Focus on Security

Ausgabe 01, Januar 2017

SECURITAS

Inhalt

Biometrie

Wie Dahua Technology Co. Ltd. in der Ausgabe 12-2016, S. 35, mitteilt, diene der weltweit angesehene Test „Labeled Faces in the Wild" (LFW) zur Prüfung der **Detektionsgenauigkeit von Gesichtserkennungssystemen** und basiere auf einer einheitlichen Datenbank. Nun sei ein neuer Rekord bei der Genauigkeit aufgestellt worden. Die Dahua-Gesichtserkennung nutze über 100 Schichten und ermögliche so eine neue Form des Metric Learning, die bessere Werte bei der Übereinstimmung von Gesichtsbildern der gleichen Person liefere. Gepaart mit einer effizienten Online-Sampling-Technik könne das Maß an Konvergenz deutlich erhöht werden. Durch das Training mit mehreren Modellen sowie durch die Verwendung einer nicht-linearen Multimodell-Integration habe Dahua eine Genauigkeit von 99,78 Prozent im LFW-Datenpool erzielt.

Brandschutz

Dr. Ing. Thomas Sindermann, Prof. Schiffers BauConsult GmbH & Co. KG, gibt in s+s report, Ausgabe 4-2016, S. 8/9 Antworten auf die Frage, ob der Brandschutz als Sündenbock für Verzögerungen und Kostenexplosionen bei öffentlichen Großbauten benutzt werde. Das Brandschutzkonzept sollte in der Leistungsphase 3 bis 4 erstellt werden. Hierin würden zunächst die grundsätzlichen funktionalen Zusammenhänge der verschiedenen sicherheitstechnischen Einrichtungen definiert. Mit fortschreitender Planungstiefe – insbesondere der technischen Gebäudeausrüstung – sollte diese Grundstruktur durch den Brandschutzsachverständigen laufend fortgeschrieben, angepasst und verfeinert werden. Im Zuge der **Erstellung des Brandschutzkonzeptes** sollten laufend Abstimmungen unter den Fachplanern erfolgen, welche Funktionen die einzelnen sicherheitstechnischen Einrichtungen im Brandfall gewährleisten müssten und wie sie untereinander zu steuern seien.

Dr. Jörg Kelleter, GTE GmbH, behandelt in Ausgabe 4-2016 von s+s report, S. 14–17, die **Brandmeldetechnik in Kraftwerken**, ihre Einsatzmöglichkeiten und Grenzen. Er befasst sich zunächst mit Brandursachen. Zur Überwachung von Kohle, die über längere Zeit in trockener Umgebung lagere, werde bevorzugt Brandgasdetektion (GSME – Gassensormeldeeinheit) eingesetzt. Der Autor hebt die besondere Eignung von Brandgasmeldern hervor, denn schwelende Kohle setze einen hohen Anteil an Brandgasen frei; Brandgasdetektoren würden nicht durch Staub verunreinigt und ein Brandgasmelder, der mehrere Gaskomponenten separat erfasse, könne ideal an das erwartete Brandszenario angepasst werden. Dr. Kelleter behandelt die Selbstentzündung von Kohle und Biomasse, den Spezialfall des Kohlenbunkers oder des Biomassesilos, die Branddetektion in mechanischen Zerkleinerern und die brandtechnische Planung. Bei der Abnahme und Prüfung stelle sich neben einer Reihe von formalen Kriterien in der Regel die Frage der Wirksamkeit der Brandmeldeanlage. Für eine Reihe von Materialien lägen Erfahrungen mit Realbrandtests vor. Der Autor beschreibt den Realbrandtest mit Steinkohle und hält den Realbrandtest in einem Bunker für sicherheitstechnisch nicht beherrschbar und zu aufwendig.

Dr. Ing. Mingyi Wang zeigt in s+s report, Ausgabe 4-2016, S. 18–22, wie sich das **Brandrisiko nach Bauartklassen** kategorisieren lässt. Die Bauartklassen der Versicherer und vergleichbare Klassenbildung von Gebäuden hätten sich in der Praxis als ein einfaches Instrument zur Einstufung baulicher Brandgefahren und der damit verbundenen Risiken bewährt. Dabei werde zwischen Wohngebäuden sowie Gewerbe- und Industriebau differenziert. Der Autor befasst sich im Einzelnen mit der Risikobewertung von Gebäuden, mit der Kategorisierung von Bauartklassen, der

Anwendung der Bauartklassen in der Praxis, mit den zu bewertenden Bauteilen und ihren Funktionen, mit dem Instrument ISO Construction Class des amerikanischen Anbieters statistischer Analyse und Informationen ISO und mit Schnittstellen zu anderen baulichen und gebäudetechnischen Gegebenheiten.

In s+s report, Ausgabe 4-2016, S. 23–25, erörtert Len Swantek, Victaulic, die Bedeutung von **Richtlinien für den Brandschutz**, und warum zertifizierte Produkte so wichtig für den wirksamen Brandschutz von Gebäuden sind. Er geht näher ein auf die Notwendigkeit früher Planung und auf die Richtlinienarbeit. Es sei ein sichtbares Zeichen der regulatorischen Kompetenz und Bestätigung, dass die höchsten Sicherheitsstandards erreicht wurden, was von der Bauindustrie gewünscht werde. Er betont ferner die Rolle der Hersteller, den Prüfprozess und die Zusammenarbeit mit den Errichterfirmen. Bei Neubauten gebe es keine ausreichende Rechtfertigung dafür, auf eine Kombination von passiven und aktiven Brandschutzsystemen zu verzichten.

Innovativer **Brandschutz auf der Baustelle** ist das Thema eines Beitrags von Dipl.-Phys. Michael Jäger, Leiter eines Büros für Bauplanung und Bauphysik, und Dipl.-Ök. Adam Kavics, Ramtech Electronics, in der Ausgabe 4-2016 von s+s report, S. 32/33. Baustellen seien immer besondere Gefahrenpunkte. Oft befänden sich auf Baustellen leicht entzündliche Materialien, Gasflaschen, gefährliche Maschinen und Werkzeuge sowie Fahrzeuge und elektrische Materialien aller Art. Die Autoren fordern praktikable Lösungen und listen branchenspezifische Anforderungen an den Brandschutz auf Baustellen auf. Und sie erläutern, was der Leitfaden VdS 2021 für Baustellen fordert. Ein drahtlos vernetztes mobiles Brandmelde- und Alarmsystem auf einer Baustelle sei ein sehr effektiver, wirtschaftlicher und praktischer Baustein im Bemühen, Personen- und Sachschäden zu vermeiden.

Frank Drolsbach, FM Global, sieht in der Ausgabe 12-2016, S. 38/39, von PROTECTOR Nachholbedarf für den **Brandschutz in Hotels**. Er plädiert für automatische Sprinkleranlagen. Die könnten für jedes einzelne Gebäude maßgeschneidert entworfen, in regelmäßigen Abständen überprüft und bei veränderten Gegebenheiten vor Ort an diese angepasst werden. Ferner müssten vor der Installation weitere Parameter berücksichtigt und bestimmt werden: die Auslösetemperatur des Sprinklers, der Spinklerdurchfluss, der die Reaktionszeit bestimmende RTI-Wert und die Ausrichtung des Sprinklers. Moderne Sprinkler könnten für ein Prozent der Gesamtbaukosten installiert werden. Forschungsergebnisse würden belegen, dass das Schadensausmaß in ungesprinklerten Betrieben vier- bis fünfmal höher ausfällt als in Betrieben, die eine automatische Sprinkleranlage installiert haben. Rund 50 Prozent aller Brandereignisse würden bei Auslösung von maximal drei Sprinklern und ungefähr 75 Prozent bei Auslösung von bis zu neun Sprinklern kontrolliert.

Aktive **Brandvermeidung im automatisierten Hochregallager** behandelt PROTECTOR in der Ausgabe 12-2016, S. 40/41. Hohe Regale und schmale Zwischenräume würden die Gefahr bergen, dass sich ein Brand schnell bis unter die Hallendecke ausbreiten kann und eine Brandlöschung mit konventionellen Mitteln wie Schaum oder Wasser erschwert wird. Wenn Kleinladungsträger und Kunststoffe zum Einsatz kommen, gebe es vor allem zwei Probleme. Eines stelle die sehr gute Brennbarkeit des Materials dar: Polypropylen und Polyethylen verhielten sich beim Brand wie brennbare Flüssigkeiten und zeigten eine vergleichbare Wärmefreisetzung wie Benzin. Wenn sich genügend Material verflüssigt habe, gebe es einen „Lachenbrand" unterhalb der Lagerkonstellation. Das brennend abtropfende Material entzünde alle benachbarten Materialien, während die große Wärmeenergie das Feuer weiter anfache. Als zweites Problem komme hinzu, dass ein

solcher Brand schwer zu löschen ist, da sich Wasser schwer auf Kunststoffoberflächen applizieren lässt. Als vorbeugende Maßnahme komme Sauerstoffreduzierung in Betracht. Die Brandvermeidungsanlage bestehe aus drei wesentlichen Komponenten: dem Stickstofferzeuger, der Steuerzentrale Oxycontrol und den Sauerstoffsensoren Oxy Sens.

Brandschutz bildet den Schwerpunkt von Nummer 23 des Sicherheits-Berater vom 1. Dezember. Behandelt werden die nachfolgenden Themen: **Polystyrol-Fassadendämmung** beeinträchtige den Fluchtweg. Im Wohnungsbau und bei kleineren Bürohäusern mit zwei oder drei Vollgeschossen sei ein zweiter Fluchtweg nicht zwingend notwendig, da man davon ausgehe, dass eine Rettung von Personen problemlos durch ein Anleitern der Feuerwehr möglich ist. Das sehe aber schnell anders aus, wenn ein solches Anleitern aufgrund eines Fassadenbrandes gar nicht möglich ist, wenn nämlich die Wärmedämmung der Fassade brennt. Derartige Brände hätten gezeigt, dass sie sich sehr schnell um das gesamte Haus herum entwickeln können und somit an keiner Stelle mehr ein sicherer Fluchtweg zur Verfügung steht (S. 369/370). 90 Prozent aller Brandopfer sterben nicht durch Flammen, sondern durch Rauch. Manchmal verlange die Architektur besondere Ideen, um die geforderten Brand- und Rauchabschnitte problemlos zu realisieren. Für eine ansehnliche Lösung böten sich textile **Rauch- und Feuerschutzabschlüsse** besonders an. Diese ermöglichten einen passenden Raumabschluss, der sich auch über mehrere Etagen erstrecken könne. Im Alarmfall würden diese Systeme automatisch schließen und frühzeitig Schutz vor der Verrauchung bieten (S. 371–372). Der Sicherheits-Berater wendet sich mit einer Vielzahl von Argumenten gegen Wasser als Löschmittel in **Rechenzentren**. Er plädiert sowohl gegen Sprinkleranlagen wie „Hochdrucksprühnebelanlagen". So könne eine Sprinkleranlage überhaupt nicht auslösen, weil bei einem Brand im Deckenbereich über dem Rechner die Temperatur die Auslösetemperatur gar nicht erreicht. Im übrigen würden Rechenzentren nicht brennen, sondern schwelen. Ein erhebliches Risiko gehe aber von Schränken mit unterbrechungsfreier Stromversorgung in Rack-Reihen aus (S. 372–376). Ein weiterer Abschnitt befasst sich mit Brandgefahren für **Photovoltaikanlagen**. Bei solchen Bränden entstünden giftige Gase, die zumeist auf die Werkstoffe zurückzuführen seien, die in diesen Anlagen verbaut sind. Die größte Gefahr für die Einsatzkräfte ergebe sich durch die Elektrizität. Denn Photovoltaikanlagen ließen sich prinzipbedingt nicht völlig stromlos schalten. Sind die Photovoltaikmodule beschädigt, könnten sehr große Gleichspannungen auftreten, die sich zu gefährlichen Lichtbögen entwickeln können. Der TÜV Rheinland und das Fraunhofer-Institut für Solare Energiesysteme hätten in einem gemeinsamen Forschungsprojekt unter anderem Anforderungen für technische Einrichtungen aufgestellt, die im Fall eines Brandes die elektrische Spannung an der PV-Anlage abschalten. Die Ergebnisse dieses Projekts seien in einem 308 Seiten starken Leitfaden ausführlich und gut verständlich aufgeführt. Der Sicherheits-Berater zeigt organisatorische, technische und bauliche Maßnahmen zum Brandschutz für Photovoltaikanlagen auf (S. 378–383). Das Prinzip der Abschottung sei im baulichen Brandschutz eine der wirksamsten Schutzmethoden. Die vorherrschende Verglasung in der modernen Architektur könne auf Brandschutzanforderungen treffen. Dann müssten **Brandschutzverglasungen** zum Einsatz kommen, und zwar G-Verglasung, bei der – zeitlich begrenzt – weder Feuer noch Rauch durchdringen kann, oder F-Verglasung, bei der auch Hitzestrahlung nicht durchdringen kann (DIN 4102). Grundsätzlich sollte die Brandschutzverglasung der Risikobewertung entsprechend sorgfältig geplant werden (S. 383/384). Ein neues Löschverfahren mit **Blähglasgranulat** habe die NEBUMA GmbH auf der Security-Messe 2016 vorgeführt.

Das Unternehmen habe die einzelnen Körner mit einer speziellen Phosphatverbindung veredelt, die auf der Oberfläche angebracht werde. Dadurch erhöhe sich die Temperaturstabilität des Materials. Es könne nun problemlos selbst bei Temperaturen von über 1.350 Grad Celsius eingesetzt werden. Bei dem neu entwickelten Löschverfahren „NEBUFight" befinde sich das Granulat in einem Behälter. Es werde bei Auslösung des Löschvorgangs durch eine spezielle Düse mit einem Bindemittel besprüht. Durch die Zufuhr des Bindemittels bleibe das Granulat im ersten Moment auf der Brandstelle haften, bevor sich in Verbindung mit den hohen Temperaturen eine keramisierende Wirkung einstelle und sich eine Kruste bilde. Dadurch werde die Sauerstoffzufuhr unterbunden und gleichzeitig die Brandtemperatur so weit isoliert, dass die Umgebung des Brandherdes vor hohen Temperaturen geschützt wird (S. 385/386).

Mit der effektiven **Ableitung von toxischem Brandrauch** befasst sich GIT in der Ausgabe 12-2016, S. 64/65. Bei jedem Brand würden sich giftige Substanzen entwickeln, die bereits nach wenigen Atemzügen zum Tod führen können. Vielen Menschen sei diese Tatsache nicht bewusst. Sie unterschätzten die Risiken von Brandrauch und brächten sich dadurch in Gefahr. In komplexen öffentlichen Gebäuden könnten selbstschließende Rauchschutztüren nach DIN 18055-1 die Verbreitung von gefährlichen Rauchgasen verhindern. Sie seien zwar nicht feuerfest, würden für eine Rettung in der Brandentstehungsphase mit beginnender Verrauchung jedoch als ausreichend angesehen. RWA leiteten die toxischen Zersetzungsprodukte zuverlässig nach außen ab. Dabei machten sie sich den physikalischen Effekt des thermischen Auftriebs zunutze. Beim Verbrennungsprozess steige der heiße Rauch nach oben. Strömt im unteren Gebäudebereich ausreichend Frischluft nach, bilde sich in Bodennähe eine stabile raucharme Schicht.

Brandschutzschalter für die U-Bahnhöfe in Nürnberg thematisiert Dipl.-Ing. Uwe Scherer, Siemens Energy, in GIT, Ausgabe 12-2016, S. 68/69. Brandschutzschalter erkennen serielle und parallele Fehlerlichtbögen und schalten im Bedarfsfall den Stromkreis eigenständig ab. Fehlerlichtbögen entstünden in aller Regel durch beschädigte Leitungen, die unter anderem durch eingeklemmte, überhitzte oder zu stark gebogene Kabel verursacht werden. In Außenbereichen seien für solche Leitungsschäden oft auch nagende Tiere verantwortlich. Gemäß IEC 60364-4-42 empfehle es sich seit 2014 dringend, Brandschutzschalter einzubauen. Hinzu komme die Norm DIN VDE 0100-420. Seit ihrer Veröffentlichung im Februar 2016 gelte der Brandschutzschalter in besonders gefährdeten Bereichen als „anerkannte Regel der Technik".

Drohnen

Nils Hellberg und Björn Karaus, GDV, behandeln in der Ausgabe 4-2016 von s+s report, S. 40–42, den **Versicherungsschutz für Drohnen**. In einer sogenannten „Drohnen-Verordnung" sollen verschiedene Regelungen zur zivilen Nutzung von Drohnen getroffen werden. Eigentlich seien alle Drohnen-Piloten gemäß § 43 Abs. 2 Luftverkehrsgesetz verpflichtet, eine eigene Luftfahrthaftpflichtversicherung abzuschließen. Der GDV plädiere für eine gesetzliche Neuregelung, denn insbesondere privaten Drohnenpiloten sei diese Versicherungspflicht oft vollkommen unbekannt. Nach Überzeugung der Autoren könnte eine sinnvolle und transparente gesetzliche Klarstellung des Spielzeugbegriffs auf die Kriterien Gewicht, Größe, Geschwindigkeit und Gefahrenpotenzial abstellen, die die Rechtsprechung bisher zur Abgrenzung heranzieht. So könnten Drohnen mit geringerem Schadenpotenzial von der Versicherungspflicht befreit werden. Schäden durch diese Drohnen wären dann automatisch über die Privathaftpflichtversicherung versichert.

Schwere und schnelle sowie gewerblich genutzte Drohnen hingegen sollten auch weiterhin der Versicherungspflicht unterliegen und über eine gesondert abzuschließende Luftfahrthalterhaftpflichtversicherung abgesichert werden müssen.

Stephan Leukert, VZM GmbH, befasst sich in Ausgabe 6-2016 des Sicherheitsforums, S. 16–19, mit der **Risikobewertung von unbemannten Luftfahrzeugen** (UAV). Er behandelt die Rechtslage, Nutzungsmöglichkeiten, Risiken und Abwehrmaßnahmen. Unabhängig vom technischen Stand stießen „aktive" Abwehrsysteme schnell sowohl an rechtliche als auch praktische Grenzen. Es sei daher zielführender, sich auf organisatorische Maßnahmen zu konzentrieren. Da man nicht die Drohne als solche „bekämpfen" könne, müsse man sich eben vor den möglichen Folgen schützen. Dazu gehörten klassische Methoden der Risikoabwehr, zum Beispiel elektronische Aspekte zur Sicherung von Konferenzräumen, Nutzung optischer Hürden zur Vermeidung von Bildaufnahmen, Nutzung sprengwirkungshemmender Bauteile, Installation von Gasdetektoren an Frischluftansaugungen und Überdeckung von Innenhöfen mit Netzen.

Einbruchmeldeanlage

Dipl.-Ing. Günter Grundmann stellt in s+s report, Ausgabe 4-2016, S. 36/37, ein Türband mit kabelloser Verbindung vor. Bei Türen, Fenstern und Toren bestehe nicht selten die Notwendigkeit, eine Verbindung zu Anlagenteilen von EMA herzustellen, die im Türblatt oder Fensterflügel verbaut sind, um Informationen und gegebenenfalls Energie zur Stromversorgung aktiver Komponenten zu übertragen. Nun sei in den VdS-Laboratorien erstmals mit positivem Abschluss eine technische Lösung geprüft worden, die ohne Kabelverbindung sowohl die Übertragung von Energie als auch von Informationen vom festen zum beweglichen Teil der zu überwachenden Tür oder des zu überwachenden Fensters übernehme. Der Autor geht näher auf die Zuverlässigkeit und Funktionssicherheit, auf die Bediensicherheit, die Sabotagesicherheit und die Sicherheit der Übertragung ein.

Energieversorgungssicherheit

Hacker gefährden die Stromversorgung, titelt die FAZ am 28. November. Während das BSI von einer neuen Qualität der Cyberkriminalität spreche, warnen Fachleute vor Hackerangriffen auf Unternehmen der Energiebranche. Wegen der mangelhaften IT-Sicherheit in den Unternehmen steige das Risiko eines Blackouts, eines kompletten Stromausfalls – mit weitreichenden Dominoeffekten. Viele Energieversorger seien weiterhin ungenügend gegen Cyberattacken gewappnet. Es fehlten neben einer funktionierenden Abwehr oft „Cybersecurity-Notfallpläne" und ein strukturiertes IT-Krisenmanagement. Erpresser könnten jede kleine Anlage angreifen und stören. Wenn sich mit der Digitalisierung das intelligente Netz mit zig Millionen Mess-, Steuer- und Kontrollpunkten übers Land verteile, gebe es ebenso viele potenzielle Angriffspunkte. Im Kampf gegen die allgemeine Cyberkriminalität habe die Bundesregierung im November ein Sicherheitspaket beschlossen. Einrichtungen mit kritischer Infrastruktur wie die Energieversorger sollten im Fall eines Angriffs Hilfe von einer schnellen Eingreiftruppe des BSI erhalten.

Evakuierung

Michel Schümperli, Siemens Building Technologies, stellt in der Ausgabe 6-2016 der Zeitschrift Sicherheitsforum, S. 46/47, die

Software Crowd Control vor, die Menschenmengen simulieren könne, die vor Gefahren fliehen. Jetzt sei der Simulationsablauf so weit automatisiert worden, dass er auf Knopfdruck durchläuft. Damit komplexe Gebäude im Katastrophenfall schnell evakuiert sind, müsse die Räumung sehr geordnet verlaufen. Mit der von Siemens Corporate Technology (CT) entwickelten Software könne man Gebäude schon am Rechner darauf prüfen, wo und wann in welchen Fällen kritische Situationen auftreten. Um mit der Software Evakuierungen komplexer Gebäude durchspielen zu können, sei sie in Kooperation mit Siemens Building Technologies entsprechend konfiguriert worden. CT sei derzeit dabei, das virtuelle Nachstellen einer Evakuierung so zu automatisieren, dass ein Anwender sie in Zukunft selbst ausführen kann. Die Software ist auch in der Lage, die Architektur zu optimieren, beispielsweise die Tür- und Treppenbreiten. Bislang sei auch das aufwendige Handarbeit. Um Türbreiten zu bestimmen, die sicherstellen, dass die zulässige Evakuierungszeit nicht überschritten wird, müssten derzeit noch mehrere Simulationen durchgerechnet und anschließend die Ergebnisse verglichen werden. Seit kurzem könne Crowd Control sogar Katastrophenszenarien in die Evakuierungssimulation einbeziehen. Im Rahmen von „Elasstic" sei Crowd Control zusätzlich um ein Plug-in für Gebäudemanagementsysteme erweitert worden. Damit könnten zum Beispiel Funktionalitäten des Brandmeldesystems schon in der Planung simuliert und geprüft werden.

Gebäudesicherheit

Integrierte Systeme für Gebäudesicherheit und Automation behandelt Deister Electronic GmbH in der Zeitschrift GIT, Ausgabe 12-2016, S. 47/48. Die Informationen von Event-Kameras und der Fahrzeugidentifikation könnten beispielsweise relevant sein für die Berechtigungen des digitalen Schließsystems. Und verbinde man Zutrittskontrolle mit dem Schlüsselmanagement, könne der autorisierte Zutritt am Eingang eine Bedingung für das Schlüsselmanagement sein. Auf die gleiche Weise ließen sich auch alle anderen Applikationen von Fuhrparkmanagement, Zutrittskontrolle, Zufahrtskontrolle bis zu den Event-Kameras individuell zu einem Gesamtsystem verbinden.

Gefahrenmeldesystem

Peter Monte, Sitasys, beschreibt im Sicherheitsforum, Ausgabe 6-2016, S. 38/39, **„Analytics"** als das Fitnesscenter für Alarmierungssysteme. Der Beitrag wende sich mit Fragen nach der Ursache bei einem Störungsfall, nach der Verantwortlichkeit für eine Systemstörung und nach der Erkennbarkeit der Störung im Vorfeld an Errichter, Alarmprovider, Leitstellen und Kunden. Er zeigt, wie moderne Systeme die Alarmübertragung sicherstellen und immer fitter werden. Der Autor behandelt Analytics und Inbetriebnahme, Analytics im operativen Betrieb und die Alarmverifikation. Moderne Alarmübertragungssysteme mit Analytics-Funktionen böten viel mehr als eine sichere Alarmübertragung. Sie nutzten die Möglichkeiten der digitalen Welt, um den Anwender bei der Arbeit zu unterstützen, die Übertragung transparent und das Übertragungssystem fitter zu machen. Darüber hinaus stellten sie Informationen zur Verfügung, die für die Prozessoptimierung und neue Services genutzt werden könnten.

Gefahrstoffe

Dr. Ing. Cornel Raicov, ICPV SA Arad, und Dipl.-Ing. Bernd Waschelewski, Swiss TS Technical Services AG, stellen in der Ausgabe 6-2016 der Zeitschrift GIT, S. 40, einen modernen **LPG-Kesselwagen** vor. Die Kon-

struktionsfirma ICPV SA (Forschungs- und Konstruktionsprüfstelle Schienenfahrzeuge Arad) musste im Auftrag des Herstellers Astra Rail Industries (ARI) einen LPG Kesselwagen für den Flüssiggastransport entwerfen und testen. Ziel sei die Entwicklung eines modernen Kesselwagens mit weniger Eigengewicht unter Einhaltung der europäischen Standards und bahntechnischen Zulassung sowie der Interoperabilität im Schienenverkehr (TSI) gewesen. Behandelt werden in dem Beitrag die Zertifizierungsschritte und die Baumusterzulassung gemäß RID und zusätzlich TPED für den Kesselwagentank.

Geldautomatensicherheit

Geldautomaten in Berlin sind unter Gaunern am beliebtesten, titelt die FAZ am 14. Dezember. Von den in diesem Jahr bisher ausspionierten 153 Geldautomaten hätten 108 – oder mehr als zwei Drittel – allein in Berlin gestanden. Damit sei zudem die Zahl der Skimming-Attacken wieder deutlich gestiegen. Die Täter stammten vor allem aus Ländern wie Rumänien oder Bulgarien. Das Auslesen der Daten erfolge längst nicht mehr nur durch externe Aufsätze, sondern auch durch kleine Geräte, die in den Einzugsschacht der Automaten eingeführt würden und damit von außen nicht mehr ersichtlich seien. Inzwischen seien alle gut 100 Mio. Girokarten, die es in Deutschland gibt, zusätzlich zum Magnetstreifen mit einem Chip ausgestattet, der bei jedem Bezahlvorgang und jedem Abheben am Automaten zur Identifikation benötigt wird. Doch noch immer gebe es viele Länder, in denen der leicht zu kopierende Magnetstreifen verwendet wird. Und genau hier versuchten die Gauner ihre Kartenattrappen einzusetzen, so in den USA.

Hotelsicherheit

Die Zeitschrift PROTECTOR beschreibt in Ausgabe 12-2016, S. 14/15 den **Brandschutz in einem „Fünf-Sterne-Hotel".** Das gesamte Hotel sei voll „besprinklert". Insgesamt seien 3.450 Sprinklerköpfe installiert. Davon dienten 843 allein dem Hohlraumschutz. Auch das zweigeschossige Parkhaus unter dem Hotel sei komplett mit Sprinklern versehen. Mehrere Hundert Brandmelder seien im Hotel verbaut, wobei je nach Umgebung unterschiedliche Typen zum Einsatz kämen. Im Saunabereich sei zudem in Absprache mit der Feuerwehr eine Zweimelder-Abhängigkeit implementiert worden, da es bedingt durch den Dampf und die Hitze sonst vermehrt zu Fehlalarmen kommen könne. Um das Risiko von Entstehungsbränden so gering wie möglich zu halten, seien ferner alle Möbel, Einrichtungsgegenstände und Betten schwer entflammbar und schwer brennbar. Die Mitarbeiter erhielten durch eine Fachkraft für Arbeitssicherheit eine umfassende Brandschutzschulung für ihren jeweiligen Arbeitsbereich. Ferner werde einmal im Jahr eine Feuerlöschübung abgehalten. Da das Hotel häufig Gäste aus Top-Unternehmen und Führungsetagen beherbergt, legten diese einen besonderen Wert auf eine umfassende Sicherheit. Dies betreffe nicht nur den Brandschutz, sondern auch Fragen der medizinischen Versorgung, Zufahrtswege, die nächsten Polizeidienststellen und andere sicherheitsrelevante Details. Hier spiele auch die Frage der Zutrittskontrolle der Zimmer und einzelner Bereiche eine große Rolle. Alle Zimmer seien über Schlüsselkarten zu erreichen, die über einen eigenen Rechner im Haus codiert würden. Die Präsidentensuite sei nochmals zusätzlich sicherheitstechnisch aufgerüstet: Neben schusssicherem Glas verfüge sie über einen eigenen Fahrstuhl, eigene Fluchtwege sowie einen eigenen „Panikknopf", mit dem ein direkter Kontakt zu einem Mitarbeiter hergestellt werde.

In derselben Ausgabe wird die **in die Hotel-Infrastruktur integrierte elektronische Zutrittslösung** behandelt (S. 26/27). Der Gast solle online über die Website reservieren, woraufhin das Property Management System (PMS) automatisch eine Buchung erzeuge, ein Zimmer zuweise und einen Check-in-Code generiere, der per E-Mail verschickt wird. Mit diesem Code checke der Gast selbstständig an einem Terminal ein und codiere seine Karte. Insgesamt seien in dem beschriebenen Hotel rund 100 Zutrittspunkte mit der Salto-Lösung ausgestattet. Im Hotelneubau kämen an den 45 Gästezimmertüren die Design-Schlösser Aelement in der funkvernetzten Version zum Einsatz. Für die Übertragung des Funksignals seien 15 Nodes installiert. Im gesamten Objekt habe die Immer AG rund 50 XS4 Original-Beschläge größtenteils ebenfalls in der Wireless-Version verbaut. Außerdem kämen noch drei XS4 Original-Wandleser am Haupteingang und Nebeneingang sowie an der Küche zur Ansteuerung der automatischen Schiebetür zum Einsatz. Im Salto Virtual Network würden die Informationen zu den Schließberechtigungen auf dem Identmedium gespeichert, wodurch eine Verkabelung der elektronischen Beschläge entfalle. Gleichzeitig würden auch Informationen über gesperrte Identmedien auf die Identmedien geschrieben und somit weitergegeben. Die Online-Wandleser übertrügen die ausgelesenen Daten an den zentralen Server und übermittelten gleichzeitig die aktuellen Schließberechtigungen auf die Identmedien.

PROTECTOR enthält in der Ausgabe 12-2016, S. 32/33, eine Marktübersicht über 57 **Hotelschließsysteme** von 28 Anbietern. Abgefragt wurden u. a. die Kriterien Preis, Art des Einsteckschlosses, Systemeigenschaften und Systemart, Offlinefähigkeit, Programmierung, optische und akustische Signale sowie Stromversorgung am Beschlag, Verkabelung, aktiver oder passiver Transponder sowie Lesedistanz und Protokollierung im Schloss.

IT-Sicherheit

Der ASW-Newsletter vom 9. Dezember weist auf einen Bericht in silicon.de hin, nach dem das testweise verfügbare **WLAN-Angebot in Wagen der zweiten Klasse in ICE-Zügen** offenbar nicht ohne weiteres sicher nutzbar ist. Im Augenblick könne ohne Eingabe eines Passworts darauf zugegriffen werden. „Andere Passagiere im Zug, die auch mit der kostenlosen WLAN-Testversion der Deutschen Bahn verbunden sind, könnten Sie mit Hilfe von leicht zugänglichen, kostenlosen Tools ausspionieren", habe Filip Chytry, Sicherheitsexperte bei Avast, erklärt. Er empfehle die Nutzung eines VPN-Tools, um Spionageversuche abzuwehren.

Das Institut für Offene Kommunikationssysteme benennt in der Dezember-Ausgabe des Behörden-Spiegel zehn **Trends für das Jahr 2017**: Blockchain (Das Register in der Blockchain ist robust gegen Manipulation und schafft durch Anreize ein System des sicheren Austausches zwischen Fremden.), algorithmisches Verwalten, vorhersagende Polizeiarbeit, Digitalisierung der Arbeit, denkende Maschinen, SG-Mobilfunk, Microservices (Flexible, skalierbare Microservices reagieren auf einzelne, in sich abgeschlossene Geschäftsaktivitäten, die zu einem Gesamtsystem kombiniert werden.), Internet der Dinge, Indoor-Navigation (die Menschen und Maschinen als Orientierungshilfe dienen kann) und Holokratie (Organisationsmodell, das hierarchische Steuerung durch fachlich bestimmte Entscheidungskreise ersetzt).

Der Behörden-Spiegel berichtet in der Dezember-Ausgabe über den **Kongress „Magenta Security"** der Deutschen Telekom, auf dem Produkte der am 1. April neu gegründeten Firma „Telekom Security", die von Dirk Backofen geleitet wird, vorgestellt worden seien. CEO Höttges habe im Zusammenhang mit der Attacke auf die Router der Telekom mit 900.000 betroffenen Kunden

gefordert, Cyberangriffe weltweit zu ächten. Tobias Schrödel habe darauf hingewiesen, dass auch die Hardware von Computern oftmals für gezielte Cyberangriffe genutzt werde. Hier seien vor allem USB-Sticks zu nennen. Verseuchte Sticks suggerierten einem Computer, dass sie eine Tastatur seien und könnten auf diese Weise Malware aufspielen. Manche Unternehmen würden auf diese unterschätzte Gefahr reagieren, indem sie die Ports aller Computer für Wechseldatenträger sperren.

Christoph Stoica bezeichnet in silicon.de am 15. Dezember **Mitdenken als die beste Verteidigung** von Daten vor Cyberangriffen. Social Media, mobiles Internet, BYOD, Cloud Computing und die „Always on"-Mentalität sorgten für eine wachsende technologische Durchdringung und Vernetzung der Unternehmen. Die IT-Landschaft werde komplexer. Mittlerweise gebe es keine Grenze mehr zwischen „innerhalb" und „außerhalb" des Netzwerkes – das Netzwerk sei heute überall und mit ihm auch der Feind. Da der klassische IT-Schutz an den Außengrenzen zunehmend erodiere, müssten Unternehmen ihre IT-Sicherheitsstrategie überdenken und den aktuellen Herausforderungen entsprechend anpassen. Die Technik dafür existiere bereits: Insbesondere ein risikobasiertes Zugriffsmanagement sollte die Grundlage eines jeden Sicherheitskonzeptes bilden. Implementiert werde die Zugriffssteuerung mit Multifaktor-Authentifizierung. Außerdem müssten Unternehmen einen Überblick über alle Berechtigungen behalten. Sie sollten auf Basis von Attributen, IT- und Geschäftsrollen sowie Richtlinien definiert und vergeben werden. Nur durch intelligente Verwaltungslösungen könnten sich Unternehmen an sich verändernde Anforderungen anpassen und je nach Situation in Echtzeit reagieren.

IuK-Kriminalität

Nach den massenhaften **Ausfällen von Internetanschlüssen der Deutschen Telekom** habe die Fahndung nach den Angreifern begonnen, schreibt die FAZ am 30. November. Das BSI vermute die Täter in den Reihen der OK. In Deutschland habe die Attacke vorübergehend 900.000 Anschlüsse lahmgelegt. Mit immer neuen Regelungen und Zertifizierungen werde man dem Problem nicht Herr, so Falk Garbsch vom Chaos Computer Club. Nach bisherigem Stand der Erkenntnisse hätten die Angreifer ein bereits bekanntes „Botnetz" benutzt, das unter dem Namen „Mirai" läuft. Der Angriff ziele auf mit dem Internet verbundene Geräte, die den Fernwartungsport 7547n geöffnet haben. „Glück im Unglück": Durch die massenhaften Anfragen sei es zu einem Absturz, nicht zu einer Übernahme gekommen. Sonst wäre das Botnetz mit 900.000 Routern und der dahinterliegende Internetverbund eine sehr mächtige Waffe für DDoS-Attacken geworden. Experten rechneten damit, dass DDoS-Attacken künftig stark zunehmen werden.

Der Fall Telekom lenke die Aufmerksamkeit auf die **Medizin- und Patientendaten**, heißt es in der FAZ am 1. Dezember. In der Diskussion um IT-Sicherheit und die Gefahr von Cyberkriminellen in Deutschland rücke die kritische Infrastruktur in den Fokus. Gerade im Gesundheitswesen sähen Fachleute große Risiken. Viele Krankenhäuser und medizinische Zentren schützten Patientendaten ungenügend gegen kriminelle Hackerattacken. Die IT-Sicherheit in Kliniken sei katastrophal, so Falk Garbsch vom Chaos Computer Club. Es gebe in Krankenhäusern besonders viele Möglichkeiten, Dokumente und Daten zu stehlen, Geräte zu manipulieren und einen ganzen Betrieb lahmzulegen. Wenn wichtige Geräte im Krankenhaus manipuliert würden, könne das für Patienten lebensbedrohend sein. Es gebe eine neue Angst: Prominente gingen immer öfter unter einem Pseudonym

in eine Klinik, weil sie befürchteten, dass Hacker ihre Patientendaten entwenden, um Geld zu erpressen. Drei Krankenhäuser in Hannover hätten für zwei Tage nicht operieren können. Das Gesundheitsministerium in NRW habe in den ersten zwei Monaten 2016 28 Cyberangriffe auf Kliniken gezählt.

Internationale Ermittler sprengten das **Botnetz „Avalanche"** nach vier Jahren Arbeit, schreibt die FAZ am 2. Dezember. Ermittler aus 39 Ländern seien beteiligt gewesen. Wie groß das Kriminellen-Netzwerk wirklich ist, lasse sich noch nicht exakt sagen. Erste Erkenntnisse zeigten, dass mehr als 50.000 PCs betroffen sind. In zehn Ländern habe es gleichzeitig Durchsuchungen, Festnahmen und Beschlagnahmungen von Servern und Domains gegeben. Die Tatverdächtigen sollen aus verschiedenen Ländern kommen. Auf Basis der vorliegenden Anzeigen werde die Schadensumme derzeit auf rund sechs Mio. Euro aus 1.336 Taten beziffert. Zuletzt habe der Schwerpunkt der Kriminellen darin gelegen, Online-Banking-Kunden zu schädigen. Sieben Tatverdächtige, gegen die Haftbefehl erlassen worden sei, gehörten zu einem international agierenden Ring von Betrügern, die seit mindestens 2009 „Avalanche" für Phishing, für den Versand von Massenspam-Werbemails und für Bankbetrug nutzten. Die meisten infizierten Rechner hätten in Russland und den USA gestanden. Am drittstärksten sei Deutschland betroffen. Die Schadprogramme könnten nicht direkt von den infizierten Rechnern gelöscht werden. Betroffene Nutzer würden von ihren Internet-Anbietern informiert.

Das BKA verzeichne im Schnitt 5.000 Fälle im Jahr, bei denen Bankräuber durch das Abfischen von Zugangsdaten Konten leerräumen, meldet die FAZ am 7. Dezember. Angesichts vieler Millionen Bankkonten in Deutschland sei das Risiko für den Einzelnen also gering. Ein vergleichbarer Fall wie jener der englischen Tesco Bank, bei der Hacker von insgesamt 20.000 Online-Konten Geld abbuchten, sei in Deutschland noch nicht bekannt. Wenn die Bank dem Kunden einen TAN-Generator zur Verfügung gestellt hat und trotzdem etwas passiert, zieht der Kunde vor Gericht inzwischen öfter den Kürzeren. Denn diese Methode hätten viele Gutachten bereits als unknackbar für Hacker beurteilt. Wer ein halbwegs modernes Handy hat, spare sich schon heute gerne die Eingabe eines Passworts und logge sich einfach mit dem Daumendruck auf den Powerknopf ein. Das nutzten nun auch Banken. Die Digitalisierung des Bankwesens habe einen **Wandel in der Finanzkriminalität** hervorgerufen. Das liege daran, dass die Banken ein attraktives Ziel für Cyberangriffe seien. Weil das Risikobewusstsein noch immer mangelhaft sei, würden 60 Prozent der Cyberattacken nicht von der Bank, sondern von Kunden oder Aufsehern bemerkt. Ein Fachausschuss der BIZ habe eine Spezialeinheit gegründet, um die großen Zahlungssysteme zu überprüfen. Zudem habe die BIZ zusammen mit der Vereinigung der internationalen Wertpapieraufsichtsbehörde Iosco einen Leitfaden entwickelt, wie sich Banken und andere Finanzinstitute besser gegen Cyberrisiken wappnen könnten.

Nach einer Meldung der FAZ vom 9. Dezember hat **Thyssen-Krupp** berichtet, Ziel einer Cyberattacke geworden zu sein. Die Angreifer hätten es auf den Diebstahl von Know-how und Forschungsergebnissen abgesehen. Die Industriespionage richte sich gegen die Sparte Industrial Solutions, in der Thyssen-Krupp den Bau von industriellen Großanlagen, zum Beispiel Dünger- und Zementfabriken sowie sein Werftengeschäft mit Schiffen und U-Booten gebündelt habe. Daneben seien die Cyberagenten in die Informationstechnik des Walzwerks Hohenlimburg eingedrungen, das in erster Linie für die Autozulieferindustrie produziere, sowie in Standorte in Indien, den USA und Argentinien. Nach bisherigem Ermittlungsstand stünden Angreifer aus Südostasien hinter der Cyberattacke. Über die in den Rechnern versteckte Schadsoftware sei es ihnen gelungen, Daten abzusaugen.

Gescheitert seien die Angreifer an den Sicherheitssystemen der Marinesparte. Auch in die ebenfalls speziell abgesicherten Steuerungssysteme und Netzwerke von Hochöfen und Kraftwerken seien die Angreifer nicht hereingekommen. Entdeckt worden sei der Angriff von der IT-Sicherheitszentrale des Konzerns, die sofort das BSI informiert habe. Man sei den Tätern etwa zwei Monate nach der Installation der Software auf die Schliche gekommen. Die Konzernsicherheit habe inzwischen ein besonders intensives Monitoring-System aufgesetzt, das bei Cyberangriffen dieser Art Alarm schlagen soll.

Online-Einkauf zieht Hacker an, titelt die FAZ am 10. Dezember. Der E-Commerce sei eine der Branchen, die die Gefahr aus dem Netz heftig umtreibe. Beim Bundesverband Onlinehandel (BVOH) nähmen die Anfragen der Mitgliedsunternehmen deutlich zu. Dass die Onlinehändler aufgeschreckt sind, zeige auch der steigende Bedarf an Cyberpolicen. Vor allem die sogenannten Ransomware-Attacken hätten in den vergangenen Monaten stark zugenommen. Insgesamt scheine das Risikobewusstsein im Onlinehandel stark zugenommen zu haben, wie Industrieversicherer übereinstimmend berichteten.

Der Newsletter des ASW vom 9. Dezember weist auf eine Meldung von heise.de hin, nach der die Drahtzieher hinter dem **Erpressungstrojaner Goldeneye** gezielt Personalverantwortliche anschreiben und sich detailliert auf offene Stellenausschreibungen beziehen, um die „Personaler" dazu zu bringen, den Trojaner auszuführen. Die Kriminellen bedienten sich dabei bei Daten, die vermutlich von der Bundesagentur für Arbeit stammen.

Krankenhaussicherheit

PROTECTOR stellt in der Ausgabe 12-2016 eine **maßgeschneiderte Zutrittsorganisation** für eine Klinik vor (S. 18/19). Das Zutrittsorganisationssystem sei sowohl mit der Zeiterfassung als auch mit dem Kantinenabrechnungssystem der Klinik kompatibel. Es könne darüber hinaus auch in die Haustechnik integriert werden. Vor allem aber überzeuge die schnelle und kabellose Befehlsverbreitung in einem virtuellen Netz. Damit verknüpfe Bluesmart die Vorteile von Offline-Lösungen mit dem Nutzen eines Online-Systems. Informationen zwischen den elektronischen Zylindern würden im täglichen Gebrauch über den batterielos arbeitenden Schlüssel übertragen. Der aus Hochleistungskunststoff gefertigte Bluesmart-Schlüssel sei wasserdicht (IP 68), stabil, wartungsfrei und unempfindlich gegen Desinfektionsmittel.

Kritische Infrastrukturen

Dr. Berthold Stoppelkamp, BDSW, befasst sich in DSD, Ausgabe 4-2016, S. 22/23 mit der **Bargeldversorgung** als Dienstleistung in der kritischen Infrastrukturbranche Finanzen. Eine funktionierende Logistikinfrastruktur, die nicht im Einflussbereich der Bundesbank liegt und die Kreditinstitute sowie die Wertdienstleister einschließt, sei für eine geordnete Bargeldversorgung der Bevölkerung unbedingt erforderlich. Seit Juli 2016 habe unter Federführung des BMI unter Beteiligung von Ministerien, Behörden, Branchenverbänden und Unternehmen die Erarbeitung der BSI-Kritisverordnung, Teil 2, unter anderem auch für die Dienstleistung Bargeldversorgung begonnen. Sobald die VO in Kraft getreten ist, hätten betroffene Unternehmen zwei Jahre Zeit, die für die Erbringung ihrer wichtigen Dienste erforderliche IT nach dem Stand der Technik angemessen abzusichern und – sofern nicht andere Spezialregelungen bestehen – diese Sicherheit mindestens alle zwei Jahre überprüfen zu lassen.

Maschinensicherheit

GIT stellt in der Ausgabe 12-2016, S. 84–86, ein **Design Tool für funktionale Sicherheit** vor. Das von ABB entwickelte Sicherheitstool FSDT-01 erleichtere durch eine übersichtliche grafische Oberfläche Konstrukteuren die Arbeit und berechne den erforderlichen, geplanten und erreichten Safety Integrity Level (SIL) bzw. den Performance Level (PO). Es unterstütze sie bei der Festlegung, Prüfung und Dokumentation mit einer sehr logischen und schrittweisen Vorgehensweise. Die Bewertung der Sicherheitsfunktion erfolge in vier Schritten: ISO- oder IEC-Projekt auswählen; Sicherheitslevel definieren; Sicherheitsfunktionen planen; Bericht erstellen.

Martina Schili, Leuze electronic GmbH, erklärt in der Ausgabe 12-2016 der Zeitschrift GIT, S. 87/88, was die Firma unter „**Smart Process Gating"** versteht. Auf Basis der Type 4 Sicherheitslichtvorhänge der Baureihe MLC 500 habe Leuze electronic das Smart-Process-Gating-Verfahren (SPG) entwickelt. Dadurch könne auf die Muting-Sensoren ganz verzichtet werden. Beim SPG komme das erste Gating-Signal von der Anlagensteuerung (SPS), während das zweite bei der Unterbrechung des Schutzfeldes vom Sicherheitslichtvorhang selbst erzeugt werde. Zusammen mit einer Standardsteuerung werde Performance Level PLd erreicht, zusammen mit einer Sicherheitssteuerung ergebe sich Performance Level PLe. Um die Schutzeinrichtung während der Durchfahrt von Transportgütern zu unterbrechen, werde beim Smart Process Gating kurz vor der Einfahrt in das Schutzfeld ein Signal von der SPS an den Sicherheitslichtvorhang gesandt. Der Zeitpunkt müsse so eingestellt sein, dass sich das Transportgut näher als 200 mm vor dem Schutzfeld befindet, um das Durchschlüpfen von Personen auszuschließen. Es würden mindestens zwei unabhängige Steuersignale zur Aktivierung der Überbrückungsfunktion benötigt, ein Schaltsignal von der Prozesssteuerung und eine vom Transportgut erzeugte Unterbrechung des Schutzfelds.

Thomas Kramer-Wolf, Wieland Electric GmbH, behandelt in der Ausgabe 12-2016, S. 89/90 der Zeitschrift GIT **Schulungen für die Sicherheit von Mensch und Maschine**. Wieland Electronic biete neben Produkten und Dienstleistungen auch ein umfangreiches Schulungsprogramm rund um die Maschinensicherheit an. Erfahrene Praktiker sowie Normen- und Safety-Experten vermittelten in praxisnahen Schulungen aktuelles Fachwissen für Management, Entwickler, Service, Instandhaltung und Betreiber von Maschinen. Die Inhalte reichten dabei von EU-Richtlinien, Gesetzen und Normen bis hin zur Nutzung und Anwendung von Softwaretools. Unternehmen erhielten somit nicht nur wichtige Kenntnisse über die Maschinensicherheit, sondern auch mehr Rechtssicherheit.

Museumssicherheit

Die Zeitschrift GIT befasst sich in der Ausgabe 12-2016, S. 42/43, mit **Videoüberwachung im Museum**. Zu einer Überwachung rund um die Uhr habe die Sicherheitsfirma Abus HD Kamera-Domes mit Nachtsichtfunktion empfohlen. Durch ihre Ultra Low-Light-Funktion eigneten sie sich hervorragend für den Einsatz in den tagsüber abgedunkelten Museumsräumen und ermöglichten auch nachts ein detailreiches und farbgetreues Kamerabild. Unterstützt würden die Kameras zudem durch kleine Infrarotscheinwerfer.

Naturgefahren

Anfang Oktober habe der GDV den **Naturgefahrenreport 2015** vorgestellt, berichtet s+s report in der Ausgabe 4-2016, S. 6. Die versicherten Schäden seien 2015 gestiegen:

Die Sachversicherer hätten rund 1,9 Mrd. Euro geschultert, die Kfz-Versicherer etwa 700 Mio. Euro. Die gesamte Schadenbilanz von knapp 2,6 Mrd. Euro im Jahr 2015, dem zweitwärmsten seit Beginn der Wetteraufzeichnungen, sei fast ausschließlich von Sturm- und Hagelschäden geprägt. Nur ein einziger Sturm habe ein Drittel aller Schäden verursacht.

NSL-Alarmvorprüfung

Dipl.-Wirtschaftsjurist (FH) Sebastian Brose, VdS, erläutert in s+s report, Ausgabe 4-2016, S. 38/39, ein Verfahren zur **visuellen Alarmvorprüfung aus der NSL**, das eine umgehende Alarmierung der Polizei ermöglicht. Auf Grundlage der VdS-anerkannten EMA und VÜA könne eine Alarmverifikation nach VdS 3415 vereinbart werden. Voraussetzungen dafür seien unter anderem die Verwendung geeigneter Anlagenteile, die Einbindung aller dieser Teile in ein integrales Sicherungskonzept, die Leistungserbringung durch ein kompetentes Errichterunternehmen und die Zusammenarbeit mit einer kompetenten Notruf- und Serviceleitstelle und Interventionsstelle. Liege der NSL im Alarmfall ein qualifiziertes Bild vor, das eine eindeutige Gefahrenlage zeige, dürfe unverzüglich die Polizei alarmiert werden. Eine Alarmvorprüfung vor Ort sei in diesem Fall entbehrlich. Die Richtlinien VdS 3415 regelten die Details.

Öffentlicher Raum

In Zusammenarbeit mit dem Meinungsforschungsinstitut YouGov habe Seetec eine repräsentative Umfrage zum Thema „Öffentliche Sicherheit" durchgeführt, meldet GIT in der Ausgabe 12-2016, S. 8. 68 Prozent der Deutschen sind danach der Auffassung, die Sicherheitslage im öffentlichen Raum habe sich in den letzten Jahren verschlechtert. 74 Prozent forderten den Einsatz von mehr Videotechnik im öffentlichen Raum.

Ordnungsdienst in Stadien

Georg Spangardt, Berufsfeuerwehr Köln, befasst sich in s+s report, Ausgabe 4-2016, S. 50–53, mit der **Qualifizierung und Weiterbildung von Ordnungsdienstkräften**. Sie müssten für den Dienst in großen Versammlungsstätten ausgebildet werden. Dafür gebe es eine Grundausbildung, ergänzt durch eine Kurzeinweisung am Veranstaltungstag und regelmäßige Fortbildungen. Als Beispiel beschreibt der Autor eine solche Fortbildung im Kölner RheinEnergieSTADION. Rund 180 Ordnungsdienstkräfte gelte es zu schulen. Angesichts der großen Teilnehmerzahl habe man sich für eine Stationsausbildung in sechs Gruppen mit je 30 Personen entschieden. Die Zeitvorgabe für jede Station habe 30 Minuten betragen. Hinzu seien Zeiten für den Stationswechsel gekommen. Die Themen: rechtliche Grundlagen für den Ordnungsdienst und Schulungsvorgaben des DFB, Neuigkeiten und Abläufe bei der Einlasskontrolle sowie Ticketingfragen, Stadionbegehung unter Brandschutz- und Evakuierungsaspekten, Rechte und Pflichten des Ordnungsdienstes insbesondere gegenüber Fangruppen und allgemeine Brandschutzbelehrung zeigten das breite Aufgabenspektrum für die Ordnungsdienstkräfte. Da die Ordnungsdienstkräfte eine Gruppe innerhalb der verschiedenen Akteure einer Veranstaltung darstellen, müssten die Schulungsveranstaltungen regelmäßig auf das verzahnte System von Teilverantwortlichen in einer Versammlungsstätte eingehen.

Outsourcing

Stephan Leukert, Von zur Mühlen'sche GmbH, beklagt in der Ausgabe 12-2016 der

Zeitschrift PROTECTOR, S. 72/73, dass die große Masse der **Aufträge an Sicherheitsdienstleister nach wie vor rein** über den Preis vergeben werde. Bei Ausschreibungen lägen zwischen dem günstigsten und dem teuersten Angebot immer wieder 30 Prozent und mehr. An die Untergrenze dieser Spanne komme man eigentlich nur, wenn man am Material, der Aus- und Weiterbildung oder am Qualitätsmanagement spart. Oder an der Entlohnung der Mitarbeiter. Die Konsequenz lasse sich schön mit einem englischen Sprichwort beschreiben: „If you pay peanuts, you get monkeys". Würden in der Ausschreibung keine klaren Vorgaben hinsichtlich des erwarteten Verhaltens gemacht beziehungsweise keine Lösungskonzepte zu bestimmten Themen gefordert, seien Verstöße gegen das Compliance-System vorprogrammiert. Mit den im Rahmen von Ausschreibungen den Bietern vorgeschriebenen vielen Details lasse sich die potenzielle Qualität kaum ermitteln. Dabei müsste der Auftraggeber einfach nur nach Lösungskonzepten fragen und diese bewerten, zum Beispiel nach der Methodik der Personalgewinnung und -auswahl für den Auftrag, dem Einweisungs- sowie Aus- und Weiterbildungskonzept oder dem Konzept zur Sicherstellung der Dienstleistungsqualität.

Perimetersicherheit

Sabotagesicherheit der Lebensmittelindustrie behandelt Willy Derichs, Novatec Sicherheit & Logistik GmbH, in der Ausgabe 12-2016 der Zeitschrift PROTECTOR, S. 42/43. Der wirkungsvolle Schutz der Lebensmittelproduktion beginne bereits bei der Perimetersicherung, die sich mit zeitgemäßer Technik durchaus auch preiswert und effizient nachrüsten lasse. Statt mit aufwendiger Verkabelung könnten intelligente Systeme heute längere Zaunstrecken mit Beschleunigungssensoren auf RFID-Basis überwachen. Sie stünden drahtlos miteinander in Verbindung. Eine intelligente Auswertungs-Software analysiere die gewonnenen Daten und erkenne, ob der Zaun nur durch einen Windstoß bewegt wurde oder ob ein Übersteig- oder Durchschneideversuch vorliege. Durch die Kombination von effektiver Videoüberwachung mit drahtlosen und drahtgebundenen Sicherungssystemen könnten Sabotageversuche meist schnell erkannt und verhindert werden.

Persönliche Schutzausrüstung

Reinhilde Burg, Claudia Horn und Silke Stephan, HB Schutzbekleidung, erläutern in GIT, Ausgabe 12-2016, S. 80–82, die **neue europäische PSA-Verordnung**. Sie sei seit 20. April 2016 in Kraft (EU 2016/425). Sie ersetze die PSA-Richtlinie 89/686/EWG und nehme zukünftig alle Wirtschaftsakteure in die Verantwortung – und die Hersteller mehr als bisher. Die Neuerungen für Hersteller und Verbesserungen für die Kunden betrügen im Wesentlichen Kennzeichnung, Dokumentation und Rückverfolgbarkeit der Ware. Auch Händler und Importeure würden ab sofort als Hersteller eingestuft, wenn sie im Ausland hergestellte PSA unter ihrem Namen oder ihrer Marke in den Verkehr bringen oder wenn sie Veränderungen am Produkt vornehmen, die die Normkonformität beeinträchtigen könnten. Die Hersteller seien verpflichtet, ihren Kunden in den sogenannten „Gebrauchsanleitungen" alle notwendigen Informationen über Benutzung, Lagerung, Reinigung, Instandhaltung, Wartung und Desinfektion der PSA mitzugeben. Der Einsatzzweck der Bekleidung müsse angegeben werden. Darüber hinaus sei künftig die Angabe von Monat und Jahr über eine erkennbare Alterung gefordert, sofern diese bekannt oder absehbar sei. Die Hersteller seien künftig verpflichtet, die sogenannte Konformitätserklärung von allen im Verkehr befindlichen Produkten dem Produkt beizufügen oder sie alternativ im Internet bereitzustellen und den

Internet-Link am Produkt anzubringen. Mit der neuen EU PSA-Verordnung müssten die Hersteller ihrem Produkt dauerhaft eine Information beifügen, die die Rückverfolgbarkeit der Produktion gewährleiste.

Personenschutz

Der neue Mercedes-Maybach S 600 Guard bietet den aktuell höchsten vom Beschussamt Ulm zertifizierten **Schutz für Serienlimousinen**. Damit erfülle erstmals ein Modell in diesem Segment die Anforderungen der höchsten Schutzklasse VR10 für Zivilfahrzeuge nach der Richtlinie BRV 2009 Fassung 2, so PROTECTOR in der Ausgabe 12-2016, S. 70/71. Das Fahrzeug biete Schutz gegen Hartkernmunition. Neben der Schutzklasse VR10 komme auch die neuartige Bodenpanzerung, die erstmals den Unterboden fast vollständig abdeckt und eine Resistenz gegen die zweifache Ansprengung mit der Handgranate HG85 nach ERV 2010 (Explosive Resistant Vehicle) – ebenso wie die Dachpanzerung – biete, zum Einsatz. Viele Achskomponenten seien beim Mercedes-Maybach Guard verstärkt, aus hochbelastbarem Stahl hergestellt und mit einer eigens neu entwickelten Bremse ausgestattet. Zusätzlich würden die Fahrzeuge mit verstärkten Stabilisatoren versehen. Auch die Regelsysteme, wie beispielsweise das ESP oder das ABS, seien an das Mehrgewicht adaptiert. An besonders kritischen Stellen wie etwa Fugen und Materialübergängen sorgten intelligente Überlappungssysteme für den umfassenden ballistischen Schutz.

Reisesicherheit

Mit **Travel Risk Management** befasst sich Joachim Leis, Mentalleis Dienstleistungen GmbH, in der Ausgabe 12-2016 der Zeitschrift PROTECTOR, S. 74. Ein im Unternehmen implementiertes Reisesicherheits-Management gehöre zum sicheren Reisen. Dieses Management wird vom Autor beschrieben. Als wichtige Reisetipps werden aufgelistet: wichtige Rufnummern im Handy abspeichern und zusätzlich ausdrucken; wichtige Daten online hinterlegen; einen ausreichenden Medikamentenvorrat anlegen; vorab klären, welche Medikamente nicht ins Reiseland mitgenommen werden dürfen; Allergien und Unverträglichkeitsreaktionen auf einem Zettel mehrsprachig notieren; Impfbedarf klären und durchführen; Daten gegen Entwendung, Kopieren oder Einsichtnahme sichern.

Schlüsselmanagement

Ein **integriertes Schlüsselmanagement** als Bestandteil umfassender Sicherheit stellt in der Ausgabe 12-2016 der Zeitschrift PROTECTOR, S. 29, Fernando Pires, Mors Watchmans Ltd., vor. Der parallele Einsatz verschiedenster Systeme, etwa für Zutrittskontrolle, Schlüsselverwaltung, Personaleinsatz oder Lohnbuchhaltung, stelle eine potenzielle Hürde beim Herstellen der Sicherheit dar. Hersteller müssten deshalb offene Komponenten anbieten, die sich leicht integrieren lassen. Die erfassten Daten ließen sich individuell gestalten und nutzen, um herauszufinden, wo sich welche Schlüssel gerade befinden und wann sie zurückgegeben werden. So könne sofort gemeldet werden, wenn eine Person mit einem Schlüssel das Gebäude verlässt, den sie längst hätte abgeben müssen. Oder aber ein besonders wichtiger Schlüssel wird von einer anderen Person als der ursprünglich berechtigten abgegeben.

Sicherheitsgewerbe

Vor gefährlichen **Sublimits in Bewachungspolicen** warnt Rechtsanwalt Matthias W. Kroll in DSD, Ausgabe 4-2016, S. 48/49. Es sei üblich, für Sachschäden Versicherungssummen ab zwei Mio. Euro in den Policen der Berufshaftpflichtversicherungen der Bewachungsunternehmen zu vereinbaren. Spätestens dann, wenn der Versicherer im Schadensfall darauf hinweist, dass „im dritten Nachtrag auf Seite vier der Nachtragspolice" ein Sublimit von 250.000 Euro je Schadensfall bei Sachschäden vereinbart sei, werde sich der Bewachungsunternehmer mit diesem Begriff beschäftigen. Im Bereich des Versicherungswesens stelle das Sublimit eine Obergrenze der Deckungssumme dar, die vom Versicherungsvertrag abweicht. Dabei beziehe sich das Sublimit nicht auf den gesamten Versicherungsvertrag, sondern nur auf ein bestimmtes Element bzw. einen Teil. Sublimits würden zwischen dem Versicherer und dem Versicherungsnehmer individuell vereinbart. Soweit das Sublimit erst in einem Nachtrag „untergeschoben" wurde, stelle sich die Frage, ob der Versicherer ordnungsgemäß darauf hingewiesen hat, dass Nachträge zum Versicherungsvertrag nach § 5 VVG mangels Widerspruchs gegen diese Änderung mit Ablauf eines Monats als genehmigt gelten. In aller Regel dürfte es dem Nachtrag schon an einem „bestätigenden" Charakter fehlen. Auch später ausgestellte Versicherungsbestätigungen, in denen das Sublimit erwähnt werde, seien keine Bestätigungsschreiben. Wenn auch kein ordnungsgemäßer Hinweis nach § 5 VVG erfolgte, seien Sublimits in Nachträgen nicht in den Versicherungsvertrag ordnungsgemäß einbezogen.

Sicherheitsgewerberecht

Mit den am 1. Dezember 2016 (BGBl. I S. 2692) in Kraft getretenen Änderungen im **Sicherheitsgewerberecht** befasst sich Dr. Berthold Stoppelkamp, BDSW, in DSD, Ausgabe 4-2016, S. 52–54. Er listet die teils ab Dezember 2016, teils ab Januar 2019 geltenden Neuregelungen auf und nimmt kritisch Stellung. Vor dem Hintergrund der seit Jahren in der Sicherheitswirtschaft eingeführten IHK Ausbildungsberufe wäre es zukunftsweisend gewesen, diese grundsätzlich als Zugangsvoraussetzung für ein unternehmerisches Tätigwerden im Sicherheitsgewerbe zu machen. Völlig ausgeklammert worden seien Qualifizierungs- und Weiterbildungsanforderungen beim Schutz kritischer Infrastrukturen, Großveranstaltungen und des öffentlichen Personenverkehrs. Der BDSW begrüße die Einrichtung eines zentralen Bewachungsregisters, da es hierdurch ermöglicht werde, schneller gefälschten IHK-Bescheinigungen oder Mitarbeitern ohne Zuverlässigkeitsüberprüfung auf die Spur zu kommen und Extremisten von der Branche fernzuhalten. Mit der Einführung der Regelabfrage beim Verfassungsschutz werde die Sicherheitsbranche erstmalig zur „ meist überprüften" Branche. Der Gesetzgeber rücke damit unter Sicherheitsgesichtspunkten die Sicherheitsbranche mittelfristig in eine neue höherwertige Sonderrolle innerhalb der Sicherheitsarchitektur. Hierdurch werde es für die Sicherheitswirtschaft in der Zukunft leichter möglich sein, im Bereich der Gefahrenabwehr enger mit der Polizei zu kooperieren und im Wege der Beleihung auch weitere hoheitliche Aufgaben wahrzunehmen.

Sicherheitstechnik

Mit **RFID-Chips** befasst sich die FAZ am 12.Dezember. Mit ihrer Hilfe ließen sich Objekte und Menschen identifizieren und exakt lokalisieren. Ein RFID-Transponder sei ein Funk-Kommunikationsprodukt. Es nehme eingehende Signale auf, leite sie weiter oder beantworte sie. Bestehend aus einem Chip und einer damit verbundenen Antenne dienten sie der

sicheren, berührungslosen Übertragung von Informationen über Funkwellen. Marktforscher von ID-Techex Research gingen davon aus, dass das Volumen von RFID-Technik im Jahr 2020 für den Gesamtmarkt auf 13,2 Mrd. Dollar ansteigt. Im Jahr 2015 seien es noch 10,1 Mrd. Dollar gewesen. Die Technik setze sich langsamer durch als erwartet. Lange Zeit sei der Barcode das Maß der Dinge gewesen, wenn es für Unternehmen darum ging, den Weg von Waren oder Bauteilen im Detail nachzuvollziehen. Doch der Barcode habe einen entscheidenden Nachteil: Er müsse stets in Richtung Scanner zeigen, damit er richtig gelesen werden kann. Das Thema Industrie 4.0 werde die RFID- Branche sicherlich zusätzlich beflügeln.

Smart City

Smart Cities sind das Thema von Dr. Ing. ETH, Exec. MBA Rolf H. Sigg, ASIS International, in Ausgabe 6-2016 des Sicherheitsforums, S. 24–27. Es gebe noch keine einheitliche Definition. Zentrale Attribute für eine hohe Attraktivität seien bestimmt eine hohe Lebensqualität mit Umweltverträglichkeit und sozialer Inklusion sowie eine hohe Effizienz aller Abläufe und Dienstleistungen. Neben einer punktuellen Betrachtung dieser Attribute benötige eine „smart city" die Fähigkeit, jederzeit erfolgreich zu funktionieren. Die Projekte müssten mit Methodik geplant und realisiert werden. Der Autor behandelt die holistische Planung, eine systematische Integration und die Erfolgsmessung. Sicherheit und Resilienz seien starke Wettbewerbsfaktoren.

Terrorismus

Wie unter anderen die FAZ am 21. Dezember meldet, war am 19. Dezember gegen 20 Uhr ein Sattelschlepper mit hoher Geschwindigkeit über den Weihnachtsmarkt an der Berliner Gedächtniskirche gefahren und nach etwa 80 Metern am Rand der Budapester Straße zum Stehen gekommen. Mindestens 12 Personen seien getötet und 48 verletzt worden. Der Fahrer sei nach der Tat geflüchtet. Den Lkw mit polnischem Kennzeichen habe er zuvor mutmaßlich gestohlen und den polnischen Fahrer erschossen. Die Zeitung verweist auf die jüngste Ausgabe des IS-Propagandamagazins „Rumiyah", in dem eine detaillierte Anleitung für derartige Anschläge zu finden sei. Immer wieder werde betont, dass es das größte Ziel sei, so viele unschuldige Menschen wie nur möglich zu töten. Nur wenige würden bis heute die tödliche und zerstörerische Wirkung von Transportfahrzeugen verstehen. Der Attentäter von Nizza habe das „großartig demonstriert"; mit Hilfe eines Lastwagens „abzuschlachten"; „Fahrzeuge sind wie Messer"; „Sie sind leicht zu bekommen". Das richtige Fahrzeug gelte den Autoren als Hauptvoraussetzung für den Erfolg eines Anschlags. Einige Kriterien würden dafür angeführt. Von kleineren Autos werde abgeraten. Lastwagen nenne der Text grundsätzlich als ideales Fahrzeug für einen Anschlag.

Manfred Buhl, Securitas Deutschland GmbH, erläutert in der Ausgabe 12-2016 von PROTECTOR, S. 66–68, in welcher Weise die **Sicherheitswirtschaft** einen **Beitrag zur Terrorismusbekämpfung** leisten kann. Sie entwickle, produziere und betreibe Sicherheitstechnik, ohne die die Abwehr und die Detektion terroristischer Anschlagsvorbereitungen und terroristischer Täter nicht möglich wäre. Sicherheitsdienstleister hätten die Möglichkeit, im Rahmen ihrer Aufträge verdächtige Umstände und Personen zu erkennen und rechtzeitig den Verfassungsschutz und/oder die Polizei zu informieren. Diese Möglichkeit bestehe insbesondere im Rahmen des Schutzes von Flüchtlingsunterkünften sowie im Öffentlichen Personenverkehr, beim Schutz anderer kritischer Infrastrukturen, bei der Einlasskontrolle in Sportstadien und beim Schutz öffentlicher Veranstaltungen.

In der Qualifizierung der Einsatzkräfte von Sicherheitsdienstleistern seien noch längst nicht alle Möglichkeiten ausgeschöpft, um ein Maximum an Awareness, an Fähigkeit im Profiling und in der Beherrschung der eingesetzten Sicherheitstechnik zu erreichen. Hier komme den Akademien der leistungsstarken Sicherheitsdienstleister und den vom BDSW anerkannten Schulen eine große Bedeutung zu.

Unternehmenssicherheit

Elke Werner-Keppner, Erziehungswissenschaftlerin M.A. und Psychologin, und Dr. Volker Koch, etalon international GmbH, befassen sich in GIT, Ausgabe 6-2016. S. 61–63, mit dem Begriff **Sicherheitskultur im Unternehmen**. Das Dilemma sei, dass die professionelle Arbeit und das Engagement der Sicherheitsfachleute dazu führe, dass alle anderen Mitglieder des Unternehmens sich von der Sicherheitsarbeit distanzieren. Während die kleinen, kurzfristigen Vorteile wie erhöhter Umsatz oder Termintreue sofort auffielen, seien die negativen Auswirkungen einer nicht eingehaltenen Sicherheitsregel nicht auf Anhieb sichtbar. Den vermiedenen Unfall könne man nicht sehen. Sicherheitsarbeit müsse integraler Bestandteil aller täglichen Arbeitsabläufe werden und nicht künstlich aufgesetzt erscheinen. Häufig würden schon die gesetzlichen Anforderungen als störend ober als unangenehme Last empfunden. Führungskräfte müssten deutlich machen, dass es sich bei der Erwartung eines sicheren Verhaltens bei der Arbeitsausführung nicht um eine Empfehlung handelt, sondern um eine Vorgabe, die einzuhalten ist. Die von den Autoren angewandte Methode des Messens der Sicherheitskultur beruhe auf einer Selbsteinschätzung anhand der Beschreibung verschiedener Evolutionsstufen, basierend auf dem Modell von Bradley. Das Instrument sei standardisiert und berücksichtige das vorhandene Managementsystem sowie die Instrumente des Arbeitsschutzes im jeweiligen Unternehmen. Mit gezielten Fragen würden ausgewählte Mitarbeitergruppen durch alle Bereiche und Ebenen der Arbeitssicherheit geführt. Anhand der nicht erreichten Antworten könnten sofort Verbesserungspotenziale erkannt und Maßnahmen eingeleitet werden. Der Entwicklungsprozess in den nächsten Reifegrad der Sicherheitskultur habe begonnen.

Veranstaltungssicherheit

Sicherheitskonzepte bei (Groß-)Veranstaltungen aus Sicht der Polizei ist das Thema von Ltd. PD Helmut Lennartz, Polizei Aachen, in s+s report, Ausgabe 4-2016, S. 54–59. Der Autor geht ein auf kritische Personendichten, Risiken durch Lage und Beschaffenheit, gewalttätige Auseinandersetzungen, Brände und andere Schadensfälle, technische Störungen, Unwetter, Anschlagsszenarien, die Einbindung der Polizei bei der Bewertung der Sicherheitskonzepte, wichtige Informationen zum Sicherheitskonzept für die Polizei, besonders relevante Aspekte aus Polizeisicht, Aufgaben der Polizei, Anforderungen an Sicherheitsdienste und vor allem persönliche Anforderungen. Mitarbeiter von Sicherheitsdiensten träfen je nach Veranstaltung auf unterschiedliche Bevölkerungskreise und müssten mit deren Einstellungen und Verhaltensweisen umgehen. Erwartet würden Neutralität und Professionalität ebenso wie zielgerichtetes und bestimmtes Handeln bei freundlichem Auftreten, Redegewandtheit und Kooperationsfähigkeit. Von Ordnern werde ferner Hilfsbereitschaft und eine angemessene äußere Erscheinung erwartet. Da viele Veranstaltungen im öffentlichen Verkehrsraum oder in Hausrechtsbereichen mit tatsächlich öffentlichem Verkehr stattfinden, dürften gem. § 34 a GewO für Bewachungsaufgaben nur Personen eingesetzt werden, die vor der IHK erfolgreich eine Sachkundeprüfung abgelegt haben. Führungskräfte

sollten Erfahrungen im Veranstaltungsschutz nachweisen können. Behandelt werden in dem Beitrag ferner aufgabenbezogene Anforderungen, nötige Qualifikationen von Ordnungsdienstkräften und die Koordinierung der Zusammenarbeit der Beteiligten. Die Zusammenarbeit und die Akzeptanz von „Privaten" und Hoheitsträgern sei der Erfolgsschlüssel für umfassende Sicherheit derartiger Veranstaltungen.

Videoüberwachung

Geutebrück habe eine neue Möglichkeit der **Integration mehrerer Systeme** zu einem homogenen Gesamtsystem entwickelt, berichtet GIT in der Ausgabe 12-2016, S. 34–36. Der Integrationsserver G-Link sei eine zentrale Plattform, auf der alle Schnittstellen im Netzwerk zentral laufen. Aufwendige Entwicklungen von Interfaces bedürfe es nicht mehr. Ein Integrationsserver sei ein echter Gewinn für ein aus vielen Komponenten bestehendes, zentralisiertes Sicherheitssystem.

Whistleblower

Die Corporate-Governance-Kommission empfehle Unternehmen, ein Whistleblowing-System einzurichten, berichtet Frank Hülsberg, Warth & Klein Grant Thomton, in der FAZ am 30. November. Whistleblowing-Systeme unterstützten die Effektivität einer Compliance-Organisation. Zudem senkten sie die Hemmschwelle für Mitarbeiter und Geschäftspartner, mögliche Rechtsverstöße vertraulich anzuzeigen. Mitarbeiter, die diese Anlaufstelle nutzten, müssten nicht befürchten, von Vorgesetzten und Kollegen gemieden oder gar vom Arbeitgeber belangt zu werden. Aus Unternehmenssicht habe die Kanalisierung vertraulicher Hinweise auch den Vorteil, dass die Vorwürfe zunächst intern aufgeklärt werden könnten und nicht immer sofort Gegenstand staatsanwaltschaftlicher Ermittlungen würden. Häufig begrenzten Unternehmen das Whistleblowing-System allerdings auf die eigene, aktive Belegschaft. Das sei unzureichend. Die Praxis zeige, dass auch Kunden, Lieferanten oder ehemalige Mitarbeiter wertvolle Hinweise über strafrechtlich relevantes oder unethisches Handeln beisteuern können. Dabei gelte: Je mehr Meldewege diesen Informanten offenstehen, desto besser. Um nicht mit Hinweisen aller Art überflutet zu werden, müsse das Unternehmen kommunizieren, zu welchen Themen Hinweise über das Whistleblowing-System erwünscht seien. Zusätzliches Vertrauen schaffe die Bestellung von Ombudspersonen.
Als Ansprechpartner müssten diese zum einen über ein Zeugnisverweigerungsrecht verfügen. Zum anderen müsse die sie beauftragende Firma auf das Auskunftsrecht und die Herausgabe von Unterlagen verzichten. Allerdings könne die Staatsanwaltschaft im Zuge von Ermittlungen Unterlagen des Ombudsmannes beschlagnahmen. Das habe das LG Bochum 2016 entschieden.

Wohnungseinbruch

Die Zeitschrift s+s report weist in der Ausgabe 4-2016 darauf hin, dass der GDV seit langem bundesweite Regelungen in den Bauvorschriften fordere, mit denen die Mindestanforderungen für neu eingebaute Fenster und Türen definiert werden. Damit könnte der Einbruchschutz wirksam verbessert werden. Bisher würden in Deutschland einbruchhemmende Fenster und Türen nicht standardmäßig eingebaut.

Zutrittskontrolle

Mobile Geräte als Konvergenzfaktor beschreibt Markus Baba, HID Global, in der Ausgabe 12-2016 der Zeitschrift PROTECTOR,

S. 22–23. Es gebe technische Unterschiede zwischen NFC- oder der Bluetooth-basierten Lösung. Während die Reichweite bei NFC nur bei wenigen Zentimetern liege, könne Bluetooth heute Entfernungen von mehreren Metern überbrücken. Das eröffne ganz neue Anwendungsmöglichkeiten. Werde die Bluetooth-Verbindung etwa mit Gestenerkennung kombiniert, so könnten Nutzer die Türen auch aus größerer Distanz öffnen. Moderne Mobile-Access-Lösungen böten aber wesentlich mehr als nur die Nutzung mobiler Geräte bei der physischen Zutrittskontrolle. Ebenso könnten Smartphones für die logische Zugangskontrolle eingesetzt werden. Mit einer multifunktionalen Lösung könnten nicht nur die Bereiche Zutritt und Datenzugang am Arbeitsplatz abgedeckt werden, sondern beispielsweise zusätzlich der Fernzugriff oder das sichere Drucken und die digitale Signierung von E-Mails und Dokumenten. Die Vorteile einer konvergenten Mobile-Access-Lösung seien weitreichend. Als erstes ist das Thema User Experience zu nennen. Dank der Konvergenz von Anwendungen und Identitäten müssten Nutzer nicht länger verschiedene Schlüssel, Ausweiskarten, Token oder Passwörter verwenden. Eine solche Lösung ermögliche eine effiziente und durchgängige Nutzung starker Authentifizierungsmethoden innerhalb der gesamten Infrastruktur. Und mobile IDs basierten auf kryptografisch geschützten Datenobjekten mit modernen Verschlüsselungsprotokollen. Die portablen Datenobjekte seien fest an ein spezifisches Gerät gekoppelt. Sie könnten damit auch nicht transferiert werden.

Kabellose Zutrittssysteme und speziell das **funkbasierte elektronische Zutrittssystem eAccess** von Glutz thematisiert GIT in der Ausgabe 12-2016, S. 46/47. Es gebe funkvernetzte elektronische Zutrittssysteme, die die Vorteile der Offline- und der Online-Welt miteinander verbinden. Funk- und RFID-Technologie würden das Programmieren und die tägliche Benutzung erleichtern. Mit Hilfe eines einzigen Mediums ließen sich Türen damit komfortabel und berührungsfrei entriegeln. Die Geräte reagierten auf Clips, Karten oder einen persönlichen Code. Eine Skalierung sei jederzeit möglich. Die Funk-Lösung ließe sich ganz einfach und ohne großen Aufwand nachträglich anpassen. Neue Kabel müssten nur sehr selten verlegt werden – etwa bei Motorschlössern. Große Bürokomplexe oder Miethäuser mit mehreren Mietparteien könnten problemlos angebunden werden. Installationsaufwand und Kosten entsprächen denen eines Offline-Systems, Komfort für Nutzer und Verwaltung dem eines Online-Systems. Die Programmierung von Beschlägen, Zylindern und Lesern erfolge ganz einfach per Funkstick über den eigenen Computer. Über ein Online-Gateway könnten auch mehrere Standorte von einem Ort und Rechner aus konfiguriert werden. Die Batterien hielten rund 50.000 Schließungen oder drei Jahre im Standby-Modus. Die Identifikationsgeräte arbeiteten auch bei Ausfall zuverlässig, da die Berechtigungen auf jedem einzelnen Gerät gespeichert seien. Für Mehrfamilienhäuser würden selbstverriegelnde Mehrfachverriegelungsschlösser mit Anti-Panikfunktion empfohlen, die mit einem speziellen elektronischen Beschlag mit funkfähigem Modul ausgestattet sind. Bewohner lösten die Türöffnung über die Telefonsprechanlage aus. Dabei kommuniziere das an der Türsprechanlage angeschlossene Input/Output-Modul den Befehl als verschlüsseltes Funk-Pairing-Signal zum einbruchgeprüften Funkbeschlag.

Impressum

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

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

Herausgeber:
Manfred Buhl, Vorsitzender der Geschäftsführung, Düsseldorf

Verantwortlicher Redakteur:
Bernd Weiler, Leiter Kommunikation und Marketing

Beratender Redakteur:
Reinhard Rupprecht, Bonn

focus.securitas.de

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

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

E-Mail: info@securitas.de