu nähern: Beurteilung durch einen Experten, Evakuierungstests, Analyse von Videoaufnahmen, Tierexperimente und Simulationen. Ganz aktuell seien wahrscheinlich „Fake News" eines der größten unterschätzten Probleme. In der Prävention müsse sehr viel mehr auf mögliche Begehrlichkeiten der Menschen geachtet werden. Die könnten unvermittelt zu Druck und hohen Dichten führen.

Polizeiliche Kriminalstatistik (PKS) 2016

Am 24. April haben Bundesinnenminister de Maizière und der Vorsitzende der IMK die PKS 2016 vorgestellt. 6.372.526 Straftaten wurden in Deutschland 2016 polizeilich registriert. Gegenüber dem Vorjahr bedeutet das einen Anstieg um 0,7 Prozent. Die Häufigkeitszahl (Straftaten pro hunderttausend Einwohner – HZ) sank von 7.797 auf 7.755 Fälle. Ohne ausländerrechtliche Straftaten waren es 5.885 Mio., und die HZ ging gegenüber 2015 um 1,9 Prozent zurück. Die Gesamtaufklärungsquote lag bei 56,2 Prozent (2015: 56,3 Prozent). Wie in den Vorjahren dominierten auch 2016 die Diebstahlsdelikte, und zwar mit 37,3 Prozent. Wohnungseinbruchdiebstahl, der von 2006 bis 2015 um insgesamt 57,5 Prozent besorgniserregend angestiegen war, ging 2016 gegenüber dem Vorjahr um 9,5 Prozent auf 151.265 Fälle zurück. Das waren aber immer noch 414 Fälle durchschnittlich pro Tag. Signifikant zugenommen haben 2016 gegenüber 2015 die Gewaltkriminalität (um 6,7 Prozent) auf 193.542 Fälle, die Rauschgiftkriminalität (um 7,1 Prozent auf 302.594 Delikte) und Straftaten gegen das Waffengesetz (um 14,8 Prozent auf 34.443 Fälle). Signifikant abgenommen hat die Wirtschaftskriminalität (um 5,6 Prozent auf 57.546 Fälle). Die Kriminalitätsbelastung war 2016 wie im Vorjahr am größten im Land Berlin (HZ 16.161), am geringsten in Baden-Württemberg (HZ 5.599). Unter den Großstädten ab 200.000 Einwohner war Frankfurt am Main am stärksten (HZ 10.550), München am geringsten belastet (HZ 7.909). Eine ausführlichere Zusammenfassung – insbesondere zu den die Wirtschaft besonders belastenden Kriminalitätsphänomenen – findet sich auf der Webseite von Securitas Deutschland (Presse/Sicherheitslage).

Produktpiraterie

Peter Niggl, Security insight, befasst sich in der Ausgabe 2-2017, S. 42–44, mit Produkt- und Markenpiraterie. Von Produktpiraten auf den Markt gebrachte Smartphone-Fälschungen verursachten jährlich einen Schaden von mehreren Milliarden Euro. Smartphone-Hersteller hätten 2015 laut einer Studie des EU-Amts für geistiges Eigentum und der Internationalen Fernmeldeunion wegen parallel verkaufter 14 Mio. Imitate 4,2 Mrd. Euro Umsatz verloren. Die Zahl der kriminellen Organisationen mit OK-Hintergrund sei in der EU von 2013 bis 2016 von 3.600 auf 5.000 gestiegen. Immer mehr Plagiatverkäufer tummelten sich unter den Online-Händlern. Die 470 mutmaßlichen Fälschungen, die das Hauptzollamt Darmstadt auf der Konsumgütermesse Ambiente im Februar 2017 sichergestellt habe, sei noch nicht einmal die Spitze

des Eisbergs. Auf der diesjährigen Ambiente seien mehr als doppelt so viele Plagiate wie 2016 gefunden worden. In der Aufzählung der Herkunftsländer rangiere bei den Zöllnern hinter China die Türkei auf Platz zwei.

Rechenzentrumssicherheit

Die neue **Normenreihe EN 50600** für Rechenzentren behandelt Lance Rütimann, Siemens Building Technologies, in s+s report, Ausgabe 1-2017, S. 55–57. Die seit 2012 sukzessive veröffentlichte Normenreihe „Einrichtungen und Infrastrukturen von Rechenzentren" schaffe erstmals einen verlässlichen Rahmen für Planung, Gebäudekonstruktion, effiziente Energieversorgung, Klimatisierung, Sicherheitstechnik sowie Management und Betrieb. In Deutschland setze die DIN EN 50600 die europäischen Vorgaben um und definiere sie als „Regel der Technik". Der Autor gibt Tipps für die Einführung und Umsetzung. Die Normenreihe sei als Leistungsvorgabe zu verstehen und lasse viel Raum für Innovation. Für den Schutz des Rechenzentrums gebe es vier Schutzklassen für die Kriterien Zugangskontrolle und Brandschutz. Mit einer normgerecht aufgestellten Infrastruktur, wie sie die DIN EN 50600 beschreibe, würden Unternehmen die Sicherheit gewinnen, dass ihr Rechenzentrum sowohl bedarfsgerecht verfügbar und geschützt als auch energieeffizient ist. Und sie würden das Potenzial für Verbesserungen erkennen.

Die Normenreihe EN 50600 ist auch Thema des Beitrags von Dipl.-Ing. Thomas Grüschow in der Ausgabe 4-2017 der Zeitschrift GIT, S. 60–62. Während eine Fülle von Leitlinien zur Infrastruktur von Rechenzentren die wichtigsten Aspekte – das Geschäftsrisiko und die konkreten Geschäftsziele – vermissen ließen, rücke die DIN EN 50600 diese Punkte ins Zentrum. Die Norm definiere nicht nur vier Schutzklassen, sondern auch vier Verfügbarkeitsklassen zur Prüfung, welche in den jeweiligen Gewerken notwendig sind, um das Geschäftsziel kosteneffizient zu erreichen. Stünden die Geschäftsrisikoanalyse und das Sicherheitskonzept, dann liefere dies valide Eingangsdaten für die effektive Anwendung diverser Managementnormen wie die ISO 20000, ISO 27001 und ISO 50001. Die Norm helfe, wichtige Leistungsindikatoren wie Ausfallraten oder Reparaturzeiten zu ermitteln. Die Qualität des Energiemanagements nach ISO 50001 werde gesteigert, weil definierte Messpunkte nach DIN EN 50600 valide Werte liefern. Sie biete erstmals eine einheitliche Grundlage für alle, die am Aufbau und Betrieb eines Rechenzentrums beteiligt sind.

Risikomanagement

Carl Ebelshäusere, Lloyds Register Deutschland GmbH, sieht im Risikomanagement den Schlüssel für eine erfolgreiche Zukunft (Security insight, Ausgabe 2-2017, S. 47/48). Die rechtliche Grundlage werde durch das KonTraG beschrieben. Es zwinge Organe von AGs und größeren GmbHs zu einem dokumentierten Risikomanagement. Mit der ISO 31000 stehe erstmals ein internationaler Leitfaden für das Risikomanagement zur Verfügung. Dass eine neue Firmenkultur der Risikolenkung entstehen solle, komme auch in der Überarbeitung der ISO 2001:2015 zum Ausdruck. Der Lieferantenaudit oder auch Kundenaudit sei eine Sonderform des Audits bestimmter Fragmente oder des gesamten Managementsystems einer Organisation. Der Lieferantenaudit könne sich zum Beispiel auf einzelne technische oder organisatorische Bereiche des Lieferanten beschränken. Um Risiken in Chancen zu verwandeln, bestehe der erste Schritt darin, die Sicherheitsrisiken der eigenen Lieferkette zu erkennen. Das Lloyds Register Managementsystem LRQA liefere mit der risikobasierten Auditmethodik die richtigen Methoden und Werkzeuge. Es sei weltweit

führend bei der Zertifizierung nach ISO 28000 (Sicherheit in der Lieferkette) sowie nach ISO 27001 (IT-Sicherheit). Der Autor beschreibt in acht Schritten die Einbeziehung der Mitarbeiter in das BCM-System. Für das BCM sei die ISO 22301 ein anerkanntes Zertifikat nach dem internationalen ISO-Standard.

Schließsysteme

Nicolas Stobbe, Deister Electronic, nimmt in der Fachzeitschrift GIT, Ausgabe 4-2017, S. 50–53, im Interview Stellung zur **digitalen Schließtechnik**. Der Feldstärke-Anzeiger POC sei ein kleines Produkt mit großer Wirkung. Der leuchte nur dann auf, wenn die gemessene Feldstärke auch stark genug ist für einen Transponder. Die digitalen Schließkomponenten seien von Deister so entwickelt worden, dass man die Lesertechnik in Form einer Leserkappe auswechseln kann, weil sie vom Rest getrennt verbaut ist.

IP-basierte Systeme für die umfassende physische Sicherheit thematisiert PROTECTOR in der Ausgabe 4-2017, S. 34/35. Durch die Integration von Zutrittskontrolle und Videoüberwachung auf einer einheitlichen **Management-Plattform** könne die Betriebseffizienz und Sicherheit weiter gesteigert werden. IP-basierte Infrastrukturen ermöglichten in Verbindung mit angepassten Management-Plattformen die vollständige Integration der gesamten physischen Sicherheit in einem einzigen, zentral verwalteten, System. Aufgrund der hohen Skalierbarkeit und einfachen Modifikation könnten auch zukünftige Anforderungen zuverlässig abgedeckt werden. Wesentlich wichtiger als bei herkömmlichen, analogen Systemen sei aber der Schutz der Infrastruktur: Hier müssten private und öffentliche Organisationen bei der Wahl von Hardware und Management-Plattform von Anfang an die richtigen Weichen stellen.

Sicherheitsarchitektur

Manfred Buhl, Securitas Deutschland, begrüßt in Security insight, Ausgabe 2-2017, S. 32–35, die Visionen von Bundesinnenminister de Maizière für eine neue Sicherheitsarchitektur. Sie betreffen die Steuerungsfunktionen des Bundes, den Verfassungsschutz, den Schutz vor Cyberangriffen, die „Polizei des Jahres 2020", eine Verbesserung der Fahndungsmöglichkeiten und den Katastrophenschutz. Zwei Säulen der Architektur der Inneren Sicherheit lasse der Minister allerdings unerwähnt: die Sicherheitswirtschaft und die Unternehmenssicherheit. Der Autor beschreibt fünf Zielrichtungen einer Vision 2020 des Sicherheitsgewerbes: Entwicklung zu einer exzellenten Wirtschaftsbranche, Entwicklung zu einem strategischen Partner der mittelständischen Wirtschaft, Digitalisierung, Optimierung der Kooperation mit der Polizei und Unterstützung der kommunalen Ordnungsdienste. Zu prüfen sei auch eine Reihe von gesetzlichen Verbesserungsmöglichkeiten für das Verfahren der Vergabe öffentlicher Aufträge, die im einzelnen benannt werden.

Sicherheitsgesetze

Dass der Bundestag am 27. April neue Sicherheitsgesetze beschlossen hat, meldet die FAZ am 28. April. So sei eine Reform des BKA-Gesetzes beschlossen worden, die für eine grundlegende Modernisierung der polizeilichen IT-Systeme sorgen solle und für die Abschaffung von Doppelstrukturen in den Computersystemen der Länder. Ein übergreifendes Informationssystem beim BKA werde es ermöglichen, Informationen, die „phänomenübergreifend" zusammengehörten, auch zusammenzuführen. Zudem ist künftig der Einsatz sogenannter elektronischer Fußfesseln bei Gefährdern erlaubt. Allerdings gilt die Regelung im BKA-Gesetz nur für Gefährder,

die auf der Bundesebene geführt werden. Die Bundesregierung hoffe, dass die Länder entsprechende Gesetze verabschieden. Der Bundestag beschloss zudem einen besseren Schutz für Polizisten und Rettungskräfte. Wer diese oder andere Amtsträger schon bei sogenannten allgemeinen Diensthandlungen wie einer Streifenfahrt angreift, müsse künftig mit einer Haftstrafe von bis zu fünf Jahren rechnen.

Sonderschutzfahrzeug

PROTECTOR berichtet in der Ausgabe 4-2017, S. 72, über das Fahrzeugkonzept „MSS – Mobile Screening Systems", das entwickelt worden sei, um eine „hundertprozentige" Personen- und Gepäckkontrolle mit hoher Durchflussrate auf Basis schneller Scan-Vorgänge bei der Absicherung großer Menschenmengen zu ermöglichen. Das Fahrzeugkonzept sei variabel gestaltet, aber auch gleichzeitig standardisiert aufgebaut, sodass alle Eventualitäten mit einem Bautyp abgewickelt werden könnten. Die Kombination von Transmission X-Ray oder Metalldetektion, optional verfügbaren X-Ray-Gepäckscannern, Gammadetektionsgeräten sowie Sprengstoff- und Flüssigkeitsdetektion ermöglichten Kontrollen zu den weltweiten Sicherheitsstandards. Die zu kontrollierenden Personen und Gepäckstücke würden im Wagen durch begehbare Slots gescannt.

Spielhallensicherheit

PROTECTOR stellt in der Ausgabe 4-2017, S. 26/27, die GPU-beschleunigte Bildverarbeitung im Casino vor. Kern des Sicherheitssystems von Geutebrück sei das Security Information Management System G-SIM, das Bedienung und Administration aller Komponenten und Subsysteme bereitstelle. Die Bildverarbeitung für Videoanalyse und Wiedergabe sei GPU-beschleunigt – und damit dreimal schneller als üblich. Auch extrem hohe Auflösungen würden flüssig dargestellt. Es gebe eine weitere Entwicklung, die über eine reine Beobachtung des Spielbetriebs hinausgehe. Dabei handele es sich um die intelligente Verknüpfung und Aufbereitung von Kassen-, Spielsystem-, Cash-Management- und Videodaten, welche dem Anwender eine zusätzliche Perspektive böten und eine detaillierte Analyse der Abläufe im Casino ermöglichten. Durch eine optimale Unterstützung des Bedienpersonals ließen sich Unregelmäßigkeiten und Anomalien frühzeitig erkennen.

Spionage

Nach einer Meldung der FAZ vom 8. April haben niederländische Strafermittler einen Mitarbeiter von Siemens Niederlande festgenommen, der unter dem Verdacht stehe, Industriespionage für China betrieben zu haben. Der deutsche Technologiekonzern habe den Vorfall bestätigt. Die FAZ berichtet, bei Siemens Niederlande, einer reinen Vertriebsgesellschaft, gebe es weder nennenswerte Produktionsaktivitäten noch Forschung und Entwicklung. Allerdings habe auch vom Ausland aus ein Siemens-Mitarbeiter Zugang zu dem umfassenden Netzwerk im Konzern, in dem unter Umständen für Externe und Unbefugte durchaus interessante und sensible Informationen abgegriffen werden könnten.

Terrorismusfinanzierung

Die FAZ weist am 25. April auf ein Buch des ehemaligen Sicherheitschefs von Lafarge in Syrien hin, in dem er beschreibt, wie er im Herbst 2012 eine sechsstellige Summe übergeben hat, um neun entführte Mitarbeiter freizukaufen. Das Geld dürfte über Umwege in den Händen der Terrormiliz

„Islamischer Staat" gelandet sein. Gleiches gelte für Schutzgelder und Wegezölle, die dafür berappt worden seien, dass Rohmaterialien in die Fabrik geliefert und Zementprodukte an Kunden in der Region ausgeliefert werden konnten. Vor diesem Hintergrund ermittele die französische Justiz wegen des Verdachts der Terrorfinanzierung.

Überspannungsschutz

Die neuen Anforderungen der DIN VDE 0100-443 und DIN VDE 0100-534 behandelt Dipl.-Ing. Holger Heckler, Trabtech Phoenix Contact GmbH & Co. KG, in GIT, Ausgabe 4-2017, S. 102–104. In diesen Normen gehe es um den Schutz vor transienten Überspannungen und um die Auswahl und Errichtung von Überspannungs-Schutzeinrichtungen (surge protective devices, SPDs). Aufgrund der im Oktober veröffentlichten Neuerungen müssten der Planer und der Elektroinstallateur einiges beachten. Die SPDs müssten gemäß DIN VDE 0100-443 installiert werden. Sie müssten so ausgewählt und errichtet werden, dass die Spitzenspannung bzw. der Verlauf der Spannung bei der Ableitung von Stoßspannungs- und Stoßstromimpulsen stets niedriger ist als die Bemessungsstoßspannung des zu schützenden Betriebsmittels. Der Autor befasst sich mit Anschlussschemata, Leitungslänge zwischen SPD und Betriebsmittel, Anschlussleitungen, Überstrom-Schutzeinrichtungen und Anlagen mit erhöhtem Sicherheitsbedürfnis.

Veranstaltungsordnungsdienst (VOD)

Für einen professionellen Veranstaltungsordnungsdienst plädiert der BDSW in Security insight, Ausgabe 2-2017, S. 51. Das gegenwärtig angewandte Unterrichtungsverfahren bzw. die Sachkundeprüfung nach § 34 a GewO werde der Vielfalt der durchgeführten Tätigkeiten nicht gerecht. Die starren, inhaltlich nicht hilfreichen Regelungen sollten durch angepasste Qualifikationsmodule ersetzt werden, die viel stärker als bisher nach Sicherheits- und Ordnungsaufgaben differenzieren. Der Gesetzgeber verlange zwar in der Muster-Versammlungsstättenverordnung den Einsatz von Ordnungsdiensten, habe diese aber nicht ausreichend definiert. Es müsse klargestellt werden, dass reine Ordnungsaufgaben nicht dem § 34 a GewO unterliegen.

Videoüberwachung

Über den Einsatz der Videoüberwachung zur Sicherung von Produktionsabläufen im **Kieswerk** berichtet GIT in der Ausgabe 4-2017, S. 40/41. Durch die Installation von insgesamt 13 Abus IP-Tube-Außenkameras an kritischen Stellen der Produktion im Innen- und Außenbereich werde ein reibungsloser Produktionsablauf ermöglicht. Aufgrund der Nachtsichtfunktion lieferten die Kameras, die unter anderem auch in Unterführungen und an dunklen Stellen der Maschinenhalle hängen, selbst unter schwierigen Lichtverhältnissen gestochen scharfe Bilder in Full-HD-Qualität. Zusätzlich zur Qualitätsüberwachung dienten die Kameras dem schnellen Erfassen von Störmomenten.

Die Fachzeitschrift GIT stellt in der Ausgabe 4-2017, S. 44/45, das **Videomanagement- und Logistiksystem für DPD Frankreich** vor. Die Videomanagement-Software der Cayuga-Produktreihe von SeeTec sei im Falle der DPD-Depots um das BVI-Logistics-Modul mit Scanner-Schnittstelle ergänzt worden. Außerdem kämen in beiden Depots I/O-Module zum Einsatz, die das Senden und Empfangen von Steuersignalen ermöglichen. Auf Basis dieser Software würden nun alle Förderbänder, die Ein- und Ausfahrtstore sowie der gesamte Innenraum mit 280 HD-Kameras am Standort Tours und 380 in

Beaune überwacht. So werde der gesamte Prozess der Paketabwicklung von der Anlieferung über die Sortierung nach dem Zielort bis zur Übergabe an den Zusteller nahtlos dokumentiert. Die Daten der Videosysteme würden zur detaillierten Auswertung mit den Daten der zahlreichen Barcodescanner an den Förderbändern kombiniert. So könne ermittelt werden, zu welchem Zeitpunkt sich jedes einzelne Paket an welcher Stelle im Verteilzentrum befand. Insgesamt seien bei der Überwachung der Förderbänder 61 Scanner installiert, die die Barcodes aus fünf Blickwinkeln auslesen. Der BVI Client ermögliche eine zielgerichtete Recherche ohne stundenlanges Durchsuchen von Videomaterial und sei deshalb perfekt geeignet, um Verluste oder Beschädigungen schnell aufzuklären.

Rechtsanwalt Dr. Ulrich Deckert geht in Teil 2 seiner Beurteilung von Rechtsfragen bei der **Baustellenüberwachung** in der Ausgabe 4-2017 von GIT, S. 20–22, auf den Beschäftigtendatenschutz und Rechte am Bild ein. Haben sich die auf der Baustelle tätigen Arbeitnehmer mit der Bilddatenerfassung schriftlich einverstanden erklärt, dann könne der Betreiber sich hierauf als Rechtfertigungsgrund berufen. Um Streit mit den Arbeitnehmern von vornherein zu vermeiden, sollte der Betreiber von Bilderfassungssystemen auf Baustellen seine Beschäftigten bereits im Vorfeld über den Einsatz, die Funktionsweise und den Umfang der Maßnahmen informieren. Verfügt das Unternehmen über einen Betriebsrat, so sollte frühzeitig der Abschluss einer Betriebsvereinbarung angestrebt werden. Die sanktionslose Verbreitung von Videobildern sei nur zulässig, wenn der Betroffene eingewilligt hat. Die Einwilligung setzt die Kenntnis des Betroffenen von Zweck, Art und Umfang der geplanten Verwendung der Bilder voraus. Nach der Ausnahmevorschrift des § 23 Abs. 1 Nr. 2 KUG dürfen solche Bilder ohne die nach § 22 erforderliche Einwilligung verbreitet werden, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeiten erscheinen. Steht die Identifizierung von Personen durch Videoüberwachung im Mittelpunkt der Anwendung, sodass man von Beiwerk nicht mehr sprechen könne, dürften die Aufnahmen bei einer grundrechtlich gebotenen Güterabwägung in der Regel zulässig sein, weil die schutzwürdigen Interessen des Betreibers bei maßvollem Einsatz der Videotechnik überwiegen. Der Autor weist auch auf den besonderen rechtlichen Schutz von Baulichkeiten als solche nach § 59 UrhG hin. Allerdings gelte für die vom Straßenrand zugängliche äußere Ansicht gemäß § 59 Abs. 1 „Panoramafreiheit". Werden Gebäude hingegen von Balkonen, Dächern oder aus der Luft fotografiert, dann könne dies eine Urheberrechtsverletzung darstellen. Die Bilderfassung auf Baustellen sei von diesen Vorschriften dann berührt, wenn Aufnahmen in einem Bildband zusammengefasst werden, der zu werblichen Zwecken verbreitet wird.

Wie der Behörden Spiegel in der April-Ausgabe berichtet hat sich neben Köln auch Essen für den Einsatz der patentierten **Panomera-Technologie** entschieden. Das Multifocal-Sensorsystem sei insbesondere für die flächendeckende Absicherung weitreichender Areale entwickelt worden. Mit Panomera würden enorme Weiten und auch Flächen mit großen Distanzen in einer vollkommen neuen Auflösungsqualität dargestellt, und zwar in Echtzeit und bei hohen Frameraten von bis zu 30 Bildern pro Sekunde. Die installierten Kameragehäuse, die mit bis zu acht Objektiven ausgestattet seien, ersetzten bis zu 30 Einzelkameras.

In der Ausgabe 4-2017 der Zeitschrift PROTECTOR, S. 14/15, wird die Funktionsvielfalt der neuen **Wisenet X-Serie** vorgestellt. Diese umfasse 26 neue Zwei- und Fünf-Megapixelkameras mit H 265-Übertragung, die vom bis jetzt stärksten integrierten Chipsatz versorgt würden. Zu den vielfältigen Features gehörten die Wide-Dynamic-Range-Technologie ohne Bewegungsunschärfe, leistungsstarkes Low-Light, um eine bis zu 99

Prozent reduzierte erforderliche Bandbreite, zwei SD-Kartensteckplätze für bis zu 512 GB Speicherplatz, Gyrosensoren für akkurate Stabilisierung bei Wind und Erschütterungen sowie Audioanalysefunktion zur Erkennung kritischer Geräusche.

Gabriel Chaher, Quantum Corporation, stellt in PROTECTOR, Ausgabe 4-2017, S. 32/33, sieben **Tipps von Video-Profis zur intelligenten Datensicherung** vor. Durch zunehmend mehr Kameras mit höheren Auflösungen und langen Vorhaltungszeiten der Aufnahmen zu Analysezwecken stoße die vorhandene Speicherinfrastruktur sehr schnell an ihre Grenzen. Doch es gebe Lösungen, die der Autor beschreibt: Storage-Ausgaben durch Datenmanagement senken; einfachen und schnellen Datenzugtriff; hohe Performance; Speicherkapazitäten an Bedarf anpassen; Lösungen in bestehende Infrastruktur integrieren; Speicherlösung kompromisslos auswählen und Gateway-Speicherarchitektur: Durch flexible, kostengünstige Einstiegslösungen für die Archivierung, die bei steigendem Bedarf auf mehrere Petabyte skaliert werden könnte, lasse sich die Speicherkapazität durch neue Speicherebenen wie Tape, Cloud oder Scale-out Storage aufstocken, ohne vorhandene Systeme für teures Geld austauschen zu müssen.

PROTECTOR stellt in der Ausgabe 4-2017, S. 42/43, 155 **hochauflösende Netzwerkkameras** von 53 Anbietern in einer Marktübersicht vor. Abgefragte Kriterien kämen unter anderem aus den Bereichen Videospezifikationen, Bildübertragung, Audiospezifikationen, Schnittstellen, Aufbau und Betrieb sowie Sicherheit.

Whistleblowing

Magdalena Gertig, Viadrina Compliance Center, erläutert in comply, Ausgabe 1-2017, S. 36–39, woran sich Unternehmen orientieren und was sie bei der **Einrichtung einer Hinweisgeberstelle** aktuell beachten sollten. § 4 d FinDAG sei durch die Einrichtung der zentralen Stelle für die Hinweisannahme zum 2. Juli 2016 von der BaFin umgesetzt worden. Der Schwerpunkt liege auf dem Schutz der Identität des Hinweisgebers und Betroffener. Die Autorin geht näher auf die Verschwiegenheitspflicht und den Beschlagnahmeschutz bei anwaltlichen Ombudspersonen ein. Auswirkungen der Änderungen von Hinweisgebersystemen einzuschätzen und in einem eigenen Hinweisgebersystem umzusetzen, bleibe eine Aufgabe der Unternehmen und Institutionen.

Alexander Matuk, Viadrina Compliance Center, vergleicht in der Ausgabe 1-2017 von comply, S. 40–43, **Grundmodelle und Funktionen von Hinweisgebersystemen**, ihre Vor- und Nachteile: anonymes vs. offenes Whistleblowing; internes vs. externes Whistleblowing; zentrales vs. dezentrales Whistleblowing; IT-basiertes vs. klassisches Whistleblowing. Für welches Modell bzw. welche Kombination der verschiedenen Komponenten sich ein Unternehmen oder eine Organisation entscheiden sollte, hänge maßgeblich von ihrem Aufbau, Größe, Struktur und vor allem den rechtlichen Rahmenbedingungen ab. Abzuwägen gelte es dabei insbesondere, ob die Mischung aus mehreren Elementen zu einem erfolgreichen Hinweisgebersystem führen könnte. Gerade mit dem Aufbau von sich unterstützenden und ergänzenden Methoden zur Hinweisgewinnung lasse sich ein flächendeckendes Whistleblowing-System aufbauen, das flexibel auf unterschiedliche Erfordernisse eingehen kann und von Whistleblowern nicht nur angenommen wird, sondern Mitarbeiter dazu motiviert, die Qualität des Unternehmens hochzuhalten und zu verbessern, indem auf Verstöße oder Unregelmäßigkeiten hingewiesen wird.

Wohnungseinbruch

Die zunehmende technische Aufrüstung von Wohnungen und Häusern, die zum Teil von der Kreditanstalt für Wiederaufbau bezuschusst wird, sei ein Faktor von vielen, warum die Zahl der Wohnungseinbrüche in Deutschland nach Jahren erstmals zurückgeht, schreibt die FAZ am 25. April: um 9,5 Prozent. 151.265 Fälle seien es 2016 gewesen. Die positive Entwicklung in Deutschland führe die Polizei auf ein Bündel von Aktionen zurück. Neben den technischen Vorkehrungen gehöre vor allem auch die verstärkte Strafverfolgung dazu. Genannt werden länderübergreifende Schwerpunktkontrollen gegen Einbrecherbanden und die Polizeipräsenz in den Straßen der Großstädte. Die spezielle Prognosesoftware „Precobs" solle den Ermittlern zudem dabei helfen, in bestimmten Stadtgebieten Einbrüche nach unterschiedlichen Kriterien zu kategorisieren. Die wichtigste kriminologische Grundlage von Precobs sei die Theorie des „near repeat", die auf kriminologischer Forschung und Vernehmungen professioneller Einbrecher fuße: Wo es einmal geglückt ist, wird der Täter es vermutlich wieder versuchen.

Zutrittskontrolle

Zutrittskontrolle im Bereich der **Zeitwirtschaft** thematisiert Security insight in der Ausgabe 2-2017 (S. 37/38). Im Bereich der Zutrittskontrolle in Unternehmen könne sich das Thema Mobilität bzw. die Zutrittskontrolle mit Hilfe von Smartphones aus Sicherheitsgründen derzeit noch weniger durchsetzen. Viele Unternehmen setzten auf eine Kombination aus Online- und Offline-Zutritt, wobei das Thema Funk bei der Online-Zutrittskontrolle eine immer größere Rolle spiele. Durch die Kombination werde ein hoher Grad an Flexibilität erreicht. Ein wichtiger Trend im Bereich Security sei, dass sich Kunden eine Komplettlösung wünschen, bei der Zutrittskontrolle, Videoüberwachung, Einbruch- oder Brandmeldeanlagen in einem System zusammengeführt und in einem Security-Dashboard überwacht werden.

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, Dr. Heiko Kroll
Vorsitzender des Aufsichtsrates: Dr. Carl A. Schade

E-Mail: info@securitas.de