Focus on Security

Ausgabe 11, November 2015

SECURITAS

Inhalt

Abhörschutz

Dr. Hans-Christoph, Secusmart, gibt in der Ausgabe 10-2015 der Zeitschrift GIT Tipps für eine sichere Kommunikation (S. 78/79). Mit der App Vodafone Secure Call biete Secusmart auch der Wirtschaft eine Lösung für die mobile sichere Kommunikation auf den gängigen Betriebssystemen an. Auf drei Punkte sollten verantwortliche Sicherheitsmanager achten: auf die Technik (Wie sicher sind die Lösungen? Wie unterscheiden sie sich?), auf die Zielgruppe (Welche Sicherheitslösung ist optimal für KMU und welche Lösung für ein DAX-Unternehmen?) und auf den Nutzer (Welche Lösung ist benutzerfreundlich? Ist der Nutzer bereit, eventuell Einschränkungen in seinem Alltag in Kauf zu nehmen?). Der Autor geht auf die drei Themenbereiche näher ein.

Arbeitsschutz

Natur als Vorbild für **textile Hightech-Sicherheit** thematisiert Dipl.-Soziologe Norbert Hüls in der Ausgabe 5-2015 der Fachzeitschrift WiK, S. 70/71. Hoch technisierte Textilien im Protech-Bereich, entwickelt von deutschen Textilforschungsinstituten, definierten auch das Arbeitsumfeld von Security Personal neu und könnten deren Sicherheit beträchtlich erhöhen. Behandelt werden in dem Beitrag insbesondere ein Perlmutt-Imitat für den Flammschutz, Schnitt-, Stich- und Prallschutz, Textilien für explosionsdruckstoßfeste Behälter und in die Schutzbekleidung integrierte intelligente Funktionen. So messe die Schutzausrüstung beispielsweise die Herzfrequenz und verfüge über einen Sensor für ein Schadensmonitoring. Textile Antennen ermöglichten eine genaue Lokalisierung der Retter. Ein ebenso leichter wie flexibler Akku beliefere leuchtende OLED-/LED-Elemente auf der Schutzbekleidung autark mit Strom.

Die Fachzeitschrift GIT befasst sich in Ausgabe 10-2015, S. 118/119, mit der Verwendung und Überwachung von **Notduschen** in Gefahrenbereichen. Augenwaschstationen seien ebenso unerlässlich wie Notduschen, für den Fall, dass eine Ganzkörperreinigung erforderlich ist. Leider gebe es keine umfassende Norm für die EU, durch die alle Arten von Notduschen für jegliche Form der Installation abgedeckt sind. Die Norm EN 15154 umfasse vier abgeschlossene Teile, die Notduschen mit Wasseranschluss für Laboratorien sowie Industrie-/Logistikstandorte und Notduschen mit Wassertank ohne Wasseranschluss für alle Standorte abdecken. Es gebe jedoch keine endgültige Norm für Notduschen mit Wasserversorgung für Industriestandorte. Die deutsche Norm 12899-3:2009 umfasse Notduschen mit und ohne Wasseranschluss für Industrie- und Logistikstandorte und schließe somit die enorme Lücke im aktuellen europäischen Normensystem. Eine Technologie für eine verkürzte Erstreaktionszeit gebe es bereits. Ein drahtloser Limitless-Schalter lasse sich leicht an vorhandenen Notduscheinheiten installieren und in lokale oder zentrale Alarm- und Gebäudemanagementsysteme sowie Videoüberwachungsanlagen einbinden. Dies verkürze nicht nur die kritischen Erstreaktionszeiten im Ernstfall, sondern liefere auch einen Audit-Trail mit genauen Angaben, wann die jeweilige Notdusche verwendet wurde.

Brandschutz

Peter Holzamer, Prymos GmbH, plädiert in der Ausgabe 5-2015 von Security insight, S. 24/25, für ein Duo aus wartungsfreien Kevlar-Feuerlöschern und zertifizierten **Löschspraydosen**. Die Feuerlöscher aus Composite-Kevlar seien leichter und kostengünstiger als herkömmliche Geräte, und sprayen könne jeder. Dazu äußert sich Dipl.-Ing. Peter Gundermann, Fachingenieur für Brandschutz, in der Ausgabe 10-2015 der

Zeitschrift GIT (S. 82–85) skeptisch. Die ASR A 2.2 biete als technische Regel eine Basislösung für wirksame und erprobte Brandschutzmaßnahmen an. Das damit definierte Sicherheitsniveau dürfe nicht unterschritten werden. Die Grundausstattung von Arbeitsstätten mit Löschspraydosen sei unter Berücksichtigung der gravierenden Unterschiede zu Feuerlöschern ein offensichtlich unüberwindbares Hindernis für den Arbeitgeber beim Nachweis der Gleichwertigkeit der Lösung. Die ArbStättV fordere für alle Sicherheitseinrichtungen und insbesondere für alle Feuerlöscheinrichtungen eine regelmäßige sachgerechte Wartung und Funktionskontrolle. Das betreffe nicht nur Feuerlöscher, sondern z. B. auch Löschanlagen, BMA, Wandhydranten und RWA-Anlagen. Mit einer Sichtkontrolle durch Beschäftigte könne diese Forderung nicht erfüllt werden.

Die Zeitschrift GIT befasst sich in Ausgabe 10-2015, S. 84/85, mit der zuverlässigen **Vernetzung von Brandmeldezentralen**. Für die Datenübertragung in BMA würden unterschiedliche Schnittstellen wie RS232, RS485 oder Ethernet eingesetzt. Da es um den Schutz von Leib und Leben geht, sei höchste Zuverlässigkeit erforderlich. Deshalb würden Brandmeldezentralen vorwiegend über Lichtwellenleiter (LWL) vernetzt. Außerdem könnten über dieses Medium auch andere Sicherheitssysteme wie Sprachalarmierung oder Zutrittskontrolle angebunden werden. Das Medium LWL sei vor allem in punkto Übertragungsentfernung und Störfestigkeit Kupferkabeln deutlich überlegen. Außerdem biete es wirtschaftliche Lösungen, da beim Einsatz anderer Schnittstellen keine neuen Leitungen installiert werden müssten.

In der Ausgabe 10-2015 der Zeitschrift GIT nimmt der bvfa Stellung zum **mobilen Brandschutz im Betrieb** (S. 86–89). Es sei von existentieller Bedeutung, die vielfältigen Gefahren frühzeitig zu erkennen, richtig einzuschätzen und die notwendigen Maßnahmen zu ergreifen, also eine Gefährdungsanalyse und ein Brandschutzkonzept zu erstellen. Ein Grundschutz mit Feuerlöschgeräten sei unabdingbar. Vom Einsatzort hänge ab, welche Löschgeräte und welches Löschmittel zur Schadenminimierung geeignet sind. Die Beachtung der anlagentechnischen und baulichen Brandschutzvorgaben sei ebenso wichtig wie die notwendige Unterweisung der Mitarbeiter und die Bestellung von Brandschutzbeauftragten. Behandelt werden in dem Beitrag die sorgfältige Gefährdungsbeurteilung, Schutzziele des Brandschutzes, die notwendigen Brandschutzkomponenten, Prüfung und Instandhaltung der Brandbekämpfungsgeräte. Die 2015 aktualisierte Betriebssicherheitsverordnung regele die Sicherheit und den Gesundheitsschutz bei der Bereitstellung von Arbeitsmitteln. Sie regele auch die Sicherheit beim Betrieb von überwachungsbedürftigen Anlagen und die Organisation des betrieblichen Brandschutzes.

Simon Ouellette, Victaulic, bezeichnet in der Zeitschrift GIT (Ausgabe 10-2015, S. 90/91) untaugliche Deckenebenen als Risiko für die ordnungsgemäße Funktion von **Sprinklern bei abgehängten Decken**. Durch ihre inhärente Flexibilität, die eigentlich den Hauptvorteil dieser Decken darstellt, neigten abgehängte Decken dazu, sich nach Installation mit der Zeit leicht zu senken, während Sprinkler fest verankert bleiben und sich so die Decke allmählich vom Sprinkler löse. Das führe zu einer Sprinkler-Fehlausrichtung. Ein bahnbrechendes Konzept zur Lösung des Problems sei die Entwicklung und Anwendung flexibler Sprinkler anstelle herkömmlicher fester Rohre. Durch flexible Schläuche könne der Sprinkler mit der Struktur gehen und seine Position relativ zur Decke beibehalten. Schläuche seien durch geringere Biegeradien und mehr mögliche Biegungen noch leistungsfähiger, dadurch lasse sich eine ordnungsgemäße Positionierung in Zwischendecken einfacher und schneller durchführen.

Cloud Computing

Das produzierende Gewerbe sei gegenüber dem Megatrend Cloud nach wie vor skeptisch, berichtet silicon.de am 28. September. Wie der IT Innovation Readiness Index für 2015 zeige, bauten sich die Hemmnisse aber offenbar ab. Der Anteil der Unternehmen, die sich der Cloud vollständig verweigern, habe gegenüber 2014 von 40 auf 36 Prozent abgenommen. Der Anteil der Unternehmen, die ausschließlich den Private-Cloud-Ansatz in Betracht ziehen, wachse allerdings. Vor allem kleinere Firmen seien skeptischer gegenüber Cloud Computing. Die Automotive-Branche scheine für den Einsatz von Software as a Service als strategischer Softwareplattform besonders aufgeschlossen zu sein.

Datenschutz

Silicon.de weist am 6. Oktober darauf hin, dass der EuGH das **Datenschutzabkommen zwischen den USA und der EU** „gekippt" hat. Das Safe-Harbor-Abkommen habe zwischen der EU und den USA die Übermittlung personenbezogener Daten von EU-Bürgern geregelt. Deutsche Unternehmen und Industrieverbände hätten mit Erleichterung auf das Urteil reagiert, mit dem die Einschätzung der EU-Kommission revidiert werde, dass die USA ein angemessenes Schutzniveau übermittelter personenbezogener Daten gewährleisten. US-Unternehmen müssten sich den geltenden US-Gesetzen unterwerfen, die sie verpflichteten, die Safe-Harbor-Regelungen nicht anzuwenden, wenn sie US-Gesetzen widersprechen. Die EU habe aber weder einen gerichtlichen Rechtsschutz gegen behördliche Eingriffe festgestellt, noch Regeln, die solche Eingriffe begrenzen. Von daher erlaube die Safe-Harbor-Regelung Eingriffe amerikanischer Behörden in die Grundrechte von EU-Bürgern.

Als erste Aufsichtsbehörde habe das Unabhängige Landeszentrum für Datenschutz von Schleswig-Holstein (ULD) auf das Safe-Harbor-Urteil reagiert, meldet die FAZ am 21. Oktober. Nach einem Positionspapier des ULD sind Datentransfers in die USA demnach auch dann unzulässig, wenn sich die Sicherheit der Daten auf Standardklauseln in Verträgen zwischen den beteiligten Unternehmen stützt. Diese waren von der EU-Kommission ebenfalls als „ausreichende Garantien" eingestuft worden. Bürger könnten nach Meinung des ULD auch nicht wirksam in die Übermittlung einwilligen.

Fachanwältin Dr. Sibylle Gierschmann beschreibt in der Fachzeitschrift comply (Oktober 2015, S. 42–45), wie sich Unternehmen auf die **Compliance-Anforderungen** der im Frühjahr 2016 in Kraft tretenden EU-Datenschutzgrundverordnung schon jetzt vorbereiten können. Neben der Implementierung von Datenschutz-Richtlinien im Unternehmen seien dies insbesondere die in Art. 22 Absatz 2 genannten Maßnahmen: Dokumentation sämtlicher Verarbeitungsvorgänge im Unternehmen gemäß Artikel 28, Umsetzung technischer und organisatorischer Maßnahmen gemäß Artikel 30, Durchführung von sogenannten Datenschutz-Folgeabschätzungen gemäß Artikel 33, Zurateziehung der Aufsichtsbehörde gemäß Artikel 34 insbesondere in Bezug zu Verarbeitungen, die aufgrund ihres Wesens, Umfangs oder Zwecks hohe Risiken für die Betroffenen bergen können und Benennung eines Datenschutzbeauftragten gemäß Artikel 35 Abs. 1.

Datensicherheit

Die Fachzeitschrift WiK weist in ihrer Ausgabe 5-2015, S. 6, auf die aktuelle Studie „IT-Sicherheit und Datenschutz 2015" der Nationalen Initiative für Informations- und Internet-Sicherheit e. V. (NIFIS) hin, nach der sich der sogenannte „Azubi-Effekt" für die

deutsche Wirtschaft zu einem gravierenden Sicherheitsproblem entwickelt habe. Auszubildende erhielten in verschiedenen Abteilungen Zugriff auf sensible Firmendaten, doch oftmals würden Berechtigungen nicht mehr entzogen, selbst wenn die Azubis die Firma bereits wieder verlassen haben. Dies könne zu Datenmissbrauch führen. Die Studie beziffere jährliche Schäden in Millionenhöhe.

Drohnen

Nach einem Bericht in der Zeitschrift WiK (Ausgabe 5-2015, S. 19) verlangt die Deutsche Flugsicherung (DFS) eine **Kennzeichnungspflicht** für Drohnen. Gedacht sei an eine Implementierung der Transponder-Technologie. Dabei beziehe sich der Vorschlag allerdings nicht auf „Hobby-Drohnen".

Die Fachzeitschrift WiK (Ausgabe 5-2015, S. 60) weist darauf hin, dass ab 2016 ein unter anderem mit Jamming arbeitendes **Drohnenabwehrsystem** von Airbus Defence and Space ein unbefugtes Eindringen von Kleindrohnen in kritische Lufträume verhindern könne. Das System verspreche die Erfassung von Drohnen auf große Entfernung und ermögliche dann elektronische Gegenmaßnahmen zur Minimierung von Kollateralschäden. Identifiziert würden die Drohnen anhand der Daten von Radarsystemen, Infrarotkameras und Funkpeilgeräten in Entfernungen von bis zu 10 Kilometern. Anschließend werde deren Gefahrenpotenzial auf Basis einer umfassenden Bibliothek an Bedrohungen ermittelt und die Steuersignale einer Echtzeit-Analyse unterzogen, sodass die Verbindung zwischen der Drohne und dem Piloten unterbrochen bzw. ihre Navigation gestört werden könne. Zudem solle mit dem Peilgerät die Position des Piloten ermittelt werden können. Auch die Klassifizierung der Fernsteuerung und das GPS-Spoofing seien möglich. Dadurch könne nicht nur gestört, sondern sogar die Drohnensteuerung übernommen werden.

Endgerätesicherheit

Der Kryptodienst Silent Circle präsentiere mit dem Blackphone 2 den Nachfolger des als sicher angepriesenen Smartphones Blackphone, berichtet heise.de am 29. September. Das Smartphone unterstütze Googles Android for Work, mit dem Unternehmen die Android-Geräte ihrer Mitarbeiter organisieren und sichern können. Wie schon der Vorgänger werde auch das Blackphone 2 mit dem Chat- und Telefondienst von Silent Circle ausgeliefert. Damit könnten Telefonate, Textnachrichten, Videokonferenzen und Datentransfer verschlüsselt werden.

Energieanlagenschutz

Mit der Absicherung von Energieanlagen befasst sich Jochen Krings, Fachautor, in der Ausgabe 10-2015 der Zeitschrift PROTECTOR, S. 28/29. In Brandenburg habe es allein 2012 mehr als 60 Angriffe auf Solarparks gegeben. Bei bandenmäßig organisierten Diebstählen seien in Einzelfällen bis zu 450 Module entwendet worden. Die Versicherer schrieben als Geländesicherung mittlerweile stabile Gittermattenzäune mit Übersteig vor. Um diese Anforderungen bei Perimeterstrecken von mehreren Kilometern wirtschaftlich erfüllen zu können, würden bei Solarparks häufig Zaunanlagen mit drei Meter breiten Gittermatten eingesetzt. In den meisten Fällen sei die Zaunanlage in 2,00 oder 2,20 Metern Höhe ausgeführt, mit verlängerten Pfosten und zwei Reihen Stacheldraht als Übersteigschutz. Neben einem äußeren Ordnungszaun solle der sicherheitskritische Teil des Geländes durch eine Hochsicherheitszaunanlage mit hohem Widerstandswert gesichert werden.

Ermittlungen im Unternehmen

In der Ausgabe 5-2015 von Security insight gibt Peter Niggl auf der Basis eines Gesprächs mit Rechtsanwalt Dr. Minoggio Empfehlungen zum Verhalten bei richterlich angeordneten **Durchsuchungen im Unternehmen** (S. 10–15). Jedes Unternehmen müsse für solche Fälle einen Alarmplan haben. Der Pförtner müsse Bescheid wissen, wen er kontaktieren soll, wenn die Staatsanwaltschaft „anklopft". Es bestehe keine Pflicht, die Ermittler bei ihrer Arbeit zu unterstützen, sie dürften jedoch auch nicht behindert werden. Geschäftsführer oder anderweitig Verantwortliche hätten ein Anwesenheitsrecht und sollten unbedingt darauf achten, Beschlagnahmungen auf Wesentliches zu beschränken. Daten zur Person müssten angegeben werden. Antworten zur persönlichen Situation und zum Sachverhalt sollten tunlichst verweigert werden. Möglichst rasch sei anwaltlicher Beistand zu holen. Nach dessen Ankunft habe der Geschäftsführer das Recht, mit ihm ein vertrauliches und nicht überwachtes Gespräch zu führen. Die Ermittler seien darauf hinzuweisen, dass jedem Mitarbeiter empfohlen werde, sich erst nach Rücksprache mit einem Anwalt zu äußern. Auf der Versiegelung beschlagnahmter Dokumente könne bestanden werden. Es sei sinnvoll, nach der Durchsuchung ein Gedächtnisprotokoll von allen Mitarbeitern über den Ablauf, eventuelle Fragen der Ermittler und eventuelle Äußerungen befragter Mitarbeiter anfertigen zu lassen.

Extremismus

Im Sonderbericht Wirtschaftsschutz vom 25. September weist das Bundesamt für Verfassungsschutz darauf hin, dass die „Interventionistische Linke" im August 2015 erstmals für die Aktionstage gegen den **Braunkohletagebau Garzweiler** mobilisiert habe. Der Braunkohletagebau Garzweiler und die Betreibergesellschaft RWE stünden bereits seit 2012 im Fokus militanter, jedoch nicht extremistischer Umweltaktivisten. Ursächlich für die Beteiligung von Linksextremisten an den Protesten dürfte die aktuelle gesellschaftliche Diskussion zum Klimawandel und der Energiewende sein. Während es den Umweltaktivisten in erster Linie darum gehe, die Folgen des Klimawandels in ein breiteres gesellschaftliches Bewusstsein zu rücken bzw. selbst durch militante Aktionen dagegen vorzugehen, versuchten Linksextremisten das Thema mit ihrer grundsätzlichen Ablehnung von parlamentarischer Demokratie und kapitalistischem Wirtschaftssystem zu verbinden. Auch zukünftig dürfe es mithoher Wahrscheinlichkeit wieder zu Aktionen kommen, welche den Betreiber RWE dazu zwingen werden, den Betrieb zeitweilig einzustellen. Es könne auch zu Angriffen gewaltbereiter Linksextremisten auf Fahrzeuge und Einrichtungen von RWE und anderen Energieversorgungsunternehmen kommen – auch mit hohem Sachschaden. Dafür spreche zumindest ein in der Szene kursierendes „Handbuch Ecodefense", in dem detaillierte Anleitungen zur Sabotage von Bau- und Arbeitsmaschinen abgedruckt seien. Es sei auch mit Sachbeschädigungen an Wohnhäusern von führenden Mitarbeitern entsprechender Unternehmen zu rechnen.

Flughafensicherheit

PROTECTOR beschreibt in der Ausgabe 10-2015, S. 20–22, die **integrierte Gefahrenabwehr** am Flughafen Düsseldorf. Im Terminal selbst sei eine moderne BMA mit Infrarotstrahlung installiert. In kurzen Abständen seien an der Decke unauffällige weiße Reflektoren angebracht, die von der gegenüberliegenden Seite einen Infrarotstrahl zurückspiegeln. Werde dieser unterbrochen, löse das System sofort Alarm aus und aktiviere an dieser Stelle einzelne der insgesamt

44 über das Terminal verteilte Rauchabzugsventilatoren. Im Alarmfall würden im Gebäude umgehend Notausgänge freigeschaltet oder geöffnet bzw. Feuer- und Rauchschutztüren bzw. -tore geschlossen. Sämtliche Treppenhäuer und Aufzugsschächte seien durch eine Überdruckbelüftung wirkungsvoll vor einer Verrauchung geschützt. Für den Gebäudeausbau und für fest installierte Einrichtungsgegenstände in den öffentlichen Terminalbereichen seien nur noch ausschließlich nichtbrennbare Materialien zugelassen. Die elektroakustische Anlage steuere und überwache rund 9.300 Lautsprecher in allen Terminbereichen. Basis für die gesamte Notfallorganisation sei der Gefahrenabwehrplan. Auch Themen wie der Umgang mit infektiösen Krankheiten, Gewaltakte, Flugunfälle und der Umgang mit gefährlichen Stoffen würden darin ausführlich beschrieben. Zäune und Türen auf dem Gelände seien elektronisch mit unterschiedlichen Systemen gesichert.

Perimeterschutz und Sicherheit am Flughafen Frankfurt/Main thematisiert die Zeitschrift PROTECTOR in der Ausgabe 10-2015, S. 24/25. Neben 42 Kilometern Außenzaun sicherten elf Kilometer Detektionszaun das Gelände. Für das Aluminiumzaunsystem Wavegard seien 150 Tonnen hitze- und korrosionsbeständiges Aluminium in modularer Bauweise für den Perimeterschutz verwendet worden. Dessen ruhestromüberwachte Drähte würden Übersteig-, Angriffs- und Unterkriechversuche oder das Anlegen von Leitern erkennen – und das bei geringen Fehlalarmraten. 2.500 Videokameras seien installiert. Dass im Einsatzfall die vorgeschriebene Eingriffszeit von maximal drei Minuten eingehalten wird, dafür sorgten 336 Feuerwehrleute. 650 Sprinkleranlagen, 205 Gaslöschanlagen, 23 Schaumlöschanlagen und 14 stationäre Pulverlöschanlagen stünden zur Verfügung. Rund 55.000 automatische Feuermelder und 200 Brandmeldezentralen seien installiert.

Mit **Videobildanalyse zur Freilandsicherung** am Flughafen befasst sich PROTECTOR in der Ausgabe 10-2015, S. 26/27. Videoüberwachungssysteme leisteten auf den Flughafen-Außenarealen vor allem zwei Aufgaben: Bewegungserkennung und People Tracking. Der Operator könne das Geschehen mit einem Klick aus verschiedenen Perspektiven in Nahaufnahmen und der Totalen betrachten. Der Videomanager verbinde 3-D-Geokoordinaten mit Videobildern und könne in Kombination mit intelligenter Videobildanalyse eine Position exakt bestimmen und Bewegungsprofile im Lageplan visualisieren. Die Aktivität einer Analyse sei individuell einstellbar. Zeitpläne könnten hinterlegt werden, bei denen Zutritte in die Caféteria tagsüber beispielsweise gestattet sind, nachts aber jegliche Bewegung zum Alarm werde. Für sensible Bereiche werde beim Betreten der überwachten Zone in Echtzeit ein Alarm ausgelöst und das Sicherheitspersonal informiert.

Freigeländesicherung

PROTECTOR gibt in der Ausgabe 10-2015, S. 30/31, eine **Marktübersicht** über 124 Systeme der Freilandsicherung von 53 Anbietern. Abgefragt wurden 24 Kriterien aus den Bereichen Produkteinordnung, Kategorie, Zweck/Funktion, Sensorprinzip, Kosten, Schutzart, technische Daten.

Gefährdungslage Südostasien

Im Sonderbericht Wirtschaftsschutz vom 25. September erläutert der BND die aktuelle terroristische Bedrohungslage in Süd-, Ost- und Südostasien. **Indonesien** sei das regionale Zentrum islamistischer Bewegungen. Die infolge der großen Terrorakte der 2000er Jahre durch zahlreiche Verhaftungswellen fragmentierte Dschihad-Szene stehe unter anhaltend hohem Verfolgungsdruck. Der Aufstieg des IS seit 2013 habe zu einer

deutlichen Wiederbelebung der lokalen dschihadistischen Szene geführt. Sorge bereite den indonesischen Behörden die potenzielle Verstärkung lokaler Gruppen durch zurückkehrende erfahrene Kämpfer. Bisher hielten sich die Rückkehrerzahlen allerdings in Grenzen. Eine wesentlich konkretere und unmittelbare Gefahr gehe dagegen von den anstehenden Haftentlassungen ehemaliger Terroristen aus, die für die Involvierung in die Bali- und Marriott-Attentate verurteilt wurden. Vor diesem Hintergrund bleibe ein abstraktes Anschlagsrisiko gegen „westliche" Ziele, wie z. B. touristische Infrastruktur, bestehen.
Auf den **Philippinen** sei vor allem im Süden des Landes die Sicherheitslage durch eine Gemengelage islamistischer, separatistischer und krimineller Aktivitäten angespannt. Möglicherweise könnten auch die Gegner der fortschreitenden Friedensverhandlungen zwischen der philippinischen Regierung und der Moro Islamic Liberation Front versuchen, mit gewaltsamen Störaktionen den friedlichen Lösungsprozess zu verhindern. Als Terrororganisation sei lediglich die Abu Sayyaf-Gruppe (ASG) mit aktuell ca. 400 Mitgliedern international gelistet. In den letzten Jahren werde sie vor allem mit Entführungen sowie Schutzgelderpressungen zur Erlangung finanzieller Mittel in Verbindung gebracht. Die ehemals dschihadistisch-separatistische Agenda spiele kaum noch eine Rolle. Ihr Aktionsradius erstrecke sich über das Sulu-Archipel und Mindanao hinaus bis auf international frequentierte Touristenorte wie die Insel Palawan oder die malaysische Halbinsel Sabah. Auch Ausländer seien wegen der erzielbaren Lösegelder erheblich gefährdet. Die ASG habe sich zu einer personenzentrierten Allianz von zwei weitgehend agierenden Hauptgruppen mit den „formellen Führern" Insilon Hapilon und Radullan Sahiron auf den Inseln Basilan und Jolo entwickelt. In **Thailand** seien die Anschlagszahlen in den Südprovinzen von August 2014 bis März 2015 gesunken. Im zweiten Quartal 2015 hätten die Anschlags- und Opferzahlen aber fast wieder den Vorjahresstand erreicht. Auch in Zukunft sei mit vermehrten und eventuell auch größeren Anschlägen – auch außerhalb der Südprovinzen – zu rechnen. In **Malaysia** würden die lokalen Strukturen und Ableger der indonesischen Terrororganisation Jemaah Islamiyah sowie die der einzigen militant-islamischen Organisation malaysischen Ursprungs weitgehend zerschlagen. Die größte Bedrohung werde in Rückkehrern aus Syrien und dem Irak gesehen.

Gefahrenmanagementsystem

Die Fachzeitschrift GIT plädiert in der Ausgabe 10-2015, S. 25, für ein integriertes Einsatzleit- und Gefahrenmanagementsystem. Um das komplette Spektrum der Leitstellenaufgaben durchgängig, komfortabel, schnell und sicher bedienbar zu machen, sei eine tiefe Integration von Einsatzleit- und Gefahrenmanagementsystem unabdingbar. So werde eine kombinierte, unabhängige Softwareplattform für alle Leitstellenaufgaben geschaffen, über welche sowohl alltägliche Steuerungsprozesse wie das Notfallmanagement optimal durchgeführt werden können. Im Meldungsfall schalte das Gefahrenmanagementsystem ereignisabhängig Videobilder auf und zeige dem Bediener dynamische Maßnahmenvorschläge. Sollte es sich bei dem gemeldeten Ereignis um einen Notfall handeln, so würden alle Informationen direkt an das Einsatzleitsystem eskaliert.

Geldautomatensicherheit

Die Fachzeitschrift WiK weist in der Ausgabe 5-2015, S. 8, auf einen neuen **Trojaner** für Geldautomaten hin. Suceful nenne sich die neue Generation von Malware. Der Trojaner scheine noch in einer Entwicklungsphase zu sein. Er solle die Geldkarte einziehen können, Alarme ausschalten und alle Kartendaten auslesen.

Wie WiK in der Ausgabe 5-2015, S. 10, berichtet, lasse sich nach Angaben der Sicherheitsspezialisten von Sec-Tec mit normalen Smartphones und passenden Wärmebildkameras der PIN-Code an einem Bankautomaten-Eingabefeld stehlen. Die Kamera erkenne die Fingerspuren auf der Tastatur. Gegen diese Art des PIN-Diebstahls helfe, wenn man nach der PIN-Eingabe die Handfläche für kurze Zeit auf das gesamte Eingabefeld presst.

Geld- und Wertdienste

Sebastian Sinemus stellt in veko-online.de eine **neue Generation** Geld- und Werttransporter vor, für die Experten verschiedener Karosseriebau- und Fahrzeugtechnikbetriebe mit dem Unternehmen Ziemann zusammengearbeitet haben. Hartmanganstahlbleche, Polykarbonat beschichtete Scheiben, Panzerung und eine automatische Einbruchmeldeanlage registriere jede unautorisierte Bewegung und leite im Bruchteil einer Sekunde Maßnahmen zur Gefahrenabwehr ein. Zur weiteren Ausstattung gehöre eine besonders ausgereifte Sicherheitstechnik, die beispielsweise im Notfall die ferngesteuerte Übernahme der Fahrzeugkontrolle zulasse und mit neuester GPS-Überwachung im permanenten Kontakt mit externen Partnern sowie der hauseigenen Notruf- und Serviceleitstelle stehe. Die Türsteuerung sei durch das Feedback der Teams im täglichen Einsatz so überarbeitet worden, dass eine maximalintuitive Bedienung entstanden sei. In der verbesserten Kontrolleinheit liefen zudem sämtliche digitalen Bildaufnahmen zusammen.

Hehlerei

Gestohlene Autos werden nach Beobachtung der Polizei zunehmend ausgeschlachtet, um die Einzelteile über das Internet zu verkaufen, meldet die FAZ am 8. Oktober. Mit dem Verkauf der Einzelteile lasse sich für Hehler mehr Geld verdienen als mit kompletten Autos, etwa das Zwei- bis Dreifache.

Industrie 4.0

Neue Sicherheitsstandards für Industrie 4.0 fordert Prof. Claudia Eckert, Fraunhofer Institut für Angewandte und Integrierte Sicherheit, in der Ausgabe 10-2015 der Zeitschrift PROTECTOR, S. 42/43. Die Politik könne durch das Festlegen von Mindestanforderungen beispielsweise bezüglich einer erforderlichen Zertifizierung und durch technische Mindestanforderungen Qualitätsleitplanken für sicherheitskritische Bereiche setzen, die derzeit noch nicht reguliert werden, also nicht unter KRITIS fielen. Das Zertifizieren und die erforderlichen Testverfahren seien durch die Industrie zusammen mit Forschungseinrichtungen zu erarbeiten. Wünschenswert erscheine es durchaus, die verschiedenen Aktivitäten zu koordinieren und beispielsweise über Referenzarchitekturen Leitplanken und Blaupausen für den Übergang von Industrie 2.0 und 3.0 zu 4.0 zu schaffen.

Die FAZ weist in einem Verlagsspezial vom 6. Oktober auf die „**Top 10 Sicherheitsbedrohungen** für Industrie 4.0" aus Sicht des BSI hin: Infektion mit Schadsoftware über Internet und Intranet; Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware; Social Engineering; menschliches Fehlverhalten und Sabotage; Einbruch über Fernwartungssysteme; internetverbundene Steuerungskomponenten; technisches Fehlverhalten und höhere Gewalt; Kompromittierung von Smartphones im Produktionsumfeld; Kompromittierung von Extranet und Cloud-Komponenten; (Distributed) Denial of Service-Angriffe. Jörg Fritsch, Gartner, habe klare Vorstellungen, wie IT-Sicherheit im Industrie 4.0-Umfeld künftig beschaffen sein sollte: „Was wir brauchen, ist eine adaptive Sicherheit, die auf Basis

von Mikro-Perimetern funktioniert, damit die Sicherheitsfunktionen immer wieder neuen Bedrohungsszenarien angepasst werden können." Diese Sicherheitsfunktionen müssten auf allen Sensoren, vernetzten Systemen, Produktionsmitteln und zentralen Steuerungselementen zur Verfügung stehen.

IT-Sicherheit

Die Haltung zu **Cyberpolicen** sei immer noch ambivalent, schreibt die FAZ am 20. September. Dies ergebe sich aus einer Befragung von 350 deutschen Unternehmen des Versicherungsmaklers Marsh. Zwei Drittel könnten den Umfang des Versicherungsschutzes nicht einschätzen, nur sieben Prozent halten das Angebot der Branche für ausreichend. 26 Prozent sagten, die Versicherungen erfüllten die Anforderungen des Unternehmens nicht oder nur in begrenztem Maße. 29 Prozent gäben an, innerhalb der nächsten zwölf Monate Deckungsschutz kaufen zu wollen. Mit den Policen sichern sich Unternehmen gegen Folgeschäden von Hackerangriffen ab. Dazu gehörten Betriebsunterbrechungen, Strafzahlungen für verlorengegangene Daten oder der Missbrauch von Telefonanlagen. Künftig dürften die finanziellen Risiken zunehmen. Vor allem die Finanzwirtschaft und die Energiebranche müssten sich durch das neue IT-Sicherheitsgesetz auf schärfere Anforderungen für ihr Risikomanagement einstellen. Nur ein Drittel der Befragten erwarte Schäden durch Hacker oder organisierte Kriminalität. 65 Prozent sähen eher interne Gefährdungen, sei es durch kriminelle, sei es durch ungewollte Schädigungen. Dennoch sei nur bei jedem sechsten Unternehmen das Thema Cyberrisiko in der Geschäftsführung angesiedelt.

Tausende **medizinische Geräte** seien aus dem Internet angreifbar, meldet heise.de am 29. September. Die Systeme seien oft mit Windows XP unzureichend abgesichert. Einige Systeme wiesen keine oder nur Standard-Passwörter auf, sodass sich Angreifer der Zugriff per FTP oder Telnet erschleichen könnten.

Security insight thematisiert in der Ausgabe 5-2015, S. 52/53, die **sichere Zerstörung digitaler Datenträger**. Wenn neue Rechner ins Haus kommen, müssten Unternehmen oft auf Tausenden alter Computer vielfach sensible Daten sicher löschen. Zwar gebe es dafür spezielle Software. Doch das sei zeitaufwändig. Der sicherste und effektivste Weg sei die mechanische Zerstörung des Datenträgers. Die DIN 66399 beschreibe anhand von drei Schutzklassen und sieben Sicherheitsstufen, wie besonders sensible Daten zu vernichten und welche Anforderungen die dafür eingesetzten Maschinen erfüllen müssen.

Drei Phasen auf dem Weg zu einer ausgereiften Cybersecurity bezeichnet TECCHANNEL.de am 4. Oktober: In der ersten Phase sollen Unternehmen ihre Informationssicherheit aktivieren. Dazu werden sechs Maßnahmen vorgeschlagen, unter anderem die Erneuerung und Aufstellung von Sicherheitsstandards und Richtlinien, um die Informationssicherheit langfristig zu steuern, zu kontrollieren und zu optimieren sowie der Aufbau eines Security Operations Center, das Dienstleistungen zum Schutz der Informationssicherheit und zur Risikovorbeugung bietet. In der zweiten Phase gehe es darum, die bestehenden Maßnahmen an die digitalen und wirtschaftlichen Veränderungen anzupassen, und zwar in fünf Schritten: unter anderem durch Implementierung eines Transformationsprogramms; Entscheidung, welche Maßnahmen intern umgesetzt werden und welche auszulagern sind; Berücksichtigung des Systems aller Geschäftspartner, deren Sicherheitsverstöße Auswirkungen auf das eigene Unternehmen haben können; Trainingsprogramme für die Mitarbeiter. In der anschließenden dritten Phase sollten Unternehmen prüfen, wo sie besonders verwundbar sind und wie sie auf mögliche Angriffe reagieren

können. Dazu werden fünf Maßnahmen vorgeschlagen, unter anderem Entwicklung und Implementierung einer „Cyber Threat Intelligence Strategie", Durchführung forensischer Datenanalysen und Sensibilisierung der Mitarbeiter für die Informationssicherheit.

In einem Verlagsspezial vom 6. Oktober behandelt die FAZ IT-Sicherheitsthemen. Unternehmen bräuchten **klare Strukturen und Richtlinien**, die Unterstützung bei den Mitarbeitern finden. Eine falsche Bedienung, die private Nutzung firmeneigener Hard- und Software sowie ein fahrlässiger Umgang mit Daten und Dokumenten bedrohten die Vertraulichkeit von Informationen. Die internen Risiken für die IT-Sicherheit müssten genauso ernst genommen werden wie Bedrohungen von außen. Dafür brauche es eine Sensibilisierung der eigenen Mitarbeiter und das ausdrückliche Bekenntnis der Unternehmensleitung, die damit den Stellenwert von IT-Sicherheit für den Geschäftserfolg unterstreiche und den verantwortlichen Mitarbeitern die nötige Durchsetzungskraft für Regeln und Maßnahmen verschafft.

Angriffe auf Drucker kämen immer häufiger nicht nur von innen, sondern auch von außen, schreibt Michael Dörfler in dem Verlagsspezial IT-Sicherheit der FAZ vom 6. Oktober. Mit eigener E-Mail-Adresse, Festplatte und direkter Netzwerkverbindung unterschieden sich Netzwerk- und Multifunktionsdrucker kaum noch von Computern. Bei ungeschützten Geräten ließen sich Druckdaten durch Kriminelle ohne Aufwand während der Übertragung abfangen, von der Festplatte auslesen oder nachdrucken. Drucker ließen sich über ungesicherte Schnittstellen oder nicht deaktivierte Protokolle im Netzwerk angreifen. Die im Gerät befindlichen Sicherheitstechnologien könnten dem Datendiebstahl aber einen Riegel vorschieben. Beispielsweise ließen sich vertrauliche Dokumente mit Pull-Printing schützen. Dabei werde ein Druckauftrag mit einer individuellen PIN versehen. Das Zugriffsmanagement könne neben dem alphanumerischen Code auch über eine Smartcard oder biometrische Verfahren wie einen Fingervenenscanner geregelt werden. IT-Experten würden die Absicherung der Schnittstellen ins Drahtlosnetzwerk über WPA2 empfehlen. Die Verschlüsselung sorge dafür, dass Datenströme auf dem Weg vom Client zum Drucker nicht von anderen Rechnern gelesen, protokolliert oder verändert werden. Mit Antimalware-Gateways ließen sich Eindringlinge erkennen und abwehren. Dann sei in einer lokalen Vernetzung die Absicherung für Drucker ähnlich wirksam wie für andere Geräte im Netz.

Mit **Alternativen zu Passwörtern** befasst sich der Behörden Spiegel in der Oktober-Ausgabe. Die Absicherung des Passwortes mit einem zweiten Faktor setze sich immer mehr durch. Es gelte das Prinzip: Der Nutzer muss etwas besitzen und etwas wissen. Beispielsweise werde zusätzlich zum Passwort ein zeitlich begrenzter Code an ein Gerät geschickt oder über eine App generiert. Dieser müsse zwingend neben dem eigenen Passwort eingegeben werden. Einige Hersteller arbeiteten aktuell an personalisierten USB-Schlüsseln. Um Zugang zu Daten zu erhalten, müssten Nutzer ein kleines Gerät anschließen, um sich zu identifizieren. Ähnlich funktioniere die Verwendung virtueller Tokens, die beispielsweise in das Smartphone integriert würden. Einen Schritt weiter gehe die Identifizierung anhand biometrischer Daten wie dem individuellen Pulsschlag, dem Fingerabdruck und der Iris.

Antiviren- und Antimalware-Programme würden der aktuellen Bedrohungslandschaft nicht mehr gerecht, ist Ammar Alkassar, Sirrix AG, überzeugt (Behörden Spiegel, Oktober-Ausgabe). Man brauche einen **Paradigmenwechsel zu proaktiven Systemen**. Als Beispiel dafür erwähnt er die Separation und die Integritätsprüfung. Bei der Separation würden, ähnlich wie in einem Schiffsrumpf, kritische Bereiche voneinander isoliert. Technisch ließe sich dies mit einem Sicherheits-

kern lösen. Er trenne die Hardware vom Betriebssystem. Als Lösung des Problems, dass es keine europäischen Hersteller für Betriebssysteme, Prozessoren, PCs und Smartphones gebe, sieht er die Replaceability-Software. Mit ihr könne man die Hardware ersetzen. Bei Cloud-Diensten könne man zum Beispiel mit dem BoxCrypter oder auch der PanBox jede beliebige Cloud auf dem Markt ohne Bedenken hinsichtlich der IT-Sicherheit nutzen.

Eine „Sicherheitskultur in Silos" sieht Jonathan Wegener, Intel Security Deutschland, darin, dass jeder die Instrumente suche, die zu seinem eigenen Zuständigkeitsbereich am besten passten (Behörden Spiegel, Oktober-Ausgabe). Die Systeme informierten sich kaum untereinander. Angreifer machten sich diesen Umstand zunutze, indem sie Trojaner entwickelten, die über unterschiedliche Medien und Wege angriffen. Informationen müssten heute schneller bereitgestellt werden. Die meisten Potenziale lägen in der frühzeitigen Erkennung von Angriffen.

IT-Sicherheit sei mehr als Hard- und Software, betont Jörg Hirschmann, NCP, in der Oktober-Ausgabe des Behörden Spiegel. Die unternehmensinterne IT-Abteilung müsse sich auf die Hersteller und das Pflichtbewusstsein der Endanwender verlassen können. Nur ein Miteinander der beiden verspreche Sicherheit vor Angriffen, Datenklau und Spionage. Eine funktionierende Vertrauenskette ermögliche zudem die gemeinsame Entwicklung von Sicherheitsprodukten und Standards zwischen Hersteller und Sicherheitsverantwortlichen.

Ein Forscherteam der ETH in Zürich wolle die **Zwei-Faktor-Authentifizierung radikal vereinfachen**, berichtet laut heise.de vom 9. Oktober die Technology Review in ihrer Online-Ausgabe. Dazu werde vorhandene Technik in PC und Handy eines Nutzers verwendet: die verbauten Mikrofone. Das Verfahren namens Sound-Proof setze auf zwei Teile. Eine browsergestützte Software im PC und eine zuvor vom Nutzer zu registrierende Login-App auf dem Handy, die für iOS und Android angeboten werden soll. Beide nähmen beim Einloggen im Browser am PC automatisch die Umgebungsgeräusche auf und gleichen sie gegeneinander ab. Empfangen beide Geräte dieselben Klänge, müssen sie folglich an einem gemeinsamen Ort sein. Hätte ein Hacker einfach nur ein Passwort erbeutet, wäre das nicht der Fall. Der zweite Faktor ließe sich nicht authentifizieren. Sound-Proof funktioniere mit aktuellen Browsern wie Chrome, Firefox oder Opera und solle sich technisch rasch umsetzen lassen. Firmen könnten es serverseitig implementieren.

In einem Verlagsspezial der FAZ am 20. Oktober fordert Mathias von Hofen **Mittelständler** auf, sich weit stärker als bisher mit dem Thema IT-Sicherheit zu beschäftigen. Sie seien bevorzugtes Ziel von Hackern, da sie in Deutschland einen großen Teil der besonders innovativen Produkte entwickelten. Auch aus der stark zunehmenden Nutzung von Smartphones ergäben sich Sicherheitslücken. Vor allem das Betriebssystem Android weise Mängel auf. Weiterhin sei durch die Cloud-Technologie das Risiko von Datenraub und -missbrauch gestiegen. Mit dem Produkt „Business Security" wende sich das Start-up-Unternehmen Secucloud vor allem an mittelständische Unternehmen. Das Produkt sei auf unterschiedlichen Geräten wie Desktops, Laptops, Tablets und Smartphones einsetzbar und enthalte unter anderem einen Webfilter, eine Antivirussoftware, eine Firewall und einen Application-Filter. Unternehmen, die das Gütesiegel „IT-Security made in Germany" erhalten wollen, müssten gewährleisten, dass sie ihren Hauptsitz in Deutschland haben, vertrauenswürdige IT-Sicherheitslösungen anbieten und den Anforderungen des deutschen Datenschutzes genügen. Außerdem müssten sie garantieren, dass ihre Produkte keine versteckten Zugänge – sogenannte Backdoors – enthalten.

Der TÜV Rheinland habe sein Angebot im Bereich Informationssicherheit um einen **Managed Service zur Abwehr komplexer Cyberangriffe** erweitert, berichtet silicon.de am 7. Oktober. Mit dieser Lösung seien mittelständische Unternehmen raffinierten gezielten Angriffen hochqualifizierter und finanziell bestens ausgerüsteter Angreifer nicht mehr schutzlos ausgeliefert. Das Angebot reduziere die Kosten, die in der Regel bei Anschaffung geeigneter Technologien für mittelständische Firmen zu hoch seien. Das mittelstandstaugliche Angebot setze auf Technologie des Spezialanbieters Lastline auf, sei aber ab einem Zehntel der üblicherweise für deren Anschaffung anfallenden Kosten verfügbar. Der TÜV Rheinland überwache im Rahmen des APT Defense Service den Netzwerkverkehr konstant durch verhaltensbasierte Analysesysteme. Würden dabei Anzeichen für einen Infektionsversuch oder einen gezielten Angriff gefunden, würden die durch Experten des Computer Security Incident Teams des TÜV Rheinland analysiert. Handele es sich tatsächlich um einen Angriff, unterstützen sie die IT-Abteilung des Unternehmens dabei, diesen abzuwehren und Maßnahmen zur Verbesserung der Sicherheit zu ergreifen.

IuK-Kriminalität

Die Zeitschrift WiK weist in der Ausgabe 5-2015, S. 9, auf eine Warnung des IT-Spezialisten Link11 vor der **cyberkriminellen Gruppe DD4BC (DDoS for Bitcoins)** hin. Die Ziele seien Großunternehmen im Finanzsektor sowie SaaS- und Hosting-Unternehmen. Es gebe eine „Warnattacke", die die Systeme der Unternehmen ohne DDoS-Schutz in den meisten Fällen überlaste und die Webseite offline nehme. Parallel dazu erhalte das Opfer eine Erpresser-E-Mail. Aktuell würden branchenabhängig bis zu 50 Bitcoins gefordert. Sollte die Zahlung ausbleiben, drohe DD4BC mit einem Volumen von 400–500 Gbps und erhöhe die Forderung auf 100 Bitcoins.

Die britische National Crime Agency (NCA) warnt Nutzer von Online-Banking vor der **Malware Bugat und Cridex**, berichtet heise.de am 14. Oktober. Cybergangster haben der Behörde zufolge englische Banken mithilfe der Schadsoftware bereits um rund 27 Mio. Euro erleichtert. Die NCA erkläre, dass sich die Malware in vermeintlich seriösen Dokumenten in gefälschten E-Mails versteckt. Lässt sich ein Nutzer austricksen und öffnet den Anhang, soll sich die Malware installieren und Bankdaten mitschneiden. Im Fadenkreuz der Cyberbankräuber stünden vor allem Unternehmen.

Kriminelle haben eine neue Masche, um über das **MTAN-Verfahren** die Konten von Bankkunden leerzuräumen, berichtet die FAZ am 22. Oktober. Sie würden zuerst den Computer der Kunden mit einer Schadsoftware infizieren und sich so Zugang zu deren Online-Konto verschaffen sowie die Handynummer und persönliche Daten auskundschaften. Gegenüber dem Provider gäben sie sich dann als Mitarbeiter eines Handy-Geschäfts aus, der für den Kunden eine neue SIM-Karte freischalten solle. Daraufhin seien die MTAN-Nummern nicht mehr auf das Handy des Kunden, sondern auf das der Betrüger geschickt worden. Dagegen betone die Kreditwirtschaft, die Nutzung des MTAN-Verfahrens sei sicher. Untersuchungen zeigten aber, dass zumindest kostenlose Antivirenprogramme viel Schadsoftware gar nicht entdeckten. Oft gelange die Schadsoftware einfach über ein Werbebanner auf einer Homepage auf den Rechner, weil der auf einen nicht ganz aktuellen Flashplayer mit Sicherheitslücke zugreife.

Kfz-Diebstahl

Nach dem vom BKA veröffentlichten **Bundeslagebild Kfz-Kriminalität** wurden 2014

insgesamt 18.549 Pkw auf Dauer entwendet. Das sind vier Prozent weniger als 2013 und drei Prozent weniger als im Durchschnitt der letzten fünf Jahre. Eine Zusammenfassung des Bundeslagebildes findet sich auf der Webseite von Securitas unter News/Sicherheitslage.

Nach einer Meldung in der Zeitschrift WiK (Ausgabe 5-2015, S. 8) warnt der Spezial-Versicherungsmakler für Omnibusunternehmen Dittmeier vor erhöhter **Diebstahlgefahr für Reisebusse**, vor allem in Paris. Die in den Bussen verbauten elektronischen Wegfahrsperren müssten dabei als wirkungslos betrachtet werden. Es empfehle sich, möglichst bewachte Parkplätze zu nutzen. Außerdem würden GPS/GSM/Funk-Ortungssysteme empfohlen, die das Wiederauffinden des Busses erhöhen.

Funkgesteuerte Autoschlüssel seien an den Rezeptionen etlicher Tophotels nicht sicher. Die Signale könnten leicht mit einem Sender abgegriffen werden. Darauf macht der auf Reisesicherheit spezialisierte Experte Ulrich Jander in der Oktober-Ausgabe von veko-online.de aufmerksam. Die Autoschlüssel der Gäste müssten in Metallkassetten oder in Geldschränken gelagert werden, nur so seien die Übertragungssignale abgeschirmt. Die Signale der Autoschlüssel könnten sonst an der Rezeption abgegriffen werden, zum Beispiel so: „In der Nähe steht ein gut gekleideter Herr mit einem Aktenkoffer, in dem sich ein Sender befindet. Er führt ein vermeintliches Handygespräch mit einem Geschäftspartner. Währenddessen steht sein Aktenkoffer auf dem Empfangstresen. In Wirklichkeit ist der Gesprächspartner ein Komplize, der sich mit dem Empfänger in der Nähe des Fahrzeugs befindet. Bekommt der Empfänger das Signal, das vom Koffer auf dem Tresen übertragen wurde, öffnet sich die Tür des Autos und das Kfz lässt sich mit Knopfdruck ohne Schlüssel starten. Der Empfänger speichert diese Daten ab, sodass später das Fahrzeug jederzeit ohne Probleme wieder gestartet werden kann."

Korruption

Die Reform der Korruptionsvorschriften (§ 299 StGB und Neueinführung der §§ 299 a und 299 b in das StGB) ziehe mit Sicherheit einen Anpassungsaufwand für die **Compliance-Richtlinien** in einigen Unternehmen nach sich, schreibt Dr. Jörg Viebranz, digital spirit GmbH, in der Fachzeitschrift comply (Oktober 2015, S. 18–20). Für alle Compliance-Verantwortlichen biete sich aber durch die zu erwartende Aufmerksamkeit in der Öffentlichkeit und bei ihren Führungskräften und Mitarbeitern die einmalige Gelegenheit, das Thema Compliance und Korruption kommunikativ zu nutzen.

Regierungsdirektorin Dr. Simone Hartmann, BMVg, befasst sich in der Fachzeitschrift comply (Ausgabe Oktober 2015, S. 26–28) mit der **Korruptionsprävention bei Beteiligungsgesellschaften des Bundes**. Unter Nr. 2 der Korruptionsrichtlinie des Bundes von 1998 werde gefordert, dass besonders korruptionsgefährdete Bereiche zu identifizieren sind. Die Umsetzung der Richtlinie müssten auch die juristischen Personen des Privatrechts und damit insbesondere die Beteiligungsgesellschaften des Bundes beachten. Zwingend sei die Beachtung nach Auffassung des Bundesrechnungshofes nicht nur für die Eigengesellschaften, sondern auch für alle Mehrheitsbeteiligungen des Bundes. Den Minderheitsbeteiligungen des Bundes werde die Beachtung empfohlen. Da auch diese korruptionspräventive Maßnahmen im Rahmen der öffentlichen Auftragsvergabe zu ergreifen hätten.

Angemessene **Compliance-Prozesse für Vertriebspartner im Ausland** thematisiert Rechtsanwalt Dr. Tobias Teicke in der Fachzeitschrift comply (Oktober 2015, S. 34–37). Dass Korruption in einigen Ländern stärker verbreitet sei als in anderen, sollte Unternehmen nicht dazu verleiten, in Risiko-Ländern unlautere Geschäftspraktiken als notwendiges

Übel zu übernehmen. Für Unternehmen und Management würden korrupte Geschäfte auch schon dann zum haftungs- und sogar strafrechtlichen Risiko, wenn das Management über die unlauteren Zahlungen überhaupt nicht im Bilde war. Die Geschäftsleitung sei zivil-, ordnungswidrigkeiten- und strafrechtlichen Risiken ausgesetzt, wenn sie im Ausland Vertriebspartner einsetzt und dabei stillschweigend billigt, dass diese zuständige Vergabestellen bestechen. Präventionsmaßnahmen müssten beim Vertriebspartner mit Augenmaß implementiert werden.

Die Fachzeitschrift comply behandelt in der Ausgabe Oktober 2015, S. 50–53, einen Erfahrungsbericht der Clyde Bergemann Power Group, Inc., zur Auswahl und Einführung von **E-Learning zur Korruptionsprävention**. E-Learning müsse mit einem geeigneten Lernmanagementsystem betrieben werden. Nur mit einem solchen System könnten die immensen Vorteile eines E-Learning voll ausgeschöpft werden. Die Auswahl eines geeigneten E-Learning für die Korruptionsprävention bedürfe einer akribischen Vorbereitung, Koordination und Umsetzung seitens der Projektleitung. Es sei wichtig, ein Produkt auszuwählen, das durch exzellente Didaktik und eine gut durchdachte Kursstruktur besticht. Ferner spiele es eine ganz bedeutende Rolle, das Training auch in der jeweiligen Landessprache anzubieten. Schließlich sollte es ein Anbieter sein, der die Lerninhalte stets auf dem neuesten Stand hält und in der Lage ist, einen guten Support bereitzustellen.

Kritische Infrastrukturen

Mit dem Funktionsbereich „Schutz kritischer Infrastrukturen" durch private Sicherheits-Dienstleister befasst sich Manfred Buhl, Securitas Deutschland, in der Ausgabe 5-2015 der Zeitschrift Security insight, S. 18/19. Der großen Bedeutung kritischer Infrastrukturen entsprechend müsse der Dienstleister zuverlässig und qualifiziert, müssten seine Leistungen fachgerecht und effizient sein. Zur Bestätigung der Zuverlässigkeit der Beschäftigten sei eine unbeschränkte Auskunft aus dem BZR erforderlich. Je komplexer der Schutzauftrag ist, desto höher müsse die Qualifikation der eingesetzten Kräfte und ihrer Vorgesetzten sein. Das zu beauftragende Sicherheitsunternehmen sollte die von der IMK seit 2009 geforderte Zertifizierung erwerben.

Logistiksicherheit

Dr. Ulrich Franke, Institute for Supply Chain Security GmbH, und Prof. Dr. Jutta Lommatzsch, HRW, befassen sich in der Fachzeitschrift WiK (Ausgabe 5-2015, S. 24/25) mit **Haftungsrisiken für die Unternehmensleitung** bei Wirtschaftskriminalität in der Supply Chain. Je fragmentierter und global verteilter Wertschöpfungsnetzwerke sind, desto größer seien die Gefahren, dass sie durch kriminelle Handlungen gestört und instabil werden. Unsichere und ungesicherte Wertschöpfungssysteme könnten zu einem unkalkulierbaren unternehmerischen Risiko werden. Potenzielle Risiken entlang der Supply Chain – von der Produktentwicklung bis zur Auslieferung der Produkte – müssten strukturiert analysiert, bewertet und priorisiert werden. Erst nach einer detaillierten Analyse der Gefährdungsquellen könnten technische Maßnahmen implementiert, organisatorische und prozessuale Strukturen und Abläufe geplant und eingeführt sowie juristische Vorkehrungen getroffen werden. Unternehmen könnten ihre Anstrengungen in Bezug auf Sicherheit durch die ISO 28000 ff. „Supply Chain Security"-Zertifizierung dokumentieren. Die Autoren analysieren und bewerten drei Fallbeispiele.

Die Fachzeitschrift WiK, Ausgabe 5-2015, S. 26–28, befasst sich mit **Resilienz**, der Widerstandsfähigkeit von Unternehmens-

prozessen gegenüber Störfällen. Der durchschnittliche Schaden durch eine Störung in der Supply Chain werde nach einer Untersuchung der Marktforscher von ChainLink auf ca. zehn Prozent des Shareholder Values geschätzt. Die Deutsche Post DHL Group, die in mehr als 220 Ländern und Regionen aktiv sei, arbeite daher an einem Konzept zur „Supply Chain Security 2.0". Ein Ergebnis sei der Service „DHL Resilience360", eine cloudbasierte Informationsplattform für Entscheider, in der die verfügbaren Informationen über eine Supply Chain und die weltweiten Risiken so verknüpft würden, dass sie die aktuelle Risikolage abbilden. Zusätzlich würden dabei möglichst viele Informationen bereitgestellt, um zeitnah qualifiziert auf neue Risiken reagieren zu können. Nutzer der „Big Data"-Plattform seien neben DP DHL insbesondere die Automobilbranche, aber auch die Chemieindustrie, Life Sciences und Unternehmen im Technologiesektor. Die Plattform werde weltweit von mehr als 1.000 Sicherheitsmitarbeitern gepflegt und genutzt. Je nach Informationsziel biete die Plattform unterschiedliche Darstellungsweisen. Grundlage sei in der Regel eine Karte, die die Informationen den jeweiligen Geopositionen zuordnet. Werde das kundeneigene Transport-Managementsystem in Resilience360 eingebunden, könnten Unternehmen den Status ihres gesamten Sendungsbestandes weltweit abrufen. Während „Resilience360 Risk Assessment" vor allem eine Analyse der Risikosituation der Supply Chain auf Basis von historischen Daten und dazu Lösungsvarianten zur Risikominderung biete, visualisiere „Resilience360 Incident Monitoring" vor allem die aktuellen Risiken für die Supply Chain des Kunden.

Luftverkehrssicherheit

Wie das BMI mitteilt, traten zum 1. September ergänzende Sicherheitsvorschriften der EU-Verordnung Nr. 185/2010 in Kraft, die die Kontrolle von Fluggästen und ihres mitgeführten Handgepäcks an allen europäischen Flughäfen betreffen (WiK, Ausgabe 5-2015, S. 6). Danach werden Passagiere und Handgepäck einschließlich elektronischer Geräte wie Laptops, Tablets oder Mobiltelefone stichprobenartig auf Spuren von Sprengstoffen kontrolliert. Dies erfolge mittels spezieller Probenehmer – Papierstreifen oder Wischpads – mit denen der Fluggast oder das Gepäck an bestimmten Stellen geprüft werde. Die chemische Analyse der Proben vor Ort ermögliche die Feststellung von Spuren sprengstoffverdächtiger Zusammensetzungen.

Maschinensicherheit

Christian Bittner, Pilz GmbH & Co. KG, befasst sich in Ausgabe 10-2015 der Zeitschrift GIT, S. 104/105, mit der richtigen Umsetzung der **Betriebssicherheitsverordnung**, deren Novellierung seit Juni in Kraft ist. Insgesamt würden besonders unfallträchtige Bereiche wie Instandhaltungsarbeiten an Arbeitsmitteln sowie der Schutz vor Manipulationen von Schutzeinrichtungen stärker berücksichtigt. Die Änderungen trägen außerdem der demografischen Entwicklung in Unternehmen sowie den ergonomischen und psychischen Belastungen Rechnung. Sprache und Struktur seien vereinfacht und Doppelregelungen gestrichen worden. Der Autor behandelt insbesondere die Gefährdungsbeurteilung als zentrales Mittel, die Umsetzung durch eine „befähigte Person". Der Unternehmer müsse sich von deren Kompetenz überzeugen, könne diese Verpflichtung aber auch an eine externe Stelle vergeben. Dies entbinde ihn aber nicht von der Pflicht, die Kompetenz des ausführenden Unternehmens zu prüfen. Im Gegensatz zu zertifizierten Unternehmen erwiesen sich hierbei akkreditierte Stellen als besonders hilfreich, da eine Akkreditierung eine rechtlich verbindliche Kompetenzaussage solcher Stellen treffe.

GIT stellt in Ausgabe 10-2015, S. 111–118, das **Safety Evaluation Tool** (SET) von

Siemens vor, das sowohl Hersteller als auch Anwender von Maschinen und Anlagen auf ihrem Weg, die weltweiten Forderungen nach erhöhter Sicherheit zu erfüllen, unterstütze. Typische Praxisbeispiele, die den hohen Nutzwert solcher Expertensysteme einfach beschreiben, seien zum Beispiel das Nachrüsten von Sicherheitsfunktionen bei der Verkettung von CE-zertifizierten Maschinen oder die Überprüfung von vorhandenen Sicherheitsfunktionen nach aktueller Normenlage. Die wichtigste Voraussetzung für den sinnvollen Einsatz des Tools sei die Risikoanalyse.

NSL

Verfügbarkeitsanforderungen von Leitstellen an Kommunikationsnetze behandelt Dipl.-Kaufmann Michael Hobeling, HWS Wachdienst Hobeling GmbH, in der Ausgabe 5-2015 der Zeitschrift WiK, S. 64/65. Jede NSL sollte Konzepte erstellen, die auch bei Ausfällen und Störungen des Kommunikationsnetzes den Empfang und die Bearbeitung eingehender Alarme garantieren sollen. Anforderungen an die Verfügbarkeit würden auch bereits in den entsprechenden Normen und Richtlinien, wie etwa in den DIN EN 50136, den DIN EN 50518 und VdS 3138 gestellt. Der Autor erläutert die Verfügbarkeitsanforderungen, die Technik zur Netzstruktur vor Ort und zum Netzumbau sowie die Vorgehensweise bei der Konzepterstellung. Für die Netzverfügbarkeit werde laut Norm bei einer Single Path 6 oder Dual Path 3-Übertragung eine jährliche Verfügbarkeit von 99,9 Prozent gefordert. Die Norm erlaube somit umgerechnet maximal 8,75 Stunden Ausfall der Übertragungsnetze in einem Jahr.

Rechtsanwalt Dr. Henning Kahlert äußert sich in der WiK (Ausgabe 5-2015, S. 66–68) zur **Haftung des Leitstellenbetreibers** bei Missachtung einschlägiger technischer Richtlinien. Er behandelt die Frage nach einem Mitverschulden des Kunden und dem vertraglichen Haftungsausschluss. Betreiber von NSL müssen sicherstellen, dass die Anforderungen der einschlägigen technischen Normen eingehalten werden. Werden sie nicht erfüllt, hafte er dem Kunden gegenüber grundsätzlich für den gesamten Schaden, wenn er nicht glaubhaft darlegen kann, dass sein Versäumnis nicht kausal für den Schadenseintritt war.

ÖPV

Mit **proaktiven Video-Lösungen** im öffentlichen Personenverkehr befasst sich Jan Engelschalt, Axis Communications GmbH, in der Zeitschrift GIT, Ausgabe 10-2015, S. 54–56. Der sogenannte Incident-Lifecycle lasse sich in fünf oder sechs verschiedene Schritte einteilen: Erfassung, Priorisierung, Reaktion, erneute Priorisierung, Untersuchung und Nachverfolgung. Netzwerk-Videos spielen in allen Phasen des modernen Zwischenfall-Managements eine bedeutende Rolle. Dazu gehöre die intelligente Analyse des Videos ebenso wie ein zusätzlicher Erfassungsmechanismus zur frühzeitigen Erfassung von Ereignissen.

Organisierte Kriminalität

Im Oktober 2015 veröffentlichte das BKA das **Bundeslagebild 2014** zur Organisierten Kriminalität (OK). 2014 waren 571 Verfahren der OK anhängig. Sie richteten sich insgesamt gegen 8.700 Tatverdächtige. Der ermittelte Schaden belief sich auf 593 Mio. Euro. Ein Hauptaktivitätsfeld bildete die Kriminalität im Zusammenhang mit dem Wirtschaftsleben (18,9 Prozent). Eine Zusammenfassung des Bundeslagebildes findet sich auf der Webseite von Securitas unter News/Sicherheitslage.

Politisch motivierte Kriminalität

Am 13. Oktober veröffentlichte das BKA eine **Gefährdungslage** der politisch motivierten Kriminalität. Nach wie vor sei im Zusammenhang mit Veranstaltungen, aber auch davon losgelöst, von einer niedrigen Hemmschwelle zur Gewaltanwendung durch Linksextremisten, insbesondere gegen eingesetzte Polizeikräfte, auszugehen. Die linksextremistische Gewalt erreiche aber weder in ihrer Gesamtheit noch in Form herausragender Einzeltaten eine erkennbare terroristische Dimension. Dagegen sei im Phänomenbereich Rechtsextremismus neben einzelnen schwersten Gewaltstraftaten auch die Bildung bislang unerkannter terroristischer Vereinigungen in Betracht zu ziehen. Außerhalb terroristischer Strukturen sei zudem mit fremden- bzw. islamfeindlichen Gewaltdelikten in Form von Körperverletzungen, auch mit Todesfolge, Brandanschlägen und in Einzelfällen mit Tötungsdelikten zu rechnen. Aus dem Bereich des islamistischen Terrorismus könne neben den religiös motivierten Tätern auch eine Vielzahl überwiegend säkular orientierter militanter Organisationen die Sicherheit der Bundesrepublik Deutschland sowie deutscher Interessen im Ausland gefährden. Deutschland diene einzelnen terroristischen Organisationen als Ruhe-, Rückzugs- und Rekrutierungsraum sowie als Basis für logistische Aktivitäten. Die Gefahr dschihadistisch motivierter Gewalttaten im Bundesgebiet sei vor dem Hintergrund der weltweiten Entwicklungen im Phänomenbereich des islamistischen Terrorismus anhaltend hoch. Sie könne sich jederzeit in Form von Gewalttaten gegen staatliche und zivile Einrichtungen sowie Personen konkretisieren. Hinsichtlich möglicher Modi Operandi seien Anschläge unter Nutzung von unkonventionellen Spreng- und Brandvorrichtungen aufgrund der Wirkung und Symbolkraft nach wie vor das Mittel der Wahl für dschihadistische Täter. Die mögliche Zielauswahl dschihadistischer Tätergruppierungen und Einzeltäter orientiere sich weiterhin an Anschlagszielen, die ein Maximum an medialer Aufmerksamkeit sowie infrastrukturellem und wirtschaftlichem Schaden garantieren. Das Engagement der Bundesrepublik gegen den sogenannten Islamischen Staat könnte, insbesondere in muslimisch geprägten Staaten, zu gefährdungsrelevanten Entwicklungen zum Nachteil deutscher Einrichtungen und Interessen führen. Bei Cyberangriffen politisch agierender Cyberkriminellen auf Unternehmen sei von einer sehr hohen Dunkelziffer auszugehen. Neben wirtschaftlichen Schäden in Millionenhöhe seien Sabotageangriffe auf kritische Infrastrukturen zukünftig in Betracht zu ziehen. Nicht zuletzt die rasant steigenden Fallzahlen von Übergriffen auf Flüchtlingsunterkünfte sowie die teils gewalttätigen Demonstrationen aus dem rechtsextremen sowie linksextremen Spektrum verdeutlichten, dass aus der Flüchtlingsthematik Gefahrenmomente erwachsen. In der Gesamtschau lägen bislang unverändert keine belastbaren Erkenntnisse in Bezug auf ein gezieltes Einschleusen von Kämpfern im Flüchtlingsstrom durch terroristische Organisationen zur Begehung von Anschlägen vor.

Proliferation

Wie das BKA in der Wochenlage am 2. Oktober berichtet, hat das OLG Frankfurt einen Deutsch-Iraner wegen ungenehmigten Exports zu dreieinhalb Jahren Gefängnis verurteilt. Er hatte über eine von ihm geleitete Import-/Exportfirma 2008 und 2009 gewerbsmäßig 20 Lieferungen von 61 Flugmotoren eines deutschen Herstellers nach Iran ausgeführt und damit gegen das AWG verstoßen. Die Motoren seien als Antriebe von Drohnen geeignet, die auch die iranischen Streifkräfte verwenden, und waren bei der Ausfahrt als Jet-Skimotoren getarnt.

Rechenzentrumssicherheit

Unternehmen hinken bei der physischen Absicherung ihrer Serverräume hinterher, berichtet die FAZ in einem Verlagsspezial am 6. Oktober. So verfügten zwei Drittel der befragten IT-Verantwortlichen über keine redundante Echtzeitalarmierung. Die Geschäftsführung eines Unternehmens stehe letztlich voll in der Haftung für die Serversicherheit.

Nicht alle Unternehmen haben, wie tecchannel.de am 13. Oktober betont, ihre Serverräume oder Rechenzentren auf einen möglichen Ausfall oder Störfall vorbereitet. **Tipps von TECCHANNEL** sollen helfen, Systemausfälle zu vermeiden und drohenden Datenverlusten vorzubeugen. Wie wichtig Verfügbarkeit ist, lasse sich daran demonstrieren, dass 2014 Unternehmen in Deutschland wegen „Downtime" Verluste von zusammengerechnet 11,6 Mrd. Euro hinnehmen müssen – so eine Schätzung von ECM. Grundsätzlich sei zwischen Hochverfügbarkeitssoftware und einer Cluster-Lösung zu unterscheiden. Bei der Softwarelösung betrage die Ausfallzeit weniger als eine Stunde pro Jahr, bei Hochverfügbarkeits-Clustern hingegen fast neun Stunden. Für jede Anwendung, bei der mit sensiblen Daten gehandelt werde und beispielsweise eine Rundum-Überwachung zu den Compliance-Richtlinien des Unternehmens zähle, sei eine Always-On-Lösung unabdingbar. Mit der richtigen Verfügbarkeitslösung ließen sich Probleme auf ein Minimum beschränken. Umgekehrt ließen sich natürlich auch Kosten senken, denn Geschäftsausfälle, Produktionseinbußen, Entschädigungszahlungen für verloren gegangene Daten oder Vertragsstrafen gehörten der Vergangenheit an. Der Vorteil einer softwarebasierten beziehungsweise softwaredefinierten Hochverfügbarkeitslösung sei, dass alle Systemkomponenten permanent überwacht, Fehler schon frühzeitig erkannt und dadurch Ausfallzeiten, Datenverluste oder Betriebsunterbrechungen vermieden werden.

Risikomanagement

Prof. Dr. Jan Jürjens, TU Dortmund, stellt in der Zeitschrift WiK, Ausgabe 5-2015, S. 29–31, ein **Tool für Wirtschaftlichkeit und Effektivität** zum Erstellen von Sicherheitskonzepten vor. Der notwendige Kompromiss zwischen sicher und wirtschaftlich lasse sich optimieren. Dazu hätten unter anderem Fraunhofer-Experten die Analyse-Software SECONOMICS konzipiert. So würden Szenarien wie (Natur-)Katastrophen, Sabotage, Terrorismus oder Wirtschaftsspionage abgedeckt und Sicherheitsmaßnahmen wie Zutrittskontrollen, Erkennung von chemischen, biologischen, radioaktiven sowie nuklearen Gefahren, Perimeter-Systemen und der Einsatzplanung von Personal sowie der IT-Sicherheit gegenübergestellt. Geplant sei, das Tool Unternehmen zur eigenen Verwendung zur Verfügung zu stellen. Neben dem Hintergrundwissen, das im Werkzeug enthalten ist, könne der Nutzer individuelle Eingaben hinzufügen, die in die Analyse mit einbezogen werden. Die Ergebnisse der Analyse würden zusammengefasst. Dies ermögliche es, Maßnahmen nach Abschluss der Analyse schnell umzusetzen.

Schließsystem

Mit dem Schließsystem für **Tresore in der Bargeldlogistik** befasst sich Security insight in der Ausgabe 5-2015, S. 40/41. Um zu vermeiden, dass im Fall eines Streiks der Geldtransporteure der Tresor für das Unternehmen nicht mehr zugänglich ist, weil nur sie den Öffnungscode der Schlösser kennen, sei der Einmal-Code pylocx entwickelt worden, der aus vier Komponenten bestehe: aus der mobilen PIN-Tastatur „pyKey", einer Kontaktstelle, einem Steuermodul und einem Schloss. Der Clou liege in der Organisation: Jeder pyKey sei nicht nur der jeweiligen Geldtransportfirma zugeordnet, sondern auch

dem einzelnen Mitarbeiter und dem jeweiligen Schloss. So lasse sich nachvollziehen, wer wann die Geldautomaten geöffnet hat. Falle die Geldtransportfirma aus, so genüge ein Mausklick, um die Berechtigungen auf die pyKeys eines anderen zu übertragen.

Schwarzarbeit

Etwa 1.200 Beamte seien am 7. Oktober rund um den Frankfurter Flughafen gegen eine mutmaßliche Betrügerbande vorgegangen, berichtet die FAZ am 8. Oktober. Im Kern gehe es um illegale Beschäftigung beim Fracht- und Gepäckumschlag, durch die ein Schaden von rund 18 Mio. Euro entstanden sei. 170 Objekte in sieben Bundesländern seien durchsucht worden. Bei der Durchsuchung eines Hauses in Rüsselsheim seien die sechs Hauptbeschuldigten aus der Führungsebene der mutmaßlich kriminellen Vereinigung verhaftet worden. Über ein internes Firmengeflecht seien Dienstleistungen im Bereich Gepäckabfertigung und Fracht angeboten worden, die dabei eingesetzten Beschäftigten seien aber nicht vorschriftsgemäß sozialversichert gewesen. Die jeweiligen Generalunternehmen sowie Fraport sollen getäuscht worden sein.

Sicherheitsgewerbe

Die **Digitalisierung des Sicherheitsgewerbes** thematisiert Manfred Buhl, Securitas Deutschland, in der Zeitschrift PROTECTOR, Ausgabe 10-2015, S. 46/47. Die Digitalisierung verbessere, beschleunige, erleichtere und reduziere personelle Sicherheitsdienstleistungen. Gleichzeitig erfasse sie mehr und mehr die Infrastruktur des Sicherheitsunternehmens, seine Organisation, die Einsatzvor- und -nachbereitung, Informationssammlung, -verarbeitung und -weitergabe. Dabei werde von der Unternehmensleitung ein nicht immer leicht zu verwirklichendes Change Management gefordert.

Dipl.-Betriebswirt Bernd Schäfer, ATLAS Versicherungsmakler für Sicherheits- und Wertdienste GmbH, plädiert in der Zeitschrift WiK (Ausgabe 5-2015, S. 16–18) dafür, bei der Übernahme von Aufträgen zur Sicherung von Asylbewerberunterkünften auf den **Versicherungsschutz** zu achten. Notwendig seien die Betriebshaftpflichtversicherung, Versicherung für Forderungen nach dem Mindestlohngesetz, AGG-Deckung, Strafrechtsschutzversicherung und D&O-Versicherung. Der Autor behandelt insbesondere Fragen im Zusammenhang mit der Betriebshaftpflichtversicherung, der Versicherung für ungepanzerte und unbewaffnete Geldtransporte, der Haftung für Subunternehmer, zu Forderungen nach dem Mindestlohngesetz, des Allgemeinen Gleichbehandlungsgesetzes (AGG), strafrechtlicher Vorwürfe, der Managerhaftung und der Betreibermodelle.

Sicherheitskultur

Wolfgang Bayer, Bayer Security Consulting & Services GmbH, betont in einem Beitrag in der Ausgabe 5-2015 von Security insight, S. 55–57, dass zur Unternehmenssicherheit auch die **Berücksichtigung von „Soft Skills"** gehört. Es sei den Verantwortlichen meist sehr wohl bewusst, dass Frustration, Unzufriedenheit oder Mobbing nicht nur die Arbeitsleistung beeinträchtigen, sondern auch zum Sicherheitsrisiko werden. Entscheidungen der Unternehmensleitung dürften nicht dazu führen, dass Mitarbeiter ihr „Gesicht verlieren", etwa wenn eine Führungskraft hinsichtlich Position oder Verantwortung herabgestuft wird und dies für Kollegen oder sogar Außenstehende offensichtlich ist. Ein Sicherheitskonzept müsse bei grundlegenden Bedürfnissen der Mitarbeiter ansetzen. Dazu gehörten Zuwendung, Respekt und Anerkennung, weitgehende Selbstbestimmung

am Arbeitsplatz, Vorgabe von Zielen statt Arbeitsmethoden, Beteiligung bei Entscheidungen, Gerechtigkeit, angemessene Entlohnung, Fürsorge, transparente vertikale und horizontale Aufstiegschancen.

Sicherheitsmarkt

Dr. Peter Fey, Dr. Wieselhuber & Partner, beschreibt in der Ausgabe 5-2015 von Security insight, S. 28–30, die Chancen der deutschen Sicherheitswirtschaft aufgrund des weltweiten **Megatrends der Urbanisierung**. Rund 2.300 Städte planten, in den nächsten Jahren immense Beträge in Safe-City-Projekte zu investieren. Adäquate Sicherheitssysteme seien dabei charakterisiert durch leistungsfähige Überwachungstechnik, hohe Konnektivität der Geräte zueinander und mit der bestehenden Netzwerk-Infrastruktur/den Managementsystemen, leistungsfähige Datenzentren in Verbindung mit Komprimierungstechnik und integrierte Managementsysteme und sicherheitstechnische Leitstände.

Sicherheitstechnik

Markus Baba, HID Global GmbH, befasst sich in der Ausgabe 10-2015 der Zeitschrift PROTECTOR, S. 32/33, mit der **Standardisierung** der Sicherheitstechnik. Standards wie die ONVIF-Spezifikation OSDP (Open Supervised Device Protocol), Badnet (Building Automation and Control Networks) oder OPC (OLE for Process Control) ermöglichten in der Informations- und Kommunikationstechnik sowie Gebäudeautomation die Konzeption konvergenter Lösungen. Das betreffe gerade auch den Bereich der Sicherheitstechnik. Eine wichtige Voraussetzung für die Realisierung vernetzter, integrierter Systeme sei die stärkere Verbreitung IP-basierter Sicherheitsprodukte. Bei Videosystemen sei der Einsatz offener, standardisierter Systeme bereits Realität. Hier habe sich ONVIF als der De-facto-Standard etabliert. Eine ähnliche Entwicklung zeichne sich im Bereich der Zutrittskontrollsysteme ab. Hier kristallisiere sich OSDP als neuer Standard heraus. Er basiere auf einer standardisierten RS 485-Schnittstelle und unterstütze die bidirektionale Kommunikation. Die Leser könnten in einer Entfernung von bis zu 1.200 Metern angeschlossen werden. Auch Reihenschaltungen seien möglich. Eine hochsichere bidirektionale Kommunikation sei durch die AES 128-Verschlüsselung gewährleistet. Der Trend zu Offenheit und Standardisierung zeichne sich auch auf der Automatisierungsebene mit den Controllern und der Managementebene mit den entsprechenden Software-Managementlösungen ab.

Sicherheitsunterweisung

Sicherheitsunterweisungen für Fremdfirmenmitarbeiter in Großunternehmen thematisiert Security insight in der Ausgabe 5-2015, S. 21. Die Deutsche Gesetzliche Unfallversicherung gelte auch für Besucher und Fremdfirmenmitarbeiter – und zwar den potenziellen Gefahren ihrer Tätigkeitsfelder entsprechend. Für jede Tätigkeit müsse eine Sicherheitsunterweisung individuell vorgehalten und auf dem aktuellen Stand gehalten werden.

Smart Home

Manfred Endt, BHE, sieht **Smart Home Security auf dem Vormarsch** (WiK, Ausgabe 5-2015, S. 52/53). Auch sicherheitstechnische Installationen aus dem Bereich der Einbruch- und Brandmeldetechnik, Videoüberwachung und Zutrittssteuerung seien immer häufiger vernetzbar. Das Anwendungsspektrum sei breit. So könnten spezielle Melder den Austritt von Gas im Haus erkennen und automatisch alle Stromkreise abschalten. Wassermelder bemerkten

Flüssigkeit auf einer überwachten Fläche und steuerten direkt die Wasserpumpe an, um eine Überflutung zu verhindern. Mit der Scharfschaltung der Alarmanlage beim Verlassen des Hauses könne das automatisierte Ausschalten des Küchenherdes bewirkt werden. Aber Geräte aus dem Baumarkt entsprächen nicht den gängigen Standards der Sicherungstechnik. Low-End-Geräten fehle es unter anderem an einer Sabotageüberwachung der Systemkomponenten zum Schutz vor mechanischer und elektronischer Fremdbeeinflussung. Auch eine Minimierung der Falschalarme, etwa durch die sogenannte „zwangsläufige Unscharfschaltung", sei nicht vorhanden. Professionelle Produkte der Smart Home Security seien dagegen nicht für den Selbsteinbau geeignet.

Ingenieurin Jessika Fritz, DKE, tritt in der Ausgabe 5-2015 der Zeitschrift WiK, S. 54–56, dafür ein, dass neu aufkommende Anforderungen durch die **zunehmende Vernetzung** von Systemen der Smart Homes und Smart Buildings auch in Normen und Standards abgebildet werden. Ein Mittel im Rahmen dieser Standardisierungsarbeit sei die sogenannte Use-Case-Methode, bei der Anwendungsfälle (Use Cases) analysiert werden. User Stories und Use Cases bildeten den Ausgangspunkt für die Definition der erforderlichen Anforderungen. In der Normung und Standardisierung würden die Analyseergebnisse in einem Konsensverfahren auf einen generischen Nenner gebracht, um eine Basis für hersteller- und systemübergreifende Smart-Home-Lösungen zu schaffen. Mit Hilfe der Anwendungsfälle und einem Smart-Home-Referenzarchitekturmodell lasse sich auch eine Gap-Analyse durchführen, die den Normungsbedarf und die Technologielücken identifiziere.

Social Engineering

Die Ermittlung des Anfälligkeitspotenzials für Social Engineerings skizziert Udo Hohlfeld, „Intelligence Specialist", in der Ausgabe 5-2015 von Security insight (S. 61). Zuerst sei wichtig, welche Informationen für andere interessant sind und warum. So lasse sich eine ganze Klassifikationshierarchie für das Unternehmens-Know-how entwickeln. Weiterhin gehöre dazu die Ermittlung, wer Zugriff auf welche Informationen hat und ob das überhaupt sinnvoll ist. Zu der Klassifizierungshierarchie komme somit ein abgestuftes Zugangs- und Prioritätensystem. Zu überprüfen seien auch die privaten Profile der Mitarbeiter. Welche Informationen sind dort veröffentlicht, die Angreifer für eine Social-Engineering-Attacke verwenden könnten?

Spionage

Mit der **EU-Richtlinie zum Know-how-Schutz** befasst sich Dr. Michael Dorner, CMS Hasche Sigle, in der Ausgabe 10-2015 der Zeitschrift PROTECTOR, S. 18/19. Weder in der EU noch in Deutschland gebe es derzeit ein übergreifendes Gesetz zum Know-how-Schutz. Ausschlaggebend für den Richtlinienvorschlag der EU-Kommission sei vor allem, dass zwischen den einschlägigen Rechtsvorschriften der EU-Mitgliedsstaaten erhebliche Unterschiede bestehen und damit kein einheitliches Schutzniveau gewährleistet sei. Insbesondere fehle derzeit eine einheitliche Definition davon, was als „Geschäftsgeheimnis" geschützt werden soll. Vertragliche Absicherungen seien zwingender Bestandteil eines Know-how-Schutzkonzepts. Ungeachtet datenschutzrechtlicher Erwägungen werde häufig unklar sein, wessen Geheimsphäre die anfallenden Daten in dynamischen, multipolaren Wertschöpfungsketten zuzuordnen sind: dem Zulieferer eines Gerätes, dem OEM, dem Endnutzer oder dem zwischengeschalteten IT-Plattformbetreiber. Die maßgebliche Herausforderung sei es, derartige Szenarien überhaupt zu erkennen, zu analysieren und die erforderlichen technischen und vertraglichen Absicherungen zu treffen.

Risiken für Geschäftsreisende skizziert die Zeitschrift PROTECTOR in der Ausgabe 10-2015, S. 48/49. Die Vertraulichkeit gespeicherter Daten sei schon bei der Einreisekontrolle generell nicht gewährleistet. Damit gesichert ist, dass Gäste ihre Laptops im Hotelzimmer stehen lassen, würden Zielpersonen beispielsweise zu einem Abendtermin eingeladen. Auch wenn es unhöflich ist, zu solchen Terminen Laptops mitzubringen, solle man das tun. Der Geschäftsreisende solle auch nur die Daten auf den Laptop laden, die für den aktuellen Anlass unbedingt notwendig sind. Aktuelle und auch bereits gelöschte Daten auf einem USB-Stick könnten auf einem fremden Rechner unbemerkt kopiert werden. Smartphone-Nutzer seien sämtlichen Gefahren des Internet ausgesetzt. Bis heute gebe es für sie kaum zuverlässige Firewalls oder Virenscanner.

Terrorismus

Über die terroristische Bedrohungslage für Unternehmen und ihre Mitarbeiter äußert sich im Gespräch mit Claus Schaffner, WiK-Redaktion, Glenn Schoen, Boardroom@Crisis (WiK, Ausgabe 5-2015, S. 20–23). Auch Unternehmen seien ein Teil des „Geschäftsmodells" des IS. Das größte Risiko ergebe sich hier für Unternehmen, die in den „hot areas" im Ausland tätig sind, die einen starken Markennamen tragen und natürlich generell für Unternehmen, die keine Sicherheitsvorkehrungen getroffen haben. Am schlechtesten vorbereitet seien Unternehmen, die internationales Neuland betreten oder sich aus bestimmten Gründen zum ersten Mal auch in ihrem Heimatland bedroht sehen. Terroristen aller Couleur sähen inzwischen den Cyberspace als unverzichtbares Mittel in ihrem „Kampf" an, ganz besonders Dschihadisten. Auch hier nehme der IS eine Führungsrolle ein. Er benutze den Cyberspace nicht mehr nur zu Rekrutierung, Propaganda oder zu Finanztransaktionen. Immer mehr kämen offensive IT-Taktiken zum Tragen. Die Kern-Voraussetzung zur Risikovorsorge seien gut „geölte" Sicherheitsabläufe, und die Hauptzutat hierzu sei eine erstklassige Kommunikation. Gebraucht würden mehr standardisierte Anti-Terrorismus-Maßnahmen, die übergreifend von Unternehmen, Industriesektoren und Ländern übernommen werden könnten, „good practices", deren Anwendung bisher nur bruchstückhaft sei.

Vernetzung

Vernetzte Sicherheit im Baukastensystem ist das Thema von Thomas Stadtmüller, Deutsche Telekom, in der Ausgabe 10-2015 der Zeitschrift GIT, S. 18–20. Auch in der Sicherheitstechnik kämen immer mehr vernetzte Lösungen zum Einsatz, weil sich die Geschäftsprozesse der Kunden so besser unterstützen ließen. Sensoren müssten künftig nicht mehr gedoppelt werden. Es stärke die Abwehrkraft der Sicherheitstechnik, wenn einzelne Bereiche zunehmend miteinander verschmelzen und verschiedene Schutzmechanismen ineinander greifen. Allerdings stiegen parallel dazu auch die Serviceanforderungen der Nutzer.

Videoüberwachung

Anwendungsmöglichkeiten des Komprimierungsstandards **H.265** behandelt GIT in der Ausgabe 10-2015, S. 48/49. Im Vergleich zum gegenwärtig etablierten AVC-Standard solle H.264/H.265 fähig sein, die für hochwertige Videokodierung erforderliche Datenrate um weitere 50 Prozent zu senken. Die Bitratenreduktion solle bei gleichbleibender subjektiver Bildqualität (1080 p) ca. 40 bis 50 Prozent betragen. Zusammenfassend sei festzustellen, dass H.265 das Videomaterial stark verringern könne, während die Wiedergabe ziemlich reibungslos und mit niedriger

Bandbreite verlaufe. Offensichtlich sei H.265 einer der wichtigsten Komprimierungsstandards, der es uns ermögliche, UHD-Lösungen wie 4K oder sogar 8K anzuwenden.

Mit dem **HD-IP-Trend** in der Videoüberwachung befasst sich Dirk Brand, Canon Deutschland, in der Ausgabe 10-2015 der Zeitschrift GIT, S. 58/59. Während die Branche den Blick bereits auf die neueste Ultra-HD(4K)-Technologie richte, spiele die Bildqualität bei der Entscheidung über CCTV-Systeme weiterhin eine zentrale Rolle. Obwohl die aktuelle Ultra HD-Nachfrage gering ausfalle, würden die Vorteile jedoch immer deutlicher. Die von 4K gebotene Bildqualität und Auflösung führen zu klareren Bildern, deutlicheren Zoom-Bildern und einem breiteren Sichtfeld.

Sascha Puppel, Sachverständiger, benennt in der Ausgabe 10-2015 der Zeitschrift GIT, S. 68–71, **typische Fehler bei Videoüberwachungsanlagen** und zeigt, wie man sie vermeidet. Durch die umfangreiche Überarbeitung der Norm DIN EN 50132-7 sei ein umfangreiches Hilfsmittel und Werkzeug für Planer, Errichter und Betreiber geschaffen worden. Die Norm biete einen Leitfaden, um das Erfassen von Leistungsmerkmalen zu erleichtern. Außerdem werde die Auswahl der Kameratechnik auf Basis der definierten Bildqualitäten deutlich vereinfacht. Immer häufiger würden im Rahmen von Begutachtungen sicherheitstechnische Geräte wie Kameras und Netzteile im Außenbereich vorgefunden, die dort aufgrund der Schutzart nach DIN 40050 ungeeignet seien. Teilweise mangele es an der korrekten Montageweise. Durch unzureichend befestigte Kameramasten würden Kamerabilder stark verwackelt. Ein typischer Fehler sei auch der nicht eingehaltene Trennungsabstand zwischen Leitungen und Geräten zu Blitzableitungen sowie der erforderlichen Trennungsabstände zwischen nachrichtentechnischen und Stromversorgungsleitungen. Oftmals finde man unzulässige Brandlasten. In der Praxis sei insbesondere der Schutz von elektronischen Systemen gegen unerwünschte Störeinflüsse von steigender Bedeutung. Elektromagnetische Störungen verursachten in der Praxis meist Bildstörungen, Ausfälle und Falschalarme.

Zutrittskontrolle

Die Zeitschrift WiK (Ausgabe 5-2015, S. 68/69) weist darauf hin, dass ab 12. Juni 2016 die neue Norm **DIN EN 60839-11-1** „Alarmanlagen – Teil 11-1: Elektronische Zutrittskontrollanlagen – Anforderungen an Anlagen und Geräte" die bisher geltende EN 50133-1 ersetzt. Über Änderungen und relevante Vorgaben der Norm informiere unter anderem der vom BHE herausgegebene und vom BHE-Fachausschuss für Zutrittskontrolltechnik erarbeitete aktuelle Praxisratgeber Zutrittssteuerung 2015/2016. In dem Beitrag behandelte Fragen sind: Was beschreibt die neue Norm EN 60839-11-1? Wie werden die vier Sicherheitsgrade definiert? Weshalb wurde die alte Norm abgelöst? Was sind die wesentlichen Neuerungen?

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