Focus on Security

Ausgabe 05, Mai 2015

SECURITAS

Inhalt

Arbeitsschutz

GIT weist in der Ausgabe 4-2015, S. 100/101, darauf hin, dass mindestens einmal im Jahr Mitarbeiter „über Sicherheit und Gesundheitsschutz bei der Arbeit" nach der DGUV Vorschrift 1 der Deutschen Gesetzlichen Unfallversicherung zu unterweisen sind und, dass die Vorschrift jetzt eindeutig klärt, dass dies auch für Besucher oder Fremdfirmenmitarbeiter beim ersten Betreten des Unternehmens gilt. Der Unternehmer könne diese Aufgabe an Mitarbeiter delegieren. Allerdings sei zu prüfen, ob die Unterweisungen tatsächlich durchgeführt wurden und dies schriftlich dokumentiert wurde.

In derselben Ausgabe befasst sich GIT mit der richtigen Wahl von **Hitze- und Flammschutzkleidung** (S. 102–104). Erörtert werden die Begriffe „schwer entflammbar", „flammhemmend" und „inhärenter Schutz" (Gewebe, die durch ihre Fasereigenschaften schwer entflammbar sind), ferner die Europäischen Richtlinien 89/656/EWG (Mindestvorschriften für Sicherheit und Gesundheitsschutz bei Benutzung persönlicher Schutzausrüstung (PSA) durch Arbeitnehmer sowie Richtlinie 89/686/EWG (Angleichung der Rechtsvorschriften der Mitgliedstaaten für PSA. Diese Richtlinie teilt Schutzkleidungen in drei verschiedene Gruppen ein: einfache PSA, bei der davon ausgegangen wird, dass Nutzer den benötigten Schutz rechtzeitig selbst einschätzen können; mittlere PSA (mittlere Schutzwirkung) und komplexe PSA, die vor tödlichen Gefahren oder ernsten Personenschäden schützen soll. Behandelt werden in dem Beitrag auch, inwieweit das Gewicht des Kleidungsstücks die Leistungsfähigkeit eines Trägers fördern oder behindern kann und das Feuchtigkeitsmanagement.

Biometrie

LKA-Wissenschaftler Dr. Norbert Buchholz dringt mit der Erfindung einer neuen chemischen Untersuchungsmethode zur **Sichtbarmachung von Fingerabdruckspuren** in eine neue Dimension der kriminaltechnischen Auswertemöglichkeiten vor, heißt es in einer Pressemitteilung des LKA Schleswig-Holstein vom 20. März. Mit der neuen Methode könnten nun auch sehr schwach ausgeprägte und bislang nicht auswertbare Fingerabdruckspuren auf einer großen Bandbreite verschiedener Untergrundmaterialien mit einem erstaunlichen Ergebnis behandelt werden. Für das von Dr. Buchholz entwickelte Verfahren würden die von den Papillarleisten übertragenen Substanzen insgesamt nur eine „Verschmutzung" darstellen, die sich von den in erster Näherung schmutzfreien Papillarzwischenräumen abhebe. Es liege daher auf der Hand, sich in der Forschung verstärkt dem nicht bzw. weniger verschmutzten Bereich der Zwischenlinien zu widmen. Um diesen Bereich, der gar keine Zielsubstanzen enthalte, sichtbar zu machen, müsse zunächst ein Material eingebracht werden, das bei einer nachgeschalteten chemischen Reaktion wirksam werden kann. Als ideales Material stelle sich sehr feinkörniges Gold in Kombination mit einem physikalischen Entwickler heraus.

Brandschutz

Security insight stellt in der Ausgabe 2-2015, S. 48/49 das größte vollautomatische Tiefkühl-Hochregallager Deutschlands inklusive effektiven Brandschutz mittels Sauerstoffreduktion vor. Während in der normalen Atemluft die Sauerstoff-Konzentration 20,9 Volumenprozent beträgt, betrage sie in der **OxyReduct**-Schutzatmosphäre nur noch 16,2 Volumenprozent. Bereits diese leicht verringerte Sauerstoff-Konzentration schütze vor dem Ausbruch von Feuer. Der für die

Absenkung des Sauerstoffgehalts notwendige Stickstoff werde durch Generatoren mit neuester VPSA-Technologie (Vacuum Pressure Swing Adsorption) energieeffizient und klimaschonend aus der Umgebungsluft gewonnen. Unter optimalen Bedingungen könne man mit diesem System bis zu 80 Prozent Energie sparen im Vergleich zu Stickstoff-Erzeugungsanlagen mit herkömmlicher Membrantechnik. Um das Schutzniveau von 16,2 Volumenprozent halten zu können, würden lediglich zwei VPSA-Anlagen benötigt. Eine dritte diene als 50-prozentige Redundanz.

Business Continuity Management (BCM)

COMPUTERWOCHE.de befasst sich am 31. März mit **BCM und Disaster Recovery.** Bei IT-Prozessen und Systemen seien die Ausfallrisiken für Unternehmen groß und die Komplexität erschwere deren Qualifizierung. Dies habe in der Vergangenheit zum strategischen Modell der „Business Continuity and Disaster Recovery" (BCDR)-Planung gegen den Ausfall von IT-Diensten geführt. Zur Sicherung der Verfügbarkeit von IT-Diensten gebe es viele Möglichkeiten. Anwendungen verfügten häufig über integrierte Absicherungen gegen bestimmte Arten von Ausfällen. Für komplexe Systeme müssten diese meist entwickelt und implementiert werden. Selbst bei vorbildlichen Business Recovery-Plänen und idealer Umsetzung komme es zu Ausfällen. Für diesen Fall diene die zweite Phase des IT-Risikomanagements: die Disaster Recovery, eine Wiederherstellung des Systems. Die meisten Wiederherstellungsstrategien verwendeten logische oder physische Mehrfachabsicherungen. Wiederherstellungstechiken und -strategien seien so vielfältig wie die Katastrophenszenarien. Cloud Computing revolutioniere derzeit die Wiederherstellungstechnik. Durch Virtualisierung könnten Unternehmen sowohl logisch als auch physisch vielfältige Wiederherstellungsoptionen in der Cloud anlegen. Die Virtualisierung verändere die DR grundlegend und füge dem Thema eine umfangreiche Komplexitätsebene hinzu. Jeder BCDR-Plan stütze sich zu einem gewissen Grad auf das Netzwerk. Dem Kommunikationsmedium komme eine zentrale Rolle zu. Aus kommunikationstechnischer Sicht sei das Verhindern von häufigen Fehlern eine Frage der Kompetenz und des Verantwortungsbewusstseins des Carriers. Ein Unternehmen sollte also dem Anbieter seiner Wahl gezielte Fragen stellen: 1. Kann die physische Routenvielfalt demonstriert werden? 2. Wie sind die Rechenzentren bezüglich Stromversorgung, Sicherheit, Kühlung und Verbindungsvielfalt ausgestattet? 3. Wird Kommunikationstechnik der Netzbetreiber verwendet? 4. Deckt das Service Level Agreement die Dienste Ende-zu-Ende ab?

Fluchtwegplanung

Im BMBF-Projekt MAusKat habe das Fraunhofer ICT-IMM gemeinsam mit Partnern ein Mess- und Analysesystem entwickelt, mit dem die **Ausbreitungswege von gasförmigen Gefahrstoffen** in Tunnelsystemen und anderen komplexen Gebäudestrukturen ermittelt werden können, sodass sich Flucht- und Rettungswege effizienter planen und Katastrophen verhindern lassen, berichtet WiK in der Ausgabe 2-2015, S.46. Kernelement des Mess- und Analysesystems sei eine mobile und infrastrukturunabhängige Sensor-Plattform. In Tests würden dann an verschiedenen Messpunkten Strömung, Ausbreitung und Konzentration eines sogenannten Tracergases erfasst. Außerdem würden Temperatur, Luftfeuchtigkeit, Luftdruck und Windgeschwindigkeit aufgezeichnet.

Flughafensicherheit

Der Sicherheits-Berater geht am 31. März auf das Forschungsprojekt SAFEST ein, eine sogenannte „Akzeptanzstudie", bei der es um den Entwurf eines **sensorbasierten Gefahrenerkennungs- und Krisenmanagementsystems** für den Flughafen gehe. Damit solle sowohl das Risiko einer Massenpanik frühzeitig detektierbar, als auch unbefugtes Eindringen auf das Flughafengelände zu verhindern sein. Voraussetzung sei die Akzeptanz von Sicherheitsmaßnahmen bei den Passagieren, deren persönliche Daten dabei erhoben werden müssen. Die Forscher hätten nun festgestellt, dass die Ausgestaltung der Sicherheitsmaßnahmen für die Mehrheit der Passagiere offenbar äußerst akzeptabel ist.

Tilo Brinkmann, Bosch Sicherheitstechnik, erläutert in Security insight IP-Vernetzung und Ethernet auf dem Weg zum **„Smart Airport"** (Ausgabe 2-2015, S. 38–40). Gerade für Flughäfen böten IP-basierende Sicherheitssysteme klare Vorteile: Sie seien sehr modular, daher flexibel und hochgradig skalierbar, verwendeten die vorhandene Netzwerk-Infrastruktur, erhöhten durch enge Integration der verschiedenen Gewerke das Sicherheitsniveau und seien über zentrale Managementsysteme sehr effizient zu betreiben. In der Videoüberwachung sei die IP-Technologie eine wichtige Voraussetzung für die Speicherung auf verteilten digitalen Rekordern. Zudem ermögliche die Digitalisierung eine lokale Videoanalyse in der Kamera, sodass Videodaten nur noch bei bestimmten, definierten Ereignissen an die Leitstelle übertragen werden. Zudem sei mit IP-basierten Lösungen die Überwachung nicht mehr an einen zentralen Leitstand gebunden. Ethernet und IP seien schließlich auch eine einheitliche technologische Basis für die Integration aller sicherheitstechnischen Systeme in ein übergeordnetes Managementsystem. Als Plattform für „Smart Buildings" oder eben „Smart Airports" ermögliche das Protokoll auch eine enge Integration der Sicherheitstechnik mit anderen Gebäudetechnologien wie HVAC (Heating, Ventilation, Air Conditioning) oder der Beleuchtungstechnik.

Gefahrenmelder

Timm Schütz, TELENOT ELECTRONIC GmbH, rät in der Ausgabe 2-2015 der Fachzeitschrift WiK (S. 54/55), **nicht IP-fähige Übertragungsgeräte jetzt** zu **ersetzen**. Bis 2018 wolle die Telekom ihr Netz komplett auf IP-basierte Technik umstellen. Dies habe auch Auswirkungen auf die Übertragung von Gefahrenmeldeanlagen. Unternehmen, die dazu noch analoge oder ISDN-Aufschaltungen betreiben, sollten schnell handeln und auf IP-fähige Übertragungseinrichtungen (ÜE) umrüsten. Nur wenn die Endgeräte IP-fähig sind, könne die volle Funktionsfähigkeit am IP-basierten Anschluss gewährleistet werden. Dies bedeute für Sicherheitsanwendungen, z. B.: Datenprotokolle werden zum Teil nicht mehr unterstützt. Umgestellte analoge oder ISDN-Anschlüsse übertragen Meldungen nicht mehr zuverlässig. Die vom DSL-Endgerät zur Verfügung gestellten Teilnehmeranschlüsse können nicht genutzt werden. Es bestehe keine Sicherheit im Hinblick auf Blockade- oder Sabotageüberwachung der Übertragungseinrichtung. Im Einzelnen skizziert der Autor die Gründe, aus denen von einer Nutzung der emulierten analogen oder des ISDN-Ports des DSL-Endgerätes dringend abzuraten ist.

Wie WiK in derselben Ausgabe berichtet (S. 57), hat die Stiller Alarm Deutschland GmbH zum Schutz vor **Gewalt gegenüber Mitarbeitern** in Behörden oder anderen öffentlichen Einrichtungen eine IT-Lösung geschaffen, die es ermöglicht, bei Gefahr unauffällig einen stillen Alarm über ein Icon am Bildschirm oder über die Tastatur auszulösen, um rasch Hilfe herbeizuholen. Die PC-Standardversion für bis zu 20 Arbeitsplätze biete

sich für kleinere Unternehmen an. Neuerdings sei mit der „Stiller Alarm Mobile App" auch eine mobile Lösung verfügbar. Neben der aktiven Alarmierung biete die App den passiven Alarm. Schließlich gebe es noch die „Business App Edition", in welcher die PC- und die mobile Lösung kombiniert werden.

Industrie 4.0

Mit Themen zur Industrie 4.0 befasst sich die FAZ in einem Verlagsspezial am 9. April. Als entscheidend für die Weiterentwicklung der „Integrated Industry" werden folgende Trends bezeichnet: Modularisation, Identification, Integration, Digitalisation, Muniaturisation und Customisation. Fünf Schritte führen nach Überzeugung von Rechtsanwalt Dr. Tobias Fuchs zur **rechtlichen Sicherheit**: Schutz geistigen Eigentums, Anpassung von Lizenzmodellen, Klärung von Haftungsfragen, Beachtung des Außenwirtschaftsrechts und Absicherung des Datenverkehrs. Datensicherheit sei die Voraussetzung für den Erfolg der neuen Technologien. Der Datenaustausch müsse in Zukunft auch technisch stärker abgesichert werden. Darüber hinaus müssten Unternehmen sich bereits vor Implementierung neuer Technologien fragen, ob die Übermittlung von Daten etwa ins Ausland von ihrer Rechtsordnung geduldet wird.

Steffen Zimmermann, VDMA, schreibt in der FAZ am 10. April, **„Industrial Security"** bekomme mit Industrie 4.0 noch größere Brisanz für den Industriestandort Deutschland. Ohne den Schutz von Daten und Know-how unternehmensübergreifender Produktionsprozesse sei Industrie 4.0 undenkbar. Der automatisierte Datenaustausch vernetzter Produktionssysteme müsse sicher und zuverlässig gestaltet sein, die eindeutige Identifizierung der Prozessakteure kontrolliert und das Know-how von Produkten, Verfahren, Maschinen und Anlagen geschützt werden. Dazu müssten internationale Handelshemmnisse wie für Kryptografieprodukte abgebaut und sichere Mikrosystemarchitekturen von „Security Made in Germany" aufgebaut werden. Wichtig sei auch die weltweite Harmonisierung. Mindestens auf europäischer Ebene müsse sich die Bundesregierung für abgestimmte Sicherheitsmechanismen einsetzen.

Industrie 4.0 werde auch verstärkt als Herausforderung für die Sicherheit der Unternehmens-IT gesehen, heißt es bei heise.de am 15. April. Der Sicherheitsspezialist Trend-Micro spreche davon, dass praktisch jedes Unternehmen, das Sicherheitslösungen bezieht, auch angegriffen wird. Für Teilbereiche würden auf der Hannover-Messe Lösungen präsentiert. So lasse die **Fernwartungs-Lösung** von GeNUA nur dann einen Zugriff aus der Ferne zu, wenn auch ein Bediener im Unternehmen die Verbindung autorisiert. Mit SafeLock von TrendMicro werde der Steuerungsrechner von der Ausführung der Malware abgehalten. SafeLock verhindere Schreibzugriffe auf die Festplatte.

IT-Sicherheit

Mit der Mobile Encryption App habe die Deutsche Telekom als einer der ersten Anbieter eine weltweit einsetzbare **mobile Verschlüsselungslösung** für Smartphones auf den Markt gebracht, meldet der Sicherheits-Berater am 2. März. Auch unter widrigsten technischen Bedingungen könne mobil verschlüsselt telefoniert werden. Die App funktioniere im Gegensatz zu anderen Lösungen in jedem Telefonnetz und sogar ohne SIM-Karte über WLAN. Selbst in Ländern, in denen das Telefonieren über das Internet blockiert wird, lasse sich mit Hilfe der Lösung verschlüsselt kommunizieren. Es genüge, dass beide Nutzer die Mobile Encryption App auf ihrem Smartphone installiert haben. Eine kundenspezifische technische Infrastruktur im Hintergrund sei nicht nötig. Die Schlüssel, die bei der Lösung die sichere Kommunikation ermöglichen, würden ausschließlich auf den

eingesetzten Smartphones selbst generiert und nach Gesprächsende sofort gelöscht. Sie seien somit immer in der Hand des Nutzers und damit vollkommen unabhängig vom Netzbetreiber. Eine weitere Innovation der Deutschen Telekom sei der Corporate Security Hub, der Schadcodes aus dem Internet herausfiltere, bevor sie Smartphones und Tablets erreichen. Die Cloud-basierte Lösung könne einfach und schnell für den Kunden bereitgestellt werden. Kunden könnten wählen, welche Quell- und Zieladressen sie im Internetverkehr zulassen oder sperren möchten.

Security Intelligence helfe nicht nur bei der Angriffserkennung. App-Kontrolle, Patch-Management und Zugangsschutz profitierten ebenso davon, schreibt die COMPUTERWOCHE.de am 31. März. Laut einer Studie von Symantec und Deloitte fehlten aber 54 Prozent der befragten Unternehmen die notwendigen Sicherheitsinformationen und Bedrohungsanalysen. Mehr als ein Drittel litten unter Fehlalarmen in der IT-Security, wodurch es bei 84 Prozent zu Netzwerkstörungen und bei 74 Prozent zu Datenverlusten gekommen sei. Nur 24 Prozent der befragten Unternehmen zeigten sich in einer Studie von Intel Security zuversichtlich, einen Angriff innerhalb von Minuten zu entdecken. Fast die Hälfte brauche dazu Tage, Wochen oder sogar Monate.

Skype for Business steht zum Herunterladen bereit, meldet silicon.de am 15. April. Microsoft verteile die Client-App auch mit dem April-Update für Office 2013. Microsoft positioniere bereits jetzt Skype als eine App für Chat, Audio- und Videoanrufe, Onlinebesprechungen und Onlinezusammenarbeit. Darüber hinaus verspreche Microsoft, dass jegliche Kommunikation über Skype for Business mit einer starken Authentifizierung und Verschlüsselung geschützt ist.

IBM mache seine Sicherheitsdatenbank per Cloud der Öffentlichkeit zugänglich, meldet COMPUTERWOCHE.de am 16. April. Den Nutzern solle so Rüstzeug für Cyberattacken an die Hand gegeben werden. Durch die Positionierung in der Cloud auf der Sharing-Plattform X-Force Exchange solle die Datenbank Zugriff auf Echtzeit-Indikatoren gewähren, um sich gegen aktuelle Hacker-Angriffe verteidigen zu können. Die User könnten Informationen untereinander austauschen und zudem in den Dialog mit Experten eintreten. Informationen auf Basis von mehr als 15 Mrd. Sicherheitsereignissen pro Tag, Malware-Datensätze von 270 Mio. Devices, Details zu Bedrohungen basierend auf 25 Mrd. Websites und Bildern, acht Mio. untersuchte Spam- und Phishing-Kampagnen, sowie Profile von knapp einer Million bösartiger IP-Adressen sorgten für einen enormen Umfang der Datenbank. Um den Bestand stetig zu ergänzen und zu erweitern, sollten die Datenbanken von IBM-Partnern künftig auch mit der Security-Datenbank verknüpft werden.

IuK-Kriminalität

Jedes zweite Unternehmen in Deutschland sei in den vergangenen beiden Jahren Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden und habe dadurch Wettbewerbsvorteile eingebüßt, berichtet der ASW am 24. April. Das habe eine **Studie von BitKOM** ergeben, die auf der Befragung der Geschäftsführer und Sicherheitschefs von 1.074 Unternehmen basiere. Am stärksten gefährdet sei die Automobilindustrie (68 Prozent). In der Chemie- und Pharmabranche seien es 66 Prozent, unter Banken und Versicherungen 60 Prozent. Der Schaden für die deutsche Wirtschaft summiere sich auf rund 51 Mrd. Euro im Jahr. Fast ein Viertel entfalle auf Plagiate. Es folgten Patentrechtsverletzungen und Verlust von Wettbewerbsvorteilen. Häufigstes Angriffsziel seien die IT-Systeme und die Kommunikationsinfrastruktur der Unternehmen. In einem Fünftel der Fälle hätten es die Angreifer auf Lager und Logistik abgesehen gehabt. Mittelstän-

dische Unternehmen seien am stärksten von Spionage- oder Sabotageakte betroffen. In der Hälfte der Fälle träten aktuelle oder ehemalige Mitarbeiter als Täter in Erscheinung. Aber nur 52 Prozent der befragten Unternehmen führten Schulungen der Mitarbeiter oder Sicherheitsüberprüfungen von Bewerbern durch. Am häufigsten registriere die Wirtschaft den Diebstahl von elektronischen Geräten (28 Prozent). 19 Prozent beklagten Fälle von Social Engineering. 17 Prozent berichteten vom Diebstahl sensibler elektronischer Dokumente oder Daten, 16 Prozent von Sabotage ihrer IT-Systeme oder Betriebsabläufe. Bei acht Prozent sei die elektronische Kommunikation ausgespäht worden. Die zweite große Tätergruppe mit 39 Prozent umfasse das unternehmerische Umfeld, bestehend aus Wettbewerbern, Lieferanten, Dienstleistern und Kunden. Aus Sicht des BitKOM müssten die Unternehmen mehr für den Schutz ihrer materiellen und immateriellen Werte tun und an folgenden Stellen ansetzen: IT-Sicherheit, organisatorische Sicherheit (insbesondere Regelungen über den Datenzugang und Zutritt zu sensiblen Bereichen), personelle Sicherheit und Sicherheitszertifizierungen. Das IT-Sicherheitsgesetz werde perspektivisch zu mehr Sicherheit in der gesamten Wirtschaft führen.

Sicherheitsforscher hätten einen neuen Trojaner entdeckt, der vor allem im Öl- und Gassektor aktiv sei, berichtet SPIEGEL ONLINE am 1. April. Symantec habe die Schadsoftware entdeckt und **„Trojan.Laziok"** getauft. Der Schwerpunkt der Aktivität liegt nach Angaben der Sicherheitsfirma im Nahen Osten. Zwischen Januar und Februar 2015 stünden die meisten Ziele in Verbindung mit der Gewinnung und Verarbeitung von Öl, Erdgas und Helium. Die Verbreitung erfolge über eine E-Mail, in deren Anhang sich eine Excel-Datei befinde. Die Malware gehe nach einem mehrstufigen Plan vor. Zunächst sammle sie Konfigurationsdaten des befallenen Windows-Rechners und sende sie an seine Auftraggeber. Dann werde entschieden, ob es sich um ein interessantes Objekt handelt. Nach Angaben der Sicherheitsexperten sitzen die Verantwortlichen unter anderem im EU-Raum. Die Downloads führten auf Server in Bulgarien, Großbritannien und den USA. Besonders komplex sei das technische Niveau des Angriffs offenbar nicht.

Kaspersky Lab habe die Spionagekampagne **„Darkhotel"** enttarnt, bei der seit mindestens vier Jahren gezielt sensible Daten von geschäftsreisenden Führungskräften gestohlen wurden, berichtet veko-online.de am 2. April. Bei einem einmaligen Zugriff über das WLAN des kompromittierten Hotels würden alle wertvollen Daten eingesammelt. Neben dem Ausspähen von Hotelgästen setze die „Darkhotel-Gruppe" auch auf Spear-Phishing und Filesharing-Serverattacken. Geschäftsreisende sollten auch halbprivaten Netzwerken in Hotels misstrauen, rät Kaspersky Lab. Virtual Private Networks ermöglichten einen verschlüsselten Kommunikationskanal. Gerade auf Reisen sollte man Software-Updates gegenüber skeptisch sein und nur solche Updates berücksichtigen, die von einem offiziellen Anbieter signiert sind.

Nach einer Meldung der Medieninformation der Schweizer Melde- und Analysestelle Informationssicherung (MELANI) vom 31. März missbrauchen Betrüger bei Phishing-Angriffen nicht mehr ausschließlich die Namen großer und bekannter Unternehmen, sondern verüben auch sehr gezielt solche Angriffe mit dem Namen kleinerer Firmen. In einer ersten Phase versuchten die Kriminellen, über die Firmenwebsite an eine Datenbank mit Kunden-E-Mail-Adressen zu gelangen. Danach würden im Namen dieser Firma gefälschte Mail-Nachrichten an die entwendeten Adressen gesendet. Absender und Inhalt seien perfekt imitiert. Die Adressaten würden auf eine gefälschte Website gelockt und gebeten, Details der Kreditkarte anzugeben. Neben der Anwendung einer Firewall empfiehlt MELANI, Kunden über die Entwendung ihrer E-Mail-Adressen sofort zu informieren und Anweisungen über das weitere Vorgehen zu geben.

Eine Hackerattacke durch mutmaßliche Anhänger der Terrororganisation IS hat den Sendebetrieb des frankophonen Fernsehkanals **TV5 Monde** in der Nacht zum 8. April stundenlang lahmgelegt, meldet die FAZ am 9. April. Die Systeme des Senders seien erheblich beschädigt worden. Der Sender habe stundenlang die Kontrolle über seine Internet-, Facebook- und Twitterauftritte verloren. Auf der TV5 Monde-Internetseite seien Propagandavideos des IS gezeigt worden. Die Hacker hätten einen Appell an Präsident Hollande gerichtet, die französische Beteiligung am Militäreinsatz gegen den IS im Irak zu beenden. „Soldaten Frankreichs, haltet Euch vom Islamischen Staat fern!", habe es auf der gehackten Facebook-Seite des Senders geheißen. Die Hacker hätten den Familien der Soldaten gedroht. „Ihr habt die Chance, das Leben eurer Familie zu retten, nutzt sie!", habe es geheißen. Die Hacker hätten auf der Facebook-Seite Dokumente veröffentlicht, bei denen es sich nach ihren Angaben um Ausweise und Lebensläufe französischer Soldaten handelt, die an Einsätzen gegen IS beteiligt sein sollen. Die Hacker hätten sich als Mitglieder der Terrorgruppe „CyperCaliphate" ausgegeben. Die Gruppe hätte im Januar das Twitter-Konto der amerikanischen Kommandozentrale CentCom gehackt. Im Februar habe die Gruppe Cyber-Kalifat minutenlang den Internetauftritt des Nachrichtenmagazins „Newsweek" kontrolliert. Der Vorfall habe, wie die FAZ am 10. April schreibt, auch die Debatte um Sicherheit von Computeranlagen in den deutschen Unternehmen befeuert. Stünden doch nach Angaben des IT-Branchenverbandes Bitkom hierzulande Zehntausende Unternehmen potenziellen Attacken wehrlos gegenüber. Beim VDMA habe es am 9. April geheißen, solch ein gewaltiger Angriff wie in Paris werfe die Frage auf, ob eine durchdigitalisierte Industrie überhaupt sicher umzusetzen ist. Würden doch nach Angaben des IT-Konzerns IBM in das Internet aufgrund Tausender Schwachstellen quasi im Sekundentakt neue Viren, Trojaner und Würmer gezielt eingespeist.

Die Analysten der Denkfabrik Rand Corp. gingen von Hunderten in aller Welt straff gemanagten Hacker-Organisationen aus. In einer Untersuchung des Potsdamer Hasso Plattner-Instituts für Softwaresystemtechnik (HPI) heiße es, Ende 2014 seien rund 6.500 Schwachstellen in verschiedener Software bekannt geworden. Ohne Sicherheit sei Industrie 4.0 undenkbar, habe ein Sprecher des VDMA erklärt. Nach einer repräsentativen Umfrage von Bitkom seien zwar 75 Prozent aller Firmen in Deutschland bereits Angriffen durch Hacker ausgesetzt. Doch nur jedes zweite Unternehmen sei für den Notfall auch gewappnet. Während Großkonzerne wie Bayer, Siemens oder BASF dreistellige Millionen Euro-Beträge in die Sicherheit ihrer Datenzentren, Computer und IT-Netzwerke steckten, zeige sich der deutsche Mittelstand hier oft knausrig.

Heartbleed bedroht Unternehmen auch 2015, titelt COMPUTERWOCHE.de am 7. April. Der Grund dafür, dass vielen Unternehmen auch noch rund ein Jahr nach der Entdeckung der Heartbleed-Sicherheitslücke massiver Schaden durch Cyberkriminelle droht, liege laut der Venafi Labs-Studie darin, dass viele Unternehmen nur unzureichend versucht hätten, die Schwachstelle zu beseitigen. Im April 2015 sollten demnach immer noch 74 Prozent der „Global 2000"-Unternehmen mit öffentlich ausgerichteten Systemen gefährdet sein, weil die Korrekturen an ihrer Netzwerkumgebung nicht vollständig abgeschlossen wurden. Allerdings wüssten deutsche Sicherheitsexperten mehr über eingesetzte Schlüssel und Zertifikate, als ihre Pendants in anderen Ländern. Ein weiterer wesentlicher Punkt für das konsequente Vorgehen deutscher Unternehmen in Sachen Heartbleed sei aber auch, dass in Deutschland viel weniger Schlüssel und Zertifikate in Unternehmen genutzt würden als im Rest Europas und den USA. Um die Heartbleed-Sicherheitslücke vollständig schließen zu können, sind laut Kevin Bocek von Venafi vier Schritte notwendig: die Generierung neuer Schlüssel für SSL/TLS, die

Nutzung neuer Zertifikate, die Erneuerung noch nicht abgelaufener Zertifikate und die doppelte Überprüfung aller Server, um sicherzustellen, dass sie mit neuen Schlüsseln und Zertifikaten laufen.

Interpol warnt vor Kriminalität im Internet, titelt die FAZ am 15. April. Sie nehme so rasch zu, dass Unternehmen und Staaten verstärkt nach gemeinsamer Gegenwehr suchen. Das IT-Unternehmen Gartner rechne damit, dass die weltweiten Ausgaben für die Sicherheit im Internet 2015 um 8,2 Prozent auf 77 Mrd. Dollar steigen werden. „Der Schutz gegen Internetkriminalität frisst einen Großteil des Geldes, das das Führen eines Unternehmens kostet", habe Interpol-Generalsekretär Jürgen Stock gesagt. „Cyberkriminalität verbreitet sich immer weiter und kostet die Weltwirtschaft jährlich rund 400 Mrd. Dollar", habe Singapurs stellv. Ministerpräsident Teo Chee Hean gewarnt. Rik Ferguson, Trend Micro, habe die Szenarien der Zukunft ausgemalt: „Allein der Versicherungssektor wird Dutzende Millionen von Dollar als Prämien verlangen, um sich gegen Cyberkriminalität abzusichern." Auf mittlere Sicht erwarte er, dass Länder von privaten Ratingagenturen auch aufgrund der von ihnen gebotenen Datensicherheit bewertet werden. Schon bald werde es einen Internationalen Gerichtshof für Cyberkriminalität geben. Interpol habe sein weltweites Innovationszentrum in Singapur eröffnet, von wo aus Polizisten aus 50 Ländern auch die Internetkriminalität bekämpfen. Es arbeite unter anderem mit dem deutschen Fraunhofer Institut zusammen.

Windows bleibe mit riesigem Abstand **das am stärksten bedrohte Betriebssystem**, stellt Eugene Kaspersky fest (FAZ am 18. April). Im Januar 2015 habe man 283 Angriffe auf Rechner mit dem iOS-Betriebssystem von Apple registriert, 12.000 auf die Mac-Rechner von Apple, 13 Mio. auf Android und 237 Mio. Attacken auf Windows-Nutzer. Längst würden die Angreifer auch auf den mobilen Datenverkehr zielen. So sei die Zahl von Attacken auf Mobiltelefone von 40.000 im Jahr 2012 auf 296.000 im Jahr 2014 gestiegen. Es gebe weltweit deutlich mehr als 100.000 Täter, die in der Cyberkriminalität arbeiten. Inzwischen würden auch „traditionelle Verbrecher" Dateningenieure anwerben, damit sie die gleichen Straftaten auf neuen Wegen begehen können. Bei Spionagefällen würde neben den traditionellen Sprachen Englisch, Russisch und Chinesisch immer mehr Französisch, Spanisch und neuerdings auch Arabisch auftauchen. Durch Sabotage gefährdet seien Energienetze, Krankenhäuser, Logistik und städtische Dienstleistungen.

Neue Herausforderungen und Werkzeuge in der **IT-Forensik** behandeln Elmar Schwager, The AuditFactory, und Joachim A. Hader, secudor GmbH, in der Ausgabe 2-2015 von Security insight, S. 28/29. Die Messlatte für IT-Forensiker werde mit dem immer währenden Wachstum in der IT und der zunehmenden Diversifikation der Geräte immer höher gesetzt. Massendaten und mobile Endgeräte seien nur zwei Beispiele, mit denen der Forensiker heutzutage kämpfen müsse. IT-Werkzeuge böten eine Vielzahl von Adaptern für die proprietäre Hardware sowie die Möglichkeit, mittels einer auf die Betriebssystemversion spezialisierten Analysesoftware auf die Daten der mobilen Endgeräte zuzugreifen. Mit dieser Software könnten z. B. der Gesprächsverlauf analysiert, gelöschte SMS, Daten und Apps wieder hergestellt sowie Bewegungsprofile erstellt werden.

Kfz-Aufbruch

Nach einer Pressemitteilung des Polizeipräsidiums Trier vom 27. März werden vermehrt Einbrüche in Firmenfahrzeuge festgestellt, die Mitarbeiter an der Wohnanschrift abgestellt haben. Die Täter schneiden ein Loch in das Blech der Heckklappe oder der Seitentür, heben die Verriegelung der Tür auf und entwenden eine Vielzahl von hochwertigen Maschi-

nen und Spezialwerkzeugen. Die Polizei rät, Firmenfahrzeuge in Garagen, Hallen oder an gut ausgeleuchteten Parkplätzen abzustellen. Außerdem sollten die Unternehmen Seriennummern ihrer Werkzeuge notieren, um die Fahndung zu erleichtern.

Kommunale Sicherheit

Fortschrittliche Kommunen verfolgten inzwischen vermehrt Projekte, die helfen sollen, das Leben ihrer Einwohner „smarter" zu gestalten, schreibt Jochen Sauer, Axis Communications, in der Ausgabe 2-2015 von Security insight (S. 18/19). Die **vernetzte Technologie der „intelligenten Stadt"** basiere dabei auf einer Systemarchitektur, die aus vier „Technologieschichten" besteht. Sensoren, die Daten durch direkte Kommunikation zwischen Geräten sammeln, akustische und visuelle Erfassung mittels IP-Kameras und die abstrakte Erfassung mobiler Endgeräte, seien über die zweite Schicht – das städtische Netzwerk – verbunden. Beide Schichten bildeten gemeinsam das Internet of Things. Daten und Anwendungen laufen dann auf einer gemeinsamen Betriebsplattform zusammen, der dritten Schicht, wo Informationsverarbeitung und Datenanalyse stattfinden. In der vierten Schicht gehe es um die Einbindung aktueller und historischer Daten und die Berechnung komplexer Modelle für diverse Anwendungen. Netzwerk-Kameras könnten als Sensoren verwendet werden, zum Beispiel für die Anpassung der Straßenbeleuchtung an den tatsächlichen Bedarf. Netzwerk-Kameras verfügten über integrierte multifunktionale Anwendungen wie Nummernschild-Erkennung, Personenzählung und Objektverfolgung, die durch Anschluss anderer Sensoren erweitert werden könnten.

Krisenregionen

Die Huthi-Miliz kontrolliere eine wichtige Schiffsroute zwischen Europa und Asien, titelt das Handelsblatt am 1. April. Die Rebellen hätten strategisch wichtige Positionen am Golf von Aden besetzen können. Sie könnten mit ihren schweren Waffen nun auch eine internationale Schiffsroute bedrohen, die zum Suez-Kanal führt. Konkret befänden sich die Huthis in einem Gebiet namens Sabab und den Scheich Said-Bergen nahe der Meerenge von Bab el-Mandeb.

Krisenstab

Corporate Trust stellt in der Fachzeitschrift WiK (Ausgabe 2-2015, S. 25/26) folgende Anforderungen an die Mitglieder eines Krisenstabes auf: hohe Fachkompetenz in der zugewiesenen Funktion; sehr gute Vernetzung innerhalb des Unternehmens; hohe psychische und physische Belastbarkeit; ausgeprägte Teamfähigkeit; hohe Sozialkompetenz und interkulturelles Verständnis; Bereitschaft zur konstruktiven Auseinandersetzung; Objektivität und emotionsfreie Beurteilungsfähigkeit; schnelle Erfassung und Einschätzung komplexer Lagen; ausgeprägte Fähigkeit, das BCM-Management auf unternehmensstrategischer Ebene zu verstehen; hundertprozentige Integrität und Erfüllung der Compliance-Regeln.

Luftsicherheit

Erhebliche **Probleme bei der Sicherheit von Luftfracht** sieht die Mitteldeutsche Zeitung (mz-web.de) am 16. April. Das ergebe sich aus der Antwort der Bundesregierung auf eine Kleine Anfrage der Linksfraktion. Demnach seien 2014 bei 38 Prozent der Kontrollen von „bekannten Versendern" Mängel festgestellt worden. Bei „reglementierten

Beauftragten" (das sind zertifizierte Logistikunternehmen) habe die Quote 40 Prozent betragen. Sechs Zulassungen seien widerrufen worden. Bei Subunternehmen habe es bei fünf von sechs Kontrollen Mängel gegeben. Die Einführung einer Luftfrachtsicherheitsgebühr sei rechtlich und wirtschaftspolitisch problematisch. Der Vorsitzende der Bundespolizeigewerkschaft habe beklagt, dass nur an drei von zwölf deutschen Flughäfen die Bundespolizei überhaupt Transferfracht-Kontrollen durchführe, und zwar stichprobenartig. Die „sichere Lieferkette" gebe es eigentlich gar nicht. Im übrigen herrsche in dem Bereich ein Kompetenzwirrwarr, weil auch die Fluggesellschaften, das Luftfahrtbundesamt und der Zoll involviert seien.

Hinweise, wie sich Reisende im Flugverkehr schützen können, gibt Security insight in der Ausgabe 2-2015, S. 32–34. Alle Airlines aus Libyen, Liberia, dem Kongo und dem Sudan unterlägen einer EU-weiten Betriebsuntersagung. Auch den meisten Airlines aus Indonesien, den Philippinen sowie Kasachstan und Kirgisistan sei der Flugbetrieb innerhalb der EU und der Schweiz aus Sicherheitsgründen untersagt. Ein Blick auf das durchschnittliche Flottenalter könne bereits wichtige Hinweise auf die Sicherheit einer Airline liefern. Zudem sollten Reisende Via-Verbindungen immer Direktflüge vorziehen, denn über die Hälfte aller Unfalltoten entfielen auf Kurzstreckenflüge. Der gefährlichste Abschnitt eines jeden Fluges sei der Start- und Landevorgang.

Maschinensicherheit

Dr. Stefan Mohr, Leuze Electronic GmbH & Co. KG, befasst sich in der Ausgabe 4-2015 der Zeitschrift GIT (S. 74–76) mit **Sicherheits-Laserscannern** und stellt die neue RSL 400 Baureihe von Leuze electronic vor, die aus 16 Gerätevarianten in vier gestaffelten Reichweiten und vier Funktionsvarianten bestehe. Ob stationär oder mobil, ob lange oder kurze Reichweiten, Basisfunktionen oder eine High-End-Ausstattung: Der Anwender erhalte ein maßgeschneidertes Gerät, das sich bei einem Geräte-Upgrade ganz einfach auswechseln lasse. Stoßrichtung der Optimierungsmaßnahmen seien: gestaffelte Erhöhung der Scanbereiche, Bereitstellung anwendungsoptimierter Funktionen, Vereinfachung der Handhabung. Der RSL 400 verfüge über zwei unabhängig voneinander einstellbare Konfigurationen und zwei Sicherheits-Schaltausgangspaare. Das ermögliche das gleichzeitige Ausführen von zwei völlig verschiedenen Schutzaufgaben mit einem Gerät.

In derselben GIT-Ausgabe behandelt Jörg Schreiber, Schmersal, die **sicherheitstechnische Bewertung** vorhandener Maschinen (S. 94/95). Im ersten Schritt werde eine Matrix erarbeitet, nach der jede einzelne Maschine bewertet werden sollte. Das Ergebnis dieser Arbeit waren bei einem Unternehmen der Medizintechnik 90 zu bewertende Eigenschaften, die es an jeder Maschine zu untersuchen galt. Berücksichtigt worden seien neben den einschlägigen Normen und Richtlinien auch Aspekte des Manipulationsschutzes sowie der Ergonomie. Auch mit Hilfe eines von Schmersal initiierten CE-Netzwerkes hätten alle Standorte der medizintechnischen Firma mit über 2.000 Maschinen innerhalb von drei Monaten bewertet werden können.

Florian Lenzmeier, Phoenix Contact GmbH & Co. KG, stellt in derselben Ausgabe die Produktfamilie Safe Energy Control (SEC) mit einer neuen **Funkenstreckentechnik**, hoher Lebensdauer und Leistungsstärke beim Blitzstrom- und Überspannungsschutz vor (S. 96/97). Der Einsatz der notwendigen Schutzgeräte erfolge abgestuft: Das leistungsstärkste Schutzorgan werde demnach direkt am Gebäudeeintritt installiert, das Schutzgerät mit dem schnellsten Ansprechverhalten unmittelbar vor dem zu schützenden Endgerät (Überspannungsableiter Typ 3). Bei Gebäuden mit äußerem Blitzschutz

könnten bei einem direkten Blitzeinschlag gewaltige Blitzenergien eingekoppelt werden. Hier sei laut VDE-Vorschrift ein Blitzstromableiter Typ 1 Pflicht. Als leistungsstärkste Technologie für Blitzstromableiter habe sich hier die Funkenstrecken-Technologie etabliert. Die Typ 1-Ableiter aus dem SEC-Produktprogramm verfügten über eine netzfolgestromfreie Funkenstrecken-Technologie. Diese Technologie sowie der vorsicherungsfreie Einsatz für jede Applikation und Ableiterklasse stellten den Überspannungsschutz auf eine neue Stufe.

Museumssicherheit

PROTECTOR stellt in seiner Ausgabe 4-2015, S. 18–20, das Sicherheitskonzept im Kunstmuseum Stuttgart vor. Ein solches Sicherheitskonzept bestehe immer aus einer Kombination mechanischer, elektronischer und alarmierender Komponenten. Das Gebäude sei in sieben Brandabschnitte im öffentlichen Bereich unterteilt. Fluchtwege führten über Treppenhäuser, die über RWA-Anlagen entraucht werden, ins Freie. Jeder einzelne Brandschott biete demnach die Feuerwiderstandsklasse F90. Das bedeute, dass diese Abschnitte mindestens eineinhalb Stunden vor Feuer schützen.

Öffentliche Sicherheit

Wie der Sicherheits-Berater am 31. März mitteilt, hat das Forschungsforum Öffentliche Sicherheit Vorabergebnisse der **Delphistudie „Sicherheit 2030"** veröffentlicht. Danach benennen die Experten in auffälliger Einigkeit (S. 46) folgende anhaltende Prozesse mit Einfluss auf die öffentliche Sicherheit: die steigende Abhängigkeit von Informations- und Kommunikationstechnologien, die steigende Vulnerabilität von Kritischen Infrastrukturen, den Anstieg der globalen Mobilität und des globalen Handels, die wachsende Schere zwischen Arm und Reich und den Anstieg der Migration nach Deutschland.

Dr. Thomas Schweer, Geschäftsführer des Instituts für musterbasierte Prognosetechnik, erläutert in veko-online.de am 2. April die Methode der **„Near Repeat Prediction".** PRECOBS (Pre Crime Observation Systems) arbeite ausschließlich mit Falldaten aus den polizeilichen Vorgangserfassungssystemen. Deliktkonzentrationen in engen zeitlichen und geografischen Räumen bildeten die Grundlage der near repeat prediction. Bei der Methodik würden Triggerkriterien aus den Kriterienbereichen Tatzeit, Beute und modus operandi festgelegt. Triggerdelikte seien Delikte, die anhand ihrer Tatmerkmale eine überdurchschnittliche Wahrscheinlichkeit aufweisen, da sie in „near repeats" aufträten. In einer zur Prognose geeigneten „near repeat area" sollte der Anteil der als Trigger klassifizierten Taten signifikant hoch sein. Seien die relevanten Trigger und Antitrigger (z. B. Beziehungstaten) sowie die „near repeat areas" ausgewählt, werde die Analysesoftware konfiguriert und eine retrospektive Simulation gestartet. Ziel sei es, für jede „near repeat area" die beste Konfiguration zu finden, um später im Echtbetrieb einen stabilen Prognoseerfolg zu gewährleisten.

Bis zum 31. März 2016 müssen in öffentlichen WLAN-Hotspots mit mehr als 10.000 Teilnehmern alle erforderlichen Techniken zur Überwachung des Telefon- und Datenverkehrs eingebaut werden, meldet wirtschaftswoche.de am 11. April. Das habe der Präsident der Bundesnetzagentur angeordnet.

ÖPV-Sicherheit

Terroristische Anschläge auf Bahnen und Busse behandelt Security insight in der Ausgabe 2-2015 (S. 8–12). Nahezu jeder dritte Nutzer öffentlicher Verkehrsmittel in Deutschland fühle sich auf Bahnhöfen oder an Halte-

stellen unsicher oder bedroht. In den Bussen und Bahnen selbst glaube etwa jeder Zehnte, „weniger oder überhaupt nicht sicher" zu sein. Das sei das Ergebnis einer repräsentativen Umfrage von Forsa. Auf dem Prüfstand stehe einerseits die Videoüberwachung der Züge und Bahnhöfe, mehr aber noch die Frage von mehr und besser organisiertem Personal.

Organisierte Kriminalität (OK)

Europol habe eine **Studie zur OK** veröffentlicht, die über die üblichen Annahmen hinausgeht, berichtet heise.de am 9. April. Die OK gehöre nach Ansicht von Europol heute schon zu den fortgeschrittenen Nutzern von IT-Produkten. Dieser Trend werde sich in Zukunft noch verstärken, mit hochspezialisierten Hackern, die beispielsweise autonome Vehikel aller Art angriffen, um Warenlieferungen hochpreisiger Güter umzulenken. In dem Maße, in dem Ausweise mit biometrischen Merkmalen eingesetzt werden, werde sich nach Ansicht von Europol ein eigenständiger Markt für biometrische Informationen entwickeln, auf dem die OK einkaufe. Mit 93,5 Mio. Tonnen insgesamt werde der illegale Handel mit Elektroschrott laut Europol das wichtigste Betätigungsfeld der OK werden. Ausgehend von den Bewegungen der Indignados und von Occupy werde sich nach der Prognose von Europol eine Mischung entwickeln, in der sich die gewaltbereite Radikalisierung mit politischen Motiven mit den Marktmotiven der OK überschneiden und zusammengehen werde. Keith Bistrow von der National Crime Agency sehe die Verschlüsselung der Kommunikation als Problem polizeilicher Ermittlungen, verweise aber auch auf erfolgreiche Anstrengungen von Europol und GCHQ. Wissenschaftler machten in der Studie darauf aufmerksam, dass Big Data und Big Analytics auch verbesserte Erkenntnischancen für die Ermittler mit sich bringen.

Polizeiliche Kriminalstatistik (PKS)

In veko-online.de vom 2. April beurteilt Heinz-Werner Aping die PKS im Allgemeinen und die Entwicklung des Wohnungseinbruchs sowie seine statistische Darstellung im Besonderen. Sinkende Zahlen würden als Erfolg der entsprechenden landeseigenen Politik, steigende Zahlen als zwangsläufiges Ergebnis bundes- oder europaweiter Entwicklungen erklärt. Nach der Durchführung des Strafprozesses böte sich gegebenenfalls ein ganz anderes Bild der Kriminalität und vor allem ihrer erfolgreichen Bekämpfung. Trotz aller Vorbehalte sei die PKS ein sehr vielschichtiges und ausdifferenziertes Produkt geworden. 2013 seien beim Wohnungseinbruch 40,2 Prozent als versuchte Einbrüche registriert worden. Dieser Anteil sei in den letzten 15 Jahren tendenziell angestiegen (1993: 28,3 Prozent). Diese Entwicklung dürfte nach der Aussage in der PKS auf Verbesserungen der Sicherheitsmaßnahmen im privaten Bereich beruhen.

Für 2014 werde die PKS erstmals nach der Jahrtausendwende wieder eine deutliche Zunahme ausweisen, meldet WiK (Ausgabe 2-2015, S. 6). Nach Zusammenfassung der PKS aus 15 der 16 Bundesländer ergebe sich ein Anstieg um drei Prozent, sodass die registrierte Kriminalität nun wieder nahe dem Niveau von 2008 liege. Überdurchschnittliche Anstiege bei den Deliktzahlen habe es 2014 in Baden-Württemberg (3,2 Prozent), im Saarland (4,4 Prozent), in Sachsen (4,7 Prozent) und vor allem in Berlin (7,9 Prozent) gegeben. Nennenswerte Rückgänge seien in Mecklenburg-Vorpommern (3,2 Prozent) festgestellt worden.

Reisesicherheit

Klaus-Henning Glitza, Fachjournalist, gibt in der Ausgabe 5-2015 (S. 40/41) der Zeit-

schrift PROTECTOR **Sicherheitstipps für Geschäftsreisende**. Unter anderem rät er: Seien Sie achtsam gegenüber Personen, die sehr schnell Ihre Bekanntschaft schließen wollen! Müssen Sie mit dem Taxi fahren, steigen Sie nur dann ein, wenn Ihnen der Fahrer vertrauenswürdig erscheint! Wenn Sie auf Reisen Bargeld brauchen, bevorzugen Sie Bankschalter in gutsituierten Stadtteilen und meiden Sie Geldautomaten! Es ist sinnvoll, eine „Vorzeige-Geldbörse" dabei zu haben, die Bargeld, aber keine Personaldokumente enthält. Nehmen Sie einen USB-Stick mit, auf dem die Scans Ihrer Personalpapiere und – falls vorhanden – medizinische Unterlagen abgespeichert sind! Bevorzugen Sie bei der Auswahl eines Hotels größere Ketten, die im Allgemeinen Wachdienste unterhalten! Machen Sie niemals den Fehler, in einem Aufzug ganz nach hinten zu gehen! Personen, die zusteigen, könnten Ihnen so leicht den Fluchtweg abschneiden. Beim Einsteigen in das geparkte Fahrzeug sollte keine unnötige Zeit verloren gehen! Nehmen Sie bereits vor Verlassen des Hauses/Hotels den Autoschlüssel in die Hand! Bleiben Sie vor Ampeln immer auf den Außenspuren! Lassen Sie bei Stopps genügend Platz zum vorderen Fahrzeug, sodass Sie notfalls seitlich ausweichen können!

Rheinschifffahrtssicherheit

Noch heute sei der Rhein ein sehr sicherer Transportweg, schreibt die FAZ am 9. April. Auch für den Ernstfall gebe es ausgefeilte Havariekonzepte, mit denen fast immer das Schlimmste verhindert werden könne. Dennoch werde es wahrscheinlich noch über Jahre Sicherheitsprobleme geben. Vor allem aufgrund der Osterweiterung der EU, insbesondere der Öffnung des Arbeitsmarkts, strömten viele osteuropäische Matrosen und sogar einige Kapitäne auf den Rhein, die nicht mehr ausreichend eine der offiziellen Rheinsprachen Französisch, Deutsch oder Niederländisch beherrschen. Zudem hätten die zuständigen Behörden große Schwierigkeiten, zu überprüfen, ob die ihnen vorgelegten Fahrtenbücher und ähnliche Dokumente echt sind. Es gelte als ein offenes Geheimnis, dass man sich zur Zeit in Osteuropa alle Dokumente kaufen kann, die man haben möchte. Es bestehe daher die Gefahr, dass unerfahrenes oder gar unfähiges Personal die Schiffe führt. Das sei ein Problem, weil bei Unfällen die Kommunikation und die Streckenkenntnis mitentscheidend seien, ob es bei einem harmlosen Unfall bleibt oder zu einer Katastrophe kommt. Über 50 Prozent der Unfälle würden durch menschliche Fehler verursacht, die in vielen Fällen auf ein Verständigungsproblem zurückzuführen seien. Seit einiger Zeit steige die Zahl der Flusskreuzfahrtschiffe deutlich an. Eine Rettung von 300 Passagieren sei eines der Horrorszenarien. Die Wasser- und Schifffahrtsverwaltung des Bundes befinde sich zudem gerade in ihrer größten Reform seit Jahrzehnten, auch weil sie in den vergangenen Jahren viele Stellen einsparen musste.

Social Engineering

Udo Hohlfeld, „Intelligence Specialist", gibt in Security insight (Ausgabe 2-2015, S. 53) Tipps zum Umgang mit den Neuen Medien und Sozialen Netzwerken, unter anderem: Seien Sie zurückhaltend mit der Breite und Tiefe an veröffentlichten persönlichen Informationen! Machen Sie sich mit den Sicherheitseinstellungen der genutzten Endgeräte vertraut, die werksseitige Konfiguration ist nicht die optimalste für die Sicherheit! Veröffentlichen Sie keine unternehmensrelevanten Informationen oder Informationen über Kollegen! „Freundschaftsanzeigen" sollten Sie nicht leichtfertig akzeptieren! Klicken Sie nicht leichtfertig auf jeden angebotenen Link! Melden Sie vermehrte oder ungewöhnliche Kontaktversuche Ihrem Arbeitgeber!

Spionage

Das BfV rät in seinem Newsletter zum Wirtschaftsschutz in Ausgabe 1-2015 zu **Vorsicht bei China-Aufenthalten**. Für einen Anwerbungsversuch eines chinesischen Dienstes spielten verschiedene Kriterien eine Rolle. So seien gute Sprachkenntnisse, ein längerer Aufenthalt in China und eine berufliche Tätigkeit im Bereich Politik oder Diplomatie sowie ein Studium der Politikwissenschaften oder der Internationalen Beziehungen von Interesse. Auch eine Verbindung zu regimekritischen Organisationen oder NGO's beziehungsweise zu den nach Unabhängigkeit strebenden Tibetern oder Uiguren könne die Dienste aufmerksam machen. In der Regel erfolge die Ansprache einer Zielperson in China. Die Nachrichtendienstmitarbeiter träten unter Legende auf und schlügen zunächst eine Mitarbeit, beispielsweise in einem Forschungsprojekt, vor. Nachdem sich eine freundschaftliche Beziehung entwickelt hat, würden konkrete Aufträge erteilt. Fremde Nachrichtendienste würden auch mitunter gezielt nach kompromittierenden Ansatzmöglichkeiten suchen, um Zielpersonen zu einer Mitarbeit zu drängen. In derselben Ausgabe teilt das BfV mit, dass es 2014 mit dem VDMA eine engere Kooperation zu mehr Sicherheit in einer zentralen Branche der deutschen Wirtschaft verabredet habe, die in besonderem Maße innovativ und technologieorientiert ist und wesentlich zum Erfolg deutscher Unternehmen auf den Weltmärkten beiträgt. Diese Zusammenarbeit beinhalte eine Vielzahl an Aktivitäten für mehr Sicherheitsbewusstsein in einer vor allem durch mittelständische Unternehmen geprägten Branche.

Nach einer Meldung im Sonderbericht Wirtschaftsschutz der deutschen Sicherheitsbehörden des Bundes vom 17. April läuft seit Januar 2015 das vom BKA initiierte Projekt Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa (**WIASKOS**), das vom BMBF gefördert wird. In einem ersten Modul soll die bestehende Rechtslage analysiert werden. Im zweiten Modul werden die im Zuge des Länder-Screenings identifizierten Länder einer Mehrebenen-Evaluation unterzogen. Im dritten Modul wird eine erweiterte Dunkelfeldbefragung durchgeführt. Die Forschungsergebnisse sollen in marktfähige Sicherheitslösungen, in Beschaffungen, Handlungsstrategien und Organisationsformen, Vorschriften und rechtliche Rahmenbedingungen umgesetzt und als Leitfäden mit praktischen Handlungsempfehlungen und Informationsangeboten zusammengefasst werden.

Sandro Gaycken, European School of Management and Technology, nimmt am 29. April in der FAZ Stellung zu den Vorwürfen, der NSA habe mit Unterstützung des BND über bestimmte „Selektoren" auch die deutsche Wirtschaft ausspioniert. **Die Spionage der USA in der deutschen Wirtschaft** sei gerechtfertigt, im deutschen Interesse. Industriespionage sei zwar nicht ausgeschlossen, aber in diesem Fall unwahrscheinlich. Deutschland sei nun einmal einer der großen Exporteure an Rüstungsgütern, sicherheitskritischen Komponenten und Infrastrukturen nach Russland, China und in den arabischen Raum. Damit liefere es den Ländern die Werkzeuge. Das sollte im eigenen deutschen Interesse kontrolliert werden. Die USA würden in diesem Bereich weiter spionieren müssen. Sowohl die Politik als auch die Rüstungs- und Infrastrukturindustrie wüssten ohnehin, dass sie beobachtet werden, wenn sie Geschäfte mit Russland, China, Nordkorea und Iran machen. Wenn wir gleichzeitig den Weltfrieden erhalten und gefährliche Geschäfte in Ost und Süd machen wollen, müssten wir strategische Spionage an der Industrie als Fakt schlucken sowie als Anreiz zur Selbstkorrektur.

Terrorismus

Rechtsanwalt Nils Neumann nimmt in der Fachzeitschrift WiK (Ausgabe 2-2015,

S. 20–22) zu der Frage Stellung, inwieweit Unternehmen überprüfen müssen, ob **Mitarbeiter auf Terroristenlisten** der EU und der USA stehen. Tatsächlich gebe es keine ausdrückliche Pflicht zur Durchführung einer solchen Überprüfung. Wenn Verstöße gegen die EU-Verordnungen zur Terrorismusbekämpfung verhindert werden sollen, gebe es aber für Unternehmen faktisch keinen anderen Weg als eben auch die Mitarbeiter zu überprüfen. Zu beachten seien so etwa die Antiterrorismus- sowie die Al Qaida-Verordnungen oder auch Embargo-Regelungen wie die Syrien- und die Iran-Verordnung. Schon Fahrlässigkeit könne zur Begründung der Verstöße gegen die EU-Verordnungen genügen. Und genau hieraus folge die faktische Pflicht zur Überprüfung. Die Verbote in den Verordnungen gelten gleichermaßen für Arbeitnehmer, Freelancer, Azubis, leitende Angestellte, Geschäftsführer oder auch Vorstände. Da auch das mittelbare Bereitstellen verboten ist, werde zum Teil sogar für eingesetzte Leiharbeitnehmer und solche, die im Rahmen von Werkverträgen tätig sind, eine Mitverantwortung angenommen.

Transportdiebstahl

Der ASW informierte am 5. und 14. April über folgende Tatorte aktueller Planen-Schlitzereien und sonstiger Ladungsdiebstähle auf Fahrstrecken im Bundesgebiet:

- 23./24. 3., Potsdam, A 115, Parkplatz Parforceheide zwischen Potsdam-Babelsberg und Kleinmachnow
- Nacht zum 25. 3., Autohof Großweitzschen
- 25./26. 3., A 5 Alsfeld, Rastanlage Pfefferhöhe
- 30./31. 3., A 5, Bühl, BAB-Parkplatz Oberfeld
- 31. 3./1. 4., Spremberg, Industriepark Schwarze Pumpe, Dresdener Chaussee
- 2. 4., Neubodenfach Industriegebiet, Maxi-Autohof Nossen
- 2.–7. 4., Weiden, Holzverladestation Dr.-Seeling-Straße
- Nacht zum 8. 4., A 4, Parkplatz Eichelborn und Parkplatz Teufelstal
- 5./6. 4., Bernburg, Kalistraße
- 10./11. 4., Brandenburg an der Havel, Parkplatz Max-Josef-Metzger-Straße
- 14./15. 4., Hörsel, OT Laucha, Gewerbegebiet; Schwabhausen, Rastplatz „Thüringer Tor" und Tankstelle in Drei Gleichen, OT Mühlberg
- 15. 4., A 72, Plauen-Stöckigt, Parkplatz Vogtland Nord
- 16./27. 4., A 72, Oelsnitz, Parkplatz Beuthenbach
- 17./18. 4., A 38, Parkplatz Eichsfeld

Thorsten Neumann, Transported Asset Protection Association (TAPA EMEA), nimmt in der Ausgabe 2-2015 der Fachzeitschrift WiK, S. 16/17, Stellung zu den **Gefahren für die Frachtlogistik**. 2014 habe Deutschland mehrfach die „Hitliste" in Bezug auf die Anzahl der Diebstähle und der Schadenshöhe angeführt. Als einen der größten Risikofaktoren habe TAPA erneut den Mangel an ausreichend sicheren und bewachten Parkplätzen identifiziert. Für die Zukunft habe TAPA eine weiter wachsende Anzahl an Frachtdiebstählen in Deutschland prognostiziert. In der gesamten EMEA-Region wurden 1.102 Frachtdiebstähle mit einem Gesamtschaden von 74,8 Mio. Euro registriert. Die „beliebtesten" Produkte seien Nahrungsmittel und Getränke, Kleidung, Kosmetika, Computer-Equipment, Konsum-Elektronik, Autoteile, Pharmazeutika und Tabakwaren.

Transportsicherheit

Dipl.-Ing. Georg Mayer und Susanne Großmann, PTV Transport Consult, und Ingo Kaundinya, Bundesanstalt für Straßenwesen, befassen sich in Ausgabe 2-2015 der Fachzeitschrift WiK (S. 28/29) mit der Abwehr von Gefahren für das europäische Verkehrsnetz. Tunnel und Brücken seien die Risikostellen.

Das von der EU geförderte internationale **Forschungsprojekt SeRoN** (Security of Road Transport Networks) konzentriere sich auf die Untersuchung möglicher Anschläge auf das gesamte Verkehrsnetz. Im Rahmen des Projekts sei eine innovative Methode entwickelt worden, wie Straßennetze und die darin befindlichen Infrastrukturbauwerke im Hinblick auf ihre Gefährdung analysiert und bewertet werden können. Die untersuchten Sicherheitsmaßnahmen hätten sich als eher kostenwirksam erwiesen, wenn diese in unterschiedlichen Szenarien Anwendung finden und ihre Wirkung sowohl im Bereich der zivilen Sicherheit als auch im Bereich der Verkehrssicherheit und der Verkehrsoptimierung entfalten.

Tresorsicherheit

Wie WiK in der Ausgabe 2-2015, S. 56, berichtet, bieten die VdS-geprüften und ECB-S-zertifizierten Möbeltresore der Serie Diplomat jetzt gleichzeitig zum Einbruchschutz (Widerstandsgrad 1 nach EN 1143-1) auch Schutz gegen Feuer (Güteklasse LFS 60 P nach EN 15659). Burg-Wächter habe hierzu einen neuartigen Aufbau für Korpus und Tür entwickelt.

Unternehmenssicherheit

In der Ausgabe 2-2015 der Fachzeitschrift WiK werden die Ergebnisse der Befragung von 160 Managern der Corporate Security zur **Sicherheits-Enquete 2014/2015** wiedergegeben (S. 10–14). Die Gefährdung von Informationstechnik und Unternehmensdaten sei für die Sicherheitsexperten in der Wirtschaft nach wie vor die gravierendste Herausforderung. Mehr als zwei Drittel gehen davon aus, dass die Belastungen durch Angriffe auf IT und Telekommunikation künftig weiter wachsen werden. Entsprechend wüchsen auch die Sicherheitsbudgets. 79 Prozent rechnen mit mehr Aufwendungen für die IT-Sicherheit. Mehr als drei Viertel wünschten sich mehr behördliches Engagement bei der Bekämpfung der Cybercrime. Auch bei der Entwicklung von Extremismus/Terrorismus sowie bei der Ausspähung rechne eine Mehrheit der Sicherheitsexperten mit einem Anstieg der Gefährdung. In den letzten 24 Monaten seien 84 Prozent der Befragten mindestens einmal mit einem Diebstahl, 78 Prozent mit einem „Zeitdiebstahl" von Mitarbeitern, 71 Prozent mit einem Einbruch, 70 Prozent mit einem Mitarbeiterdelikt (zum Beispiel Untreue) konfrontiert gewesen. In der Bewertung der Notwendigkeit einzelner IT-Sicherheitsmaßnahmen nehmen Firewalls, Virenschutzprogramme, Brandmeldetechnik in Serverschränken und -räumen, Authentisierung beim Zugriff und sichere Datenträgerlagerung die vorderen Plätze ein. Nur 46 Prozent haben ein Konzept zum Know-how-Schutz (weitere 16 Prozent würden ein solches Konzept planen). Dabei gingen 49 Prozent aller Befragten für 2015 im Vergleich zum Vorjahr von höheren Ausgaben für den Know-how-Schutz aus. Nur 29 Prozent haben in Wirtschaftsschutzfragen schon Kontakt zum Verfassungsschutz aufgenommen. Und nur 23 Prozent antworteten, sie wüssten, dass die Bundes- und Landesbehörden Beratung und Sensibilisierungsmaßnahmen im Wirtschaftsschutz anbieten. Für 2015 meldeten 42 Prozent der Sicherheitsmanager ein gestiegenes Budget an, und für 2016 erwarteten 40 Prozent wieder ein reales Wachstum. 67 Prozent der Sicherheitsmanager berichteten von Einsparmaßnahmen seit 2013, zumeist (44,4 Prozent) Ersatz von personellen Leistungen durch Technik, 33,3 Prozent durch Fremdvergabe von Aufgaben. Aktuell verteilten sich die Budgets in der Unternehmenssicherheit im Durchschnitt so, dass auf Sachkosten, eigenes Personal und fremdes Personal jeweils ca. ein Drittel entfällt. Als Technologien, in die bis Ende 2017 investiert werden soll, wurden in erster Linie genannt: Biometrie (33,3 Prozent), Elektronische Schließtechnik und Videoüberwa-

chungstechnik (30,8 Prozent), Alarmierungssysteme und Verschlüsselungstechnik (28,2 Prozent), elektrischer Perimeterschutz (25,6 Prozent). Für 2015 bis 2017 sollen jährlich ca. 700.000 Euro für Investitionen bereitstehen, je Mitarbeiter im Durchschnitt jährlich 176 Euro pro Jahr. Knapp 30 Prozent der befragten Unternehmen schrieben Neuanschaffungen von Sicherheitstechnik nie oder nur gelegentlich aus. Bei der Wahl zwischen den Anbietern spielten Zertifikate eine wichtige Rolle, und zwar in folgender Reihenfolge: VdS-Anerkennung, nach DIN gefertigt, TÜV-Zulassung, BSI-zertifiziert, BHE-Gütesiegel, RAL-geprüft.

In derselben Ausgabe der WiK berichtet Dipl.-Ing. Robert Eck, r.o.l.a. Business Solutions GmbH, über die **6. Anti-Fraud-Management-Tagung des DIIR**, bei der der Technologiewandel und die damit einhergehenden Angriffsszenarien, die Digitalisierung, der Know-how-Schutz und die Nutzung digitaler Daten für „Internal Investigations" wichtige Themen gewesen seien (S. 28–30). Staatlich gelenkte Angriffe gegen deutsche Firmen zielten überwiegend auf die Bereiche Automobil, Raumfahrt, Rüstung, erneuerbare Energien, Hochtechnologie, IT, neue Werkstoffe, Biotechnologie und Energieeinsparung. Das Thema IT-Sicherheit mit den Komponenten Datenschutz und Datensicherheit finde zunehmend Berücksichtigung bei der Entwicklung der ganzheitlichen Risk-Managementmaßnahmen. Problematisch sei aber, dass die Einführung neuer Technologien in den diversen Unternehmensprozessen voranschreitet, ohne dass im gleichen Tempo über wirksame und angemessene Sicherheitsmaßnahmen eine effiziente Risikosteuerung erreicht werden könne.

Verschlüsselung

Verschlüsselung bleibe „erste Wahl" der digitalen Selbstverteidigung, ist Thorsten Sprenger, Kenthor GmbH, überzeugt (WiK, 2-2015, S. 23/24). Neben der strategischen Schwächung von Verschlüsselung setzten Geheimdienste neuerdings auch auf sogenannte Implantate. Sie ähnelten klassischen Trojanern, auch wenn sie deutlich ausgefeilter und komplexer seien. Der Arbeitskreis Datensicherheit und Verschlüsselung des Bayerischen IT-Sicherheitsclusters habe praxisnahe Musterkonzepte entworfen, die – zurechtgeschnitten für das jeweilige Unternehmen – schnell und kostengünstig Maßnahmen definieren, die eine sofortige Verbesserung des Schutzniveaus ermöglichten. Leider gebe es keine einzelne, alles schützende Form der Verschlüsselung. Die Zukunft werde neue Formen bringen: Softwareprodukte, die von sich aus sicher konstruiert wurden und dennoch für jeden einfach zu bedienen sind.

Videoüberwachung

PROTECTOR gibt in der Ausgabe 4-2015 (S. 26/27) eine **Marktübersicht über Monitore** von 33 Anbietern mit 92 Produkten. Abgefragt werden 52 Kriterien, unter anderem aus den Bereichen Zertifizierungen, Auflösung, Betrachtungswinkel, Schwenkbereich, Sicherheitseinrichtungen, Preis.

Videosicherheitslösungen im Retailbereich stellt Thomas J. Achter, Dallmeier, in vekoonline.de am 2. April vor. Der Schwerpunkt bei den Retaillösungen liege in der präventiv sichtbaren Installation von hochauflösenden Kameras mit aktivitätsbezogener Digitalaufnahme, die potenzielle Täter schon vor einer Tat abschrecken. Je nach Anforderung und entsprechend der Bildszene und der Details, die man erkennen möchte, müsse eine Vielzahl von Pixeln am Objekt bzw. an der Person im Bild vorhanden sein. Mit sogenannten Multifocal-Sensorsystemen könne man mehrere herkömmliche Megapixel- bzw. HD-Kameras ersetzen, und das von nur einem Installationspunkt aus. Eine integrierte Bewegungserkennung in den Aufzeichnungs-

servern sorge für eine effiziente Auslastung der Festplattenkapazität. Erheblichen Mehrwert biete die Videokamera, wenn sie mit anderen informationsgebenden Gewerken wie Einbruch- und Brandmeldesystemen, Zutrittskontrolle, Tür- und Torkontakten, Barcode-Scannern, Kassen oder Bezahlautomaten gekoppelt wird.

In mehreren Beiträgen thematisiert GIT in der Ausgabe 4-2015 die Videoüberwachung. Katharina Geutebrück befasst sich mit der **Redundanz bei Hardware und Software** (S. 50–52). Der Hersteller Geutebrück biete je nach Rekorderserie folgende Komponenten standardmäßig oder optional in redundanter Ausführung an: Netzteil, Lüfter, Netzwerkanbindung, Festplatten, RAID(Redundant Array of Independent Disks)-Controller und Solid State Disks für das Betriebssystem. Sollten dennoch ein Gerät oder mehrere Geräte komplett ausfallen, würden Failover(Ausfallsicherungs)-Konzepte vorbeugen, die dank intelligenter Steuerung durch die Software die Verfügbarkeit sichern. Bei der Variante NVFR-Failover „n+1" würden die Primärrekorder durch mindestens einen zusätzlichen Standby-Rekorder ergänzt. Multicast-Failover zeichne gleichzeitig alle Kamera-Streams auf mindestens zwei Rekorder via Multicast auf. Dadurch werde eine zusätzliche Belastung des Netzwerks vermieden. Bei der virtualisierten Lösung für die Server-Hardware würden auf einem größeren physikalischen Rechnerverbund aus (meist) hochredundanten Servern „virtuelle Rekorder" installiert, die für das Videosicherheitssystem wie eigenständige Geräte arbeiten. Zur Systemüberwachung überprüfe das Videoanalyseverfahren „Scene Validation" in regelmäßigen Abständen automatisch, ob alle Kameras die vordefinierte Szene überblicken und ob die Bildqualität noch stimmt. „Health Monitoring" gehe noch einen Schritt weiter und erlaube sogar das präventive Eingreifen.

In derselben Ausgabe präsentiert GIT mit zwei neuen **Netzwerkkameras von Digital Data Communications** sicherheitsrelevante Komponenten für den professionellen In- und Outdoor-Einsatz. Während die Kuppelkamera FCS-3102 ihre Stärken vor allem in der Überwachung von Eingangsbereichen und Lagern ausspiele, kämen die Vorteile der PoE-fähigen Zoomkamera FCS-5043 insbesondere in Außenbereichen großflächiger Gelände zum Tragen (S. 53).

Axis Communications befasst sich mit dem **Störfallmanagement im öffentlichen Verkehrssystem** (S. 56/57). Video in Echtzeit erlaube es, bereits bei Erkennen eines Zwischenfalls Maßnahmen einzuleiten. Sowohl die Hersteller von Physical Security Information Management-Software (PSIM) als auch von Video Management Systemen (VMS) böten professionelle Störfall-Managementmodule an, die sich mit modernen digitalen Kamerasystemen integrieren lassen. Besonders hilfreich sei, dass die Videobilder auch auf mobilen Geräten zur Verfügung stehen. Wenn öffentliche Verkehrsbetriebe planen, ältere Sicherheitssysteme nachzurüsten, sollten sie auf ein zentralisiertes Sicherheitssystem mit Echtzeit-Funktionen setzen. Das Ziel sollte sein, das gesamte Verkehrssystem mit einem zentralen Sicherheitszentrum zu verbinden.

In mehreren Beiträgen in der Ausgabe 2-2015 der Fachzeitschrift WiK wird die Videoüberwachung thematisiert. Axis prognostiziert **für 2015 die wichtigsten Trends** der Videoüberwachung: Wachstum bei Video Surveillance as a Service (VSaaS); Analysetechniken, die dafür sorgen, dass der Nutzer die richtigen Daten zur richtigen Zeit erhält; und der neue Videokomprimierungs-Standard H.265 (S. 46). Dipl.-Ing. Helmut Manthey befasst sich mit der **4K-Technologie**, die eine viermal höhere Auflösung als HDTV 1080p biete (S. 49–51). Unterstützt werde die Entwicklung durch ein schnell wachsendes Angebot an kostengünstigen Wiedergabegeräten, etwa 4K-Monitore. So ließen sich große Flächen wie Parkareale, Einkaufszeilen,

Industrie-, Bahnhofs- oder Wartehallen mit nur einer Kamera detailgenauer überwachen. Der Hersteller Bosch habe auf die Möglichkeit hingewiesen, auf einem Bildschirm eine Weitwinkel-Übersicht und gleichzeitig mehrere Fokuspunkte darzustellen. Eine wichtige Rolle im Bereich Megapixel-Auflösungen spielten die eingesetzten Objektive. Ein hochauflösender Bildsensor benötige auch ein hochauflösendes und lichtstarkes Objektiv. Beim Einsatz von IP-Kameras, die mit erheblichen Datenströmen arbeiten, seien zwei wesentliche Aspekte zu beachten: Erforderlich sei die exakte Erfassung jedes einzelnen Bildes mit mindestens 16 Bildern/Sekunde. Und Netzwerkkameras benötigten Netzwerkressourcen. Unter der Annahme einer Überwachungsanlage mit 20 IP-Kameras würde ohne eine entsprechende Technologie zur Datenreduzierung das zu erwartende Datenvolumen schnell die Ressourcen eines Fast-Ethernet-Netzwerkes auslasten. Das bisher eingesetzte Kompressionsverfahren H.264 werde nicht mehr ausreichen und könnte durch H.265 ersetzt werden. Axis setze bei seinen neuesten Netzwerkkameras und Video-Encodern auf den Einsatz von Speicherchips zur lokalen Aufzeichnung der Bilddaten. Die Aufzeichnungen verblieben in der Kamera und könnten von der Auswerteanwendung zeitgesteuert oder zum benötigten Zeitpunkt per Download geholt werden.

Jochen Sauer, Axis Communications, befasst sich mit der **„Video-Norm" DIN EN 50132-7** (S. 52/53). Teil 7 decke bei den CCTV-Überwachungsanlagen alle Bereiche ab, von der Entwurfsplanung bis zum Betrieb. Als essentieller Leitfaden für die technische Planung gebe sie Empfehlungen zur Auswahl, Planung, Installation sowie Inbetriebnahme und Wartung. Zudem unterstütze sie Fachplaner und Benutzer bei der Festlegung der geeigneten Anlagenteile einer Videoüberwachungsanlage, die für eine vorgegebene bzw. gewünschte Anwendung des Sicherheitssystems erforderlich sind. Dies geschehe einerseits durch eine Checkliste für die Kriterien zur Auswahl der Kamera/Objektive und Gehäuse sowie über allgemeine Hinweise zur Betriebszentrale. Ebenfalls würden Mittel zur objektiven Bewertung der Eigenschaften der CCTV-Anlage bereitgestellt. Die aktualisierte Fassung, für die die Übergangsfrist am 17. Juni 2015 abläuft, trage den technischen Innovationen im Bereich Videosicherheitstechnik Rechnung. Welche Kameraauflösung für welche Überwachungsszene notwendig ist, sei eine komplexe Entscheidung. Zuerst müsse die Frage nach dem Einsatzzweck beantwortet werden: Identifikation oder Übersichtsfunktion? Beide Zwecke dürften prinzipiell nicht vermischt werden. Auch für den Datenschutz biete die Norm eine existenzielle Hilfestellung. Sie gehe insgesamt auf die Bedürfnisse der Facherrichter und Planer ein und spreche „die Sprache der Branche".

Security insight gibt in Ausgabe 2-2015 Themen aus dem Bereich Videoüberwachung ebenfalls breiten Raum. Simone Gerrits, Mobotix, stellt ein **Videosicherheitssystem für ein Hochregallager** mit 18.000 Paletten vor (S. 20/21). Für die Regalbediengeräte im vollautomatisierten Hochregallager bedeute jedes noch so kleine Hindernis, etwa ein Stück flatternde Folie, Stillstand. Ausgestattet mit zwei hemisphärischen Objekteinheiten ermögliche die Kamera S14D von Mobotix eine 360 Grad-Rundumsicht ohne toten Winkel. Um die Bilddaten ins Unternehmensnetzwerk zu übertragen, sei ein Ethernet-System installiert worden. Das Infrarot-Datenübertragungssystem ermögliche die drahtlose Kommunikation und sende die Informationen in Echtzeit vom mitfahrenden Gerät. Der Vorteil liege vor allem im dezentralen Konzept, das die Speicherung der Aufnahmen in der Kamera selbst erlaubt. Bertrand Völckers, FLIR Systems GmbH, erklärt, warum der Betreiber eines **Solarparks** in Wärmebildkameras investiert (S. 24/25). Bei einer zehn Kilometer langen Umzäunung seien Boden- und Zaunsensoren aus Kostengründen nicht in Frage gekommen. Wegen fehlender Beleuchtung seien 110 Wärmebildkameras die beste Wahl

gewesen. Das Livebildmaterial werde über Glasfaserkabel zu einem lokalen Encoder transportiert und dann über ein lokales Netz zu einem Server im Kontrollraum übertragen, auf dem die Videoanalyse-Software Evitech läuft. Da der thermische Kontrast zwischen einer Person und ihrer Umgebung sogar tagsüber im Allgemeinen viel größer sei als der Farbkontrast, könne die Analyse-Software unbefugte Personen auf Wärmebildern exakter erkennen. Durch den höheren thermischen Kontrast verringere sich auch die Anzahl der Fehlalarme. In derselben Ausgabe von Security insight wird das Videoanalyse-Modul **„IPS Public Transport Protection"** vorgestellt (S. 42/43). Intelligente Videobildanalyse-Software erkenne heute weitgehend fehlerfrei Ereignisse wie Gleisbetteintritte, Personen in Tunneln oder Abstellanlagen, Vandalismus, abgestelltes Gepäck, herumlungernde Personen, Graffiti-Sprayer und Zaunübertritte. Die Software beherrsche auch schwierige Situationen: Schwache Beleuchtung, Nebel, Regen, Schnee, Scheinwerfer-Blendungen von Fenstern, Pfützen und Autos – immer bessere Algorithmen erhöhten die Präzision. Die intelligente Wiedergabesteuerung moderner Videomanagement-Software gestatte es, mit Maus und Tastatur die Bilder zahlreicher Kameras synchronisiert auf einem Zeitstrahl zu betrachten. Ein Rückwärts-Tracking von Personen sei ebenfalls möglich.

Wohnungseinbruch

Welt.de berichtet am 9. April, in welchen Bundesländern Einbrecher am häufigsten „zugeschlagen" haben: Die HZ (Zahl der Einbrüche je 100.000 Einwohner) betrug in Bremen 465, in Hamburg 429, in Berlin 355 und in NRW 300. Die Bundesländer hätten 2014 einen durchschnittlichen Anstieg der von der Polizei erfassten Einbruchdelikte um rund zwei Prozent registriert. Der Zuwachs sei in Bayern mit 28,6 Prozent am höchsten gewesen. Den stärksten Rückgang habe Thüringen mit 11,3 Prozent gemeldet. Für die steigenden Zahlen mache der Bundesinnenminister vor allem die Zunahme der internationalen Bandenkriminalität verantwortlich. Wie eine Förderung des Einbruchschutzes steuerlich oder über Förderprogramme erfolgen könne, werde derzeit geprüft.

Die KfW unterstützt, wie GIT in seiner Ausgabe 4-2015, S. 23, berichtet, Vorsorgemaßnahmen zum Einbruchschutz. Sie fördere den Einbau einbruchhemmender Haus- und Wohnungstüren sowie diverser Nachrüstprodukte, wie z. B. Sonderverriegelungen, Zusatzschlösser oder Bewegungsmelder. Rund 44 Prozent der Täter scheiterten inzwischen an vorhandener Sicherungstechnik.

Die Zahl der Wohnungseinbrüche in Deutschland steigt, meldet die FAZ am 14. April. Sie nehme seit etwa 2006 stetig zu. Der höchste Zuwachs sei 2009 registriert worden. 2014 registrierten die Bundesländer einen Anstieg von rund zwei Prozent auf 152.000 Fälle. Die Täter teile die Polizei in drei Gruppen: Gelegenheitsdiebe, Drogenabhängige und professionelle Banden aus dem Ausland. In Bayern seien 43 Prozent der 2014 gefassten Einbrecher Ausländer gewesen, meist aus Rumänien, Serbien, Polen, Bosnien-Herzegowina und Georgien.

Zufahrtskontrolle

Security insight macht in der Ausgabe 2-2015, S. 27, auf ein **neues Lichtgitter für Industrietore** aufmerksam, das direkt mit dem am Tor eingesetzten Positionswertgeber verbunden ist. Bei jeder Torfahrt vergleiche das Lichtgitter die Belegung jedes einzelnen Lichtstrahls mit der vom Geber ermittelten Referenzposition des Torblatts, blende diese aus und schaffe so höchste Sicherheit. Eine Besonderheit sei die Fähigkeit, das Tor in Abhängigkeit der Gefährdungslage entweder hart oder weich zu stoppen. Dazu unterteile

das Lichtgitter seinen Erfassungsbereich in einen „Gefahren-" und einen „Objektschutzbereich". Das neue Lichtgitter sei auch mit der Torsteuerung verbunden. Dadurch stünden dem Torbetreiber zahlreiche Zusatzoptionen zur Verfügung, etwa Diagnosemöglichkeiten, Aus- und Einrichthilfen bei der Installation der Lichtgitter in der Torzarge sowie die Möglichkeit der Anpassung an die jeweiligen „Torgegebenheiten".

Zutrittskontrolle

In der Ausgabe 4-2015 der Zeitschrift PROTECTOR, S. 30/31, wird das elektronische Schließsystem für **Wohnheime einer Universität** vorgestellt. Es basiert technologisch auf dem Salto Virtual Network (SVN) mit patentierter Schreib/Lese-Funktionalität und verschlüsselter Datenübertragung. Im SVN würden die Informationen zu den Schließberechtigungen auf dem Identmedium gespeichert, wodurch eine Verkabelung der elektronischen Beschläge und Zylinder entfalle. Gleichzeitig würden auch Informationen über gesperrte Identmedien oder beispielsweise Batteriestände in den Beschlägen und Zylindern auf die Identmedien geschrieben und somit weitergegeben. Die Online-Wandleser übertragen die ausgelesenen Daten an den zentralen Server und übermitteln gleichzeitig die aktuellen Schließberechtigungen. Durch die Programmierung einer „Zuschließfunktion" würden die Türen praktisch aktiv verschlossen. Die Karten seien mit einem Mifare Desfire EV1 Chip bestückt.

Veko-online.de stellt am 2. April die **Personenvereinzelung Galaxy Gate** mit der INTUS PS Handvenenerkennung vor. Die INTUS PS Zutrittskontrolle verifiziert den Kartennutzer sicher und eindeutig. Bei Missbrauch reagiert die Vereinzelungsanlage mit optischen und akustischen Warnsignalen. Das Verfahren sei schnell, im Vorübergehen bedienbar und höchst hygienisch. Das Galaxy Gate sei die ideale Lösung für Eingangsbereiche mit hoher Besucherfrequenz und zugleich maximalen Sicherheitsanforderungen.

Mit **intelligenten Zugangskontrollsystemen in öffentlichen Verkehrssystemen**, die den Passagierfluss steuern und zugleich die Ticketkontrolle ermöglichen, befasst sich Albert Schürstedt, Gunnebo Deutschland GmbH, in Security insight, Ausgabe 2-2015, S. 44/45. Um den unterschiedlichen Belastungen im Alltag standzuhalten, seien individuelle Lösungen etwa in der Durchgangsbreite, behindertengerechte Ausführungen und Lesesysteme für verschiedene Tickettypen notwendig. So können die Systeme vor Schwarzfahrern schützen und Passagierströme effizient lenken. Die Abläufe bei der Einreisekontrolle an der Grenze ließen sich durch biometrische Erkennungssysteme optimieren. Die Basis dafür schafften Reisedokumente mit biometrischen Daten, die bis 2016 EU-weit verpflichtend sind.

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

E-Mail: info@securitas.de