FOCUS ON SECURITY

AUSGABE 11, NOVEMBER 2017

SECURITAS

Inhaltsverzeichnis

Arbeitsschutz

In der Ausgabe 10-2017 der Zeitschrift GIT, S. 87, wird auf die sicheren **GfG-Mehrgaswarngeräte** Microtector III G888 und Polytector III G999 hingewiesen, die höchste Ansprüche an Technik, Funktion, einfache Bedienung, Langlebigkeit und Design erfüllten. Im Alarmfall würden die Geräte durch eine Hupe mit 103 dB Schalldruck vor Gasgefahren warnen. Anhand unterschiedlicher Tonsequenzen sowie der Displayfarben grün, gelb und rot erkenne der Anwender zuverlässig, ob er sich in einer sicheren, belasteten oder sogar gefährlichen Atmosphäre befindet. Die neuen Gaswarngeräte verfügten standardmäßig über einen Man-Down-Alarm und optional über ein Funkmodul mit Signalüberwachung. Im G888 und G999 könnten bis zu fünf Sensoren für unterschiedlichste toxische und brennbare Gase sowie Sauerstoff verbaut werden.

Sean Clay, Honeywell Industrial Safety, plädiert in der Ausgabe 10-2017 der Zeitschrift GIT, S. 100/101, dafür, dass eine vernetzte Sicherheitslösung, bei der modernste Technologie zur kontinuierlichen Überwachung **der Umwelt- und Mitarbeiterbelastung** eingesetzt wird, dazu beitragen könne, dass Manager besser fundierte Entscheidungen treffen können. Kleinere sensortechnische Lösungen, reduzierter Stromverbrauch, die allgegenwärtige drahtlose Konnektivität und das Smartphone als persönlicher Netzknoten sorgten gebündelt dafür, dass diese Lösung verwirklicht werden könne. Sensoren könnten in der persönlichen Schutzausrüstung (PSA) integriert werden, um Daten an der Stelle zu erfassen, an der die einzelne Person in die Arbeitsumgebung eintritt.

Betrug

Die FAZ weist am 5. Oktober auf **„Ping Calls"** hin, die in den vergangenen Monaten öfters vorkämen. Das Handy klingele nur ganz kurz und dann erscheine die Anzeige „verpasster Anruf" mit einer Telefonnummer wie 21628792676 oder zum Beispiel 2122602763941. Bevorzugt werde der Anruf in die Netze solcher Länder ausgelöst, deren nationale Kennung den lokalen Vorwahlen des Landes ähnelt, in dem der Angerufene sich befindet. Wer die Nummer zurückrufe, lande auf einer besonders teuren Nummer in dem Land, aus dem der Anruf kommt. Der Betrüger bekomme das Geld, der Anrufer zahle per Telefonrechnung.

Biometrie

Die FAZ zitiert am 4. Oktober Chinas obersten Sicherheitschef Meng Jianzhu mit den Worten **„Künstliche Intelligenz** ist schneller als die menschliche und wird die Berechenbarkeit und die Genauigkeit von gesellschaftlicher Steuerung drastisch verbessern". Bei großen Menschenansammlungen **in China** solle „intelligentes Spüren" eingesetzt werden, um Gefahrenquellen zu identifizieren. Meng Jianzhu fordere auch, dass die einzelnen Behörden ihre Datenbanken abgleichen. Die Aufzeichnungen aller Überwachungskameras im ganzen Land sollten verbunden werden. Schon jetzt werde Gesichtserkennungssoftware in China eingesetzt, von der Verkehrspolizei, an Flughäfen, Bahnhöfen und U-Bahn-Stationen. Wie weit sie genau verbreitet ist, werde nicht veröffentlicht. Es gebe aber Berichte, nach denen die Polizei sie auch schon bei Großveranstaltungen einsetzt, etwa kürzlich bei einem Fest, bei dem 2,3 Mio. Besucher gescannt und dabei 15 polizeilich gesuchte Personen gefunden worden seien. Die Pekinger Zeitung „Global Times" berichte, dass bereits jetzt die Aufklärung von Verbrechen zu 50 Prozent mit Hilfe von Überwachungstechnologie gelinge. China sei eines der sichersten Länder der Welt. Die Rate schwerer Verbrechen sei von 2012 bis 2016 um 43 Prozent zurückgegangen.

Jan Engelschalt, Axis Communications, thematisiert in GIT 10-2017, S. 64/65, den Einsatz von **Videokameras mit Gesichtserkennung**. Die Funktion Wide Dynamic Range – Forensic Capture erlaube den Kameras, sich ändernden Lichtbedingungen sofort anzupassen und immer scharfe Bilder zu liefern. Das Ergebnis sei eine hohe Bildqualität, die es dem Gesichtserkennungssystem ermögliche, präzise zu arbeiten, selbst dann, wenn das Gesicht teilweise bedeckt ist, der Gesichtsausdruck sich ändert oder das Gesicht sich dreht. Der Genauigkeitsgrad liege bei über 99 Prozent.

PROTECTOR enthält in der Ausgabe 10-2017, S. 34/35 eine Marktübersicht über **111 Biometriesysteme** von 55 Anbietern. Die Tabelle bietet abgefragte Kriterien, unter anderem aus den Bereichen Verfahren, Einsatzbereich, Vertrieb, Installationen, Referenzen, Installationskosten & Betriebskosten, Fehlerraten, Identifikation, Verifikation, Erkennungsdauer und Schnittstellen.

Brandschutz

s+s report enthält in der Ausgabe 3-2017 mehrere Beiträge zur Brandschutz-Thematik: Dipl.-Ing. Rüdiger Kopp, FOGTEC Brandschutz GmbH & Co. KG, befasst sich mit der **Wassernebel-Technologie** (S. 14–18). Kabelkanäle stellten besondere Risiken mit hohem Schadenpotenzial dar. Kunststoffe, wie sie zur Isolierung von Kabeln verwendet werden, führten im Brandfall zu extremen Temperaturen und starker Entwicklung von Brandgasen. Aufgrund der extremen Kühlwirkung zusammen mit der eintretenden lokalen Inertisierung eigne sich Hochdruck-Wassernebel besonders gut zum Schutz solcher Anlagen. In zahlreichen Brandversuchen sei die Effektivität sogar in zwangsbelüfteten Kabeltunneln nachgewiesen. Der Einsatz von nur ca. zehn Prozent der Wassermenge eines konventionellen Sprühflutsystems garantiere einen minimalen Löschwasserschaden. In der Regel könnten Kabelanlagen, in denen ein Hochdruck-Nebelsystem ausgelöst wurde, bereits nach kurzer Zeit wieder genutzt werden.

Jens Stubenrauch, Dr. Richard Sthamer GmbH & Co. KG, erläutert in s+s report, Ausgabe 3-2017, S. 20–22, Möglichkeiten und Grenzen für den **Einsatz fluorfreier Schaumlöschmittel in Sprinkler- und Sprühflutanlagen**. Der Verordnung (EG) Nr. 1907/2006 zufolge dürften Schaumlöschmittelkonzentrate, die ab dem 4. Juli 2020 in Verkehr gebracht werden, eine maximale Konzentration von 25 ppb PFOA und deren Salzen oder 1.000 ppb für eine Kombination von PFOA-verwandten Substanzen aufweisen. In Zukunft benötigten Brandschützer umweltverträgliche Schaumlöschmittel. Es könne nicht länger toleriert werden, dass fluoridhaltige Schaumlöschmittel für Brandrisiken eingesetzt werden, die im Brandfall ähnlich gut mit fluorfreien Schaumlöschmitteln gelöscht werden können. Es sei eindeutig erwiesen, dass jedes Löschanlagenprojekt einer Einzelfallbetrachtung unterzogen werden muss, wenn die Wirksamkeit der Anlage unvermindert erhalten bleiben soll. Deshalb empfehle sich folgende Vorgehensweise: Zunächst sollte eine Bestandsaufnahme der aktuellen Löschanlage erfolgen. Dann müsse geprüft werden, ob der Schaummittel-Vorratstank und die Rohrleitungsisometrie vom Schaumtank zum Zumischer zu den chemisch-physikalischen Eigenschaften des gewünschten Schaumlöschmittels passen oder ob Umbauten erforderlich werden. 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 für eine erste Beratung und Bewertung einer Löschanlage bezüglich einer Umstellung auf fluorfreie Schaumlöschmittel benötigten Daten und Informationen werden vom Autor aufgelistet.

Dipl.-Ing. Heike Siefkes, VdS Schadenverhütung behandelt in s+s report, Ausgabe 3-2017, S. 24/25, den **Brandschutz in Lagerliften und Umlauflagersystemen**. In Lagerliftsystemen sei Brandschutz durch automatische Feuerlöschsysteme möglich. Die besonderen Gegebenheiten der Geometrie des Regals und der hohen Warendichte machten eine genaue Risikobetrachtung notwendig, um das jeweils geeignete Löschsystem zu finden. Die Autorin verweist auf das Merkblatt VdS 3430, Brandschutz für geschlossene dynamische Lagersysteme.

Brandschutzverglasungen sind das Thema für Helmut Kugelmann, SCHOTT Technical Glass Solutions GmbH, in s+s report, Ausgabe 3-2017, S. 26–28. Trotz der bereits eingeführten europäischen Regularien fänden gerade für feststehende Brandschutzverglasungen die deutschen Normen weiterhin Anwendung. Unterschieden würde zwischen Brandschutzverglasungen der Feuerwiderstandsklasse F und G. Während F-Verglasungen überwiegend in Fluchtwegsituationen eingesetzt würden, um diese vor Flammen und Hitzestrahlung zu schützen, könnten G-Verglasungen eingesetzt werden, um der Ausbreitung des Feuers entgegenzuwirken. Gerade bei Horizontal- und Schrägverglasungen müsse sichergestellt werden, dass die Verglasung über die geforderte Feuerwiderstandsdauer einen wirksamen Raumabschluss für die darüberliegenden Fenster bietet. Der Einbau von Türen in eine Brandschutzverglasung nach DIN 41002-13 sei mit allgemeiner bauaufsichtlicher Zulassung nur in der Kombination F30/T30 möglich. Da für die Funktionsweise das Zusammenwirken aller Komponenten entscheidend ist, müsse jede Brandschutzverglasung prüftechnisch nachgewiesen werden.

Eine neue GDV-Publikation zur **Vermeidung von Schäden durch Rauch und Brandfolgeprodukte** stellt Marco von Lier, GDV, in s+s report, Ausgabe 3-2017, S. 30/31, vor. Bereits kleine Brandereignisse könnten wegen der Einwirkung des Feuers auf Baustoffe und Bauteile, Einrichtungen und Vorräte und Brandfolgeschäden durch Rauch und Ruß zu empfindlichen Schäden führen. Nach der GDV-Statistik hätten sich in dem Jahrzehnt 2003–2012 5.876 Großschäden mit Schadenssummen über 500.000 Euro ereignet. Davon sei in 47,7 Prozent der Fälle (1.752) der Folgeschaden die Hauptursache für den Schadenumfang (3,8 Mrd. Euro) gewesen. Die neue GDV-Publikation beschreibe Maßnahmen, mit denen

angepasste Schutzkonzepte insbesondere für den Sachschutz geplant und umgesetzt werden können. Dies schließe auch die Reduzierung von Betriebsunterbrechungen ein.

Im Interview mit Security insight, Ausgabe 5-2017, S. 50/51, stellt Ulf Stremmel, SKUTA, das **neue Produkt SKUTA2** vor, das mehr könne als herkömmliche Löschmíttel. Es sei ein hochwirksames Feuerlöschmittel der Brandschutzklasse A43 und gleichzeitig ein Brandschutzprodukt, das zur Imprägnierung von Flächen eingesetzt werde, um deren Entflammbarkeit zu erschweren. Es gebe derzeit kein wasserbasierendes Löschmittel, das die hohe Klasse von SKUTA2 hat. Das Mittel sei weder für die agierenden Personen, noch für die Umwelt gefährlich.

Cloud Computing

Mit **Cloud-Durchsuchungsbefehlen des US-Justizministeriums** (DOJ) befasst sich Peter Marwan auf silicon.de am 24. Oktober. Das DOJ wolle die Anzahl der Anordnungen einschränken, mit denen Technologiefirmen zur verdeckten Herausgabe von Daten ihrer Kunden gezwungen werden. Insbesondere Microsoft habe sich vehement gegen diese Praxis gewehrt und sogar mehrfach dagegen geklagt. Das Unternehmen habe befürchtet, dass durch diese Anordnungen sein gesamtes Cloud-Geschäft gefährdet sei. In Deutschland habe es mit dem mit der Deutschen Telekom vereinbarten Datentreuhändermodell sogar schon einen Modus gefunden, die Anordnungen des DOJ nicht erfüllen zu müssen. Wie Bloomberg berichte, erhielt allein Microsoft in den 18 Monaten, bevor es im April 2016 gegen diese Praxis klagte, von US-Behörden 2756 Anfragen nach Daten seiner Kunden, bei denen es zum Stillschweigen verpflichtet worden sei. Deutsche Unternehmen stünden Cloud-Angeboten von Microsoft bisher skeptisch gegenüber. Nun solle ein komplexes Vertragswerk Bedenken ausräumen. Dabei übernehme T-Systems die Rolle als Datentreuhänder. Im September habe Microsoft mit Azure Confidential Computing eine zusammen mit Intel entwickelte **Verschlüsselungsmöglichkeit für Cloud-Daten** vorgestellt. Laut Microsoft ermögliche man mit dem Angebot, „dass Daten in der Cloud verarbeitet werden können mit der Gewissheit, dass sie immer unter der Kontrolle des Kunden sind". Die neuen Richtlinien des DOJ sähen vor, dass Staatsanwälte künftig in jedem Fall eine „individuelle und aussagekräftige Bewertung" vornehmen müssen, um zu ermitteln, ob die Geheimhaltung tatsächlich erforderlich ist.

Compliance

„Rechtsstaat kann nicht auf private Ermittler verzichten – **Unternehmen setzen bei Straftatverdacht auf die externe Hilfe"**, titelt die FAZ am 30. Oktober. Die Zeitung berichtet über eine Tagung des Richterbunds Hessen unter dem Titel „Kooperation oder Kapitulation?". Das personelle Ungleichgewicht von Staat und privaten Ermittlern solle nicht überdramatisiert werden. Rechtsanwalt Duve fordere für sein Team von Anwälten bei unternehmensinternen Untersuchungen „möglichst großen Freiraum". Die Befugnisse der staatsanwaltschaftlichen Ermittler würden deutlich weiter reichen. Es bestehe „keine begründete Sorge für ein Erodieren des Rechtsstaates".

Datenschutz

Das Fachmagazin InfoSicherheit weist in der Ausgabe 3-2017, S. 48, darauf hin, dass das BMI Leitlinien für die **rechtssichere Nutzung von Pseudonymisierungslösungen** veröffentlicht. Die DS-GVO verlange unter anderem Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen. Die Pseudonymisierung sei eine mögliche Methode. Es bedeute, dass Daten durch entsprechende Verfahren von ihrem Personenbezug befreit werden. Die Pseudonymisierung führe zu einer „Win-win-Situation". Das nun veröffentlichte Whitepaper möchte in Form von Leitlinien praktische Impulse geben, wie eine Pseudonymisierung datenschutzkonform realisiert werden kann.

Datensicherheit

Den Schutz Kritischer Infrastrukturen im Zeitalter von Cyberangriffen thematisiert die Zeitschrift Security insight in der Ausgabe 5-2017, S. 20–22. Erforderlich sei ein **Paradig-**

menwechsel für Kontrollräume und Leitstellen. Es müsse in sogenannte Backup-Kontrollzentren an Zweit- oder Mehrstandorten investiert werden. Eine georedundante Backup-Leitstelle stelle die derzeit höchste Form eines Backups dar und könne aus technischer Sicht über Ländergrenzen oder Kontinente hinweg durchgeführt werden. Die Entfernung spiele keine Rolle. Sowohl der Hauptstandort als auch der Notfall-Backup-Standort seien in die normalen Betriebsabläufe integriert. Die KVM (Keyboard, Video and Mouse)-Switch-Technologie des Kontrollraum-Anbieters WEY Technology eröffne der Teamarbeit in Leitstellen neue Dimensionen. KVM-Switches und -Extender integrierten alle Betriebssysteme, Schnittstellen und Übertragungskanäle.

Diebstahl

Der **„Diebstahl fest eingebauter Navigationsgeräte"** richte in Deutschland jährlich einen Schaden von ca. 200 Mio. Euro an, berichtet die FAZ am 6. Oktober. Die Täter seien überwiegend Litauer. Konkurrenz bekämen sie in letzter Zeit durch Niederländer nordafrikanischer Herkunft oder auch Serben. Die Banden mieteten sich in günstigen Hotels ein, spionierten Tatorte aus und fahren nachts mit dem Fahrrad oder Bus und Bahn zu den hübschen Häusern, vor denen die Autos der Marken parken, auf die es ihnen ankomme: BMW, Mercedes und Audi. Die Täter würden arbeitsteilig vorgehen. Jeder Schritt von der Beschaffung bis zum Absatz der Beute, etwa in Asien, sei bestens organisiert. Eine wirksame Bekämpfung sei nur durch enge Zusammenarbeit der Polizeien über Landesgrenzen hinweg möglich. Hersteller arbeiteten seit langem intensiv daran, die Sicherheit der Geräte zu verbessern. Es sei sehr schwierig, zeitnah auf jede technische Versiertheit der Täter reagieren zu können.

Einbruchmeldeanlage

Dipl.-Wirtschaftsjurist Sebastian Brose, VdS Schadenverhütung, erläutert in s+s report, Ausgabe 3-2017, S. 36–38, die grundlegende Überarbeitung der Richtlinien für Einbruchmeldeanlagen (EMA) **VdS 2311**. In Bezug auf die Alarmierung hätten sich mit Anpassung an die DIN EN 50136 die gravierendsten Änderungen ergeben. Die aus der vorherigen VdS 2311 bekannte bunte Übertragungsmatrix sei ebenso entfallen wie die über Jahrzehnte geprägten Begriffe „bedarfsgesteuerte" und „stehende Verbindung". Eine weitere wesentliche Änderung sei die Einführung eines Sicherungskonzepts. Das bedeute, die EMA in die dreigliedrige Sicherheitsstrategie, bestehend aus baulich-mechanischen Maßnahmen zum Erreichen eines hinreichenden Widerstandszeitwerts, elektronische Maßnahmen zur frühzeitigen Erkennung von Einbruchversuchen und organisatorische Maßnahmen zur Unterstützung des sicheren Betriebs und zur situationsgerechten Reaktion im Alarm- oder Störungsfall so einzubetten, dass ein bestmögliches Zusammenwirken erwartet werden könne. Für die Praxis würden die Technischen Kommentare, VdS 3134, zunehmend an Bedeutung gewinnen.

Einbruchschutz

Die **Aktualisierung der Technischen Kommentare** (VdS 3134) im Zusammenhang mit der Überarbeitung von VdS 2311 erläutert in s+s report, Ausgabe 3-2017, S. 39–41, Paulus Vorderwülbecke, VdS Schadenverhütung. Mit den TK würden Hintergrundinformationen angeboten, die trotz ihrer technischen Ausrichtung lesbar geblieben seien. Sie umfassten vier Themenkomplexe: Wertbehältnisse, Einbruchmeldetechnik, Verglasung sowie Fenster, Türen und Tore. Die Planungsrichtlinien wiederum würden beschreiben, wie die technisch hochwertigen Produkte in der Praxis eingesetzt werden müssen, um eine VdS-gerechte Anlage zu erhalten.

Endgerätesicherheit

PROTECTOR gibt in der Ausgabe 10-2017, S. 31, Sicherheitsempfehlungen für Endanwender von Smartphones: nutzen Sie starke Kennwörter und halten Sie diese geheim; aktivieren Sie die Mehrfaktor-Authentifizierung; Updates aktivieren; nutzen Sie Smartphones in der vom Anbieter voreingestellten Konfiguration; installieren Sie keine Apps aus fremden Quellen!

Evakuierung

Dipl.-Ing. Rolf Maniago, Maniago & Henss GmbH, behandelt in PROTECTOR, Ausgabe 10-2017, S. 32, die **Steuerung von Fluchttüren**. Mit dem Terminal FT-16 uP/aP komme 2017 ein Fluchttür-Steuerungskonzept auf den Markt, das mit neuer Technik, innovativen Funktionalitäten und Designvielfalt herkömmliche Einschränkungen beseitige. Der Hersteller Maniago & Henss setze dabei erstmals auf die Integration eines Farbdisplays und löse somit die interpretierungsbedürftige Symbolik durch Klartext ab. Dies ermögliche zum einen die verständliche Anzeige für Betriebszustände und zum anderen eine einfache Einstellung der Parameter mittels Servicemenü.

Flughafensicherheit

Die **Komplexität des Flughafen-Sicherheitssystems** wird in der Zeitschrift PROTECTOR, Ausgabe 10-2017, S. 36/37, behandelt. Es bedürfe eines komplizierten Zusammenspiels der verschiedenen Subsysteme wie Überwachungssysteme, Alarmanlagen, Zutrittskontrolle, Netzwerkverwaltung und Management-Plattform. Jeder Flughafenbereich besitze sein eigenes vertikales Management. Wegen der Unterschiede in den einzelnen Bereichen ergäben sich sehr viele Risiken. Um mit den genannten Schwierigkeiten umzugehen, habe Dahua eine spezielle Flughafenlösung entwickelt, die unter einer einheitlichen Plattform die multifunktionale HD-Überwachung mit einer Deep-Learning-Architektur verbinde, die eine höchste präzise Gesichtserkennung und E-Pass-Verifikation ermögliche. Falls ein Verdächtiger auftaucht, werde Alarm gegeben. Beim Schutz am viele Kilometer langen Perimeter komme die Wärmebildkamera mit 100-Millimeter-Objektiv zum Einsatz, die bei einer Auflösung von 640 mal 512 Pixeln und einer Installationshöhe von fünf Metern Personen auf eine Distanz von etwa drei Kilometern erfassen könne.

Sicherheit am Flughafen Frankfurt a. M. thematisiert Security insight in der Ausgabe 5-2017, S. 22–24. Die Investitionen für die Sicherheit lägen im zweistelligen Millionenbereich. Als ein Bestandteil des umfassenden Sicherheitskonzeptes installiere primion seit 2008 ein eigens für Ausweisprozesse eines europäischen Flughafens entwickeltes Ausweisverwaltungs-System (AVS). Rund 1.500 Zutrittskontroll-Leser habe primion installiert. Am Frankfurter Flughafen arbeiteten über 81.000 Personen aus 70 Nationen in 450 verschiedenen Arbeitsstätten. Im „Servicecenter Flughafenausweise" würden Anträge im AVS erfasst, Sicherheitsüberprüfungen und Schulungen eingeleitet, Zutrittsrechte erteilt und die Ausweise nach Bewilligung produziert und über das flugplangesteuerte Gate-Managementterminal (GMT) würden alle Abläufe am Gate gesteuert und dabei rechtliche Vorgaben berücksichtigt. Alle Vorgänge würden im primion Gefahrenmanagement-System psm2200 dargestellt und seien jederzeit abrufbar. Zudem würden alle Komponenten wie Leser, GMT und Server-Dienste sowie Schnittstellen zu Fremdsystemen in Echtzeit überwacht, um Ausfälle frühzeitig zu erkennen.

Pinkerton Managing Director Weynand Haitjema zeigt in der Fachzeitschrift Security insight, Ausgabe 5-2017, S. 30/31, wie **Personenkontrollen** die Sicherheit an Flughäfen steigern könnten. Mit Kontrollen von Fahrzeugen und Personen, bevor sie das Flughafengebäude erreichen, werde eine wichtige erste Verteidigungslinie erreichtet. Terroristen nutzten im Vorfeld eines Anschlags in der Regel Taxis oder Lieferwagen und trügen wahrscheinlich gefälschte oder gar keine Ausweise bei sich. Ergänzt werden müssten die externen Kontrollen durch den Einsatz verdeckter Ermittler im Flughafengebäude. Von entscheidender Bedeutung sei die umfassende Kontrolle aller Mitarbeiter, vom Verkaufspersonal in Ladengeschäften bis zu Mitarbeitern der Gepäckabfertigung.

Gebäudesicherheit

GIT weist in der 10-2017, S. 30, darauf hin, dass VdS mit der neuen Richtlinie VdS 3406, **„Sicherheitsmanagement für bauliche Objekte"** erstmals alle Anforderungen und Sicherungsmaßnahmen in einen sämtliche relevanten unternehmerischen Aspekte abdeckenden Kontext integriert habe. Das erste VdS-Zertifikat für dieses so umfassende wie besonders effiziente und zuverlässige Sicherheitsmanagement habe die Nürnberger Versicherung überreicht bekommen.

Gefahrstofflagerung

Durch die im November 2016 veröffentlichte Gefahrstoffverordnung sei die **Einstufung und Kennzeichnung chemischer Stoffe** aus der CLP-Verordnung in deutsches Recht überführt worden, heißt es in der Ausgabe 10-2017 der Zeitschrift GIT, S. 104/105. Dies habe unmittelbare Auswirkungen auf die Lageranforderungen, z. B. für giftige, entzündbare sowie krebserzeugende und keimzellenmutagene Stoffe. Die komplexe Gefahrstoff-Thematik sei in der aktuellen Gefahrstoffbroschüre von Asecos detailliert dargestellt mit Begriffserklärungen, Definitionen und Kennzeichnungen. Der Fokus der Broschüre liege auf der Gefahrstofflagerung in Sicherheitsschränken nach DIN EN 14470-1 und auf der Lagerung und Bereitstellung von Druckgasbehältern nach DIN EN 14470-2. Zusätzlich fänden Nutzer Tipps für den richtigen Umgang mit den einzelnen Stoffklassen sowie zur Entsorgung von Chemikalienabfällen.

Geldautomatensicherheit

Marwan beschreibt die **Gefahr für Geldautomaten durch veraltete Software** (silicon.de am 27. September). In einer gemeinsam erstellten Studie hätten Europol und Trend Micro die möglichen Gefahren für Geldautomaten durch Angriffe auf Netzwerke von Banken untersucht. Hacker erhielten beispielsweise über zielgerichtete Phishing-E-Mails Zugang zu einem Netzwerk. Nachdem sie da einmal eingedrungen sind, sei es ihnen möglich, sich bis zu den Geldautomaten vorzuarbeiten. Die allermeisten Geldautomaten seien technisch gesehen nichts anderes als von einem Windows-PC gesteuerte Geräte zur Geldausgabe. Damit seien sie auch ein mögliches Ziel für Hacker. Eine Schadsoftware mit Wurmfunktion, die lediglich ungepatchte und nicht einmal veraltete Betriebssysteme ins Visier nehme, könnte es Kriminellen erlauben, Geldautomaten über das Netzwerk anzugreifen. Versuche habe es schon früher gegeben.

Geldtransportüberfall

Wie die FAZ am 9. Oktober berichtet, ist es OK-Fachleuten der Polizei Hagen gelungen, mehrere brutale Überfälle auf Geldtransporter seit 20 Jahren im Ruhrgebiet aufzuklären und anhand von DNA-Analysen fünf Männern Überfälle in Hagen (1998), Neuss (2000), Werl (2001 und 2002), Volmarstein (2014) und Dortmund (2015) zuzuordnen. Die Überfälle seien jeweils nach einem ähnlichen Schema abgelaufen. Mit gestohlenen Autos hätten die Täter die Geldtransporter eingekeilt und die Wachleute zum Anhalten gezwungen. Ohne Vorwarnung hätten sie dann die gepanzerten Transporter aus Schnellfeuerwaffen beschossen. In zwei Fällen seien die Wachleute auch mit Panzerfaust-Attrappen bedroht worden.

Incident Management

Alexander Berger, Smart Data Deutschland UG, befasst sich in der 10-2017 der Zeitschrift PROTECTOR, S. 70/71, mit Incident Management. Es beginne mit einem grundsätzlichen Verständnis der Unternehmensumwelt und umfassenden organisatorischen und operativen Vorbereitungen, basierend auf der Analyse des individuellen Incident-Potenzials der Unternehmung. Die unternehmensglobale Plattform für die zentrale Aggregierung aller Incidents erfülle die umfassenden Anforderungen des Sourcings der Informationen über Incidents aus verschiedenen Quellen, einer redundanten Dokumentation und Bereitstellung der Informationen, des Informationsmanagements im Anschluss an das Sourcing, der Bearbeitung und Resolution des Incidents und integrierter Eskalationsstufen bis hin zum Krisenmanagement. Aus der Bearbeitungsansicht des Incidents in Form eines Reports auf der Plattform könne jeder Incident von Berechtigten zum Krisenmanagement eskaliert werden.

IT-Sicherheit

Der 1994 eingeführte **IT-Grundschutz des BSI** sei der wohl meistgenutzte Standard für Informationssicherheit in Deutschland, betont heise.de am 12. Oktober. Er solle Einsteigern und Fortgeschrittenen eine modulare und flexible Methode zur

Erhöhung der IT-Sicherheit in Behörden und Unternehmen ermöglichen. Nun sei er vom BSI grundlegend überarbeitet worden. Die modernisierte Fassung solle vor allem die spezifischen Bedürfnisse und Anforderungen kleiner und mittlerer Unternehmen stärker berücksichtigen als zuvor. Der überarbeitete Grundschutz gliedere sich in ein IT-Grundschutz-Kompendium, das die früheren Grundschutzkataloge ersetze, die neuen BSI-Standards 200-1, 200-2 und 200-3 als Ersatz für die bisherige 100 x-Reihe sowie einen „Leitfaden zur Basisabsicherung", der auf 44 Seiten drei grundlegende Schritte zur Umsetzung erster Sicherheitsmaßnahmen beschreibe.

Der App-Entwickler Felix Krause habe mit einem Proof of Concept belegt, dass App-Entwickler mit geringem Aufwand das Passwort für die Apple ID-Konten abgreifen können, berichtet Peter Marwan auf silicon.de am 12. Oktober. Als Manko von **Apples Mobilbetriebssystem** sehe Krause, dass sich Apples eigene Aufforderungen zur Passworteingabe nahezu nicht von Aufforderungen unterscheiden lassen, die von einzelnen Apps stammen. So ließen sich mit 30 Programmzeilen Pop-ups erzeugen, die denen von iOS aufs Haar gleichen. Krause rate Nutzern bei der Einblendung eines solchen Pop-ups den Home Button zu betätigen. Bleibe die Passwort-Abfrage sichtbar, handele es sich tatsächlich um einen echten Systemdialog. Weiter empfehle er, Anmeldedaten grundsätzlich nicht in einem Pop-up einzugeben, sondern dieses zu schließen und die Anmeldung in den System-Einstellungen selbst vorzunehmen.

61 Prozent der deutschen Unternehmen fürchten Angriffe auf ihre IT, titelt Anja Schmoll-Trautmann auf silicon.de am 12. Oktober. 67 Prozent der Unternehmen seien in den vergangenen zwölf Monaten Opfer von mindestens einem IT-Angriff gewesen, 14 Prozent vermuteten einen Angriff. Das seien **Ergebnisse einer repräsentativen Umfrage von Bitkom Research**. Dabei seien 750 für IT-Sicherheit verantwortliche Personen aller Branchen ab 50 Mitarbeitern in Deutschland befragt worden. Vor allem Phishing-Angriffe und Angriffe mit Malware seien weit verbreitet. 41 bzw. 36 Prozent der Unternehmen hätten solche Attacken festgestellt. Elf Prozent der Unternehmen seien mit Ransomware infiziert worden. Aktuell nutzten neun von zehn Unternehmen Virenscanner und Firewalls und erstellten regelmäßig Backups (88 Prozent). Jeweils gut drei Viertel setzten einen Passwortschutz auf allen ein. 73 Prozent hätten die Möglichkeit, den E-Mail-Verkehr zu verschlüsseln. Rund jedes zweite Unternehmen verschlüssele Daten auf Datenträgern, betreibe ein Patchmanagement und habe sein internes Firmennetzwerk gegen Datenabfluss von innen abgesichert. Vier von zehn Unternehmen führten Penetrationstests durch. Jeweils ein Drittel nutze ein Intrusion Detection System oder ein Security Information and Event Management System oder setze ein erweitertes Verfahren zur Benutzeridentifikation auf Endgeräten ein.

Dipl.-Phys. Bernd Schöne, freier Autor, befasst sich in der Ausgabe 10-2017 von PROTECTOR, S. 42-44, mit dem Quantencomputer, der in kurzer Zeit Aufgaben lösen könne, für die herkömmliche Rechner Jahrtausende benötigen würden. Mit Quantencomputern seien asymmetrische Verschlüsselungsverfahren so gut wie gebrochen. Damit böten sie keinen Schutz mehr vor Manipulation oder Missbrauch. Alle Public-Key-Algorithmen wie RSA, Diffie Hellman, elliptische Kurven wären wertlos. Auch symmetrische Verschlüsselungsverfahren wie AES würden durch Quantenrechner an Sicherheit einbüßen. Daher werde nach neuen Verschlüsselungsverfahren gesucht. Sie hießen PQK (**Post-Quantum-Kryptografie**)-**Verfahren** und sollen gegen die Entschlüsselungsversuche von Quantenrechnern ebenso gefeit sein wie gegen Attacken von klassischen Rechnern. Welches PQK-Verfahren sich durchsetzen wird, sei derzeit vollkommen offen.

Ammar Alkassar, Rohde & Schwarz Cybersecurity GmbH, behandelt in der Ausgabe 10-2017 der Zeitschrift PROTECTOR, S. 45, den **IT-Schutz für Kritische Infrastrukturen**. Moderne Cyberattacken ließen sich mit Sicherheitsupdates und herkömmlicher Virenschutzsoftware nicht mehr abwehren. Benötigt würden Sicherheitslösungen, die Angreifer „proaktiv" aus dem IT-System fernhalten. Vor allem Industrieunternehmen und Kritische Infrastrukturen benötigten neue „proaktive" Firewall-Technologien. „Next Generation-Firewalls" ließen nur die Datenpakete passieren, die sich als gutwillig identifizieren können. Zudem würden Firewalls benötigt, die im Inneren des Netzes arbeiten und dieses in mehrere Zonen („Brandabschnitte") segmentieren.

Dr. Erlijn van Genuchten, SySS GmbH, zeigt in PROTECTOR (Ausgabe 10-2017, S. 46/47), dass **IoT-Geräte von digitalen Angreifern missbraucht** werden könnten. Mögliche Gefahren entstünden auf mehreren Ebenen: der Wahrnehmungs- oder Hardwareebene, der Netzwerkebene, der Backend-Ebene und der Applikationsebene. IT-Sicherheit sollte schon bei der Planung und Entwicklung von IoT-Geräten berücksichtigt werden. Auch die Sicherheit der Sensoren sollte beachtet werden. Von zentraler Bedeutung sei ein Sicherheitstest vor der Markteinführung durch einen unabhängigen Dienstleister.

Eine **Abwägung zwischen Zweifaktor- oder Multifaktor-Authentifizierung** nimmt Marc T. Hanne, HID Global, in der Zeitschrift PROTECTOR, Ausgabe 10-2017, S. 48/49, vor. Das Unternehmen sollte die Alternative wählen, die eine optimale Balance zwischen Sicherheit und Benutzerkomfort gewährleistet. Zu kurz greife die Zweifaktor-Authentifizierung zum Beispiel im Bankenbereich. Bei der Multifaktor-Authentifizierung würden üblicherweise traditionelle besitz- und wissensbasierte Faktoren um eine weitere Komponente aus den Bereichen Eigenschaft oder Verhalten ergänzt, etwa durch biometrische Merkmale.

Die **Relevanz und Nützlichkeit von Antimalware-Lösungen** wird in Ausgabe 10-2017 von PROTECTOR, S. 50/51, in Frage gestellt. Die am weitesten verbreitete Methode zur Erkennung unbekannter Malware sei die „Heuristik". Nahezu jeder Hersteller von Antimalware-Lösungen benenne heuristische Verfahren als wirksamen Schutz gegen die sogenannte Zero-Day-Malware. Noch vor wenigen Jahren habe man mit Antimalware-Lösungen noch 70 bis 80 Prozent der Cybersicherheitsvorfälle aufdecken oder verhindern können. Seither hätten sich Methoden und Techniken von Angreifern massiv verändert, die Funktionsweise von Antimalware-Lösungen jedoch kaum. Nicht mehr Computersysteme seien das erste Angriffsziel, sondern der Faktor Mensch, der mit weniger Aufwand zu „hacken" sei. Dagegen helfe aber keine Sicherheitssoftware der Welt.

Golem.de meldet am 18. Oktober, ein Team von tschechischen und slowakischen Forschern habe eine schwere Sicherheitslücke in einer von Infineon entwickelten Verschlüsselungsbibliothek entdeckt. Die damit erzeugten **Schlüssel mit dem RSA-Verfahren** seien unsicher und ließen sich mit größerem Aufwand knacken. Es handele sich nicht um eine Schwäche im RSA-Algorithmus selbst, sondern um gravierende Fehler bei der Implementierung der Schlüsselerzeugung in Infineon-Produkten. Die betroffenen Geräte seien alle Hardware-Kryptomodule. Allerdings seien die Fehler nicht in der Hardware direkt implementiert, sondern in der darin vorhandenen Embedded-Software.

Netzwerk-Monitoring reduziere Zeit und Kosten bei Cyberattacken, heißt es in der Zeitschrift Security insight, Ausgabe 5-2017, S. 8. Nur so würden eindeutige Beweise geliefert, wann, wo und wie genau eine Attacke aufgetreten ist und welche Kundendaten möglicherweise gestohlen worden sind. Das Unternehmen Endace habe den Netzwerkrekorder EndaceProbe vorgestellt. Er sei skalierfähig und lasse sich in andere Open-Source- und kommerzielle Lösungen integrieren, um die Problemuntersuchung sowie forensische Datenanalysen zu optimieren und zu automatisieren. Damit lasse sich die Zeit für Sicherheitsanalysen im Vergleich zu anderen Netzwerkrekordern um die Hälfte reduzieren.

Die Bundesregierung setzt ihren Plan zur **Einführung eines IT-Sicherheitsgütesiegels** um, berichtet der Behörden Spiegel in der Oktober-Ausgabe. Während einige Anbieter von IT-Sicherheitslösungen für klare Herstellerverpflichtungen zur IT-Sicherheit plädierten, forderten einige mittelständische IT-Unternehmen konkrete und transparente Standards ohne ein Sanktionsregime. Unter Federführung des BSI und in enger Zusammenarbeit mit Wirtschaft und Verbrauchervertretern sollten nun transparente, produktgruppenspezifische IT-Sicherheitsstandards als Basis für ein Gütesiegel entwickelt werden. Rein rechtlich wäre die Einführung eines Pflichtgütesiegels nur in Deutschland nicht möglich. Ein verpflichtendes IT-Gütesiegel könne nur auf EU-Ebene eingeführt werden.

Jan Lindner, Panda Security, stellt in der Oktober-Ausgabe des Behörden Spiegel **Panda Adaptive Defense 360** vor. Angreifer hätten es vermehrt auf Endpoints abgesehen, weil sie von dort aus leicht Informationen herausfiltern, Daten stehlen oder andere Angriffe starten könnten. Intelligente Systeme, die mithilfe cloudbasierter Scan-Technologien alle laufenden IT-Prozesse kontinuierlich überwachen, analysieren und klassifizieren, seien heute und in Zukunft alternativlos. Eine gute Endpoint-Protection-Plattform müsse in der Lage sein, jederzeit Veränderungen in den Datenmustern zu erkennen. Nur durch kontinuierliches Monitoring sei es möglich, auf neue Bedrohungen unmittelbar zu reagieren. Panda Adaptive Defense 360 sei der erste und bisher einzige gemangte Cyber-Security-Service, der Prävention, Erkennung und Reaktion kombiniert.

Deutsche Unternehmen haben Nachholbedarf bei der IT-Sicherheit, berichtet Leila Haidar in der FAZ vom 19. Oktober (Verlagsspezial Zukunft Mittelstand). Mit 62 Prozent weise Deutschland im Ländervergleich (USA: 40 Prozent) den höchsten Anteil an Firmen auf, die unzureichend auf Cyberattacken vorbereitet sind. Von Cyberangriffen seien in der Branche Fertigungsindustrie 65 Prozent, bei den Medien und dem Kommunikationsbereich ebenfalls 65 Prozent, in der Sparte Finanzdienstleistungen 64 Prozent betroffen gewesen. Deutsche Unternehmen planten, in den kommenden 12 Monaten die Investitionen allgemein für Cybersicherheit um 55 Prozent zu steigern, und zwar 68 Prozent für neue

Sicherheitstechnologien und 57 Prozent in das Cybertraining für Mitarbeiter. Aber nur jedes vierte Unternehmen verpflichte seine Mitarbeiter zum Cybertraining. Cyberversicherungen würden boomen. Viele Versicherer wie HDI oder Hiscox hätten sehr individuelle Angebote. Bei AXA hätten Unternehmen die Wahl zwischen verschiedenen Policen. Neben Versicherungen für Vermögensschäden gebe es Zusatzversicherungen, die Entschädigungsansprüche Dritter abdeckten.

Olivia von Westernhagen geht am 24. Oktober auf heise.de auf den **Google Transparenzbericht** ein. Danach habe der Anteil an HTTPS-verschlüsseltem Traffic 2017 gegenüber dem Vorjahr weltweit stark zugenommen. Dem Report sei unter anderem zu entnehmen, dass aktuell 71 der 100 meistbesuchten Webseiten weltweit standardmäßig HTTPS nutzen. Vor einem Jahr seien es erst 37 gewesen. Als einen der möglichen Gründe für die aktuelle Entwicklung nenne Google den Hinweis auf „nicht sichere" Verbindungen in der Chrome-Adressleiste, der Anfang des Jahres mit der Chrome-Version 56 eingeführt worden sei.

Mögliche Abhörattacken infolge fehlerhafter Verwendung eines Zufallsgenerators thematisiert Olivia von Westernhagen am 25. Oktober auf heise.de. Die **fehlerhafte Verwendung eines Zufallsgenerators** in der Firmware von Internet-Geräten von Fortinet ermögliche das Knacken von Krypto-Keys und in der Folge das Mitlesen von VPN und SSL/TLS-verschlüsseltem Internet-Traffic. Den auf den Namen **DUHK** (Don't Use Hardcoded Keys) getauften Angriff habe ein Team bekannter Kryptoforscher entdeckt und in einem Whitepaper beschrieben. Den Ausgangspunkt für den DUHK-Angriff bilde laut Forscherteam der mittlerweile überholte ANSI-Standard X9.31 Random Number Generator (RNG) zum Generieren von Zufallszahlen. Obgleich aktuelle FortiOS-Versionen die mit der Kennung CVE-2016-8492 bezeichnete Schwachstelle nicht mehr aufweisen würden, hätten die Forscher im Internet mehr als 25.000 theoretisch mit DUHK angreifbare Fortinet-Geräte identifiziert. Wie auch die Hersteller selbst rieten sie deshalb dringend zu einem Update auf FortiOS ab Version 4.3.18.

IuK-Kriminalität

Wie heise.de am 27. September berichtet, hat Europol den **Bericht zum Internet Organised Crime Threat Assessment für das Jahr 2017** veröffentlicht. Die organisierte Internet-Kriminalität beschäftige sich vor allem mit der Erpressung durch Ransomware. Insgesamt verzeichne der Bericht, dass Cyberkriminelle E2E-Verschlüsselungsverfahren zunehmend nutzten, sich dabei jedoch gängiger Software bedienten und keine eigenen Systeme entwickelten. Cyberkriminelle akzeptierten über Bitcoins auch Währungen wie Monero, Ethereum und Zcash. Wissenschaftler und Entwickler müssten besser mit den Behörden bei der Frage zusammenarbeiten, wie neu entstehende Kryptowährungen entdeckt werden können. Für die Zukunft sähen die Autoren der Studie nach dem Großschadensereignis WannaCry die Möglichkeit, dass Firmen verstärkt Versicherungen gegen Cybercrime-Attacken eingehen.

Zeit.de weist am 2. Oktober auf das sogenannte **Netzwerkdurchsetzungsgesetz (NetzDG)** hin, das am 1. Oktober in Kraft getreten ist. Es sei eine Maßnahme gegen Hass, Hetze und gezielte Falschdarstellungen im Internet. Es verpflichtet die Betreiber sozialer Netzwerke wie Facebook, Twitter und YouTube, „offensichtlich rechtswidrige Inhalte innerhalb von 24 Stunden" nach Eingang einer Beschwerde zu löschen oder zu sperren. Für nicht offensichtlich rechtswidrige Inhalte haben die Betreiber sieben Tage Zeit. Wenn die Entscheidung von einer unwahren Tatsachenbehauptung abhängt, kann dem betroffenen Nutzer zunächst Gelegenheit zur Stellungnahme gegeben werden. Bei wiederholten Verstößen droht ein Bußgeld von bis zu 50 Mio. Euro. Die Unternehmen müssten außerdem einen Ansprechpartner in Deutschland benennen. Betroffene bekommen im Einzelfall einen zivilrechtlichen Auskunftsanspruch nach Bestandsdaten des Täters, wenn das zuständige Landgericht es anordnet. Registrieren die großen Netzwerke mehr als 100 Beschwerden über illegale Inhalte pro Jahr, sind sie verpflichtet, halbjährlich Berichte über den Umgang mit den Beschwerden zu erstellen.

Dem Bericht „Cybercrime tactics and techniques" zufolge hatten bekannte Malware-Familien im dritten Quartal 2017 ein Comeback und sorgten für **mehr Infektionen auf Mac-Rechnern**. Spam-Kampagnen hätten für eine Verbreitung des Banking-Trojaners Emotel auf Windows-Systemen gesorgt. Eine wachsende Zahl von Android-Trojanern ermögliche den Hintermännern Klickbetrug.

„Zeitbombe Produktionsrechner" titelt InfoSicherheit in der Ausgabe 3-2017, S. 47. Nicht nur Konzerne wie Mondelez, Beiersdorf oder der russische Ölkonzern Rosneft seien in Mitleidenschaft durch digitale Erpressungen gezogen worden, auch zahlreiche kleinere Firmen in Deutschland. Eine immense Sicherheitslücke liege immer noch im Verborgenen: Die Rechner, mit denen Produktionsanlagen betrieben werden – und die häufig noch Altsysteme wie Microsoft Windows 2000 oder XP nutzten. Zu den Risiken der Digitalisierung gehörten auch aktuelle Windows-Rechner mit einer bekannten Schwachstelle, die vor allem in internen Netzwerken genutzt werden könne. Eine intensive und lückenlose Überwachung von Firmennetzwerken sei daher umso wichtiger.

Experten warnen nach einem Bericht in golem.de vor einem **„Cyber-Hurrican" durch ein neues Botnetz**. Kriminelle nutzten Sicherheitslücken in IoT-Geräten zum Aufbau eines großen Botnetzes aus. Dabei verwende der Bot Code von Mirai, unterscheide sich jedoch von seinem prominenten Vorgänger. Mehrere IT-Sicherheitsunternehmen warnten vor einer Bedrohung durch ein neu aufgebautes Botnetz mit weltweit Hunderttausenden angeschlossener Geräte. Dabei sollen die unbekannten Hacker Sicherheitslücken zahlreicher IoT-Geräte ausnutzen, darunter der Hersteller Goahead, D-Link, TP-Link, Avtech, Netgear, Mikrotik, Linksys und Synology. Nach Angaben des israelischen Sicherheitsunternehmens Checkpoint seien weltweit bereits eine Million Organisationen von dem Botnetz betroffen. Anfällig seien demnach unter anderem IP-Kameras, Router und NAS-Systeme. Die chinesische Sicherheitsfirma Qihoo 360 Netlab registriere ebenfalls den Aufbau eines umfangreichen neuen Botnetzes. Der Analyse zufolge borge sich der Bot einigen Code von dem im vergangenen Jahr aufgetretenen Mirai-Botnetz. Während Mirai jedoch das Netz nach Geräten abscanne, die mit Standardeinstellungen der Passwörter und ohne Firewall betrieben wurden, nutze das neue Botnetz gezielte Sicherheitslücken.

Kommunale Sicherheit

Ohne effektive Kräfte auf lokaler Ebene könne es keine neue Sicherheitsarchitektur in der Bundesrepublik geben, meint der Terrorismusexperte Jörg H. Trauboth nach einem Bericht des Behörden Spiegel über den diesjährigen „Bundeskongress kommunale Ordnung" in der Oktober-Ausgabe. Entscheidend für die Gewährleistung von Sicherheit sei das Bilden von Netzwerken, wie dies mit der Bildung der „Ordnungspartnerschaft Nordkopf" in Wolfsburg im Jahr 2000 geschehen sei.

Krankenhaussicherheit

Peter Niggl, Chefredakteur der Zeitschrift Security insight, befasst sich in der Ausgabe 5-2017, S. 18/19, mit der **Sicherheit von Patienten** im Krankenhaus. Wissenschaftler der Universität Herdecke hätten hochgerechnet, dass möglicherweise bis zu 21.000 Patienten pro Jahr durch die Hände von Klinikpersonal ums Leben kommen. Allein zwischen den Jahren 1975 bis 2008 sei es weltweit zu 35 Tötungsserien in Kliniken und Heimen gekommen. Der Krankenpfleger Niels H., 2015 vom LG Oldenburg wegen zweifachen Mordes, zweifachen Mordversuchs sowie gefährlicher Körperverletzung zu lebenslanger Haft verurteilt, könnte in Kliniken in Oldenburg und Delmenhorst zwischen 1999 und 2005 mehr als 90 Patienten, möglicherweise sogar mehr als 200, getötet haben. Eines der Mittel, um schneller auf verdächtige Vorgänge in einem Krankenhaus oder Pflegeheim reagieren zu können, sei die Einrichtung einer anonymen Meldeplattform.

Logistiksicherheit

PROTECTOR weist in der Ausgabe 10-2017, S. 72, darauf hin, dass das BMBF am 15. September 2017 die Förderrichtlinie „Zivile Sicherheit – Kritische Strukturen und Prozesse in Produktion und Logistik" veröffentlicht hat. Seit Beginn des Programms 2007 habe das BMBF für **das nationale Sicherheitsforschungsprogramm** für mehr als 300 Verbundprojekte über 540 Mio. Euro Fördermittel zur Verfügung gestellt. Ein Fokus liege auf innovativen Ansätzen für die Modellierung und Analyse von komplexen Prozessen in Produktion und Logistik.

Maschinensicherheit

Bislang waren für die temporäre Überbrückung von Schutzfeldern Muting-Sensoren erforderlich, heißt es in der Ausgabe 10-2017 der Zeitschrift GIT, S. 110–112. Mit dem von Leuze electronic entwickelten **„Smart Process Gating-Verfahren"** (SPG) könne auf die Muting-Sensoren ganz verzichtet werden. Beim SPG komme das erste Gating-Signal von der Anlagensteuerung, während das zweite bei der Unterbrechung des Schutzgeldes vom Sicherheits-Lichtvorhang selbst erzeugt werde. Der Autor behandelt Anforderungen an eine sichere Lösung (Eine wichtige Anforderung sei die Kenntnis der aktuellen Position des Transportgutes durch die Anlagensteuerung.), das Funktionsprinzip (Signal der Prozesssteuerung an den Sicherheits-Lichtvorhang kurz vor der Einfahrt in das Schutzfeld), das Grundprinzip Signalverlauf, verschiedene Betriebsarten für unterschiedliche Fördergeschwindigkeiten, den Synchronisationsstrahl und die feste Strahlausblendung. Die Sensoren und die zugehörige Dokumentation zur Integration der Lösung seien von unabhängiger Stelle zertifiziert.

Jens Rothenburg, Euchner, behandelt in der Ausgabe 10-2017 der Zeitschrift GIT, S. 120/121, die Risikobeurteilung mit der **Maschinensicherheitsnorm EN ISO 12100**. Eine generelle Strategie, wie das Risiko einer Maschine gemindert werden muss, sei einer der Hauptpunkte in der Norm. Sie informiere auch darüber, welche Lebensphasen einer Maschine abgesichert werden müssen und liste eine große Anzahl an Aufgaben während des Betriebs einer Maschine auf, die alle beurteilt werden müssten. Im Anhang der Norm finden sich Beispiele für die verschiedenen Möglichkeiten der Gefährdung.

Notfall

Jana Domrose, Tobias Zweckerl und Olaf Jastrob, Technisches Sachverständigenbüro Jastrob, behandeln in s+s report, Ausgabe 3-2017, S. 50–55, die **Notfallkommunikation bei Veranstaltungen**. Sie erläutern, welche Faktoren in einem Kommunikationskonzept als Teil eines Sicherheitskonzepts gem. § 43 MStättVO, betrachtet werden müssen, damit die Notfallkommunikation mit den verschiedenen Parteien einer Veranstaltung so effektiv wie möglich gestaltet werden kann. Die Formulierung knapper, aber präziser Informationen und Anweisungen sei eine der wichtigsten Herausforderungen. Die Verantwortlichen sollten sich über Antworten auf folgende Fragen verständigen: Was ist passiert? Wo ist es passiert und wer hat was zu tun? Es könne nützlich sein, sogenannte Code- oder Signalwörter für Notfallsituationen festzulegen. Auch sogenannte Notfall-Kommunikationsmittel sollten regelmäßig während der alltäglichen Arbeit genutzt werden. Wichtig seien in der Notfallkommunikation die deutliche Artikulation und der Tonfall, um die Dringlichkeit einer Botschaft zu betonen. Nach wissenschaftlichen Erkenntnissen müsse Notfallkommunikation mit Laien immer auf zwei Informationen eingehen: auf die Art und Ernsthaftigkeit des Notfalls und, welche sicheren Handlungsmöglichkeiten sich für den Empfänger der Botschaft ergeben. Eine Notfalldurchsage solle vor allem ehrliche, konkrete Informationen beinhalten. In manchen Notfällen mit hohem Panikpotenzial könne es aber durchaus sinnvoll sein, eine glaubwürdige Notlüge für die Räumung der Veranstaltung „in der Hinterhand" zu haben. Notfalldurchsagen sollten mehrmals wiederholt und mit Signaltönen oder -wörtern angekündigt werden. Die technische Ausstattung müsse einem Kommunikationsplan folgen, der wiederum die tatsächliche Organisation im Betrieb widerspiegelt. Die Kommunikation mit Menschenmengen in einem Panikstadium oder Vorstadium müsse aufgrund der geringen Wahrnehmungsfähigkeit besonders einfach und deutlich gestaltet werden.

Guido Gloy, Ascom Deutschland GmbH, erläutert in der Zeitschrift PROTECTOR, Ausgabe 10-2017, S. 52/53, die **Ersthelferalarmierung** bei lebensbedrohlichen Notfällen. Rund 10.000 Personen erleiden jährlich einen außerklinischen Herz/Kreislauf-Stillstand im betrieblichen Umfeld. Die Zeit bis zum Eintreffen der Rettungskräfte zu überbrücken, sei Aufgabe von Ersthelfern. Sie auszubilden und bereitzustellen sei Aufgabe des Arbeitgebers. Dabei gebe es branchenspezifische Regelungen, zum Beispiel in der DGUV Vorschrift 1. Bei zwei bis zu 20 Versicherten sei ein Ersthelfer vorgeschrieben. Bei mehr als 20 gelten prozentuale Anteile, und zwar in Verwaltungs- und Handelsbetrieben fünf Prozent, in sonstigen Betrieben zehn Prozent. Nach spätestens drei Minuten muss qualifizierte Hilfe vor Ort sein, sonst reißt die Rettungskette und weitere Bemühungen des Notarztes blieben häufig erfolglos.

Michael Schenkelberg, Schneider Intercom GmbH, stellt in der Oktober-Ausgabe des Behörden Spiegel die **Notfall-App „SaveME"** vor. In Deutschland sei heute jeder Arbeitgeber dazu verpflichtet, für jeden angebotenen Arbeitsplatz eine individuelle Gefährdungsanalyse anzufertigen. Schneider Intercom biete unter dem Namen „SaveME" eine hochverfügbare Notfall-App für Smartphones oder Tablet-PCs, die Mitar-

beiter in Notlagen hocheffizient unterstützen könne. Dank der Verbindung zwischen App und mit dem von Schneider Intercom angebotenen Commend-Intercomserver könne eine ständige Verfügbarkeit sichergestellt werden. Unabhängig vom jeweiligen Szenario reiche stets ein einfaches Fingertippen auf das Smartphone-Display aus, um einen Alarm auszulösen. Die App bringe eine neue, eigenständige Lösung zur präzisen Inhouse-Lokalisierung. Sie sei konzeptionell so flexibel aufgebaut, dass sie auf die Bedürfnisse verschiedener Anwendungsumfelder, Kunden und Märkte angepasst werden könne.

Öffentlicher Raum

Rund zwei Drittel aller **Ordnungsamtskräfte in Berlin** wurden bereits **Opfer von Straftaten,** berichtet der Behörden Spiegel in der Oktober-Ausgabe. Scheinbar unbeeindruckt seien die Täter von dem Umstand, dass die Kräfte überwiegend als Doppelstreife unterwegs sind. Gewalt werde gegenüber Männern wie gegenüber Frauen angewendet. 78 Prozent der bekannt gewordenen Angriffe erfolgten durch Einzeltäter. In 88 Prozent der Fälle sei die Attacke für den Betroffenen überraschend gekommen. Unerheblich für die Anzahl der Angriffe seien Tageszeiten und Lichtverhältnisse. Der „typische" Täter sei männlich, mittleren Alters, von normalem Körperbau und weder alkoholisiert noch unter dem Einfluss von Drogen stehend. Vor der Tat führe er einen Dialog mit dem Ordnungsamtsmitarbeiter, greife dann für diesen überraschend an, fliehe nach der Attacke nicht vor dem Eintreffen der Polizei und nehme keine Rücksicht auf möglicherweise vorhandene Zeugen.

Perimeterschutz

Michael Grau, Novatec Sicherheit & Logistik GmbH, beschreibt in PROTECTOR, Ausgabe 10-2017, S. 38/39, die **Objektsicherheit nach dem Zwiebelschalenprinzip**. Alarmsysteme zur Zaunsicherung auf RFID-Basis nutzen nach IP68 staub- und wasserdichte Beschleunigungssensoren, die an jedes Zaunsegment montiert würden. Die Tags kommunizierten untereinander und mit einer Alarmzentrale. Sabotageversuche führten zu Lücken in der Meldungskette und würden vom System sofort erkannt, ebenso wie die charakteristischen Erschütterungen, die bei Durchschneide- oder Überkletterversuchen entstehen. Wird der Zaun nur durch einen Windstoß bewegt, entstünde ein völlig anderes Schwingungsbild. Eine RFID-Zaunsicherung sei auch mit Videoüberwachung kombinierbar. Im Vergleich zu herkömmlichen, verkabelten Anlagen ließen sich durch das RFID-System bis zu 30 Prozent der Gesamtkosten einsparen.

Resilienz

Das Fachmagazin InfoSicherheit weist in der Ausgabe 3-2017, S. 36, darauf hin, dass im März 2017 von der Internationalen Organisation für Normung eine **Norm zur organisationalen Resilienz** veröffentlicht wurde. Diese Norm gebe Unternehmen aller Branchen Richtlinien zur Entwicklung einer resilienten Organisation an die Hand. Im Einzelnen zeige sie, auf welchen Prinzipien ein widerstandsfähiges Management aufgebaut sein sollte und welche Elemente eine konsistente und resistente Organisation haben muss. Neben den Kernpunkten Informationssicherheit und BCM würden in der ISO 22316 auch Bereiche wie die Finanzkontrolle, die strategische Planung und das Personalmanagement in Unternehmen behandelt.

Sicherheitsgewerbe

Manfred Buhl, Securitas Deutschland GmbH, äußert sich im Interview in Security insight, Ausgabe 5-2017, S. 35/36, zum Change Management, künstlicher Intelligenz, Videoüberwachung, „Predictive Services", dem Image der Sicherheitswirtschaft, Billiganbietern und Forderungen des Sicherheitsgewerbes zur **Optimierung der rechtspolitischen Rahmenbedingungen**. Entsprechend der Rechtslage in den meisten EU-Staaten solle die Zuständigkeit für die Betreuung und Kontrolle des Sicherheitsgewerbes vom Geschäftsbereich der Wirtschaftsminister in den der Innenminister in Bund und Ländern übergehen. Das gewerberechtliche „Bewachungsrecht" müsse durch ein modernes Sicherheitsleistungsgesetz abgelöst werden, in dem auch unternehmenseigene Sicherheitsdienstleistungen außerhalb des Sicherheitsgewerbes in öffentlich zugänglichen Räumen wie

Einzelhandelsobjekten oder Fußballstadien reguliert werden könne. Das Vergaberecht müsse so geändert werden, dass die Vergabe zu Dumpingpreisen möglichst verhindert wird.

Sonderschutzfahrzeuge

Robert Frischbier, Apprich Secur GmbH, wirft in der Ausgabe 10-2017 der Zeitschrift PROTECTOR, S. 68/69, einen Blick auf jüngste Entwicklungen im Bereich der Sonderschutzfahrzeuge: „Soft Skin"-Fahrzeuge, die über keine physische Panzerung im herkömmlichen Sinn verfügten, sondern ausschließlich über einen elektronischen Schutz. Heute sichere komplexe Elektronik die Werte. Einfärbungssysteme – IBNS – machten das Geld im Falle des Falles unbrauchbar, und biometrische Systeme sicherten die Zugänge zu den Schleusen in den Fahrzeugen anstelle von zentimeterdicken Stahlwänden. Die heutigen Sicherungssysteme bestimmten dank der Elektronik auch, wer und wie viele Personen Zugang zum Fahrzeug bekommen und wer es fahren darf. Den Kern der von Apprich Secur entwickelten neuen Steuerungsgeneration „CANcom2" bildeten drei Module: ein Alarmmodul, ein Startfreigabe- und Autorisierungsmodul und ein Verriegelungsmodul.

Spionage

Zeit.de meldet am 5. Oktober, dass die Bundesanwaltschaft nach eigenen Angaben **keine konkreten Hinweise auf illegale Spionage der NSA** gegen die Bundesrepublik Deutschland gefunden habe. Sie sehe demnach keinen Raum für weitere staatsanwaltschaftliche Untersuchungen. Auch die Aufklärung durch den NSA-Untersuchungsausschuss des Deutschen Bundestages habe „keine belastbaren Anhaltspunkte dafür ergeben, dass US-amerikanische oder britische Nachrichtendienste das deutsche Telekommunikations- und Internetaufkommen rechtswidrig systematisch und massenhaft überwachen". Der NSA-Untersuchungsausschuss hätte nach mehr als drei Jahren seine Arbeit im Streit beendet. Während Union und SPD keine Belege für illegale Massenüberwachung gesehen hätten, habe die Beweisaufnahme nach Ansicht der Opposition belegt, dass die Geheimdienste sehr wohl anlass- und unterschiedslos auch Deutsche überwacht hätten. Die Bundesanwaltschaft sehe auch keine Hinweise für die systematische Überwachung der Kommunikation, die über in Deutschland verlaufende Glasfaserkabel abgewickelt wird. Sie berufe sich dabei auch auf die Einschätzung des BfV und des BSI.

Das Deutsche Zentrum für Luft- und Raumfahrt (DLR) habe seine Router ausgetauscht, meldet golem.de. **Statt Cisco-Produkten** würden aus Angst vor Industriespionage und Überwachung künftig solche von **Lancom** zum Einsatz kommen. Das geschehe auch aus staatsbürgerlicher Verantwortung, denn Lancom sei ein deutscher Hersteller und gehe dem DLR zufolge mit Kunden besser um als „Cisco, Microsoft oder Oracle", die selbst große Kunden wie „kleine Bittsteller" behandelten. In einem „besonders sensiblen Bereich" des DLR-Netzwerkes sollen diese Konsequenzen nun gezogen worden sein.

Tankstellenüberfall

GIT weist in der Ausgabe 10-2017, S. 24, darauf hin, dass seit sieben Jahren die **Zahl der** Überfälle auf Tankstellen kontinuierlich zurückgeht und 2016 mit 571 registrierten Fällen auf dem niedrigsten Stand seit der Wiedervereinigung lag. Zum einen würden die Sicherheitskonzepte immer mehr greifen. Dazu komme, dass an Tankstellen nur wenig Bargeld, bei gesicherten Kassensystemen gar kein Bargeld, zu erbeuten sei.

Terrorismus

Nach der Darstellung der Bedrohungslage Deutschlands durch den internationalen Terrorismus (Focus on Security, Ausgabe Oktober 2017) geht Dr. Peter Roell, ISPSW, in der Ausgabe Nr. 510, Oktober 2017, der ISPW-Publikationen auf **Abwehrmaßnahmen** ein. Es werde deutlich, dass der „IS" ganz gezielt in den Strom der Flüchtlinge auch Personen einschleust, die in Deutschland und der EU Anschläge durchführen sollen. In der EU seien 16 solche Fälle bekannt geworden. Der Autor erläutert das am 24. Juni 2016 im Bundestag verabschiedete sogenannte Antiterrorpaket und den Neun-Punkte-Plan der Bundeskanzlerin, der am 28. Juli 2016 vorgestellt worden ist. Der Autor kommt schließlich zu folgen-

den Ergebnissen: 1. Der „IS" habe seine Aktivitäten bereits weltweit ausgebaut. Deutschland, die EU und befreundete Staaten müssten sich auf die neuen Gegebenheiten einstellen. 2. Ein besonderes Augenmerk sollte vermehrt auf Entwicklungen in Südostasien und eine engere Kooperation mit den Nachrichten- und Sicherheitsdiensten der Philippinen, Indonesien, Singapur und Malaysia gelegt werden. 3. Da der „IS" mehr und mehr verschlüsselt kommuniziert, sei es völlig richtig, dass die Nachrichten- und Sicherheitsdienste gesetzlich und technisch in die Lage versetzt werden, in diese Verkehre einzudringen. 4. Operative Terrorismus-Fachgespräche sollten sich auf nachweislich besonders kompetente Dienste fokussieren. Ergänzend sei auch ein Austausch mit führenden Think Tanks und Terrorismusexperten weltweit gewinnbringend. 5. Alle staatlichen Ressourcen müssten gebündelt, die Bevölkerung, die Wirtschaft und die Industrie zur Bewältigung dieser herausfordernden Aufgabe mit eingebunden werden.

„Sicherheitsassistenzsystem warnt vor schmutzigen Bomben" thematisiert das Fachmagazin InfoSicherheit in der Ausgabe 3-2017, S. 30. Experten warnten seit langem vor Anschlägen mit schmutzigen Bomben. Sie befürchteten, dass Terroristen konventionellem Sprengstoff radioaktives Material beimischen könnten. Die für den Bau von schmutzigen Bomben erforderlichen Radioisotope seien leichter zu beschaffen als spaltbares Material für Kernwaffen. Ein Assistenzsystem, das radiologische Gefährder in einem Personenstrom erkenne und das Sicherheitspersonal alarmiere, sei der Beitrag des Fraunhofer Instituts FKIE zum deutsch-französischen Projekt REHSTRAIN, das die **Verwundbarkeit der Hochgeschwindigkeitszüge** erforscht. Das Assistenzsystem setze sich aus mehreren Komponenten zusammen: einem Sensornetzwerk, handelsüblichen Kinect-Kameras sowie einer Software zur Datenfusion. Die vernetzten Geräte erfassten Menschen zeitlich und räumlich, die Daten würden fusioniert. Dank ausgeklügelter mathematischer Auswertealgorithmen würden die gewünschten Informationen aus den riesigen Datensätzen herausgefiltert. An neuralgischen Punkten angebracht könnten solche Assistenzsysteme künftig Informationen über radiologische Gefährder an die Überwachungssysteme etwa der Verkehrsbetriebe übertragen.

Unternehmenssicherheit

Peter Niggl, Chefredakteur von Security insight, befasst sich in der Ausgabe 5-2017, S. 14–17, mit der Rolle und dem **Status des Sicherheitsverantwortlichen im Unternehmen**. Der Autor bezieht sich auf einen 2015 verfassten „Kompetenzatlas", in dem festgestellt werde: „Der moderne CSO wird vom einstigen Wächter über physische Unternehmenswerte zum global denkenden Business Advisor, der Teams mit Mitarbeitern unterschiedlicher Kulturen, Mentalitäten und Qualifikationen führt." Eine Hochschulqualifikation sei dafür sicher Voraussetzung, aber auf keinen Fall ausreichend. Der Sicherheitsverantwortliche müsse die Sicherheitslage auch in anderen Ländern im Blick behalten und sich auf eine interkulturelle Belegschaft einstellen. Auslandserfahrung dürfte für ihn eine wichtige Rolle spielen. Der Manager und Mediator sei gefragt, die Mehrsprachigkeit spiele eine immer größere Rolle. Last but not least: Der CSO müsse die Unternehmensphilosophie und -strategie verinnerlicht haben.

„Müssen die Schwestern **Safety und Security unter eine Haube?",** fragt Security insight in der Ausgabe 5-2017, S. 44–47. Die organisatorische Trennung der beiden Sicherheitsbegriffe habe sich in der Praxis überlebt. Beim Internet der Dinge oder Industrie 4.0 ließen sich die beiden Begriffe in den Abläufen praktisch nicht mehr trennen. Dies führe in der logischen Konsequenz dazu, dass auch die administrative Verantwortung für die Abläufe in einer Hand zusammengeführt werden müsse.

Unternehmensstrafrecht

Ein Strafrecht für Unternehmen werde es nach dem Willen von Peter Biesenbach, dem Justizminister des Landes NW, nicht geben, berichtet die FAZ am 4. Oktober. Damit stelle er sich gegen die Position seines Vorgängers Thomas Kutschaty. Höhere Bußgelder für ein Fehlverhalten von Unternehmen könne er sich aber durchaus vorstellen. Die VW-Abgasaffäre sei kein Argument dafür, auch Unternehmen mit Strafen zu überziehen. Strafe kläre nicht auf. Als Unternehmen habe VW nichts getan. Ein Unternehmensstrafrecht könnte die Manager sogar entlasten.

Videoüberwachung

Nach einer Untersuchung der Stiftung Warentest haben **die meisten Überwachungskameras Sicherheitsmängel** (golem.de vom 29. September). Trotz der Gefahr durch schlecht abgesicherte Geräte lieferten Hersteller weiterhin unsichere Überwachungskameras aus. Bei einem Vergleich von 16 IP-Kameras hätten die Tester nur ein einziges Gerät gefunden, das gut abgesichert war, die D-Link 2330L. Von den übrigen 15 Kameras hätten zehn ein Befriedigend, zwei ein Ausreichend und drei ein Mangelhaft beim Thema Sicherheit erhalten. Als kritisch bis sehr kritisch hätten die Tester zudem bei zehn Kameras die Einbindung der Smartphone-Apps für die Kontrolle der Kameras eingeschätzt. Geräte von Instar und Technaxx seien durchgefallen, weil sie triviale Zugangsdaten wie „admin" als Nutzername oder „instar" und „admin" als Passwort verwenden. Ob solche Kameras tatsächlich ein Sicherheitsrisiko darstellen, hänge vor allem von den verwendeten Router-Einstellungen ab. Sind schlecht gesicherte IP-Kameras offen im Internet zu finden, könnten sie leicht in ein Botnetz eingebunden werden.

Eine **Software-Lösung zur automatischen Kontrolle von Video-Sicherheitssystemen** stellt das Unternehmen Geutebrück in der Ausgabe 10-2017 der Zeitschrift GIT, S. 44/45, vor. Mit G-Health werde das Video-Sicherheitssystem permanent von einer unabhängigen, eigenständig arbeitenden Monitoring-Software überprüft, die wie ein virtueller Techniker im 24/7-Dienst vor Ort unablässig teste. Dabei würden alle Betriebsparameter jedes einzelnen NVRs von einem lokal installierten Überwachungs-Client analysiert, der mittels spezialisierter Plugins permanent die Leistungsdaten aller aktiven Hard- und Software-Komponenten überwacht. Das umfasse alle Rekorderfunktionen, von der Kamerakonfiguration bis zum Datendurchsatz der Aufzeichnung, es umfasse die Computerfunktionen wie die Speichermedien. Diese Daten würden im Netzwerk an einen zentralen Überwachungs-Server übermittelt, der eine Vielzahl Überwachungs-Clients an unterschiedlichen Standorten verwalten könne. Abweichungen vom Normalzustand oder Störungen würden von diesem Server per Anlagenevent oder per E-Mail gemeldet. Der Wartungstechniker habe zu jeder Zeit Zugriff auf alle relevanten Systemparameter, um vorsorglich erkennen zu können, ob in absehbarer Zeit Störungen an „Verschleißteilen" zu erwarten sind.

In der Ausgabe 10-2017 der Zeitschrift GIT, S. 48/49, wird die **„extended Power over Ethernet IP-Lösung"** von Dahua vorgestellt, die die Möglichkeit zur Übertragung von Videodaten erweitert, eine elegante Lösung, um Videodaten über weite Strecken zu übertragen und Geräte über das Netzwerk mit Strom zu versorgen. Die ePoE-Technologie von Dahua arbeite mit moderner 2D-PAM3-Codierungsmodulation von der physischen Schicht und implementiere Vollduplex-Übertragungen über 800 Meter mit einer Geschwindigkeit von 10 Mbps oder über 300 Meter mit einer Geschwindigkeit von 100 Mbps über Cat5- oder Koaxialkabel.

WLAN-Analysen zur Ergänzung von Videoanlagen thematisiert GIT in der Ausgabe 10-2017, S. 51. Besonders in großflächigen Installationen sei es oft schwierig, flächendeckende Analysedaten rein über das Kamerabild zu erhalten. Zur Ergänzung der Videoanlagen eigneten sich WLAN-Analysen, die zudem die Investition in ein Public-WLAN noch sinnvoller machten. Als Zusatz zu den gelieferten Bilddaten der Videoanlage erhalte man ein detailliertes Bewegungsprofil von Personen, sowie Informationen über Stoßzeiten und Ballungsgebiete, beispielsweise an öffentlichen Plätzen oder Bahnhöfen.

Der Behörden Spiegel weist in der Oktober-Ausgabe auf ein Urteil des OVG Lüneburg hin, nach dem für die Frage der **Zulässigkeit von Videoüberwachung im ÖPNV** das BDSG anwendbar ist. Die Überwachung diene der Wahrnehmung berechtigter Interessen der Verkehrsbetriebe. Dazu gehörten unter anderem die Verhütung und Verfolgung von Straftaten gegen ihre Fahrzeuge. Diese seien im Verhältnis zu den schutzwürdigen Interessen der von der Überwachung Betroffenen vorrangig.

Wohnungseinbruch

Gina Rosa Wollinger M.A. und Nadine Jukschat M.A., Kriminologisches Forschungsinstitut Niedersachsen e. V., stellen in s+s report, Ausgabe 3-2017, S. 42–45, eine Studie zu 30 qualitativ-biografischen **Interviews mit einsitzenden Einbrechern** vor. Drei typische Deutungen und Selbstreflexionen der Täter hätten herausgearbeitet werden können: Einbruch „aus der Not heraus", Weg zu „schnellem Geld" und Einbruch als „Beruf". Verschiedene Strukturen seien innerhalb Deutschlands für die Begehung von Wohnungseinbrüchen

zentral: „Ankerpunkte vor Ort", Kontakt zu einem kriminellen Milieu und Absatz der Beute. Dem Fokus der Prävention auf mechanische Sicherungen komme zentrale Bedeutung zu. Als weniger relevant hätten sich technische Maßnahmen wie Alarmanlagen und Videokameras erwiesen. Typischerweise stellten sich die Täter mit ihrem Verhalten auf Alarmanlagen ein. Abschreckend wirke das Gefühl, leicht aufzufallen und beobachtet zu werden. Das Entdeckungsrisiko – und nicht die angedrohte Strafe – sei für die Täterentscheidung wichtig.

Zutrittskontrolle

Gilbert Hödl und Gregor Zehetner, Tapkey GmbH, stellen in der Ausgabe 10-2017 der Zeitschrift PROTECTOR, S. 30/31, eine von Tapkey entwickelte **Smartphone- und Cloudbasierte Zugangsplattform** vor, die digitale Zutrittskontrolle und physischen Zugang über das Smartphone verbindet. Die offene, herstellerunabhängige Plattform bilde die Basis für ein ganzes Ökosystem an Lösungen, die mit Hardware, Software oder App-zu-App-Lösungen integriert werden könnten. Die Plattform eigne sich für Anwendungen aus den verschiedensten Branchen, bei denen der identitätsbasierte Zutritt einfach, sicher, flexibel und schnell ablaufen soll. Typische Einsatzgebiete seien die Automobilbranche, Logistik und Lieferdienste, Facility- und Immobilienmanagement. Die Autoren behandeln die Anbindung weiterer Smart-Home-Systeme und die Anmeldung ohne Passwort mit digitaler ID.

VERANSTALTUNGSHINWEIS

Sehr geehrte Damen und Herren,

da Sie sich in der Vergangenheit an einer unserer Informationsveranstaltungen interessiert gezeigt hatten, erlauben wir uns, Sie auf drei DIN-Informationsveranstaltungen zum Thema „Sicherungsdienstleistungen – Veröffentlichung der DIN 77200-1 und DIN 77200-3" aufmerksam zu machen.

Die kostenpflichtigen Veranstaltungen des DIN e. V. in Berlin, Köln und München werden mit freundlicher Unterstützung von BDSW, VdS und ASW durchgeführt.

Zur Anmeldung und Information

Mit freundlichen Grüßen
die Securitas Unternehmenskommunikation

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