Focus on Security

Ausgabe 07, Juli 2017

SECURITAS

Anschläge ... 3
Arbeitsschutz ... 3
Bahnsicherheit ... 3
Brandschutz ... 3
Business Continuity Management (BCM) ... 4
Compliance ... 5
Diebstahl ... 6
Endgerätesicherheit ... 6
Entführung ... 6
Geldautomatensicherheit ... 7
Geldwäsche ... 7
Internet der Dinge (IoT) ... 7
IT-Sicherheit ... 8
IuK-Kriminalität ... 9
Krankenhaussicherheit ... 11
Kritische Infrastrukturen ... 12
Luftverkehrssicherheit ... 13
Maschinensicherheit ... 14
Öffentliche Sicherheit ... 14
Personenschutz ... 15
Produktfälschung ... 15
Rechenzentrumssicherheit ... 15
Resilienz ... 15
Schließsysteme ... 16
Schwarzarbeit ... 16
Sicherheitsarchitektur ... 16
Sicherheitsgewerbe ... 17
Sicherheitsleitsystem ... 17
Sicherheitsmanagement ... 18
Sicherheitstechnik ... 18
Stadionsicherheit ... 19
Terrorismus ... 20
Unternehmensstrafrecht ... 20
Veranstaltungssicherheit ... 20
Vergabeverfahren ... 21
Videoüberwachung ... 21
Zutrittskontrolle ... 23

Anschläge

Deutschlandweit sei es in der letzten Juni-Woche zu Brandanschlägen auf **Signalanlagen der Bahn** gekommen, die zu massiven Verspätungen und Zugausfällen führten, meldet daserste.ndr.de am 28. Juni. Auf der linken Internetplattform „Indymedia" sei dazu ein Selbstbezichtigungsschreiben von vermeintlichen G20-Gegnern veröffentlicht worden.

Arbeitsschutz

Carsten Hippler, Pfannenberg Europe GmbH, stellt in der Ausgabe 6-2017 der Zeitschrift PROTECTOR, S. 42/43, **3D-Coverage für die Leistung von Signalgeräten** vor. Diese neue Planungsmethode erlaube erstmals, die tatsächliche Leistung von Signalgeräten im Raum unter den realen Umgebungsbedingungen sichtbar zu machen. Zudem liefere sie auch sofort eine qualifizierte Empfehlung für die optimalen Signalgeräte sowie deren Positionierung. 3D-Coverage decke dabei bislang nicht erkennbare Leistungsunterschiede auf. Die Signalisierungslösungen verfügten über einen optimierten Schallaustritt, wodurch eine großflächige Ausbreitung des Schalls ermöglicht werde. 3D-Coverage mache die Leistung von Signalgeräten unter Berücksichtigung realer Umgebungsbedingungen für jede Applikation und Alarmierungsart sichtbar und vergleichbar – ob für die Brandalarmierung, Maschinen- und Instrumentensicherheit, Gasalarmierung oder für die generelle Sicherheit am Arbeitsplatz.

In der Ausgabe 6-2017 von GIT Sicherheit, S. 188–191, plädiert Kjersti Rutlin, Honeywell Industrial safety, dafür, die richtige Lautstärke für den **Gehörschutz** zu treffen. Lärm werde von der EU als ein erhebliches Gesundheitsrisiko eingestuft. In der neuen PSA-Verordnung (EU) 2016/425 werde deshalb der Gehörschutz einer deutlich höheren Kategorie zugeordnet. Die Autorin behandelt die Bereitstellung persönlicher Schutzausrüstung, aufsichtsrechtliche Maßnahmen, Schulungen, Passformtest und Motivation sowie verbesserte Möglichkeiten durch neue Technologien.

Bahnsicherheit

Das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) stellt in der Ausgabe 6-2017 von GIT Sicherheit, S. 141, einen hardwarebasierten Schutz für die Kritische Infrastruktur des Schienennetzes vor. Im Zuge einer umfangreichen Modernisierung werde die Leit- und Sicherungstechnik der Deutschen Bahn schrittweise flächendeckend digitalisiert. Durch die vernetzten Steuergeräte würden allerdings neue Angriffspunkte für Hacker geschaffen. Das neue Forschungsprojekt „Haselnuss" entwickele ein Sicherheitssystem, welches gegen Angriffe schützt und die langen Lebenszyklen der Bahninfrastruktur berücksichtige. Dabei arbeiteten DB Netz, das Fraunhofer SIT, Sysgo sowie die TU Darmstadt mit dem Profilbereich CYSEC gemeinsam. Die entwickelte Architektur basiere auf einem **Hardware-Sicherheitsmodul neuester Generation**, dem „Trusted Platform Module/(TPM) 2.0".

Mit **Körperkameras** will die Deutsche Bahn künftig ihr Sicherheitspersonal bei Einsätzen auf großen Bahnhöfen und zu Sport- und Großveranstaltungen ausstatten, meldet die FAZ am 30. Juni. Die Aufzeichnungen würden verschlüsselt gespeichert.

Brandschutz

Wie effektiv **technischer Brandschutz** vor großem Schaden schützt, zeige die Statistik über Löscherfolge des bvfa, heißt es in

GIT.de am 29. Mai. Allein 2016 seien mehr als 80 Prozent aller beim bvfa gemeldeten Löscherfolge durch Sprinkleranlagen mit nur einem oder zwei Sprinklern gelöscht worden. 86 Prozent der gemeldeten Brandfälle seien während der Arbeitszeit passiert. 89 Prozent der eingesetzten Löschanlagen hätten automatisch ausgelöst. 95 Prozent der gemeldeten Löscherfolge seien durch Sprinkleranlagen von weniger als fünf Sprinklerköpfen erzielt worden, mehr als 80 Prozent sogar von nur ein bis zwei Sprinklern.

Den **Fernzugriff auf BMA** thematisiert PROTECTOR in der Ausgabe 6-2017, S. 40/41. Das Handling von Brandmeldesystemen verändere sich zurzeit grundlegend. Bedienung und Steuerung einer BMA fänden nicht mehr unbedingt vor Ort statt, sondern könnten auch am Computer oder per App auf mobilen Endgeräten durchgeführt werden. Möglich mache den Fernzugriff eine IP-fähige Brandmeldezentrale. Nach DIN VDE 0833-1 müsse ein Zugang aus der Ferne vorab schriftlich zwischen Betreiber und Instandhalter festgehalten werden, ebenso wenn Änderungen am System vorgenommen werden. Zudem müsse jeder Zugang auf die BMA automatisch im Ereignisspeicher und durch den Betreiber im Betriebsbuch protokolliert werden. Ein Gesamtpaket aus Brandmeldezentrale, Sonderbrandmeldern, Software und Direktzugriff habe Securiton entwickelt. Das Herzstück sei eine tiefgehende Integration von Sonderbrandmeldetechnik in das Brandmeldesystem. Die Funktion namens Config over Line, die ohne eine zusätzliche Verkabelung auskommt, ermögliche einen vollumfänglichen Fernzugriff. Sonderbrandmelder würden via Interface über die Ringleitung an das Brandmeldesystem angebunden. Im alarmbereiten Zustand könne dann ein Fernzugriff mittels Tunneling-Technologie über die Brandmeldezentrale zu den Sonderbrandmeldern hergestellt werden. Die Ringleitung sei quasi eine Datenautobahn, an die alle Sonderbrandmelder angeschlossen seien. Hierbei könnten wesentlich mehr Informationen an die Brandmeldezentrale übertragen werden, etwa auch Rauchdichte und Temperaturprofile.

Den sicheren Schutz von Chemikalien durch **Sauerstoffreduzierung im Gefahrgutlager** thematisiert GIT Sicherheit in der Auflage 6-2017, S. 154–156. Beim Umgang mit Gefahrstoffen gebe es verschiedene Sicherheitsbestimmungen für Unternehmen, wie die Technischen Regeln für brennbare Flüssigkeiten sowie die Technischen Regeln für Gefahrstoffe. Bei dem Unternehmen Fuchs Lubritech sollte die Vielzahl unterschiedlicher Gefahrstoffe ohne räumliche Trennung in einem Hochregallager zusammen gelagert werden. Das Schutzkonzept basiere daher auf der Kombination von zwei unterschiedlichen Brandschutzsystemen. Ein Teil dieses Konzeptes bestehe aus dem Brandvermeidungssystem Oxyreduct. Da bei einigen Stoffen Entzündungsgrenzen unterhalb einer Konzentration von 13,5 Vol.-% liegen, sei eine durch ein Ansaugrauchmeldesystem angesteuerte CO_2-Löschanlage installiert worden, die im Alarmfall bis zu einer Höhe von etwa fünf Metern einen CO_2-Löschsee aufbaue.

Business Continuity Management (BCM)

Franziska Hain und Annekathrin Enke, PwC Deutschland, befassen sich in Security insight, Ausgabe 3-2017, S. 36/37, mit **BCM als Erfolgsfaktor**. Vor allem der Business Impact Analyse komme im BCM eine erhebliche Bedeutung zu. Hierbei werden kritische Geschäftsprozesse identifiziert und deren Abhängigkeiten eingehend untersucht. Anschließend seien im Zuge der Notfallkonzeption all jene Ressourcen zu erheben, welche seitens der kritischen Prozesse für den Wiederanlauf in den Notbetrieb und die Wiederherstellung des Normalbetriebs benötigt würden. Hierzu zählten neben

Personal, Arbeitsplätzen und IT-Applikationen auch Leistungen vorgelagerter Prozesse, einschließlich externer Dienstleister und Lieferanten. In Bezug auf das Providermanagement seien die identifizierten Dienstleister und Lieferanten hinsichtlich ihrer prozessualen Relevanz zu bewerten und spezifische BCM-Anforderungen zu definieren. Um das BCM eines Zulieferers entsprechend zu bewerten, böte die ISO 22301 einen regulatorischen Maßstab. Ergänzend sei auch der BSI-Standard 100-4 ein Anhaltspunkt für die Absicherung des Geschäftsbetriebs. Die technische Spezifikation ISO 22318 sei ein zusätzlicher Standard für das Supply Chain Continuity Management.

Compliance

Die FAZ berichtet am 17. Juni über das Ergebnis einer Befragung von 480 Geschäftsreisenden durch den Geschäftsreisedienstleister Concur. 15 Prozent der **Fehler in den Abrechnungen** würden absichtlich gemacht. Das BAG habe falsche Abrechnungen als Kündigungsgrund bestätigt. Hinter fünf von sechs zu beanstandenden Abrechnungen stecke keine kriminelle Energie. Die kleinen „illegalen Schummeleien" ergäben für die deutsche Wirtschaft aufsummiert einen Schaden, der in den dreistelligen Millionenbereich reichen dürfte. Ein „Klassiker" sei die fingierte handschriftliche Quittung von Taxifahrten. Die meisten absichtlichen Falschangaben würden bei eintägigen Reisen gemacht werden.

Peter Dehnen, Vereinigung der Aufsichtsräte in Deutschland, beschreibt in der FAZ am 20. Juni, woran es den Corporate Governance-Regeln mangele. Es gebe zahlreiche Regeln, Prozesse und Strukturen, die die Unternehmensführung nicht automatisch verbessern. Dennoch kämen ständig neue Regeln hinzu, so die jüngsten Ergänzungen des Deutschen Corporate Governance Kodex, der inklusive Anlagen nun 20 DIN-A4-Seiten umfasse. Ein Blick ins Ausland zeige, dass die neue Generation von Kodizes meist deutlich kürzer ist. Die Vorgabenflut gehe deutlich zu Lasten von Klarheit und Verständlichkeit. Zugespitzt formuliert würden oft nur noch Checklisten abgehakt, statt zu reflektieren, was zum Wohl des Unternehmens und im Licht eigener ethischer Ansprüche geboten ist. Im deutschen **Corporate Governance Kodex** seien Empfehlungen oder gar Ermahnungen, was das Verhalten einzelner Organmitglieder angeht, nicht vorgesehen gewesen. Das habe sich leider geändert. Aufgrund unscharfer Begriffe wie das „Leitbild des Ehrbaren Kaufmanns" bestehe die Gefahr, dass schon bald rechtliche Zweifelsfragen über mögliche Kodizes-Verstöße zu klären sind. Notwendig sei, sich von dem Wunschdenken zu verabschieden, dass alles regel- und reglementierbar ist. Im zweiten Schritt sollte man trennen zwischen „Corporate" und „Personal Governance". In diesem Bereich brauche man keine Gesetze und Verordnungen, sondern Berufsgrundsätze. Für Aufsichtsräte gebe es sie schon. Die Vereinigung der Aufsichtsräte in Deutschland habe auf zwei Seiten festgehalten, welchen Ansprüchen Aufsichtsräte genügen müssen.

Jacqueline Kessler, Dipl.-Fachfrau Finanz- und Rechnungswesen, stellt in der Ausgabe 3-2017 der Zeitschrift Sicherheitsforum, S. 50–52, die Frage: **Ist der Nutzen von Compliance messbar?** Die Grundlage für die Beantwortung der Frage basiere auf der Wirksamkeit von Compliance im Drei-Ebenen-Konzept nach Rasmussen: die Effektivitäts-, die Effizienz- und die Leistungserstellungsebene, das mit einer vierten Ebene der Gesetzesgrundlage und den Zielwerten des Unternehmens ausgebaut wurde. Effektivitätsebene: Der Nutzen von Compliance wird durch die Verhinderung von dolosen Handlungen generiert. In der Effizienzebene finde aufgrund des Bearbeitens der Prozesse eine Optimierung statt. In der Leistungserstellungsebene resultiere die Rendite von Compliance aus

dem Unterschied des Output-Koeffizienten mit dem Unterschied des Economic Value Added.

Diebstahl

Wie die FAZ am 23. Juni berichtet, wurden am 10. Mai innerhalb weniger Stunden auf den Autobahnen A 4 und A 13 gleich 28 **Lkw** angegriffen, Planen der Sattelauflieger zerschnitten, die Ladeflächen leergeräumt, das Diebesgut weggeschafft – während die Lkw-Fahrer offenbar schliefen. In einem Fall hätten die Kriminellen 117 Fahrräder für 105.000 Euro gestohlen, woanders seien Computermonitore im Wert von 50.000 Euro verschwunden. Mehr als jeder neunte Fall in Europa entfalle auf Deutschland, rechne der internationale Verband Tapa im Jahresbericht vor. Deutschland und Großbritannien seien in Europa die führenden Nationen im Transportdiebstahl. Auf 1,2 Mrd. Euro beziffere Tapa den Wert der Waren, die jedes Jahr in Deutschland erbeutet werden. Der wirkliche volkswirtschaftliche Schaden liege, insbesondere durch Lieferausfälle, fünf- bis achtmal so hoch. Offensichtlich werde der große „Autobahn-Klau" von der organisierten Kriminalität vornehmlich aus Osteuropa gesteuert. Für die Prävention sei im polizeilichen Bereich das LKA Niedersachsen federführend. Ein Präventionskonzept mit Checklisten für Unternehmer, Disponenten und Fahrer sei aufgelegt worden. Dass Laster komplett und dauerhaft gestohlen werden, sei 2015 nach BAG-Angaben 1.605 Mal passiert. Besonders beliebt seien bei den Dieben Laptops und andere Computer, Baumaterial und Werkzeuge, Haushaltsgeräte, Möbel und Kleidung. Als Brennpunkte gelten die Grenzregionen von Sachsen und Brandenburg, das Ruhrgebiet sowie die Umgebung der Großstädte Berlin, Hamburg und Hannover. Die Dresdner Polizei glaube, dass Lasterfahrer, ohne dass sie es mitbekommen, in der Nacht mit Gas betäubt werden. Daher werde jetzt im Verdachtsfall das Blut der Trucker getestet. Ein neues Risiko seien die sozialen Medien. Immer mehr Fahrer nutzten Plattformen und hinterließen so Statusmeldungen über Routen und Aufenthaltsorte, die für Diebe interessant sein könnten.

Während die Zahl der einfachen **Ladendiebstähle** seit zwanzig Jahren kontinuierlich gesunken sei, habe sich die Zahl der schweren Fälle in den zurückliegenden neun Jahren fast verdreifacht, stellt das Kölner Handelsinstitut EHI nach einem Bericht in der FAZ am 28. Juni fest. Nach den Erfahrungen der befragten Händler würden die Diebstähle immer häufiger in organisierter Form erfolgen. Wertmäßig gehe nach Schätzungen des Instituts rund ein Viertel aller Ladendiebstähle auf Banden und organisierte Kriminalität zurück. Das EHI veranschlage die gesamten Inventurdifferenzen auf rund 4 Mrd. Euro im Jahr. Kunden verursachten einen Schaden von fast 2,3 Mrd. Euro, Mitarbeiter einen Schaden von rund 820 Mio. Euro, Servicekräfte einen Schaden von rund 300 Mio. Euro. Die Branche investiere jährlich rund 1,3 Mrd. Euro in Präventions- und Sicherheitsmaßnahmen.

Endgerätesicherheit

Golem.de befasst sich am 2. Juni mit der Diebstahlgefahr. „Siri" könne die mobile Datenfunktion von iPhones auch bei einem gesperrten Gerät abschalten, wenn der Anwender richtig frage. Das könne es Dieben erleichtern, Smartphones unauffindbar zu machen. Zur Umgehung der Sperre reiche ein leicht modifizierter Sprachbefehl.

Entführung

Pascal Michel, SmartRiskSolutions GmbH, befasst sich im Newsletter des ASW am 9. Juni mit der Bedeutung von

Lebensbeweisfragen bei Entführungen. Ziele von Lebensbeweisfragen seien, den Kidnappern zu signalisieren, dass man nur für eine lebende Geisel verhandelt, und dem Entführungsopfer zu zeigen, dass das Unternehmen oder die Familie in Kontakt mit den Entführern steht. Die Fragen sollten so ausgewählt werden, dass sie positive Erinnerungen bei der Geisel erzeugen. Lebensbeweisfragen seien mindestens zweimal erforderlich: zu Beginn der Entführung und unmittelbar vor der Zahlung des Lösegeldes. Bei einem Ultimatum gegen die Geisel oder einer tatsächlichen Misshandlung sei ein erneuter Lebensbeweis erforderlich. Wichtig sei es, niemals für einen Lebensbeweis zu bezahlen. Würde bei jedem Täterkontakt ein Lebensbeweis gefordert, dann würde der Fokus von den Verhandlungen genommen, die Verhandlungsdynamik gestoppt und der Entführer verärgert.

Geldautomatensicherheit

Die Zahl der **Sprengungen von Geldautomaten** (GA) habe sich nach einem Bericht des BKA 2016 mehr als verdoppelt, meldet die FAZ am 30. Juni. Von den rund 58.000 GA in Deutschland seien im Jahr 2016 318 gesprengt worden, mehr als doppelt so viele wie 2015. Zudem seien 2016 rund 400 Fälle angezeigt worden, in denen die Täter mit Schneidwerkzeugen an das Geld in den Automaten kommen wollten. 369 Fälle von Datenklau seien registriert worden, 94 Prozent mehr als im Vorjahr. Bei den Sprengungen seien in Einzelfällen Hunderttausende Euro erbeutet worden. Eine besondere Häufung habe es wieder in Nordrhein-Westfalen und Niedersachsen an der Grenze zu den Niederlanden gegeben. Immerhin 20 der 45 im vergangenen Jahr festgenommenen Verdächtigen seien aus den Niederlanden gekommen. Viele gesprengte Automaten stünden in ländlichen Regionen oder am Stadtrand. Die meisten Taten passierten zwischen zwei und fünf Uhr morgens. So könnten schon nächtliche Sperrungen helfen. Zudem gebe es eine Reihe technischer Möglichkeiten. In den Niederlanden beispielsweise seien die Räume von Geldausgabe und -bestückung getrennt. Zudem könne das für die Sprengung eingeleitete Gas in den GA neutralisiert werden.

Geldwäsche

Das neue Geldwäschegesetz ist am 26. Juni in Kraft getreten, meldet die FAZ am 28. Juni. Die sich daraus ergebenden Pflichten zielten auf zahlreiche Branchen aus Industrie und Handel ab. Allen voran beträfen die Änderungen aber die **Glücksspielbranche.** Künftig sollten sämtliche Veranstalter und Vermittler von Glücksspielen als Verpflichtete gelten und damit den strengen geldwäscherechtlichen Vorgaben unterliegen. Betreiber von Geldspielgeräten in Spielhallen und Gaststätten sollten aber ebenso vom Anwendungsbereich ausgenommen sein wie Pferdewetten von Renn- und Zuchtvereinen nach dem Totalisator-Prinzip. Ausgenommen sei ferner das klassische staatliche Lotto. Kern der geldwäscherechtlichen Sorgfaltspflichten blieben die „Know Your Customer"-Maßnahmen, zu denen das Prüfen der Identität der Geschäftspartner gehöre. Dabei dürften die Anbieter wählen, ob sie sich nach den geldwäscherechtlichen oder den glücksspielregulatorischen Vorgaben des Glücksspielstaatsvertrages richten wollen. Wer als Verpflichteter die Vorgaben nicht beachtet, müsse künftig mit verschärften Sanktionen rechnen.

Internet der Dinge (IoT)

Das Zeitalter des „echten Internets der Dinge" habe das Unternehmen Lupus Electronics eingeläutet, heißt es in der Ausgabe 6-2017 von PROTECTOR, S. 15. Smarte Sensoren

würden von ihrer Ortsgebundenheit befreit, indem sie direkt ans Internet angebunden werden. Eine physische Steuereinheit vor Ort werde dadurch nicht mehr benötigt. Ihre Funktionalität werde vollständig in die Cloud verlegt. Ermöglicht werde das durch das neue **Narrowband-IoT-Netz** von Vodafone. Diese neue Netztechnologie gewährleiste eine stark verbesserte Sendeleistung, was auch die Vernetzung von Sensoren tief unter der Erde möglich mache.

Thomas Snor, NTT Security, behandelt in der Ausgabe 3-2017 der Zeitschrift Sicherheitsforum, S. 24–27, die **Nutzung des IoT durch Botnetze** für DDoS-Angriffe. Das sei erstmals Ende 2016 geschehen. Das beteiligte Botnetz habe aus rund 300.000 IoT-Geräten bestanden, vor allem aus ungesicherten Überwachungskameras, die mit der Schadsoftware Mirai infiziert worden waren. Auf dieser Basis sei dann ein DDoS-Angriff auf DYN, den DNS-Provider von namhaften Content-Anbietern wie Amazon, Spotify oder Netflix erfolgt. Erstmals sei bei einer DDoS-Attacke das Volumen von einem Terabit pro Sekunde überschritten worden. Das IoT wachse nicht nur deutlich stärker als die Zahl klassischer Computer. Es erweise sich in seiner derzeitigen Verfassung als geradezu ideale Plattform für Botnetze. Für die notwendige Sicherung von IoT-Geräten bieten sich drei Ansatzpunkte an: Die Hersteller müssten für eine sinnvolle Grundabsicherung ihrer Systeme sorgen. Die Nutzer sollten an die Sicherheit ihrer Geräte denken. Und die Provider könnten erkennen, ob beispielsweise in Home-Netzen plötzlich unüblicher Traffic entsteht und müssten diesen unterbinden.

IT-Sicherheit

Telekom-Chef Timotheus Höttges wünsche sich ein **internationales Abkommen gegen Cyberattacken**, ähnlich einem Verzicht auf Landminen, meldet golem.de am 2. Juni. Zudem fordere er eine generelle Meldepflicht für Sicherheitslücken, die auch Sicherheitsbehörden umfassen müsse. Eine solche Meldepflicht sei Voraussetzung für eine gesetzliche Verpflichtung für Hard- und Softwarehersteller, Sicherheitsupdates bereitzustellen.

Mit der **Abwehr von Ransomware-Attacken** befasst sich PROTECTOR in der Ausgabe 6-2017, S. 66/67. Netzwerk-Rekorder oder -karten erfassten, katalogisierten und zeichneten den Datenverkehr bei Übertragungsraten von bis zu 100 Gigabit/Sekunde auf. Somit erhalte das IT-Team bei einem Hackerangriff wichtige Informationen, um schnell die Ursache der Probleme zu erkennen und zu lösen. Es existierten Geräte, die sich in bestehende Infrastrukturen einfach und flexibel integrieren lassen und skalierbar sind sowie die Fähigkeit besitzen, bereits bestehende Prozesse, Werkzeuge und Infrastruktur zu verbessern. Das Netzwerk-Monitoring erlaube den Analysten eine genaue Darstellung, was und in welchem Ausmaß passiert ist und welche Daten eventuell gestohlen worden sind.

Mit Erfahrungen der Industrie 4.0 für das **Gesundheitswesen** befasst sich Dr. Klaus Mittelbach, ZVEI, in einem Verlagsspezial „Digitale Medizin" der FAZ am 9. Juni. Medizinische Geräte und Informationssysteme müssten vernetzt werden, um die Versorgungsprozesse zu optimieren. Dadurch entstehe ein Reservoir an Daten aus der realen Versorgung, die mit Hilfe von Big-Data-Analysen ausgewertet und mit anderen Daten aus der Versorgungsforschung und der medizinischen Forschung kombiniert werden. Die Nutzung von personenbezogenen Daten müsse immer auf der ausdrücklichen Zustimmung des Patienten beruhen. Die Gesundheitseinrichtungen müssten mehr Ressourcen in die IT-Sicherheit investieren. Denn ohne sichere IT funktioniere keine Gesundheitsversorgung.

Das Sicherheitsunternehmen **Radar-Services** überwache laufend die gesamte IT-Landschaft und Anwendungen und bewerte alle Ereignisdaten, suche gezielt nach Schwachstellen in Systemen und deren Konfiguration und analysiere den Netzwerkverkehr, schreibt die FAZ am 29. Juni. Aus Millionen von Ereignissen würden diejenigen herauskristallisiert, welche auf einen Missbrauch der Informationstechnik und Anwendungen, auf interne oder externe Angriffe hinweisen. Für seine Kunden analysiere das Unternehmen 514 Petabyte Daten, 61 Bio. Einzelinformationen und 764 Mio. Schwachstelleninformationen im Jahr. Dabei würden durchschnittlich 2,4 Mio. Vorfälle identifiziert. Gemessen an diesen Zahlen unterhalte Radar-Services nach eigener Darstellung das mit Abstand größte Cyberverteidigungszentrum in Europa. Datenmengen würden innerhalb einzelner Risikoerkennungsmodule analysiert. Eine mehrstufige Korrelation – also eine Verknüpfung von verschiedenen Informationen und Ereignissen, nicht nur automatisiert, sondern auch durch Expertenarbeit – komme zum Einsatz. Das Unternehmen werbe mit einer Erkennungsquote von 99,9 Prozent der Sicherheitsprobleme. Im Gegensatz zu anderen Branchenvertretern blieben bei Radar-Services die Daten im Unternehmen. Gegebenenfalls würden Spezialcomputer zum Kunden gebracht und die Probleme an Ort und Stelle behoben.

Restaurants, Hotels, Kaufhäuser: Sie alle sollen ihren Kunden künftig ein **WLAN-Netz** anbieten können, ohne mit rechtlichen Konsequenzen rechnen zu müssen, wenn jemand in ihrem Netz etwas Verbotenes tut, berichtet die FAZ am 1. Juli. Der Bundestag habe eine entsprechende Änderung des Telemediengesetzes beschlossen. Anbieter müssten ihr Wlan weder verschlüsseln, noch bräuchten sie eine vorgeschaltete Seite. Sie müssten auch die Identität ihrer Nutzer nicht überprüfen. Die Neuregelung sei ein wichtiger Baustein der Digitalen Agenda und schaffe Rechtssicherheit.

IuK-Kriminalität

Die Bielefelder Polizei habe einen Verdächtigen festgenommen, der bundesweit als **DDoS-Erpresser** agiert haben soll, meldet heise.de am 2. Juni. Unter dem Pseudonym „ZZB00t" habe er deutsche Unternehmen erpresst.

Viele **Hidden Champions unterschätzen Hackerangriffe**, titelt die FAZ am 8. Juni unter Hinweis auf Warnungen des BfV-Präsidenten Georg Maaßen. Die Sicherheitsbehörden in Deutschland sähen mittelständische Unternehmen schlecht geschützt gegen Hackerangriffe und warnten vor Wirtschaftsspionage von Geheimdiensten aus dem Ausland. Auf einer Internetseite der „Initiative Wirtschaftsschutz" würden Unternehmen Ratschläge gegeben, wie sie sich vor Angriffen schützen und an wen sie sich im Notfall wenden können. In einem passwortgeschützten Bereich erhielten Nutzer auch aktuelle Lageinformationen. Die Behörden müssten kommunikativ noch wesentlich aktiver auf die Wirtschaft zugehen, rät Michael Blaumoser, Sius Consulting. Eine Meldepflicht über Cyberangriffe, wie es sie etwa für Unternehmen der Kritischen Infrastruktur gibt, stehe die Industrie häufig noch skeptisch gegenüber.

Mit der anonymen Gruppierung Shadow Brokers befasst sich der Behörden-Spiegel in der Juni-Ausgabe. Mithilfe eines Exploits sei es Hackern gelungen, den Verschlüsselungstrojaner **WannaCry** so zu programmieren, dass er sich nach einer Initialinfizierung mittels einer schadhaften E-Mail selbstständig innerhalb eines Netzwerks auf Windows-Rechnern verbreiten konnte. Wer hinter WannaCry steckt, sei bisher unklar. Zunächst sei eine bekannte Hackergruppe aus Nordkorea verdächtigt worden. Eine linguistische Analyse des Programmcodes deute aber auf einen Ursprung in Südchina hin. Es spreche Einiges dafür, dass auch beim Fall Shadow Brokers Innentäter zumindest eine Rolle

spielten. Der Rechtsvorstand von Microsoft habe gefordert, dass Sicherheitslücken an die Softwarehersteller gemeldet werden, statt sie für geheimdienstliche Zwecke auszunutzen. Durch WannaCry seien zwar innerhalb weniger Tage mehr als 230.000 Computer in über 150 Ländern befallen worden. Im Verhältnis zum Umfang des Angriffs sei der Erlös für die Urheber aber gering ausgefallen. Insgesamt sollen nur etwa 0,1 Prozent der Betroffenen das geforderte Lösegeld gezahlt haben. Experten zufolge hätten mehrere glückliche Umstände die weitreichendere Verbreitung von WannaCry verhindert: Erstens sei die ausgenutzte Sicherheitslücke schon einige Wochen vor ihrer Veröffentlichung durch die Shadow Brokers von Microsoft geschlossen worden. Betroffen gewesen seien also nur ungepatchte Systeme. Und anders als zunächst angenommen seien einer Analyse der IT-Sicherheitsfirma Kaspersky zufolge fast nur Windows-7-Rechner betroffen gewesen. Drittens habe ein Sicherheitsforscher zufällig einen Stoppmechanismus, einen sogenannten Kill Switch, aktiviert, den die Hacker vermutlich als Notausschalter vorgesehen hatten. Wie Gerhard Schabhüser und Holger Junker vom BSI in der FAZ am 30. Juni erklären, habe die Gruppe Shadow Brokers digitale Angriffswerkzeuge einer Einheit für Cyberkriegsführung der NSA genutzt. Die klingenden Codenamen der Programme lauteten: Danderspiritz, Oddjob, Fuzzbunch, Darkpulsar, Eternalsynergy, Eternalromance, Explodingscan, Ewoldfrenzy und Eternalblue. Die NSA habe die „Exploits" jahrelang bewusst geheim gehalten. Die **„fehlende Patchkultur"** sei eine der größeren Baustellen des BSI. Je stärker es sich um kritische Geschäftsprozesse handelt, desto schwieriger sei der Freigabeprozess eines Patches innerhalb eines Unternehmens. Wenn der nicht mit allen Anwendungen kompatibel sei, stehe der Betrieb im schlimmsten Fall still.

Auf über 250 Mio. Rechnern weltweit wütet derzeit eine gefährliche Adware – rund in jedem zehnten deutschen Unternehmensnetzwerk sei mindestens ein infizierter Rechner aktiv, berichtet heise.de am 2. Juni. Der **Fireball** getaufte Schädling komme im Bundle mit anderer Software wie „Deal Wifi", „Mustang Browser", „Soso Deskop" oder „FVP Imageviewer" auf den Rechner. Gefährlich werde es, weil Fireball laut Security-Unternehmen Check Point einen beliebigen Code auf dem Rechner ausführen und so auch Malware nachladen könne. Es handele sich also faktisch um eine Backdoor – und es beruhige wenig, dass der dazugehörige Schlüssel in der Hand einer Marketingfirma aus Peking liege. Das Programm lasse sich aber über die Systemsteuerung deinstallieren. Check Point empfehle zudem, die Browser auf Standardeinstellungen zurückzusetzen und sowohl einen Malware- als auch einen Adware-Scanner auf das System anzusetzen.

Nach einem Bericht von silicon.de am 12. Juni hat das BKA zusammen mit der Zentralstelle zur Bekämpfung der Internetkriminalität bei der Staatsanwaltschaft Frankfurt a. M. den mutmaßlichen Betreiber einer **deutschsprachigen Darknet-Plattform** festgenommen. Außerdem hätten die Server lokalisiert und beschlagnahmt werden können. Über die Plattform soll auch die beim Amoklauf in München im Juli 2016 verwendete Waffe erworben worden sein. Dem 30-jährigen Tatverdächtigen werde vorgeworfen, seit März 2013 als Administrator eine deutschsprachige Darknet-Plattform betrieben zu haben. Auf dieser sollen zuletzt über 20.000 Mitglieder registriert gewesen sein.

Mit einer **„Mouse-over-Malware"** befasst sich Peter Marwan am 12. Juni in silicon.de. Malwarebytes und Trend Micro hätten entsprechenden Schadcode analysiert. Er werde über Office 365 verteilt und finde sich da bevorzugt in Powerpoint-Dateien. Allerdings sei die Malware für eine erfolgreiche Infektion derzeit noch auf Mithilfe der Opfer angewiesen. Experten der IT-Sicherheitsanbieter Malwarebytes und Trend Micro hätten sich

mit einer neuen Malware beschäftigt, die sich selbsttätig auf dem PC eines Opfers installieren könne. Es reiche aus, wenn der Nutzer mit dem Mauszeiger über einen entsprechend präparierten Link in einer Microsoft-Office-Datei fährt.

VEKO Online berichtet in der Juni-Ausgabe über einen Cyberangriff auf Netzwerke von Banken mit im Speicher versteckter Malware. Die **ATMitch-Malware** werde aus der Ferne über die bankinterne Fernwartung auf den Geldautomaten der Bank gespielt und dort ausgeführt. Sobald ATMitch installiert ist und in Verbindung mit einem Geldautomaten steht, kommuniziere die Malware mit diesem wie eine legitime Software. Angreifer könnten so bestimmte Befehle ausführen und beispielsweise Informationen über die Anzahl der im Automaten enthaltenen Geldscheine sammeln. Zudem könnten die Cyberkriminellen per Klick den Befehl zur Ausgabe eines beliebigen Geldbetrags geben.

Etwas mehr als einen Monat nach der Wannacry-Attacke habe **abermals ein Ransomware-Angriff** viele Unternehmen in Europa unter Druck gesetzt, berichtet die FAZ am 28. Juni. Besonders betroffen sei nach ersten Erkenntnissen die Ukraine. Die Lösegeldforderung betrage 300 Dollar je infiziertem System. Einhundertfünfzig Länder seien von der Attacke betroffen, 75.000 Computer lahmgelegt. Am 29. Juni berichtet die Zeitung, nach einer Analyse der Strategieberatung Oliver Wyman drohe der Logistikbranche rund um die Welt bis 2020 ein Schaden von rund 6 Mrd. Euro durch Cyberkriminalität. Nach Daten von IBM hätten 70 Prozent der betroffenen Unternehmen das Lösegeld bezahlt. Die Hälfte von ihnen habe mehr als 10.000 Dollar, ein Fünftel sogar mehr als 40.000 gezahlt. Nach einem Bericht des GDV koste es deutsche Unternehmen im Durchschnitt 609.000 Euro, Schäden durch die Verletzung von Betriebsgeheimnissen auszugleichen. Durch Cybererpressungen entstünde im Schnitt ein Schaden von 337.000 Euro.

Das BSI habe Funktionsträger in Wirtschaft und Verwaltung vor Angriffen auf privat genutzte E-Mail-Konten gewarnt, meldet silicon.de am 26. Juni. Demnach versuchten Angreifer vermehrt, mittels sogenannter **Spear-Phishing-E-Mails** – E-Mails, die gezielt an die persönlichen E-Mail-Adressen sorgfältig ausgesuchter Personen verschickt werden – Zugriff auf private E-Mail-Konten zu erlangen. Die Angreifer würden entweder vorgeben, es seien „Auffälligkeiten bei der Nutzung des Postfachs" beobachtet worden oder es seien neue Sicherheitsfunktionen verfügbar. In beiden Fällen sollten die Empfänger verleitet werden, einen Link anzuklicken und auf der verlinkten Website Nutzername und Passwort einzugeben. Am häufigsten seien diese Versuche vom BSI aktuell bei Konten bei Yahoo und Gmail verwendet worden.

Krankenhaussicherheit

Auswirkungen von **Cyberangriffen auf Krankenhäuser** behandelt PROTECTOR in der Ausgabe 6-2017, S. 20–22. Die durchgängige Digitalisierung der Arbeitsabläufe im medizinischen Bereich erzeuge eine große Menge personenbezogener Daten, deren Veröffentlichung negative Auswirkungen hätte. Gleichzeitig bedeute dies, dass unterschiedliche Systeme miteinander kommunizieren, von Abrechnungsstellen über Labore bis hin zu Datenbanken. Ähnliches gelte für die Medizintechnik als solche, in der die Digitalisierung zu einem beinahe ständigen Datenaustausch zwischen einzelnen Geräten und Systemen geführt habe. Die relativ offenen IT-Systeme in Krankenhäusern ermöglichten daher auch Angriffe, die letztlich auch die Steuerungen medizinischer und anderer Geräte treffen können. Die umfangreiche Vernetzung in Krankenhäusern lasse ein in sich geschlossenes System so gut wie nicht zu. Das größte Problem aber sei der Mensch und sein Nutzerverhalten. Derzeit existierten – im Unterschied etwa zu den detaillierten

Vorgaben zum Brandschutz – noch wenige rechtliche Verpflichtungen zur Absicherung des Gesundheitswesens. Bislang sei noch unklar, wie viele der rund 2.000 Krankenhäuser letztlich zu den Kritischen Infrastrukturen zählen werden.

Albert Schöppl, Forcepoint in CEUR, zeigt in der Ausgabe 3-2017 von Security insight, S. 20/21, wie man Mitarbeiter und Daten im Gesundheitswesen vor Cyberkriminalität schützt. Ein neuer Trend sei es, **auf Basis von Patienteninformationen Rechnungen** zu stellen. Mittels eines im Internet legal erhältlichen Tools für Penetrationstests ließen sich automatisiert Daten aus dem Krankenhausnetzwerk schleusen. Dazu sei es nur nötig, sich Zugang zu einem unbeaufsichtigten Rechner zu verschaffen und das Tool an der LAN-Verbindung einzustecken. Einmal im Unternehmensnetzwerk könne der Datendieb auf Belegzeiten, Operations- und Behandlungskosten zugreifen, um eine glaubwürdige Rechnung zu erstellen. Wichtig sei es auch, das Bewusstsein für die Gefahren von innen zu schärfen. Einem Datendiebstahl oder Datenverlust gingen immer verdächtige oder auffällige Verhaltensweisen voraus. Mit den richtigen Software-Tools ließen sich illegale oder gefährdende Tätigkeiten im Firmennetzwerk erkennen, vorhersagen und verhindern. Da die Vorgehensweise sowohl bei kriminellen Machenschaften als auch bei gefährdenden Handlungen bestimmten Mustern folge, könne durch User Behavior Analytics ein **automatisches Frühwarnsystem** eingerichtet werden. Überschreite ein User einen bestimmten Wert (Score), werde das Verhalten genauer unter die Lupe genommen. Die Informationen zum Nutzerverhalten würden zunächst anonymisiert erfasst. Es müsse auch verhindert werden, dass sensible Daten und Informationen das Unternehmensnetzwerk verlassen. Eine Data Leakage Prevention erkenne automatisch und mit hoher Trefferquote sensiblen Content und hindere diesen am Verlassen des Netzwerks.

Das **Türsystem eines Krankenhauses** müsse viele unterschiedliche Voraussetzungen erfüllen, heißt es in Security insight, Ausgabe 3-2017, S. 24/25. Nicht jeder Besucher solle Zugang zu allen Bereichen haben, aber alle Zugänge müssten barrierefrei sein. Die Mitarbeiter sollten unkompliziert auf ihre Stationen kommen und es müsse für alle eine schnelle Flucht ins Freie gewährleistet sein. Ein wesentlicher Bestandteil des Türsystems seien die Fluchttürsteuerterminals. Durch das Drücken des Nottasters werde die Rettungswegtür zum Öffnen freigegeben. Türschließer sorgten insbesondere bei Brandschutztüren dafür, dass eine Tür von allein zuverlässig und sicher schließt. Türschließer hätten aber den Nachteil, dass mehr Kraft benötigt wird, um die Tür zu öffnen. In einem Krankenhaus sei Barrierefreiheit eine Grundvoraussetzung. Assa Abloy habe deshalb den Türschließer DC700 mit der Cam-Motion-Technologie entwickelt. Dadurch werde der Gegendruck des Türschließers deutlich reduziert.

Kritische Infrastrukturen

Die Bundesregierung habe am 31. Mai eine Änderung der VO zur Bestimmung Kritischer Infrastrukturen auf den Weg gebracht, meldet heise.de am 2. Juni. Geregelt werde, welche Firmen aus den Sektoren Transport, Verkehr, Finanzen, Versicherungen und Gesundheit unter die Vorgaben des IT-Sicherheitsgesetzes fallen. Betroffen seien 918 „Kritische Infrastrukturen". Die Betreiber würden verpflichtet, dem BSI innerhalb von sechs Monaten eine zentrale Kontaktstelle zu benennen und der Behörde innerhalb von zwei Jahren nachzuweisen, einen Mindeststandard an IT-Sicherheit einzuhalten.

Mit dem **„zweiten Korb" der Verordnung zur Bestimmung Kritischer Infrastrukturen** (BSI-KritisV) befasst sich auch die Juni-Ausgabe des Behörden-Spiegel. Grundlage für die Identifizierung als Kritische

Infrastruktur seien sektorenspezifische Schwellenwerte. Grundlage für die Schwellenwerte seien Überlegungen, ab welcher Größenordnung ein Ausfall oder eine erhebliche Beeinträchtigung der Geschäftsprozesse eine nicht ohne Weiteres zu lösende Versorgungskrise auslösen könnte. Für die Sektoren des zweiten Korbes sollten laut Referentenentwurf z. B. Krankenhäuser ab 30.000 stationären Fällen, Autorisierungssysteme für Bargeldabhebungen ab 15 Mio. Transaktionen und Flughäfen ab 20 Mio. Passagieren oder 27.700 Tonnen im Jahr als kritisch gelten. Erheblich und damit melderelevant sei eine Störung den Kriterien des BSI zufolge, wenn sie zu Beeinträchtigungen der Geschäftsprozesse führt oder ein außergewöhnlicher technischer Defekt oder unbekannter Typ von Cyberangriff zugrunde liege. Die zweite wesentliche Pflicht sei die Umsetzung von IT-Sicherheitsmaßnahmen nach dem Stand der Technik. Die Einhaltung solle alle zwei Jahre überprüft werden.

Allgemeine Mindestanforderungen an die IT-Sicherheit würden in einschlägigen Standards wie dem IT-Grundschutz des BSI oder dem internationalen ISO/IEC 27001 festgehalten. Schlankere Vorgabenkataloge, die sich möglichst direkt im Unternehmen umsetzen und leicht überprüfen lassen, würden deshalb durch branchenspezifische Sicherheitsstandards (B3S) ermöglicht. B3S könnten von KRITIS-Betreibern und Branchenverbänden in Kooperation mit BBK und BSI erarbeitet werden. Als Plattform für die Aussprache über B3S dienten Branchenarbeitskreise des UP KRITIS. Als Konsequenz, insbesondere des weltweiten Angriffs mit dem Schadprogramm WannaCry, wolle der Bundesinnenminister eine Ausweitung des IT-Sicherheitsgesetzes anstoßen. Ziel sei es, auch große Industrieunternehmen als Kritische Infrastrukturen einzuordnen, um deren IT-Systeme in Zukunft besser schützen zu können.

Luftverkehrssicherheit

Juliane Holtz, BDSW, weist in der Ausgabe 3-2017 von Security insight, S. 50, darauf hin, dass unter den vom BMBF seit 2007 mit über 500 Mio. Euro geförderten 260 Verbundprojekten im Rahmen des **Forschungsprogramms für die zivile Sicherheit** mehrere die Luftverkehrs- und Flughafensicherheit betreffen: so die Entwicklung eines neuen Körperscanners R&S QPS 200. Wegweisend seien die beiden Verbundvorhaben TERATOM und QPASS gewesen. Dabei habe im Vordergrund die Erarbeitung von Methoden und Algorithmen zur dreidimensionalen Mustersuche und automatischen Objekterkennung gestanden. Ziel des Verbundprojekts ChemAir sei die Entwicklung einer luftfrachtspezifischen Kontrolltechnik zur Detektion von chemischen Gefahrstoffen gewesen. Und in dem Projekt IRLDEX sei ein Verfahren für eine berührungslose Nah- und Ferndetektion von Explosivstoffen erarbeitet worden.

Die Bedeutung der Sicherheitsforschung thematisiert Juliane Holtz, BDSW, auch in DSD 2-2017, S. 45/46. Sie skizziert die beiden vom BMBF geförderten Verbundvorhaben **TERATOM und MoQPASS, ChemAir und IRLDEX**. Ergebnis des ChemAir-Projekts sei ein „Flussfeld-Temperaturgradienten-Gaschromatograph" gewesen. Da auch Explosivstoffe Ausgasungen aufweisen, könne mit diesem Nachweisverfahren ein einziges Sprengstoffmolekül unter einer Billion Moleküle erkannt werden. Während andere Analysen bis zu 30 Minuten dauerten, gelängen Messungen durch diese Technologie im Minutentakt, was zu einem klaren Vorteil im Bereich der zeitsensiblen Luftfrachtkontrolle führe. Durch das im Projekt IRLDEX entwickelte Detektionsverfahren könnten geringste Spuren von Explosivstoffen, die beispielsweise durch Fingerabdrücke auf der Oberfläche von Gegenständen hinterlassen werden, erkannt werden. Das herrenlose Gepäckstück

könne aus einigen Metern Entfernung mit Wärmestrahlung beleuchtet werden. Bisheriges Projektergebnis sei ein Demonstrator, der bereits nach einer Sekunde die korrekte Bezeichnung der Substanz anzeigt, auf die die Infrarotlaserquelle gerichtet war. Der Abgleich mit einer Datenbank, in der Infrarotspektren zahlreicher Substanzen hinterlegt sind, mache es möglich, Ammoniumnitrat, TNT usw. zu erkennen. Nachgewiesen werden könne bereits im Mikrogrammbereich.

In Heft 2-2017 des DSD, S. 48, werden die je nach Flughafen unterschiedlichen **Sicherheitsgebühren für 2017** aufgelistet. Die Spanne reicht von 4,33 Euro (Hahn), 4,55 Euro (Memmingen) und 4,86 Euro (Dortmund) bis 19,66 Euro (heruntergesetzt gemäß Anlage zur LuftSiGebV auf 10,00 Euro).

Maschinensicherheit

Ein **Feldbusmodul für sicherheitstechnische Installationen** stellen Michael Greiner und Alexander Hornauer in GIT Sicherheit in der Ausgabe 6-2017, S. 180/181, vor. Fragen der Sicherheit würden in der Automatisierungstechnik einen hohen Stellenwert genießen. Murrelektronik biete mit dem Feldbusmodul MVK Metall Safety eine Lösung für sicherheitstechnische Installationen. Damit könnten höchste Standards erreicht werden: Safety Integrity Level 3 (nach IEWC 61508 und IEC 62061) und Performance Level e (nach EN ISO 13849-1). Von MVK Metall Safety gebe es für den applikationsgerechten Einsatz zwei Varianten: ein reines Eingangsmodul und ein gemischtes Modul mit Ein- und Ausgängen. Da der Schlüssel zu Wirtschaftlichkeit in der Maschinen- und Anlageninstallation vor allem darin liege, ungeplante Stillstandzeiten zu reduzieren, seien die ausgeprägten Diagnosefunktionalitäten ein wesentlicher Pluspunkt von MVK Metall Safety.

Um ein sicherheitstechnisches „Röntgenbild" ihrer Maschinen und Anlagen zu erhalten, nutzen immer mehr Betreiber das **Know-how von Sick zu Komplettlösungen** als akkreditierte Inspektionsstelle für Sicherheitstechnik, davon sind Harald Schmidt und Olaf Zbikowski, Sick AG, überzeugt (GIT Sicherheit, Ausgabe 6-2017, S. 182–185). Sick sei von der Datech als Inspektionsstelle nach IEC bzw. EN ISO 17020 akkreditiert. Ihre mehr als 150 geschulten Experten für Maschinensicherheit in über 80 Ländern könnten sicherheitstechnische Prüfungen und Abnahmen neuer oder modernisierter Maschinen und Anlagen durchführen. Die Autoren behandeln mangelhafte Schutzfunktionen, die oft fehlerhafte Auswahl von Schutzeinrichtungen, die Maschinensicherheitsbewertung, die eingehende Prüfung von Funktion und Verdrahtung bei der Inspektion und Sicherheits-Komplettlösungen.

Öffentliche Sicherheit

Lvz.de berichtet am 14. Juni über Ergebnisse der Frühjahrskonferenz der Innenminister. Ein **„Musterpolizeigesetz"** sollte künftig wieder deutschlandweit für einheitliche Standards sorgen. Auf der Grundlage eines neuen Analysemodells des BKA sollten Gefährder künftig besser eingestuft werden können. Um die Sicherheit bei Großveranstaltungen zu erhöhen, soll die Zugangsberechtigung etwa für Aufbauhelfer künftig mit einem Lichtbild versehen werden. Einig sei man sich auch, dass Ermittler auf Messenger-Dienste wie WhatsApp zur Verfolgung schwerer Straftaten zugreifen können müssen. Ergebnisse von DNA-Analysen sollten künftig auf die Feststellung des Alters, der Hautfarbe, der Augenfarbe und der Herkunft erweitert werden.

Personenschutz

Aufklärung 2.0 – Personenschutz im Wandel – titelt Security insight in der Ausgabe 3-2017, S. 51. Für die früher als „erweiterter Personenschutz" bezeichnete Aufklärung benötige man spezielle Strukturen, Ausrüstung, Fachwissen, geeignetes Personal und klare Anweisungen. Das Erstellen einer hierfür notwendigen Dienstanweisung sei nur einer von etwa 40 Punkten in den vier Planungsgruppen organisatorische Vorbereitung, materielle Planung, Modus Operandi der „Aufklärer" und Vorfallbearbeitung einschließlich Definition der Meldeschwelle.

Steffen Kunze, Trumpf GmbH + Co. KG, geht in Security insight, Ausgabe 3-2017, S. 52/53 auf die **Sensibilisierung der Schutzperson** ein. Es gebe verschiedene Argumente, um potenzielle Schutzpersonen vom Personenschutz zu überzeugen: Nutzwert als Dienstleister und Teil des BCM, Einbindung in die Unternehmensstrategie, Verantwortung auch für das Unterlassen und mögliche Haftungsverstöße durch Organisationsverschulden. Im Übrigen gelte: Die Schutzperson prägt das Personenschutzteam – und nicht umgekehrt.

Produktfälschung

Produktfälscher machen weltweit einen Gewinn von 461 Mrd. Euro jährlich. Darauf wiesen Experten vom Forum Vernetzte Sicherheit nach einem Bericht in der Juni-Ausgabe des Behörden-Spiegel hin. Geschmuggelt werde alles, was billig zu produzieren, teuer zu verkaufen und einfach zu transportieren ist. Wie René Matschke vom Hamburger Zollfahndungsamt mitteilte, würden unter anderem die Schiffsmanifeste mittels EDV-Anwendungen und zöllnerischer Erfahrung ausgewertet. Anschließend erfolge eine Einteilung jedes Einzelfalls anhand eines Ampelsystems. Faktoren, anhand derer die Risikobewertung erfolge, seien zum Beispiel das Ursprungsland der Ware, der Abgangshafen sowie eine niedrige Qualität der angemeldeten Waren.

Rechenzentrumssicherheit

Sven Östlund, Siemens Schweiz Building Technologies, stellt in der Ausgabe 3-2017 der Zeitschrift Sicherheitsforum das **Datacenter Infrastructure Management** (DCIM) mit Mehrwert für Colocation-Rechenzentren vor (S. 31–33). Colocation-Rechenzentren würden immer populärer. Gleichzeitig forderten Unternehmen immer höhere Betriebseffizienz, gestützt durch Service-Level-Agreements, Transparenz und Reporting. DCIM-Tools böten Asset-Management, zentrales Rechenzentrumsmanagement, verbesserte Prognosemethoden und einen erweiterten Lebenszyklus. Die Integration heterogener Business-Systeme bedeute auch, dass die Systemkapazität von Colocation-Rechenzentren skalierbar sein und auf globaler Basis effizient verwaltet und bereitgestellt werden muss.

Resilienz

Security insight geht in der Ausgabe 3-2017, S. 38/39, auf den FM **Global Resilience Index 2017** ein. Es sei das erste datenbasierte und interaktive Tool, das 130 Länder und Territorien nach der Resilienz ihrer Unternehmen gegenüber unvorhersehbaren Ereignissen einstuft. Der Index bestehe aus drei Faktoren: Wirtschaft, Risikoqualität und Lieferkette, die sich in weitere Treiber unterteilen. Der Index 2017 sei um weitere drei Treiber erweitert worden: inhärentes Cyberrisiko, Grad der Urbanisierung (stellvertretend für Belastungen, die durch Naturkatastrophen verschärft würden) und Transparenz

der Lieferkette. Im Ranking liege die Schweiz auf Platz 1, gefolgt von Luxemburg, Schweden, Österreich und Deutschland. Der Index beruhe auf geprüften Daten von Quellen wie dem Internationalen Währungsfonds, der Weltbank, dem Weltwirtschaftsforum, der US Energy Information Administration, den Vereinten Nationen, dem Freedom House und der FM Global-Datenbank RiskMark mit mehr als 100.000 versicherten Standorten.

Schließsysteme

Mechatronische Schließsysteme für Kritische Infrastrukturen behandelt PROTECTOR in der Ausgabe 6-2017, S. 34/35. Die Absicherungen müssten so beschaffen sein, dass ein hohes Sicherheitsniveau gewährleistet ist, gleichzeitig aber die Zugänge und Berechtigungen für Mitarbeiter so unkompliziert wie möglich gestaltet werden. Ein mechatronisches Schließsystem vereine beide Bedürfnisse. Eine elektromechanische Lösung verbinde hoch entwickelte Mikroelektronik mit einer intelligenten Softwarelösung in einem sicheren mechatronischen Schließzylindersystem. Dies gewährleiste die größtmögliche Flexibilität bei der Berechtigungsvergabe sowie höchste Sicherheitsstandards. Ein mechatronisches System erspare die schwierige Schlüssel-Organisation, denn die Verwaltung könne an zentraler Stelle dezentral Berechtigungen vergeben. Und ein verlorener Schlüssel stelle kein Sicherheitsrisiko mehr dar. Wetterfeste Materialien und robuste, vor Vandalismus geschützte Wandprogrammiergeräte hielten auch extremen Bedingungen stand.

Petra Eisenbeis-Trinkle, Kaba GmbH, stellt in der Ausgabe 6-2017 der Zeitschrift PROTECTOR, S. 36/37, das elektronische **Zutrittssystem Matrix** von Dormakaba vor. Die Software überzeuge durch ihre Einfachheit. Sie laufe komplett im Browser und könne von mehreren Clients aufgerufen werden. Nach dem Prinzip „Access on Card" seien die jeweiligen Berechtigungen der Mitarbeiter (des Städtischen Krankenhauses Heinsberg) auf ihrem Ausweismedium gespeichert. An den Schiebetüren des Krankenhauses seien Online-Leser und an Brandschutz- und Schallschutztüren die Matrix-Air-Beschläge montiert worden. Alle Mitarbeiter hätten neue Mifare Desfire Chips als Schlüsselanhänger erhalten. An zwei Aufladestationen holten sie sich regelmäßig ihre jeweiligen Zutrittsberechtigungen, bevor sie an den Türen buchen. Alle Mitarbeiter seien in das System eingebunden, auch die Chefärzte.

Schwarzarbeit

Mehr Schäden aus Schwarzarbeit, titelt die FAZ am 8. Juni. In einem vom Bundeskabinett verabschiedeten Bericht werde der im Rahmen von Ermittlungen aufgedeckte Schaden aus **Schwarzarbeit** für 2016 auf 875 Mio. Euro beziffert, gut 50 Mio. Euro mehr als 2014. Bestimmte Tätergruppen würden immer häufiger in organisierten Strukturen über die Grenzen Deutschlands hinweg arbeiten. Schwerpunkte für Schwarzarbeit seien unter anderen das Baugewerbe, Gaststätten und Hotels, Personenbeförderung, Gebäudereinigung und Fleischwirtschaft.

Sicherheitsarchitektur

Peter Niggl, Security insight, befasst sich in der Ausgabe 3-2017, S. 10–13, mit der **Sicherheitsarchitektur in Deutschland**. Wenn man schon die Geschicke Europas bei der Neuausrichtung der Sicherheitsarchitektur im Auge habe, sei es unverständlich, warum man sich der Praxis fast aller EU-Staaten nicht anschließt, die Aufsicht über die privaten Sicherheitsdienstleister vom Innenministerium oder Justizministerium ausüben

zu lassen. Niggl verweist weiterhin auf die Forderung des ehemaligen BKA-Präsidenten Jörg Ziercke, endlich auch einmal über eine „strategische Partnerschaft" von staatlichen Sicherheitsorganen und der privaten Sicherheitswirtschaft zu diskutieren.

Sicherheitsgewerbe

Neue **Herausforderungen für das Sicherheitsgewerbe** im Gewerberecht und im Recht der Arbeitnehmerüberlassung sieht Dr. Harald Olschok, BDSW (PROTECTOR, Ausgabe 6-2017, S. 68/69). Die Bearbeitungszeit zwischen der Meldung einer Bewachungsperson an die Ordnungsbehörde und dem Abschluss der Zuverlässigkeitsüberprüfung betrage in vielen Kommunen acht bis zehn Wochen. Dies sei für seriöse und rechtskonform arbeitende Sicherheitsunternehmen viel zu lang. Eine einfache, rechtskonforme Maßnahme bestünde darin, dass bereits bei der Anmeldung einer Person zur Unterrichtung bei einer IHK die zuständige Ordnungsbehörde die Zuverlässigkeitsprüfung einleite. Die rechtlichen Risiken des am 1. April in Kraft getretenen Arbeitnehmerüberlassungsrechts seien vielen Kunden und auch Sicherheitsunternehmen noch nicht ausreichend bekannt. Bei der Durchführung von Sicherheitsdienstleistungen bestünde – je nach Auftragsgestaltung – die Gefahr, den Bereich der Arbeitnehmerüberlassung (AÜ) zu tangieren, vor allem dann, wenn zusätzliche Dienstleistungen neben der eigentlichen Sicherheitstätigkeit erbracht und/oder keine organisatorischen Vorkehrungen getroffen wurden. Mitarbeiter des Kunden dürften keine Weisungsbefugnis gegenüber dem Sicherheitsmitarbeiter ausüben. Diese dürften auch nicht in den Kundenbetrieb eingegliedert werden. Es müssten Ansprechpartner beim Sicherheitsunternehmen vorhanden sein, die gegenüber den eingesetzten Sicherheitskräften weisungsbefugt sind. Die Haftungsverteilung und die Zusammenarbeit zwischen den Mitarbeitern des Kunden und des Dienstleisters müssten geregelt werden. In der Praxis gebe es auch Aufträge, die eine AÜ darstellten, weil zusätzliche Aufgaben vereinbart wurden, zum Beispiel die Organisation der Poststelle. Diese Aufträge müssten als solche gekennzeichnet sein und könnten nur dann wahrgenommen werden, wenn eine AÜ-Erlaubnis vorliegt. Das AÜG sei nicht anwendbar zwischen Arbeitgebern in der Sicherheitswirtschaft, wenn der Arbeitnehmer nicht zum Zweck der Überlassung eingestellt und beschäftigt wird und der Personalbedarf des Entleihers nicht auf andere Weise kurzfristig gedeckt werden kann.

Die Staatsanwaltschaft Kassel habe beim LG Kassel Anklage gegen den Chef des **insolventen Sicherheitsdienstes 24** wegen des Verdachts des Vorenthaltens und Veruntreuens von Arbeitsentgelt sowie Steuerhinterziehung und Fälschung beweiserheblicher Daten erhoben, meldet hna.de am 9. Juni. Die Ermittlungsbehörden schätzten, dass rund 4,8 Mio. Euro Steuern hinterzogen wurden. Allein bei der Sozialversicherung soll ein Schaden von rund 3,3 Mio. Euro entstanden sein. Dem Beschuldigten werde vorgeworfen, tatsächliche Arbeitsverhältnisse und deren Umfang mithilfe von Scheinrechnungen vermeintlicher Subunternehmer verschleiert zu haben. Außerdem soll er Arbeitnehmer veranlasst haben, Rechnungen zu schreiben, um deren Selbstständigkeit vorzutäuschen.

Sicherheitsleitsystem

Mit der **Integration von Sicherheitstechnik in das Leitsystem** befasst sich Dipl.-Ing. ETH Reto Felix, AWK Group, in der Ausgabe 3-2017 der Zeitschrift Sicherheitsforum, S. 18–21. Der Weg zur optimalen Integration führe über das systematische und umfassende Management von Anforderungen der am System beteiligten Organisationen und Personen. Wichtig sei, die Anforderungen

möglichst komplett und lösungsneutral zu definieren. Sie würden von drei Seiten an das System gestellt. Dabei hätten Nutzer, Betreiber und Management jeweils eine unterschiedliche Sicht auf das System. Die Kunst des Anforderungsmanagements sei es, Anforderungskonflikte durch optimale Kompromisse zu lösen. Als Nutzen und Kosten bestimmende Faktoren bezeichnet und beschreibt der Autor die Betreibbarkeit, Betriebsabläufe, die Nachvollziehbarkeit, das Risiko, Synergien, die Technologie, Verfügbarkeit und Vision.

Sicherheitsmanagement

Almut Eger, 4 Management 2 Security GmbH, und Jürg Sager, IMS Integrierte Managementsysteme AG, behandeln in der Ausgabe 3-2017 der Zeitschrift Sicherheitsforum, S. 46–49, das **integrierte Managementsystem (IMS**). Eine stufengerechte Sicht (Management – mittlere Führungsebene – Mitarbeiterin und Mitarbeiter) mache das IMS sicherheitsrelevant auf verschiedenen Ebenen: durch das „Personal", durch „Technik/Ablauf" und durch die „Organisation". Durch die Vernetzung von Informationen in einem IMS entstehe Wissen, das äußerst sicherheitsrelevant ist. Der Prozess stehe im Vordergrund, die Organisation mit der Bezeichnung von Abläufen, Aufgaben, Verantwortungen und Kompetenzen sei Mittel zum Zweck. Das Wissen über Abhängigkeiten, Anforderungen und Verantwortungen sei die Basis für eine nachhaltige Sicherheitskultur und sollte in einem IMS abgebildet sein und kontinuierlich gepflegt werden.

Sicherheitstechnik

Die **Integration der Zutrittskontrolle in das Videomanagementsystem** (VMS), Trends im Videomarkt und bei der Zutrittskontrolle sowie internationale Standards behandelt Roland Hunkeler, Siemens Building Technologies, im ZK-Spezial der Zeitschrift Sicherheitsforum vom Juni 2017, S. 18/19. Die Systeme für komplexe Anlagen würden immer performanter und intelligenter, seien also umfangreicher und müssten mehr können. Diese Anforderungen verlangten, dass die einzelnen Systeme autonom laufen und funktionieren müssen, auch wenn sie vernetzt sind. Der Videomarkt habe sich stark geöffnet, sodass die Integration von Fremdsystemen über ein Gateway viel einfacher geworden sei. Zurzeit würden prozessautomatisierte Zutrittslösungen, sogenannte Identity Access Managements (IAM) vermehrt nachgefragt. Das „Siveillance Identity Self-Service Portal" von Siemens sei intuitiv zu bedienen und webbasiert. Es ermögliche das Zutrittsberechtigungsmanagement über eine Vielzahl von Standorten hinweg. Zudem biete es eine leicht konfigurierbare Web-Applikation, die es Systemadministratoren erlaube, alle relevanten Zutrittsprivilegien zu definieren sowie jene Entscheidungsträger zu bestimmen, die Teil des Genehmigungsprozesses für Zutrittsprivilegien sein müssten. Im Hardwarebereich gehe der Trend bei der Zutrittskontrolle in Richtung 3-D-Gesichtsleser und 3-D-Terminals.

Mit dem **Effizienzdruck auf die Forschungs- und Entwicklungsabteilungen** (F&E) der Unternehmen befasst sich Dr. Peter Fey, Dr. Wieselhuber & Partner GmbH, in der Ausgabe 6-2017 der Zeitschrift PROTECTOR, S. 12/13. Um die Performance der eigenen F&E nachhaltig zu steigern, sei eine mehrdimensionale Betrachtung anzulegen. Wirklicher Erfolg stelle sich nur dann ein, wenn der betreffende Führungskreis dem F&E-Bereich eine klare operative und strategische Richtung vorgebe. Zur Steigerung der Innovationskraft sollte dieser Bereich konsequent an den übergeordneten strategischen Zielen ausgerichtet sein. Ebenso wichtig werde es, bislang branchenfremde „Schrittmacher-Technologien" zu adaptieren. Um die

Potenziale eines leistungsfähigen F&E-Managements freizusetzen, sollten bei seiner Gestaltung systematisch alle operativen wie auch strategischen Parameter in ihrer ganzen Bandbreite einer abgestimmten Optimierung unterworfen werden.

Laut der aktuellen Konjunktur-Umfrage des BHE ist die **Marktsituation der Facherrichter** anhaltend gut, berichtet PROTECTOR in der Ausgabe 6-2017, S. 14. Etwa zwei Drittel aller Befragten hätten für die Auftragslage die Note gut vergeben. Der gewerbliche Bereich erhalte mit 1,86 die beste Durchschnittsnote auf der Schulnotenskala seit Beginn der Erhebungen. Der private (2,36) und behördliche (2,61) Kundenkreis werde zwar vergleichsweise schlechter bewertet, entwickle sich aber seit Jahren positiv. Hiervon profitierten insbesondere die Einbruchmeldetechnik (1,98) und der Brandschutz – die Sparten Brandmeldetechnik (1,9) sowie Rauch- und Wärmeabzugsanlagen (2,0) erreichten neue Bestnoten.

Verknüpfung und Vernetzung statt Integration thematisiert PROTECTOR in der Ausgabe 6-2017, S. 26/27. Gerade kleine und mittlere Unternehmen hätten ebenso wie Konzernanwender den Bedarf, ihre Daten zu verknüpfen und Interoperabilität zu schaffen, damit ihr Sicherheitskonzept effizienter und leistungsstärker wird. Es gebe Möglichkeiten, diesen Bedarf mit modernen und dabei günstigen Technologien zu decken. Ein modernes Videomanagementsystem (VMS) biete in der Regel zwei Lösungen: das sogenannte Data Channel Recording als Standardfunktion und eine Smart Event Management-Oberfläche. Ein intelligentes VMS lese im ersten Schritt Daten und speichere sie in der Datenbank ab. Ein zweiter Schritt sei die Validierung der Daten. Hierbei würden die Daten mittels Standardprogrammiertools wie zum Beispiel XPath oder „BoostRegEx" ausgewertet und dann mit VMS in Ereignisse umgewandelt. Erfordere der Bedarf aber eine tiefer gehende Automatisierung der Prozesse, die bessere Visualisierung der Vorgänge oder den Einsatz von situationsbezogenen Ablaufplänen für den Nutzer, dann sei der Weg zum Einsatz einer PSIM-Lösung (Physical Security Information Management) oder eines Gebäudemanagementsystems eigentlich vorprogrammiert. Doch es gebe einen Mittelweg, weniger aufwändig, weniger investitionsintensiv: das Smart-Event-Management. Dieses browserbasierende Tool ermögliche die kundenspezifische Abbildung jeder Lage ohne zu großen Aufwand. Es visualisiere aber, und das sei der wesentliche Mehrwert, alle Vorgänge, Sensoren, Videodaten und anderes auf Open-Source-Karten und mache sie so effektiver handhabbar.

Stadionsicherheit

Dirk Dernbach, Securitas Deutschland, beschreibt im DSD, Ausgabe 2-2017, S. 10/11, Herausforderungen für **Veranstaltungsdienste im Stadionbereich** bei Sportgroßveranstaltungen. Sollten VOD-Kräfte neben Ordnungsfunktionen auch Sicherheitsaufgaben ausüben, bedürfe es einer Unterrichtung durch die IHK. Rechne man jetzt noch eine Evakuierungsübung, in Teilbereichen eine Ausbildung in waffenloser Selbstverteidigung und weitere einsatzbezogene Schulungen dazu, komme man schnell auf über 70 Stunden Ausbildung. Das seien mehr Ausbildungsstunden, als die meisten Sicherheitskräfte in anderen Bereichen vorweisen könnten. Dass die Bezahlung nicht der primär motivierende Faktor für diese Tätigkeit sein kann, zeige schon, dass die durchschnittliche Einsatzzeit bei viereinhalb Stunden pro Spiel und der Stundenlohn oftmals unter zehn Euro liege.

Terrorismus

Klaus Henning Glitza, Fachjournalist, befasst sich in der Beilage „Info Wirtschaftsschutz" zum DSD Heft 2-2017 mit der Frage, welche **Anzeichen im Vorfeld auf Terroristen** deuten können. Ein Terrorist werde in den seltensten Fällen so aussehen, wie wir uns einen typischen Täter vorstellen. Aber es sei faktisch unmöglich, „mit dem Körper zu lügen". Deshalb solle, so Prof. Dr. Dietmar Heubrock von der Universität Bremen, vor allem auf das Verhalten des Körpers geachtet werden: auf die Hände (mit den Fingern spielen; an die Nase fassen; an der Kleidung zupfen, Hand/Hals-Gesten; Hände falten; Hände in den Taschen), auf die Augen (Augensuchbewegungen; häufiges Blinzeln; auf den Boden gucken; Fixieren des Opfers; unruhiges Blickverhalten; starrer Blick), auf den Kopf (Mund verziehen; Wangenkauen; Lippen kauen; husten; sich räuspern; Nasenzucken; starre Mimik) und auf den Körper (verschränkte Arme; auf die Uhr schauen; mit den Füßen wippen; Bewegungsintensität; hochgezogene Schultern). Anlass zu besonderer Vorsicht sollte auch eine deutliche Asymmetrie der Kleidung, eine unnatürliche Körperhaltung und Gehweise sein.

Unternehmensstrafrecht

Vor allem der VW-Skandal befeuere rechtspolitische Debatten, einerseits um Sammelklagen und andererseits um Strafen für Unternehmen, schreibt die FAZ am 17. Juni. Bislang könnten in Deutschland nur natürliche Personen, etwa verantwortliche Vorstände, strafrechtlich belangt werden. Nur durch das Ordnungswidrigkeitenrecht könnten bislang Bußen auf das Unternehmen durchschlagen. Außerstrafrechtliche Möglichkeiten wie die Einführung des Korruptionsregisters seien flexibler als ein Unternehmensstrafrecht, meint Prof. Mark Zöller, der das Unternehmensstrafrecht als „Glaubenskampf" bezeichnet. Und sie würden Unternehmen mit kriminogenen Strukturen oftmals viel härter treffen als Zahlungspflichten. Auch die Auswirkungen einer breiten, gelegentlich auch ausufernden Berichterstattung könnten Unternehmen faktisch deutlich empfindlicher treffen als vermögensabschöpfende Maßnahmen. Dagegen fänden sich in der Schweiz und Österreich Regelungen, die für ein Unternehmensstrafrecht ins Feld geführt werden.

Veranstaltungssicherheit

Malte Schönefeld, Dr. Patricia M. Schütte-Bestek und Prof. Dr.-Ing. Frank Friedrich, Bergische Universität Wuppertal, sehen den **Veranstaltungsordnungsdienst** (VOD) im Fokus der Forschung (DSD, Heft 2-2017, S. 3-5). Ein herausragendes Projektergebnis auf drei Jahren Forschungs- und Entwicklungsarbeit sei der „BaSiGo-Guide". Er stelle den aktuellen Wissensstand zur Sicherheit bei Großveranstaltungen dar. Dem VOD sei bisher nicht die gebührende Beachtung geschenkt worden. Das BaSiGo-Folgeprojekt „ProVOD – Professionalisierung des Veranstaltungsordnungsdienstes" (2016–2019) werde unter Koordinierung durch die Bergische Universität Wuppertal im Verbund mit der IBIT GmbH und dem BBK durchgeführt. In diesem Projekt arbeite man daran, Begriff und Bedeutung in Übereinstimmung zu bringen. Ein Vorschlag könnte sein, „VOD"-Positionen mit Sicherheitsbezug als „Veranstaltungssicherheitskräfte" zu bezeichnen und von „Veranstaltungsservicekräften" abzugrenzen und beiden Gruppen ein angemessenes Aufgabenprofil mit den entsprechenden Anforderungen zuzuweisen.

Lucien Schibli, Pantex AG, beschreibt in der Zeitschrift Sicherheitsforum, Ausgabe 3-2017, S. 14–17, **fünf zentrale Einflussfaktoren für das Sicherheitskonzept** von Indoor-Veranstaltungen: die Natur und der

Inhalt der Veranstaltung, die Lokalität, die Raumordnung, die Organisation und das Publikum. Ziele der Sicherheitskonzeption sollten sein: klare Definition der Schutzziele, Analyse möglicher Gefahren, Dokumentation des Handlungsbedarfs mit Definition der Maßnahmen, Restrisiko, eindeutige Regelung der Pflichten und Grenzen der Sicherheitsdienstleister.

Vergabeverfahren

Den Risikofaktor Einkauf bei der Vergabe von Sicherheitsdienstleistungen thematisiert Manfred Buhl, Securitas Deutschland, im DSD, Heft 2-2017, S. 33–38. Er geht den Fragen nach, warum Einkäufer auf das billigste Angebot fixiert sind; wann und warum **das billigste Angebot zu teuer eingekauft** ist; welche Auswirkungen die Annahme des billigsten Angebots für den Auftragnehmer hat; welche Auswirkungen die Praxis der Ausschreibung zum billigsten Preis und des Billigangebots für die Sicherheitswirtschaft insgesamt hat; was Bieter tun können, um den Ausschreibenden davon abzuhalten, den „niedrigsten Preis" als alleiniges oder dominierendes Zuschlagskriterium zu bestimmen; woran sich der Einkäufer von Sicherheitsdienstleistungen orientieren soll, um nicht in die Falle des niedrigsten Angebotspreises zu geraten; und was die Politik leisten kann und muss, um das Missverständnis zwischen wirtschaftlichstem und niedrigstem Angebotspreis zu verhindern. Der Autor räumt ein, dass sich in den letzten Jahren manches zum Besseren gewandelt habe. Aber die Hauptursachen der Fixierung der Auftragsvergabe auf das billigste Angebot seien geblieben: Schwächen des Vergaberechts, Dominanz der Einkäufer gegenüber den Sicherheitsverantwortlichen im Unternehmen, schlecht vorbereitete Ausschreibungen, wenig durchdachte Dienstleistungsverträge, eine zu niedrige Eintrittsschwelle in den Beruf des Sicherheitsunternehmers und – daraus resultierend – „schwarze Schafe" im Sicherheitsgewerbe, Sozialbetrug gegenüber Mitarbeitern und fehlende Tariftreue.

Videoüberwachung

Die PROTECTOR-Ausgabe 6-2017 enthält eine **Marktübersicht** über 115 Videomanagement-Softwareprodukte von 64 Anbietern (S. 32/33). Abgefragt wurden unter anderem Kriterien aus den Bereichen Funktionsumfang und IT-Basis.

Berliner SPD streitet über Videoüberwachung, titelt DER TAGESSPIEGEL am 8. Juni. 80 Prozent der Berliner wollten laut Forsa-Umfrage mehr Videokameras im öffentlichen Raum. In Berlin gebe es 14.765 Videokameras im öffentlichen Raum, davon 13.643 im öffentlichen Personennahverkehr. Eine Echtzeitbeobachtung ermöglichten 3.267 Videokameras, davon 2.369 im öffentlichen Personennahverkehr, so das Ergebnis einer parlamentarischen Anfrage von Anfang Februar 2016. Ein parteiübergreifendes Bündnis wolle einen Volksentscheid. An 50 kriminalitätsbelasteten Orten solle intelligente Videotechnik installiert werden. Bei bestimmten Bewegungen könnten auf den Plätzen zum Beispiel Lichtanlagen aktiviert werden. Das Bündnis wolle den Ausbau der Videotechnik mit einem verstärkten Datenschutz kombinieren. Flächendeckend werde es keine Videoüberwachung geben, heißt es aus der Innenverwaltung.

Lidl führt die Videoüberwachung wieder ein, titelt die FAZ am 17. Juni. Notwendig sei der punktuelle Einsatz der Videotechnik, weil immer wieder Einbrüche und Überfälle passierten. In den vergangenen fünf Jahren seien das mehr als 600 Fälle gewesen. In jedem dritten Fall seien Mitarbeiter bedroht und sogar verletzt worden. Aktuell gebe es nirgends in den 3.200 deutschen Lidl-Filialen eine Videoüberwachung. Bis zu zwölf

Kameras würden pro Filiale installiert, je nach Gefährdungslage nur im Außenbereich oder auch in der Filiale sowie am Tresen. Nach jeweils zwölf Monaten solle der Datenschutzbeauftragte prüfen, ob die Videoüberwachung noch notwendig ist.

Die **Kompatibilität von Videosystemen in Leitstellen** thematisiert Dipl.-Ing. Hardo Naumann, Accellence Technologies GmbH, in Security insight, Ausgabe 3-2017, S. 26/27. Die mangelnde Kompatibilität stelle alle Leitstellen vor große Herausforderungen, bei denen Daten aus unterschiedlichen Anlagen zusammenkommen. Eine integrative Videomanagement-Software wie EBÜS helfe dabei, diese Herausforderungen zu bewältigen. Weit verbreitet sei Videomanagement-Software, die IP-Kameras mehrerer Hersteller aufschalten kann. Damit sei aber oft kein Zugriff auf Aufzeichnungen (Rekorder) und keine umfassende Steuerung und Recherche möglich. Die optimale Lösung bestehe in der Kombination verschiedener auf ihre jeweiligen Aufgaben spezialisierter Produkte, die über offene Schnittstellen miteinander verbunden werden. Über diese Schnittelle könne eine Leitstellensoftware je nach Prioritäten und konfigurierten Maßnahmen in stets gleicher Weise die zur jeweiligen Situation passenden Kameras aufschalten, unabhängig davon, an welchen Typ von Videosystem sie angeschlossen sind.

Security insight beschreibt in der Ausgabe 3-2017, S. 40/41, die **visuelle Überwachung einer „Dükerleitung“** mit Wärmebildkameras. Zwischen zwei Schiffsanlegern verlaufe eine ca. 1.000 Meter lange Unterwasserpipeline, in der die flüssigen Rohstoffe transportiert werden. Aus Sicherheits- und Umweltschutzgründen müsse die Wasseroberfläche entlang der Pipeline mehrmals täglich nach eventuell austretendem Öl abgesucht werden. Bisher seien Kontrollfahrten mit einer bemannten Schifffahrt durchgeführt worden. Jetzt sei auf beiden Schiffsanlegern jeweils eine Convision D98-T Thermalkamera mit salzwasserbeständiger Sonderbeschichtung montiert worden, welche die Überwachung der Wasseroberfläche zu jeder Tages- und Nachtzeit und bei jeder Witterung gewährleiste. Dabei überwache jede der beiden D98-T Kameras eine Strecke von über 500 Metern und zeige Ölbildungen auf der Wasseroberfläche bereits ab einem Durchmesser von wenigen Metern an.

Die Handelskette Real habe ihren **Test mit Gesichtsanalyse** an den Supermarktkassen gestoppt, meldet die FAZ am 30. Juni. Hintergrund dieser Entscheidung sei die in den vergangenen Wochen öffentlich geführte Diskussion, die den Eindruck erweckt habe, in den Real-Märkten würden im Kassenbereich ohne Wissen der Kunden Daten erhoben. In den betroffenen Real-Märkten hatte Echion, ein Spezialist für digitale Kommunikationskonzepte auf Handelsflächen, an Werbebildschirmen in der Nähe der Kassen Kameras installiert, die den Blickkontakt der Kunden aufzeichnen. Mit diesen Kameras sei aufgenommen worden, wann und wie lange der Kunde die Werbebildschirme anschaut. Dank einer speziellen Software würden sodann Rückschlüsse auf Alter und Geschlecht gezogen. Ziel sei es gewesen, herauszufinden, auf welche Produktwerbung die Kunden in welcher Weise anspringen.

Rahmenbedingungen, die es in der **Abwägung von Videoüberwachung und Datenschutz** zu beachten gelte, behandelt die Zeitschrift GIT Sicherheit in der Ausgabe 6-2017, S. 106–108: Hinweispflicht, rechtliche Vorgaben, Speicherfrist, Zweckerfüllung, Tonaufzeichnungen, Persönlichkeitsschutz, Privatzonen, Scrambling/Blurring (Personenverpixelung durch spezielle Filter), Verschlüsselung, Vieraugen-Prinzip, Unterbrechung der Bildanzeige- und Aufzeichnung sowie Rechtekonzept.

Stefan Palm und Kevon Shen, Moxa Europe GmbH, behandeln in der Ausgabe 6-2017 der Zeitschrift GIT, S. 109–111,

Herausforderungen bei der Anbringung von Überwachungskameras an den Außenseiten von Zügen: Funktionalität bei hohen und bei niedrigen Temperaturen, Wasserbeständigkeit, Kondensation, Korrosionsbeständigkeit, Kratzfestigkeit, einfache Installation und Wartung. Die Anbringung von Überwachungskameras an Zügen sei sowohl für Zughersteller als auch für Bahnbetreiber ein nutzbringendes und rentables Vorhaben.

Steve Hein, Actemium Cegelec GmbH, befasst sich in GIT Sicherheit, Ausgabe 6-2017, S. 114–117, mit **mobiler Territorialüberwachung**. Diebstahl und Vandalismus auf Baustellen, Containerparkplätzen oder auf Lagerflächen verursachten jedes Jahr Schäden im hohen Millionenbereich. Die mobile Lösung von Actemium zur Territorialüberwachung kombiniere effiziente Überwachungstechnologie mit flexibler Standortbestimmung und umfangreichen Kommunikationsmitteln. Die hochauflösenden 5-Megapixel-Digitalkameras erlaubten eine Detektion sogar bis zu einer Entfernung von 145 Metern. Das ergebe bei einer 360-Grad-Überwachung eine Detektionsfläche von rund 66.000 Quadratmetern. Komme es in vordefinierten Bereichen zu Auffälligkeiten, werde ein Alarm ausgelöst. Die intelligente Software sei in der Lage, zwischen Ein- und Austritt aus dem Detektionsfeld zu unterscheiden. Die Steuerung der Anlage erfolge über eine intuitiv bedienbare Weboberfläche, die über einen Browser läuft und sich damit direkt über das Internet regeln lässt.

In Heft 2-2017, S. 50, weist der DSD auf ein Urteil des BAG vom 22. September 2016 zur **Zulässigkeit der Verwertung eines Zufallsfunds** bei einer verdeckten Videoüberwachung hin (2 AZR 848/15). Eingriffe in das Recht der Arbeitnehmer am eigenen Bild seien zulässig, wenn ein konkreter Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers bestehe. Zudem müssten mildere Mittel ausgeschöpft werden und die Videoüberwachung dürfe nicht unverhältnismäßig sein. Auch wenn der Kreis der Verdächtigen möglichst weit eingegrenzt werden müsse, sei es nicht zwingend notwendig, eine Überwachungsmaßnahme so einzuschränken, dass sie ausschließlich Personen erfasse, für die bereits ein konkretisierter Verdacht bestehe. Zum Verhältnis von § 32 Abs. 1 Satz 2 und § 6b Abs. 1 Nr. 3 BDSG bei öffentlich zugänglichen Verkaufsräumen hebt das BAG hervor, dass, wenn die Voraussetzungen nach § 32 Abs. 1 Satz 2 gegeben seien, die Maßnahme jedenfalls im Verhältnis zu den von ihr betroffenen Arbeitnehmern auch nach § 6b Abs. 1 Nr. 3 zulässig sei.

Zutrittskontrolle

In einem ZK-Spezial der Zeitschrift Sicherheitsforum vom Juni 2017 geht Dipl.-Ing. (FH) Lutz Rossa, Von Zur Mühlen'sche GmbH, S. 6–9, der Frage nach, ob **Mobile Devices als Identifikationsmerkmalträger** der Zukunft Chipkarten, Token und Badges über kurz oder lang ablösen. Der Autor wägt Vor- und Nachteile der einzelnen Medien ab. Das Smartphone erhöhe die Sicherheit. Dürfen aber Mitarbeiter für die Zutrittskontrolle das private Smartphone statt der Chipkarte nutzen, entfielen viele Vorteile. Das Unternehmen habe keine Kontrolle über diesen Identifikationsmerkmalträger. Statt Ablösung sei wohl eher von einer Ergänzung auszugehen. Wenn viele kleine Standorte zentral verwaltet werden sollen, Mitarbeiter keinen festen Arbeitsplatz, sondern sogenannte Roaming Offices haben oder nicht vernetzte Standorte wie Windkraftanlagen oder Photovoltaikparks gesichert werden sollen, könne mittels Smartphone und Berechtigungsvergabe schnell und einfach Zutritt ermöglicht werden.

Fabian Lange, SBB Immobilien, erörtert im ZK-Spezial des Sicherheitsforums vom Juni 2017, S. 15–17, ob die **mit dem**

Zutrittskontrollsystem verbundene Einbuße an Komfort zur Firmenkultur passt. Am wichtigsten sei, dass die Mitarbeiter die neue Sicherheitskultur kennen, verinnerlichen und entsprechend umsetzen. So ließen sich Schäden und Missbräuche reduzieren. Andererseits nutze die beste bauliche Maßnahme und die detaillierteste Arbeitsanweisung nichts, wenn sie von den Mitarbeitern als Schikane empfunden und sabotiert werde. Sicherheit sei ein Kostentreiber ohne messbare Wirtschaftlichkeit. Es empfehle sich dringend, bei der Beschaffung von Apparaten, Anlagen und Komponenten zur Steigerung der Unternehmenssicherheit den ganzen Lebenszyklus der Anlagen mit allen Aufwänden im Blick zu haben. Von zentraler Bedeutung bei der Einführung einer Zutrittskontrolle sei die Einbeziehung der Mitarbeiter von Anfang an, die Beratung durch Experten, die Definition der angestrebten Prozesse und die Kalkulation von zehn Prozent mehr Budget bei der Planung und Beschaffung. Die Geschäftsleitung müsse vorleben, was sie von den Mitarbeitern verlangt.

Dieter Dreiszker, PKE Electronics AG, befasst sich im ZK-Spezial der Zeitschrift Sicherheitsforum, Juni 2017, S. 20–23, mit der **Kombination von Videosecurity und Zutrittskontrolle**. Der Autor erklärt die Problematik anhand eines Praxisbeispiels. Bei einem Öffnungszeitalarm bzw. Aufbruchsalarm lasse sich die Situation nur in Kombination mit einem Videosystem korrekt beurteilen. Die optimale Lösung liege im integrierten System. Durch die zentrale Verwaltung aller Objekte entstehe eine Datenintegrität. Das Problem der notwendigen Schnittstellen zwischen den einzelnen Subsystemen (Video, Zutritt usw.) respektive deren Vernetzung sei bereits im Kern der Managementsoftware gelöst. Nebst Video- und Zutrittskontrollsystemen ließen sich in einem umfassenden Sicherheitsmanagementsystem weitere Subsysteme wie Brandmeldeanlagen, Intrusionssysteme, Kommunikationsanlagen und diverse Steuerungen nahtlos integrieren. Dadurch bestehe eine hohe Skalierbarkeit, die es ermöglicht, dass das Sicherheitssystem mit den Bedürfnissen des Kunden laufend mitwächst.

Schutz vor Insidergeschäften sei auch eine Frage der physikalischen Sicherheit, schreibt Frank Richter, Honeywell Security and Fire Solutions, in der Ausgabe 6-2017 der Zeitschrift GIT Sicherheit, S. 132/133. Ergänzend zu Informationsbarrieren, auch „Chinese Walls" genannt (funktionale und informationstechnologische Trennungen) sei eine physische Trennung mit den entsprechenden Sicherheitsmaßnahmen ein wichtiges Element, um diese Abschottung sicherzustellen. Lücken in der physischen Sicherheit könnten ein Finanzunternehmen teuer zu stehen kommen, weil durch die unzureichende Abgrenzung der verschiedenen Geschäftsbereiche Insidergeschäfte stattfinden könnten. Insidergeschäfte und Marktmanipulationen zu verhindern, liege im Interesse jedes Finanzunternehmens.

Impressum

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

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

Herausgeber:
Manfred Buhl, Vorsitzender der Geschäftsführung, Düsseldorf

Verantwortlicher Redakteur:
Bernd Weiler, Leiter Kommunikation und Marketing

Beratender Redakteur:
Reinhard Rupprecht, Bonn

focus.securitas.de

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

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

E-Mail: info@securitas.de