Focus on Security

Ausgabe 09, September 2015

SECURITAS

Inhalt

Altenheimsicherheit

Günther Ohland, Smarthome Paderborn, befasst sich in der Ausgabe 7/8-2015 der Zeitschrift PROTECTOR mit „smarter Sicherheit im Altenheim und der ambulanten Pflege" (S. 46/47). Er sieht ein **Spannungsfeld zwischen dem Einbruchschutz und der Unfallrettung**. Laut der Initiative Hausnotruf seien in deutschen Haushalten nur etwa 400.000 Hausnotrufanlagen installiert. Spezialisierte mobile Alarmsysteme oder Senioren-Tastenhandys mit Notfallknopf seien für Senioren besser geeignet. In der Küche aktivierten in Ergänzung zur Dunstabzugshaube bestimmte Kriterien auf der Herdoberfläche nicht nur die Stromabschaltung. Entdeckt der Infrarotsensor eine Flammenbildung, werde schlagartig eine Löschgaswolke auf den Herd geschossen, um die Flammen zu ersticken. Hilfreich sei auch eine Art Hotel-Kartenschalter neben der Wohnungstür. Ist die Karte gesteckt, seien die Verbraucher eingeschaltet oder einschaltbar. Wird die Karte entnommen, würden bestimmte Verbraucher automatisch stromlos geschaltet.

Ines Pettigrew, Tyco Integrated Fire & Security, befasst sich in einem Brandschutz Special der Zeitschrift PROTECTOR vom August 2015 mit dem **Brandschutz in Pflegeheimen** (S. 12/13). Pflegeheime zählten in puncto Brandschutz zu den Hochrisikozonen. Sie würden heute immer häufiger mit leicht zu reinigenden Kunststoffen ausgestattet. Für den Brandschutz bedeute dies eine Risikoerhöhung durch erhöhte Brandlast. Parallel zu den wachsenden Gefahrenquellen habe sich die Zahl der Brandschutztechnologien in den letzten 20 Jahren verdoppelt. Gerade in Pflegeheimen seien stationäre Löscheinrichtungen besonders wichtig. Hier habe sich die Liste der verfügbaren Technologien erheblich erweitert: Neben den klassischen Wasser- (Sprinkler-) und Gaslöschanlagen seien viele individuelle Sonderlösungen auf dem Markt, zum Beispiel chemische Löschgase, Schaumanwendungen sowie Sprühwasser- und Wassernebel.

Anschläge

Im Juli 2015 verübten Unbekannte mindestens zweimal Brandanschläge auf **Telekommunikations-Masten**. In der Nacht zum 29. Juli setzten sie nach einer Pressemitteilung des PP Berlin vom 29. Juli einen solchen Mast des TK-Dienstleisters Vodafone in Berlin mit sieben Autoreifen am Fuß des Mastes in Brand. Eine mögliche politische Tatmotivation werde geprüft. Nach einer Meldung des Informationsservice IBWS vom 3. August wurden während der Nacht zum 20. Juli in den Hamburger Stadtteilen Bahrenfeld und Billstedt Feuer in Kabelschächten von Mobilfunk-Masten gelegt. Die Betreiber der Installationen seien die Deutsche Telekom und O_2. Zu der Tat sei ein Selbstbezichtigungsschreiben einer „AG Laufmasche" dokumentiert. Die Verfasser würden zu weiteren Gewaltakten aufrufen.

Das Informationsbüro IBWS berichtet am 12. August über die Selbstbezichtigung eines „service champion" vom 30. Juli von Sabotagehandlungen an **Fahrkartenautomaten** im Stadtgebiet von Leipzig am 29. Juli. Als Motive werden die Erhöhung von Ticketpreisen und die Forderung eines kostenlosen Nahverkehrs angegeben. Es werden vor allem bestimmte Linien und Tarifzonen benannt. Unter der Überschrift „doch jeder kann etwas unternehmen" werden Tipps für Anschläge und für taktisches Verhalten bei der Fahrscheinkontrolle gegeben.

Am 6. August wurden von drei schwarz gekleideten Personen auf dem frei zugänglichen Gelände der Firma **Purivent System GmbH** in Leipzig acht Fenster eingeschlagen. Das Gebäude sowie ein in der Nähe geparktes Firmenfahrzeug des Sicherheitsdienstleisters **WIS** wurden mit Buttersäure beschädigt.

Bei der Wohnungsdurchsuchung von sechs Tatverdächtigen seien brennbare Flüssigkeiten, eine Vielzahl von Mobiltelefonen und Propagandamaterial gefunden worden. Nach einem Selbstbezichtigungsschreiben auf einer Internetseite von „linksunten.indymedia.org" sollte mit der Sachbeschädigung „auf die sich drastisch zuspitzende rassistische Stimmung in Deutschland aufmerksam gemacht" werden (BKA-Wochenlage vom 14. August).

Autohaussicherheit

Im Newsletter von GIT-SICHERHEIT.de vom 31. Juli nimmt Wolfgang Neuscheler, öffentlich bestellter und vereidigter Sachverständiger, zur möglichen Sicherung von Autohäusern Stellung. Er betont die Wirksamkeitsgrenzen von mechanischen Sicherungen, von Videoüberwachung mit Videoanalysen und Wärmebildkameras sowie Kamera-Attrappen und von Überwachung durch Kontrollgänge. Ein vorbeugendes Sicherheitskonzept gegen Autodiebstahl sollte ein ausgewogenes Kosten/Nutzen-Verhältnis beachten – allerdings unter der Vorgabe, dass ein Autohausgelände für den Publikumsverkehr frei zugänglich sein muss. Gleichzeitig sollten die Autos auf dem freien Gelände vor Vandalismus, Teilediebstahl sowie vor Fahrzeugdiebstahl gesichert sein. Hierbei helfe ein Sicherheitskonzept, das individuell eine Risiko-, Schwachstellen- und Sicherheitsanalyse vornimmt.

Bahnsicherheit

Nach dem vereitelten Attentat in einem Thalys-Zug steige der Druck auf die EU-Staaten, mehr für die Sicherheit im internationalen Bahnverkehr zu tun, meldet n-tv.de am 25. August. Es gebe dafür mehrere Möglichkeiten, unter anderem das systematische Durchleuchten von Fahrgastdaten oder den Einbau von Überwachungskameras an Bord. Europa würde damit Neuland betreten. Bisher gebe es – anders als für die Luft- und Schifffahrt – keine gemeinsame Gesetzgebung zu Sicherheitsmaßnahmen im Schienenverkehr. Auch innerhalb des Schengen-Gebiets für den freien Reiseverkehr seien bei Zügen Sicherheitsüberprüfungen möglich. Es dürften jedoch nicht Pässe oder Ausweise wie bei klassischen Grenzkontrollen überprüft werden.

Am 31. August meldet die FAZ, Innen- und Verkehrsminister neun europäischer Länder – darunter auch Deutschlands – hätten sich auf **verstärkte Sicherheitsvorkehrungen für den Bahnverkehr** verständigt. Auf internationalen Strecken solle es künftig zusätzliche Personen- und Gepäckkontrollen geben. Geplant seien außerdem multinationale Polizeipatrouillen in den Zügen und personengebundene Fahrscheine. Über die Möglichkeit personengebundener Bahnfahrkarten in Hochgeschwindigkeitszügen solle ein Gutachten eingeholt werden. Ein von der EU-Kommission ausgearbeiteter Vorschlagskatalog über Videoüberwachung in Hochgeschwindigkeitszügen sowie Ganzkörperscans für Bahnreisende habe laut Verkehrsminister Dobrindt nicht zur Debatte gestanden.

Betrug

Mit Insiderwissen sollen Hacker und Händler amerikanischen Behörden zufolge rund 100 Mio. Dollar erbeutet haben, berichtet die FAZ am 13. August. Die Gruppe mit mehr als 30 Mitgliedern könnte in den vergangenen fünf Jahren mehr als 150.000 Pressemitteilungen mit relevanten Unternehmensnachrichten gestohlen haben, bevor diese über Fachdienste wie Business Wire oder PR Newswire an Investoren verschickt wurden. Dann betrieben sie offenbar systematisch Insiderhandel. Und stets sollen die Hacker und Händler ihre Taten in nur wenigen Stunden, manchmal nur in wenigen Minuten, begangen haben.

Brandschutz

Die Zeitschrift PROTECTOR befasst sich in einem Brandschutz Special vom August 2015 mit einer Fülle von Brandschutzthemen. Dipl.-Ing. Jürgen Siewert, BHE, erläutert die **Muster-Industriebaurichtlinie 2014** (S. 6/7), deren Ziel es sei, die Mindestanforderungen an den Brandschutz von Industriebauten zu regeln. Besonderes Augenmerk werde auf die Entrauchung, die Rauchableitung und den Rauchabzug gelegt. Der Begriff „Geschoss" sei präzisiert und neu als „Ebene" definiert. In sieben Punkten erläutert der Autor die Anforderungen nach der Richtlinie. Im Gegensatz zu Rauch- und Wärmeabzugsanlagen (RWA) werde die Brandmeldeanlage (BMA) in der neuen Richtlinie stiefmütterlich behandelt.

In demselben Special geht Joachim Meisehen, Novar GmbH a Honeywell Company, der Frage nach, **wann Rauchmelder getauscht werden müssen** (S. 8/9). Auch wenn inzwischen hochwertige Melder mit mikroprozessorgesteuerter Messwertnachführung Störgrößen erkennen und bis zu einem gewissen Grad kompensieren können, sei auch deren Lebensdauer begrenzt. Die DIN 14675 schreibe vor, dass für baurechtlich geforderte BMA ein Austausch punktförmiger Rauchmelder in definierten Zeiträumen zu erfolgen hat. Punkt- oder linienförmige Wärmemelder unterlägen hingegen keinen Tauschfristen. Um als Errichter im Schadensfall nicht in Haftung genommen zu werden, ließen diese inzwischen häufig vom Bauherrn eine Haftungsfreistellung unterzeichnen. Moderne Rauchmelder mit automatischer Verschmutzungskompensation und Ruhewertnachführung könnten die Belastungen, die sich im Laufe der Betriebszeit ergeben, mikroprozessorgesteuert ausgleichen und daher bis zu acht Jahre in Betrieb bleiben. Grundsätzlich sollte sich der Betreiber einer BMA von einem qualifizierten Fachbetrieb beraten lassen.

Patrick Banholzer, Hekatron Vertriebs GmbH, behandelt in dem Brandschutz Spezial **Trends in der Brandmeldetechnik** (S. 20/21). Drei Aspekte seien aus heutiger Sicht besonders prominent: die zunehmende Verbreitung des Fernzugriffs, eine immer smarter werdende Anwendersoftware sowie eine objektspezifische Alarmierung. Errichter hätten heute die Möglichkeit, mit Software zu arbeiten, die auf Basis eines integrierten Ereignisspeichers automatisch Inspektions- und Wartungsprotokolle inklusive Datum und Anzahl der Auslösungen liefert. Mit der Alarmierung über die Ringleitung habe sich ein Quasi-Standard herausgebildet. Vorteil: Sie komme mit einer einzigen Leitung aus. Als Alternative bei großen Alarmierungsanlagen gebe es das Einbinden von „Alarmboxen" in die Ringleitung.

Dr. Oliver Linden, Wagner Group GmbH, berichtet in dem Brandschutz Spezial über **aktuelle Technologien gegen Täuschungsalarme** (S. 22/23), und zwar über technische Maßnahmen (Zweimeldungsabhängigkeit, Brandmustererkennung und Mehrkriterienauswertung), über Driftkompensation (die Alarmschwelle wird dabei im Rahmen normativ vorgegebener Grenzen an die Veränderung des Ruhewertes angepasst), Störabstand, physikalische Staubfilterung und Sammeleffekt. Die Implementierung der technischen Maßnahmen in punktförmigen Brandmeldern sei sehr kostenintensiv, da der hohe technologische Aufwand für jeden Detektionspunkt einzeln betrieben werden müsse. Ansaugrauchmelder böten hier eine kostengünstige Variante, da es sich dabei um zentrale Systeme handele, mit denen Dutzende von Detektionspunkten abgedeckt werden können. Ansaugrauchmelder böten weitere Vorteile für den Einsatz in kritischen Umgebungsbedingungen, wie die Immunität gegen elektromagnetische und radioaktive Strahlung bei Installation des Detektors außerhalb des Überwachungsbereichs, die Abscheidung von Kondenswasser zur Verhinderung von Fehlfunktionen und Melderdefekten.

In derselben Ausgabe behandelt Matthias Glock, Panasonic Deutschland, **intelligente Multimelder** (S. 24/25). Der Multimelder könne fünf unterschiedliche Zustände unterscheiden: normaler Raum (Büro/Lager), sauberer Raum (Büro/Reinraum), Hitze (Heizungskeller), Rauch/Dampf (Raucherraum), erschwerte Bedingungen (Küche/Schweißen). Diese Zustände würden in einer Lernphase von circa einer Woche anhand der Umgebungsbedingungen erlernt. Ändern sich nun im Laufe der Zeit die Umgebungsbedingungen, passe sich der Melder eigenständig den neuen Bedingungen wieder an. Dabei werde eine geringere Empfindlichkeit langsamer und eine höhere Empfindlichkeit schneller angepasst. Das vom VdS anerkannte Verfahren unterscheide sich durch ein extrem engmaschiges Metallnetz, das es mit einem Lochdurchmesser von gerade einmal 0,3 mm Kleinstinsekten und Staub unmöglich mache, in die Melderkammer zu gelangen. Dadurch könne die Fehlalarmquote deutlich gesenkt werden.

Sonja Ewers, UTC Building & Industrial Systems, beschreibt in dem Brandschutz Spezial den **Einsatz stationärer und mobiler Löschsysteme** (S. 26/27). Ein ganzheitliches Brandschutzkonzept zeichne sich durch Maßnahmen aus, die den jeweiligen Herausforderungen angepasst werden sowie sämtliche für den Brandschutz relevanten Gewerke mit einbeziehen. Ob in IT-Bereichen Wassernebel-Technologien wie das Marioff Hochdruck-Wassernebelsystem, Hi-Fog oder das Löschgas Novec 1230 eingesetzt wird, hänge ganz vom Kundenwunsch ab. Häufig sei das zu schützende Raumvolumen für die Wahl des Löschmittels relevant.

Intelligente Entrauchungskonzepte behandelt in dem Brandschutz Spezial Harald Rudelgaß, Systemair GmbH (S. 30/31). Um bei technischen Brandschutzmaßnahmen die Bau- und Betriebskosten signifikant reduzieren zu können, habe Systemair speziell für die Entrauchung neue Lösungsansätze entwickelt. Dazu zählten: elektronisch geregelte Differenzdruckanlagen als Alternative zu mechanisch geregelten Rauch-Druckanlagen in Sicherheitstreppenhäusern, Jet-Ventilatoren in Tiefgaragen und Parkhäusern statt der üblichen, kanalgebundenen Entrauchung und Entlüftung sowie der Einsatz von EC-Motoren in Anlagen, die im Brandfall wirkungsvoll entrauchen, im Normalfall aber der dem Komfort steigernden Raumentlüftung dienen.

Wulf Statz, Vollmer Brandschutzservice GmbH & Co. KG, plädiert in dem Brandschutz Spezial für die **Brandschutzunterweisung** (S. 32/33). Als Basisinhalte einer Brandschutzunterweisung bezeichnet er: Brandgefahren am Arbeitsplatz, Umgang mit Zündquellen, Maßnahmen zur Abwendung von Brandgefährdungen, Maßnahmen gegen Entstehungsbrände und Explosionen, Verhalten im Brandfall und Flucht- und Rettungswege.

Das Brandschutz Spezial der Zeitschrift PROTECTOR vom August 2015 enthält **Marktübersichten** zu:

- 63 Brandmeldesystemen von 31 Anbietern mit Angaben zu Zertifizierungen, zum Systemaufbau und der Programmierung
- Brandmeldern von 46 Anbietern (Streulichtrauchmelder, Mehrfachsensor-Rauchmelder, linienförmige Rauchmelder, Ansaugrauchmelder, Wärmedifferenzialmelder, Wärmemaximalmelder und IR-Flammenmelder)
- 67 Löschsystemen von 25 Anbietern
- 51 Rauch- und Wärmeabzugsanlagen von 20 Anbietern mit Angaben zur Produkteinordnung, zu Zertifizierungen, der maximalen Anzahl von RWA-Gruppen und der Betriebsdauer mit Batterie (S. 34–39).

Matthias Siebenborn, KRIWAN Testzentrum GmbH & Co. KG, stellt in der Ausgabe 4-2015 der Zeitschrift WiK (S. 68/69) die **Ferninspektion von Rauchwarnmeldern** der Sichtprüfung gegenüber. Zur Klärung des schon Jahre dauernden Expertendissens solle eine Studie Fakten zur Vergleichbarkeit beider Methoden liefern. Unter der Leitung

des KRIWAN-Testzentrums habe sich ein Arbeitskreis gebildet, dessen Ziel es sei, eine Richtlinie für RWM zu erarbeiten, die die funktionale Wirksamkeit beider Inspektionsverfahren im Hinblick auf die Anforderungen aus der DIN 14676 und eventuell darüber hinausgehender Anforderungen bewertbar machen soll. Die WiK-Redaktion weist auf ein Gutachten des TÜV Rheinland aus dem Jahr 2012 hin (S. 70). Es nenne unter anderem folgende Bedingungen: Ausrüstung des RWM mit technischen Funktionen, die die Kontrollen nach der DIN-Norm ermöglichen; Melder-Montage durch geschulte Fachkräfte; vertragliche Verpflichtung des Vermieters, den RWM-Dienstleister bei baulichen Änderungen oder geänderter Raumnutzung schriftlich zu informieren; monatliches automatisches Prüfintervall; Überprüfung durch den Dienstleister mindestens jährlich.

Frank D. Stolt befasst sich in veko-online.de am 7. August mit **Bränden im Hotel**. Deutschland habe im Vergleich zu anderen Ländern ein niedriges Brandschutzniveau. Bei Brandermittlungen nach Hotelbränden stelle sich immer wieder heraus, dass der bauliche und anlagentechnische Brandschutz gut bis hervorragend war. Allerdings werde beim organisatorischen Brandschutz „gesündigt": verkeilte oder festgebundene Brandschutztüren, Durchbrüche in Wänden oder Decken sowie unzureichende Schulung des Personals. Ein Beispiel für zusätzliche Sicherheit sei das Projekt „SAFEHOTEL". Schon vor einigen Jahren hätten engagierte Feuerwehrvertreter aus europäischen Ländern gemeinsam mit einem Touristikunternehmen, einer Hotelkette und zwei Universitäten eine Initiative für ein interaktives Brandschutztraining von Hotelpersonal gestartet: SAFEHOTEL. Daraus sei zwischenzeitlich „Sicherheits-Qualitätssiegel für Hotels" geworden. Voraussetzung für die Aushändigung des Siegels sei eine freiwillige Überprüfung durch Feuerwehren oder sonstige Fachleute des vorbeugenden Brandschutzes, die national/international akkreditiert sind.

Cloud Computing

Silicon.de weist am 4. August auf eine aktuelle Studie „Sicherheit und Datenschutz 2015" der Nationalen Initiative für Informations- und Internet-Sicherheit e.V. (NIFIS) hin, nach der das Misstrauen deutscher Anwender in die Services von großen US-Anbietern in den vergangenen Monaten deutlich gestiegen zu sein scheine. So sollen inzwischen 90 Prozent der deutschen Unternehmen die Cloud-Dienstleister im Vorfeld sehr genau analysieren. Es zeige sich auch, dass viele Anwender den US-Angeboten misstrauen. So seien rund 80 Prozent der deutschen Unternehmen überzeugt, dass lediglich die Cloud-Anbieter einen hinreichenden Schutz für Daten gewährleisten könnten, die strengen Datenschutzgesetzen unterliegen.

Corporate Security Officer (CSO)

Wie die Zeitschrift WiK in der Ausgabe 4-2015 berichtet (S. 45/46) haben der VSW NW, die EBS Executive Education Egon Zehnder und die Horvath Akademie mit dem „Kompetenzatlas für den modernen CSO" ein **zukunftsgerichtetes Kompetenzmodell** veröffentlicht. Für die einzelnen Kompetenzen lege der Atlas die SOLL-Anforderungen an den modernen CSO als Business Manager fest. Insbesondere in den folgenden vier Kernaspekten attestiere der Atlas Kernfähigkeiten eines CSO als Business Manager: Kommunikation; Kollaboration und Netzwerken; strategische Steuerung und flexibles Handeln; unternehmerisches Denken.

Datenschutz

Das vorrangige Ziel des Datenschutzes sei nicht der Täterschutz, heißt es in der Begrün-

dung einer Entscheidung des LAG Köln (2 Sa 181/14). Ein Arbeitgeber hatte die Dateneingaben einer Arbeitnehmerin ausgewertet, weil er Zweifel an der Richtigkeit der angeblich im Homeoffice gearbeiteten Stunden gehabt habe. Dabei habe sich herausgestellt, dass die Arbeitnehmerin deutlich zu viele Stunden eingegeben hatte. Zwar habe der Arbeitgeber bei der Auswertung der IT-Systeme den Betriebsrat nicht wie gesetzlich vorgeschrieben beteiligt. Dennoch dürfe sich der Arbeitgeber vor Gericht auf solche **mitbestimmungswidrig erhobenen Daten** nach der Rechtsprechung des BAG berufen, denn er konnte das Auswerten seiner IT-Systeme im speziellen Fall gut begründen. Danach sei die Kontrolle verhältnismäßig gewesen. In einem solchen Fall überwiege das Aufklärungsinteresse das Persönlichkeitsrecht der Arbeitnehmerin.

US-Firmen wollen Datenschutz im **Internet der Dinge** stärken, berichtet heise.de am 13. August. Vernetzte Geräte wie Thermostate oder Smart-TV seien als Datenschleudern verschrien, die ihre Nutzer ausspähen. Schuld daran seien teils undurchsichtige Richtlinien der Hersteller zum Absichern der Privatsphäre der Anwender. Ändern wolle dies die Online Trust Alliance. Das Bündnis habe jetzt einen Entwurf für einen Selbstregulierungsrahmen veröffentlicht, mit dem der Datenschutz im Internet der Dinge verbessert werden solle. Die Verfasser der 23 Empfehlungen für neue Mindeststandards wollten die Sicherheitsanforderungen an Gerätehersteller deutlich nach oben schrauben. So sollten sie auch bei Verbindungen zu mobilen Gadgets oder zur Cloud auf Ende-zu-Ende-Verschlüsselung setzen und vergleichsweise strenge Passwortregeln beachten. Weiter sollten sich Produzenten und Dienstleister verpflichten, Sicherheitsupdates baldmöglichst einzuspielen. Eine Datenweitergabe an Dritte solle begrenzt, Nutzer müssten über eventuelle Sicherheitspannen rasch aufgeklärt werden.

Gartner warnt CIOs vor dem neuen **Datenschutz in Russland**, berichtet silicon.de am 17. August. Am 1. September trete ein neues russisches Gesetz in Kraft, das den Schutz personenbezogener Daten neu regele. Damit folge Russland dem Beispiel Deutschlands und schreibe darin vor, dass sämtliche personenbezogenen Daten russischer Bürger in Russland gespeichert und verarbeitet werden müssen. Das Gesetz gelte offenbar für alle Unternehmen mit einer selbstständigen Niederlassung in Russland. Ausgenommen sollten laut dem Text aber Mitarbeiter von ausländischen Unternehmen sein.

Datensicherheit

Norbert Wulst, Dica Technologies GmbH, geht in der Zeitschrift PROTECTOR, Ausgabe 7/8-2015, S. 40/41, der Frage nach, was sich in den zwei Jahren nach der Veröffentlichung streng geheimer Informationen durch Snowden in Sachen Verschlüsselung und sicherer digitaler Kommunikation getan hat. Alle mit Standardverfahren verschlüsselten Daten könnten mit den Methoden der Geheimdienste decodiert werden. Dabei gebe es durchaus Lösungen für eine sichere Kommunikation: für die einfache Kommunikation zwischen zwei Kommunikationspartnern etwa weiter entwickelte PGP-Verschlüsselungsverfahren wie Scryptguard. Wichtigstes Merkmal sei bei dieser Lösung die **Dezentralisierung der Schlüsselverwaltung**. Die Möglichkeit, bei Kenntnis des Algorithmus jeden Schlüssel zu probieren, könne eliminiert werden, wenn zum Beispiel das One Time Pad-Verfahren eingesetzt wird. Dabei würden Einmalschlüssel in der Länge der Klarschrift mit dieser über das exklusive Oder (XOR) verknüpft. Unter der Voraussetzung, dass der als Schlüssel verwendete Zufallstext die entsprechende Güte hat, sei dieses Verfahren von niemandem zu decodieren. Die Kunst liege darin, den Schlüssel zum Dechiffrieren der Nachricht sicher zum Empfänger zu bringen.

Diebstahl

Das LKA Rheinland-Pfalz warnt in einer Medieninformation vom 12. August vor Diebstählen hochwertiger Pkw, die mit sogenannten **Keyless Entry-Systemen** ausgestattet sind. Die Fahrzeuge seien vermutlich unter Zuhilfenahme von sogenannten „Funkwellen-Verlängerern" entwendet worden. Diese Geräte bestünden aus zwei Teilen, dem „Car-Scanner" und dem „Key-Scanner". Das Prinzip der Funkwellen-Verlängerer beruhe auf der Verlängerung der Signale, die zwischen dem Fahrzeug und dem Fahrzeugschlüssel ausgetauscht werden. In der Praxis sehe das Vorgehen der Täter wie folgt aus: Einer steht mit einem Car-Scanner in der Tasche am Fahrzeug und ein weiterer Täter mit einem Scanner in der Nähe der Haustür, da viele Autofahrer ihren Autoschlüssel in der Nähe der Haustür aufbewahren. Die Verlängerer passten in eine handelsübliche Aktentasche. Das LKA Rheinland-Pfalz gibt eine Reihe von Ratschlägen, insbesondere, den Fahrzeugschlüssel nicht in der Nähe von Eingangstüren, Fenstern usw. abzulegen, sondern möglichst in einem Schlüsseltresor aus Metall, um die „Abstrahlungssicherheit" zu gewährleisten.

Drohnen

In der Ausgabe 4-2015 der Zeitschrift WiK beschreiben Autoren der LUCIUS Consulting GbR erste **Ansätze für eine erfolgreiche Drohnenabwehr** (S. 24–28). Sie skizzieren Bedrohungspotenziale sowie Abwehr- und Gegenmaßnahmen. Insgesamt gebe es keine Pauschallösung zum Schutz von Unternehmen gegen eine UAV (unmanned air vehicle)-Bedrohung. Eine allumfassende technische Lösung sei derzeit nicht verfügbar. Eine effektive UAV-Abwehr sei immer von mehreren Faktoren abhängig: von der jeweiligen Stufe der UAV-Bedrohung, den Gegebenheiten vor Ort, den zu schützenden Gütern und den einsetzbaren Mitteln. Die passgenaue detaillierte Analyse der UAV-Bedrohungslage und die Planung, Konzeption und Abwägung der Möglichkeiten sowie der zielgerichtete Einsatz der eigenen Mittel seien die wesentlichen Schlüsselfaktoren für eine umfassende und erfolgreiche UAV-Abwehr.

Nach einer Pressemitteilung der PD Limburg-Weilburg wurde die Landung eines Rettungshubschraubers in Elbtal-Dorchheim durch eine privat genutzte Drohne gestört, sodass der Rettungshubschrauber auf einen anderen Landeplatz ausweichen musste.

Einzelhandelssicherheit

Wie veko-online.de am 7. August berichtet, gaben die Teilnehmer der Umfrage **„Videoüberwachungssysteme im Einzelhandel 2015"** erstmals die Reduzierung der Gesamtbetriebskosten als einen der ausschlaggebenden Gründe an, in ein IP-Videosicherheitssystem zu investieren. Rund 84 Prozent der Teilnehmer bestätigten diesen Trend und planten im Vergleich zum Vorjahr ein konstant hohes oder erhöhtes Budget für Videoüberwachung ein. Insgesamt 43,4 Prozent der Händler – und damit 8 Prozent mehr als 2014 – überwachten die Vorgänge in ihrem Warenlager mit Hilfe von Kameras.

Endgerätesicherheit

Auf Basis der Ergebnisse einer Befragung von IT-Verantwortlichen nach dem Umgang mit Smartphones und Tablets und dabei auftretenden Sicherheitsproblemen gibt das Marktforschungsunternehmen IDC Empfehlungen, meldet TECCHANNEL.de am 24. August: 1. Betrachten Sie Mobile Security nicht isoliert, sondern als wichtigen Teil Ihres IT-Sicherheitskonzepts. 2. Finden Sie die richtige

Balance aus Produktivität und Sicherheit. 3. Sensibilisieren Sie Anwender für die Risiken im Umgang mit mobiler IT. 4. Verschaffen Sie sich Transparenz in einem unübersichtlichen Markt. 5. Holen Sie sich externe Unterstützung. 6. Setzen Sie sich mit den Auswirkungen von Wearables auf Ihre IT-Sicherheit auseinander.

Fälschung von Zahlungskarten

Das LG Hannover verurteilte am 24. Juli einen rumänischen Staatsangehörigen wegen gewerbs- und bandenmäßiger Fälschung von Zahlungskarten. Der Verurteilte war Mitglied einer arbeitsteilig operierenden Tätergruppe und hatte als Techniker die Aufgabe, die Skimmingtechnik zum Auslesen der Kartendaten in die Point of Sale-Terminals in Bau- und Supermärkten in Deutschland einzubringen. Der hierbei entstandene Gesamtschaden durch Barabhebungen mittels der hergestellten Kartendubletten an Geldautomaten in den USA und in Mexiko belaufe sich auf 3,4 Mio. Euro. Das sei etwa ein Drittel des Gesamtschadens von ca. zehn Mio. Euro, der 2011/2012 durch Manipulationen von POS-Terminals deutscher Supermärkte/Baumärkte entstanden war (BKA-Wochenlage vom 14. August).

Fluchtwegsicherung

Ingo Hahn, Teckentrup GmbH & Co. KG, behandelt in einem Brandschutz Spezial der Zeitschrift PROTECTOR vom August 2015 Anforderungen an **Türen auf Fluchtwegen** (S. 14–17). Die Planung attraktiv gestalteter, sicherer Fluchtwege sei eine komplexe Aufgabe. Einfacher werde die Wahl durch moderne Baukasten-Systeme. Bei Hinterausgängen im Handel gelte sowohl die Anforderung „immer zu öffnen", als auch „immer geschlossen". Bei Türen in Fluchtwegen gelte das Gebot der Schwellenfreiheit. Weitere gesetzliche Vorschriften würden vom Gebäudetyp abhängen. Bei der Wahl der Beschläge kämen nur Drücker/Schloss-Kombinationen beziehungsweise Panikstangen-Schlösser infrage, die als geprüfte Einheit zugelassen sind. Besonders elegant seien „Pushbars": Sie laufen über die gesamte Türbreite, stünden aber im Gegensatz zu den sonst üblichen Stangengriffen rund ein Drittel weniger in den Raum. Bei Außentüren würden selbstverriegelnde Anti-Panikschlösser (SVP) höheren Einbruchschutz bieten bis zur Widerstandsklasse 4. Derart ausgestattete Türen ließen sich von innen einfach über den Türdrücker öffnen, schlössen dann selbsttätig und verriegelten sofort. Für Gebäudeteile, die zugleich Fluchtweg sind und nur von ausgewählten Mitarbeitern genutzt werden, gebe es Zugangskontrolle mit Fluchtweg-Terminal. Im Notfall könne eine Scheibe am Terminal eingeschlagen werden. Damit viele Feuerschutzabschlüsse im Normalbetrieb offen stehen, kämen Feststellanlagen mit autarker Rauch-/Brand-Erkennung zum Einsatz, die die Flügel im Notfall selbstständig schließen. Der Einsatz von Technik steige: Einbindung in das Facility Management über Bus-Systeme, Zugangskontrolle mit Chip oder Iris-Kennung, Antipanik-Schlösser mit Mehrfachverriegelung erweiterten die Variabilität und Individualisierung der nutzerabhängigen Fluchtwegplanung.

In demselben Brandschutz Spezial erläutert Martin Grell, GfS-Gesellschaft für Sicherheitstechnik mbH, die **Sicherung von Notausgangstüren** (S. 18/19). Um Notausgangstüren und Paniktüren gegen missbräuchliche Begehung zu sichern, sei die einzig sinnvolle, gesetzeskonforme Möglichkeit die Installation von Alarmgebern, die eine Hemmschwelle gegen die missbräuchliche Nutzung darstellen. Ist eine Tür gemäß der EN 179 ausgestattet, so empfehle sich die Fluchtwegsicherung zum Beispiel mit einem EH-Türwächter: Beim Herunterdrücken der Türklinke verschiebt sich der EH-Türwächter

senkrecht nach unten, die Tür geht auf. Sei eine Tür gemäß EN 1125 ausgestattet, so ist eine Druckstange mit integriertem Alarm eine geeignete Möglichkeit, den Fluchtweg abzusichern.

Das Brandschutz Spezial von PROTECTOR vom August 2015 enthält eine **Marktübersicht** über 32 Fluchtwegsicherungssysteme von 15 Anbietern (S. 42/43). Angegeben sind u. a. Bauweise und Funktionen.

Gefährdungshinweise Ukraine

Jona Martin Ruso, Result Group GmbH, gibt in der Ausgabe 2-2015 der Zeitschrift WiK Hinweise für Reisen in die Ukraine (S. 20–22). Reisen und geschäftliche Aktivitäten in den Kriegsgebieten sollten aufgrund der extremen Risiken bis auf Weiteres unterbleiben. Für Reisen in andere Gebiete der Ukraine werden unter anderem empfohlen: aufgrund der oft widrigen Straßenbedingungen sollte für Autofahrten ein einheimischer Fahrer engagiert werden; Fotografien von Regierungsgebäuden und Militäreinrichtungen sind verboten; Kreditkartenbetrug sei relativ häufig; die Einbruchsraten in Hotels und abgestellte Autos seien hoch; die aktuelle Lage sollte über Medien und staatliche Quellen mit professioneller Unterstützung verfolgt werden.

IT-Sicherheit

Im Umgang mit dem neuen Microsoft-Betriebssystem **Windows 10** sollten Nutzer vorsichtig sein, meint zeit.de am 10. August. Es verwandle den Computer „in eine Art private Abhöranlage". Wer die Datenschutzbestimmungen akzeptiere, willige in „eine umfassende Ausforschung" der Nutzung ein. Die Auswertung durch Microsoft gehe über Daten wie Name, Adresse, Alter, Geschlecht und Telefonnummer hinaus. Ermittelt würden demnach auch der Standort des Geräts, in den unternehmenseigenen Diensten aufgerufene Websites, genutzte Suchbegriffe, Kontakte zu anderen Personen und gekaufte Artikel. Die Verbraucherzentrale Rheinland-Pfalz rate Nutzern, die zusätzliche Datenübertragungen an Microsoft nicht wünschen, die Datenschutzeinstellungen anzupassen. Es sei nicht nötig, ein Microsoft-Konto einzurichten, über das Einstellungen und Dokumente im Internet gespeichert werden.

Umgebungsgeräusche als zweites Identifizierungsmerkmal stellt spiegel.de am 17. August vor. Wem Sicherheit wirklich wichtig ist, der verlasse sich beim Einloggen nicht allein auf gute Passwörter, sondern lieber auf einen zusätzlichen Schutz, die sogenannte Zweifaktor-Authentifizierung. Die Sicherheit werde dadurch deutlich erhöht, doch der Komfort leide. Man müsse zum Beispiel immer erst auf die Zusendung des Zugangscodes warten: Steckt man in einem Funkloch, habe man ein Problem. Schweizer Forscher vom Institute of Information Security an der ETH Zürich wollten die Zweifaktor-Technik nun leichter bedienbar und schneller machen. Auf dem Usenix Security Symposium in Washington hätten sie Sound-Proof vorgestellt, ein System, das Umgebungsgeräusche als zweites Identifizierungsmerkmal auswertet. Alles laufe automatisch. Sogar wenn das Mobiltelefon in einem Rucksack steckt, gelinge es, die Umgebungsgeräusche abzugleichen. Das Technikportal „Wired" glaube trotzdem nicht an eine 100-prozentige Sicherheit von Sound-Proof. Ein gewiefter Hacker müsste seinem Opfer im Grunde nur lange genug folgen, nachdem er dessen Passwort erbeutet hat. Schließlich würde es ausreichen, sich im selben Raum wie die Zielperson zu befinden. Würde der Hacker dann das gestohlene Passwort in sein Notebook eintippen, würde dieses vom nahen Handy des Opfers bestätigt.

Nutzer von **iPhones** im Firmenumfeld müssen sich vor einer Schwachstelle in Acht

nehmen, meldet heise.de am 24. August. Über die Lücke in Apples Mobile Device Management könnten Angreifer Firmendaten, wie etwa Benutzernamen und Passwörter, auslesen. Eine Aktualisierung auf iOS 8.4.1 schließe die Schwachstelle.

IuK-Kriminalität

TECCHANNEL.de befasst sich am 13. August mit der **Abwehr von DDoS-Angriffen**. Bevor man sich für eine Lösung zum Schutz vor DDoS-Angriffen entscheidet, sollte man den Schutzbedarf des Unternehmens analysieren. Entscheidend sei dabei, welche über das Internet erreichbaren Systeme das Unternehmen einsetzt, wie kritisch die dazugehörigen Geschäftsprozesse sind und welche Auswirkungen ihr Ausfall hätte. Ein durch eine DDoS-Attacke verursachter System- oder Netzausfall dauere durchschnittlich zwölf Stunden. Um sich gegen DDoS-Angriffe abzusichern, benötige man einen Schutz im Internetzugang, der den Angriffs-Traffic filtert und nur „saubere" Daten weiterleitet. Je nach Schutzbedarf würden sich hier die Varianten „On-Premise" oder „in the Cloud" empfehlen. Am sichersten sei eine Lösung, die beide Varianten kombiniert. Bei On-Premise werde eine Appliance im Internetzugang installiert – entweder direkt im Unternehmen oder im Backbone des Providers. Mit der Variante „in the Cloud" ließen sich Angriffe möglichst nah an ihrem Ausgangspunkt abfangen. Wie in vielen Bereichen gelte auch beim Thema DDoS: Die Implementierung entsprechender Sicherheitsmaßnahmen sei ein Prozess. Es reiche nicht, eine passende Lösung zu implementieren, sie müsse auch in entsprechende Notfallpläne wie Incident Response und BCM integriert werden. Man solle dabei nicht nur an die IT-Abteilung denken. Auch die Pressestelle und je nach Art des Unternehmens weitere Abteilungen benötigten einen Notfallplan. Der Notfall müsse in regelmäßigen Abständen geprobt werden. Nach einem überstandenen Angriff müsse dafür gesorgt werden, dass alle Verantwortlichen die Situation gründlich reflektieren und daraus Handlungsanweisungen für eventuelle künftige Angriffe ableiten. Wichtig sei auch, die eigenen Mitarbeiter entsprechend aufzuklären und ihr Bewusstsein für die Gefahren von DDoS-Angriffen zu schärfen.

Der **Computervirus „Dridex"** ist momentan besonders in Deutschland aktiv, meldet TECCHANNEL.de am 1. August. Experten zufolge seien hierzulande bereits sechs von zehn Computern in Unternehmen mit dem gefährlichen Trojaner infiziert. Und bald könnten es erheblich mehr sein, denn der Banking-Trojaner verbreite sich über präparierte Word- oder pdf-Anhänge. Wird der Anhang geöffnet, installiere sich die Schadsoftware automatisch auf dem Computer, sofern dieser mit dem Internet verbunden ist. Das Besorgniserregende an Dridex sei, dass er erschreckend präzise arbeitet. Sobald der befallene Computer eine Banking-Seite öffnet, greife er in den Datenstrom ein und ändere die legitime Bankseite. Er werde ständig weiterentwickelt. Er nutzte in jüngster Zeit die Makro-Funktionen von Microsoft Office. Laut einem Bericht von IBM habe Dridex im letzten Jahr vor allem Online-Banking-Konten von Unternehmen ins Visier genommen. Zusätzlich zu bereits bestehenden Soft- oder Hardware-basierenden Schutzmaßnahmen sollten Mitarbeiter, deren Office-Versionen aus dem Jahr 2010 oder früher stammen, in den Sicherheitseinstellungen die Makro-Funktion deaktivieren und nur in bekannten Fällen aktivieren.

Die aktuelle **KPMG-Studie „Computerkriminalität 2015",** für die Führungskräfte aus 500 deutschen Unternehmen unterschiedlicher Größen und Branchen befragt worden seien, habe ergeben, dass 40 Prozent der Unternehmen in den vergangenen zwei Jahren Opfer von Computerkriminalität geworden seien (2013: 27 Prozent), meldet WiK in der Ausgabe 4-2015 (S. 7).

Mit **Versicherungen zum Schutz vor Cyberkriminalität** befasst sich die FAZ am 13. August. Selbst mittelgroße Versicherer hätten inzwischen eine eigene Cyberdeckung auf den Markt gebracht. Rund 20 Unternehmen würden auf dem deutschen Markt wetteifern. Wer als Vorstand das Cyberrisiko allein der Systemadministration überlässt, handele grob fahrlässig. Schon das Aktiengesetz verlange, Risikovorstände einzusetzen. In Londoner Taxis blieben im Jahr 50.000 bis 80.000 Firmenhandys liegen. Gingen nur 100 davon an Hacker, hätten sie leichten Zugang zu Firmennetzwerken. Die Unternehmen müssten sich gegen Betriebsunterbrechungen wappnen, denn wenn sie durch einen Cyberangriff eine zugesagte Ware nicht liefern können, drohen in der Regel Vertragsstrafen. Das deckten neuartige Cyberpolicen ab, nicht aber die klassischen Vertrauensschaden-Versicherungen, mit denen sich Unternehmen traditionell gegen strafbare Handlungen von Mitarbeitern oder externen Kriminellen absichern.

Der niedersächsische Verfassungsschutz berichtet in einem Wirtschaftsschutz-Info vom August 2015, dass unbekannte Angreifer mit einer modifizierten E-Mail-Adresse (Name des Geschäftsführers@provider.com) den Mitarbeiter des Rechnungswesens des Unternehmens über die Identität des Kommunikationspartners täuschen konnten. Der habe dann von diesem Absender den Auftrag erhalten, einen sechsstelligen Betrag auf ein Konto in China zu überweisen. Nach Durchführung der Überweisung habe sich der Irrtum über die E-Mail-Adresse herausgestellt.

Dipl.-Inf. Florian Oelmaier, CORPORATE TRUST Business Risk & Crisis Management GmbH, befürchtet im ASW-Newsletter vom 28. August, dass Cyberangriffe vermehrt zu kompletter Netzübernahme führen. Die Corporate Trust GmbH bearbeite vermehrt Cyberangriffe, bei denen die Angreifer sich so umfassend und tief in die IT-Netze einnisten, dass nur noch einschneidende Maßnahmen helfen könnten. Aktuell nutzten die Angreifer eine Ende-zu-Ende-stufige Angriffskombination. In einem ersten Schritt werde über eine Phishing-Mail der PC eines Nutzers im Netzwerk mit Schadsoftware infiziert. Eine gut recherchierte und passgenaue Phishing-Mail habe eine Erfolgschance von mehr als 50 Prozent. Einmal im Netz nutzten die Hacker im zweiten Schritt eine Kombination aus bekannten Softwarelücken durch veraltete oder nicht aktualisierte Systeme um Admin-Rechte zu bekommen und sogenannten Pass-the-Hash-Angriffen. Letztere basierten auf Standard Microsofttechnologien, sodass faktisch kein Schutz vor dieser Art Angriffen möglich sei. Ziel der Angreifer sei die Berechtigung eines sogenannten Domänen-Administrators. Mit dieser Berechtigung könne sich ein Angreifer im dritten Schritt dann ein sogenanntes „Golden Ticket" erstellen. Es sei für die Firma absolut notwendig, eine Reihe von grundlegenden Präventionsmaßnahmen gegen diese Angriffe umzusetzen. Die Corporate Trust GmbH habe die wichtigsten auf ihrer Webseite (www.corporate-trust.de) unter „Presse & Medien" > „Pressemeldungen & Security News" im Artikel „27.08.2015 ASW Newsletter: Zusatzinformationen und Handreichungen zum Thema Pass-the-Hash und Golden Ticken Angriffe" zusammengestellt.

Logistiksicherheit

Dr. Nils Meyer-Larsen und Rainer Müller, Institut für Seeverkehrswirtschaft und Logistik (ISL), befassen sich in der Zeitschrift Homeland Security (Ausgabe 1-2015, S. 11–15) mit der **Bedrohung von Lieferketten**. Das ISL sei im Rahmen von EU- und nationalen Projekten im Container Security-Bereich tätig, so auch in den aufeinander aufbauenden Projekten INTEGRITY, CASSANDRA und CORE. Im Rahmen von INTEGRITY sei die Software-Plattform SICIS (Shared Intermodal Container Information System) entwickelt

worden, die eine Data-Pipeline nutzt. Ziel der Data-Pipeline sei es, alle relevanten Daten der jeweiligen Supply Chain zu aggregieren und den Akteuren in hoher Qualität zeitnah zur Verfügung zu stellen. SICIS biete die Möglichkeit, Daten von verschiedenen Quellen sowie Positionsmeldungen der Seeschiffe über deren AIS-Transponder zu integrieren und mit Hilfe einer Webanwendung zu visualisieren. In dem Folgeprojekt CASSANDRA sei der Ansatz der Data-Pipeline weiter ausgebaut und auf weitere Transportkorridore ausgedehnt worden. Ziel des laufenden EU-Forschungsprojektes CORE sei es, globale Supply Chains zu schützen und resilient zu machen, unabhängig davon, ob es sich um Naturkatastrophen, terroristische Aktivitäten oder andere illegale Aktivitäten handelt. CORE ziele darauf ab, einen effizienten Handel innerhalb der EU und anderen Ländern sicherzustellen und beziehe dabei die Ergebnisse der Vorprojekte INTEGRITY und CASSANDRA mit ein.

Feuerrisiken entlang der Supply Chain behandelt Frank Drolsbach, FM Global Deutschland, in einem Brandschutz Special der Zeitschrift PROTECTOR vom August 2015 (S. 10/11). Der FM Global Resilience Index sei das erste datenbasierte Tool, das die Resilienz von Lieferketten in 130 Ländern weltweit in einem Ranking vergleicht. Datenquellen seien u. a. Veröffentlichungen des Weltwirtschaftsforums und der Weltbank sowie die Datenbank Riskmark. Im jährlich erscheinenden Index würden neun Treiber, die sich auf die Widerstandsfähigkeit von Lieferketten auswirken, zu Ende-zu-Ende-Faktoren zusammengefasst: Wirtschaft, Risikoqualität und die Lieferkette selbst. Der Faktor Risikoqualität setze sich aus den vorherrschenden Naturgefahren sowie der Qualität des Risikomanagements bei Elementar- und bei Feuerrisiken in den einzelnen Ländern zusammen. Die BRIC-Staaten belegten mittlere bis hintere Plätze im Ranking. Indien beispielsweise finde sich im Gesamtranking auf Platz 119 (von 130). Pakistan finde sich mittlerweile im Mittelfeld auf Rang 61 des Resilience Index bei der Feuerprävention. Pakistan zähle zu den „Next Eleven", die als die „neuen BRIC" angepriesen würden. Negative Ausreißer in Sachen Feuerprävention seien die Türkei und Ägypten (Platz 98). Insbesondere bei Betrachtung der Feuerprävention würden Indonesien (Platz 70) und Vietnam herausragen.

Luftverkehrssicherheit

INGENIEUR.de weist am 3. August darauf hin, dass die **Körperscanner**, die an deutschen Flughäfen eingesetzt werden, nicht den gesamten Körper von Fluggästen scannen. Die Füße würden von den Geräten nicht erfasst. Doch für die individuelle Überprüfung der Schuhe fehle oft die Zeit. Auch Gegenstände, die in Körperöffnungen verborgen sind, spüre der neue Scanner nicht auf. Die neue Technik habe aber zwei Vorteile: Die Strahlen seien nicht gesundheitsschädlich und sie machten nicht nur metallische Gegenstände sichtbar, sondern auch solche aus anderen Werkstoffen, etwa Keramik. Wenn sie etwas Verdächtiges entdeckt, dann begutachte ein Experte das Bild. Dieses Verfahren sei allerdings noch nicht ausgereift.

Mitarbeiterkriminalität

Der niedersächsische Verfassungsschutz weist in einem Wirtschaftsschutz-Info vom August 2015 auf einen Fall hin, in dem ein leitender Mitarbeiter eines Unternehmens aus Verärgerung über Kompetenzbeschneidungen kündigt und ein eigenes Unternehmen gründet, das von demselben IT-Dienstleister betreut wird wie das Unternehmen seines bisherigen Arbeitgebers. Eine Prüfung seines ehemaligen Arbeitsplatz-PCs habe ergeben, dass der Mitarbeiter Unternehmens-Know-how aus dem Firmennetz mit Unterstützung des IT-Dienstleisters nach extern ausgeleitet hatte. Der Verfassungsschutz empfiehlt, dass

in die Verfahrensweise für ausscheidende Mitarbeiter auch externe Dienstleister einbezogen werden sollten.

Notruf- und Service-Leitstelle

Michael Hobeling, Fachausschuss NSL des BHE, behandelt in der Ausgabe 4-2015 der Zeitschrift WiK, S. 64/65, das **Outsourcing der Alarmempfangsstelle** (AES) und des Interventionsdienstes aus der NSL als Option für mittelständische NSL. Beim Verzicht auf eine eigene AES müssten die entsprechenden technischen Dienste an ein Subunternehmen vergeben werden. Der Qualität abträglich sei das Vorgehen vieler Alarmdienste: Eine einzige, oft sogar die eigene Einbruchmeldeanlage, werde richtlinienkonform als Muster für die VdS-Prüfung nach VdS 3138 aufgeschaltet. Dies könne zur Folge haben, dass alle anderen Aufschaltungen außerhalb einer Zertifizierung, eines fixierten Mindeststandards und VdS 3138 erfolgen.

Personenschutz

Wie veko-online.de am 7. August berichtet, bietet Securiton mit „Premium Private" ein **ganzheitliches Personenschutzkonzept** mit allen Vorteilen einer vernetzten Gebäudetechnik an. Im Fokus stünden unter anderen die Videoüberwachung, Zutrittskontrolle, Einbruch- und Brandmeldung. Möglich seien die zahlreichen Funktionen durch Hard- und Softwarekomponenten für Gebäudesteuerungs- und Visualisierungssysteme. Wärmebildkameras eigneten sich für die Grundstückssicherung. Die intelligente Software werte die Bilder aus und erkenne ungewöhnliche oder bedrohliche Situationen sowie das Eindringen Unbefugter. In möglicher Kombination mit einem Detektionszaun alarmiere das Videosicherheitssystem im Ernstfall umgehend die Notruf- und Serviceleitstelle oder andere Interventionsorganisationen. Ein Rückzugsraum – oder auch eine Rückzugsebene – werde ganz nach den persönlichen Vorstellungen gestaltet. In jedem Fall besitze dieser Bereich eine unabhängige Infrastruktur und eine Kommunikationsanlage.

Laut Arbeitsagentur sei die Zahl der sozialversicherungspflichtig beschäftigten Frauen in privaten Wach- und Sicherheitsdiensten in den vergangenen sieben Jahren von 24.800 auf mehr als 30.200 gestiegen, schreibt welt.de am 30. August. Der Anteil von **Frauen in der Sicherheitsbranche** nehme seit Jahren kontinuierlich zu, bestätige der BDSW. Das Anforderungsprofil für Sicherheitskräfte habe sich grundlegend gewandelt. Wo früher Abschreckung und sichtbare Präsenz gefragt waren, werde heute eher aufs Gegenteil gesetzt. „Die oberste Maxime lautet heute Deeskalation", habe eine Sprecherin der Branche gesagt. Kunden erwarteten von Sicherheitskräften ein möglichst unauffälliges, repräsentatives und diplomatisches Auftreten. Und viele wollten für den Job eine Frau. Das BKA setze im Personenschutz schon seit Langem auch Frauen ein, mitunter schon aus kulturellen Gründen, etwa beim Schutz weiblicher Staatsgäste. Doch auch aus taktischer Sicht hätten Frauen im Personenschutz besondere Vorteile. „Aus Frauen und Männern bestehende Teams haben nachweislich eine deeskalierende Wirkung", habe eine Sprecherin des BKA gesagt. Zudem belege eine wissenschaftliche Untersuchung, dass Frauen besondere Fähigkeiten besäßen, wenn es darum gehe, potenzielle Attentäter zu identifizieren.

Risikomanagement

Im ASW-Newsletter vom 17. August plädiert Henry Smith, Control Risks, für die frühzeitige Einbindung des Risikomanagements in **strategische Unternehmensentscheidungen.**

Risikomanager seien auf den Erhalt von Vermögenswerten fokussiert. Der falsche Umgang mit strategischen Risiken bedeute aber einen viel größeren Schaden für den Unternehmenswert. Während also die Hauptaufgabe des Risikomanagers der Schutz der Unternehmenswerte ist, könnten und sollten sie gleichzeitig durch proaktives Risikomanagement in der Chancenevaluierung echten Mehrwert für ihr Unternehmen generieren. Falls Risikomanager dabei helfen, eine Länderstrategie von Anfang an mitzugestalten, könnten interne wie externe Stakeholder sicher sein, dass ein ganzheitlicher Ansatz verfolgt wird. Wenn Strategieabteilung und Risikomanagement eng bei der Auswahl von Geschäftspartnern und den erforderlichen Due Diligence-Prüfungen zusammenarbeiten, führe dies zu einer schnelleren und vor allem einheitlichen Risikoeinschätzung, die interne Ressourcen schone.

Schließsysteme

Philipp P. Spangenberg, baimos technologies GmbH, erläutert in der Ausgabe 4-2015 der Zeitschrift WiK, S. 61–63, Chancen und Risiken des Internets der Dinge (IoT) für die Schließtechnik. Die **Schließtechnik der Zukunft sei vernetzt** – mit dem Smartphone und der Cloud. Nutzer würden somit in der Lage sein, ihre Infrastruktur einfach zu verwalten und mobile Geräte unkompliziert einzubinden. Zudem würden die Systeme redundant ausgelegt und hochverfügbar sein. Die Interaktion mit dem Schließsystem könne über die Cloud laufen, um eine Fernschließung zu ermöglichen, die aber vornehmlich lokal über Bluetooth Low Energy und Near Field Communication (NFC) abgewickelt werde, um den Nutzerkomfort zu gewährleisten. Nutzer erwarteten auch zunehmend die Interaktion zwischen Smartphones, Wearables und der Infrastruktur. Schließsysteme mit weltweiter Erreichbarkeit per IP-Verbindung seien im Vergleich zu Offline-Systemen besonders gefährdet. Die in klassischen Smartcard-Systemen verwendete symmetrische Kryptografie mit PSK stelle eine weitere Gefahrenquelle im IoT-Ansatz dar, wenn sie nicht vollständig abgesichert wird. Eine asymmetrische Kryptografie eigne sich besonders gut für den IoT-Ansatz. Als technische Grundlage für eine sichere Kommunikation im IoT werde seit Jahren an dem „neuen" Internet-Protokoll IPv6 gearbeitet. Es ermögliche eine nahezu unbegrenzte Zahl an IP-Adressen. Als Mechanismen für die Sicherheit der Vernetzung der Vielzahl von kleinen Geräten bezeichnet der Autor die Verschlüsselung, eine transparente Firewall und Maßnahmen zum Perimeterschutz.

Sicherheitsgewerbe

Manfred Buhl, Securitas Deutschland, stellt in Ausgabe 1-2015 der Zeitschrift Homeland Security (S. 5–10) **„Das neue Sicherheitsunternehmen"** unter den Veränderungsaspekten der Integration von Dienstleistungen und Technologie entsprechend sich tendenziell wandelnder Kundenforderungen, der demografischen Entwicklung und der digitalen Technologie vor. Begründet werde dieser Paradigmenwechsel vor allem durch ein steigendes Sicherheitsbedürfnis, steigende Kosten personeller Dienstleistungen und eine immer leistungsfähiger und „intelligenter" werdende Sicherheitstechnik. Voraussetzung für das Gelingen des Paradigmenwechsels im Leistungsportfolio sei ein konsequentes Change Management. Das durch den demografischen Wandel hervorgerufene doppelte Dilemma von zu wenig jungen und zu wenig qualifizierten Bewerbern könne langfristig durch eine nachhaltige Imageverbesserung der Branche und der Attraktivität des einzelnen Sicherheitsunternehmens überwunden werden. Der Megatrend Digitalisierung habe längst auch die Sicherheitswirtschaft erreicht. Der Autor führt Beispiele für eine digitale Optimierung von Sicherheitsdienstleistungen

durch Digitalisierung an und weist nach, wie dieser Trend auch die innerbetriebliche Organisation, Einsatzvorbereitung und -nachbereitung sowie die Informationssammlung und -verarbeitung erfasst.

„**Digitaler Wachdienst**" titelt das Magazin FOCUS am 29. August. Bisher würden zur Sicherheit in großen Konzernen für viel Geld etwa 200 lokale Speichergeräte aufgestellt, die ein Wächter mit Spezialkarte nachts ablaufen muss. Tage später lese ein Kontrolleur die Geräte umständlich aus. Bei Coredinate werde jedem Wachdienst jetzt ein NFC-fähiges Smartphone ausgehändigt. Dann scanne der Wächter am Kontrollpunkt einen einfachen Aufkleber. Auch könne er von unterwegs Sprachmemos senden, etwa wenn eine Dachluke offen steht.

Sicherheitstechnik

Die Fachzeitschrift WiK weist in Ausgabe 4-2015 (S. 60) auf die vom BHE und vom ZVEI-Fachverband Sicherheit veröffentlichten **Umsatzzahlen für den Markt der elektronischen Sicherheitstechnik 2014** hin. Der Umsatz sei im Vergleich zu 2013 um 7,4 Prozent auf 3,3 Mrd. Euro angestiegen. Für Brandmelder sei der Umsatz sogar um 11,5 Prozent angewachsen (1,52 Mrd. Euro nach ZVEI-Angaben). Überdurchschnittlich gewachsen sei auch der Markt der Sprachalarmierung (um 11,1 Prozent). Videotechnik (450 Mio. Euro) und Zutrittskontrolltechnik (285 Mio. Euro) verzeichneten Wachstumsraten von 4,7 bzw. 4,4 Prozent. Ein leichtes Wachstum verzeichnete auch die Überfall- und Einbruchmeldetechnik (2,5 Prozent auf 290 Mio. Euro). Die vom BHE veröffentlichten Zahlen weichen teilweise von diesen Zahlen ab. Insgesamt sei nach seinen Messungen der Gesamtumsatz für elektronische Sicherungstechnik 2014 auf rund 3,18 Mrd. Euro gestiegen, ein Wachstum um 3,7 Prozent.

Peter Sehr beschreibt in veko-online.de am 7. August virtuelle Welten in der täglichen Wahrnehmung (**augmented reality – AR**). Darunter verstehe man die computerunterstützte Erweiterung der Realitätswahrnehmung. Umfasst werde die Erweiterung der menschlichen Sinne wie Sehen und Hören, Riechen und Fühlen. Google Glasses werde im Wesentlichen Ende-zu-Ende-Komponenten miteinander verbinden: die Analyse dessen, was der Benutzer sieht sowie deren Einordnung in den Kontext, die anschließende Verknüpfung mit digitalen Daten sowie eine optimale Darstellung der virtuellen Erweiterung in das reale Sichtfeld. Der Nutzen von AR dürfte einer Revolution gleichkommen. Beispiele: Gefahren würden rechtzeitig erkannt, Gegenmaßnahmen seien sofort abrufbar und damit umsetzbar. In Katastropheneinsätzen seien alle hilfreichen Maßnahmen verfügbar, zum Beispiel das Aufzeigen gangbarer Evakuierungswege. Für Feuerwehr und Polizei würden nützliche Informationen, zum Beispiel über Gebäude, vorrätig gehalten. Möglichkeiten der Schadensminderung bei Unfällen mit Gefahrgut würden angeboten, Gefahren wie Giftwolken rechtzeitig erkannt.

Die FAZ weist am 22. August auf eine Analyse der Deutschen Bank hin, nach der das Weltmarktvolumen für AR bis 2020 von derzeit 500 Mio. auf 7,5 Mrd. Euro steigen soll. Es sei wichtig, die Technologie nicht wegen einzelner Anwendungen unter dem Aspekt des Datenschutzes als Ganzes zu verteufeln, sondern die Risiken – auch durch Rechtsnormen – zu begrenzen. Die Technologie werde auch die Entwicklung von Industrie 4.0 begünstigen, denn in der hochintegrierten, datenorientierten **„Smart Factory"** der Zukunft sei der schnelle, zuverlässige und medienbruchfreie Informationsaustausch vom Zulieferer bis hin zum Endkunden zentral.

Social Engineering

Gefahren und Abwehr bei Social Engineering behandeln Dietmar Pokoyski, known_sense, Dipl.-Psych. Ivona Matas und Dirk Fleischer, LANXESS AG, in Ausgabe 4-2015 der Zeitschrift WiK (S. 29–33). Eine neue Studie des Beratungsunternehmens known_sense zusammen mit der IT-Fachzeitschrift <kes> verdeutliche die Aktualität der Gefahren für diese Methode der Ausspähung. Für eine Bekämpfung reiche eine Hotline nicht aus. Die meisten Opfer würden den Angriff nicht bemerken. So sei es höchste Zeit, ein tragfähiges Incident Management implementiert zu haben. Meldewege müssten stärker als derzeit auf Auseinandersetzungen mit dem Thema innerhalb vertrauter Settings setzen, etwa im Rahmen eines moderierten Erfahrungsaustauschs. Für den Unternehmensschutz habe sich auch gezeigt, dass der Erfolg von Maßnahmen stark von der Authentizität und Glaubwürdigkeit derer abhängt, die das Thema vermitteln.

Sprachalarmierung

Das Brandschutz Spezial der Zeitschrift PROTECTOR vom August 2015 enthält eine **Marktübersicht** zu 39 Sprachalarmierungssystemen von 21 Anbietern (S. 40/41) mit Angaben zu Funktionen, Anschlüssen und Sicherheitsfunktionen.

Transportdiebstahl

Nach einer Pressemeldung des PP Osthessen vom 29. Juli führten umfangreiche Ermittlungen Anfang Juli zu einem bemerkenswerten Fahndungserfolg. Eine Diebesbande aus fünf Männern sitze wegen des dringenden Tatverdachts des Diebstahls zahlreicher Lkw-Ladungen in U-Haft. Ende des Jahres 2014 habe sich ein Tatschwerpunkt auf den Parkplätzen an den osthessischen Autobahnen A5 und A7 in den Landkreisen Vogelsberg und Hersfeld-Rotenburg herauskristallisiert. Durch die umfangreichen Ermittlungen sei es schließlich gelungen, die Tatverdächtigen zu ermitteln und das mutmaßliche Lager für das Diebesgut in Peine zu lokalisieren. Insgesamt gingen die Ermittler inzwischen davon aus, dass die Bande bei ihren bekannt gewordenen Diebestouren, bei denen sie die Planen der Lkw-Anhänger aufgeschnitten hätten, um das Vorhandensein lohnender Beute zu prüfen, Waren im Gesamtwert von rund 150.000 Euro gemacht habe.

Die ASW hat im Monat August folgende Tatorte mitgeteilt, an denen auf Fahrstrecken im Bundesgebiet Planen von **Lkw aufgeschlitzt** und Ladungsdiebstähle begangen wurden:

- 5./6. August, A 245, Wittstock, Rastanlage Prignitz Ost
- 10. August, A 10, Michendorf, Raststätte Michendorf-Süd, Fahrtrichtung Frankfurt (Oder).

Veranstaltungssicherheit

In der Ausgabe 7/8-2015 der Zeitschrift PROTECTOR beleuchtet Hendrick Lehmann Sicherheitsprobleme bei Großveranstaltungen. Um keine Staus aufkommen zu lassen, setze die Polizei **„Diamanten"** ein. Dies seien aus Gittern zusammengesetzte Dreiecke, die den Besucherstrom verlangsamen, damit den Durchfluss verengen und den zur Verfügung stehenden Weg dem Querschnitt einer Unterführung anpassen. Um einen Überblick über die Anzahl der auf einem Gelände befindlichen Personen zu erhalten, könnten die Eintrittskarten mit einem Chip versehen werden, der beim Einlass erfasst wird (S. 20–22).

Um bei Großveranstaltungen den Überblick zu behalten, könnte auch ohne Strom- oder Internet-Verbindung ein **mobiles Video-**

überwachungssystem eingesetzt werden. Es sei im Vergleich zu einer Feldverkabelung kostengünstig, wirtschaftlich und vor allem einfach zu handhaben. So könnten neuralgische Punkte schneller identifiziert und Hilfskräfte zielgerichtet gesteuert werden. Mit intelligenter Software sei Sabotage zwecklos: Ob die Kamera verdreht, geblendet oder besprüht wird – das System bemerke solche Manipulationsversuche und schlage Alarm (PROTECTOR, Ausgabe 7/8-2015, S. 28/29).

Verfassungsschutz

ZEIT ONLINE berichtet am 27. August, der Verfassungsschutz habe vom NSA die begehrte Spionagesoftware **XKeyscore** bekommen. Das sei ein Datenbanksystem, das eine Sammlung von Funktionen enthalte, um Daten zu sortieren und zu analysieren. NSA und der BND würden XKeyscore nutzen, um damit im Internet nach Hinweisen und Verdächtigen zu fahnden. Der Verfassungsschutz dürfe das rechtlich nicht. XKeyscore laufe bei ihm daher als komplett geschlossenes System. Es durchsuche Daten, die zuvor bei genehmigten Abhör- und Überwachungsmaßnahmen gesammelt wurden. XKeyscore könne IP-Daten zuerst einmal klassifizieren, also darin die Daten von ungefähr 800 verschiedenen Applikationen, Internetanwendungen und Protokollen erkennen und zuordnen. Die vorsortierten Daten könne das Programm entschlüsseln, also das Datenformat, in dem sie programmiert wurden, übersetzen und den Inhalt in eine Form bringen, die die Auswerter auch lesen können.

Verschlüsselung

Wie heise.de am 21. August meldet, sollen künftig Internetnutzer die Sicherheit von verschiedenen E-Mail-Anbietern eindeutig erkennen und miteinander vergleichen können. Dafür habe das BSI den Entwurf der **Technischen Richtlinie „Sicherer E-Mail-Transport"** veröffentlicht. Darin definiere das BSI verbindliche Sicherheitsvorgaben, die ein E-Mail-Anbieter erfüllen müsse. Die Anforderungen schlüsseln sich in gesicherte DNS-Abfragen, obligatorische Verschlüsselung, sichere Kryptografie und vertrauenswürdige Zertifikate auf. Das Sicherheitskonzept müsse dem BSI zufolge der E-Mail-Anbieter selbst erstellen und umsetzen. In Zukunft solle der Anbieter dann von einer unabhängigen Stelle ein Zertifikat erhalten.

Videoüberwachung

In der Zeitschrift PROTECTOR stellt in Ausgabe 7/8-2015 Dahua Technology Co Ltd. den neuen **H.265-Videokompressionsstandard** vor, der die Datenrate signifikant reduziere (S. 24/25). Verglichen mit dem aktuell weit verbreiteten AVC-Standard H.264 solle der neue H.265-Codec eine Reduktion der Datenrate um etwa 50 Prozent bei hochqualitativen Videos ermöglichen. Die Bitrate dürfte in der Praxis bei etwa 40 bis 50 Prozent für 1080p-Material liegen, wobei eine herausragende Videogüte erzielt werden solle. Im Bereich der Kamera habe Dahua seine neueste 5 Megapixel-IP-Kamera mit einem H.265/H.264-Dual-Codec ausgestattet, der bis zu 40 Prozent an Bandbreite einspare und gleichzeitig eine Kamera eingeführt, die den H.265-Standard beherrsche und simultan mehrere Videoströme decodieren könne.

Softwarelösungen, die **auf einer offenen Plattform** aufbauen, würden immer interessanter, ist Marco Schwitz, Milestone Systems, überzeugt. Sie böten ein Höchstmaß an Flexibilität und Zukunftssicherheit (PROTECTOR, Ausgabe 7/8-2015, S. 26/27). Zuverlässigkeit, Offenheit, Innovation, Flexibilität und Unabhängigkeit seien die Grundeigenschaften einer offenen Plattform. Ein Software Development Kit (SDK) sei ein unverzichtbares

Element in einer offenen Plattform. Darüber ließen sich alle Funktionseigenschaften der genutzten Komponenten implementieren, um sie in einer Plattform zu einer Gesamtlösung zu vereinen. Auf einer offenen Plattform lasse sich ein System einfach mit neuen Funktionen ergänzen. Ein weiterer Vorteil sei die Qualität, die sich aus einer partnerschaftlichen Zusammenarbeit ergibt. Von großer Wichtigkeit sei die Möglichkeit einer direkten Integration in die Oberfläche der Video-Management-Software (VMS). In der offenen Plattform können leicht Abhängigkeiten zwischen den einzelnen Komponenten hergestellt werden, durch die die einzelnen Auswertungsergebnisse miteinander logisch verknüpft werden, um beispielsweise bei der Gebäudeüberwachung eine Reduzierung der Fehlalarme zu erreichen.

Die FAZ weist am 14. August darauf hin, dass grundsätzlich bei einer Videoüberwachung auf einem Privatgrundstück zum **Schutz des Persönlichkeitsrechts** gewährleistet sein müsse, dass keine öffentlichen Bereiche oder Nachbargrundstücke von der Kamera erfasst werden. Wie das AG Wedding jedoch mit Urteil vom 25.06.2014 entschieden habe, sind Aufnahmen von Kameras, die gerade so installiert sind, dass Nachbargrundstücke oder öffentliche Straßen verpixelt dargestellt werden, ausnahmsweise zulässig, wenn eine Aufhebung der Verpixelung nur mit einem hohen bürokratischen und technischen Aufwand möglich wäre (Az. 8a C 63/13).

Wegfahrsperre

Spezialisten sei es gelungen, Wegfahrsperren namens **Megamos** zu knacken, die auch VW verwendet, berichtet die Wirtschaftswoche am 21. August. Die Technik komme vom Schweizer Hersteller EM Microelectronic und habe als besonders sicher gegolten. Hersteller wie VW, Audi, Fiat, Honda oder Volvo würden sie einbauen. Bei neueren Modellen wie dem aktuellen Passat und Golf sei die Wegfahrsperre nun besser verschlüsselt. Ältere Autos seien theoretisch weiter gefährdet, weil der kleine Megamos-Chip in der Plastikummantelung des Schlüssels eingegossen ist und sich daher kein Software-Update aufspielen lasse. VW-Mitarbeiter halten neue Schlüssel für verzichtbar, weil Diebe den Schlüssel selbst benötigten und monatelang den aufwendigen Hack vorbereiten müssten.

Wirtschaftsschutz

Peter Hohl, SecuMedia Verlags GmbH, berichtet in Ausgabe 4-2015 der Zeitschrift WiK (S. 18/19) über eine vom Verfassungsschutz veranstaltete Wirtschaftsschutztagung am 21. Juli in Stuttgart. Sechs Maßnahmen habe der Verfassungsschutz als existentiell für den Wirtschaftsschutz identifiziert: „Kronjuwelen" identifizieren; Zugangsrechte regeln; IT-Sicherheitsplan erstellen; mobile Endgeräte einbeziehen; Human Firewall: Mitarbeiter einbeziehen; Auslandskontakte sorgfältig gestalten. Der Vizepräsident des BSI, Andreas Könen, habe die aktuelle Gefahrenlage für die Informationstechnik wie folgt skizziert: Jede 40. Website ist mit „Drive by Malware" infiziert. Botnetze kann man für 5 US$ pro Stunde mieten. Ergebnis: 34.000 DDoS-Angriffe pro Jahr auf deutsche Unternehmen; 1,7 Mio. neue Malware-Programme zielten 2013 allein auf mobile Technik mit Android-Betriebssystemen. Besonders dramatisch: 243 Tage vergehen im Durchschnitt zwischen Angriff und Entdeckung.

Zutrittskontrolle

Axel Schmidt, SALTO Systems GmbH, befasst sich in Ausgabe 4-2015 der Zeitschrift WiK, S. 56–58, mit **mobilen Zutrittslösungen**. Man könne das Smartphone als Update-Terminal nutzen und darüber die

Zutrittsberechtigungen auf der Karte aktualisieren. Diese fungiere dann als Identmedium am Zutrittspunkt. In mobilen Zutrittslösungen würden die Berechtigungen in der Zutrittsmanagementsoftware vergeben und „over the air" an das zuvor registrierte Smartphone verschickt. Zur Ablage kritischer Daten müsse ein gesicherter Speicher als „Secure Element" (SE) vorhanden sein. Das sei notwendig, da nur zertifizierte Unternehmen die Schnittstelle für das SE erhalten. Es gebe verschiedene Arten von Secure Elementen. Eine Möglichkeit sei, einen logisch abgetrennten Speicherbereich auf der SIM-Karte zu verwenden. Bei einer anderen Variante werde ein zusätzlicher Chip ins Handy eingebaut, der als SE fungiere. Oder das SE befinde sich auf dem Zutrittsmedium. Sollte jemand an die Daten des Smartphones gelangen, könne er dennoch keine Tür öffnen, denn es fehlten die notwendigen Informationen aus dem gesicherten Bereich des Ausweises. Eine zusätzliche hohe Hürde bilde die ohnehin standardmäßige Verschlüsselung der übertragenen Informationen mittels 125 Bit-AES-Encryption. Die Türöffnung erfolge bei dieser Systemarchitektur immer mit dem Zutrittsausweis und nicht mit dem Smartphone. Für die Übermittlung der Daten vom Smartphone zum Ausweis komme die NFC-Schnittstelle zum Einsatz. Die Übertragungssicherheit sei abhängig vom Sicherheitsniveau der verwendeten Identifikationstechnologie. Eine weitere Variante, Smartphones in Zutrittslösungen einzubinden sei, sie direkt für das Öffnen von Türen einzusetzen. Dazu bedienten sich viele Hersteller der jüngsten Version der Bluetooth-Schnittstelle.

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,
Elke Hollenberg, Gabriele Biesing
Vorsitzender des Aufsichtsrates: Dr. Carl A. Schade

E-Mail: info@securitas.de