Focus on Security

Ausgabe 01, Januar 2016

SECURITAS

Inhalt

Arbeitsschutz ... 3
Aufzugssicherheit ... 3
Besuchermanagement ... 3
Brandschutz ... 4
Cloud Computing ... 5
Compliance ... 5
Datenschutz ... 7
Diebstahl ... 7
Einbruch ... 8
Einzelhandelssicherheit ... 8
Evakuierung ... 8
Geldautomatensicherheit ... 9
Geldraub ... 9
Industrie 4.0 ... 9
IT-Sicherheit ... 10
IuK-Kriminalität ... 12
Krisenmanagement ... 15
Krisenregionen ... 15
Maschinensicherheit ... 15
Organisierte Kriminalität ... 16
Perimetersicherung ... 16
Personenschutz ... 17
Piraterie ... 17
Rauchwarnmelder ... 18
Schließsysteme ... 18
Sicherheitsgewerbe ... 19
Sicherheitsmanagementsystem ... 19
Sicherheitsmarkt ... 20
Spielbanksicherheit ... 21
Spionage ... 21
Steuerhinterziehung ... 22
Terrorismus ... 22
Veranstaltungssicherheit ... 23
Videoüberwachung ... 23
Zahlungskartenkriminalität ... 24
Zutrittskontrolle ... 25

Arbeitsschutz

Jan Kuntze, DBL-Vertragswerk Kuntze und Burgheim Textilpflege GmbH, erläutert in der Ausgabe 6-2015 der Fachzeitschrift WiK, S. 26/27, die neue Norm EN ISO 20471 **„Hochsichtbare Warnkleidung".** Sie bringen einige grundsätzliche Änderungen mit sich. Bisher stand die Beschreibung der Tätigkeit im Mittelpunkt. Der neuen Norm liege dagegen eine Risikobetrachtung zugrunde. Eine präzise Risikoanalyse und Gefährdungsbeurteilung sei daher die Grundlage für die Auswahl der korrekten Warnkleidung. Dazu würden gleichzeitig neue Risikostufen definiert. Die EN ISO 20471 beziehe sich dabei ausschließlich auf Warnkleidung für hohes Risiko. Die neue Norm lege die Mindestflächen des Hintergrundmaterials sowie die Anordnung der Materialien in der Schutzbekleidung je nach Schutzklasse (1–3) fest. Die drei Bekleidungsklassen unterschieden sich anhand von drei unterschiedlichen Mindestflächen von retroreflektierendem Material, fluoreszierendem Material und/oder Material mit kombinierten Eigenschaften. Der Autor behandelt insbesondere das Ziel (360-Grad-Sichtbarkeit), die neuen Klassen, die neue Kennzeichnung und Regeln für Veredelung und Pflege.

Christine Wendl, ASTRUM IT GmbH, befasst sich in der Ausgabe 6-2015 von WiK (S. 28/29) mit der **Gefahrenunterweisung betriebsfremder Personen**. Nicht nur die eigenen Mitarbeiter, auch betriebsfremde Personen müssten gem. § 12 ArbeitsschutzG, der DGUV Vorschrift 1 und § 9 BetriebssicherheitsVO über Gefährdungen informiert werden. Unterweisungen müssten auch immer wieder aktualisiert werden. Das zu organisieren sei äußerst komplex, gerade wenn viele Menschen in Art und Zeitpunkt unterschiedlich zu unterweisen sind. Bei ausländischen Besuchern und Mitarbeitern führe das zu neuen Herausforderungen. Das Besuchermanagementsystem VISIT.net von ASTRUM IT unterstütze neben dem Ein- und Austritt von Besuchern und der Besucherverwaltung im engeren Sinne auch die allgemeine Sicherheitsunterweisung. Das neue Modul arbeite so: Meldet sich ein Besucher oder Fremdfirmenmitarbeiter an der Pforte an, sei im System hinterlegt, ob er bereits eine Unterweisung erhalten hat und ob diese noch gültig ist. Die Unterweisung könne auf einem Terminal oder einem Mobilgerät über eine App durchgeführt werden. Der Empfang stehe dabei für Fragen zur Verfügung. Da der Unternehmer nicht nur die Pflicht habe, über Gefahren zu informieren, sondern auch zu prüfen, ob die eingeführten Maßnahmen verstanden wurden, werde im Programm ein Fragenpool hinterlegt, aus dem automatisch eine Reihe von Fragen generiert werde.

Aufzugssicherheit

Die Zeitschrift WiK weist in Ausgabe 6-2015, S. 60, darauf hin, DEKRA habe mit der **LiKoS BlackBox** ein automatisches Fernüberwachungssystem für Aufzüge entwickelt. Die Messsysteme erfassten kontinuierlich die Kabinenposition, die Bündigkeit in der Haltestelle sowie den Sicherheitskreis der Türen. Sie würden Fahrtstrecken messen, Vibrationen und Geräusche im Fahrkorb und am Türlauf registrieren. Verschleiß, Störungen und die Folgen von Vandalismus würden frühzeitig erkannt und automatisch gemeldet. In Notfällen signalisiere die Anlage, ob sich Personen im Fahrkorb befinden.

Besuchermanagement

Katja Rümmele, Astrum IT GmbH, thematisiert in der Ausgabe 12-2015 der Zeitschrift PROTECTOR, S. 28, **Anforderungen an moderne Besuchermanagementsysteme**. Sie unterstützten Mitarbeiter, Empfangspersonal, Werkschützer, IT und Management gleichermaßen. Betriebsfremde Personen

müssten zunehmend den gleichen Prozessen unterworfen werden wie solchen, die für festangestellte Mitarbeiter vorgeschrieben sind. Hierzu zählten die gesetzlichen und betrieblichen Vorgaben wie Sicherheits- und Datenschutzunterweisungen, Gefährdungsbeurteilungen, Unterweisungen im Umgang mit Gefahrstoffen und dergleichen. Die Prüfung des Besuchers gegen Sanktionslisten und betriebseigene Werkverbote verlaufe im Hintergrund. Der Lieferant erhalte, nachdem er seinen Lkw nach automatischer Kennzeichenerkennung auf einem zugewiesenen Platz abgestellt habe, im Pförtnerhaus einen PIN-Code zusammen mit der Aufforderung, sich an einem Touch-Terminal zu identifizieren, um die Sicherheitsunterweisung in einem eLearning-Tool zu durchlaufen. Nach Wirksamkeitskontrolle erhalte er seinen Besucherausweis.

Brandschutz

PROTECTOR weist in der Ausgabe 12-2015, S. 44/45, darauf hin, dass bereits im Oktober 2014 der Arbeitskreis vorbeugender Brand- und Gefahrenschutz im Deutschen Feuerwehrverband eine Bewertung zur vorübergehenden **Unterbringung von Flüchtlingen** und Asylbewerbern vorgenommen und entsprechende Empfehlungen gegeben hat. Für Asylbewerber-Wohnheime forderten die Experten eine Brandmeldeanlage nach DIN 14675, Schutzkategorie 3, mit Alarmübertragung zur Feuerwehr, sowie einen lauten Innenalarm; außerdem Rauchmelder in jedem Beherbergungsraum. Bei der Unterbringung von Flüchtlingen in Hallen empfehle die Feuerwehr neben einer Notbeleuchtung die Anlage von Flucht- und Rettungswegen sowie eines Sammelplatzes und eine spezielle Brandwache. Die Betten müssten nach Brandschutzgesichtspunkten aufgestellt und die Aufsichtspersonen entsprechend eingewiesen werden. Die Nutzung eines Hotels als Unterkunft, bei der die Feuerwehr die Betriebsstättenverordnung als ausreichend ansieht, bewerte das Bauministerium Nordrhein-Westfalen als genehmigungspflichtige Nutzungsänderung zum Sonderbau. Die installierten Brandmelder sollten mit einem Mehrkriterien-Analyseverfahren arbeiten. Moderne Geräte würden auch Schwelbrände durch eine Kombination aus hochsensiblen optischen Rauch-Detektoren mit Kohlenmonoxid- und Wärmesensoren erkennen. Bei der Auswertung der Signale hätten sich digital adressierbare Brandmeldesysteme bewährt, die heute über einen benutzerfreundlichen Farb-Touchscreen verfügen und auf das robuste MZX-Ringbusprotokoll setzen. Sie eigneten sich für kleinere Anlagen ebenso wie für größere Installationen.

Brandschutz mit Kabelbandagen thematisiert GIT in der Ausgabe 12-2015, S. 70/71. Sie kämen in Verbindung mit einem Gesamt-Brandschutzkonzept zum Einsatz und bestünden in der Regel aus einem Glasträgergewebe, auf dem beidseitig ein dämmschichtbildender Baustoff aufgebracht wird. Bei Hitzeeinwirkung schäume das Material auf und verzögere so die Brandausbreitung. Da die Dicke der Bandagen oftmals nur wenige Millimeter beträgt, ließen sie sich einfach nachträglich um die zu schützenden Kabel legen, selbst an beengten Stellen. Seit 2006 gebe es für die Produkte Anwendungszulassungen vom Deutschen Institut für Bautechnik (DiBt). In diesen Anwendungszulassungen werde bescheinigt, dass Kabelbandagen die Brandentstehung behindern und eine Brandweiterleitung im Fall der Selbstentzündung durch Kurzschluss oder Überhitzung der Kabel verhindern, oder dass Kabelbandagen bei einer Brandbeanspruchung von außen die Anforderungen an schwer entflammbare Baustoffe erfüllen. Der Einsatz von Kabelbandagen in Flucht- und Rettungswegen sei nur über eine genehmigte Abweichung durch die Untere Bauaufsichtsbehörde zulässig. Klassifizierte Elektroinstallationskanäle seien als Abschottungsmaßnahme in der Wanddurchführung und

Brandlastenkapselung im Rettungsweg das optimale Brandschutzprodukt für Neubauten und hätten sich über Jahrzehnte bewährt. Es gebe unterschiedliche Lösungsansätze, Brandlasten in Rettungswegen zu kapseln und die gestellten Schutzziele zu erfüllen. Die sicherste Maßnahme stellten klassifizierte Installationskanäle dar.

Cloud Computing

Seit viele Public-Cloud-Dienste kostenfrei verfügbar sind, nutzten Mitarbeiter diese in großem Stil – vorbei an der Unternehmens-IT –, berichtet TECCHANNEL.de am 15. Dezember. Das belege die Skyhigh-Studie **„Cloud Adaption & Risk Report" Q1 2015**. Danach kämen in Unternehmen durchschnittlich 738 Cloud-Dienste zum Einsatz, aber nur weniger als ein Zehntel davon seien bei der IT-Abteilung bekannt und genehmigt. Als Hauptgründe für inoffizielle Cloud-Apps seien Vertrautheit mit den betreffenden Anwendungen aus dem Privatgebrauch sowie langwierige Genehmigungsverfahren in der jeweiligen IT-Abteilung genannt worden.

Compliance

Laut Sonderbericht Wirtschaftsschutz der deutschen Sicherheitsbehörden des Bundes vom 7. Dezember hat das BKA zum Thema „Compliance-Systeme und ihre Auswirkungen auf die Verfolgung und Verhütung von Straftaten der Wirtschaftskriminalität und Korruption" ein **Forschungsprojekt** mit einer bundesweiten Befragung zu den Bereichen wahrgenommene Veränderungen durch Compliance, Anzeigeverhalten, Erfahrungen in der Zusammenarbeit und Maßnahmen zur Förderung der Zusammenarbeit durchgeführt und auswertbare Antworten von 371 Großunternehmen, 238 Polizeibeamten und 145 Staatsanwälten bekommen. **Auszüge aus den Ergebnissen**: Compliance sei in deutschen Großunternehmen stark verbreitet. Ab 5.000 Beschäftigten verfügten etwa 80 Prozent der Unternehmen über ein Compliance-System. Durch die Einführung sei eine stärkere Professionalisierung bei der Vorbeugung und Bekämpfung von Wirtschaftskriminalität erkennbar. Bei der Prävention arbeiten Unternehmen mit Compliance besonders häufig mit externen Dienstleistern zusammen, selten mit Strafverfolgungsbehörden. Hier werde Entwicklungspotenzial gesehen. Je größer das Unternehmen ist, desto höher sei die Anzahl der im Unternehmen bekannt gewordenen Verdachtsfälle. Umgekehrt verhalte es sich bei der Anzeigequote: Je größer das Unternehmen ist, desto geringer sei die durchschnittliche Anzeigequote. Unternehmen mit Compliance-System geben im Vergleich zu Unternehmen ohne Compliance deutlich mehr Verdachtsfälle an. Die Quantität der entdeckten Verdachtsfälle könne durch höhere Investitionen in und den stärkeren Einsatz von Kontrollmechanismen gesteigert werden. Insbesondere wiesen Unternehmen auf den positiven Nutzen elektronischer Hinweisgebersysteme hin. Die Anzeigequote liege durchschnittlich bei ca. 50 Prozent. In Unternehmen mit Compliance-System würden zwar mehr Verdachtsfälle bekannt, es komme aber zu keiner höheren Anzeigequote in Unternehmen mit einem Compliance-System. Aus Sicht der Unternehmen werde die Entscheidung über eine Strafanzeige fallabhängig und deliktsunabhängig getroffen. Die befragten Polizeibeamten geben dagegen deutlich häufiger an, dass ihren Erfahrungen nach Insiderdelikte und Korruption eher nicht angezeigt werden. Eine hohe Schadensumme und die zu erwartende Überführung des Tatverdächtigen förderten die Entscheidung der Unternehmen zur Anzeigenerstattung. Bereitschaft zur Schadenswiedergutmachung und Kooperation des Täters führten dagegen eher dazu, von einer Strafanzeige abzusehen. Weitere Gründe für das Absehen von einer Strafanzeige seien aus Sicht der Unternehmen z. B. Angst vor Kontrollverlust

und Imageschäden, fehlender Nutzen der Anzeige sowie Schutz des betroffenen Beschäftigten. Als Grundlage einer erfolgreichen Zusammenarbeit in konkreten Fällen seien transparentes und kooperatives Handeln, eine offene und regelmäßige Kommunikation sowie Vertraulichkeit und Verbindlichkeit bei Absprachen genannt worden. Unternehmen forderten fundierte (betriebs)wirtschaftliche Kenntnisse auf Seiten der Strafverfolgungsbehörden und einen sensiblen Umgang mit den unternehmensinternen Daten. Das Legalitätsprinzip und einengende Datenschutzbestimmungen benennen die Strafverfolger und Unternehmen als größte Hürden für eine Zusammenarbeit. Im Rahmen der Projektarbeit seien aus den gewonnenen Ergebnissen Handlungsempfehlungen erarbeitet worden, die im Schlussbericht dargestellt und erläutert werden.

Julia Deuker, otris software AG, erläutert in der Ausgabe 6-2015 der Zeitschrift Security insight (S. 40/41) eine **Software zur Ausschaltung von Compliance-Risiken**. Die Kosten der Aufarbeitung eines Compliance-Verstoßes seien oft enorm hoch. In der Regel lägen sie weit über den Kosten, die für die Einrichtung eines effektiven Compliance-Systems notwendig gewesen wären. Compliance verringere nicht nur das zivil- und strafrechtliche Haftungsrisiko, sondern sie schaffe auch Vertrauen, sowohl bei Geschäftspartnern als auch bei Kunden. An der Verbesserung ihrer Compliance-Struktur arbeiteten derzeit viele Unternehmen. Im stetig wachsenden Meer aus Richtlinien sei es ohne erheblichen Mehraufwand praktisch unmöglich, sämtliche Vorgaben umzusetzen. Ein Programm wie otris COMPLIANCE diene hier als Leuchtturm: Sie strukturiere alle Corporate-Governance- und Compliance-Themen unternehmensspezifisch und stelle sie im Rahmen eines modernen Management-Informationssystems übersichtlich bereit. Mit der Software würden alle relevanten Governance-, Risk- und Compliance-Informationen, -Berichte und -Dokumente zentral gesammelt, themenbezogen klassifiziert und mit den erforderlichen Berechtigungen versehen. Automatisch überprüfe die Software zudem sämtliche Informationen, Berichte und Dokumente auf Aktualität und Vollständigkeit. Regelmäßige Reports, übersichtliche Listen und ein einfaches Ampelsystem unterstützten sowohl das Management als auch die operative Ebene.

Die Zeitschrift WiK stellt in der Ausgabe 6-2015, S. 6, das **Compliance-Barometer 2015** vor, bei dem durch einen speziell berechneten Index aktuelle Trends in Sachen Compliance erfasst würden. Dazu habe das Marktforschungsinstitut Ipsos 175 zufällig ausgewählte Compliance-Verantwortliche in deutschen Großunternehmen interviewt. Das größte Compliance-Risiko sähen die meisten Befragten im Datenschutz, gefolgt von Produkthaftung, Korruption, Arbeitsrecht und Kartellrecht. Geldwäsche, Außenwirtschaft und Wirtschaftsspionage hingegen spielten in der Wahrnehmung der Befragten kaum eine Rolle. Eine wesentliche Herausforderung für Compliance liege aus Sicht der Befragten in der Reaktion auf zunehmende staatliche Regulierung. Immer häufiger verlangten Geschäftspartner Nachweise über Compliance-Systeme.

Die FAZ befasst sich am 7. Dezember mit der **Führungskultur in deutschen Konzernen**. Abgasskandal bei Volkswagen, Geldwäsche, Zinsmanipulation und Steuerkriminalität bei der Deutschen Bank, Wahlfälschung beim ADAC, institutionalisierte Korruption bei Siemens: Angstkultur, Gruppendruck und die Tendenz, „wegzusehen, solange das Ergebnis stimmt", seien Kontextbedingungen, die kollektives Betrügen möglich machen. Die heutige Komplexität im Organisationsgeschehen erlaube es Chefs nicht mehr, mit Mitarbeiterinnen und Mitarbeitern nach Gutsherrenart umzugehen. Ein einseitig autokratischer Führungsstil neutralisiere die Vielfalt des Wissens, der Perspektiven und Herangehensweisen, die zur Bewältigung der heutigen Komplexität im Organisations-

geschehen dringend benötigt werde und die prinzipiell jeder Belegschaft innewohne. Mit Diversity Management sei eine neue Management-Disziplin entstanden. Der Erfolgsbeitrag sei nicht unmittelbar messbar. Vielfalt sei eine immaterielle Ressource, die sich meist indirekt, verzögert und im Verbund mit anderen Ressourcen auf den Ertrag auswirke. Diversity Management müsse integrativ gedacht werden. Intelligent genutzte Vielfalt trage zur Abwehr von Unternehmenskrisen bei, weil sich dadurch Unternehmen schneller an sich ändernde Marktbedingungen anpassen können.

Datenschutz

Security insight plädiert in Ausgabe 6-2015 für **Datenschutz im Unternehmen** (S. 8–11). Werde dem Datenschutzbeauftragten des Unternehmens von der Aufsichtsbehörde die notwendige Fachkunde nicht zuerkannt, so werde der Fall so behandelt, als sei überhaupt kein Datenschutzbeauftragter bestellt worden. Das Bayerische Landesdatenschutzamt habe im Fall einer datenschutzrechtlich unzulässigen Übertragung von E-Mail-Adressen von Kunden eines Online-Shops im Zuge eines Asset Deals Geldbußen in fünfstelliger Höhe sowohl gegen das veräußernde als auch gegen das erwerbende Unternehmen festgesetzt. Datenschutz beginne bereits mit einer zuverlässig arbeitenden elektronischen Zutrittskontrolle im Unternehmen. Auf jeden Fall sei gefordert, den Server in einem gesonderten Raum unterzubringen, zu dem nur Berechtigte Zutritt haben (§ 9 Abs.1 BDSG). In dieser Norm seien auch Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrollen geregelt. Außerdem sei „zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können".

WiK berichtet in der Ausgabe 6-2015, S. 7, über eine europaweite Umfrage von Ipswitch bei 300 IT-Spezialisten in GB, Deutschland und Frankreich zum Thema neue **EU-Datenschutz-Grundverordnung** (GDPR). Die Verordnung habe vor allem Auswirkungen auf alle Unternehmen, die personenbezogene Daten von Mitarbeitern, Kunden oder Partnern sammeln, speichern, verarbeiten und weitergeben. Mehr als zwei Drittel der befragten IT-Experten erwarteten dabei eine finanzielle Belastung für ihr Unternehmen allein dadurch, dass sie sich über die neuen Datenschutzanforderungen auf dem Laufenden halten müssen. 69 Prozent hätten angegeben, in neue Technologien und Dienstleistungen investieren zu müssen. Immerhin 18 Prozent der Umfrageteilnehmer wüssten überhaupt nicht, ob die GDPR Auswirkungen auf ihr Unternehmen haben wird.

EU-Kommission verlangt Zusagen bei Datenschutz, titelt die FAZ am 7. Dezember. Google, Facebook, Amazon und andere **amerikanische Internetunternehmen** sollten künftig keinen Freischein mehr für die Übertragung europäischer persönlicher Daten in die USA mehr bekommen. Dafür habe sich EU-Justizkommissarin Véra Jourová ausgesprochen. Das Nachfolgeabkommen für das vom EuGH für nichtig erklärte Safe-Harbor-Abkommen solle engmaschig überwacht werden können. Sie fordere ein „System von Vertrauen und Kontrolle". Es dürfe nie mehr der Verdacht einer Massenüberwachung durch die amerikanischen Geheimdienste aufkommen.

Diebstahl

Der Diebstahl von Oberleitungen, Signalkabeln und sonstigen Kupfergegenständen bei der Bahn sei 2015 deutlich geringer ausgefallen als in früheren Jahren, meldet die FAZ am 31. Dezember: ein Rückgang um gut 30 Prozent. Als ein Grund werde der drastisch gesunkene Kupferpreis genannt. Zugleich schreibe sich die Bahn aber auch Erfolge bei der Bekämpfung dieser Kriminalität zu. Dazu

gehörten häufigere Streifen der Bundespolizei an gefährdeten Stellen. Außerdem sei Material mit sogenannter künstlicher DNA gekennzeichnet worden.

Einbruch

Über den Einsatz des Softwareprogramms „Precobs" zur **Vorhersage von Einbruchsörtlichkeiten** durch die Züricher Polizei berichtet die FAZ am 15. Dezember. Ein erfolgreicher Einbruch sporne den Einbrecher an, an den Ort des Geschehens zurückzukehren. Dann steige die Wahrscheinlichkeit, dass der Täter in den nachfolgenden vier Wochen im Umkreis von 200 bis 400 Metern wieder zuschlägt. Da setze Precobs an. Die Polizeibeamten geben noch am Tatort alle relevanten Informationen zum Tathergang in ihre iPads ein. Bereinigt um personenbezogene Daten errechne die Software darauf binnen Minuten die künftige Einbruchswahrscheinlichkeit in dem betreffenden Stadtgebiet. Precobs verbessere die Prognosequalität und erlaube es, die Polizeikräfte effizienter einzusetzen. Die Einbrüche seien in den mit Precobs überwachten Gebieten 2014 um 15 Prozent gesunken, wobei allerdings die Ursache für den Rückgang nicht eindeutig dem neuen Computerprogramm zugeschrieben werden könne.

Einzelhandelssicherheit

Dass Einzelhändler auch beim **Ladenbau** Sicherheitsaspekte beachten müssen, betont Dr. Wolfram Krause, div-Netzwerk Ladenbau e. V., in Security insight (Ausgabe 6-2015, S. 44/45). Einzelhändler, Planer und Ladenbauer müssten bei der Erstellung des Sicherheitskonzepts eng zusammenarbeiten. So würden Kenntnisse über mögliche Sicherheitslücken, der Umgang mit Kunden mit bestehenden Sicherheitseinrichtungen und aufgetretene neue Betrugs- und Diebstahlmaschen mit den Informationen über modernste Möbel-, Schließ- und Sicherheitssysteme, intelligente Videoüberwachung und sinnvolle Integration von Alarmanlagen zusammengebracht und aufeinander abgestimmt. Wichtig sei auch das Wissen um versicherungsrechtliche Erfordernisse und die dazugehörigen rechtlichen Grundlagen.

Videosurveillance as a service werde immer attraktiver, betont Axis Communications GmbH in der Ausgabe 12-2015 der Zeitschrift GIT, S. 40/41. Der Einzelhändler spare sich dadurch jeglichen Aufwand, wenn er sein Kamerasystem über einen Hosted Video Service bucht. Eine gehostete Lösung beschränke die Grundinvestition auf eine Kamera und eine Internetverbindung. Der Hosting-Provider übernehme die Datenspeicherung gegen eine geringe monatliche Gebühr.

Evakuierung

Michael Schümperli, Siemens Building Technologies, befasst sich in der Ausgabe 6-2015 der Zeitschrift Sicherheitsforum, S. 35/36, mit der **Vorbereitung einer Gebäudeevakuierung**. Es seien komplexe Simulationstechnologien entwickelt worden, die präventiv erkennen, wo bei einer Gebäudeevakuierung gefährliche Situationen entstehen könnten. Siemens habe eine solche Software entwickelt, die die Bewegung von Personenströmen vorausberechnet und Evakuierungsszenarien testet. Die Forscher nutzten ein aggregierendes Verfahren: Räume würden in einzelne Zellen unterteilt, die dem Platzbedarf eines Menschen entsprechen. Das Verhalten leerer und besetzter Zellen werde mittels Kraftfelder definiert. Ausgangspunkte und Zielorte der Personen könnten eingefügt werden, ebenso Hindernisse wie geparkte Fahrzeuge oder Feuer. Gegenständen werde dabei eine andere Wirkung zugewiesen als Menschen, das Verhalten Einzelner wiederum

anders definiert als das einer Gruppe. Das Modell könne auf diese Weise simulieren, wie sich Mengen von Hunderten oder Zehntausenden von Menschen verhalten – und zwar zehnmal schneller als sie sich in Echtzeit bewegen. Koppele man die **Cowd Control Software** mit realen Informationen aus Überwachungskameras lasse sich die Bewegung von Menschenmassen bis zu fünf Minuten im Voraus prognostizieren. Basierend auf CAD-Daten des Baukörpers generiere die Software automatisiert ein 3-D-Modell. Sie errechne und visualisiere in 2-D oder 3-D die möglichen Fluchtwege sowie das zu erwartende Menschenaufkommen. Crowd Control simuliere auch die Auswirkung von Hindernissen auf die Evakuierung.

Geldautomatensicherheit

Beim BKA sind nach einer Meldung der FAZ vom 23. Dezember in diesem Jahr **bis November 63 Fälle** bekannt geworden, bei denen Kriminelle Geldautomaten in die Luft sprengten. Nur in 34 Fällen seien sie dabei an Geld gelangt. 2014 und 2013 seien es deutlich mehr Fälle gewesen. In der Regel würden die Täter die Automaten luftdicht abkleben, Gas hineinleiten und sie dann in die Luft sprengen. Sprengstoff komme nur in wenigen Fällen zum Einsatz. Das LKA NRW vermute Gruppen aus den Niederlanden hinter den Taten. In NRW hätten die Sprengräuber 2015 schon 40 Mal zugeschlagen. Der Dachverband Deutsche Kreditwirtschaft betone, gemessen an der Gesamtzahl von mehr als 60.000 Geldautomaten in Deutschland sei die Zahl der Angriffe überschaubar. Je nach Standort und Gefährdungslage würden die Institute selbst entscheiden, was sinnvoll sei: Einbruchmeldeanlagen, Videoüberwachung oder Erschütterungsmelder, in Einzelfällen auch Einfärbesysteme oder Gasdetektoren. Einige Banken würden ihre Selbstbedienungsläden über Nacht abschließen. Dass der Einsatz von Farbkartuschen Aufbrüche verhindere, dafür gebe es keinen statistischen Beleg.

Im Interview nimmt im Sicherheits-Berater direkt vom 17. Dezember Uwe Hoffmeister, von zur Mühlen'sche Sicherheitsberatung, zur Möglichkeit der **Sicherung von Geldautomaten (GA) gegen Sprengung** Stellung. Da die Sprengungen mit Hilfe von Gas vorgenommen werden, wäre hier der Hebel anzusetzen. Es dürfe einfach kein Gas mehr in Geräteöffnungen eingeleitet werden können. Hier seien bauliche Veränderungen am GA, speziell am Shutter, dringlich. Es gebe im übrigen zahlreiche Ansatzpunkte für Vorbeugungsmaßnahmen, die ausführlich in der VdS 5052 beschrieben seien.

Geldraub

Bei dem Überfall auf der Richterstraße im Dortmunder Stadtteil Bodelschwingh haben nach einem Bericht der WAZ vom 14. Dezember die Täter mit zwei Fahrzeugen den Geldtransporter des Sicherheitsunternehmens Kötter eingekeilt. Sie bedrohten den Fahrer mit einer Panzerfaust und eröffneten das Feuer mit Schnellfeuerwaffen noch unbekannter Bauart. Dabei zielten sie auf die Motorhaube des gepanzerten Geldtransporters. Die Geschosse trafen nicht das Personal im Transporter. Nachdem die Räuber mitten im Wohngebiet eine Seitentür des Transporters aufgeflext hatten, flüchteten sie mit einem Teil der Beute. Die Polizei geht davon aus, dass bei dem Überfall vier Täter am Werk waren. Ein Fahrzeug ließen die Täter mit laufendem Motor stehen, ein anderes setzten sie in Brand.

Industrie 4.0

Bernd Schöne, freier Journalist, befasst sich in der Ausgabe 12-2015 von PROTECTOR,

S. 46/47, mit der **Sicherheitsproblematik der Industrie 4.0**. Die Herausforderung bestehe darin, Connectoren beziehungsweise Gateways so zu entwickeln, damit bestehende Maschinen in die Wertschöpfungsnetzwerke integriert werden können, wie Michael Jochem, Sicherheitsexperte beim Bosch **Innovationscluster „Connected Industry"** erläuterte. Darüber hinaus müssten neue Industrie 4.0-Komponenten die nötigen Security-Fähigkeiten bereits erhalten. Erstmals sei die Produktionstechnik direkt mit Schädlingen aus der PC-Welt konfrontiert. Den klassischen Virenscanner werde es definitiv nicht geben. Schon der Update-Prozess würde zum Stillstand der Maschinen führen. Whitelisting sei ein geeigneteres Mittel. Nur erlaubte und geprüfte Software komme dann im Maschinenpark zum Einsatz. Selbstverständlichkeiten der Office-IT könnten schnell desaströse Reaktionen auslösen, wenn man sie ohne Anpassung auf die Produktion überträgt. Unternehmen wäre zu empfehlen, kombinierte Teams aus IT-Experten und Produktionsspezialisten zu bilden, die auf gleicher Augenhöhe eine gemeinsame Sicht auf die Risiken und Gegenmaßnahmen einer vernetzten Produktion entwickeln, erläutert Marcel Kisch, IBM. Da sich die Produktionsumgebung vielschichtig von der Office-Umgebung unterscheide, sollte die Bereitschaft zur Entwicklung risikobasierter kompensierender Maßnahmen gefördert werden. Vertraulichkeit, Integrität und Verfügbarkeit des Netzwerks müssten gewährleistet sein.

Ein Verlagsspezial der FAZ am 15. Dezember enthält Diskussionsbeiträge von Experten zur Problematik der Vernetzung der Unternehmen mit Kunden und Lieferanten im Rahmen von Industrie 4.0. Die Produktion sei bei **Industrie 4.0 höheren Risiken ausgesetzt**. Bei der Frage nach der Sicherheit gehe es darum, wer alles auf eine Maschine zugreifen dürfe. Die Möglichkeit der Fernwartung berge auch ein Gefahrenpotenzial. Perimeterschutz sei heute nicht mehr das einzige Mittel der Wahl. Man gehe bei der IT-Sicherheit vielmehr weg vom reinen Schutz und von der reinen Absicherung, das heißt, es komme zusätzlich verstärkt auf die Erkennung von Vorfällen und die Reaktion darauf an. Abschotten sei früher gewesen. Jetzt gehe es um Awareness in der IT-Security. Die Awareness sei sehr hoch. Wichtig sei die Zusammenarbeit der Fertigung und der IT, um im Fertigungsbereich die IT-Sicherheit zu gewährleisten. Am besten sei immer ein optimales Update der Software für die Maschinen. Auf bestimmte Muster müsse man schnell reagieren, ein Fehlverhalten lasse sich beispielsweise an den Veränderungen von Kennziffern in der Produktion oder auch über einen durch eine End-to-End-Security-Überwachung entdeckten unangebrachten Datenaustausch erkennen. Der Schutz der Programme erfolge am besten über eine Whitelist. Da werde nur das ausgeführt, was da eingetragen ist. Aber das sei Aufwand, das müssten Mitarbeiter ständig überwachen. Eine Whitelist sei ein von den Mitarbeitern akzeptiertes Mittel.

IT-Sicherheit

Nach einer Meldung in der Ausgabe 6-2015 der Zeitschrift WiK, S. 11, rechnen laut einer aktuellen Studie der NIFIS Nationale Initiative für Informations- und Internet-Sicherheit mehr als die Hälfte der befragten Unternehmen mit steigenden **Ausgaben für IT-Sicherheit und Datenschutz 2016**. Dabei gingen 44 Prozent von einer Steigerung um mindestens ein Drittel, neun Prozent von einer Verdopplung der Ausgaben aus.

Wie die Zeitschrift GIT in der Ausgabe 12-2015, S. 63/64, berichtet, hat das Marktforschungs- und Beratungshaus Techconsult ein Strategiepapier erstellt, das Mittelstand und Behörden Hilfestellung dabei bieten solle, die IT- und Informationssicherheit langfristig zu verbessern. Die Basis bilde eine repräsentative Befragung mit über 500 Interviews

in Unternehmen und Verwaltungen mit 20 bis 2.000 Mitarbeitern. Ein Fazit der Studie: Knapp die Hälfte der befragten mittelständischen Unternehmen und öffentlichen Verwaltungen wiesen dringenden Handlungsbedarf auf. Das Strategiepapier beschreibt fünf Schritte zur IT-Sicherheit: Standortbestimmung, Budgetplanung, Umsetzung, Überprüfung der Umsetzung und Security-Check, basierend auf der Studie.

Privilegierte Benutzerkonten stellen für jedes Unternehmen eine erhebliche Sicherheitsgefahr dar, heißt es in der Dezember-Ausgabe des Behörden Spiegel. Die klassische Perimetersicherheit mit der Nutzung von Firewalls, Antiviren-Scannern oder Webfilter-Techniken biete keinen ausreichenden Schutz mehr vor externen Angriffen. Die Frage: „Wie kann die Sicherheit aufrechterhalten werden, wenn sich der Angreifer bereits innerhalb des Netzwerks befindet?" sei in der Vergangenheit eher nicht gestellt worden. Es gehe um einen Paradigmenwechsel im Bereich der IT-Sicherheit. Der Fokus dürfe heute nicht nur auf dem Aufspüren und der Abwehr von Angriffen liegen. Ebenso wichtig sei auch das Ergreifen geeigneter Schutzmaßnahmen, und zwar in den Bereichen Rechtemanagement und privilegierter Zugriff. Systeme und Applikationen selbst in den Mittelpunkt der Sicherheitsstrategie zu rücken, das sei auch der Ansatz von Privileged Account Security-Lösungen, mit denen privilegierte Zugriffe auf beliebige Zielsysteme zentral berechtigt, jederzeit kontrolliert und revisionssicher auditiert werden könnten. Zur Sicherung von Benutzerkonten mit erweiterten Rechten seien mehrere Tools auf dem Markt verfügbar. Konkret müsse eine Sicherheitsapplikation drei Leistungsmerkmale bieten: Zugriffskontrolle, Überwachung und Reaktionsmöglichkeit. Grundvoraussetzung sei, dass sie eine Kontrollfunktion für die Verwendung von Passwörtern und den Zugriff auf Zielsysteme enthalte. Eine zukunftsweisende Lösung im Bereich Privileged Account Security biete auch Echtzeit-Analytik und -Alarmierung bereits bei verdächtigen Aktivitäten im Zusammenhang mit privilegierten Konten; das betreffe z. B. abweichende Zugriffszeiten oder die ungewöhnliche Häufung von Zugriffen. Das biete Unternehmen einen Basisschutz, um die Gefahr der Wirtschaftsspionage zu vermindern.

Mit **Microsoft Azure** seien die Bereitstellung von Remote-Desktops sowie die Authentifizierung aus einer Hand möglich, meldet TECCHANNEL.de am 15. Dezember. Um Prozesse zu beschleunigen, sei die Verfügbarkeit von Remote-Diensten über das Internet heute unabdingbar. Doch dies berge bei fehlender Verschlüsselung höhere Risiken für das Unternehmen. In der klassischen Konfiguration werde oft nur auf Benutzername und Passwort zur Anmeldung gesetzt, während die Verbindung zwischen Endnutzer und Rechenzentrum nicht gesichert sei. Gefälschte E-Mails an die Buchhaltung seien schnell gesendet und schon stünden Tür und Tor offen, um sich am Remote Desktop WebAccess anzumelden und eine Verbindung direkt in das Rechenzentrum aufzubauen. Multifaktor-Authentifizierung sei eigentlich bereits Branchenstandard im Netz. Doch es verwundere mitunter, dass sogar große Anbieter mit der Umsetzung des zusätzlichen Sicherheitsfaktors noch hinterherhinken.

Angreifer nehmen vor allem kleine und mittlere Unternehmen ins Visier, berichtet die Wirtschaftswoche am 4. Dezember. Denn diese gelten nicht nur als innovativ, sondern verfügten oft über besonderes Know-how. Insbesondere kleine Unternehmen nähmen es zugleich mit der Sicherheit nicht immer genau. Zwar setze die Mehrzahl der Unternehmen heute Abwehrprogramme wie Virenscanner und Firewalls ein. Doch dieser Grundschutz reiche nicht mehr. Längst seien die Angriffe von Cyberkriminellen so raffiniert, dass sie von herkömmlichen Antivirenprogrammen nicht mehr erkannt werden. Dabei sei es gar nicht so schwer, ein höheres Sicherheitsniveau zu erreichen. Das beginne damit,

dass Betriebssysteme und Softwarepakete regelmäßig auf den neuesten Stand gebracht sowie die Sicherheitsaktualisierungen eingespielt werden. Die nächste Sicherheitsstufe erreichten Unternehmen durch mehr Passwörter und Verschlüsselung. Firmen, die ihre Beschäftigten mit Schulungen auf die Risiken vorbereiten, würden sicherer leben.

„Die beliebtesten Passwörter heißen 123456 und password", titelt die FAZ am 31. Dezember. Wie das Hasso-Plattner-Institut auf der Basis von Millionen Datensätzen festgestellt habe, stehen bei den Internetnutzern in aller Welt immer noch Zahlenreihen oder Zeichenfolgen auf der Tastatur an der Spitze der Beliebtheitsskala bei Passwörtern. Gern würden auch Vornamen oder andere Begriffe aus dem Wörterbuch verwendet. Unangefochten auf dem ersten Platz liege nach wie vor die Zahlenreihe „123456", obwohl automatische Cracker solche simplen Passwörter als erstes und blitzschnell ermitteln. In Fällen von geraubten Identitätsdaten stehen laut den Statistiken des Instituts Passwörter mit weitem Abstand an der Spitze der entdeckten sensiblen Informationen. Nach Häufigkeit sortiert folgten dann Vor- und Zunamen und Kreditkartendaten.

IuK-Kriminalität

Die EU verschärft ihren Kampf gegen die Angriffe von Hackern auf wichtige Infrastrukturbetreiber und Internetdienstleister, berichtet die FAZ am 9. Dezember. Die neue **Richtlinie zur Netzwerk- und Informationssicherheit**, kurz NIS, soll für wichtige Infrastrukturbetreiber im Energie-, Transport-, Bankensektor, der Wasserversorgung und im Gesundheitswesen gelten. Betroffen seien zudem Internetkonzerne von Suchmaschinen wie Google über Internetmarktplätze wie Ebay bis zu Anbietern von Cloud-Diensten wie Amazon. Die Unternehmen sollten größere Vorfälle den nationalen Behörden melden. Dabei gehe es nicht um Vorfälle, die den Verlust persönlicher Daten betreffen, sondern um Schäden für die Sicherheit der betroffenen Netze. Im Mittelpunkt stünden Betrugsversuche und die gezielte Überlastung von Servern durch Angriffe von Hackern. Für soziale Netzwerke wie Facebook sollten die Vorgaben hingegen grundsätzlich nicht gelten. Geben die Unternehmen die Vorfälle nicht weiter, drohten ihnen Strafen. Die EU-Staaten werden aufgefordert, nationale Strategiepläne für den Kampf gegen die Kriminalität im Internet vorzulegen. Jede Regierung solle eine zentrale Einrichtung für die Cyberabwehr aufbauen sowie Notfall- und Abwehrpläne erstellen. Zudem solle die Kooperation zwischen den nationalen Behörden verbessert werden. Nach Angaben der zuständigen EU-Agentur ENISA verursachten Cyberattacken jährlich einen Schaden von bis zu 340 Mrd. Euro.

In manchen Postfächern landen täglich Dutzende **von Trojaner-verseuchten Mails**, berichtet heise.de am 8. Dezember. Antiviren-Programme hielten Mail-Nutzern zwar viele davon automatisch vom Leib, aber bei Trojanern, die neu konzipiert sind, könne es eine Weile dauern, bis die Antiviren-Hersteller ihre Software angepasst haben. Ein aktuelles Beispiel dafür seien Trojaner-Mails, die mit dem Mail-Envelope Sender kreditoren@dertour.de übermittelt werden. Die unter diesem Absender verschickten Trojaner-Mails enthielten Schadroutinen, die noch kaum ein Viren-Scanner erkennt. Unter anderem verschlüssele die Schadsoftware die Festplatte des Empfängers, wenn dieser den Anhang per Doppelklick öffnet. Als erste Hilfe, bis die Antiviren-Software auf den neuen Angreifer anschlägt, könnten Administratoren von zum Beispiel Firmen-Mailservern einen einfachen Reject-Filter aufsetzen.

Der Sonderbericht Wirtschaftsschutz der Bundessicherheitsbehörden vom 14. Dezember geht auf einen mutmaßlichen **Versuch eines elektronischen Angriffs gegen Ener-**

gieversorgungsunternehmen ein. Mit dem Hinweis auf einen möglichen Hackerangriff und die Domain „domaintoolz.net" habe sich das Unternehmen an das BfV gewandt. Die daraufhin vorgenommenen Analysen hätten zu einer möglichen Verbindung zum Schadprogramm „Energetic-Bear" geführt. Hierbei handele es sich um einen Schadcode, der in sogenannten „Advanced Persistent Threats" (APT) eingebunden wird. APT seien komplexe und nachhaltige elektronische Angriffe zur Ausforschung bzw. Sabotage. Von „Energetic-Bear" seien Pressemeldungen zufolge in der Vergangenheit weltweit u. a. zahlreiche Unternehmen angegriffen worden, darunter auch europäische und US-amerikanische Energieunternehmen. Der vermutete osteuropäische Ursprung dieser Schadsoftware habe bisher nicht eindeutig verifiziert werden können. Das vertrauliche Zusammenwirken des Unternehmens mit dem BfV habe zu einer schlüssigen Bewertung des Datenverkehrs und nachfolgenden Maßnahmen zum Schutz der Informationstechnik des betroffenen Unternehmens geführt.

Seit mindestens Juni 2015 sei eine Gruppierung aktiv, die weltweit Wirtschaftskonzerne angreift, meldet der Sonderbericht Wirtschaftsschutz der Bundessicherheitsbehörden vom 14. Dezember. Dabei nutze sie ein hochprofessionelles Schadprogramm, welches oftmals von kommerziellen Antivirenprogrammen nicht erkannt wird. Das in der Angriffs-Mail verwendete Social-Engineering sei als besonders hochwertig zu bezeichnen. Es habe allerdings auch einen hohen Wiedererkennungswert. Um festzustellen, ob das Unternehmen von dieser Angriffskampagne betroffen ist, empfiehlt das BfV: „Suchen Sie in den E-Mail-Eingängen nach dem oben in der Mail genannten Absender und Betreff. Überprüfen Sie, ob ähnliche E-Mails (z. B. Reporter droht mit imageschädigender Veröffentlichung) eingegangen sind. Wenn das Unternehmen Netzwerk-Logs nach Netzwerk-IOC durchsehen oder nach Host-IOC (z. B. extrahierte Dateien) überprüfen möchte, wenden Sie sich bitte per E-Mail an das BfV: sensea@bfv.bund.de."

In den vergangenen Monaten beobachteten das BSI und andere Sicherheitsbehörden vermehrt Angriffe auf deutsche Unternehmen, heißt es im Sonderbericht Wirtschaftsschutz der Bundessicherheitsbehörden vom 14. Dezember. Einfallstor seien häufig Personalabteilungen, denen in einem aktuellen Fall die **Ransomware Chimera** untergeschoben werden sollte. Bei genauer Betrachtung des Download-Links habe sich jedoch herausgestellt, dass es sich bei den angeblichen Dokumenten in Wirklichkeit um eine exe-Datei handelte. Diese habe die Ransomware Chimera installiert, welche Festplatteninhalte verschlüsselt und mit der Veröffentlichung droht, falls ein gefordertes Lösegeld nicht gezahlt wird. Ist der Computer, auf dem die Malware installiert ist, mit einem Netzlaufwerk verbunden, würden mitunter nicht nur die eigene Festplatte, sondern auch die Daten auf den Netzlaufwerken verschlüsselt. Existierten keine Backups, habe das Unternehmen in der Folge keinen Zugriff mehr auf die eigenen Daten. Ob diese wiederhergestellt werden können, sei zum jetzigen Zeitpunkt noch unklar. Für die Opfer könne der Chimera-Angriff somit existenzbedrohende Folgen haben.

Über neue Bedrohungsszenarien auf Smartphone und Tablets berichtet der Sonderbericht Wirtschaftsschutz der Bundessicherheitsbehörden vom 14. Dezember. Mobile Endgeräte und die darauf installierten Anwendungen spielten im Kampf gegen Cyberangriffe eine immer größere Rolle. Ständig werde neue Malware entdeckt, mit deren Hilfe Täter versuchten, Kommunikationsdaten auf Smartphones und Tablets oder in deren unmittelbarer Umgebung, mitzuschneiden. In seinem **Mobile Malware Report** berichte das Unternehmen G-DATA, dass es bei Untersuchungen verschiedener Android Smartphones 24 Modelle von zum Teil namhaften Herstellern gefunden hat, bei denen bereits ab Werk Malware zur Spionage vorinstalliert

war. Im September 2015 seien Meldungen aufgetaucht, wonach mehrere hundert Apps im Store von Apple mit Schadsoftware infiziert seien. **Im November 2015 hätten zwei Sicherheitsforscher auf der PacSec-Konferenz in Tokio gezeigt, wie sich** das derzeitige Top-Smartphone eines bekannten Herstellers zu einer Wanze umfunktionieren lässt.

Deutsche Unternehmen sehen sich einer latenten Cyberbedrohung unterschiedlicher Quantität und Qualität ausgesetzt, die sowohl von ausländischen staatlichen als auch von nichtstaatlichen Stellen ausgeht, heißt es im Sonderbericht Wirtschaftsschutz der Bundessicherheitsbehörden vom 14. Dezember. Die dafür erforderliche Spionage-Software werde auf kommerzieller Basis weltweit vertrieben. Insbesondere die staatlichen Kunden dieser Software setzten oft mehrere unterschiedliche „Cyberspionage"-Produkte ein. So sei beispielsweise nach den Veröffentlichungen sensibler interner Daten eines ausländischen Unternehmens für Überwachungs- und Spionagesoftware ein Teil von dessen vertriebenen und in Betrieb befindlichen Produkten quasi unbrauchbar. Infolgedessen sei ein Rückgriff ausländischer staatlicher Akteure auf nationale, kommerzielle Spionagesoftware eine plausible Alternative. Die weit verbreitete Abstützung von ausländischen Sicherheitsbehörden auf kommerzielle Cyberspionageprodukte aus dem Internet zeige den hohen Stellenwert dieser Beschaffungsart in vielen Staaten. Es seien einige Fälle bekannt, bei denen ausländische Staaten Produkte von mindestens drei unterschiedlichen Anbietern aus verschiedenen Ländern einsetzen.

Sicherheitsforscher seien einer Advanced Persistent Threat-Gruppe auf der Spur, die Android-Nutzern **Weihnachts-Apps** unterjubeln wollen, die Smartphones in Wanzen verwandeln, meldet heise.de am 16. Dezember. Die Command and Control-Server zum Sammeln der Daten sollen von Deutschland aus arbeiten. Die Sicherheitsforscher hätten verschiedene Spionage-Apps in Google Play vorgefunden, die sich etwa als Weihnachtsspiel tarnen.

Wie die FAZ am 23. Dezember meldet, haben es beim IT-Sicherheitsunternehmen „SR Labs" Hacker geschafft, die Funktion der Überweisung des Kaufpreises zu hacken und Geld von den Konten der Händler auf ihre eigenen Konten zu überweisen. Kriminelle könnten so potenziell unbegrenzt Geld stehlen. Die Vorgehensweise sei übersichtlich: Kriminelle müssten sich auf Ebay ein gebrauchtes Kartenterminal kaufen. Dann würden sie eine Verbindung zum Kartenzahldienst aufbauen und ihr den Auftrag geben, Geld auf ihr Konto zu überweisen. Dabei würden sie sich als Händler ausgeben. Dazu bräuchten sie vor allem die Nummer des Händlerterminals, und die stehe auf jedem EC-Beleg. Zudem ließen sich die Nummern leicht erraten, wenn man erst mal eine kennt. Zwar seien die Terminals mit einem Passwort geschützt, aber gerade beim wichtigsten Terminalhersteller sei das Passwort immer das gleiche. Das Geld müsse nicht einmal auf ein Konto fließen. Denn die Terminals könnten oft auch Guthaben für Handy-Prepaidkarten ausstellen.

„Kunden aus dem Darknet" titelt die Wirtschaftswoche am 18. Dezember. Eigentlich habe die Post ihre **Packstationen** neben Supermärkten oder auf Parkplätzen gebaut, damit Berufstätige dort nach Feierabend ihre online bestellten Sendungen abholen können. Doch die gelben Kästen lockten neue, ungebetene Kunden an: Drogendealer würden über sie Stoff vertreiben, Hehler das System als Umschlagsort missbrauchen. Empfänger könnten sich hinter einem falschen Namen verstecken. Dazu verwendeten sie gefälschte Ausweise, um sich für die Packstation zu registrieren. Oder sie würden die Daten im Internet stehlen oder kaufen. So ein Account koste 20 bis 30 Euro. Inzwischen müssten Kunden für jede Abholung einen neuen Code eingeben, den sie aufs Handy erhalten: Doch

auch dieses System könnten die Darknet-Verbrecher jetzt umgehen. Sie eröffneten ein Nutzerkonto bei der Post unter falschem Namen und kauften eine SIM-Karte für ein Handy bei einem Billiganbieter, der schon mal auf die vorgeschriebene Ausweiskontrolle verzichte.

Krisenmanagement

Die FAZ weist am 7. Dezember auf ein Buch von Marco Mansdörfer/Jörg Habetha mit dem Titel „Strafbarkeitsrisiken des Unternehmens" (Verlag C.H. Beck, München 2015, 270 Seiten, 65 Euro) hin. Verhaltensstrategie, Krisenmanagement und Compliance für Unternehmer würden versiert beschrieben. Viele Praxishinweise und Checklisten gäben dem Leser ein Gefühl, wann der „Ernstfall" eintreten kann und was zu tun ist, um genau dies zu verhindern.

Krisenregionen

Von CONIAS Risk Intelligence (CRI) würden seit mehr als 20 Jahren Häufigkeiten und Dynamiken politischer Konflikte systematisch in einer Datenbank erfasst und analysiert, meldet WiK in der Ausgabe 6-2015, S. 11. Die Daten sowie die daraus gewonnenen Erkenntnisse würden der Industrie aussagekräftig zur Risikobewertung und -minimierung zur Verfügung gestellt.

Maschinensicherheit

Eine **neue Generation von Sicherheits-Laserscannern** stellt Patrick Hochleitner, Sick AG, in der Ausgabe 12-2015 der Fachzeitschrift GIT, S.76/77, vor. Sicherheits-Laserscanner arbeiteten nach dem Funktionsprinzip der Lichtlaufzeitmessung und würden Distanzen sicher und zuverlässig messen. Bei der Lichtlaufzeitmessung sende der Sensor einen Pulsstrahl aus, den das zu detektierende Objekt – z. B. eine sich nähernde Person – reflektiert. Die Laufzeit, die der Strahl für die Strecke benötigt, werde ausgewertet und so die Distanz zum Objekt berechnet. Befindet sich eine Person im Gefahrenbereich, sende der Sicherheits-Laserscanner ein Stoppsignal an die Maschine. Mit dem microScan3 präsentiere Sick die neue Generation. Der Scanner erfülle hohe internationale Sicherheitsstandards und sichere Gefahrbereiche, Zugänge und Gefahrstellen zuverlässig ab. Jedes Detail sei neu durchdacht worden. Die Zuverlässigkeit des microScan3 sei herausragend. Der Laserscanner sei äußerst belastbar und zeichne sich durch seine Langlebigkeit aus. Die neue Konfigurations- und Designsoftware Safety Designer ermögliche eine spielend einfache Konfiguration und Inbetriebnahme. Das patentierte Verfahren liefere durch intelligente Filterung und Auswertung der vielen Einzelpulse ein für Sicherheits-Laserscanner einzigartiges Messergebnis. Die Anwendungsgebiete seien vielfältig: Er sichere Gefahrbereiche an Belade- und Entladestationen, mehrseitige Zugänge an Maschinen und Materialschleusen, Maschinen in rauen Umgebungen sowie Gefahrstellen mit bis zu 30 mm Objektauflösung ab und gewährleiste Hintertretschutz, um unbeabsichtigtes Wiederanlaufen einer Maschine zu verhindern.

Dr. Volker Rohbeck, Leuze electronic, setzt in der Ausgabe 12-2015 der Zeitschrift GIT, S. 80/81, seinen Beitrag in der Ausgabe 11-2015 zum Trendthema **Muting** fort. Beim meist verwendeten zeitgesteuerten Muting sei keineswegs nur die häufig anzutreffende Kreuzstrahl-Anordnung der Muting-Sensoren normativ zulässig. Besser geeignet könnten beispielsweise tastende Sensoren sein, die aus dem Gefährdungsbereich ausfahrendes Transportgut erfassen. Allerdings könnten tastende Sensoren in einigen Anwendungen in Verbindung mit bestimmten Materialien zu einer geringeren Verfügbarkeit der Objekterkennung führen. Bei der Appli-

kation sei stets darauf zu achten, dass keine ungesicherten großen Lücken neben dem Transportgut entstehen, die während des Mutings den Zutritt durch Personen ermöglichen. Aus Security-Sicht besser als Muting-Sensor geeignet seien solche optische Sensoren, die von Personen nicht mit einfachen Mitteln ausgelöst werden können, etwa induktive Sensoren, im Boden verlegte Induktionsschleifen, Codeleser oder RFID-basierte Systeme, sofern das zulässige Gebinde durch diese Sensoren erkannt wird. Die ursprüngliche Forderung nach einem überwachten Leuchtmelder werde durch die aktuelle Fassung der IEC/TS 62046 praktisch umgekehrt, weil ein Leuchtmelder nicht nur ein Warnsignal, sondern auch ein Manipulationsanreiz sein könne. Ein ebenso oft diskutierter als auch kritischer Punkt sei die von IEC/TS 62046 als eine Maßnahme normativ geforderte Muting-Zeitbegrenzung.

Organisierte Kriminalität

Wie das BKA in der Wochenlage am 11. Dezember mitteilt, ermittelt die Zentrale Kriminalinspektion Oldenburg seit Ende 2014 gegen eine bundes- und europaweit agierende litauische Tätergruppierung wegen Verdachts des schweren Bandendiebstahls. Die durch die Tätergruppierung entwendeten Sattelzugmaschinen und -Auflieger bzw. hochwertigen Pkw seien auf eigener Achse oder im Sammeltransport mit entwendeten Lkw per Kurierfahrer ins Ausland (Baltikum) verbracht worden. Vor Ort hätten Residenten mit russischem Migrationshintergrund Wohnungen für die Täter beschafft und potenzielle Tatorte ausgespäht. Vier Angeklagte wurden nun zu hohen Freiheitsstrafen verurteilt.

Perimetersicherung

Um ein Schutzkonzept optimal auf die Bedürfnisse großer Freilandflächen auslegen zu können, müssten mechanische Sicherungsmaßnahmen, elektronische Überwachung und organisatorische Sicherungsmaßnahmen zur Intervention ineinandergreifen, heißt es in Security Insight, Ausgabe 6-2015, S. 14/15). Für Großflächen sei die Kombination aus geschultem Personal und Sicherheitstechnik die optimale Lösung, um Manipulationen oder Vandalismus zu verhindern. Speziell für den Einsatz an abgelegenen, ungeschützten oder vorübergehenden Standorten habe VPSitex Deutschland GmbH das **System SmartTower** konzipiert. Die Produktserie vereine eine nachtsichtfähige, vandalismussichere Schwenk/Neige-Zoomkamera, eine Infrarotbeleuchtungseinrichtung, eine Vielzahl von Bewegungsmeldern, digitale Aufzeichnungssysteme und eine Lautsprecheranlage auf einem schnell einsatzfähigen Videoüberwachungsturm mit einer Höhe von sieben Metern. Neben der wetterfesten Sensorik lasse das System auch ein Ansprechen über Lautsprecher sowie das Einschalten von Infrarotscheinwerfern zu.

Cornelia Groß, Securiton, plädiert in der Ausgabe 6-2015 von Security insight, S. 16/17, für **Videoüberwachung mit Bildanalyse zur Sicherung von Freiflächen**. Das Firmengelände werde zumeist als Alarmzone definiert. Der Vorbereich stelle die Erfassungszone dar. Übertritt nun jemand diese imaginäre Grenze von außen nach innen, werde Alarm ausgelöst. Wer von innen nach außen geht, dürfe hingegen passieren. Intelligente Videobildanalyse schaue nicht nur einfach zu, sie erkennt schon vor der Tat das Gefahrenpotenzial durch den Grenzübertritt. Potenzielle Fehlerquellen wie stromernde Hunde, Vogelflug oder Dauerbewegungen von Bäumen im Wind sortiere das System aus. Für Freiflächen empfehle sich der Einsatz von Wärmebildkameras. Immer wichtiger werde der Schutz der Privatsphäre. Dafür habe Securiton das Videobildanalyse-Modul IPS Privacy Protection entwickelt. Damit würden Menschen und Gebäudeteile verschleiert und auf den Videobildern nur verpixelt dargestellt.

Ulrich Schwieger, Xtralis, geht in Ausgabe 6-2015 der Zeitschrift Security insight, S. 18/19, auf interdisziplinäre, multifunktionale, videobasierte **Sicherheitskonzepte zur Gefahrenfrüherkennung** und -abwehr bei der Perimetersicherung ein. Hervorragend geeignet für die Bewegungsdetektion im Außenbereich seien leistungsfähige Videoanalyse oder Hochleistungs-Passivinfrarotmelder (PIR). Beide Technologien erfüllten bei qualifizierter Planung und Installation ein hohes Maß an Detektionssicherheit. Eine besonders effektive Maßnahme, um Fehlalarm zu verhindern, die durch Umwelteinflüsse hervorgerufen werden, sei die Kombination unterschiedlicher Detektionstechnologien. Hier habe sich die Kombination und logische Verknüpfung von Videobewegungsanalyse und Passiv-Infrarotdetektion als zielführend erwiesen. Die Anforderungen an multifunktionale und interdisziplinäre Plattformen seien vielfältig. So müsse die Möglichkeit gegeben sein, unter Verwendung vorhandener oder leicht realisierbarer Kommunikationsstrukturen Sensoren, Aktoren, Bedienelemente und Kameras anzuschließen. Die Systeme müssten sich einfach in komplexe Kommunikationsinfrastrukturen, auch mit Fremdgewerken, integrieren lassen.

Personenschutz

Mit **notfallmedizinischer Ausbildung** im Personenschutz befasst sich Christian Schaaf, Corporate Trust Business Risk & Crisis Management GmbH, in Ausgabe 6-2015 der Zeitschrift WiK, S. 43/44. Die „unterste" Ausbildung, eine Sanitätshelferausbildung, werde in der Regel in 40–50 Stunden zu absolvieren sein. Die nächste Stufe sei die Ausbildung zum Rettungsdiensthelfer (Bayern) mit 160 Stunden Theorie sowie der gleichen Anzahl an Stunden im Krankenhaus und in der Rettungswache. Ergänzt man die Rettungsdiensthelferausbildung um jeweils 160 Stunden Rettungswagen-Praktikum auf einer Rettungswache und 160 Stunden in einem Krankenhaus (Notaufnahme, Intensivstation und OP), könne man sich am Ende eines weiteren 40-stündigen Lehrgangs zum Rettungssanitäter qualifizieren. Bereits in der Ausbildung könne mit einem speziell für den Personenschutz entwickelten Notfallrucksack trainiert werden.

Piraterie

Das Institut für Wirtschaftsschutz und Sicherheitsforschung (IWiS) vermittelt in Ausgabe 6-2015 der Zeitschrift Security insight, S. 54/55, Hintergrundinformation zur Pirateriepproblematik. Weltweit würden die Fallzahlen im ersten Halbjahr 2015 gegenüber dem Vergleichszeitraum 2014 deutlich ansteigen, vor allem vor Südostasien (um 21 Prozent), das sich damit als Pirateriebrennpunkt etabliert habe. Auch vor der Küste Westafrikas bleibe es gefährlich, Schwerpunkte seien die Gewässer vor Nigeria und das Nigerdelta. In Deutschland niedergelassene Sicherheitsunternehmen dürften nur mit BAFA-Zulassung bewaffnete Dienstleistungen zur Piratenabwehr anbieten. Sie hätten aufgrund von drei Umständen dadurch erhebliche Wettbewerbsnachteile: Das Verfahren gelte als zeitaufwändig und ressourcenfressend. Die Genehmigung von „Floating Armouries" sei ebenfalls zeitaufwändig. Und laut BAFA müssten die für maritime Sicherheit zugelassenen Teams mindestens vier Personen umfassen, die nachweislich nach § 10 SeeBewachV ausgebildet sind. Deutsche Sicherheitsdienstleister forderten an erster Stelle situationsbezogene Ausnahmeregelungen, die kleinere Sicherheitsteams möglich machten. Darüber hinaus solle die Einhaltung der Auflagen auch kontrolliert werden, um Chancengleichzeit zu schaffen. Hilfreich wäre sicherlich zudem, dass ausländische Unternehmen bei der Betreuung deutsch geflaggter Schiffe an die gleichen Auflagen gebunden sind wie deutsche Wettbewerber.

Rauchwarnmelder

Die **Brandschutznachrüstung in Nordsee-Filialen** thematisiert PROTECTOR in der Ausgabe 12-2015, S. 42/43. Rauchwarnmelder bewährten sich auch beim Schutz von Menschen und Sachwerten in kleineren gewerblichen Einrichtungen. Unterschiedliche Arten von Objekten stellten unterschiedliche Anforderungen an den anlagentechnischen Brandschutz. Beim typischen Altbau mit vielleicht einem einzigen Ladenlokal im Erdgeschoss seien dies funkvernetzte Rauchwarnmelder. Überall dort, wo sich auch während der Geschäftszeiten nicht ständig Personen aufhalten, sodass ein entstehender Brand unter Umständen erst spät bemerkt wird, in Lagerräumen, Toiletten, Sozial- und sonstigen Nebenräumen sowie auf den sie verbindenden Fluren seien in bisher 117 Nordsee-Filialen 1.845 Melder vom Typ Hekatron Genius Hx, jeweils mit Funkmodul Basis, montiert worden. Zur sicheren Übertragung des Funksignals besitze jeder funkvernetzbare Genius Hx einen Repeater. Er fungiere als Signalverstärker, indem er das Funksignal aufnimmt und an den nächstgelegenen Melder weiterleitet.

Schließsysteme

Fernando Pires, Morse Watchmans, behandelt in Ausgabe 12-2015 der Zeitschrift PROTECTOR, S. 34, das **Schlüsselmanagement in Gerichtsgebäuden**. Digitale Technologie und Systemintegration hätten im Zusammenspiel mit dem Wachstum netzwerk- und IP-basierter Systeme die Kapazitäten des Schlüsselmanagements grundlegend gewandelt. Während Schlüsselschränke früher lediglich abschließbar waren, könnten die Tools zur Verwaltung heute mit anderen physischen Sicherheits- und Betriebssystemen kommunizieren und seien in diese integrierbar. Berichte per E-Mail, in denen im Einzelnen aufgeführt ist, welche Schlüssel vorhanden oder entnommen seien und wer sie hat beziehungsweise hatte, informierten das Sicherheitspersonal und andere Beteiligte.

PROTECTOR gibt in Ausgabe 12-2015 (S. 35) eine **Marktübersicht zu 57 Hotelschließsystemen** von 29 Anbietern. Abgefragt wurden allgemeine Angaben und Systemeigenschaften (unter anderem Offlinefähigkeit, Programmierung, optische und akustische Signalisierung am Beschlag, Verkabelung, Protokollierung im Schloss).

In einem in der Ausgabe 12-2015 der Zeitschrift GIT veröffentlichten Interview nimmt Prof. Dr.-Ing. Kai-Dietrich Wolf, Bergische Universität Wuppertal, zu Übertragungssystemen und der **Authentifizierung mit Mobiltelefonen** Stellung (S. 17–19). Es handle sich im immobilen Bereich meist um RFID-Systeme, die die drahtlose Authentifizierung bewerkstelligen. Das funktioniere mit passiven Transpondern, zum Beispiel Chipkarten über kurze Distanzen. Mit batteriebetriebenen aktiven Transpondern könne man auch größere Entfernungen überbrücken. Selbst entwickelte proprietäre Standards für die Kryptografie seien eigentlich immer schlechter als Standardverfahren, wie etwa AES. Man könne aber durchaus bewährte Standards durch Zusätze proprietär machen. Das sei gegebenenfalls sogar empfehlenswert. Die Herausforderung liege oft darin, mit möglichst wenig Elektronik und wenig Energieverbrauch eine sichere Authentifizierung durchzuführen. Wie die Online-Verwaltung von NFC-gesteuerten Schlössern funktioniere, sei sicher die Königsfrage. Viele Experten hätten Stellung dazu genommen, wie genau die verschiedenen Stakeholder zusammenspielen müssen, damit die Administration der Berechtigungen sicher funktioniert. Die **Trusted Service Management (TSM)-Plattform** übernehme eine zentrale Rolle in der Vernetzung der Stakeholder, sodass nicht jeder Anbieter eines Dienstes mit jedem Mobilfunkbetreiber oder Hersteller von Smartphones Verträge

abschließen muss. Die Rollenverteilungen und Abläufe in einem TSM-Ecosystem seien auf der Global Plattform definiert und erstreckten sich über viele weitere Serviceleistungen.

In seinem Praxisratgeber Sicherungstechnik befasst sich der BHE mit **Mechatronik** (GIT, Ausgabe 12-2015, S. 35). Traditionelle mechanische Schlüsselsysteme würden in zunehmendem Maße von mechatronischen Schließsystemen abgelöst. Diese seien eine Kombination aus Mechanik und Elektronik, die den Zugang beispielsweise durch die Verwendung einer Chipkarte, eines Zahlencodes oder biometrischer Merkmale ermöglichen. Zu den wesentlichen Vorteilen zählten, dass derartige Systeme nicht einfach aufgebohrt werden können und zum Beispiel auf verlorene Zugangskarten mit einer kostengünstigen Umprogrammierung reagiert werden könne, ohne das komplette Schloss auszutauschen. Mechatronische Systeme seien daher oft fester Bestandteil moderner Techniken der Zutrittssteuerung.

Sicherheitsgewerbe

Dipl.-Betriebswirt Bernd M. Schäfer, ATLAS Versicherungsmakler für Sicherheits- und Wertdienste GmbH, gibt in der Ausgabe 4-2015 der Zeitschrift DSD Tipps für Auftraggeber und Sicherheitsdienstleister zum notwendigen **Versicherungsschutz bei der Übernahme von Aufgaben in Asylbewerberunterkünften** (S. 32–34). Auftraggeber sollten in jedem Fall darauf bestehen, dass auf der Bestätigung der Betriebshaftpflichtversicherung ausdrücklich auf die §§ 34a GewO und 6 BewV Bezug genommen wird, denn nur dann handle es sich um ein Bewachungsunternehmen. Soweit Sicherheitsdienstleister mit Geldtransporten zur Barauszahlung an die Asylbewerber beauftragt werden, fielen die beförderten Gelder nicht in die Position „Abhandenkommen von bewachten Sachen" der Betriebshaftpflichtversicherung. Nötig sei eine spezielle Versicherung für ungepanzerte und unbewaffnete Geldtransporte, über die dann zusätzlich auch noch das Risiko der Unterschlagung durch eigene Mitarbeiter versichert werden könne. Der Versicherungsschutz für strafbare Handlungen der Sicherheitsdienstleister finde sich auf den wenigsten Bestätigungen wieder, da er auch in den meisten Verträgen in Deutschland nicht versichert werden könne. Kommt es zu Schäden durch Diebstahl oder Brandstiftung durch Sicherheitskräfte, hafte der Auftraggeber und könne den Schaden nicht an die Versicherung seines Subunternehmers weitergeben. Werde der Hauptauftraggeber wegen nicht gezahlter Mindestlöhne in Anspruch genommen, könne der aus solchen Forderungen resultierender Schaden bei verschiedenen Versicherern versichert werden. Gegen den damit verbundenen Vorwurf der Hinterziehung von Steuern und Sozialabgaben sei der Abschluss einer Strafrechtsschutzversicherung wichtig. Führe eine Verletzung des Gleichbehandlungsgesetzes gegenüber einem Flüchtling zu einem Haftungsanspruch gegen den Sicherheitsdienstleister, könne eine entsprechende Versicherung als Ergänzungsbaustein zu einer Betriebshaftpflichtversicherung abgeschlossen werden.

Sicherheitsmanagementsystem

Ludger Remler und Dominic Gißler, Landesbank Baden-Württemberg, bezeichnen in Security insight, Ausgabe 6-2015, S. 31/32, das Festlegen von Kennzahlen und das **Etablieren eines Controlingsystems** als eine Herausforderung für die Konzernsicherheit. Bis dato ergäben sich die Anforderungen an ein ganzheitliches Unternehmenssicherheits-Managementsystem aus einer Vielzahl von Grundlagen wie der ISO 23001 Business Continuity Management oder der ISO 27001 Informationssicherheit. Die Einführung eines

Sicherheitsmanagementsystems erfolge in Reifegraden und nehme sehr ambitioniert etwa drei Jahre in Anspruch. Die entscheidenden Merkmale des ganzheitlichen Managementsystems seien: Rahmenwerk mit Sicherheitspolitik, Risikoinventar, Sicherheitsmodulen und die wichtigsten Standards als Voraussetzung zur Befähigung; Arbeitsanweisungen mit Risikobeurteilungsmethoden, Maßnahmen sowie Üben und Testen; weitere Dokumente mit internen Prozessabläufen und zur Konkretisierung; Controlling-Prozesse mit Dokumentenorganisation, Kennzahlen, Reporting, Wirksamkeitsprüfung und Revision als Grundlage für den Etablierungsprozess und Wirksamkeitsprüfungsprozeduren als abrundendes Element im kontinuierlichen Verbesserungsprozess.

Die **Integration von Sicherheitssystemen** in ein übergeordnetes Sicherheitsmanagementsystem thematisiert Michael Klitsch, ensecco, in der Ausgabe 6-2015 der Zeitschrift WiK, S. 52–54. Der Einsatz eines zentralen SMS sei selbst in kleineren Gebäudeleitstellen aufgrund der Vielzahl von Meldungen und Informationen als sinnvoll und notwendig anzusehen. Zwangsläufig erwachse aus der Entscheidung für ein zentrales Sicherheitsmanagementsystem auch die Notwendigkeit, Schnittstellen zwischen den vorhandenen oder neuen Subsystemen – z. B. Alarm- oder Video-Empfangseinrichtungen, Alarmzentralen, Gebäudeleittechnik – und dieser zentralen Instanz herzustellen. Die Diskussion um Standardschnittstellen sei seit vielen Jahren ein Thema bei der Integration von Subsystemen. Einige Standards hätten sich etabliert, so etwa OPC (OLE for Process Control) und das Netzwerkprotokoll für die Gebäudeautomation, BACNet (Building Automation and Control). Sie böten eine stabile und gute Kommunikationsgrundlage, um zuverlässig zwischen zwei oder auch mehreren Systemen Informationen über verschiedene Kommunikationswege (z. B. auf Basis von TCP/IP) auszutauschen. Der Nachteil von Standards liege darin, dass sie die Vielfalt des möglichen Informationsaustausches meistens einschränken und gerade komplexere Zusammenhänge oft nicht sauber abbilden. In vielen Fällen sei der Einsatz einer gut implementierten direkten proprietären Schnittstelle der Umsetzung mittels Standardschnittstelle vorzuziehen. ONVIF als Spezialschnittstelle für den Videobereich habe sich in sehr kurzer Zeit fast flächendeckend durchgesetzt. ONVIF arbeite bereits seit einigen Jahren an der Integration von Zutrittskontrollsystemen, doch sei bisher nicht die Dynamik erreicht worden, die im Videobereich vorgelegt wurde. Der Autor geht insbesondere auf die Qualität von Schnittstellen ein. Meldungen der Subsysteme mit Einzelmeldeerkennung und detaillierten Auslösekriterien sollten die Basis einer Schnittstellenanpassung sein. Weitgehend selbstverständlich sei heute auch die Übertragung Schaltbefehlen an einzelne Melder oder Gruppen der Zentralen. Entscheidend gerade für den wirtschaftlich sinnvollen Einsatz übergeordneter Systeme sei aber der sinnvolle und zuverlässige Austausch von Stammdaten.

Sicherheitsmarkt

Top-Trends der Sicherheitstechnik als Ergebnis des Branchenbarometers erläutert Dr. Peter Fey, Dr. Wieselhuber & Partner, in Ausgabe 12-2015 der Zeitschrift PROTECTOR, S. 10/11. Die teilnehmenden Unternehmen kommen zu 74 Prozent aus den Branchensegmenten Videoüberwachung, Zutrittskontrolle sowie Einbruch- und Brandmeldung. 71 Prozent seien Systemanbieter oder Komponentenhersteller, 17 Prozent Errichter. Die höchsten Ausprägungen des Einflusses spezifischer sicherheitstechnischer Trends auf die Marktentwicklung der nächsten drei bis fünf Jahre erhielten die sechs Trends digitale Systeme, Systemlösungen, mobile beziehungsweise Funklösungen, Remote-Management-Systeme und -Services sowie kundenindividuelle Lösungen und die Konver-

genz von Security- und IT-Welt (zwischen 4,7 und 4,2 von maximal 5 Punkten). Dem entsprechend werde den analogen Systemen der geringste Einfluss auf die Marktentwicklung zugeschrieben. Die Automotive-Industrie zeige, dass Self-ware- und Self-protecting-Systeme ein Muss sind, wenn es um die Aufrechterhaltung des Betriebs quasi autonomer Systeme geht. Bei der Videoüberwachung würden mit den höchsten Ausprägungen (zwischen 4,0 und 4,3) die folgenden drei Trends in absteigender Reihenfolge gesehen: H.265-Datenkomprimierung, HD-Kameras und 4K-/UHD-Kameras. Der Einfluss der Analog-Kameras auf die zukünftige Marktentwicklung werde mit der Ausprägung von 2,0 folgerichtig als abgeschlagen beurteilt. Bei der Zutrittskontrolle werde die höchste Bedeutung auf die Marktentwicklung den Bluetooth- und Bluetooth-Low-Energy-Lösungen zugeschrieben (beide 4,2). Nahezu gleichauf rangieren NFC-/RFID-Lösungen beziehungsweise die klassischen Smart Cards (3,9 und 3,8). Bei den Einbruchmeldesystemen führe der Trend zur Meldung auf mobile Endgeräte mit 4,6 deutlich die Liste an. An zweiter Stelle folgten Wireless-Übertragungsstandards und Touchpads beziehungsweise moderne Mensch-Maschine-Interfaces (beide 4,1). Bei den Trends zu den Übertragungsstandards im Sektor der Videoüberwachung fielen die Ergebnisse der Befragung noch heterogen aus: Mit 3,98 werde die Liste zwar angeführt vom Onvif-Protokoll, mit etwas Abstand folgten jedoch schon RTSP-/RTP-Protokolle (3,4). (beide 3,3). An zweiter Stelle folgten Enocean-Technologien (3,0).

Die Zeitschrift WiK (Ausgabe 6-2015, S. 48) weist auf eine **BHE** (Bundesverband der Hersteller und Errichter)**-Untersuchung des Marktes** hin. Danach habe sich die Geschäftslage deutlich verbessert. In der Prognose für 2015 habe die Geschäftslage für Brandmeldetechnik den Wert von 2,09 (Schulnotenskala) erreicht. Der Gewerbebereich liege mit 1,92 deutlich vor den behördlichen Nachfragern (2,60). Die erwartete positive Entwicklung im Markt für elektronische Sicherungstechnik sei nach der Umsatzprognose des BHE, nach der deutsche Sicherheitstechnik-Anbieter mit einem Umsatzzuwachs von 3,0 Prozent rechneten, relativ gleichmäßig von allen Fachbereichen zu verzeichnen. Der deutlichste Zuwachs werde in der Videoüberwachungstechnik (+ 3,8 Prozent) und den Sprachalarmsystemen (+ 3,6 Prozent) prognostiziert, gefolgt von Zutrittssteuerungssystemen (+ 3,2 Prozent), der Brandmeldetechnik (+ 3,0 Prozent) und sonstigen Sicherungssystemen (+ 3,1 Prozent).

Spielbanksicherheit

Stefan Bauboeck, Sony Professional Europe, erläutert in der Ausgabe 12-2015 der Zeitschrift PROTECTOR, S. 40, die **Videoausrüstung des Hamburger Spielkasinos**. Neben der Bildqualität habe eine weitere technische Anforderung im Fokus gestanden: die visuelle Dokumentation des Auszahlungsprozesses an den Spielautomaten. Mehr als 300 Kameras schmückten den täglichen Kasinobetrieb. Je nach Einsatzbereich kämen Box oder „360-Grad-Kameras" zum Einsatz. Eine eigens programmierte und an den Kundenbedürfnissen ausgerichtete Applikation, basierend auf Milestone XProtect Corporate, stelle eine Echtzeit-Aufzeichnung sicher. Die teils gravierenden Unterschiede in den Lichtverhältnissen, vor allem zwischen den sehr dunklen Räumen und hellen Spieltischen, würden durch den extrem hohen Dynamikbereich (90–130 dB) von Sony geschickt ausgeglichen.

Spionage

Für das im Sonderbericht Wirtschaftsschutz deutscher Sicherheitsbehörden des Bundes am 7. Dezember dargestellte **BKA-Projekt „Wirtschaftsspionage und Konkurrenzausspähung** – eine Analyse des aktuellen

Forschungsstandes“ wurden im Rahmen einer Sekundäranalyse Beiträge aus der Fachliteratur sowie empirische Studien, die Unternehmensbefragungen umfassten, systematisch ausgewertet. Geleitet worden sei die Aufarbeitung von der zentralen Frage, wie sich die Phänomene Wirtschaftsspionage und Konkurrenzausspähung aus Sicht deutscher Unternehmen darstellen. Folgende Ergebnisse seien abgeleitet worden: Die strafrechtlich relevante Unterscheidung zwischen Wirtschaftsspionage und Konkurrenzausspähung sei für Unternehmen weniger bedeutsam. Die Mehrheit der Unternehmen schätze die Bedrohung als hoch bis sehr hoch ein und gehe von einem künftig weiteren Anstieg der Bedrohung aus. Im Durchschnitt gebe ungefähr jedes vierte Unternehmen an, bereits Opfer von Ausforschungshandlungen geworden zu sein. Nur ein kleiner Teil bringe entsprechende Vorfälle zur Anzeige. Etwa jeder dritte Fall von Ausforschung sei rein zufällig entdeckt worden. Die Sicherheitsbehörden spielten bei der Aufdeckung eine untergeordnete Rolle. Aktuelle und ehemalige Mitarbeiter bildeten die wichtigste Tätergruppe. Schätzungen zum jährlichen Schaden in Deutschland reichten von ein- bis zu dreistelligen Milliardenbeträgen. Hochrechnungen auf der Grundlage der Schadensangaben gingen dagegen „lediglich“ von einstelligen Milliardenbeträgen aus. Unternehmen kooperierten bei der Abwehr häufiger mit privaten Akteuren als mit Behörden. Viele Unternehmen sähen die Notwendigkeit von organisatorischen, personellen, technischen und IT-spezifischen Sicherheitsvorkehrungen. Sie seien sich aber häufig nicht der schwerwiegenden Auswirkungen solcher Angriffe bewusst. Schlussfolgerungen aus der Sekundäranalyse: Die behördlichen Akteure im Wirtschafts- und Informationsschutz sollten ihre Kräfte zusammenführen, wie in der „Erklärung für eine Nationale Wirtschaftsschutzstrategie“ von BDI, DIHK und BMI vorgesehen. Besonders wichtig als Kooperationspartner der Sicherheitsbehörden seien die IHKs und die Handwerkskammern. Der Ergebnisbericht kann über die Seite www.bka.de/Publikationen heruntergeladen werden.

Steuerhinterziehung

Zwölf Mrd. Euro durch Aktiengeschäfte hinterzogen, titelt die FAZ am 15. Dezember. Mehr als 100 Banken und Fondsgesellschaften im In- und Ausland stünden mittlerweile im Blickpunkt der Ermittlungsbehörden wegen sogenannter „Cum-Ex“-Geschäfte. Es bestehe der Verdacht, dass sie sich mit Aktiengeschäften rund um den Dividendenstichtag eine nur einmal gezahlte Kapitalertragssteuer mehrfach haben erstatten lassen. Nordrhein-Westfalens Finanzminister Norbert Walter-Borjans habe auf Anfrage gesagt, für die Banken sei es „höchste Zeit zu handeln“. Durch Kooperation mit den Behörden sollten sich die Banken „wenigstens im Nachhinein vom Betrug an der Allgemeinheit verabschieden“. Ermittelt werde wegen Steuerhinterziehung. Das Land habe für fünf Mio. Euro eine CD mit etlichen Tausend Datensätzen gekauft. Das Handelsvolumen, um das es dabei gehe, soll rund 72 Mrd. Euro betragen.

Terrorismus

Renate Köcher, Institut für Demoskopie Allensbach, weist in der Wirtschaftswoche am 18. Dezember, S. 40, darauf hin, dass 71 Prozent der Deutschen überzeugt sind, dass von terroristischen Gruppen zurzeit große Gefahren für das Land ausgehen. Das persönliche Bedrohungsgefühl habe sich gravierend erhöht. Noch vor wenigen Monaten habe sich knapp die Hälfte der Bürger nicht vorstellen können, selbst durch Terrorismus gefährdet zu werden. Jetzt teilen nur noch 27 Prozent diese Zuversicht.

Veranstaltungssicherheit

Das BKA weist in der Wochenlage vom 15. Dezember darauf hin, dass terroristische Selbstmordattentäter versucht haben, am 13. November während des Fußball-Länderspiels zwischen Frankreich und Deutschland ins Stadion zu gelangen und es der Wachsamkeit der eingesetzten Ordner zu verdanken ist, dass ihnen das nicht gelang. Von besonderer Relevanz für die Gefährdung von Großveranstaltungen seien Innentäter, die sich nach erfolgter Radikalisierung durch Dschihadisten gezielt eine Tätigkeit im Sicherheitsgewerbe suchen, um hierüber terroristische Taten zu begehen oder zu ermöglichen. Für potenzielle Täter bestehe die Möglichkeit, Waffen-, Spreng- und Brandmittel legendiert in einen Veranstaltungsort einzubringen und eine taktisch günstige Gelegenheit, die Durchführung terroristischer Anschläge durch eine umfassende Aufklärung vorzubereiten.

Videoüberwachung

Martin Liebezeit, Bosch Sicherheitssysteme GmbH, erläutert in Security insight, Ausgabe 6-2015, S. 36/37, das Erfordernis flexibler und effizienter Sicherheitssysteme für **neue Filialkonzepte** der Banken und Sparkassen. Der Videoüberwachung komme heute bei der Absicherung von Bankfilialen eine noch stärkere Bedeutung zu. Intelligente Algorithmen in der Kamera könnten kritische Situationen automatisch erkennen und Meldungen generieren, die dann spezifische Maßnahmen einleiten, beispielsweise in unbemannten Selbstbedienungsfilialen. Die integrierte Intelligenz könne genutzt werden, um die Kameraeinstellungen in Echtzeit an veränderte Lichtbedingungen anzupassen, was beispielsweise in Bankenfoyers mit Sonneneinstrahlung die Bildqualität erheblich verbessern könne. Zudem könnten solche Anlagen einfach in ebenfalls netzwerkbasierte Alarmierungssysteme integriert werden. Um die Übertragung nutzbarer Live-Videos auch über vergleichsweise langsame Mobilfunknetze zu ermöglichen, habe Bosch Sicherheitssysteme das „Dynamic Transcoding" entwickelt. Bei Bedarf könne ein solches Video so angezeigt werden, dass einzelne Szenen in voller HD-Auflösung auf dem Smartphone oder Tablet erscheinen. Bei mobilen Filialen schaffe „Dynamic Transcoding" überhaupt erst die Voraussetzung für die wirtschaftliche Übertragung von Live-Videodaten an eine Leitstelle. Remote-Service-Technologien ließen sich über die Netze der Dienstleister implementieren, sofern der Anbieter des Sicherheitssystems solche anbietet.

Mit der **Videoüberwachung von Freigelände** befassen sich in Ausgabe 6-2015 der Zeitschrift WiK, S. 55–57, Michael Luckey, Perimeter Protection Germany GmbH, und Thomas Hermes, Securiton GmbH. Heute stünden für die Sicherung der Perimetergrenzen moderne und kosteneffiziente Lösungen bereit. Dazu gehörten etwa mikrowellenbasierte Volumensensoren, seismische, ortungsfreie Bodendetektionssysteme bis hin zu Zaundetektionssystemen. Die Auswahl des „passenden Systems" und der optimalen Kombination sei von verschiedenen Kriterien abhängig. Neben der Risikoart, dem Schutzniveau, dem Täterprofil und der möglichen Bedrohung bildeten die Gebäude- bzw. Geländekontur oder -beschaffenheit die entscheidenden Faktoren. Die Autoren behandeln die Videoüberwachung als Teil eines umfassenden Schutzkonzeptes, die Metadateneinblendung, Anforderungen an die Perimeterüberwachung, die Darstellung des Alarmobjektes im Lageplan und die Abstimmung von Perimeterdetektion und Videoverifikation. Im Bereich der Liegenschaftssicherung sollten spezielle für den Außenbereich geeignete Videosicherheitssysteme genutzt werden. So biete etwa der IPS Video Manager entsprechende Funktionen für Außenanwendungen wie Witterungsfilter

und automatische Empfindlichkeitsberechnung, Störgrößen-Eliminierung, Objekterkennung- und -verfolgung sowie Freund-/Feind-Erkennung. Denn für die Klassifizierung eines Alarms müssten aussagekräftige Videobilder zur Verfügung stehen.

Die **Brandfrüherkennung durch intelligente Videoanalyse** behandelt in Ausgabe 6-2015 der Zeitschrift WiK, S. 58/59, Sören Wittmann, Bosch Sicherheitssysteme GmbH. Die einzige Technologie, die einen entstehenden Brand auch über größere Distanzen hinweg frühzeitig erkennen kann, sei Video. Mit Video werde ein beginnendes Feuer in der Regel innerhalb von Sekunden erkannt. Die Flammencharakteristika unterschiedlicher Feuer seien bestens bekannt, und so könnten diese über entsprechende Algorithmen ebenfalls in Echtzeit erkannt werden. Solche Lösungen eigneten sich auch sehr gut für eine Vielzahl „rauer" Umgebungen, etwa Gebäude mit staubigen und feuchten Bereichen, wie sie in Produktionsbetrieben oder bei der Müllaufbereitung gängig sind, aber auch Tunnels und Parkhäuser, Sägewerke und Generatorhallen von Kraftwerken. Die videobasierte Branderkennung sei unempfindlich gegenüber Fehlalarmen, da die intelligente Videoanalyse in der Kamera es ermögliche, Störgrößen wie Bewegung, Reflexionen oder wechselnde Lichtverhältnisse zu erkennen und ihre Einflüsse auszugleichen. Kameras deckten weitere Bereiche ab als lineare -, Punkt- oder Ansaugmelder und benötigten weniger Wartung. Für die Brandfrüherkennung eingesetzte Kameras könnten auch die Security erhöhen. Gerade in Lagerhäusern sei dies eine attraktive Option, um Schwund zu reduzieren. Derzeit noch nicht möglich sei ein Ersatz von EN 54-zertifizierten Systemen, da es hierfür in Europa noch keine Zertifizierung gebe.

Zahlungskartenkriminalität

„Sicherheitslücken bei der Kartenzahlung im Supermarkt" titelt die FAZ am 29. Dezember. Es gäbe in Deutschland etwa 770.000 Kartenterminals im Handel, von denen etwa 60 Prozent auf den Marktführer Telecash entfielen. Shell und Rewe hätten eigene Systeme. Innerhalb der Systeme besäßen leichtsinnigerweise viele Terminals dieselben Schlüssel. Innerhalb der Netze gebe es jeweils auch alte, schlecht geschützte Terminals, die als Erstes in den Blick der Hacker gerieten. Wenn es Betrügern gelinge, ein relativ altes, schlecht geschütztes Terminal aus einem System zu bekommen, könnten sie dann auch auf alle anderen Geräte zugreifen. Der Kryptograph Nohl forderte deshalb eindringlich, alte Geräte endlich auszumustern und den einheitlichen Schlüssel abzuschaffen. Beim „Girocard"-System der Deutschen Kreditwirtschaft, bei dem der Chip auf der Karte und die Pin-Nummer zusammen eingesetzt würden, seien die Hackerangriffe nicht möglich. Die Angriffe erfolgten auf die Magnetstreifentechnik und seien nicht auf Chipkarten übertragbar. Geldautomaten in Deutschland arbeiteten zwar mittlerweile überall mit Chip und PIN-Nummer. Entsprechend ist nach Angaben des BKA die Zahl der Betrugsfälle an Geldautomaten seit 2011 erheblich zurückgegangen. Große Teile der Zahlungsinfrastruktur beruhten auf Protokollen aus den neunziger Jahren, die große Sicherheitsmängel aufwiesen. Das in Deutschland für die Kommunikation zwischen Zahlungsterminal und Kasse verwendete Protokoll ZVT („Zahlen-Verbindungs-Test") erlaube es, Kartendaten aus dem lokalen Netzwerk auszulesen. Zudem erlaube es ZVT auch, PINs aus der Ferne auszulesen. Diese seien zwar durch eine Signatur geschützt, diese werde jedoch bisweilen in Hardware-Modulen gespeichert, von denen einige anfällig für einfache Timing-Attacken seien.

Zutrittskontrolle

Das Thema **verschlüsselnde Kartentechnologien** werde für die Einbruchmelde- und Zutrittskontrollbranche immer aktueller, schreibt Carsten Hoersch, Sesam Elektronische Sicherheitssysteme GmbH, in der Ausgabe 12-2015 der Zeitschrift PROTECTOR, S. 23. Die Verschlüsselung könne entweder am Leser oder aber über die angeschlossene Auswerteeinheit aktiviert werden. Dies hänge in der Regel von der Komplexität der Schnittstelle zwischen Leser und Auswerteeinheit ab. Der VdS fordere derzeit die Verschlüsselung zwischen Karte und Leseeinheit und eine Kabelführung im gesicherten Bereich.

Frauke Petzold, Slat GmbH, behandelt in der Ausgabe 12-2015 der Zeitschrift PROTECTOR, S. 31, die **Notstromversorgung für Zutrittskontrollanlagen**. Ab 11. Juni 2016 werde die bisher geltende EN 50133-1 von der EN 60839-11-1 (Elektronische Zutrittskontrollanlagen – Anforderungen an Anlagen und Geräte) abgelöst. In dieser Norm seien vier Risikostufen vorgesehen, die von dem zu schützenden Sachwert sowie dem Wissens- und Fertigkeitsgrad eines potenziellen Angreifers ausgingen. Die Stufen drei und vier deckten das mittlere und hohe Risiko ab und forderten den Einsatz einer Notstromversorgung, um auch im Störfall eine hohe Öffnungsverfügbarkeit zu gewährleisten. Diese reiche von zwei bis vier Stunden Überbrückungszeit unter Volllastbedingungen. Laut Sascha Puppel, öffentlich bestellter und vereidigter Sachverständiger für elektronische Sicherheitstechnik, würden DC-Notstromversorgungen immer wichtiger, um die verteilte Intelligenz, aber auch das Herzstück einer Zutrittskontrollanlage, die Zentrale selbst, zu sichern.

GIT stellt in der Ausgabe 12-2015, S. 50–52, die **Plattform der neuen Zutrittskontroll-Lösung iSAC-3** vor, die alle Funktionalitäten eines qualitativ hochwertigen Zutrittskontroll-Systems auf moderner Oberfläche mit intuitivem Bedienkomfort biete. Die Möglichkeiten reichten von der kostengünstigen vorkonfigurierten Standard-1-Türlösung bis hin zum komplexen Zutrittskontroll-System für bis zu 200.000 Online-Türen und/oder Türen mit mechatronischen Komponenten. In der sogenannten Zutrittsmatrix seien alle Elemente wie Personen, Gruppen, Zutrittspunkte, Zeitmodelle und Bereiche enthalten. Sie können von hier aus schnell und einfach verändert werden. Das Konzept von iSAC-3 eigne sich gleichermaßen für kleine, mittelständische und große Unternehmen aller Branchen.
Die Software der Lösung arbeite rein Web-Browser-orientiert als Java-Applikation und sei dadurch betriebssystemunabhängig. Sie unterstütze neben den gängigen PC-Betriebssystemen auch Tablets und Smartphones. Die Kommunikation zwischen der Benutzeroberfläche und dem Server sei durch das hybride Verschlüsselungsprotokoll SSL abgesichert. Zusätzlich enthalte das System einen Zugriffsschutz über eine rollenbasierte Passwort-Verwaltung mit einer revisionssicheren Historie inklusive Rückwicklung. Die Software liefe automatische Hilfestellungen zur Reduktion oder gar Vermeidung von Fehlern. Mit dieser Funktion seien Fehlbedienungen weitestgehend ausgeschlossen. Durch die Komponenten der Wireless-Technologie könne die Menge an Kabeln erheblich reduziert werden. Die gesamte Systemlösung werde neben der Software durch den **intelligenten Door Controller (iDC)** abgerundet. Der iDC unterstütze alle Zutrittsfunktionen von bis zu 16 Türen. Er stelle die Verbindung zu Applikationen selbstständig her und steuere ebenso selbstständig alle Zutrittsfunktionen. Schreib- und Leseeinheiten zeichneten sich durch in verschiedene Schalterprogramme integrierbare Designs aus.

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