Focus on Security

Ausgabe 09, September 2016

SECURITAS

Inhalt

Arbeitsschutz

Die Zeitschrift GIT befasst sich in der Sonderausgabe PRO-4-PRO (2016, S. 125) mit einer **aktiv leuchtenden Not-Halt-Taste**. Bisher habe – um eine Verwechslung auszuschließen – der Not-Halt bei Inaktivität abgedeckt werden müssen. Eine Fehlbedienung sollte so ausgeschlossen werden. Dieses Risiko werde mit der neuen aktiv leuchtbaren Not-Halt-Taste auf ein Minimum reduziert: Ist das Bedienterminal oder der modulare Anlagenteil nicht mit dem Gesamtsystem verbunden, werde dies durch den nichtleuchtenden grauen Pilzknopf eindeutig angezeigt.

Außerdem stellt GIT in der Sonderausgabe PRO-4-PRO (2016, S.128/129) den **Safeguard Detector**, ein TÜV-zertifiziertes Sicherheitssystem zur Reststapeldetektion in Zuführmagazinen für Kartonzuschnitte, vor. Intelligente Sensor- und Steuerungslösungen hätten es in den letzten Jahren ermöglicht, Produktivitäts- und Sicherheitsziele gleichzeitig zu erreichen. Der Safeguard Detector sei ein alternativer Ansatz, der eine zertifizierte Sicherheitsüberwachung gewährleistet und in konstruktiver Hinsicht neue Möglichkeiten für eine ergonomischere und platzsparendere Maschinengestaltung eröffne. Die Systemlösung bestehe aus zwei MultiPulse-Lichttastern sowie einer modularen Sicherheitssteuerung.

Awareness

Mit einem Awareness-Training für Sicherheitskräfte befasst sich Klaus Kapinus, Hochschule für Management und Sicherheit Northern Business School Hamburg, in der Ausgabe 9-2016 der Zeitschrift PROTECTOR, S. 70–72. Auch wenn Planung und Vorbereitung terroristischer oder krimineller Aktionen nicht entdeckt werden, bestehe bis kurz vor der Tatbegehung, also in der „Vortatphase", eine Chance, das Vorhaben zu erkennen und zu verhindern. Diese Chance lasse sich erhöhen, wenn Sicherheitspersonal systematisch dafür sensibilisiert und ausgebildet wird. In Zusammenarbeit mit der Security des Airport Hamburg und Studierenden der Hochschule der Polizei Hamburg sowie mit der Hochbahnwache Hamburg (ÖPNV) hätten Dozenten des VSWN ein diesbezügliches Trainingsprogramm entwickelt, dessen Praxistauglichkeit belegt worden sei. In allen Fällen hätten der bzw. die Täter in den Tatplanungsphasen in zwei Stadien, nämlich der Vortat- sowie der Entschlusstatphase, im Rahmen der Tatbegehung typische Täterprofile und Verhaltensmuster gezeigt, die vom normalen Verhalten stark abweichen. Insbesondere die „Adaptoren" könnten Hinweise auf den Grad der Erregung geben. So deuteten zum Beispiel Händekneten, „Nesteln" oder Hand/Hals-Gesten auf den Versuch der Erregungsabfuhr hin. Auch wenn die Täter aus anderen Kulturkreisen stammen, seien die Adaptoren vergleichbar und kaum trainierbar. Nach diesen Erkenntnissen dürfe sich das Sicherheitspersonal von kulturellen und äußerlichen Unterschieden nicht leiten lassen und daraus Schwerpunkte ableiten. Vermittelt würden im „AGO (Awareness an Gefahrenorten)-Seminar" wissenschaftliche, psychologische und sicherheitsrelevante Erkenntnisse, das Beobachten des Arbeitsumfeldes, das Erkennen von besonderen Verhaltensweisen und verdächtigen Gegenständen, das Einschätzen als mögliche Vorbereitungshandlung terroristischer und krimineller Aktionen und das Reagieren als professioneller und umsichtiger Mitarbeiter.

Betrug

Mit einer äußerst dreisten Masche erbeuteten Betrüger Ende Juni 2016 bei einer Bretzfelder Metallfirma Edelstahl im Wert von mehreren tausend Euro, heißt es in einer Pressemitteilung des PP Heilbronn vom 10. August 2016.

Zunächst habe ein angeblicher Angestellter einer britischen Firmengruppe telefonisch Kontakt mit der Firma aufgenommen. Da ein französischer Akzent bei dem Anrufer aufgefallen sei, habe man über eine Kreditprüfungsgesellschaft die Bonität überprüft. Einige Tage später habe ein Sattelzug mit polnischer Zulassung im Auftrag des vermeintlichen Kunden die Edelstahlplatten abgeholt. Eine Nachfrage bei der existierenden englischen Firma habe ergeben, dass sie die Bestellung nicht getätigt hatte. Da die Kriminellen bereits in anderen Bundesländern aufgetreten seien, rechne die Polizei damit, dass noch weitere Unternehmen mit betrügerischen Aufträgen hinters Licht geführt wurden.

Der **Kabelhersteller Leoni** habe bekannt gegeben, dass er einem groß angelegten Betrug durch Cyberkriminelle zum Opfer gefallen ist, berichtet die Deutsche Inkermann Fraud Weekly, Ausgabe 174. Durch gefälschte Dokumente habe man ihn um zweistellige Millionensummen „erleichtert". Die Gelder wurden angeblich auf Konten im Ausland überwiesen. Es werde geschätzt, dass der Betrug das Unternehmen bisher 40 Mio. Euro gekostet hat.

Bitcoins

Nach einer Meldung der FAZ vom 4. August wurden der Hongkonger Bitcoins-Börse Bitfinex nach eigenen Angaben 120.000 Bitcoins gestohlen, was in etwa 58 Mio. Euro entspricht. Der gesamte Handel auf der Tauschbörse sei daraufhin eingestellt worden, solange der Diebstahl untersucht werde. Noch sei zum Beispiel völlig unklar, ob der Einbruch von Insidern ausgeübt wurde oder es Hackern möglich gewesen sei, von außen auf die Systeme des Betreibers Bitfinex zuzugreifen. Der Preis für die virtuelle Währung Bitcoin sei daraufhin deutlich eingebrochen, teilweise um bis zu 20 Prozent. Der Diebstahl werde wohl nie aufgeklärt werden, denn die Bitcoin-Kontonummern seien zwar eindeutig, aber nicht auf den Nutzer zurück verfolgbar.

Brandschutz

Die Zeitschrift GIT befasst sich in der Sonderausgabe „PRO-4-PRO" (2016, S. 51) mit der **Steuerung gebäude- und sicherheitstechnischer Anlagen**. Insbesondere bei der Kopplung von Brandmeldeanlagen (BMA) hätten Schaltvorgänge eine besondere Bedeutung. Werden Brandmelder bei Wartungsarbeiten nicht korrekt abgeschaltet, können Fehlalarme ausgelöst werden. Wird die spätere Zuschaltung nach Abschluss der Arbeiten vergessen, könne die Nichterkennung eines echten Brandes verheerende Folgen haben. Mit dem neuen Funktionsmodul „Schaltvorgänge" biete WinGuard ein Konzept, das ein sicheres Abschaltungsmanagement ermögliche. Mit Hilfe des Moduls ließen sich Zeiträume einzeln oder zyklisch festlegen, in denen bestimmte Datenpunkte (angeschlossene Sensoren und Aktoren) in einen definierten Zielzustand versetzt werden sollen.

In der Ausgabe 9-2016 der Zeitschrift PROTECTOR, S. 18–20, befasst sich Hendrik Lehmann, Redaktion PROTECTOR, mit **Brandschutzkonzepten für große Holzgebäude**. Mehrgeschossige Holzbauten seien keine Seltenheit mehr, stellten aber individuelle Herausforderungen an den Brandschutz. Baurechtlich sei es lange Zeit nicht möglich gewesen, bestimmte Gebäudehöhen zu verwirklichen. Erst mit der Novellierung der MBO 2002 und der Einführung der Muster-Holzbaurichtlinie 2004 seien in den meisten Bundesländern fünfgeschossige Holzbauten bis Gebäudeklasse vier zulässig. Bei Hochbauten bildeten die Decken die kritischen Komponenten. Denn sie fungierten als Barriere für das vertikale Ausbreiten eines Brandes und müssten entsprechend einen Feuerwiderstand REI 90 aufweisen. Hierfür stelle die

Holz-Beton-Verbundrippendecke (HBV) den Lösungsansatz dar, um in die Höhe zu bauen, denn sie ermögliche es, die jeweiligen Geschosse durch eine nicht brennbare Schicht konsequent zu trennen. Allgemein könne der Feuerwiderstand von tragenden Elementen in Holzgebäuden durch eine Beschichtung oder Verkapselung erhöht werden. Hierzu würden zum Schutz des Holzes vor Entzündung nicht brennbare Plattenwerkstoffe eingesetzt.

Cloud Computing

Frank Marcus Schille, Schille Informationssysteme GmbH, beschreibt in der Ausgabe 9-2016 der Zeitschrift PROTECTOR, S.21–23, die **Vorteile der Cloud-Technologie**. Beim Ansteigen der Anforderungen an die Cloud, wie etwa durch die Anzahl der Videokanäle, würden lediglich Ressourcen hinzugefügt. Mehr Rechnerhardware erhöhe beispielsweise die Kanalanzahl, mehr Speicher die Aufzeichnungsdauer. Der Autor geht insbesondere auf die Eignung der Cloud-Lösung in der Videoüberwachung ein. Digitale Videokameras seien für sich gesehen bereits Server mit vergleichsweise hohen Bitraten, die wiederum von den Videoservern aufzubereiten sind. Netzwerkauslastungen von 30 Prozent und mehr bei Gigabit-Netzwerken, CPU und Grafikprozessorauslastungen von 50 Prozent und Festplatten im Dauerstress seien daher insbesondere in großen Anlagen keine Seltenheit. Die Cloud-Technologie biete mit einer ihrer wesentlichen Eigenschaften eine vorzügliche Lösung an: das Ressourcenmanagement. Auf einer Wunschliste der Anwender von großen Videoüberwachungsanlagen stünden eine einfache Planung, Konfiguration und Wartung sowie eine kalkulierbare Verfügbarkeit an höchster Stelle; darüber hinaus eine möglichst optimale Auslastung der zu verwendenden Hardware und eine Migration bestehender Komponenten. Diese Anforderungen hätten Anlass gegeben, bei der Neuentwicklung der Serversysteme nicht mehr dem klassischen Server/Client-Konzept zu folgen, sondern zwischen den digitalen Videokameras und den Anwendern eine reine Cloud-basierende Lösung bereitzustellen. Bereits ein einzelner Server könne die gesamte Cloud-Technologie für mehr als 100 Kamerakanäle bereitstellen und erfülle vollständig die Aufgaben eines klassischen Videoservers. Ab einem zweiten Server sei bereits ein redundanter Betrieb gewährleistet. Vom Meldungsmanagement über Lageplan- und GIS-Dienste bis hin zu den Schnittstellen für Subsysteme und IoT-Anwendungen biete diese Technologie eine ideale Plattform für ein zukunftsweisendes und nachhaltiges Sicherheitssystem.

Datenschutz

Warum die Unternehmenssicherheit gut daran tut, sich vom Datenschutzexperten beraten zu lassen, erklärt Dr. Roland Weiß in der Fachzeitschrift Security insight in der Ausgabe 4-2016, S. 22/23. Sicherheitsmaßnahmen für die Verarbeitung von personenbezogenen Daten würden durch das BDSG stark unterstützt. Hier habe der Sicherheitsverantwortliche eine gesetzliche Grundlage, die als Argumentation für seine Maßnahmen herangezogen werden könne. Der Wertebeitrag von Datenschutz für die Konzernsicherheit sei direkt gegeben, da mit den angeführten gesetzlichen Grundlagen das eine oder andere Sicherheitsbudget eher von der Geschäftsleitung freigegeben werde.

Datensicherheit

Die Zeitschrift GIT geht in einer Sonderausgabe im August 2016 (PRO-4-PRO, S. 59), auf die physische Vernichtung elektronischer Datenträger ein. Das Unternehmen HSM biete mit dem mechanischen Festplattenvernichter HSM Powerline HDS „die perfekte“

Lösung. Er vernichte digitale Datenträger in kleinste Streifen und mache eine Wiederherstellung unmöglich – sicher, wirtschaftlich und datenschutzkonform. Die Schneidwellen aus gehärtetem Vollstahl zerteilten die zu zerstörenden Datenträger in ca. 40 mm breite Streifen, was nach der DIN 66399 den Sicherheitsstufen T-1, E-2 und H-3 entspreche.

Einbruchmeldesysteme

Die Zeitschrift PROTECTOR enthält in der Ausgabe 9-2016, S. 42/43, eine Marktübersicht für 77 Einbruchmeldeanlagen von 32 Anbietern. Neben allgemeinen Angaben wurden 30 Leistungsmerkmale abgefragt und ausgelistet, u. a. Anzahl der Meldergruppen, Meldepunkte, der Melder, Stichleitungen, Ringe, Teilnehmer und Partitionen, Schnittstellen, Zugriffsschutz, Integration in übergeordnete Managementsysteme.

Einzelhandelssicherheit

Frank Richter, Honeywell Security & Fire, behandelt in der Ausgabe 9-2016 der Zeitschrift PROTECTOR, S. 40/41, die zentrale Steuerung von Sicherheitssystemen im Einzelhandel. Cloud-Video und Zutrittskontrollsysteme könnten einfach über IP-Vernetzung implementiert werden und seien damit wirtschaftliche und einfach zu wartende, fernüberwachte Sicherheitssysteme. Lediglich die Hardware müsse am jeweiligen Einsatzpunkt vor Ort installiert werden. Die einzelnen Objekte würden dann via IP zentral durch einen Standort überwacht, der über einen Server Zugriff erhalte. Das sei besonders im Einzelhandel ein entscheidender Vorteil, da es den Aufwand für Sicherheitspersonal in den einzelnen Filialen reduzieren könne.

Ermittlungen

Da interne Ermittlungen in Unternehmen immer größere Ausmaße annehmen, empfiehlt Marko Rogge in der Ausgabe 4-2016 der Zeitschrift Security insight, S.52, „Kollaboration-Forensik". Dazu würden Daten aus einer forensischen Maßnahme auf einem zentralen Storage vorgehalten, die gesondert abgesichert sein sollten und physikalisch vom Netz getrennt erreichbar sind. Ermittler und Analysten würden hierbei den Zugriff auf die Falldaten haben und könnten diese auswerten oder analysieren. Ermöglicht werde „Kollaboration-Forensik" durch den Einsatz modernster Technologien und leistungsstarker Server. Es sei empfehlenswert, ein separates Netzwerksegment aufzubauen, auf dem nur die dafür fest konfigurierten Forensik-Workstations Zugriff haben. Dieses Forensik-Netzwerk habe keine Anbindung ans Internet und erfülle somit alle Anforderungen an die Forensik. Ein Vorteil sei das Datenmanagement, das es dem Forensiker erlaube, unterschiedliche Datenquellen heranzuziehen, um diese in einem Fall vereint bereitstellen zu können.

Gefahrenmeldetechnik

Die Zeitschrift GIT behandelt in einer Sonderausgabe (PRO-4-PRO) die VdS-Anerkennung 2.0 für Errichter von Gefahrenmeldetechnik (S. 67–69). Die zentrale Neuerung sei, dass der Kompetenznachweis durch die VdS-Anerkennung den Entwicklungen des Marktes entsprechend verfahrensübergreifend angeboten werde. Dieses eine Verfahren **„Errichter 2.0"** umfasse derzeit die Fachgebiete Brandmeldeanlagen, Einbruchmeldeanlagen und Videoüberwachungsanlagen. Die Überprüfung der Unternehmen sei modular aufgebaut. Man unterscheide dabei nach den Modulen „A: Planung und Projektierung", „B: Montage, Inbetriebsetzung, Anlagenüber-

prüfung und Abnahme" und natürlich „C: Instandhaltung".

Eine Erleichterung der **Wartung von BMA** thematisiert die Sonderausgabe PRO-4-PRO im August 2016, S. 111/112. Die Betreiber von GMA stünden vor der Herausforderung, die kryptischen Informationen, die ihnen das System liefert, interpretieren zu müssen. Das Unternehmen luuta biete Unterstützung, um den Verpflichtungen als Betreiber nach DIN VDE 08333 Teil 1 nachzukommen. Die luutaBOX werde lokal über eine serielle Verbindung mit dem BM-System verbunden und sammle kontinuierlich alle Daten der Brandmeldezentralen, ohne diese zu belasten. Die Daten würden zyklisch an die luutaNET übermittelt. Diese Verbindung könne nur über eine SSL-gesicherte HTTPS-Browser-Verbindung hergestellt werden. Die luutaAPP sei die Lösung für mobile Endgeräte wie Smartphone oder Tablet. Sie biete die Möglichkeit einer aktiven Benachrichtigung in Echtzeit über push-Service und die direkte Kommunikation der Wartungstechniker.

Gefahrstofflagerung

Explosionsschutzeinrichtungen für höchste Energieeffizienz und Sicherheit für brennbare Medien behandelt GIT in der Sonderausgabe PRO-4-PRO im August 2016, S. 116. Unter dem Aspekt der Energieeinsparung biete die Firma Säbu den SAFE Tank ECO an. Dieser sei ausgestattet mit einem explosionsgeschützten Lüfter in Verbindung mit einem Türkontaktschalter zur Gewährleistung des Explosionsschutzes unter Einhaltung der Vorschriften nach TRGS 510. Der SAFE Tank CONTROL sichere Personen und Objekte vor gefährlichen Gasen und Gas/Luft-Gemischen. Ein serienmäßig eingesetzter Sensor messe im Innenraum permanent die vorhandene Gaskonzentration der üblich eingesetzten Gase. Sobald die Konzentration zehn Prozent der untersten Explosionsgrenze (UEG) des Gas/Luft-Gemisches übersteigt, schalte sich automatisch der Lüfter ein. Bei einer Überschreitung von 20 Prozent unterbreche die Gaswarnanlage automatisch und umgehend die Stromzufuhr zu allen elektrischen Geräten im Innenraum.

Geldautomatensicherheit

Seit Monaten sprengten Banden in vielen westdeutschen Regionen Geldautomaten – allein in NRW 87, vor allem in Bankfilialen im ländlichen Raum, berichtet die FAZ am 18. August. Als besonders professionell und skrupellos gelte die Audi-Bande, die in wechselnder Besetzung unterwegs sein soll. Die Bande soll sich aus bis zu 250 Niederländern vor allem aus Utrecht und Amsterdam zusammensetzen. Bei ihnen solle es sich überwiegend um junge Männer nordafrikanischer Herkunft handeln. Für ihre Überfälle würden die Straftäter in der Regel extrem leistungsstarke Audi-Fahrzeuge der Reihe „RS" stehlen.

Geschäftsgeheimnis

Die Initiative Wirtschaftsschutz weist am 28. Juli auf die neue **„EU-Richtlinie Geheimnisschutz"** [Richtlinie (EU) 2016/943 vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung] hin. Ihre nationale Umsetzung erfolge in den nächsten zwei Jahren. Unternehmen sollten bereits jetzt ihre Schutzmechanismen überprüfen. Ziel sei die Erreichung einheitlicher Mindeststandards in den EU-Mitgliedsländern zum Schutz von Betriebs- und Geschäftsgeheimnissen. Die Richtlinie definiere den Begriff Geschäftsgeheimnisse. Kumulativ gehöre dazu erstens, dass es sich um geheime Informationen

handeln muss, dass die Informationen zweitens einen kommerziellen Wert besitzen und drittens die Informationen Gegenstand von angemessenen Geheimhaltungsmaßnahmen seitens des Inhabers sind. Die Richtlinie (Art.2 Nr. 1, Punkt c) verlange effektive Maßnahmen der Unternehmen zum Schutz von Betriebs- und Geschäftsgeheimnissen („angemessene Geheimhaltungsmaßnahmen"). Sie seien Voraussetzung für einen umfassenden Schadensersatzanspruch, den die Richtlinie in den Artikeln 6–16 im Detail regele. Dazu gehörten auch Nutzungsverbote, Rückruf- und Vernichtungsansprüche, die Herausgabe des Gewinns durch den Geheimnisverletzer oder die nachträgliche Berechnung gemäß Lizenzpraxis. Neu für Deutschland sei die Regelung, dass „Reserve Engineering" statthaft ist, also die Untersuchung oder der Rückbau eines öffentlich erhältlichen Produkts (Art. 3 Abs. 1, Punkt b). Know-how-Schutz und damit Wirtschaftsschutz erhielten durch die neue EU-Richtlinie eine weiter steigende Bedeutung für deutsche Unternehmen. Die seien gut beraten, interne Regelungen zum Know-how-Schutz und Informationsschutzmanagement im Hinblick auf die neuen EU-Vorgaben zu überprüfen oder erstmalig zu entwickeln.

Industrie 4.0

Im Interview nimmt Dr. Jörg Wissdorf, Interflex Datensysteme GmbH & Co. KG, in der Sonderausgabe PRO-4-PRO, 2016, S. 90, Stellung zur **Zukunft der Zutrittslösung**. Das erste Kriterium für die Zutrittslösungen sei der ganzheitliche Lösungsansatz. Das zweite Kriterium sei erfüllt, wenn Komponenten miteinander vernetzt werden können. Das dritte Kriterium gestatte es dem Kunden, selbst im Sinne von Industrie 4.0 zu agieren. Die Individualisierung von Produkten für globale Märkte erfordere ein hohes Maß an Flexibilität. In Zeiten von Industrie 4.0 sprächen Maschinen oder Systeme miteinander. In „Smart Factories" würden mechanische Fähigkeiten mit Software verknüpft. Zukünftig würden auch die Maschinen mit Menschen kommunizieren („Zutritt 5.0").

Eine der Voraussetzungen für die Entwicklung neuer Fertigungskonzepte im Rahmen von Industrie 4.0 sei die **Kommunikationsfähigkeit der Objekte** (GIT, Sonderausgabe PRO-4-PRO, August 2016, S. 126). Eine neue Generation von Sicherheitssensoren und Sicherheitszuhaltungen von Schmersal nutze die RFID-Technologie – auch, um ein hohes Maß an Manipulationssicherheit gemäß ISO 14119 zu gewährleisten. Hier könne die RFID-Technologie die Basis sein für das „intelligente Produkt".

IT-Sicherheit

Wie silicon.de am 2. August meldet, hat der auf SAP-Sicherheit spezialisierte Anbieter ERPScan einen **Jahresbericht für die Sicherheit von SAP-Systemen** vorgelegt. Nach diesem Bericht sollen nach wie vor mehrere zehntausend Systeme über das Internet angreifbar sein. Im SAP-Heimatmarkt Deutschland gebe es vergleichsweise wenige unsichere Konfigurationen, weil hier das Internet of Things und Industrie 4.0 noch nicht so stark verbreitet seien. Bei SAP sei man auf allen Ebenen des Entwicklungsprozesses darum bemüht, die Produkte so sicher wie möglich zu machen. Seit einigen Jahren gehe die Zahl der veröffentlichten Patches im SAP-Umfeld zurück. Von ERPScan heiße es, dass SAP nun dazu übergehe, mehrere Updates in umfangreicheren Bulletins zusammenzufassen. Viele SAP-Produkte seien inzwischen über das Web oder mobil erreichbar, und die Zahl der betroffenen Nutzer könne dann schnell in die Höhe schnellen. Am häufigsten träten die Produkte CRM, Enterprise Portal Implementierung zu einem Sicherheitsrisiko. Auch von einigen Unternehmen würden Sicherheitsupdates regelmäßig nicht aufgespielt. Cross Site Scripting sei zusammen mit

Authentifizierungsproblemen der häufigste Grund für Patches von SAP.

Golem.de weist am 5. August auf eine Studie der Universität Nürnberg-Erlangen hin, der zufolge **menschliche Nutzer** einen nicht zu eliminierenden **Unsicherheitsfaktor in Computersystemen** darstellen. Fast die Hälfte der Versuchsteilnehmer habe sich durch eine Phishing-Mail dazu verleiten lassen, auf einen nicht vertrauenswürdigen Link zu klicken. Dabei sei der großen Mehrheit von ihnen klar gewesen, dass solche Links eine Sicherheitsgefahr darstellen können. Bei dem Test seien 975 E-Mail-Nutzern und 289 Facebook-Nutzern Fotos von einer Silvester-Party versprochen worden. 20 Prozent der E-Mail-Nutzer und 42 Prozent der Facebook-Nutzer hätten auf den gefährlichen Link geklickt. Dabei seien sich 82 Prozent der Teilnehmer der Gefahren bewusst gewesen, die durch das Anklicken eines Links entstehen können. Die Analyse der Daten habe gezeigt, dass es zwischen diesem Bewusstsein und dem Klickverhalten keine Verbindung gebe. Der häufigste Grund für die Sorglosigkeit sei reine Neugier. Die Forscher rieten, mit einer tief gestaffelten Sicherheitsarchitektur Nutzer und Organisationen zu schützen. Die menschliche Neugier sei schließlich eine hoffentlich nicht zu patchende Sicherheitslücke.

In der Ausgabe 9-2016 der Zeitschrift PROTECTOR, S. 65, teilt Hans Elstner, E-Networkers GmbH, mit, sein Unternehmen habe in Kooperation mit der Allianz für Sicherheit in der Wirtschaft Mitteldeutschlands e. V. den **„IT-Check-Up"** entwickelt. Damit würden alle notwendigen Daten der IT eines Unternehmens erfasst und analysiert und ein strukturierter Ergebnisbericht zur IT-Infrastruktur erstellt. Dieser werde in einem Auswertungsgespräch erläutert. So werde deutlich, welche Bereiche den aktuellen Erfordernissen entsprechen und wo Handlungsbedarf bestehe. Der „IT-Check-Up" zeige Unternehmen, wie sie ihre Informationen und Daten besser schützen.

Immer mehr Versicherer drängen auf den **Markt für Cyberversicherungen**, schreibt die FAZ am 19. August. Sie wollten mit Innovationen punkten und nicht nur Produkte auf Services der Konkurrenz kopieren. Derzeit hätten Anbieter wie Hiscon, das die erste Cyberpolice auf den deutschen Markt gebracht hat, die Allianz-Tochtergesellschaft AGCS, AXA, AIG und Chubb die Nase vorn. Mit den Policen könnten sich Unternehmen gegen finanzielle Risiken aus Hackerangriffen schützen. Es gehe um zwei Kategorien, die die ERGO-Versicherung in ihrem neuen Angebot in zwei separate Bausteine gepackt hat: Das Kompakt-Produkt umfasse das Krisenmanagement, die Abwendung von Reputationsschäden, Dienstleistungen rund um den Schaden sowie die Abwehr von Erpressungsversuchen. In der umfassenden Deckung, die sich an Betriebe mit mehr als einer Million Euro Umsatz richtet, seien zwei weitere Kosten gedeckt: Drittschäden durch gestohlene Kundendaten und Betriebsunterbrechungen, die sich durch ein lahmgelegtes Computersystem ergeben. Diese Elemente seien inzwischen marktüblich.

60 Krankenhäuser wurden in Deutschland bisher 2016 durch Ransomware angegriffen, berichtete BSI-Präsident Schönbohm beim Münchner Cyber-Dialog nach einer Meldung des Behörden Spiegel in der September-Ausgabe. Das Thema **Awareness sei in Bezug auf Ransomware-Angriffe besonders wichtig**, da drei Viertel aller Attacken über infizierte E-Mail-Anhänge erfolgten. Bei dem Cyberangriff auf das Atomkraftwerk in Grundremmingen habe das BSI verhindert, dass der Angriff die Steuerung des AKWs erreichte. Im Anschluss sei die gesamte Branche informiert worden, um die eigenen Systeme besser schützen zu können. Schönbohm hält es für zwingend erforderlich, dass das Thema IT-Sicherheit bei allen Unternehmen auf Vorstandsebene angesiedelt werde. Elementar sei ein intensiver Dialog zwischen Wirtschaft und Politik. Anders könne das Niveau der IT-Sicherheit nicht angehoben werden.

IuK-Kriminalität

Eine mysteriöse Gruppe mit dem Namen **„Shadow Broker"** beanspruche, Geheiminformationen von den Computern des NSA gehackt zu haben, berichtet die FAZ am 19. August. Damit sei eine Gruppe von Hackern, die selbst offenbar bisher im Auftrag der NSA Cyberattacken unternehme, zum Opfer einer Cyberattacke geworden. Die „Shadow Brokers" präsentierten auf der Website Daten, die von Experten als authentisch angesehen werden. Sie behaupteten ferner, weiteres Material in Reserve zu haben, das sie bei Zahlung von einer Mio. Bitcoins (eine halbe Mrd. Dollar) an eine bestimmte Adresse zugänglich machen würden. Die Washington Post berichte, die auf der Website von der Gruppe veröffentlichten Daten enthielten sogenannte „Hacking Tools", welche die NSA offenbar zu nutzen pflegte. Die Instrumente seien ausgeklügelt und in der Lage, Firewalls auszuhebeln, Informationen abzuschöpfen oder Falschinformationen einzuspeisen. Selbst Unternehmen oder Behörden, die sich als gut geschützt gegen Cyberattacken fühlten, könnten mit diesen Instrumenten ausgeleuchtet werden.

Die Direktorin des hessischen LKA, Sabine Thurau, verlangt nach einem Bericht des Behörden Spiegel in der September-Ausgabe **mehr Engagement der Wirtschaft** im Bemühen gegen Cybercrime. Nicht die Daten an sich seien das Problem, sondern der Umgang mit ihnen. Täter und Tatort würden bei Cybercrime zunehmend auseinanderfallen. Insbesondere habe Thurau vor dem sogenannten „CEO-Fraud" gewarnt. Dabei treten Betrüger an Mitarbeiter eines Unternehmens heran und geben sich als Vorstandsvorsitzender einer anderen Firma aus. Dann versuchen sie, dem Beschäftigten ein Vertrauensverhältnis vorzugaukeln und ihn so zu einer diskreten Geldüberweisung zu bewegen.

Wie der ASW am 24. August mitteilt, konnte die Cyberabwehr des BfV die Domain gmx-service.net aufklären. Die Cyberware gehe davon aus, dass die Domain für **Phishing-Angriffe gegen deutsche GMX-Kunden** genutzt wird. Da gmx-service.net erst am 17. August registriert worden sei, müsse mit Angriffen über diese Domain in unmittelbarer Zukunft gerechnet werden. Die bisherigen Erkenntnisse zu dieser Spionagekampagne sprächen dafür, dass im Fall eines erfolgreichen Angriffs auf ein Postfach dieses in seiner Gesamtheit vom Angreifer kopiert und entwendet werde. APT 28 attackiere in der Regel gleichzeitig die privaten und dienstlichen E-Mail-Accounts von Zielpersonen. Es sei davon auszugehen, dass sich Phishing-Angriffe über gmx-service.net gegen gezielt ausgewählte Opfer richten. APT 28 stelle derzeit eine der aktivsten und aggressivsten Cyberspionageoperationen im virtuellen Raum dar. Bei APT 28 bestünden Indizien für eine Steuerung durch staatliche Stellen in Russland.

Schadsoftware, die in Amerika Millionenschäden angerichtet haben soll, tauche jetzt verstärkt in Europa auf, berichtet die FAZ am 24. August. Die Kunden von immerhin 13 deutschen Banken sollen derzeit verstärkt das Ziel von Internetkriminellen sein, die mit einer **Schadsoftware namens „Goznym"** versuchten, Bankkonten leerzuräumen. Das berichteten Sicherheitsexperten von IBM. Die Hackersoftware sei den Angaben zufolge schon im Frühjahr in den USA aufgetaucht. Im April soll sie einen Millionenschaden bei Kunden von mehr als 24 amerikanischen und kanadischen Banken angerichtet haben. Danach sei die Schadsoftware in Polen aufgetaucht. Jetzt seien offenbar Banken in deutschsprachigen Ländern an der Reihe. Laut IBM hat die Zahl der **Angriffe von Goznym** in Europa **im August zugenommen**. Man habe knapp 1.500 Angriffe registriert. Goznym sei ein sogenannter hybrider Trojaner. Sein Name soll aus zwei Begriffen von Schadprogrammen zusammengesetzt

sein, die zusammenarbeiteten: Nymaim und Gozi ISFB. Nymain sei ein Trojaner, also ein Instrument, mit dem sich von Betrügern auf versteckte Weise schädliche Programme auf fremde Computer spielen lassen. Mit Gozi ISFB wiederum ließen sich Anmeldedaten abfangen, wenn Opfer eine Online-Banking-Seite besuchen. Die Betrüger arbeiteten dabei offenbar u. a. mit gefälschten Bank-Internetseiten, auf denen der Kunde zur Eingabe von Kontodaten und PIN-Nummern aufgefordert wird. Diese Seiten sähen mittlerweile täuschend echt aus. Ziel des Internetbetrugs sei es, Konten von Bankkunden leerzuräumen und das Geld auf schwer erreichbare Konten in anderen Ländern zu transferieren. Beim Deutschen Sparkassen- und Giroverband hieß es, in den Rechenzentren der Sparkassengruppe seien im Juni und Juli tatsächlich Angriffe von Goznym in überschaubarer Zahl registriert worden. Beunruhigte Bankkunden sollten nach Angaben des BSI auf zwei Punkte achten: Auf der einen Seite sollten sie ihre Rechner so gut wie möglich schützen, indem sie regelmäßig Antiviren-Programme aktualisieren und Sicherheits-Updates für Betriebssystem, Browser und sonstige genutzte Software aufspielen. Auf der anderen Seite sollten sie vorsichtig sein, wenn sie den Kontakt zu ihrer Bank über einen Link aus einer E-Mail oder einen am Telefon genannten Link herstellen sollen.

Nach einer Meldung von golem.de haben Cyberkriminelle eine Malware programmiert, mit der sie auf fremden Geräten Krypto-Mining betreiben. Der autonome Wurm verbreite sich über verschiedene Wege und nutze als Wirtsystem auch industrielle Kontrollsysteme. Eine Analyse von Internetwache.org zeige, wie die Malware arbeitet, was sich damit vermutlich verdienen lässt und warum das Vorgehen erhebliche Gefahren mit sich bringt. Auf den ersten Blick sehe die Datei, hinter der sich die **gefährliche Krypto-Mining-Schadsoftware** verbirgt, harmlos aus, beinahe wie ein normaler Ordner unter Windows.

Körperscanner

Tagesspiegel.de berichtet am 11. August, Rohde & Schwarz habe vom Beschaffungsamt des BMI den Zuschlag für den R&S QPS200 **Körperscanner der neuesten Generation** erhalten. Der auf drei Jahre angelegte Rahmenvertrag umfasse 300 Systeme sowie Zubehör und Service. Als ausgewählter Körperscanner für Sicherheitskontrollen auf Basis von Millimeterwellen-Technologie werde die Bundespolizei ihn deutschlandweit für die Fluggastkontrolle auf Flughäfen nutzen. Die Millimeterwellen-Technologie basiere auf der Erfahrung des Unternehmens mit der Entwicklung von international führenden Messtechnikprodukten. Der Körperscanner detektiere automatisch, ob eine überprüfte Person potenziell bedrohliche metallische oder nichtmetallische Objekte unter der Kleidung oder am Körper mitführt. Falls ja, werde der entsprechende Bereich an einer symbolischen Personengrafik markiert, was die Privatsphäre der Überprüften wahre.

Korruption

Aus einer Pressemitteilung der britischen Korruptionsbehörde Serious Fraud Office (SFO) vom 8. August geht hervor, dass die Behörde eine strafrechtliche Untersuchung wegen des Vorwurfs des Betrugs, der Bestechung und der Korruption gegen das Luftfahrtunternehmen Airbus eingeleitet hat. Konkret gehe es um Unregelmäßigkeiten bei externen Beratern. Airbus gab am selben Tag bekannt, dass die Untersuchung vom Konzern selbst initiiert und die Informationen schon im April an die Behörde gegeben worden seien. Das Unternehmen habe strenge Richtlinien und kooperiere zur Aufklärung.

Kreditkartenbetrug

Big Data entlarvt Kreditkartenbetrüger, titelt silicon.de am 31. Juli. Bis der Betrug entdeckt wird, könnten Tage vergehen. Unternehmen müssten daher „prädiktive Modelle" in großem Umfang entwickeln. Es gebe bereits eine große Zahl erfahrener „Machine-Learning-Experten", die an neuen Techniken, Methoden und analytischen Modellen arbeiten, um potenziell betrügerische Transaktionen, Identitätsdiebstahl und Phishing-Attacken aufzudecken. Doch die wenigsten Unternehmen würden freiwillig personenbezogene Daten an externe Experten preisgeben. In Zukunft könnte ein neues Verfahren genau dieses Problem lösen. Es erlaube es, selbst Betrugsfälle mit nur einem Angriffspunkt aufzudecken. Eine neue Masche von Betrügern sei es, von großen auf viele kleine Transaktionen zu wechseln, für die sie die gestohlenen Nutzerdaten von mehreren hunderttausend Kunden einsetzen. Ziel sei es, eine vielleicht sechsstellige Summe in kürzester Zeit zu entwenden, ohne dabei entdeckt zu werden. Eine Bank verfüge über eine große Menge an Daten zum Transferverhalten zwischen Händlern und Kunden. Um herauszufinden, mit welchem Händler die Kunden interagierten, bevor die Betrugsfälle auftraten, würden die Transferdaten entsprechend zugeordnet und für jeden Händler ein „Breach Score" gebildet, der die relative Wahrscheinlichkeit der Händler ausdrückte, der gemeinsame Ursprung des Betrugs zu sein. Um das Dilemma zu umgehen, dass die Bank die Transferdaten nicht an Außenstehende geben möchte, habe die Firma MapR eine Erweiterung für ein Open-Source-Programm entwickelt. Dadurch ließen sich Transfers zwischen fingierten Nutzern und Händlern simulieren. In den Experimenten mit den simulierten Daten habe der kompromittierte Händler mit einem sehr hohen „Breach Score" herausgestochen. Big Data werde somit zu einem realistischen Werkzeug im Kampf gegen neue Arten des Betrugs.

Kriminalitätsentwicklung

Mit dem **Einfluss der Kriminalitätsentwicklung auf den Sicherheitsmarkt** befasst sich in der Ausgabe 4-2016 von Security insight, S. 40/41, Manfred Buhl, Securitas Deutschland. Nach seiner Überzeugung ist die Kriminalitätsbelastung einschließlich ihrer Entwicklungstendenzen einer der stärksten Einflussfaktoren für den Sicherheitsmarkt. Allerdings gelte dies nur unter Berücksichtigung wichtiger Eingrenzungen: Nicht die Gesamtkriminalität, sondern nur Deliktsbereiche, die sich durch Sicherheitstechnik und Sicherheitsdienstleistungen einschränken lassen, seien für uns relevante Einflussgrößen. Außerdem wirke sich die Kriminalitätsentwicklung nicht direkt auf den Markt aus, sondern über Entscheidungen der Marktteilnehmer. Und diese Entscheidungen würden von Risiko-Erfahrungen, vor allem aber von der Kriminalitätsdarstellung in Medien, von finanziellen Faktoren, von rechtlichen und technischen Normen sowie vom Angebot beeinflusst. Beispielhaft wirkten sich folgende Kriminalitätsentwicklungen auf den Sicherheitsmarkt aus: der hohe Anstieg des Wohnungseinbruchs, vorsätzliche und fahrlässige Brandstiftungen sowie die ansteigende IuK-Kriminalität.

Outsourcing

Das wachsende Outsourcing von Sicherheitsdienstleistungen habe das Aufgabenfeld der Anbieter gewandelt und erweitert, ist Michael Liehm, Daimler AG, überzeugt (Security insight, Ausgabe 4-2016, S. 48/49). Die Anbieter müssten ein Sicherheitskonzept für das zu vergebende Gewerk eigenständig entwickeln, um aus arbeitsrechtlicher Sicht ein Maximum an unternehmerischer Dispositionsfreiheit auszuüben. Es habe ein Umdenken stattgefunden. Der Auftraggeber beauftrage heute in der Regel komplett eigenständige Ge-

werke. Immer wichtiger werde es, zulässige Prüfungsmethoden zu entwickeln, um die gelieferte Qualität nachhaltig sicherzustellen. In der Praxis habe sich ein System bewährt, das aus zwei Teilen besteht: „Prüfung des Managements des Dienstleisters" und „Prüfung der vergebenen Gewerke am Standort". Empfehlenswert sei die Auditierung des Managements während der Vertragslaufzeit etwa alle anderthalb Jahre, die Auditierung der Gewerke vor Ort etwa alle sechs Monate. Im Nachgang werde ein Auditprotokoll mit einer Zeitleiste erstellt, bis wann gegebenenfalls bemängelte Punkte abgearbeitet sein müssen.

Rechenzentrumssicherheit

Mit dem **Schutz von hochverfügbaren IT-Sicherheitsräumen** befasst sich der Journalist Simon Federle in der Ausgabe 9-2016 der Zeitschrift PROTECTOR, S. 44/45. „Raum-in-Raum-Lösungen" seien eine Möglichkeit, die IT zu schützen. Sie sollten so konzipiert sein, dass sie in einem bestehenden Gebäude eingepasst und modular zu jeder Größe erweitert werden können. Den baulichen Schutz gewährleisteten beispielsweise die Bitkom RZ-Kategorien C & D, BSI und die geltende Norm EN 50600. Selbstverständlich müsse das Material, inklusive Dichtungen und Isolierplatten, auch widerstandsfähig, feuer- und temperaturfest sein. Modular erweiterbare Schranksysteme sollten ebenfalls allen wesentlichen physikalischen Gefahren wie Gas, Explosion sowie Löschwasser standhalten.

Risikomanagement

Drei Thesen zu Risikomanagement-Systemen stellt Jens Washausen, GEOS Germany, in der Ausgabe 4-2016 der Zeitschrift Security insight, S. 18/19, auf: 1. Der klassische „Risiko"-Begriff ist für Sicherheitsverantwortliche problematisch. Das Risiko werde definiert als Produkt aus der Höhe des zu erwartenden Schadens und der Eintrittswahrscheinlichkeit. Das führe in der betriebswirtschaftlich dominierten Entscheidungsfindung dazu, dass wichtige Risikoräume als nicht bearbeitungswürdig übersehen oder ausgeklammert würden. Wenn aber das Schadensereignis erhebliche Auswirkungen auf kritische Geschäftsprozesse haben würde, sei die ursächliche Gefährdung von großer Relevanz. 2. Wir kümmern uns zu wenig um die Schwachstellen. Der nur allzu oft anzutreffende Hunger nach schnellen und einfachen Prozessen habe in nicht wenigen Unternehmen dazu geführt, dass man sich im Risikomanagement darauf konzentriere, ein Risikoportfolio aufzustellen und für kritische Geschäftsprozesse Notfallpläne zu etablieren. Die größte anzunehmende Schwachstelle sei nach wie vor die selbstgefällige Aussage, dass es 100-prozentige Sicherheit nicht gibt und dass sich Terroristen und Hacker nicht für das eigene Unternehmen interessieren. 3. Die Risikoabdeckung über Versicherungslösungen ist oft sinnvoll, führt aber nicht selten zum Verzicht auf die notwendige Präventionsarbeit. Hier entwickle sich eine Mentalität, die nicht von unternehmerischem Verantwortungsbewusstsein geprägt sei.

Schwertransportbegleitung

Security insight weist in der Ausgabe 4-2016, S. 6, darauf hin, dass mit der Änderung des Straßenverkehrsgesetzes erstmals die Möglichkeit geschaffen wird, dass private Sicherheitsdienste die Begleitung von Schwertransporten übernehmen. Der BDSW begrüße diese Gesetzesänderung, obwohl die Transportbegleitung kein „Massengeschäft" für die Branche ergebe.

Schulsicherheit

In der Sonderausgabe von GIT PRO-4-PRO vom August 2016, S. 56, wird auf die am 1. Juli 2016 in Kraft getretene neue technische Norm für Notrufsysteme in Schulen und Behörden hingewiesen. Die unter Federführung des VDE entwickelte Richtlinie 0827 beschreibe ganz konkret jene Anforderungen, die neue Kommunikationsanlagen in Not- und Gefahrenfällen künftig zu erfüllen haben. Neu sei die Position des technischen Risikomanagers, der innerhalb einer Organisation bestimmt, welcher Sicherheitsgrad umgesetzt werden müsse. Er sei es auch, der entscheiden kann, ob eventuell von den Vorgaben der Norm abgewichen werden könne.

Sicherheitsplattform

In der Sonderausgabe PRO-4-PRO der Zeitschrift GIT vom August 2016 (S. 58) wird die jüngste Version der integrierten Sicherheitsplattform von Genetec vorgestellt, die noch mehr Authentifizierungs- und Autorisierungssicherheit, neue Verschlüsselungs- und Datenschutzfunktionen, einen Disaster-Recovery-Modus, ein verbessertes Videomanagement sowie erweiterte Zutrittskontrollfunktionen biete. Das System sei auch als Abonnementmodell auf Prepaid-Basis erhältlich.

Sicherheitstechnik

Einen Überblick über verfügbare ONVIF-Profile enthält die Sonderausgabe PRO-4-PRO von GIT (August 2016, S. 52/53). ONVIF sei von Axis, Sony und Bosch gegründet worden, um einen globalen Standard für die Schnittstelle zwischen Netzwerkkameras und Videomanagementsystemen zu entwickeln. So sollten Inbetriebnehmer und Anwender größere Wahlfreiheit bei der Auswahl von Produkten verschiedener Anbieter erhalten. Die Zeitschrift gibt einen Überblick über die **ONVIF-Profile**: Profil S für Video-Streaming; Profil G für Aufzeichnung und Speicherung; Profil C für Zutrittskontrolle; Profil Q für einfache Installation und das neue Profil A für Zutrittskontrollkonfiguration. Es ergänze Funktionen von Profil C und umfasse die alltäglichen Betriebsabläufe bei der Konfiguration von Anmeldedaten, Zutrittsregeln und Zutrittsplänen sowie Profil S für Videomanagementsysteme. Die ONVIF-Spezifikation sei in die neue IEC-Norm 62676 für Videoüberwachungssysteme aufgenommen worden, der erste internationale Standard für derartige Systeme. Auch in die demnächst erscheinende Norm IEC 60839, die IEC-Norm für elektronische Zutrittskontrolle, sei die neueste ONVIF-Spezifikation für Zutrittskontrollsysteme integriert.

Wie PROTECTOR in der Ausgabe 9-2016, S. 15, berichtet, ist der Gesamtumsatz im **Markt der elektronischen Sicherungstechnik** 2015 nach einer Erhebung von BHE und ZVEI um 7,8 Prozent gestiegen. 3,71 Mrd. Euro markierten einen neuen Bestwert. Folgende Zuwächse verzeichneten die Sparten Brandmeldetechnik: 11,2 Prozent, vor allem wegen der Nachfrage nach Rauchwarnmeldern; Einbruchmeldetechnik: 7,4 Prozent; Sprachalarmanlagen: 5,6 Prozent; Videoüberwachung: 5,1 Prozent; Zutrittssteuerung: 2,8 Prozent; Rufanlagen und sonstige Sicherungssysteme: 2,3 Prozent.

Dr. Peter Fey, Unternehmensberatung Dr. Wieselhuber & Partner, erläutert in der Ausgabe 9-2016 der Zeitschrift PROTECTOR, S. 16/17, **Ergebnisse des vierten Branchenbarometers** von PROTECTOR & WiK. Die Erhebungen stammten zu 59 Prozent aus den Branchensegmenten Videoüberwachung, Zutrittskontrolle, Einbruch- und Brandmeldung und zu 25 Prozent aus dem Segment der mechanischen Sicherheitslösungen. Auf die Frage, welche zentralen

Einflussgrößen den strategischen Anpassungsbedarf des Geschäftsmodells in den nächsten zwei bis drei Jahren am stärksten bestimmen werden, seien die Nennungen mit den größten Ausprägungen (je 4,1 von 5,0 möglichen Punkten) der wachsende Druck zur Digitalisierung der Prozesse und Produkte/Leistungen und der Druck zur Steigerung der Wirtschaftlichkeit gewesen. Auf die Frage zur Anpassung des Vertriebskonzeptes sähen die Teilnehmer der Befragung die Notwendigkeit zur Stärkung des Vertriebs über den Fachgroßhandel an der Spitze (3,6 Punkte).

Signalgeber

Mit der Leistung von Signalgebern in Räumen befasst sich GIT in der Sonderausgabe PRO-4-PRO vom August 2016, S. 104/105. Bislang gebe es in Deutschland keine konkreten Vorgaben hinsichtlich der **Effizienz von Signalisierungslösungen**. Je größer die sicherheitsrelevante Funktion eines Signalgebers in der Anwendung ist, desto wichtiger sei der tatsächlich abgedeckte Signalisierungsbereich. Um den passenden Signalgeber auswählen zu können, müssten in der Planungsphase unbedingt die Umgebungsbedingungen am Einsatzort berücksichtigt werden. Mit „3-D-Coverage" präsentiere das Unternehmen Pfannenberg als erster Hersteller eine praxisorientierte Darstellungsmethode für die effektive Leistung von akustischen und optischen Signalgebern im Raum. Beispielsweise werde der Signalisierungsbereich von akustischen Signalgebern stets unter Berücksichtigung von Störschall dB(A) und Signalton ermittelt. Bei vielen „günstigen" Schallgebern komme die Piezo-Technologie zum Einsatz. Ihre geringe Stromaufnahme mache sie insbesondere in der Brandalarmierung auf dem Papier attraktiv. Betrachtet man jedoch ihre Leistung, so lasse sich ein weitaus geringerer Signalisierungsbereich als bei der elektrodynamischen Schallerzeugung feststellen.

Spionage

Wie KMU zum Sicherheitsleck für die Großunternehmen werden, beschreibt Peter Niggl, Security insight, in der Ausgabe 4-2016, S. 12–15. Und er bringt Beispiele: Das Vorgehen von „Wasserloch-Angreifern" (vergleichbar dem Jagdinstinkt der Raubtiere) sei raffiniert und doch leicht verständlich. Irgendwo in den sozialen Netzwerken werde über das ins Visier genommene Unternehmen und dessen führende Mitarbeiter recherchiert. Die Angreifer hätten es auf die Vorlieben der Unternehmensverantwortlichen abgesehen. In Nigeria werde Reinigungspersonal von der Mafia für Spionagezwecke ausgebildet und später in ausgewählte Unternehmen eingeschleust. Häufig würden Strukturen, Kontrollen oder Prozesse, die dazu dienen, ein regelkonformes, ethisch korrektes Verhalten von Vertragspartnern einzufordern und ihr Geschäftsgebaren zu überprüfen, nur in Ansätzen etabliert. „Watering-Hole"-Attacken seien vor allem dem Umstand geschuldet, dass die Sicherungsmaßnahmen großer, wichtiger Unternehmen personell und technisch immer perfekter werden und deshalb „direkte" Angriffe immer weniger zum Erfolg führten.

Unternehmen im Hochtechnologiebereich sind besonders anfällig für Wirtschaftsspionage, ist nach einem Bericht in der September-Ausgabe des Behörden Spiegel der CIO des Deutschen Zentrums für Luft- und Raumfahrt überzeugt. Der „Wilde Westen im Cyberraum" sei völlig ohne Regulierung. Es sei unerlässlich, dass Unternehmen und Staat eng miteinander zusammenarbeiteten und ihr Wissen teilten. Die zunehmende Vernetzung mache es zudem unerlässlich, dass die Nutzung sämtlicher IT durch die Unternehmen kontrolliert wird. Dies gelte insbesondere dann, wenn die Mitarbeiter ihre privaten Endgeräte beruflich nutzen würden.

Stadionsicherheit

In einer Pressemeldung des BDSW vom 26. August weist Harald Olschok darauf hin, dass pro Spieltag in den drei Bundesligen bis zu 12.000 private Sicherheitskräfte zum Einsatz kommen. Eine **Umfrage von PriceWaterhouseCoopers** unter 1.000 Dauerkartenbesitzern habe ergeben, dass 94 Prozent der Befragten für schärfere Sicherheitsvorkehrungen in den Stadien Verständnis äußerten. 75 Prozent sprachen sich explizit für höhere Standards in diesem Bereich aus. Der BDSW weise seit vielen Jahren auf die Notwendigkeit gesetzlicher Voraussetzungen für den Einsatz von Sicherheits- und Ordnungskräften in Fußballstadien hin. Dazu gehöre vor allem eine tätigkeitsspezifische Qualifizierung. Im Mittelpunkt müssten praktische Kenntnisse im Umgang mit Menschen („Crowdmanagement") stehen und es müssten rechtliche Grundlagen vermittelt und abgeprüft werden. Auch die Überprüfung der Mitarbeiter im Vorfeld müsse verbessert werden. Olschok forderte eine über die derzeit geltenden gewerberechtlichen Regelungen hinausgehende unbürokratische und schnelle Zuverlässigkeitsprüfung.

Steuerhinterziehung

Die engere Zusammenarbeit zwischen der NRW-Polizei und der Steuerfahndung hat sich aus Sicht der Landesregierung ausgezahlt, berichtet die FAZ am 19. August. Eine Anfang vorigen Jahres eingerichtete Sondereinheit habe durch ihre Ermittlungen bisher mehr als 75 Mio. Euro aus zusätzlichen Steuereinnahmen und Geldbußen eingetrieben. Etliche Verfahren mit einer Schadenssumme von rund einer Mrd. Euro liefen noch. Die Sondereinheit operiere an der **Schnittstelle von organisierter Kriminalität und Steuerhinterziehung**. Unter anderem sei im Umfeld der „Russen-Mafia" und zahlreicher illegaler Offshore-Gesellschaften ermittelt worden. Dabei seien Verbindungen zu mehreren Groß- und Privatbanken sichtbar geworden. Weitere Schwerpunkte seien die Bekämpfung von Geldwäsche, Umsatzsteuerkarussellen und dem Steuerbetrug mit sogenannten Cum-Ex-Geschäften. Es handele sich nicht um „kleine Fische", sondern um organisierte Kriminalität in Banden, die das Gemeinwesen um dreistellige Millionenbeträge betrügen.

Terrorismus

Wie die FAZ am 6. August berichtet, werde im Zuge der Ermittlungen gegen die Attentäter von Ansbach und Würzburg (Focus 8-2016) immer deutlicher, dass beide Männer mehrfach Kontakt zu Personen hatten, die mutmaßlich dem „Islamischen Staat" (IS) angehören, und dass sie bei der Ausführung ihrer Anschläge bis in deren Einzelheiten hinein gesteuert wurde. Das habe die FAZ aus Sicherheitskreisen erfahren. Ermittler hätten mehrere Telefonnummern gefunden, die solche Kontakte belegen.

Am 22. August hat das BKA die **Gefährdungslage islamistischer Terrorismus** im Inland, in der EU und für deutsche Interessen im außereuropäischen Ausland fortgeschrieben. Danach wird Deutschland von verschiedenen international ausgerichteten dschihadistischen Organisationen weiterhin als Gegner wahrgenommen und steht in deren erklärtem Zielspektrum. Es bestehe kein Zweifel an dem ungebrochenen Willen, jede sich bietende Gelegenheit für islamistisch motivierte Gewalttaten zu nutzen. Sowohl für das Bundesgebiet als auch für deutsche Interessen in verschiedenen Regionen der Welt bestehe eine anhaltend hohe abstrakte Gefährdung, die sich jederzeit konkretisieren könne. Neben dem sogenannten Islamischen Staat sei dem Al-Qaida-Netzwerk trotz eingeschränkter operativer Fähigkeiten von Kern-Al-Qaida der Anspruch zu unterstellen,

groß angelegte terroristische Operationen gegen westliche Ziele durchführen zu wollen. Der internationale Dschihad-Schauplatz Syrien und Irak mit den dort aktiven terroristischen Gruppierungen übe weiterhin einen maßgeblichen Einfluss auf die Gefährdungssituation in Deutschland aus. Angesichts der Entwicklungen im Zusammenhang mit der Zuwanderungsbewegung nach Europa und Deutschland sei davon auszugehen, dass sich unter den Flüchtlingen auch aktive und ehemalige Mitglieder, Unterstützer und Sympathisanten terroristischer Organisationen sowie Einzelpersonen mit extremistischer Gesinnung und islamistisch motivierte Kriegsverbrecher befinden können. Der sogenannte Islamische Staat (IS) habe bereits in mehreren Propagandabotschaften damit gedroht, sich gegen die USA, Europa und alle an der „Anti-IS-Koalition" beteiligten Staaten zu stellen. Die Organisation sei in der Lage, gut ausgebildete und zu allem entschlossene Täter mit einem Auftrag in westliche Länder (zurück-) zu senden. Zur Minimierung des Entdeckungsrisikos werde auf unauffälliges, sozial- und gesetzeskonformes Verhalten unmittelbar nach der Rückkehr sowie auf konspirative Kommunikation geachtet. Neben den von terroristischen Organisationen selbst gesteuerten Taten bestehe zudem weiterhin die erhöhte Gefahr, dass Sympathisanten und Anhänger einer islamistischen Gruppierung ohne direkte Anbindung oder entsprechenden Auftrag der Führung eigenständig Taten planen oder durchführen. Als tatgeneigter Personenkreis könnten nicht nur die Rückkehrer aus Konfliktregionen angesehen werden. Insbesondere bei Personen mit einer Ausreiseabsicht, die entweder behördlicherseits an einer geplanten Ausreise gehindert wurden oder deren Reisewunsch in ein Dschihad-Gebiet aus anderen Gründen scheiterte, müsse von einer hohen Gefährdung ausgegangen werden. Die gesamte Bandbreite terroristischer Tatbegehungsweisen sei einzukalkulieren. Dschihadistische Tätergruppierungen und Einzeltäter orientierten sich unverändert an Anschlagszielen, die ein Maximum an medialer Aufmerksamkeit sowie infrastrukturellem und wirtschaftlichem Schaden garantieren. Als „weiche" Ziele würden neben Einrichtungen des Flug- und Bahnverkehrs weiterhin auch Großveranstaltungen sowie andere öffentliche Veranstaltungen in Betracht kommen, bei denen eine hohe Anzahl von Opfern zu befürchten sei. Westliche Interessen und Einrichtungen seien weltweit potenzielle Ziele von terroristischen Aktivitäten. In den verschiedenen Krisengebieten der überwiegend muslimisch geprägten Staaten sei jederzeit mit terroristischen Anschlägen gegen Interessen und Einrichtungen der Bundesrepublik sowie mit Entführungen westlicher Staatsbürger zu rechnen. Jede als Blasphemie verstandene Veröffentlichung islamkritischer Aussagen oder bildlicher Darstellungen in Deutschland oder durch Personen mit erkennbaren Deutschlandbezügen sei weiterhin als Emotionalisierungsfaktor bzw. Tatmotivation in besonderem Maße geeignet.

In silicon.de vom 23. August befasst sich Peter Marwan mit der geplanten **Abfrage von Social Media-Konten bei der Einreise in die USA**. Die Angaben zu den Konten sollen im Zuge der bei der Einreise auszufüllenden Formulare ESTA respektive I-94 abgefragt werden. US-Zoll und das Heimatschutzministerium hätten ihren Vorstoß damit verteidigt, dass die Angabe sowohl in dem sogenannten ESTA-Formular als auch im Formular I-94, die beide gegebenenfalls bei der Einreise in die ISA ausgefüllt werden müssen, freiwillig sein soll. Amerikanische Bürgerrechtsgruppen fürchteten, dass die Zusatzfragen zu tief in die Privatsphäre eingreifen und die Rede- und Meinungsfreiheit gefährden.

Überwachungstechnik

Nach einem Bericht von netzpolitik.org vom 2. August gibt es in Deutschland über 40 Firmen, die Überwachungs-Technologien

produzieren und in die ganze Welt verkaufen. Das gehe aus einer neuen Datenbank hervor, die Privacy International am 2. August veröffentliche. Die 528 Überwachungsfirmen des Index seien überwiegend in wirtschaftlich fortgeschrittenen Staaten ansässig, die ebenfalls eine große Rüstungsindustrie haben. Die Top 5 seien: USA, Großbritannien, Frankreich, Deutschland und Israel. Der Bericht präsentiere eine Analyse der Überwachungsindustrien in diesen fünf Ländern, einschließlich einer Analyse bekannter Exporte sowie spezifischer Eigenschaften der Firmen.

Unterschriftsfälschung

Mit der Möglichkeit von Unterschriftsfälschungen befasst sich Peter Niggl, Security insight, in der Ausgabe 4-2016, S. 44/45. Unterschriften seien immer nur so fälschungssicher, wie es Mittel gebe, diese Fälschungen zu beweisen. Und diese Beweisführung sei schwieriger geworden. In der digitalisierten Welt werde zwar nicht auf Unterschriften verzichtet, aber sie würden häufig nicht mehr im „klassischen" Sinne geleistet. Ob jemand seinen Personalausweis oder einfache Bankverträge unterschreibt – er tut es heute auf sogenannten Pads. Diese ließen aber zumeist nicht mehr die für die Echtheitsprüfung so wichtigen Charakteristika einer Unterschrift erkennen wie Ansatz und Schriftstärke. Ein weiteres Problem liege darin, dass Unterschriften, die einstmals auf Papier geleistet wurden und somit alle wichtigen Merkmale aufwiesen, im Zeitalter der papierlosen Archivierung dieser Dokumente entweder eingescannt – also digitalisiert – oder auf Mikrofilm festgehalten werden, was zum Verlust entscheidender und verifizierbarer Eigenheiten der Signaturen führe.

Verschlüsselung

Das BMI begrüßt den Start der von der Deutschen Telekom AG und dem Fraunhofer Institut für Sichere Informationstechnologie (SIT) angebotenen **Ende-zu-Ende-Verschlüsselung**, berichtet der Behörden Spiegel in der September-Ausgabe. Diese sei ein wichtiger Beitrag für Deutschland als Verschlüsselungsstandort. Mit der „Volksverschlüsselung" könnten Windows-Nutzer über E-Mail-Programme wie Outlook oder Thunderbird basierend auf dem S/MIME-Standard verschlüsselt per E-Mail kommunizieren. Das Programm könne mit dem Internet Explorer von Microsoft, Google Chrome und Mozilla Firefox genutzt werden.

Versicherungsbetrug

Peter Niggl, Security insight, behandelt in Ausgabe 4-2016, S. 16/17, **Versicherungsbetrug als Geschäftskalkül**. Vier Mrd. Euro – rund zehn Prozent der jährlichen Schadenszahlungen – würden pro Jahr durch Versicherungsbetrug ergaunert. Der GDV gehe nach einer Untersuchung 2011 davon aus, dass vermutlich jeder zehnte gemeldete Schaden betrügerisch ist. Das BKA sei einem gigantischen Abrechnungsbetrug durch Pflegedienste auf der Spur. Die Betrugsformen seien nach Einschätzung des BKA vielfältig. So würden Pflegedienste zum Beispiel systematisch mit gefälschten Pflegeprotokollen nicht erbrachte Leistungen abrechnen.

Videoüberwachung

Die Zeitschrift GIT stellt in der Sonderausgabe PRO-4-PRO vom August 2016, S. 60, eine neue Suchfunktion für ViconNet Video Management Software vor. **Museum Search** sei eine zeitsparende Funktion zur ultraschnellen

Suche der Aufzeichnungen. Dieses leistungsstarke Forensikinstrument ermögliche das rasche Durchsuchen eines großen Volumens an Videoaufzeichnungen, um Videosegmente mit spezifischen Handlungen oder Vorkommnissen in einer bestimmten Region zu finden.

Mit **Videosicherheitslösungen für KMU** befasst sich GIT in einer Sonderausgabe PRO-4-PRO vom August 2016, S. 72/73. Die Sicherung von Innen- und Außenbereichen bei Tag und bei Nacht sei der wichtigste Einsatzbereich von Videokameras. Moderne Systeme böten noch mehr Möglichkeiten, wie zum Beispiel eine IP-Video-Türstation, die den schlüssellosen Zutritt ins Gebäude ermögliche. Der Nutzer könne sich auf seinem mobilen Endgerät benachrichtigen lassen und mit dem Besucher sprechen, ihm Zutritt gewähren oder verweigern sowie die Beleuchtung ein- und ausschalten. Um sich nicht auf ein Anwendungsszenario festlegen zu müssen, böten sich Kamerasysteme an, bei denen sich die Sensormodule ganz einfach austauschen lassen. So müsse keine zusätzliche Kamera gekauft werden, wenn eine Sicherung des Geländes in der Dunkelheit wichtiger geworden sei als die Aufzeichnung spezieller Details. Moderne Videosysteme hätten bei den Kosten die Nase vorn. Bei einer Leistungsaufnahme von weniger als vier bzw. sechs Watt könnten die Kameras auch in das bestehende Netzwerk eingebunden werden, denn die notwendige Stromversorgung erfolge über ein Ethernet-Kabel (PoE, Power oder Ethernet). Auch die Kosten für Zusatzsoftware und Wartung seien bei herkömmlichen Lösungen deutlich höher. Der mobile Zugriff auf die Bilddaten, geringere Betriebskosten, flexible Einsatzmöglichkeiten, höhere Langlebigkeit und Wetterfestigkeit, einfache Installation und Bedienung sowie zahlreiche Zusatzfunktionen sprächen eindeutig für digitale Videokameras.

Mit **Videoüberwachungslösungen für KMU** befasst sich auch AXIS Communications GmbH in der Sonderausgabe PRO-4-PRO vom August 2016. S. 83. KMU benötigten ein zuverlässiges, nicht überdimensioniertes System mit einfacher Bedienung, das innerhalb eines bestimmten Budgetrahmens liege. IP-basierte Lösungen seien aufgrund ihrer Skalierbarkeit für einen so dynamischen Markt sehr viel besser geeignet als analoge Systeme. IP-Systeme verursachen deutlich niedrigere Gesamtbetriebskosten. Einzelhändler nutzten die Analysefunktionen der Kameras als kostengünstige Alternative, um ihre Kunden besser zu verstehen und ihre Geschäftsabläufe zu optimieren. Ein Sicherheitssystem müsse, unabhängig davon, ob es für eine Schule, ein Geschäft, Hotel, Büro oder ein anderes kleines Unternehmen gedacht ist, ein ausgewogenes Verhältnis zwischen Kosten und Qualität bieten. Immer mehr KMU würden die erforderlichen Investitionen in eine hochwertige IP-basierte Lösung als eine sinnvolle, lohnenswerte und langfristige Investition begreifen.

Optimale Möglichkeiten für das Monitoring auf Videowände stellt GIT in der Sonderausgabe PRO-4-PRO vom August 2016 vor (S. 74/75). Die moderne Technologie mache es möglich, den Kontrollraum und die Anzeige von Videoquellen gemeinsam mit weiteren wichtigen Informationen zu vereinfachen. Dank neuer Displaytechnologien könnten jetzt mehrere Bilder auf einem Display dargestellt werden oder sich über viele Displays erstrecken. Inhalte könnten dynamisch zugewiesen und über die Videowand im Kontrollraum bewegt werden. Es bestehe auch die Möglichkeit, PC- oder server-basierte Hardware zur Erweiterung einiger Grafikkarten zu nutzen und Software zu entwickeln, mit der die Ausgabe der Grafikkarte gesteuert wird. Virtuelle Matrix-Switches würden ganz spezielle Nachteile aufweisen. Aufgrund von Schwachstellen des Betriebssystems, Einschränkungen der Grafikkarte und begrenzter Skalierbarkeit sei diese Lösung nicht optimal. Die Netzwerk-Videomatrix von Dahua bestehe aus Embedded-Hardware, die speziell für Videowand-Lösungen konzipiert

wurde. Auf der Grundlage von Advanced Telecom Computing Architecture biete sie Redundanz für viele wichtige Teile wie Lüfter und Stromversorgung. Für die Anwendung bei zusammengesetzten Videowänden seien die Technologien LCD und DLP ausgereift. Die LED-Modultechnik trete jetzt allerdings in diesen Markt ein und sichere sich zunehmend Marktanteile. LED-Module besäßen überzeugende Vorteile, wie: keine physischen Abstände, hohe Helligkeit, hohe Bildwiederholungsfrequenz, lange Lebensdauer und einfache Wartung.

GIT zeigt in der Sonderausgabe PRO-4-PRO vom August 2016, S. 78/79, wie die **Multifocalsensor (MFS)-Technologie** die Effizienz von Videoanlagen erhöht. Die patentierte MFS-Technologie Panomera zeichne sich durch ein völlig neuartiges Objektiv- bzw. Sensor-Konzept aus, das mit mehreren Sensoren mit jeweils unterschiedlichen Brennweiten arbeite. Dadurch werde die abzusichernde Fläche „gestaffelt", sodass auch weiter entfernte Objekte mit derselben Auflösung dargestellt werden können wie Objekte im vorderen Bildbereich. Die Möglichkeit, den kompletten abzusichernden Bereich in einem zusammenhängenden Bild zu sehen und nicht zwischen zahlreichen verteilten Kameras hin und her schalten zu müssen, mache die Bedienung des Systems einfacher. Sie verkürze die Reaktionszeiten für die Einsatzkräfte. Das Kernthema der Videosicherheitstechnik habe sich deutlich gewandelt: weg von bloßer Überwachung hin zu Prozessoptimierung und Prozesssteuerung durch deutlichen Informationsgewinn mit Hilfe intelligenter und analytischer Videolösungen.

GIT berichtet in der Sonderausgabe PRO-4-PRO vom August 2016, S. 80/81, über eine neue Secvest Funkalarmanlage von ABUS. Sie böte einen weltweit einzigartigen **mechatronischen Einbruchschutz**, der den Einbrecher bereits beim Einbruchversuch abwehren könne. Der Nutzer erhalte mit der Secvest App die Möglichkeit, von überall auf der Welt seine Alarmanlage zu bedienen und Rückmeldungen zu erhalten – beispielsweise Alarmmeldungen oder Live-Videoverifikationen direkt aufs Smartphone. ABUS habe mechatronische Funkalarm-Präventionsmelder für Fenster und Türen entwickelt, die vor Einbruch schützen, ihn detektieren und melden. Während eine klassische Außenhautabsicherung nicht erkennen könne, ob Fenster oder Türen nur angelehnt oder wirklich verschlossen sind, böten alle ABUS Mechatronik-Komponenten eine Verschlussüberwachung als zusätzliches Sicherheitsfeature.

Wirtschaftskriminalität

Das BKA hat im August das **Bundeslagebild Wirtschaftskriminalität** (Wikri) für das Jahr 2015 veröffentlicht. In der PKS wurden insgesamt 60.977 Fälle registriert, 3,5 Prozent weniger als im Vorjahr und weniger als im Durchschnitt der letzten fünf Jahre (71.428). Wegen gering ausgeprägten Anzeigeverhaltens sei von einem großen Dunkelfeld auszugehen. Der Anteil der Wikri an allen polizeilich bekannt gewordenen Straftaten betrug 2015 rund ein Prozent, aber die durch Wikri verursachten Schäden (2.887 Mio. Euro) erreichten 41,3 Prozent des durch die Gesamtkriminalität verursachten erfassbaren Schadens von fast 7 Mrd. Euro. Dabei sei unstrittig, dass gerade die nicht erfassbaren und quantifizierbaren immateriellen Schäden, die durch Wikri verursacht werden, wesentliche Faktoren für die Bewertung des Schadenspotenzials seien. Die Aufklärungsquote betrug 2015 92,9 Prozent (Gesamtkriminalität 56,3 Prozent). Ursächlich hierfür ist vor allem, dass Geschädigte den Täter häufig kennen. In 9,3 Prozent der Fälle von Wikri wurde 2015 das Internet genutzt. Die Nutzung dieses Tatmittels sei damit gegenüber 2011 um mehr als die Hälfte gesunken. (Details zum Bundeslagebild Wikri 2015 auf der Webseite von Securitas – Presse – Sicherheitslage)

Wohnungseinbruch

Die FAZ weist am 2. August auf den neuen **„Einbruch-Report" des GDV** hin. Die Zahl der Wohnungseinbrüche in Deutschland steige dramatisch. Der Kriminologe Christian Pfeiffer habe Tausende Fälle ausgewertet und errechnet, dass von 100 Einbrüchen bloß 2,6 mit einer Verurteilung endeten. Damit würden 97,4 Prozent der Einbrecher geradezu ermutigt, ihre kriminellen Aktivitäten fortzusetzen. Etwas mehr als die Hälfte der rechtskräftig verurteilten Täter hätten eine ausländische Staatsangehörigkeit. Die Zunahme der Einbrüche sei vor allem auf „reisende Tätergruppen aus Ost- und Südosteuropa zurückzuführen", stellte Innenminister de Maizière fest. Umso mehr rieten Polizei und Versicherungen den Bürgern zu einer besseren Prävention durch einbruchhemmende Türen und Fenster. Für etwa 150 bis 200 Euro seien Fensterbeschläge mit sogenannter Pilzkopfverriegelung zu haben. Ein solideres Türblatt koste weniger als 1.000 Euro. Mechanische Sicherung gehe vor elektronischer Sicherung. Die staatseigene KfW-Bank vergebe zinsgünstige Darlehen für Bürger, die ihre Wohnung durch Umbauten einbruchssicherer machen wollen. Bis zu 50.000 Euro Darlehen zum Zins von 0,75 Prozent könne man beantragen oder – seit Ende 2015 – einen Zehn-Prozent-Zuschuss zu Umbaumaßnahmen von 200 bis maximal 1.500 Euro.

Zivilschutz

Das Bundeskabinett hat, wie Der Tagesspiegel am 24. August berichtet, das umstrittene **Konzept zur Zivilverteidigung** verabschiedet und damit Planungen für den Fall einer Terrorattacke oder eines Cyberangriffs auf den Weg gebracht. Die Regierung reagiere mit der neuen „Konzeption Zivile Verteidigung" auf die veränderte sicherheitspolitische Lage. Bundesinnenminister de Maizière sagte, für ihn persönlich sei „am wahrscheinlichsten ein regional oder überregional lang anhaltender" Ausfall der Stromversorgung. Er könne sich vorstellen, dass es Gruppen oder Staaten oder eine Mischung von Gruppen und Staaten gibt, die ein Interesse daran hätten, einmal auszuprobieren, wie resilient, wie anpassungsfähig die deutsche Gesellschaft ist mit Blick auf die Abhängigkeit von der Stromversorgung. Der Bund müsse außerdem eine Notversorgung mit Trinkwasser bieten – über „autarke Brunnen und Quellen in Verbindung mit einer mobilen Trinkwassernotversorgung". Eine staatliche Lebensmittelreserve gebe es bereits, die unter anderem Reis, Hülsenfrüchte, Kondensmilch und Getreide umfasst. Der Präsident des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe, Christoph Unger sagte, wichtig sei die Fähigkeit, Erste Hilfe zu leisten oder mit einem Brand selbst zurechtzukommen. Untersuchungen seines Amtes hätten gezeigt, dass es hier in der Bevölkerung deutliche Defizite gebe. In dem Konzept zur Zivilverteidigung sei auch enthalten, wie die Bürger bei besonderen Gefahrenlagen gewarnt werden können.

Zutrittskontrolle

Die Zeitschrift GIT stellt in der Sonderausgabe PRO-4-PRO vom August 2016, S. 94/95, eine flexible Lösung der Zutrittskontrolle für Unternehmen mit verteilten Standorten vor. Mit dem **AirKey** aus dem Hause EVVA habe der Filialleiter seine Filiale fest im Griff. Dazu brauche er nicht mehr als ein Smartphone, einen Internetzugang und einen AirKey-Zylinder oder Wandleser. Mit AirKey ließen sich Unternehmen mit verteilten Standorten und komplexen Strukturen sehr einfach verwalten, auch über Ländergrenzen hinweg. Die Multi-Administratoren-Fähigkeit von AirKey erlaube die Ernennung mehrerer Administratoren, die nicht nur ihren eigenen Standort selbstständig verwalten können, sondern

auch übergreifend alle anderen Standorte des Unternehmens. Gebäudeeigentümer oder -verwaltungen könnten durch Komponenten-Sharing auch Teile ihrer Schließanlage ihren Geschäfts- oder Wohnungsmietern per Knopfdruck zur Eigenverwaltung überlassen.

Wie sich **Personensperren effizient einsetzen** lassen, beschreibt Elena Dilba, Automatic Systems, in Security insight, Ausgabe 4-2016, S. 20/21. Sensorschleusen bestünden aus ein- oder zweiflügeligen Glastüren sowie einem Detektionssystem und könnten mit Kartenlesegeräten ausgestattet werden, wodurch sich höchste Flexibilität ergebe. Bei einem gewaltsamen Öffnungsversuch trete eine elektromechanische Verriegelung in Kraft. Die elektronische Erkennung erfasse beispielsweise das „Durchschlüpfen" oder den Versuch, eine zweite Person „im Huckepack" durchzuschleusen. Ein Durchlass von bis zu 60 Personen in der Minute sei sichergestellt. Zusätzlich seien die Schleusen für Geschäftsreisende mit Trolley-Koffern konzipiert. Die Kontrolle erkenne die Trolleys und verschließe die Türen nicht wieder, bevor der Reisende samt Koffer die Sperre passiert hat. Für Breite und Höhe der Personensperre böten sich zahlreiche Kombinationsmöglichkeiten an.

Die elektronische **Zutrittskontrolle per Smartphone** behandelt Markus Baba in Security insight, Ausgabe 4-2016, S. 34/35. Ein zentrales Ergebnis einer aktuellen Untersuchung von ASIS International, bei der HID Global als technischer Ratgeber fungiert habe, laute, dass bezüglich der sicheren Smartcard-Verwendung bei der Zutrittskontrolle auf Anwenderseite vielfach Unkenntnis herrsche. Nur eine Minderheit wisse, dass Kartenprüfnummern nicht verschlüsselt sind und deshalb zusätzliche Sicherheitslösungen genutzt werden müssten. Die multifunktionale Nutzung von Smartcards für unterschiedlichste Anwendungen sei kein Einzelfall mehr. 26,1 Prozent der Befragten nutzten sie sowohl bei der Zutrittskontrolle als auch für die Authentifizierung beim Zugang zu IT-Systemen wie PCs oder Applikationen. Die Card Serial Number (CSN) oder Unique ID (UID) sei als eindeutiges Identifizierungsmerkmal auf der Karte gespeichert. Über ein Drittel der Befragten habe nicht gewusst, um was es sich dabei überhaupt handelt. Und mehr als 80 Prozent hätten nicht gewusst, dass CSNs bzw. UIDs nicht verschlüsselt sind. 57,4 Prozent der Befragten würden das Sicherheitsniveau ihrer Zutrittskontrolllösung für ausreichend halten. Sicherheitsstandard sollte die Nutzung aktueller Verschlüsselungstechnologien wie kryptografische AES-128-Bit-Algorithmen sein.

Eine elektronische Zutrittslösung für das Max-Planck-Institut für Plasmaphysik (IPP) in Greifswald erläutert PROTECTOR in der Ausgabe 9-2016, S. 32/33. Sie schütze nicht nur den Bürotrakt, sondern auch die Experiment- und Montagebereiche der Kernfusionsanlage. Dabei handele es sich um ein kombiniertes online und virtuell vernetztes System, das überdies organisatorisch die Maßnahmen zur Personensicherheit unterstütze. Bei der Netzwerkverkabelung setze das IPP auf Lichtwellenleiter, um so wenig wie möglich elektromagnetische Störungen durch Streufelder zu erzeugen. Zu den Speziallösungen gehörten auch die Ansteuerung des Fluchtwegsystems an etlichen Türen sowohl von der Innen- als auch Außenseite sowie die Integration der Zeiterfassung. Das IPP setze an über 600 Zutrittspunkten die elektronische Zutrittslösung von Salto ein.

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