FOCUS ON SECURITY

AUSGABE 01, JANUAR 2018

SECURITAS

Inhaltsverzeichnis

Anschläge

Nach IBWS-Informationen vom 11. Dezember sind am 13. November in Hamburg zwei Kfz durch einen Brandanschlag zerstört worden, die durch Aufschriften als Arbeitsfahrzeuge der Unternehmensgruppe „Sicherheit Nord" zu erkennen gewesen seien. Das Grundstück sei zur Tatzeit unbewacht gewesen und von jedermann frei zu betreten. Ein Selbstbekennungsschreiben sei unterzeichnet durch „Für die Anarchie – Autonome Gruppen".

Arbeitsplatzsicherheit

In der Dezember-Ausgabe von veko-online befasst sich Steffen Meltzer mit **Bedrohungen am Arbeitsplatz durch Kunden**. Als hauptsächliche Ursachen für gesteigertes Angriffspotenzial sieht der Autor eine grundlegende Bereitschaft einzelner Menschen für Aggressionen. Des Weiteren gebe es eine große Anzahl an Persönlichkeitsstörungen und psychischen Erkrankungen. In den Medien sei ein Überangebot an Gewalt zu sehen. Eine wesentliche Ursache sei auch im Konsumdruck zu suchen. Nach einer Studie seien durch 144 Unternehmen und Behörden folgende Anteile bestimmter Personengruppen am Aggressionspotenzial genannt worden: 21,7 Prozent Menschen mit Migrationshintergrund; 19,6 Prozent Arbeits- und Erwerbslose; 16,6 Prozent alkoholisierte Personen; 11,8 Prozent Personen unter Drogeneinfluss; 9,7 Prozent Kinder und Jugendliche. In der Präventionsarbeit stünden ein gutes Kommunikationstraining und eine rechtzeitige Gefahrenerkennung durch die Körpersprache in Verbindung mit dem gesprochenen Wort am Anfang.

Arbeitsschutz

Ergebnisse einer **Umfrage zum Umgang mit persönlicher Schutzkleidung** im Auftrag von CWS-boco stellt GIT in der Ausgabe 12-2017, S. 104/105 vor: 63 Prozent der Arbeitnehmer in Deutschland müssen ihre Berufskleidung selbst waschen. 68 Prozent gehen Kompromisse bei ihrer Sicherheit am Arbeitsplatz ein. 44 Prozent lassen auch mal notwendige Teile ihrer Schutzausrüstung weg. Ältere Arbeitnehmer nehmen Arbeitsschutz ernster als jüngere. 52 Prozent finden, dass in ihrem Unternehmen Produktivität über Sicherheit steht. Nur 53 Prozent geben an, dass die Einhaltung der Sicherheitsvorschriften am Arbeitsplatz regelmäßig kontrolliert wird.

Arzneimittelfälschung

Die FAZ weist am 30. November auf eine Studie der WHO hin, nach der jedes zehnte Medikament in Ländern mit niedrigen und mittleren Einkommen gefälscht oder minderwertig ist. Es handele sich vor allem um Antibiotika und Medikamente gegen Malaria und Krebs.

Betrug

Das BKA hat im Oktober 2017 einen Bericht zu deutschsprachigen Forschungsbeiträgen und Publikationen über **Social Engineering und CEO-Fraud** veröffentlicht. Sozialwissenschaftliche Untersuchungen zeigten, dass die Auskunftsbereitschaft von Mitarbeitern bei persönlich durchgeführten Abschöpfungsversuchen (ohne IT-basierte Angriffe) mit der räumlichen Entfernung zum Arbeitsplatz zunehme. Prognostisch bleibe zu befürchten, dass Social-Engineering-Fälle in Zukunft eher ansteigen als abnehmen und die Aufklärung problematisch bleibe. Gründe hierfür seien insbesondere: Die Betrügereien würden weiterhin und zunehmend aus dem Ausland oder von nicht zu identifizierenden Rechnern oder Personen begangen. Scham oder die Angst vor Reputationsverlust könne die Anzeigebereitschaft hemmen. Die Aussicht auf immense Gewinne erhöhe den Tatanreiz. Die Verfügbarkeit relevanter offener Informationen, die genutzt werden könnten, werde eher ansteigen. Der Druck auf einzelne Mitarbeiter steige eher als dass er sinkt und das Vertrauen, um sich vermeintlichen Anweisungen zu widersetzen, sei nicht immer vorhanden**.** Und die internationale Rechtshilfe sei in hohem Maße defizitär.

Nach einer Meldung der FAZ am 19. Dezember ist dem BKA ein Ermittlungserfolg gelungen. In Israel seien sechs mutmaßliche Betrüger festgenommen worden, die seit 2014 einen Schaden von 175 Mio. Euro durch **„CEO-Fraud"** verursacht haben sollen.

Fälle dieser Deliktsart seien 2015 bei 56 Versuchen 25-mal erfolgreich, 2016 bei 383 Versuchen 56-mal erfolgreich und 2017 bisher bei 239 Versuchen 23-mal erfolgreich gewesen. Der potenzielle Schaden sei gewaltig: 2016 hätten die Täter 223 Mio. Euro gefordert und 83 Mio. Euro erzielt, 2017 bisher 142 Mio. Euro gefordert und 24 Mio. Euro erzielt.

Über einen Betrugsfall mit Millionenschaden zu Lasten der **Ergo-Versicherung** berichtet die FAZ am 29. Dezember. Über mehrere Jahre hinweg sollen zwei lokale Geschäftsleiter in Russland Firmengelder durch Autoschiebereien veruntreut haben. Seit 2011 hätten die Mitarbeiter ihre kriminellen Aktivitäten rund um die Autoversicherung im Lauf der Zeit offenbar systematisch ausgebaut. Gestohlene und dann wieder aufgefundene Fahrzeuge habe die Clique nach der Rückgabe an die Ergo einfach auf dem Gebrauchtwagenmarkt weiterverkauft und den Verkaufserlös in die eigene Tasche gesteckt. Ein noch deutlich größerer Schaden sei im Zuge des Verkaufs von Tagesversicherungen als Ergänzung der nur im Inland gültigen Kfz-Haftpflichtversicherung für Auslandsfahrten entstanden.

Biometrie

Microsofts biometrisches Anmeldeverfahren sei unsicher, meldet heise.de am 18. Dezember. Der Ansatz komme bei **Windows 10** zum Einsatz. Nutzer könnten sich per Gesichtserkennung an Geräten anmelden. Sicherheitsforscher von SSS zeigten, wie sie das Verfahren mit einem auf Papier ausgedruckten Gesicht einer berechtigten Person erfolgreich umgehen. Das klappe aber nicht immer. Damit der Spoofing-Angriff funktioniert, müsse das ausgedruckte Gesicht diverse Kriterien erfüllen.

BMA

Mit innovativen Lösungen, die auch Architekten zufrieden stellen, befasst sich Security insight in der Ausgabe 6-2017, S. 26/27. **Multifunktionale Melder**, die neben ihrer reinen Detektionsfähigkeit weitere wichtige Aufgaben erfüllen können, behaupteten sich im Bereich der Brandmeldetechnik immer mehr. Mit der VdS-zugelassenen Kombination des Brandmelders IQ8Quad von ESSER mit einer Designleuchte komme ein Alleinstellungsmerkmal hinzu. Die Neuentwicklung bleibe nicht auf den Einsatz von Brandmeldern begrenzt, sondern berücksichtige auch die Integration von Lautsprechern für Sprachalarmierung in den Leuchten. Selbst eine Notbeleuchtung im Fall des Netzausfalls könne integriert werden.

Brandschutz

Intelligente **Brandschutzsysteme für Klinik und Pflege** werden in der Ausgabe 12-2017 der Zeitschrift PROTECTOR beschrieben. In Gesundheitseinrichtungen gebe es viele Anwendungsfelder mit den unterschiedlichsten Risiken und Herausforderungen für die Branddetektion – vom Aufzugsschacht über den Operationssaal bis zur Zwischendecke. Eine Herausforderung für den Brandschutz seien schwer erreichbare Orte wie Luft- oder Kabelkanäle, Zwischendecken, Versorgungsschächte und Fahrstühle. Andere Bereiche, zum Beispiel Intensivstation oder OP, dürften vom Servicetechniker nicht betreten werden. Die Lösung sei eine Überwachung mit Ansaugrauchmeldern wie dem „SecuriRAS ASD". Konfiguration, Wartung und Instandhaltung erfolgten ausschließlich außerhalb der abgelegenen oder gesperrten Zonen. Die Alarmierung in kürzester Zeit gelinge mit Sprachalarmierung, denn Menschen reagieren auf das gesprochene Wort bis zu viermal schneller als auf Signale.

s+s report enthält in der Ausgabe 4-2017 interessante Beiträge zum Thema Brandschutz:
Arkadiusz Dziminski, Fire Service Systems s.c., Polen, und Faru Fakrou, T&B electronic GmbH, befassen sich mit der **Wartung und Instandhaltung von Funkenlöschanlagen** (S. 14–16). VdS-zugelassene Funkenlöschanlagen stellten sicher, dass Zündpotenziale nicht in die Ex-Zonen gelangen können. Wesentliche Voraussetzung hierzu sei, dass die eingesetzten Funkenlöschanlagen gemäß VdS 2518 zugelassen sind und von einem VdS-anerkannten Errichter gemäß VdS-Richtlinie 2106 projektiert und installiert wurden. Es sei unerlässlich, dass der Servicetechniker, der die Wartung durchführt, auch in der Lage ist, sicherheitsrelevante bauliche Veränderungen oder Erweiterungen der Absauganlage zu erkennen. Eine Wartung oder Inspektion des Brandschutzsystems sollte also zwingend durch einen Errichter erfolgen, der gemäß VdS 2132 zugelassen ist und eine Anerkennung für das installierte System hat. Die Bedeutung einer regelmäßigen Funktionskontrolle ergebe sich gerade für Funkenlöschanlagen aus der

Tatsache, dass die Funkenmelder und die Löschdüsen einer kontinuierlichen mechanischen Belastung durch das abrasive abgesaugte Material ausgesetzt sind. Eine wachsende Anzahl von Alarmen und damit von detektierten Funken deute darauf hin, dass im Bereich der Produktion ein Defekt vorliegen kann.

Dr. Wolfram Krause, bvfa, behandelt **Einsatzgebiete von Spezial-Löschanlagen** (S. 20–24). 44 Prozent der gemeldeten und durch Spezial-Löschanlagen gelöschten Brände seien in Maschinen entstanden, insbesondere bei der Metallbearbeitung. Bei der spanenden Metallbearbeitung könne es durch Werkzeugbruch, Fehlsteuerungen oder Trockenlaufen der Werkzeuge zur Zündung des Öl/Luft-Gemisches im Innenraum der Maschine und damit zu einer Verpuffung mit Folgebrand kommen. Mehr als ein Viertel der Brände seien außerhalb der Arbeitszeit gelöscht worden. 88 Prozent der Spezial-Löschanlagen hätten automatisch ausgelöst. Die Brände an Maschinen würden nach der bvfa-Statistik vor allem mit Kohlendioxid-Löschanlagen bekämpft, die in elektrischen Anlagen überwiegend mit Inertgasen. Die verwendete Löschmittelmenge habe in 78 Prozent der Anlagen durchschnittlich nur 115 kg betragen.

Dipl.-Ing. Jan Hohmann, R+V Allgemeine Versicherung AG, beurteilt die **Industriebaurichtlinie Abschnitt 7** aus Sicht des Sachwertschutzes (S. 26/27). Er erläutert die Schutzziele des Abschnitts 7 und die sich daraus ergebenden Nachteile aus Sicht der Sachversicherer. Die Brandlastberechnung entsprechend Abschnitt 7 sei für Betriebe der metallverarbeitenden Industrie sowie für Lager geeignet, in denen ausschließlich nichtbrennbare Materialien und Güter ohne nennenswerte Verpackungsmaterialien gelagert werden.

Stephanie Brandt, Dr. Aleksandar Duric und Christian Lais, Siemens AG, befassen sich mit der **Brandfrüherkennung durch CO-Melder** (S. 28–32). Sie gehen ein auf Kohlenmonoxid (CO) als Indikatorgas zur Brandfrüherkennung, auf die Voraussetzungen für die Eignung als Indikatorgas, die Kombination mehrerer Detektionsprinzipien, die Brände von Täuschungsgrößen zu unterscheiden helfe, auf Normen für Brandmelder mit CO-Detektion, verschiedene Brandmelder-Typen mit CO-Sensor, auf die länderspezifisch geregelte Planung, Projektierung und Instandhaltung und auf die intelligente Mehrfachsensor-Brandmelder mit CO-Detektion. Die besondere Herausforderung liege darin, die richtigen Sensorprinzipien zu wählen und die Sensoren mit der optimalen Charakteristik so zu kombinieren, dass sowohl die Detektionseigenschaften als auch die Täuschungsimmunität bestmöglich ausfallen.

Blitzschutz für Sonder- und Standardbauten thematisieren Dipl.-Ing. Joseph Messerer und Reinhard Schüngel, bestellter und vereidigter Sachverständiger für Elektroinstallation und Blitzschutzanlagen (S. 34–37). Sie erläutern, ob für bauliche Anlagen Blitzschutzanlagen erforderlich sind und wie eine ordnungsgemäße Blitzschutzanlage geplant und ausgeführt werden muss. Die Autoren befassen sich mit den Bestimmungen der MBO, mit Arten von Blitzeinschlägen, Gefahren des Blitzstroms, mit äußerem und innerem Blitzschutz, Planungsgrundlagen für Blitzschutzanlagen und der Blitzschutz-Risikoanalyse für Gebäude. Durch die Risikoanalyse nach DIN VDE 0185-305-2 würden die Bestimmungen des Baurechts über Blitzschutzanlagen nicht hinfällig. Die Anwendung dieses Teils der Norm führe in vielen Fällen zu einer Fehleinschätzung und zu einer Fehlplanung. Für Gebäude, für die das Baurecht keine Blitzschutzanlagen vorschreibt, könne eine Risikoanalyse eine zusätzliche Entscheidungshilfe für den Bauherrn sein.

Dipl.-Ing. Frank Hombach, VdS, weist darauf hin, dass Bosch Sicherheitstechnik mit **Aviotec IP starlight 8000** erstmals ein System entwickelt habe, das Flammen und auch Rauch videobasiert direkt an der Brandquelle erkennt (S. 38/39). Die Technik verwende intelligente Algorithmen, direkt in der Kamera integriert, zur Analyse und Verarbeitung der aufgenommenen Bilder. Diese videobasierte Branderkennung könne zwischen echtem Feuer und Störgrößen wie Reflektionen, Bewegungen oder Gegenlicht unterscheiden. Die Kamera dürfe nicht als Brandmelder im Sinne der EN 54-Reihe fungieren. Es gehe vielmehr um eine Ergänzung bestehender Systeme. Das Produkt könne als einzelne Kamera oder auch in vernetzten Systemen mit verteilten Aufnahmegeräten, einer gemeinsamen Benutzeroberfläche und einem zentralen Managementsystem eingesetzt werden. Und beim Einsatz von PoE-Kameras würden keine individuellen Stromversorgungen und Kabel gebraucht.

Die Fachzeitschrift GIT befasst sich in der Ausgabe 12-2017, S. 84–86, mit aktiver **Brandvermeidung in einem automatisierten Kleinteilelager**. Mögliche Kabelbrände durch Überhitzung an Fördermotoren oder technische Anlagendefekte stellten statistisch gesehen die häufigste Brandursache in automatisierten Hochregallagern dar. Um die Gefahr einer brandbedingten Lieferunterbrechung zu bannen, werden ein Brandfrüherkennungssystem und ein aktiver Schutz mit Oxyreduct empfohlen. Das bestehe aus drei wesentlichen Komponenten: dem Stickstofferzeuger, der Steuerzentrale Oxycontrol und den Sauerstoffsensoren Oxy Sens. Alle seien redundant vorhanden.

Jens Stubenrauch, Sachverständiger für Schaumlöschmittel und Schaumlöschtechnik, befasst sich in der Ausgabe 6-2017 des Sicherheitsforums, S. 16–19, mit **fluorfreien Schaumlöschmitteln**. Bei der Umrüstung auf fluorfreie Schaummittel solle zunächst eine Bestandsaufnahme der aktuellen Löschanlage erfolgen. Es müsse dann geprüft werden, ob der Schaummittel-Vorratstank und die Rohrleitungsisometrie vom Schaumtank zum Zumischer zu den chemisch-physikalischen Eigenschaften des gewünschten Schaumlöschmittels passt oder Umbauten notwendig sind. Sofern die Datenlage keine sichere Bewertung zulässt, ob die vorhandene Anlagenkonfiguration für den Einsatz mit fluorfreien Löschmitteln übernommen werden kann, müssten Tests durchgeführt werden, die alle vorgenannten Parameter berücksichtigen. Fluorfreie Schaummittel würden auf unterschiedlichen Brennstoffen sehr unterschiedliche Löschleistungen aufweisen. Für eine grobe Bewertung einer möglichen Umstellung auf fluorfreie Schaumlöschmittel würden benötigt: Brennstofflisten und Sicherheitsdatenblätter der Brennstoffe, SIN-Nummern bzw. Datenblätter der Sprinkler oder der anderen schaumerzeugenden Bauteile, Typbezeichnung und Datenblatt des Zumischers und eventueller Schaummittel-Förderpumpen, Daten zur Rohrleitungsauslegung, Angaben zur eingesetzten Wasserqualität, Angaben zum Druck an hydraulisch günstigsten und ungünstigsten Sprinkler und Angabe der Applikationsrate.

Rainer Klose vom schweizerischen Forschungsinstitut Empa weist in der Ausgabe 6-2017 der Zeitschrift Sicherheitsforum, S. 30/31, darauf hin, dass Chemiker der Empa einen neuen Syntheseweg für **umweltfreundliche Flammschutzmittel** entwickelt und patentiert haben. Diese seien für Matratzen und Polster geeignet. Anders als bisherige Flammschutzmittel aus chlorhaltigen Chemikalien sei die neue Stoffklasse ungiftig und effizient. Schaumstoffe, die EDA-Dopo (ein Derivat des Flammschutzmittels Dopo) enthalten, erfüllten die höchste Flammschutz-Klassifikation (UL94HB).

Dipl.-Ing. Pascal Geiger, ift Rosenheim, befasst sich in der Ausgabe 6-2017 der Zeitschrift Sicherheitsforum, S. 38–40, mit der **Normierung bei Feuerschutzbeschlägen**. Dies sei ein weites Feld, gerade auch im Hinblick auf die unterschiedlichen Ansätze, die sich in nationalen Normen und Vorschriften sowie in der europäischen Normierung und Rechtsprechung widerspiegeln. Der EUGH spreche sich gegen nationale Regelwerke aus. Deutschland arbeite an einem neuen Verfahren, der Muster-Verwaltungsvorschrift Technische Baubestimmungen, die die Bauregelliste ersetzen sollen. Der Autor behandelt die nationale und die europäische Normung. Die Zeit werde zeigen, ob und wann die jeweiligen überarbeiteten Produktnormen harmonisiert werden.

Datenschutz

Rechtsanwältin Anna Cardillo stellt im Fachmagazin s+s report, Ausgabe 4-2017, S. 60–62, den Entwurf der **VdS-Richtlinien 10010** vor. Sie zeigten einen Weg auf, die rechtlichen organisatorischen und technischen Anforderungen der DS-GVO so strukturiert wie möglich und mit überschaubarem Aufwand umzusetzen. Sie beschrieben ein auditier- und zertifizierungsfähiges Datenschutzmanagementsystem (DSMS), das vor allem auf KMU zugeschnitten ist und dem ein kontinuierlicher Verbesserungsprozess zugrunde liegt. Die Autorin erläutert den Geltungsbereich der VdS 10010, Eckdaten, Eigenschaften und Regelungsinhalte.

Die FAZ-Beilage Mediaplanet KMU vom Dezember 2017 enthält einen Überblick wesentlicher Änderungen durch die DS-GVO: die sogenannte Rechenschaftspflicht, die faktisch eine Art Beweislastumkehr im Datenschutzrecht verankert, und die erhebliche Ausweitung und Konkretisierung der Betroffenenrechte, insbesondere eine Erweiterung der Informationspflichten. Als Umsetzungsmaßnahmen in Unternehmen werden skizziert: die Integration der Datenschutzgrundsätze der DS-GVO in das interne Regelwerk; die Überprüfung und Anpassung der Dokumentation von Verarbeitungstätigkeiten; die Überprüfung und Anpassung von Verträgen mit Dienstleistern; die Gewährleistung von Betroffenenrechten und Informationspflichten und die Installation entsprechender Prozesse sowie die Installation von Meldepflichten im Unternehmen.

Diebstahl

Von den Höfen landwirtschaftlicher Betriebe, aber auch von Feldern und Äckern verschwinden immer wieder Maschinen oder Teile davon, meldet die FAZ am 15. Dezember. Vor allem der Osten der Bundesrepublik habe es den Dieben angetan. Vermutlich seien die nahen Grenzen zu den osteuropäischen Staaten der Grund. Von dort vermute die Justiz organisierte Banden.

Drohnen

Allein in Deutschland gibt es nach einer Meldung in der FAZ vom 27. Dezember mehr als **500.000 Drohnen**. Seit 2011 habe sich die Zahl der privat genutzten Fluggeräte jedes Jahr verdoppelt. Die Flugsicherung schätze, dass im Jahr 2020 mehr als eine Million Drohnen in Deutschland unterwegs sind. Es gebe inzwischen grundlegende Regeln für den Betrieb der zivilen Drohnen: Nicht erlaubt sei der Betrieb in der Nähe von Flughäfen, Verkehrswegen, Kraftwerken und militärischen Anlagen, an Einsatzorten von Polizei und Rettungskräften, in der Nähe von Krankenhäusern oder Gefängnissen, über Industrieanlagen oder wichtigen Behörden und nicht in Naturschutzgebieten. Höher als 100 Meter dürften die Geräte auch nicht fliegen und nicht über Menschenansammlungen. Und Drohnen, die mehr als ein Viertel Kilogramm wiegen, dürften auch in Wohngebieten nur dann aufsteigen, wenn es die Nachbarn ausdrücklich erlaubt haben.

Einbruch

Ungewöhnlich viele Einbrecher hätten in diesem Jahr den **Weg über das Dach** gewählt, schreibt Security insight in der Ausgabe 6-2017, S. 20. Dabei seien sowohl Wohn- wie auch Geschäftshäuser im Fokus. Nach Ansicht von Experten habe das seine Ursache darin, dass der Einbruchschutz und die Alarmsysteme deutlich effektiver geworden seien und großflächiger angewendet würden. Das Dach hingegen sei oft eine „offene Flanke". Besonders einzelnstehende Supermärkte zeigten sich dabei als „gefundenes Fressen".

Die FAZ weist am 19. Dezember darauf hin, dass fast alle Einbrüche in Häuser über Fenster und Terrassen- oder Balkontüren stattfinden. Nur zwei Prozent erfolgten über die Eingangstür. Alarmanlagen gebe es in jeder Preisklasse und mit unterschiedlichen Systemen. Private Alarmanlagen dürften nur mit einem Sicherheitsdienstleister, nicht direkt mit der Polizei verbunden sein. Das sei nur Banken und Juwelieren gestattet. Sicherheitsdienstleister forderten etwa 30 Euro Monatspauschale zuzüglich Einsatzgebühr. Wird die Polizei vom Eigentümer alarmiert und stellt am Einsatzort einen **Falschalarm** fest, verlange sie eine Gebühr von 200 Euro. Denn ein solcher Polizeieinsatz diene in erster Linie dem Schutz des privaten Eigentums. Dagegen müssten Nachbarn oder Passanten, die einen Alarm hören und die Polizei verständigen, eine solche Gebühr nicht entrichten.

EMA

Digitale Einbruchmeldetechnik behandelt in der Ausgabe 12-2017 der Zeitschrift PROTECTOR, S. 46/47, Frank Bärmann, AMG Sicherheitstechnik GmbH. Alarmtab von AMG Sicherheitstechnik vollziehe technologisch den Sprung in die Digitalisierung und sei ein System, das den Einbruch nicht nur meldet, sondern von Anfang an aktiv auf den Tathergang Einfluss nimmt. Die von Alarmtab genutzte Funktechnologie basiere auf dem weltweit genutzten Bluetooth LE – Low Energy (BLE)-Standard – der von AMG mittels neuem Funkprotokoll speziell für den Sicherheitsbereich entwickelt worden sei. Die Software in der Alarmzentrale definiere, welche Rolle der Sender im Netzwerk übernimmt, welche Zustände er zukünftig übermittelt und welche Auslösung zu einem Alarm führt. Kennzeichen dieser neuen Technik seien die verfügbaren Reichweiten von bis zu 250 Metern im Freien und bis zu 50 Metern innerhalb von Gebäuden sowie die hohen Sicherheitsstandards gegen Manipulation. Anstatt einen Alarm nur zu melden, sorge Alarmtab für Einbruchprävention, Meldung, Ablenkung, aktive Verjagung des Täters und Unterstützung bei der Aufklärung. Fehlalarme würden durch eine intelligente Steuerungssoftware ausgeschlossen.

Einzelhandelssicherheit

Security insight weist in der Ausgabe 6-2017, S. 36–38, darauf hin, dass nach einer neueren Studie pro 69 Euro Umsatz der Handel im Durchschnitt einen Euro durch Diebstähle verliere. Die Zahl der schwerwiegenden Diebstähle ist nach Ansicht des Handelsverbandes HDE zwischen 2013 und 2016 kontinuierlich um fast 30 Prozent gestiegen. Nur jeder 50. Täter werde überhaupt ertappt. Die Belastungszahl sei in einigen grenznahen Städten (Flensburg auf Rang 1 mit 1.308, Saarbrücken mit 1.150 auf Rang 2) besonders hoch. Ladendiebe setzten gegen die Warensicherungsantennen **neuartige Störsender** ein. Der Störsender oder Jammer, der im Internet frei erhältlich sei, verhindere in der

Tasche getragen das Auslösen des Alarms am Ausgang. Als Anhaltspunkte für einen Tatverdacht werden in dem Beitrag unter anderen genannt: Zwei Personen trennen sich sofort nach dem Betreten des Geschäfts und gehen in verschiedene Richtungen; ein Kunde läuft scheinbar ziellos im Geschäft herum; ein Kunde verfolgt die Abläufe im Geschäft ganz genau; eine Kundengruppe schirmt sich gegenseitig ab.

Erpresserschreiben

Die Möglichkeit der **Spurensuche auf Erpresserschreiben** erläutert KD Jens-Peter Geuther, Landespolizei Schleswig-Holstein, im Fachmagazin info Sicherheit, Ausgabe 4-2017, S. 44/45. Fingerabdrücke blieben auch auf Papier zurück. Das sei mit bloßem Auge zwar nicht zu erkennen, aber im Spurensicherungslabor werde das Papier mit Chemikalien behandelt. Dann reagierten die in den Abdrücken enthaltenen Fette und Eiweiße chemisch und würden durch einen deutlichen Farbumschlag sichtbar. Auch DNA finde sich an Erpresserbriefen, z. B. bei den mit Speichel befeuchteten Klebeflächen der Briefmarke und Umschlaglasche oder überall dort, wo besonders intensiv angefasst wurde. Weil sich aber kaum vermeiden lasse, dass sich auch Spuren Unverdächtiger am Brief ablagern, müsse das Erpresserschreiben so schnell wie möglich vor der Kontaminierung durch weitere Personen bewahrt werden. Durchdruckspuren, die entstehen, wenn die obere von mehreren Papierlagen handschriftlich beschrieben wird, könnten mit einem Spezialverfahren sichtbar gemacht werden. Das Verfahren arbeite mit elektrostatischer Aufladung und sei so empfindlich, dass auch tiefer liegende Papierlagen ausgezeichnete Ergebnisse lieferten. Passspuren finde man dort, wo Teile früher eine Einheit bildeten, z. B. wenn man einen Papierbogen an der Perforation vom Schreibblock reißt oder eine Briefmarke aus dem Wertzeichenheftchen heraustrennt. Um Spuren nicht zu vernichten, sollten in Unternehmen klare Handlungsanweisungen gegeben werden: verdächtige Briefe nicht öffnen, bereits geöffnete nur mit Einweghandschuhen anfassen und nicht mehr in die Hände anderer Personen geben; keine Kunststofftüten verwenden, keine Kopien anfertigen; nicht auf das Papier atmen; Personalien aller festhalten, die Kontakt zum Brief hatten.

Freilandsicherung

PROTECTOR enthält in der Ausgabe 12-2017, S. 52/53, eine **Marktübersicht** über 122 Freilandsicherungssysteme von 52 Anbietern. Die Tabelle zeigt Antworten zu Produktkriterien wie Zweck/Funktion, Kosten, Schutzart, Sensorprinzip und Technikkriterien wie Fläche und Zonenlänge, maximale Elemente pro Gesamtsystem, Detektionswahrscheinlichkeit, Fehlalarmquote, Lebensdauer, Frequenzbereich.

Gasspeichersicherheit

Dipl.-Ing. Martin Paproth, ö.b.u.v. Sachverständiger für Biogastechnik, thematisiert in s+s report, Ausgabe 4-2017, S. 64–67, die technische Dichtheit von **Membranspeichersystemen bei Biogasanlagen**. Der Beitrag befasst sich mit den inhaltlichen Schwerpunkten des neuen Merkblattes DWA-M 375 vor dem Hintergrund der bestehenden Situation und des Handlungsbedarfs hinsichtlich der Vermeidung von Leckagen bei den Gasspeichersystemen von Biogasanlagen. Der Autor befasst sich mit der Ausführung von Gasspeichersystemen, dem Regelungsbedarf, den Schwerpunkten des Merkblatts (Definition der Anforderungen an die Gasdichtheit von Membranspeichersystemen, potenzielle Gasfreisetzungsstellen an Membranspeichersystemen, Prüfmethoden zum Nachweis der Dichtheit). Es dürften in Zukunft nur noch Membranen zur Anwendung kommen, die eine eindeutige Kennzeichnung mit Angabe des Herstellers, der Membranbezeichnung, des Herstelldatums und des zulässigen Betriebsdrucks tragen. Es bestehe weiterer Regelungsdarf. Ein wesentlicher Bedarf liege in der Erarbeitung von anwendungsspezifischen Produktnormen, auf die die Hersteller ihre Membranprodukte ausrichten können.

Falschgeld

Wie das Fachmagazin DSD in der Ausgabe 4-2017, S. 14/15 berichtet, hat die Deutsche Bundesbank im ersten Halbjahr 2017 rund 39.700 falsche Euro-Banknoten mit einem Wert von 2,2 Mio. Euro aus dem Verkehr gezogen. Das seien 8,7 Prozent mehr als im zweiten Halbjahr 2016.

Dabei hätten vor allem Fälschungen der 50-Euro-Note der ersten Serie zugenommen. 63 Prozent aller gefälschten Banknoten seien auf diesen Wert entfallen. Es folgten 20-Euro-Noten mit 23 Prozent. Die im April 2017 eingeführte neue 50-Euro-Banknote gelte als besonders fälschungssicher. Nach Angaben der Europäischen Zentralbank ist die Zahl der registrierten Fälschungen im Euroraum insgesamt gesunken. Im DSD werden die Sicherheitsmerkmale aufgeführt, die besonders zu beachten seien. Bei der Prüfung einer verdächtigen Banknote sei es empfehlenswert, eine zweifelsfrei echte Banknote zum Vergleich heranzuziehen. Bei der Prüfung von Banknoten mit Lupen, Prüfstiften oder UV-Lampen lasse sich nicht immer ein eindeutiges Prüfergebnis erzielen.

Gefahrenmelderzentrale

Telenot stellt in der Ausgabe 12-2017 der Fachzeitschrift GIT, S. 48/49, eine neue Generation von Gefahrenmelderzentralen mit dem Namen **„Hiplex"** vor. Sie wachse im wahrsten Sinne des Wortes als systemoffene Plattform mit den Anforderungen, die in Zukunft an Sicherheitstechnik gestellt werden. Diese einzigartige Flexibilität umfasse etwa die unbegrenzte Zahl von Schnittstellen, BUS-Adressen und Meldergruppen, die Verschlüsselungstechnik und die Integration in das Gebäudemanagement. Die neue „Hiplex" entspreche und erfülle sämtliche Anforderungen der EN-Normen an Einbruchmeldezentralen. Außerdem sei sie vom VdS zertifiziert.

Geldautomatensicherheit

Immer mehr Länder setzten auf moderne EMV (Elektromagnetische Verträglichkeit)-Technik. Bezahlkarten seien mit einer Art Mini-Computer ausgestattet, meldet die FAZ am 12. Dezember. Der Datensatz werde verschlüsselt, die Karte bei Gebrauch auf Echtheit geprüft, sowohl am Geldautomat als auch an der Ladenkasse. In Deutschland seien seit Ende 2010 alle inzwischen gut 100 Mio. **Girokarten mit EMV-Chip** ausgestattet, ebenso sämtliche knapp 60.000 Geldautomaten und 720 Terminals im Handel. Dennoch seien die Fallzahlen des „Skimmings" als auch der Bruttoschaden 2017 wieder nach oben gegangen. 476 Manipulationen von Geldautomaten in Deutschland habe die Einrichtung EURO Kartensysteme gezählt. Brennpunkt sei Berlin. Mit 267 Fällen hätten Fahnder dort 56 Prozent aller Skimming-Attacken registriert.

Dipl.-Ing. Günter Grundmann, VdS, befasst sich in s+s report, Ausgabe 4-2017, S. 52/53, mit der **Unbrauchbarmachung von Banknoten**. Mit den Richtlinien VdS 2538 existiere ein in Europa einzigartiger Anforderungskatalog an diese Systeme, mit dem ein besonders hohes Niveau an Wirksamkeit und Zuverlässigkeit erreicht werde. Sie berücksichtigten hierbei die besondere Funktionsweise von Einfärbesystemen sowie deren unterschiedliche Auslösemechanismen. Darüber hinaus orientierten sich die in den VdS-Richtlinien formulierten Anforderungen an den Bedienprozessen, die besondere Maßnahmen gegen Fehlauslösungen erfordern, ohne dabei gewollte Auslösungen zu verhindern.

Am 21. Dezember meldet die Berliner Polizei die Festnahme von zwei Angestellten der mit dem Befüllen von Geldautomaten beauftragten Sicherheitsfirma, die in Verdacht stehen, aus zwei dieser Geldautomaten in Berlin mit Originalschlüsseln das Geld gestohlen zu haben. Einer der beiden Tatverdächtigen soll sowohl am Tag der Befüllung wie am Tattag im Dienst gewesen sein.

Geldwäsche

Auf das neue **Transparenzregister** weist die FAZ am 28. Dezember hin. Unternehmen, Stiftungen und Genossenschaften müssen in diesem Register hinterlegen, wer „wirtschaftlich Berechtigter" ist. So solle verhindert werden, dass Vermögen verschleiert wird. Das Regelwerk ziele eigentlich darauf ab, Geldwäsche zu bekämpfen. Doch zugleich sei es eine Informationsquelle für Erpresser. Zugreifen auf das Register dürften nur „berechtigte Personen". Das seien Nichtregierungsorganisationen, die sich gegen Geldwäsche engagieren, aber auch jeder Journalist, sofern er einen Presseausweis besitzt und „getätigte oder geplante Recherchen" vorweisen könne.

Hotelsicherheit

PROTECTOR enthält in der Ausgabe 12-2017, S. 32/33, eine **Marktübersicht** über 57 Hotelschließsysteme von 28 Firmen. Abgefragt wurden außer allgemeinen Angaben Systemeigenschaften: unter anderen Systemart, Offline-Fähigkeit, Programmierung, optische und akustische Signale, Stromversorgung am Beschlag, Verkabelung, Mediumart (Transponder), Protokollierung im Schloss.

IT-Sicherheit

Alexander Clemm und Mark Alexander Butzke, Ebner Stolz, behandeln in dem Verlagsspezial IKT-Trends 2018 der FAZ am 7. Dezember die **Sicherung von Unternehmensdaten** mit System. Projekte zur Verbesserung der IT-Sicherheit würden scheitern, weil nicht umsetzbare oder von den Mitarbeitern nicht akzeptierte Konstrukte geschaffen werden, oder die operative Arbeit wird über das notwendige Maß hinaus belastet. Die Inventur und Absicherung beginne bei komplexen IT-Systemen und ende bei den Gewohnheiten einzelner Mitarbeiter. Die wesentliche Herausforderung bestehe darin, die Sicherheitsanforderungen und die organisatorischen Abläufe an Größe und Struktur den Bedürfnissen sowie den Unternehmenszielen der Organisation auszurichten. Bei jeder der von der ISO-Norm 27001 vorgeschlagenen 114 Kontrollen müssten Betriebe ihren individuellen Schutzbedarf berücksichtigen. Die Analyse des Schutzbedarfs starte zunächst bei den eigentlichen Unternehmensprozessen. Im Anschluss würden die relevanten Hilfsprozesse und schließlich die IT-Systeme betrachtet. Bei gezielter Umsetzung der ISO 27001 ergäben sich Synergien und Verbesserungspotenziale in Prozessabläufen.

Zertifizierung der Informationssicherheit ist das Thema eines Beitrags von Thomas Schmidt, Telefonbau Arthur Schwabe GmbH & Co. KG, in s+s report, Ausgabe 4-2017, S. 42–44. Durch die Zertifizierung werde eine kontinuierliche Informations-/Datensicherheit im Unternehmen verankert. Zudem ließen sich sowohl geschäftliche Risiken als auch die Gefahr einer individuellen Haftung der Geschäftsführer reduzieren. Der Autor behandelt bekannte Standards (ISO 27001, BSI IT-Grundschutz, Sicherer IT-Betrieb und die VdS 3473), die Umsetzung nach dem PDCA-Modell und den Weg zur Zertifizierung nach VdS 3473. Er listet die Themenblöcke auf, die im Rahmen dieser Zertifizierung bearbeitet werden.

Olaf Janßen, Sopra Steria Consulting, nimmt in der Dezember-Ausgabe des Behörden Spiegels zur **Automatisierung der Informationssicherheit** Stellung. Das IT-Sicherheitsmanagement müsse stärker automatisiert werden, beispielsweise über regelbasierte Prozeduren. Handlungsfelder seien: Prävention; Detektion von Anomalien, die auf mögliche Angriffe hindeuten; automatisierte Bewertung als erste Indikation; Reaktion zur Wiederherstellung von sicheren Systemen. Security Automation könne viele dieser Maßnahmen beschleunigen oder signifikant verbessern im Hinblick auf Qualität und Verlässlichkeit.

Virtual Private Network (VPN) als wichtiger Baustein für mobile Sicherheit thematisiert Jürgen Hönig, NCP engineering GmbH, in der Dezember-Ausgabe des Behörden Spiegels. VPN sicherten alle Daten zwischen Sender und Empfänger in einem verschlüsselten, hochsicheren Tunnel auf Basis bewährter und ausgereifter Technologie ab. Durch die Wahl der für das jeweilige Einsatzfeld richtigen Lösung sei selbst die Übertragung hochsensibler Daten durch das Internet absolut sicher. Der Schlüssel müsse sicher verwahrt sein, in der Regel über Hardware-Security-Module wie eine Smartcard. Und die Verschlüsselung dürfe nicht mit vertretbarem Aufwand aufhebbar sein. Aktuell bedeute das meist eine Verschlüsselung mit AES (Advanced Encryption Standard) auf Basis von elliptischen Kurven sowie den Einsatz eines sicheren Pseudozufallszahlengenerators.

Nach einer Meldung in der Dezember-Ausgabe von vekoonline baut die **Deutsche Telekom** die Cyberabwehr weiter aus. Das Unternehmen habe ihr neues integriertes Cyber Defense und Security Operation Center (SOC) in Bonn eröffnet. Rund 200 Experten überwachten dort und in den angeschlossenen Standorten national und international im 24-Stunden-Betrieb die Systeme der Telekom und die ihrer Kunden. Sie würden Cyberangriffe erkennen, die Angriffswerkzeuge analysieren, Angriffe abwehren und daraus Prognosen über zukünftige Muster von Attacken ableiten. Zahlen eines Arbeitstages: Analyse von einer Milliarde sicherheitsrelevanter Ereignisse aus 3.000 Datenquellen täglich; Auswertung von mehr als 6 Mrd. Datensätzen der Telekom DNS-Server bezüglich Cyberattacken; durchschnittlich 6 Mio. Angriffe auf die Honeypots. In der Malware-Library befänden sich mehr als 20 Mio. Schadcode-Samples.

„Sicherheitslücken im elektronischen Anwaltspostfach" titelt die FAZ am 28. Dezember. Eigentlich seien zum Jahreswechsel alle Anwälte in Deutschland gesetzlich verpflichtet, für elektronischen Postempfang bereitzustehen. Aber nun habe die Bundesrechtsanwaltskammer (BRAK) das umstrittene Digitalisierungsprojekt gestoppt. Ein Hacker vom Chaos Computer Club habe herausgefunden, dass ein wichtiger Code für die Authentifizierung sämtlicher Anwälte öffentlich abrufbar war. Das mache die Juristen anfällig für Hacker. T-Systems habe daraufhin den digitalen Ausweis eingezogen. Die darauf folgende Veröffentlichung einer Anleitung der BRAK, mit deren Hilfe die Nutzer ein neues Zertifikat herunterladen sollten, habe dazu geführt, dass die Nutzer, die die Anleitung befolgten, eine ungleich größere Sicherheitslücke öffneten: Sie reichten quasi den Schlüssel zum kompletten Internetverkehr des Rechners ein. Hacker hätten nun die Möglichkeit gehabt, sich in die Inhalte sämtlicher Kommunikation aller Nutzer des elektronischen Anwaltspostfaches einzuschleichen. Die BRAK habe den Anwälten daraufhin „dringend zur Deinstallation" des zuvor empfohlenen Zertifikats geraten.

IuK-Kriminalität

Olivia von Westernhagen weist auf heise.de am 30. November darauf hin, dass derzeit eine **Windows-Malware** im Umlauf sei, die auf infizierten Rechnern einen Bluescreen simuliert und den Bildschirm sperrt. Sie beende sich erst, wenn die Opfer Geld für eine nicht existente Sicherheitssoftware überweisen. Außerdem fertige sie einen Screenshot des Desktops an, um ihn an eine feste IP-Adresse zu verschicken. Diese Malware, Troubleshooter genannt, solle sich als Installationsprogramm für nicht näher bezeichnete gecrackte Software tarnen, um auf Rechner zu gelangen. Nach Download und Ausführung lade er mehrere Dateien nach, die unter anderem der Darstellung von Bluescreen und Warnhinweisen dienen. Eine der Dateien registriere sich als Windows-Dienst, um diverse Tastenkombinationen zu deaktivieren und so das Aufheben der Bildschirmsperre durch den Nutzer zu verhindern. Ein von Sicherheitsforschern erdachter „Workaround", der ganz ohne Zahlung auskomme, nutze ein von den Troubleshooter-Machern wohl unbeabsichtigt eingebautes „Feature". Der Nutzer könne so die Webseite mit dem Textstring eigenständig ansteuern, den Betrügern die erfolgte Zahlung vorgaukeln und Troubleshooter dazu bringen, sich vollständig zu beenden.

Eines der zentralen Probleme der E-Mail sei, dass deren **Absenderadressen nicht wirklich vertrauenswürdig** sind, sondern sich sogar leicht fälschen lassen (heise.de am 5. Dezember). Mit Hilfe von Anti-Spamtechniken wie DMARC (DKIM/SPF) könnten Mail-Server solche Tricksereien mittlerweile oft entlarven. Durch zusätzliche Tricks könnten Spammer das jedoch umgehen, wie der Sicherheitsforscher Sabri Haddouche demonstriere. Anfällig für diese Tricks sind laut Haddouche über 30 E-Mail-Programme.

Sicherheitsforschern zufolge nutzten 2017 ein Viertel aller Phishing-Webseiten HTTPS, um Opfer effektiver zu ködern (heise.de am 7. Dezember). Einer Umfrage zufolge würden viele denken, dass die **HTTPS-Kennzeichnung** Webseiten als sicher und legitim einstuft. In Wirklichkeit sorge die Kennzeichnung aber nur dafür, dass die Übertragung von Nutzerdaten an die Webseite verschlüsselt stattfindet.

Seit 2015 sei die Zahl der Angriffe mit **Ransomware** um den Faktor 2.000 gestiegen, schreibt Martin Schindler auf silicon.de am 7. Dezember. Im Vergleich zu 2016 steige die Zahl der Angriffe auf Unternehmen laut der Malwarebytes-Studie „The New Mafia: Gangs and Vigilantes – A Guide to Cybercrime for CEOs" um 23 Prozent. Es könne gefährliche Folgen haben, wenn Unternehmen nicht offen gegen Cyberattacken vorgehen. CEOs dürften Cyberkriminalität nicht mehr als ein technologisches Problem betrachten, sondern als geschäftskritisch. Die schädlichsten Cyberangriffe seien diejenigen, die lange unentdeckt bleiben.

Im **Jahresrückblick** hebt die FAZ am 2. Januar 2018 einige **Hackerangriffe** hervor: 150 Länder seien von der Hackerattacke namens „Wannacry" im Mai betroffen gewesen. Hunderttausende Computer hätten nicht richtig funktioniert. Noch härter habe es den britischen Gesundheitsdienst NHS getroffen. Wie bei „Wannacry" habe mit „Petya" eine sogenannte Ransomware-Attacke die Reederei Maersk lahmgelegt. Der dänische Logistiker schätze den Schaden auf 300 Mio. Dollar. Drei Mrd. Nutzerkonten seien vom Hackerangriff auf Yahoo schon 2013 betroffen gewesen, was das Unternehmen allerdings erst im Oktober 2017 eingestanden habe. 57 Mio. Kunden und Fahrer von Uber seien von einem Hackerangriff betroffen. Das habe der Fahrdienstleister Ende November 2017 eingeräumt. Uber habe den Angreifern sogar 100.000 Dollar gezahlt, damit diese die kompromittierenden Daten nicht weiterverkauften.

Im **Dark Web** habe man eine **Datenbank mit 1,4 Mrd. Log-in-Daten** im Clearformat gefunden, teilt der ASW-Newsletter am 21. Dezember mit. Es sei die bisher größte aufgetauchte Datenbank in dieser Form. Die Datensätze stammten aus 252 Angriffen und seien größtenteils bereits bekannt. 133 neue Datenleaks seien hinzugefügt worden. Die Datenbank enthalte die Zugangsdaten nicht nur in unverschlüsselter Form, sondern ermögliche die Suche über Benutzernamen. Stichproben der Sicherheitsforscher hätten ergeben, dass die meisten Datensätze gültige Zugangsdaten enthielten. Die Gefahren für betroffene Unternehmen seien nicht zu unterschätzen. Auch wenn nicht unbedingt die firmeninternen Zugangsdaten (Log-in) in der Datenbank zu finden sind, sei es Kriminellen möglich E-Mail- oder Social Media-Accounts zu übernehmen. Dadurch sei Betrug – wie CEO-Fraud – Tür und Tor geöffnet.

Kaspersky Lab habe eine neue, geradezu beeindruckend vielseitige **Android-Malware** entdeckt, heißt es in zeit.de am 20. Dezember. Loapi nenne das Unternehmen den Trojaner, der nach erfolgreicher Installation eine ganze Palette von Modulen nachladen könne. Diese bombardierten betroffene Nutzer mit Werbeeinblendungen, meldeten sie heimlich bei Bezahldiensten an, beteiligten sich an DDoS-Angriffen und schürften die Kryptowährung Monero. Das könne sogar dazu führen, dass sich der Smartphone-Akku „bis zu seiner Deformation aufheizen kann". Loapi werde laut Kaspersky Lab in inoffiziellen Android-App-Stores verbreitet sowie über bösartige Werbung auf Websites, etwa für Pornoseiten und vermeintliche Antivirus-Software. Infizierte Apps bäten nach der Installation so lange um Administratorrechte, bis Nutzer zustimmen. Symantec habe im laufenden Jahr 35 verschiedene Android-Apps entdeckt, die heimlich Kryptowährungen schürfen.

Krisenmanagement

In einem Hintergrundbericht im Newsletter des ASW vom 15. Dezember nimmt Marc Brandner, SmartRiskSolutions GmbH, Stellung zum **Krisenmanagement nach einem Datendiebstahl**. Es sei Cyberkriminellen im Oktober 2016 gelungen, rund 57 Mio. Daten von Kunden und Fahrern von einem Server beim Fahrdienst-Vermittler Uber zu entwenden. Die Erpresser kontaktierten Uber und verlangten 100.000 Dollar für die Löschung der Kopien. Die Lösegeldzahlung sei durchgeführt worden. Zur weiteren Verschleierung des Datendiebstahls sei die Zahlung firmenintern als Honorar für einen Penetrationstest durch Hacker verbucht worden. Erst ein Jahr später habe das Unternehmen diesen schwerwiegenden Vorfall eingeräumt. Gegen folgende Grundsätze des Krisenmanagements wird nach Überzeugung des Autors oft verstoßen: 1. Einen Vorfall zu vertuschen ist oft schlimmer als der Vorfall an sich. 2. Eine Krisenkommunikation sollte Antworten auf die Fragen liefern, die von Interesse sind. 3. Bei Cyberangriffen ist die Krisenreaktion oft zu sehr auf die Technologie gerichtet.

Kritische Infrastrukturen

Nach einer Meldung in GIT, Ausgabe 12-2017, S. 73, hat das BSI mit dem branchenspezifischen **Sicherheitsstandard (B3S) Wasser/Abwasser** die Eignung des ersten Sicherheitsstandards für einen KRITIS-Sektor festgestellt. Betreiber Kritischer Infrastrukturen aus dem Sektor Wasser, die den Anforderungen des IT-Sicherheitsgesetzes unterliegen, müssten ihre Informationstechnologie nach dem Stand der Technik absichern und könnten dies nun anhand des B3S umsetzen. Der B3S Wasser/Abwasser enthalte Rahmenanforderungen, die auf die tatsächlichen Gegebenheiten im KRITIS-Sektor Wasser zugeschnitten sind, eine Vorgehensweise zur Risikoanalyse sowie eine Sammlung von Sicherheitsmaßnahmen, um den identifizierten Risiken zu begegnen.

Auf eine neue **Cyberattacke namens Triton** auf Kritische Infrastrukturen weist die FAZ am 20. Dezember hin. Es sei Hackern wiederholt gelungen, sich Zugang zu den Systemen Kritischer Infrastrukturen zu verschaffen. Die Täter ließen sich kaum ermitteln, denn mitunter lösche sich die Schadsoftware nach getaner Arbeit selbst. Jetzt hätten die amerikanischen Cybersicherheitsfirmen FireEywe und Dragos einen Angriff auf die Sicherheitsmechanismen eines Kontrollsystems nachgewiesen, wie es in Atom-, Wasser- oder Gaskraftwerken eingesetzt wird. Schadprogramme, die auf Kritische Infrastrukturen zielen, gebe es seit längerem. Die bekannteste Malware dieser Art, „Stuxnet", habe 2010 auf die Datenströme der Mess-, Steuer- und Regelungstechnik in der Urananreicherungsanlage im iranischen Natanz gezielt. Betroffen seien im jüngsten Fall die industriellen Sicherheitssysteme von Schneider Electronics, einem Elektrotechnik-Konzern mit Sitz in Frankreich. Triton gehöre zu einer der schon identifizierten Software-Familien, die es gezielt auf industrielle

Kontrollsysteme abgesehen hätten. Daher ähnele es sowohl Stuxnet als auch Industroyer, das im Dezember 2016 die Steuerungssoftware ukrainischer Umspannwerke angegriffen habe. Nach einer Analyse des US-Heimatschutzministeriums übertrifft die Schadsoftware Stuxnet und Industroyer, da sie fähig sei, direkt mit Sicherheitsmechanismen zu interagieren, „sie fernzusteuern und zu kompromittieren".

Logistiksicherheit

Für eine umfassende Überwachung des **Transports von Pharmazeutika** plädiert PROTECTOR in der Ausgabe 12-2017, S. 68/69. Die Pharmaspedition Transco lasse den gesamten Transport ab Verladerampe bis zum Empfänger rund um die Uhr in Echtzeit überwachen. Der Auflieger, ein High Security-Trailer, verfüge über diverse Sicherheitsfunktionen, so zum Beispiel alarmgesicherte Seitenwände und Dachfläche, ein per Code und Fernsteuerung nur vom Disponenten zu öffnendes Heckportal und die GPS-Fernüberwachung von Laderaum-Temperatur, Türstatus sowie Fahrzeugposition. Bei Abweichungen alarmiere TCS umgehend alle relevanten Prozessbeteiligten.

Das Fachmagazin info Sicherheit, Ausgabe 4-2017, S. 39, weist auf die Gründung einer **Kommission Logistiksicherheit des Deutschen Speditions- und Logistikverbandes** im Oktober hin. Ziel des Ausschusses sei die Entwicklung verkehrsträgerübergreifender Strategien zur Gefahrenabwehr sowie die Bewertung zukünftiger Gesetzgebungsvorhaben.

Maschinensicherheit

Integrierte Sicherheitstechnik für alle Maschinenversionen thematisiert Franz Kaufleitner, B&R, in GIT, Ausgabe 12-2017, S. 92/93. Bei Low-Cost-Maschinen mit wenigen Funktionen komme häufig immer noch hartverdrahtete Sicherheitstechnik zum Einsatz. Bei Varianten mit anspruchsvollerer Sicherheitstechnik hingegen seien programmierbare Sicherheitssysteme der Standard. Effizient wäre es, wenn die programmierbare Sicherheitsapplikation das gesamte Funktionsspektrum kosteneffektiv abdecken würde. Mit der sogenannten **Safelogic-X von B&R** sei integrierte Sicherheitstechnik zu einem Preis erreichbar, der mit hartverdrahteter Relaistechnik oder kompakten Sicherheitsgeräten konkurrieren könne. Möglich sei dies, weil die Aufgaben einer Sicherheitssteuerung auf sowieso vorhandene Komponenten im Automatisierungssystem verteilt werden. Während die hartverdrahtete Sicherheitstechnik als Reaktionsmöglichkeit im Prinzip nur das Abschalten zulasse, unterstütze Safelogic-X auch sichere Antriebe mit umfangreichen Funktionen und besonders kurzen Reaktionszeiten. Die Kleinst-Sicherheitssteuerung unterstütze auch die Vorteile modularer Maschinenkonzepte und die integrierte Diagnose. Die Lösung von B&R mache integrierte Sicherheitstechnik über alle Maschinenkategorien hinweg durchgängig und skalierbar.

Sicherheitssteuerungen mit Funktionsblöcken für **mechanische und hydraulische Pressen** präsentiert Jörg Packeiser, Leuze electronic, in der Zeitschrift GIT, Ausgabe 12-2017, S. 96/97. Die Sicherheitssteuerungen MSI400 von Leuze electronic seien kompakt aufgebaut und speziell für den Einsatz an Exzenter- und Hydraulikpressen ausgelegt. Außerdem erfüllten die neuen Steuerungen die Anforderungen nach den Normen EN 692 für mechanische sowie EN 693 für hydraulische Pressen. Die vordefinierten Pressen-Funktionsblöcke, Simulations-Funktion und Log-Generator machten die Programmierung und Projektierung schnell und einfach. Sie ermöglichten die Überwachung des Pressenablaufs und die einfache Realisierung verschiedener Betriebsarten. Bediengeräte wie z. B. Zweihand-, Fuß-, Not-Aus und Betriebsartenwahlschalter sowie Sicherheits-Sensoren könnten flexibel eingebunden werden. Der Autor beschreibt vielfältige Kommunikationsmöglichkeiten und die Erweiterbarkeit, die hohe Funktionsreserve und einfache Programmierung mit MSI.designer. Das MSI-Basismodul sei über kompakte Erweiterungsmodule nach Baukastenprinzip auf bis zu 116 sichere Eingänge und 56 sichere Ausgänge erweiterbar. Damit eigne sich die Produktfamilie auch gut für die sichere Steuerung größerer Maschinen und Anlagen.

Sicherheitsingenieur Peter Keller erläutert im Sicherheitsforum, Ausgabe 6-2017, S. 14/15, die grundlegenden Sicherheits- und Gesundheitsschutzanforderungen, die Maschinen bei wesentlichen Änderungen erfüllen müssen. Eine solche **wesentliche Änderung** läge vor, wenn mindestens eines der folgenden drei Kriterien erfüllt ist: Die bestimmungsgemäße Verwendung wird erweitert. Oder es entstehen neue Gefährdungen, vor denen die bestehenden Schutzmaßnahmen nicht schützen. Oder eine alte Technologie wird durch eine neue ersetzt. Bei einer

„verketteten" Anlage würden diese Kriterien auch bei einer wesentlichen Änderung einer Teilanlage gelten.

Naturkatastrophen

Der **VdS GeoRiskReport** bildet das Thema eines Beitrags von Svenja Welter M.A., VdS, in s+s report, Ausgabe 4-2017, S. 58/59. VdS Schadenverhütung unterstütze die deutsche Versicherungswirtschaft mit professionellen Geodaten und deren Anwendungen für Risikoabschätzungen oder für die Überprüfung von Schadenfällen. VdS GeoExpertise biete eine fundierte Datenbasis in Form eines Kompaktreports für Betriebe und Unternehmen.

Unwetter, Stürme und Hagel haben die Versicherer in Deutschland 2017 zwei Mrd. Euro gekostet, meldet die FAZ am 29. Dezember. Damit sei **2017 ein unterdurchschnittliches Naturkatastrophenjahr** gewesen. Am heftigsten hätten die Sturmtiefs „Paul" und „Rasmund" gewütet, die Ende Juni und Anfang Juli in Norddeutschland versicherte Schäden von 300 Mio. Euro angerichtet hätten. Im langjährigen Durchschnitt zahlten die Versicherer rund 2,4 Mrd. Euro im Jahr für die Folgen von Naturereignissen in Deutschland.

Notruf

Personenortung in Gebäuden thematisiert das Unternehmen SoftClean GmbH in PROTECTOR, Ausgabe 12-2017, S. 72. Dies ermögliche eine neue Technologie: Bluetooth-Low Energy-Beacons seien fest angebrachte Sender, die dank eingebauten Batterien über Jahre hinweg permanent ein Signal versenden. Jeder Sender könne dabei mit Hilfe einer Konfigurationsanwendung individuell an die Bedürfnisse und Örtlichkeiten angepasst werden. Die Signale würden dabei bis zu 50 Meter weit und im Millisekundentakt versendet. Je mehr Sender sich in der Umgebung der Örtlichkeit befinden und vom Smartphone erfasst werden, desto genauer sei die errechnete Position. Die Erfassung der Signale geschehe dabei völlig automatisch durch die Smartphones der Mitarbeiter. Automatisch könne in bestimmten Bereichen eine erhöhte Überwachung mit Lagesensor, Fallsensor oder Totmannschaltung erfolgen.

Mit **Notfall- und Notruf-Lösungen** befasst sich Security insight in der Ausgabe 6-2017, S. 34/35. Mit der Norm VDE 0827 stehe ein ausführliches Regelwerk zur Verfügung, das im Lösungs-Dschungel Orientierung schaffe. Dargestellt würden darin unter anderem technische Systeme, die sich in individuellen Gefahrenfällen dazu eignen, Hilfe herbeizurufen, Amokalarme auszulösen und Handlungsanweisungen zu übertragen. Als besonders sinnvoll hätten sich Notfall- und Gefahren-Reaktionssysteme auf Intercom-Basis herausgestellt. Sie bestünden in aller Regel aus einer individuell festgelegten Anzahl von fest integrierten Sprechstellen und ermöglichten durch eine ständige Sprechverbindung den direkten Austausch zwischen Leitstelle und der meldenden Person. Inzwischen seien für den Einsatz in Behörden oder in Einrichtungen wie Bürgerbüros auch hochverfügbare Notfall-Apps verfügbar. Die Norm 0827 erlaube ausdrücklich den Einsatz mobiler Systeme.

Perimeterschutz

Carsten Hoersch, SESAM GmbH, befasst sich in der Ausgabe 12-2017 von PROTECTOR, S. 36/37, mit der Einbruchtechnik. Seit einiger Zeit seien **Dualbewegungsmelder** am Markt erhältlich, die durch die Verwendung von Passiv-Infrarottechnik, gekoppelt mit einer digitalen Temperaturkompensation und fortschrittlicher Mikrowellentechnik, zuverlässig melden und Störeinflüsse ausblenden. Ein solcher Melder finde seinen Platz besonders im Außenbereich. Um Manipulationen zu verhindern, seien Melder erhältlich, die eine zuverlässige, integrierte Abdecküberwachung beinhalten. Bei besonders empfindlichen Detektoren sei ein Beschleunigungssensor integriert, der Bewegungen des Melders selber erkennt und dann eine Sabotagemeldung absetzt. In Kombination mit einem Alarmsignal, einer automatischen Lautsprecherdurchsage in Verbindung mit dem Schalten von Licht oder dem Absetzen einer Meldung an die angebundene NSL erlange man eine große Bandbreite von möglichen Gegenmaßnahmen, um effektiv gegen Vandalismus vorgehen zu können.

Martin Vogler, Senstar, beschreibt in der Ausgabe 12-2017 der Zeitschrift GIT, S. 50/51, **aktuelle technische Entwicklungen** in der Perimetersicherheit. Der Autor geht auf die Videotechnik, auf kombinierte Lösungen und unverzichtbare Technologien ein. Faseroptische Systeme hätten in den letzten Jahren stark an Interesse gewonnen. Mit faseroptischen

Kabeln ließen sich auch Systeme über größere Distanzen relativ simpel und ohne große zusätzliche Infrastrukturinvestitionen verwirklichen. Einige bereits bekannte Systeme und Technologien seien unverzichtbar. Ganz oben zu nennen sei das Bodendetektionskabelsystem. Kein anderes System sei so zuverlässig und vertrauenswürdig bei geringsten Unterhaltungsaufwendungen.

Produkterpressung

Wie die FAZ am 5. Dezember berichtet, geht das Risiko- und Krisenberatungsunternehmen Result Group von **50 bis 200 Produkterpressungsfällen jährlich** in Deutschland aus. Eine Einschätzung des Phänomens werde durch die Tatsache erschwert, dass Unternehmen fast immer die Öffentlichkeit scheuen. Die Täter seien in der Regel überdurchschnittlich intelligent, selten Mitarbeiter der betroffenen Unternehmen. Zu mehr als 90 Prozent handele es sich um Männer. Sie seien meist nicht vorbestraft, hätten aber finanzielle Probleme. Die Geldübergabe gelte als der kritische Punkt, an dem Erpresser ihre Anonymität verlassen müssen und in den meisten Fällen gefasst werden. Allerdings hätten sie in den letzten Jahren dazugelernt und tendierten beim Transfer des Erpressungsgeldes mehr zu Kryptowährungen als Alternative zu Bargeld.

Schließsystem

Security insight stellt in der Ausgabe 6-2017, S. 22/23, das Zutrittskontrollsystem für das **Forum Museumsinsel** in Berlin-Mitte mit acht denkmalgeschützten Gebäuden vor. Es nutze ein besonders widerstandsfähiges, mechanisches System: 3KS (3-Kurvensystem). Die Sperrelemente im 3KSplus-Zylinder würden über die Kurvenfräsung am Schlüssel bewegt und nicht gegen eine Federkraft gedrückt. Insgesamt werde während des Sperrvorgangs der Schlüssel in diesem System „in Summe 4-mal abgefragt". Die federnfreie Sperrstiftfunktion garantiere dabei höchste Verschleißfestigkeit und Pickingschutz.

Erläutert wird in Security insight, Ausgabe 6-2017, auch das Schließsystem von CES für die **Elbphilharmonie** (S. 24/25). Das Schließsystem funktioniere im Zusammenspiel mit der elektronischen Zutrittskontrolle und der Fluchttürsteuerung (FTS). So könnten die Haustechniker mit ihrem Bereichsschlüssel gleichzeitig die in die FTS-Terminals integrierten Schlüsselschalter bedienen und damit Verbindungstüren und Lastenaufzüge flexibel steuern. Im Normalfall erfolge für eine Kurzzeitfreigabe der Zutritt über eine Transponderkarte. Ein Plus an Sicherheit gewährleiste die Verknüpfung von elektronischer Zutrittskontrolle und mechanischem Schließsystem auch bei der Steuerung der Besucherströme. Bis in die 20. Etage seien dezentrale Schlüsseltresore angebracht. Mithilfe eines untergeordneten Schlüssels könne die Entnahme eines ranghöheren Schlüssels elektronisch abgesichert erfolgen, sodass im Bedarfsfall der Zugang zu zentralen Gebäudebereichen möglich ist. Auf dem Schlüsseltresor befinde sich ein elektronischer Leser. Mithilfe eines Kombischlüssels identifiziere sich der Nutzer über den Leser. Der ebenfalls auf dem Schlüsseltresor angebrachte Bereichsschlüssel werde damit freigeschaltet und über die mechanische Schließung ausgegeben.

Sicherheitsgewerbe

Jens Müller, Securitas Deutschland, erstellt in der Ausgabe 12-2017 der Zeitschrift GIT, S. 30/31, den **politischen Forderungskatalog des Sicherheitsgewerbes** zu Beginn der 19. Legislaturperiode. Nach seiner Überzeugung könnte das Potenzial des Sicherheitsgewerbes zur Unterstützung der Polizei und der Sicherheitsbehörden wesentlich stärker ausgeschöpft werden, wenn einige politische und rechtliche Rahmenbedingungen verbessert werden würden. Im Vordergrund des Beitrags stehen die Forderungen nach Erhöhung der Barriere zur Gründung eines Sicherheitsunternehmens, nach Verbesserungen des Vergaberechts, nach einem spezifischen Sicherheitsleistungsgesetz und nach Übergang der staatlichen Aufsicht von den Wirtschaftsministerien zu den Innenministerien des Bundes und der Länder.

Sicherheitsmarkt

Kirsten Wiegand, BDSW, stellt in der Ausgabe 4-2017 des DSD, S. 32/33, das Forschungsprojekt „Die Ordnung des Sicherheitsmarktes" (**OSiMa**) vor. Auf Grundlage der Forschungsergebnisse werde eine Informationsplattform entwickelt. Diese solle

Führungskräften in Politik, regulierenden Behörden und in Unternehmen als Entscheidungshilfe dienen, wenn in Bezug auf „bestehende oder sich entwickelnde Aufgabenfelder" zu klären sei, ob, in welcher Weise oder in welchem Umfang Schutzleistungen unter Mitwirkung nichtstaatlicher Akteure erbracht werden können und sollen.

Sicherheitstechnik

Die Fachzeitschrift GIT stellt in der Ausgabe 12-2017, S. 12–16, die Gewinner des **GIT Sicherheit Award 2018** vor. Es sind – jeweils in der Reihenfolge 1.,2. und 3. Sieger – in den Kategorien sichere Automatisierung: Sicherheits-Laserscanner Keyence SZ-V, Sicherheitslichtschranken Schmersal SLB 240/440 und bidirektionales Funk-Sicherheitsmodul UH 6900 von Dold; Brandschutz, Ex- und Arbeitsschutz: Brandmelder Novar in Kombination mit Designerleuchte, Gefahrstoffschrank Asecos V-MOVE-90 und Kombi-Brandschutz von Prymos (Feuerlöscher-Spray und PM10 DIN EN 3 Feuerlöscher); in der Kategorie Videosicherheit: optische und thermische Kamera MIC IP fusion 9000i von Bosch, Netzwerk-Kamera P1368-E von AXIS und F8225IH-A von Hikvision; in der Kategorie Einbruch- und Perimeterschutz: mechatronisches Zutrittskontrollsystem Cliq Go von Assa Abloy, schlüsselloses Zutrittsmanagement MobileKey von SimonsVoss und elektronischer Türbeschlag mit Kurzschild CX6174 von Uhlmann & Zacher; in der Kategorie Sicherheitsmanagement: virtuelle Schlüsselbund-App Tapkey von Dom, Gefahrenleitsystem Siveillance Viewpoint von Siemens und Entscheidungshilfesystem Mission Control von Genetec.

Wartung und Unterhalt von Sicherheitsgewerken thematisiert Thomas Streit, Bouygues Energies & Services Schweiz AG, im Sicherheitsforum, Ausgabe 6-2017, S. 50–53). Für die Gewährleistung der Betriebssicherheit sei eine angemessene und rechtskonforme Instandhaltungsstrategie inklusive Wartung und Unterhalt von Sicherheitsgewerken erforderlich. Der Autor behandelt integrale System- und Verbundtests, Blackout-Tests, die Life-Cycle-Bewirtschaftung, die Rolle des Facility Management-Providers bei Umbauprojekten und die Qualitätssicherung. Für den erfolgreichen Betrieb von sicherheitsrelevanten Anlagen seien primär die dafür verantwortliche Organisation mit ihren Mitarbeitenden, deren Fachkenntnisse und ihr tägliches Engagement sowie die erarbeiteten Prozesse von erfolgsentscheidender Bedeutung.

Spionage

Die **Machenschaften chinesischer Geheimdienste im Internet** machen den deutschen Sicherheitsbehörden zunehmend Sorgen, heißt es auf tagesspiegel.de am 11. Dezember. Das BfV habe nach eigenen Angaben „massive Aktivitäten" in sozialen Netzwerken festgestellt. Bei mehr als 10.000 deutschen Staatsangehörigen sei es zu Kontaktversuchen gekommen. Die Experten des BfV beobachteten, dass die Nachrichtendienste Chinas in sozialen Netzwerken eine Vielzahl von Fake-Profilen einrichteten. Die Akteure tarnten sich als Mitarbeiter von Headhunting-Agenturen, Consulting-Firmen, Think Tanks oder als Wissenschaftler. Besonders aufgefallene „Fake-Profile" werden in dem Beitrag angeführt. Auch bei chinesischen Cyberattacken sehe das BfV neue Methoden. Verstärkt genutzt würden „Supply-Chain-Angriffe". Sie richteten sich nicht mehr direkt gegen das eigentliche Opfer. Stattdessen würden zunächst IT-Dienstleister angegriffen, die für die auszuspähende Organisation tätig sind. Solche „Infektionen" seien nur schwer zu erkennen, da die Netzwerkverbindungen zwischen Dienstleister und Kunde nicht auffällig seien.

Terrorismus

Die FAZ berichtet am 22. Dezember über die Festnahme eines in Deutschland geborenen Mannes mit irakischen Wurzeln, der dringend verdächtigt werde, er habe ein Fahrzeug in die Stände rings um die Eisfläche auf dem Karlsruher Schlossplatz steuern wollen. Er soll auch Propaganda für die Terrororganisation IS verbreitet und sich während zweier Aufenthalte im Irak dem IS angeschlossen haben.

Unternehmenssicherheit

Unter dem **Begriff „integrierte Sicherheit"** verstehe man eine ganzheitliche Betrachtung der Unternehmenssicherheit in den Bereichen Technik, Organisation und Personal, wobei einzelne Sicherheitsmaßnahmen aufeinander abgestimmt seien und zu einer ganzheitlichen Lösung führten. Dabei umfasse integrierte Sicherheit den kompletten Prozess von der Projektinitialisierung, der Planung, der Realisierung über

die Abnahme bis zum Betrieb einschließlich aller technischen, organisatorischen und personellen Anforderungen. Experten des BDSW und des Verbandes für Sicherheitstechnik (VfS) haben eine Handlungsempfehlung für integrierte Sicherheit erarbeitet (Security insight, 6-2017, S. 53).

Christian Schaaf, Corporate Trust, Business Risk & Crisis Management GmbH, erläutert in der Dezember-Ausgabe von veko-online **zukünftige Anforderungen an Sicherheit**. Sein Unternehmen habe zusammen mit dem Bayerischen Verband für Sicherheit in der Wirtschaft und der Brainloop AG einen Future Report herausgegeben, in dem weltweite Megatrends und ihre Sicherheitsherausforderungen betrachtet würden. Dazu seien in Deutschland und Österreich 4.738 Vorstände bzw. Leiter der Bereiche Unternehmenssicherheit, Risikomanagement, Informationsschutz, Compliance, Recht, Finanzen, Controlling, IT oder Personal zu ihren Schäden befragt worden. Danach sei über die Hälfte der Unternehmen in Deutschland in den letzten zwei Jahren Opfer eines Angriffs durch OK geworden. Auf der Grundlage des Global Risk Report 2017 des World Economic Forum seien die zehn wichtigsten Sicherheitstrends der Zukunft für Deutschland abgeleitet worden. Der Autor befasst sich mit dem Informationsschutz, dem „Faktor Mensch" und der Organisierten Kriminalität (OK). Sie werde bei den Angriffen auf Unternehmen künftig eine ganz herausragende Rolle spielen. Bei der oben genannten Befragung hätten 51,6 Prozent der Unternehmen angegeben, bereits Opfer eines OK-Angriffs geworden zu sein. In 38,6 Prozent der Fälle sei es zu Social Engineering durch Cyberattacken gekommen. Bei 25,6 Prozent sei es zu einer „Fake-President-Attacke" gekommen und 16,1 Prozent seien nach einem Ransomware-Angriff oder einer DDoS-Drohung erpresst worden.

Veranstaltungsordnungsdienst

Ass. Jur. Martin Hildebrandt, BDSW, stellt in der Ausgabe 4-2017 des DSD, S. 34, das **Projekt „ProVOD"** zur Professionalisierung des Veranstaltungsordnungsdienstes vor. Es entwickele in einem interdisziplinären Verbund Lösungsansätze für eine Professionalisierung durch Sondierung der tätigkeitsspezifischen Problemstellungen. Das Projekt verfolge insbesondere folgende Ziele: Erhebung von Kennzahlen zur Bestimmung und Abgrenzung der Teilbranche VOD; Etablierung des VOD als eigenständige Teilbranche mithilfe der Definition rechtlicher und organisationaler Standards; Professionalisierung durch Erarbeitung von einheitlichen Qualifizierungsmaßnahmen; Verbesserung der öffentlichen Wahrnehmung des VOD; Übertragung der Ergebnisse auf einen internationalen Kontext. Eine Umfrage unter Mitarbeitern im VOD habe zum Beispiel ergeben, dass 75 Prozent mindestens eine interne VOD-Schulung absolviert haben, wobei die Dauer zwischen 30 Minuten und zwei Tagen variiere. Ein knappes Drittel habe gar keine VOD-Qualifikationen. Die vom BDSW entwickelte Definition des VOD, in der die Tätigkeit vom Sicherheitsdienst bei Veranstaltungen abgegrenzt wird und die nur die Erfüllung nicht sicherheitsrelevanter Tätigkeiten umfasst, werde nur teilweise angewandt.

Videoüberwachung

Optimale Storage-Lösungen für Videoanlagen stellt Gabriel Chaher, Quantum GmbH, in der Ausgabe 12-2017 der Zeitschrift PROTECTOR, S. 42/43, vor. Um schnell auf die Werkzeuge in einer Videoanlage zugreifen zu können, benötigten Unternehmen eine Technologie-Infrastruktur, die auf einem Storage-File-System basiert, das auf Videoanlagen spezialisiert ist. Für die Steuerung umfangreicher Prozesse werde eine spezielle Videomanagementsoftware (VMS) eingesetzt. Dazu werde ein Dateisystem benötigt, das für Schreib- anstatt Lesevorgänge optimiert ist. Dabei müsse das System in der Lage sein, simultan Videomaterial von zahlreichen Kameras einzuspeisen und gleichzeitige Schreiboperationen auszuführen, ohne dass es zu Engpässen bei der Ein-/Ausgabe kommt – eine große Herausforderung. Die Storage-Kosten machten bis zu 60 Prozent des Budgets für ein Videoüberwachungssystem aus. Für eine ausgeglichene Storage-Konfiguration seien Tiered-Storage-Architekturen mit mehreren Speicherebenen der Schlüssel, denn sie setzten Speicherkosten und Datenwert in das richtige Verhältnis. Der Vorteil: ältere oder selten benötigte Daten könnten auf kostengünstigeren Speicherebenen, wie Tape, Object-Storage oder Cloud vorgehalten werden. File-Systeme verfolgten einen Ansatz, der sich besser für die Verwaltung von Video eignet als „Information Lifecycle Management". Filesysteme seien für Videoanwendungen mit der VMS-Software integriert und erforderten keine separate Archivierungs- oder Data-Mover-Anwendung. Aus Benutzersicht seien die unterschiedlichen Ebenen nicht erkennbar.

Wichtige Anpassungen der **VdS 2366** an technische Neuerungen erläutert Dipl.-Wirtschaftsjurist (FH) Sebastian Brose in s+s report, Ausgabe 4-2017, S. 54/55. Mit der Überarbeitung seien die VdS 2366 nun noch praxisnäher und böten fachkundigen Betreibern und Errichterunternehmen eine ideale Grundlage zu Planung, Projektierung, Betrieb und Instandhaltung von hochwertigen Videoüberwachungsanlagen. Zur Dokumentation einer VdS-anerkannten Videoüberwachungsanlage diene das Attest VdS 3426.

Die Entwicklung **„von der Diode bis zum neuronalen Netz"** beschreibt Peter Treutler, IPS Intelligent Video Analytics, in der Ausgabe 12-2017 der Zeitschrift GIT, S. 66–68. Es bestehe nach wie vor hohes Interesse der Kunden an serverbasierten Videoanalysen, auch weil sie „performanter" seien als kameraintegrierte Systeme. Aufgabe der an das Videomanagementsystem (VMS) von IPS angebundenen Radar-Sensorik sei die Drohnendetektion. Die Sensorik sei ebenso wie die Kameras 3-D-kalibriert und georeferenziert und gebe die 3-D-Koordinaten an das VMS weiter. Das steuere dann Dome Kameras genau an diese Stelle. Die technische Herausforderung der Videoanalyse bestehe heute darin, Objekte zu erkennen und zu verfolgen, die sich in belebten Szenarien bewegen. Hinzu kämen die in diesen Szenarien auftretenden Störgrößen, wie z. B. Blätter oder gar die zeitweise komplette Verdeckung des Zielobjekts. Diese Störgrößen zu minimieren, sei der wichtigste technologische Trend. Die Analyse IPS Public Transport Protection erkenne z. B., wenn eine Person sich auf dem Gleisbett befindet, wenn ein Zug einfährt. Das sei für die Analysesoftware viel komplexer als eine normale Trip/Wire-Anwendung. Es gehe um Höhenunterschiede und viele besondere Abhängigkeiten und Kriterien.

In einem Modellprojekt in Mannheim sollen Kameras mithilfe von Algorithmen Kriminalität bekämpfen, berichtet die FAZ am 30. Dezember. Der Bahnhofsvorplatz, der Alte Messplatz, die Breite Straße und der Plankenkopf sollen von 2018 an mit einem intelligenten Videosystem überwacht werden. Die Software zur Auswertung der Aufnahmen sei so intelligent, dass sie künftig **typisches kriminelles Verhalten erkennen** soll. Es handele sich um ein System mit einer automatischen Aktivitätserkennung und „Multi-Kamera-Tracking". Hinter einer erfolgreichen Videoüberwachung müsse zwingend ein Interventionskonzept der Polizei stehen. Die Software sei noch in der Entwicklung. Die Stadt entwickele das System gemeinsam mit dem Fraunhofer Institut für Optronik, Systemtechnik und Bildauswertung. Erste Erfahrungen könnten Ende 2018 vorliegen.

Wettbewerbsregister

DSD stellt in der Ausgabe 4-2017, S. 43–45, **das neue Wettbewerbsregister** vor. Es solle gewährleisten, dass bundesweit alle Auftraggeber tatsächlich von Delikten der Bieter erfahren. Künftig reiche eine elektronische Abfrage beim bundesweiten Wettbewerbsregister, damit öffentliche Auftraggeber schnell und einfach zuverlässige Informationen über Rechtsverstöße von Unternehmen erhalten. In das Register würden Unternehmen eingetragen, gegen die selbst ein Bußgeldbescheid erlassen wurde oder die sich die Straftat eines Mitarbeiters zurechnen lassen müssen. Dem Unternehmen zugerechnet würden dabei nur Straftaten von Führungspersonen des Unternehmens. Bevor ein Unternehmen den Zuschlag für einen öffentlichen Auftrag mit einem Auftragswert von über 30.000 Euro erhält, müsse der öffentliche Auftraggeber durch Abfrage beim Wettbewerbsregister prüfen, ob dieses Unternehmen eingetragen ist. Daneben könnten Auftraggeber freiwillig auch bei kleineren Aufträgen die Informationen aus dem Register abfragen. Sie hätten auch die Möglichkeit, schon zu Beginn eines zweistufigen Vergabeverfahrens von der Registerbehörde Angaben zu in Frage kommenden Unternehmen zu erlangen. Bei Delikten, bei denen nicht zwingend der Ausschluss von Vergabeverfahren vorgeschrieben ist, entscheide der öffentliche Auftraggeber eigenverantwortlich je nach Einzelfall, ob er das eingetragene Unternehmen von der Teilnahme ausschließt. Die Entscheidung des Bundeskartellamtes, dass die „Selbstreinigung" eines in das Wettbewerbsregister eingetragenen Unternehmens erfolgreich war, habe Bindungswirkung für die öffentlichen Auftrag- und Konzessionsgeber.

Wirtschaftsschutz

In seinem Newsletter vom 15. Dezember kündigt der Bundesverband ASW einen neuen **Baustein des Wirtschaftsgrundschutzes** an. Er liefere Verantwortlichen einer Institution eine Hilfestellung für die strukturierte Vorgehensweise zur Erreichung eines angemessenen Produkt- und Know-how-Schutzes und zeige die wesentlichen Grundsätze für das Etablieren eines angemessenen Management- und Regelsystems für diesen Bereich auf. Das Handbuch umfasse nun drei Standards und dreizehn Bausteine.

Impressum

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

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

Herausgeber
Manfred Buhl, Vorsitzender der Geschäftsführung, Düsseldorf

Verantwortlicher Redakteur
Bernd Weiler, Leiter Kommunikation und Marketing

Beratender Redakteur
Reinhard Rupprecht, Bonn

www.securitas.de/focus

Kontakt

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

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

E-Mail: info@securitas.de