Focus on Security

Ausgabe 07, Juli 2015

SECURITAS

Inhalt

Arbeitsschutz

Aus aktuellen Daten der Verwaltungs-Berufsgenossenschaft ergibt sich nach einer Meldung von haufe.de vom 19. Juni, dass sich rund 36,5 Prozent Stolper-, Rutsch- und Sturzunfälle in der Sicherheitsdienstleistung und hier vor allem beim Werk- und Objektschutz ereignen. Hoch sei mit rund 31,5 Prozent auch die Zahl der Konfrontationsunfälle, allerdings seien hiervon vor allem Warenhausdetektive sowie Kontroll- und Ordnungsdienste betroffen.

Bankensicherheit

Spezielle Aspekte der **Videoüberwachung und Zutrittskontrolle** für die Sicherung von Banken werden in der Ausgabe 6-2015 der Zeitschrift GIT (S. 100/101) behandelt. Es empfehle sich, in den Geldautomaten geteilte Kameras zu verbauen, bei denen sich Prozessor, Netzwerk-, Strom- und weitere Anschlüsse in einem separaten Gehäuse befinden, das über ein Kabel mit der Sensoreinheit verbunden ist, die sich aus Objektiv- und Bildsensor zusammensetzt. Dieses Konzept ermögliche die unauffällige Installation kleiner Sensoreinheiten an engen Stellen, wodurch Beschädigungen und Manipulationen an Automaten gezielt nachverfolgt werden können. Um trotz widriger Umstände gute Aufnahmen zu erhalten, sei die Verwendung einer Kamera mit Side Dynamic Range unabkömmlich. Axis Communication gehe mit ihrer WDR-Forensic Capture Technologie noch einen Schritt weiter. Die Rauscheffekte im Bild würden stark reduziert und die Bildsignale weiter verstärkt. Geeignet für unkomplizierte Zutrittsregelungen seien IP-basierte Zutrittskontrollsysteme.

Betrug

Die Maschen beim **Telefonbetrug** wechselten ständig und zeigten eine unglaubliche Vielfalt, schreibt die FAZ am 13. Juni. Beliebt seien auch betrügerische Gewinnspiele oder Gewinnversprechen am Telefon. Die Anrufe erfolgten überwiegend aus Call-Centern in der Türkei. Sei eine erste Zahlung erfolgt, müsse das Opfer damit rechnen, nochmals angerufen zu werden. Das BKA beziffere die Zahl der bis April 2014 insgesamt durch Telefonbetrug Geschädigten auf rund eine Million, wobei es hier allein um Gewinnspiele ging. Der Schaden habe sich damals auf 117 Mio. Euro belaufen.

Henning Glitza, Fachjournalist, befasst sich in der Juniausgabe von Veko-online mit Lkw-**Ladungsbetrug** und -Unterschlagung. Rund 70 Prozent der betroffenen Unternehmen sähen einen unmittelbaren Zusammenhang zwischen den Täuschungsdelikten und der Nutzung von Internet-Frachtbörsen. Der Trick der Kriminellen bestehe darin, dass sie überwiegend im östlichen Ausland Scheinfirmen gründen, die kaum aus mehr als einem Briefkasten, einem Handy und einem Briefkopf bestehen. Diese gefakten Unternehmen würden sich in die Frachtbörsen einklinken und mit Dumpingpreisen locken. Entweder schickten die Gangster einen eigenen Lkw, der häufig mit falschen Kennzeichen und Papieren ausgestattet sei. Oder sie setzten andere Frachtführer als Subunternehmer ein. Scheinfirmen nutzten meistens Prepaid-Handys statt Festnetztelefone und Free-Mail-Adressen. Andere Ganoven schlüpften unter den Deckmantel einer bestehenden Firma. Kontakt zu den Opfern werde mit dem original wirkenden Briefbogen der Firma hergestellt, wobei die tatsächliche Rufnummer durch eine Handynummer ersetzt werde.

BOS-Digitalfunk

Der G7-Gipfel stellte den Digitalfunk für Behörden und Organisationen mit Sicherheitsaufgaben (BOS) europaweit vor seine bislang größte Herausforderung, heißt es in einer Pressemitteilung des Bayerischen Innenministeriums vom 8. Juni. Auch unter Volllast und bei Unwetter habe die Technik einwandfrei funktioniert. Über den gesamten Einsatz hinweg seien deutlich mehr als 30.000 verschiedene Einsatzgeräte genutzt worden – an einer Basisstation mitunter bis zu 7.500 Endgeräte zeitgleich. Ob Polizei, Feuerwehr oder Rettungsdienst – alle Einsatzkräfte seien mit dem BOS-Digitalfunk mehr als zufrieden gewesen. Der Aufbau des Digitalfunknetzes befinde sich in Bayern nun in seiner Schlussphase. Ab dem Jahr 2016 werde der Digitalfunk allen BOS in Bayern zur Verfügung stehen.

Brandschutz

In der Ausgabe 3/2015 der Fachzeitschrift Security insight befassen sich mehrere Beiträge mit Brandschutzthemen: Vorgestellt wird das **Brandforschungszentrum** des Industrieversicherers FM Global, in dem Industriebrände mit einer Wärmefreisetzung von bis zu 1.000 Grad Celsius im Originalmaßstab nachgestellt werden können (S. 22/23). FM Global habe auf Basis von Forschungsergebnissen eine spezielle Sprinklerdüse entwickelt, die „resistent" gegen viele in der Industrie erzeugte korrosive Gase ist. Joachim Meisehen, Esser Systems, behandelt **Rauchansaugsysteme** für Industriestandorte, Flughäfen, Lagerhäuser, Einkaufszentren, Kraftwerke und Nuklearanlagen (S. 24/25). Vorgestellt wird das Rauchansaugsystem FAAST 8100E von Honeywell für die Klassen A, B und C gemäß EN 54-20 mit den Eigenschaften doppelter Filter, doppelte Optik, doppelte Intelligenz und exakte Kategorisierung. Heidi Burow-Strathoff, G+H Isolierung GmbH, beschreibt Brandschutzlösungen für **Flucht- und Rettungswege.** Klassifizierte Elektroinstallationskanäle (I-Kanäle) seien als Abschottungsmaßnahme in der Wanddurchführung und Brandlastenkapselung im Rettungsweg das optimale Brandschutzprodukt für Neubauten und habe sich über Jahrzehnte bewährt. G+H habe 2007 einen Installationskanal entwickelt und geprüft, der aus einem Blechkanal besteht, in dessen Innerem ein Dämmschichtbildner aufgebracht ist. Dieser reagiere aktiv bei Hitze, schäume auf, schmiege sich wie eine innen liegende Isolierung an die Kabel und Rohre und verhindere damit eine Brandweiterleitung im Inneren des Kanals. Er sei schnell und einfach zu montieren. Ralf Jock und Joachim Schütz, Siemens Buildings Technologies, befassen sich mit dem technischen **Brandschutz in Produktionsumgebungen** (S. 28/29). Mit großvolumigen Räumen und vielfältigen Störgrößen stellten Produktionsbereiche besonders komplexe Anforderungen an den technischen Brandschutz. Eine parametergestützte Branddetektion mit punktförmigen Meldern liefere in diesem Zusammenhang optimale Ergebnisse für geringe und mittlere Raumhöhen. Ansaugrauchmelder der neuesten Generation böten nun auch für größere Höhen detektions- und täuschungssichere Alternativen zu den bisher eingesetzten Systemen. Simon Trippler behandelt den technischen **Brandschutz für Kraftwerke** (S. 31/32). Die Brandszenarien seien für die Bereiche Materialanlieferung, Transport und Lagerung zu unterscheiden. Thermalkameras ließen sich überall dort einsetzen, wo heiße Oberflächen oder offene Flammen detektiert werden sollen. Zudem würden sie eine Lösung für offene Bereiche oder hohe Hallen darstellen. Auch um Glutnester auf Förderbändern zu erkennen, habe sich die Thermografie bewährt. Zur Früherkennung von Schwelbränden entlang eingehauster Bandanlagen habe sich der Brandgasmelder

etabliert. Ein zentraler Punkt sei die Art der Einbettung der Sondermeldetechnik in das brandschutztechnische Gesamtkonzept.

In der Ausgabe 6-2015 der Zeitschrift GIT stellt Peter Holzamer, Prymos GmbH, ein Kombi-Konzept aus **Feuerlöscher-Sprays** und leichten Composite-Feuerlöschern vor (S. 109–111). Bei Bekämpfung von Entstehungsbränden gemäß ASR A2.2 sei der Zeitfaktor der Wesentlichste. Intuitiv bedienbare und hochmobile Feuerlöscher in Spraydosen – möglichst nah am Arbeitsplatz erreichbar – seien das Rezept für schnellen Löscherfolg. Der neue Kevlar-Feuerlöscher sei 25 Prozent leichter als herkömmliche Stahlfeuerlöscher und zudem korrosions- und wartungsfrei.

Kurt Seifert, BTR Brandschutz-Technik und Rauchabzug GmbH, weist in der Ausgabe 3-2015 der Fachzeitschrift WiK (S. 51/52) darauf hin, dass in Studien des ZVEI in Abhängigkeit von der Technologie (Verschmutzungskompensation) **Tauschzyklen für Rauchmelder** definiert worden seien, die normativ in den Anhang der **DIN 14675** eingeflossen seien. Darüber hinaus biete der ZVEI seit 2010 den Errichtern von BMA, RWA oder FSA das Merkblatt „DIN 14675 Austausch von Brandmeldern" zur Interpretation der dort festgelegten Austausch- und Prüfverfahren im Feld. Wenn mit der Zeit Staub in den Rauchmelder eindringe, könne es vermehrt zu sogenannten Täuschungsalarmen kommen, oder die Auslösung im Brandfall werde verhindert. Um diese zu vermeiden, seien moderne hochwertige Geräte mit einer Verschmutzungskompensation ausgestattet. Bei der Reinigung oder dem Teileaustausch bzw. dem Austausch der gesamten Messkammer müsse sichergestellt und durch Dokumentation nachgewiesen werden, dass sich das Ansprechverhalten des automatischen Brandmelders in dem vom Hersteller nach der DIN EN 54 festgelegten Bereich befindet.

Im Special Brandschutz der Ausgabe 3-2015 der Zeitschrift WiK stellt Katrin Strübe, WAGNER Group GmbH, maßgeschneiderte Brandschutzkonzepte für mehr Sicherheit im **Tiefkühllager** vor (S. 7–9). In vielen Ländern Europas komme OxyReduct Vacuum Pressure Swing Adsorption- (VPSA)Technologie zum Einsatz. Sie ermögliche unter optimalen Bedingungen bei der Stickstofferzeugung Einsparungen bei den Betriebskosten von bis zu 80 Prozent im Vergleich zu Anlagen mit herkömmlicher Membrantechnik. Weltweit entwickle sich OxyReduct zur Standardlösung im Logistikbereich.

Die **Zahl der Brände** in Deutschland hat nach den Worten des Präsidenten der Vereinigung zur Förderung des Deutschen Brandschutzes (vfdb), Dirk Aschenbrenner, in den vergangenen Jahren alarmierende Ausmaße angenommen, berichtet der Behörden Spiegel in einem Spezial Interschutz zur Juni-Ausgabe. Sie sei von etwa 177.000 im Jahr 2006 auf rund 194.000 im Jahr 2012 gestiegen. Entsprechend seien auch die Brandschäden immer größer. Zu Beginn des 21. Jahrhunderts habe es deutlich mehr Brände als zu Beginn des 20. Jahrhunderts gegeben. Wesentliche Ursachen seien heutzutage immer stärker Faktoren wie zum Beispiel Elektrizität, Fahrlässigkeit oder Umgang mit offenem Feuer. Dagegen seien klassische Ursachen wie Funkenflug oder Selbstentzündung fast vollständig aus der Statistik verschwunden.

Cloud Computing

Technische Versiegelung empfehlen Dr. Ralf Rieken, Dr. Hubert Jäger, Arnold Monitzer und Edmund Ernst, Uniscon GmbH, im Tagungsband zum 14. Deutschen IT-Sicherheitskongress (S. 211–222) als effektiven Schutz für Inhalte und Metadaten in der Cloud. Das Konzept einer rein technischen Versiegelung des Rechenzentrums verhindere den Zugriff zu den physischen Signalen und Daten wäh-

rend der Vermittlung und Verarbeitung. Damit könne der Betreiber einer Cloud weder Inhalt noch Metadaten lesen. Das Konzept sei in der EU und in den USA patentiert.

In demselben Tagungsband empfiehlt Dr. Günther Hoffmann, Humboldt-Universität Berlin, für den sicheren Austausch und die sichere Speicherung von Dateien in cloudbasierten Speichern die **Integration mehrerer Sicherheitsverfahren** (S. 223–228). Dateien werden verschlüsselt, fragmentiert und redundant auf mehrere Speicher verteilt. Das vorgestellte Verfahren verschalte mehrere unsichere Speicher zu einem sicheren, dezentralen Speicherverbund.

Bei 84 Prozent der deutschen Unternehmen herrsche Unsicherheit darüber, ob ihre Daten in der Cloud noch sicher sind. Das gehe – wie WiK in der Ausgabe 3-2015, S. 7, meldet, aus der aktuellen Studie „IT-Sicherheit und Datenschutz 2015" der Nationalen Initiative für Informations- und Internet-Sicherheit e. V. (NIFIS) hervor. Demnach seien Kontrollverlust über die eigenen Daten (73 Prozent), interne und externe Hackerangriffe (71 Prozent) und die eigene Unwissenheit über die vorhandenen Risiken (89 Prozent) derzeit die Haupthemmnisse für die deutsche Wirtschaft beim Cloud Computing. Fast die Hälfte der deutschen Firmen gehe davon aus, dass die IT-Sicherheitsinvestitionen in diesem Jahr um 50 Prozent zunehmen werden.

BSI gibt Tipps für **sicheren Einsatz von ownCloud** in Unternehmen, meldet heise.de am 17. Juni. Viele Unternehmen übten begründete Zurückhaltung gegenüber öffentlich zugänglichen Diensten in der Public Cloud. Sie installierten stattdessen lieber on-premise eine Private Cloud auf Ressourcen, die unter ihrer Kontrolle stehen. Aus Kostengründen bedienten sie sich bei der Open Source. Dazu zähle ownCloud, von dem es eine allerdings kostenpflichte Enterprise-Version samt Support gebe. Das BSI habe ownCloud unter die Lupe genommen und einige Fallstricke in der Software, beim Installieren, Administrieren sowie im Anwenderverhalten aufgedeckt. Im dazu veröffentlichten Papier führe das BSI Gegenmaßnahmen an, mit denen bei einem „normalen" Schutzbedarf ein sicherer Betrieb von ownCloud realisierbar sein soll. Da sich das Paket um eigene Apps erweitern lässt, könne auf diesem Wege Gefährdungen begegnet werden. In der Untersuchung, die das BSI vorgelegt habe, seien solche Verfahren beschrieben. Ferner diene das Papier des BSI als Grundlage für Anwender mit höherem Schutzbedarf.

Drohnen

Im 2. Teil der rechtlichen Betrachtung der **Videoüberwachung durch Drohnen** in der Ausgabe 6-2015 der Zeitschrift GIT (S. 50–52) behandelt Rechtsanwalt Dr. Ulrich Deckert das Recht am eigenen Bild (§§ 22 ff. KunstUrhG), Rechte an der Abbildung von „Werken der Baukunst" (§ 59 Abs. 1 UrhG), den strafrechtlichen Schutz und Abwehrrechte des BGB (§§ 823 Abs. 2, 1004) des BDSG (§ 6b). Dem Eigentümer stehe ein Unterlassungsanspruch zu, wenn sein Grundstück permanent und zielgerichtet von Drohnen an- bzw. überflogen wird und, wenn dies mit unzumutbaren Belästigungen verbunden ist. Die auf dem Markt befindlichen technischen Abwehrlösungen (Störsender, elektromagnetische Wellen, Beschuss durch Laser oder Schusswaffe, Kollision mit eigener Drohne) seien alle nicht sonderlich überzeugend.

Energiesicherheit

Matthias Hofherr, atsec information security GmbH, befasst sich im Tagungsband zum 14. Deutschen IT-Sicherheitskongress (S. 321–328) mit dem Aufbau von Informationssicherheits-Managementsystemen **(ISMS)** in der Energiebranche, die sich als

Kritische Infrastruktur zunehmend größeren Gefahren ausgesetzt sehe. Dies sei auch ein gangbarer Weg für Unternehmen, die unter die Vorgaben des IT-Sicherheitsgesetzes fallen. Beschrieben wird der Aufbau der ISMS-Prozesse, die Umsetzung von Maßnahmen und Einsparpotenziale durch die Implementierung und durch die Umsetzung eines integrierten Management-Systems.

Falschgeldkriminalität

Nach dem vom BKA veröffentlichten **Bundeslagebild** Falschgeldkriminalität wurden in Deutschland im Jahr 2014 fast 60 Prozent mehr Falschgelddelikte als im Vorjahr polizeilich registriert: insgesamt 60.800. Der hohe Anstieg sei vor allem auf ein Internet-Angebot falscher Banknoten aus italienischer Massenfertigung und das Angebot von Hologrammen für Euro-Banknoten auf einer chinesischen Internetplattform zurückzuführen. Eine Zusammenfassung des BKA-Lageberichts enthält die Securitas-Webseite www.securitas.com/de/de/news/sicherheitslage/falschgeldkriminalität.

Nach einer Pressemeldung der Kriminaldirektion Kaiserslautern vom 11. Juni gab es in der Westpfalz mehrere Fälle von Falschgeld (20, 50 als auch 100 Euro-Scheine). Bei Banknoten helfe die Regel „Fühlen–Sehen–Kippen", um die folgenden wichtigsten Sicherheitsmerkmale zu erkennen: Stichtiefdruck, Sicherheitsfaden, Wasserzeichen, Mikroschrift und Spezialfolienstreifen.

Fluchtwegsicherung

Jürgen Rumeney, Siemens Building Technologies, befasst sich in der Ausgabe 6-2015 der Zeitschrift GIT (S. 89–91) mit Simulationen der Flucht. Siemens habe eine **Simulationssoftware** entwickelt, die die Bewegung von Personenströmen vorausberechnet und Evakuierungsszenarien testet. Voraussetzung für die Simulationssoftware „Crowd Control" sei eine innovative Berechnungsmethode mit einem aggregierenden Verfahren: Räume würden in einzelne Zellen unterteilt, die dem Platzbedarf eines Menschen entsprechen. Das Verhalten leerer und besetzter Zellen werde mittels Kraftfelder definiert. Ausgangspunkte und Zielorte der Personen könnten eingefügt werden, ebenso Hindernisse wie geparkte Fahrzeuge oder Feuer. Dabei werde Gegenständen eine andere Wirkung zugewiesen als Menschen und das Verhalten Einzelner wiederum anders definiert als das einer Gruppe. Das Verhalten der Menschen in Personenströmen könne so zehnmal schneller simuliert werden, als sie sich in Echtzeit bewegen. Werde die Software mit realen Informationen aus Überwachungskameras gekoppelt, lasse sich die Bewegung von Menschenmassen bis zu fünf Minuten im Voraus prognostizieren. Die Software errechne und visualisiere in 2-D oder 3-D die möglichen Fluchtwege sowie das zu erwartende Personenaufkommen.

Crowd Control sei auch in der Lage, die Auswirkung von Hindernissen auf die Evakuierung zu simulieren. So berücksichtige das Programm automatisch, welche alternativen Wege genutzt werden, wenn ein Fluchtweg plötzlich versperrt ist. Crowd Control biete sich auch als Übungstool an. Über eine proaktive Steuerung der Fluchtwege innerhalb eines Gebäudes lasse sich der Ablauf von Evakuierungen beeinflussen. Im Panikfall könnte der kürzeste und sicherste Fluchtweg durch Massen-SMS und Sprachalarme, durch Warnungen auf den Computerbildschirmen an den Arbeitsplätzen, durch Hinweise auf großen Digitalscreens in Treppenaufgängen oder mittels Pfeilen auf dem Smartphone aufgezeigt werden. Wird das Gebäudemanagementsystem direkt an das Computersystem der Feuerwehr gekoppelt, dann erhielten die Rettungskräfte einen digitalen Gebäudeplan, der nicht nur den Brandherd, sondern auch die Ausbreitungsrichtung des Feuers anzeige.

Gefahrenmanagement-system

Die Fachzeitschrift Security insight zeigt in der Ausgabe 3/2015, S. 33, wie ein integriertes Einsatzleit- und Gefahrenmanagementsystem die Arbeit in Leitstellen effizienter macht. Eine tiefe Integration des Systems sei dafür unabdingbar. Auf einer Plattform des Anbieters Advancis schalte im Meldungsfall das Gefahrenmanagementsystem ereignisabhängig Videobilder auf und zeige dem Bediener dynamische Handlungsvorschläge an. Die Meldungen würden entsprechend ihrer Priorisierung signalisiert. Dank der automatischen Einbindung von CAD-Grundrissplänen würden die zugehörigen Ortsinformationen direkt angezeigt.

Gefahrstoffe

Wie GIT-SICHERHEIT.de am 2. Juni mitteilt, endete am 1. Juni die Übergangsfrist für die Umstellung nach der neuen CLP (Classification, Labelling, Packaging)-Verordnung (EU-VO Nr. 1272/2008). Zuerst müsse die Einstufung des Produkts aus der Rezeptur nach den Regeln der **CLP-VO** ermittelt werden. Aus der Einstufung ergäben sich dann die Kennzeichnung mit Piktogrammen und Signalwort sowie die H-Sätze (Gefahren) und P-Sätze (Vorsichtsmaßnahmen). Diese Angaben würden im Sicherheitsdatenblatt und auf dem Etikett dokumentiert. Die Einstufung des Produkts könne in einigen Fällen schärfer ausfallen als bisher. So werde die augenätzende Wirkung häufiger auf dem Etikett zu sehen sein.

Der Behörden Spiegel befasst sich in seiner Juni-Ausgabe mit dem Informationssystem Gefährliche Stoffe **(IGS)**. 1992 sei das Fachinformationszentrum NRW (FIZ) gegründet worden, das mit der Gefahrstoffdatenbank der Länder und der Nationalen Alarmzentrale der Schweiz zusammenarbeitete. Derzeit enthalte die Datenbank Informationen zu rund 145.000 Stoffen. Dabei könne es sich sowohl um Chemikalien als auch um Naturstoffe, Radionuklide, aber auch um Bakterien, Viren, Pilze oder Parasiten handeln. Zu diesen Stoffen würden Informationen zur Bewertung, rechtliche Regelungen und Empfehlungen öffentlicher Institutionen sowie vor allem für Ersteinsatzkräfte relevante Informationen angeboten. Für die Stoffe beleuchte IGS Rechtsthemen von Abfall bis Zoll. Ziel des Systems sei die Zusammenführung aller Informationen, die zu einem bestimmten Stoff vorliegen. Trotz der komplexen Materie sei das System auf eine möglichst intuitive Bedienung ausgelegt. Der Beitrag geht auf Spezialanwendungen wie IGS-Public, IGS-Stoffliste, IGS-Fire, IGS-Polizei und IGS-OW (für die Gewässerüberwachung) näher ein.

Geldwäsche

Rechtsanwalt Jürgen Taschke weist in der FAZ am 3. Juni darauf hin, dass das Europäische Parlament die vierte „Richtlinie zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung" beschlossen hat. Sie sehe eine Reihe von Maßnahmen vor, die weitreichende Auswirkungen nicht nur auf die Finanzindustrie haben würden. So müssten Verantwortliche nach dem Geldwäschegesetz ihre Geschäftspartner auf der Grundlage von Dokumenten und Daten identifizieren. Dazu gehöre bei juristischen Personen jetzt auch die Feststellung des wirtschaftlichen Eigentümers. Die Mitgliedsländer sollten ein zentrales Register führen, in dem diese Informationen festgeschrieben werden. Die Angaben sollten allen Personen oder Organisationen zugänglich sein, die ein „berechtigtes Interesse" nachweisen können. Detaillierte Regeln werde es künftig auch im Hinblick auf „politisch exponierte Personen" geben. Finanzinstitute müssten angemessene Risikomanagement-

systeme unterhalten, um festzustellen, ob ein Kunde oder der wirtschaftlich Berechtigte einer Transaktion in diese Kategorie gehört. In diesem Fall müsse die Bank angemessene Maßnahmen ergreifen, um die Herkunft des Vermögens zu bestimmen und die Geschäftsbeziehung verstärkt zu überwachen – und das fortlaufend. Auch sollten Finanz- und Kreditinstitute geeignete Maßnahmen ergreifen, damit die Geldwäschestandards konzernweit Anwendung finden. Dadurch würden sie auch bei Tochtergesellschaften in Ländern mit lascheren Vorschriften greifen. Neu und für die Praxis von großer Bedeutung sei zudem die Festlegung von Sanktionen. Dabei würden die einzelnen Staaten stark in die Pflicht genommen. Zu den Strafmaßnahmen gehöre neben hohen Geldbußen auch der Entzug oder die Aussetzung der Bankzulassung. Noch massiver wirke die Veröffentlichung unanfechtbarer Entscheidungen durch die Behörden. Die Richtlinie werde in der Finanzwelt europaweit zu tiefgreifenden Änderungen bei der Risikobewertung von Kundenbeziehungen führen. Absehbar sei, dass damit ein erheblicher Aufwand für die Banken verbunden sein wird.

Industriesicherheit

Andreas Martin Floß, HiSolutions AG, befasst sich im Tagungsband zum 14. Deutschen IT-Sicherheitskongress mit der Sicherheit von industriellen Steuerungssystemen (Industrial Control Systems – ICS) durch einen erweiterten BSI IT-Grundschutz (S. 167–175). Perspektivisch sollten neue Bausteine, wie z. B. Werkshalle, Leitstand oder SCADA-System für normalen Schutzbedarf erstellt und bereits vorhandene Maßnahmenkataloge neu angepasst werden, z. B. für Patch- und Änderungs- oder für Netz- und Systemmanagement. So könne die Industrie ein adäquates Basis-Sicherheitsniveau für ICS erreichen.

In demselben Tagungsband stellen Michael Gröne, Sirrix AG, und Andre Wichmann, BSI, LARS (Light And Right Security), eine leichtgewichtige Lösung zum Einstieg in IT-Sicherheit für Betreiber von **Industriesteuerungsanlagen** vor (S. 177–190). LARS bewerte den aktuellen Sicherheitslevel aufgrund einer für die Zielgruppe optimierten Metrik. Durch die vielfältigen Berichtsfunktionen könnten anschließend die Anwender den aktuellen Status abrufen und beispielsweise erforderliche Maßnahmen einsehen, die zur Erreichung der nächstbesseren Sicherheitsstufe umgesetzt werden müssten. Weiterhin ermittele LARS die Auswirkungen von Maßnahmen auf den Sicherheitslevel. Ein Mapping auf das ICS Security Kompendium des BSI und Standards wie IEC 62443, ISO 27001 und IT-Grundschutz des BSI runde die Funktionalität ab.

Heiko Rudolph, Aaron Brown, Michael Klassen und Dominik Goergen, admeritia GmbH, befassen sich in dem Tagungsband mit technischen **Sicherheitstests für ICS-Anlagen** (S. 191–206). Herkömmliche Security-Tests seien für ICS-Anlagen nicht geeignet. Die Autoren beschreiben detailliert die Methodik des Applied Methodology ICS Security Testing, das den De-Facto-Standard OSSTMM um ICS-spezifische Aspekte erweitere. Die Methode biete enorme Vorteile in ihrer Reproduzierbarkeit und Validität. Das Ergebnis des Sicherheitstests gebe die Wirksamkeit der eingesetzten Sicherheitsmaßnahmen wieder, stelle die Angriffsfläche dar und zeige die Anfälligkeiten als Security Limitations auf.

IT-Sicherheit

Der Behörden Spiegel berichtet in seiner Juni-Ausgabe über Vorträge im Rahmen des 14. Deutschen IT-Sicherheitskongresses. Leicht gemachte Sicherheit muss ein Kriterium für gute IT-Sicherheit sein, habe der Präsident des BSI, Michael Hange, gesagt. Das BSI habe sich für die Zukunft mehrere Ziele auf die

Fahnen geschrieben: zum einen die verstärkte Standardisierung und Zertifizierung der IT-Sicherheit in Deutschland, die Förderung der Anwendung sicherer Technologien sowie die Kampagne „Deutschland sicher im Netz". Eine Schwäche des geplanten IT-Sicherheitsgesetzes sei für viele, dass noch nicht exakt definiert ist, was genau Kritische Infrastrukturen sind. Auf dem Kongress sei deutlich geworden, dass die IT-Sicherheitsstruktur des Bundes neu geordnet werden soll. Jedoch befänden sich viele Vorhaben erst noch am Anfang.

Im Tagungsband zum 14. Deutschen IT-Sicherheitskongress befasst sich Florian Oswald, TU Darmstadt, mit dem **Secure Session Protocol (SSP),** einem Ansatz zur garantierten Durchsetzung von Web-Sicherheitsmaßnahmen auf dem Client (S. 263–274). Es diene zur Generierung einer sicheren Umgebung im Browser des Nutzers, die individuell erzeugte Web-Sicherheitsregeln des Web-Applikationsanbieters umsetzt und deren Durchsetzung für die Dauer der Nutzung der Web-Applikation garantiere. Der Autor gibt eine Übersicht über das SSP und beschreibt den Ablauf. Die Clientumgebung sei derzeit das „schwächste" Glied in der Kette vom Webserver zum Browser.

COMPUTERWOCHE.de stellt am 1. Juni **Operational Intelligence** vor. Maschinengenerierte Daten gehörten zum komplexesten und am schnellsten wachsenden Bereich von Big Data. Lückenlose Aufzeichnungen über getätigte Käufe, Kunden, Nutzer- und Maschinenverhalten sowie Sicherheitsbedrohungen verleihen ihnen einen großen Wert. Mit Hilfe von maschinengenerierten Daten biete Operational Intelligence die Möglichkeit, genau zu verstehen, was in IT-Systemen und der firmeneigenen Technologieinfrastruktur geschehe, und zwar in Echtzeit. Durch fortwährendes Monitoring und schnelle Reaktionszeit ermögliche Operational Intelligence Unternehmen bekannte sowie neue und hoch entwickelte Bedrohungen zu identifizieren und auf sie zu reagieren. Die Herausforderung bestehe darin, die gewonnenen Daten so nutzbar zu machen, dass sie Unternehmen neue, gewinnbringende Einsichten liefern. IT-Strategen sollten eine Kombination aus bewährten Methoden und neuen Datenanalyseverfahren heranziehen, um Cyberattacken und Datenmissbrauch zu verhindern.

In der Informationssicherheit werde ein **Paradigmenwechsel** sichtbar, ist Dr. Johannes Wiele, Managing Security Consultant, überzeugt (WiK, Ausgabe 3-2015, S. 20/21). Weil die präventiven Maßnahmen mit vertretbarem Aufwand kaum noch zu verbessern seien, konzentrierten sich Anwender und Anbieter auf die aktive Abwehr unvorhergesehener gezielter Angriffe. Hier machten derzeit Maßnahmen wie Security Incident and Event Management (SIEM) und Security Operation Center (SOC) Furore. Ein SIEM-System errichte zunächst im Bereich der technischen Angriffserkennung eine neue Intelligenzebene. SIEM-Systeme „korrelieren" Informationen aus Log-Files und Traffic-Detectoren, wobei als Log-Quellen Netzwerkgeräte, Sicherheitsinstanzen wie Firewalls, Intrusion Detection und Virenschutz, Server, das Identitäts-Management, physische Security und Anwendungen wie etwa Datenbanken in Frage kämen. Anhand von Regeln prüften SIEM-Systeme permanent, fast in Echtzeit und ermüdungsfrei, ob sich Angriffe ergeben könnten. Immer dann, wenn ein Einzelevent dies rechtfertigt oder wenn die Kombination mehrerer Einzelinformationen eine Attacke vermuten lässt, alarmiere das SIEM die zuständigen SOC-Analysen in der Schaltzentrale, die dann über die richtigen Gegenmaßnahmen entscheiden.

Unternehmen aus zahlreichen Wirtschaftszweigen sowie Behörden seien künftig verpflichtet, ihre Computernetze nach dem neuesten Stand der Technik vor Hackern zu schützen und Angriffe zu melden, berichtet die FAZ am 13. Juni. Ein entsprechendes **IT-Sicherheitsgesetz** habe der Bundestag

verabschiedet. In die Pflicht genommen würden große und mittlere Anbieter aus den Branchen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen, die „Kritischen Infrastrukturen" aufrecht erhalten. Sie müssten künftig regelmäßig nachweisen, dass sie sich ausreichend schützen, etwa durch Zertifizierungen. Gravierende Störungen müssten Betroffene dem BSI mitteilen; in leichteren Fällen dürfe dies anonym geschehen. Das BSI müsse solche Informationen sammeln und gefährdete Unternehmen warnen. Auch könne es verlangen, dass Hersteller von Hard- und Software bei Pannenhilfe und Abwehr von Cyberkriminellen mitwirken. Schutzstandards dürften die verschiedenen Branchen selbst vorschlagen. Verbindliche Regelungen wolle die Bundesregierung dann in einer Verordnung festlegen. Nach Ansicht der Wirtschaft seien die Gesetzesregelungen für sich genommen zu unkonkret, um feststellen zu können, welche Unternehmen darunter fallen. Die Koalition gehe davon aus, dass rund 2.000 Firmen erfasst werden. BitKOM rechne mit Ausgaben für die Betreiber von bis zu 1,1 Mrd. Euro pro Jahr.

Wie silicon.de am 17. Juni meldet, warnt NowSecure, ein auf mobile Sicherheit spezialisiertes Unternehmen, vor einer gravierenden Schwachstelle in **Samsung-Smartphones.** Der Fehler stecke demnach in der Software für die SwiftKey-Tastatur, die nach Schätzungen von NowSecure auf mehr als 600 Mio. Mobiltelefonen installiert ist. Angreifer könnten damit remote ein betroffenes Gerät vollständig unter Kontrolle bringen.

IuK-Kriminalität

Hacker nehmen nach Einschätzung von Experten zunehmend auch die **Energiewirtschaft** ins Visier, berichtet welt.de am 3. Juni. Computerviren, die sich etwa in die Steuerzentralen von Versorgern oder Netzbetreibern einschleichen, dort Abläufe manipulieren und in der Lage wären, sogar Blackouts auszulösen, würden als Bedrohung immer ernster genommen. Organisierte Kriminalität, aber auch möglicher Netzterrorismus mit dem Ziel einer Sabotage der Grundversorgung seien heute keine Hirngespinste mehr. Bei kaum einem anderen Thema würden zudem neben den Licht- auch die Schattenseiten des Zusammenwachsens von Kommunikation und Energie in intelligenten Netzen so offensichtlich. Hackern eröffne die Technologie (smart metering) ein riesiges Einfallstor.

Nach einer Meldung von heise.de vom 10. Juni hat die Polizei in sechs Ländern eine internationale Bande von Cyberkriminellen ausgehoben. 49 Verdächtige seien verhaftet und 58 Häuser durchsucht worden, habe EUROPOL mitgeteilt. Die meisten Verdächtigen seien aus Nigeria, Kamerun und Spanien gekommen. Die Bande sei in Italien, Spanien, Polen, Großbritannien, Belgien und Georgien aktiv gewesen. Sie sei in Computernetzwerke mittlerer und größerer Firmen in Europa eingebrochen und soll mit Malware, aber auch Social Engineering, deren E-Mail-Systeme gehackt haben. Zahlungsaufforderungen an die Firmen seien dann gefälscht und die Bankkonten der Kriminellen angegeben worden. Sechs Mio. Euro seien über ein ausgeklügeltes Geldwäsche-Netzwerk aus der EU geschleust worden.

Nach einer Meldung von TECCHANNEL.de vom 10. Juni sehen neun von zehn Deutschen die Gefahr, dass bei **mobilen Bezahlverfahren** Daten gehackt und missbraucht werden. Das sei ein Ergebnis einer repräsentativen Befragung von 1.020 Erwachsenen im Auftrag der Wirtschaftsprüfungsgesellschaft PwC.

Im Sonderbericht Wirtschaftsschutz der Bundessicherheitsbehörden (Stand 12.06.2015) befasst sich das BSI mit Schwachstellen in **Content-Managementsystemen** bzw. de-

ren Plug-ins, die immer wieder Cyberangriffe auf Webangebote begünstigten. Die Täter nutzten diese Anfälligkeiten häufig, um Daten abzugreifen oder Webseiten zu entstellen. So sei die auf Basis des Content-Managementsystems (CMS) „WordPress" erstellte Webseite eines Unternehmens kompromittiert worden. Häufig stellten die Angreifer Suchanfragen nach potenziell verwundbaren Webseiten und versuchten bei den Suchergebnissen mithilfe von größtenteils bereits veröffentlichten Exploits die Schwachstellen auszunutzen. IT-Sicherheitsverantwortliche sollten prüfen, ob in der Organisation eine Übersicht aller (extern) erreichbarer Webanwendungen – inklusive der zugrunde liegenden Technologien – existiere, um das Gefährdungspotenzial bei relevanten veröffentlichten Schwachstellen bzw. Exploits einschätzen zu können. Standard-Webanwendungen und deren Plug-ins sollten bei Verfügbarkeit von Sicherheitsupdates aktualisiert werden. Vor Inbetriebnahme einer Webanwendung sollte ein Penetrationstest erfolgen.

LastPass sei ein beliebter Passwort-Manager, der für die meisten Betriebssysteme erhältlich ist. Die Anwendung diene als Container für Zugangspasswörter für Webseiten und andere Programme und werde über ein Master-Passwort geöffnet. Dieses Master-Passwort sollten Nutzer von LastPass nun ändern, wie die App seit kurzem einigen Nutzern beim Start mitteilt und wie das Unternehmen nun auch selbst schreibt. Es soll zu einem Hacker-Angriff auf das Firmennetzwerk gekommen sein, bei dem einzelne Nutzerdaten wie E-Mail-Adresse, Passwort-Hinweise, Authentifizierungs-Hashes und die zufällig generierten Passwort-Anhänge erbeutet wurden. Die einzelnen Container, in denen die Passwörter verschlüsselt gespeichert sind, seien laut Angabe von LastPass allerdings nicht kompromittiert (TECCHANNEL.de am 16. Juni).

Rund die Hälfte aller Cyberattacken auf Unternehmen komme nicht von Profi-Hackern, sondern aus den eigenen Reihen. Zu diesem Ergebnis komme IBM in seinem **2015 Cyber Security Intelligence Index,** wie heise.de am 18. Juni berichtet. Unter den Angreifern fänden sich ehemalige Angestellte, Dienstleister mit Systemzugriff oder Mitarbeiter als Opfer von Kriminellen. Rund ein Viertel der Attacken gehe auf Anwenderfehler zurück, etwa beim Klicken auf präparierte Links in Spam-E-Mails. Oft schlüpften unzufriedene Ex-Angestellte in die Rolle des Bösewichts. Sie verfügten noch über Passwörter oder richteten Zugänge ein, bevor sie das Unternehmen verlassen. Diese Insider mit Motiv seien für fast ein Drittel der Angriffe zuständig. Neben Mitarbeitern könnten auch Dienstleister mit Systemzugriff eine Gefahr sein. Von Outsidern ohne Zugriffsrechte komme nur weniger als die Hälfte aller Attacken (45 Prozent). Der Anteil von mit Schadsoftware infizierten Spam sei seit 2013 von einem auf derzeit vier Prozent angestiegen. Laut IBM-Studie seien dies die größten Sicherheitslöcher. Im X-Force Threat Intelligence Quarterly zögen die Forscher den Schluss, dass Spam mittlerweile eine ernsthafte Bedrohung darstellt. Kriminelle böten schon kommerzielle Spamkampagnen an, die Anwender über infizierte Links oder Anhänge etwa in E-Mails zu Kollaborateuren umfunktionierten.

Nach einer Meldung in der FAZ am 23. Juni hat die polnische Fluggesellschaft **LOT** berichtet, dass eine Attacke aus dem Internet seine Bodensysteme am Flughafen manipuliert und zeitweise außer Betrieb gesetzt habe. Mit den Rechnern würden die Flugpläne der Gesellschaft und ihrer Allianzpartner erstellt. Durch den Aussetzer im Betrieb seien die Flüge von 1.400 Passagieren verzögert oder storniert worden. Eine Gefahr für die in der Luft befindlichen Flugzeuge habe jedoch nicht bestanden. Auf eine Twitter-Meldung des IT-Sicherheitsexperten Chris Robert, er habe sich während eines Flugs mit United Airlines in das Steuerungssystem einer

Boeing 737 eingeklinkt und so zeitweise die Kontrolle im Cockpit übernommen, hätten IT-Experten der Branche erklärt: Keine Änderung im Flugablauf könne in das System eines Flugzeugs geladen werden, ohne dass der Pilot sie sehe und dieser Änderung ausdrücklich zustimme.

Das Wochenmagazin WirtschaftsWoche befasst sich am 19. Juni mit dem **Darknet** (S. 18–23). Im Internet sei eine Parallelwelt entstanden. Dort ließen sich Daten, Drogen, Waffen und alles handeln, was das Licht der Öffentlichkeit scheut. Verbrechen sei plötzlich skalierbar. Laut EUROPOL würden jährlich mehr als 300 Mrd. US-Dollar an Schäden entstehen. Der „Felsspalt" in diese virtuelle Welt sei der Browser Tor. Knapp drei Mio. Internetnutzer aktivierten täglich diese Software, die alle Daten so verschlüsselt, dass nicht mehr feststellbar ist, welcher Computer gerade welche Inhalte abruft. Die Internet-Adressen der Marktplätze bestünden aus kryptischen Zahlen- und Buchstabenkolonnen. Eine Liste mit „Links" zu rund 250 Marktplätzen erscheine in Kategorien wie „Financial Services", „Hacking" oder „Drugs" unterteilt. Weil im Darknet in der Regel mit Bitcoins bezahlt werde, blieben neben den Nutzerdaten auch die Zahlungsströme verborgen. Das Angebot auf den weit mehr als 40.000 Marktplätzen im Darknet sei so vielfältig, dass eine Gruppe unter der Marke „Grams" ein Pendant zu Google aufbaue. Am teuersten gehandelt würden Sicherheitslücken in IT-Systemen. Mit dem „Bitcoin Fog" betreibe die organisierte Kriminalität sogar eine eigene Geldwaschanlage. Rand Corporation mutmaße über den digitalen Schwarzmarkt, dass 30 Prozent aller Darknet-Verkäufer Betrüger sind. Eine Bande nenne sich „Erfurt Connection". Sie biete auch das Kopieren von elektronischen Autoschlüsseln an.

Krisenmanagement

Ein reaktions- und funktionsfähiges Krisenmanagement zu gewährleisten sei die persönliche Verantwortung der Geschäftsführer und Vorstände, schreibt Jens Washausen, GEOS Germany, in der Ausgabe 3-2015 von Security insight (S. 52/53). Den Krisenstab selbst zu leiten, sei aber in der Regel der falsche Weg, denn eine starke und dominante Führungspersönlichkeit sei für Krisenstäbe selten eine gute Konstellation. Es sei besser, dessen Kompetenzrahmen so auszugestalten, dass er zu einem effektiven Organ der Aufbauorganisation in Krisensituationen wird. In unserer exportorientierten Industrie werde nicht ausreichend thematisiert, dass Lösegeldzahlungen an extremistische und terroristische Gruppen verboten sind. Das sei für den Rechtsraum EU seit Inkraftsetzung der Council Regulation No. 881/2002 klar geregelt.

Kritische Infrastrukturen

Die Zeitschrift PROTECTOR thematisiert in der Ausgabe 6-2015 (S. 26–28) die **Europäische Sicherheitspolitik** für Kritische Infrastrukturen. Probleme lägen vor allem in der unzureichenden Zusammenarbeit und dem mangelnden Austausch über Sicherheitsvorfälle zwischen den Mitgliedsstaaten. Das Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme (IAIS) verfolge mit dem Projekt „Critical Infrastructure Preparedness and Resilience Research Network" (CIPRNet) das Ziel, ein europäisches Kompetenzzentrum für die Simulation und Analyse kritischer Infrastrukturen aufzubauen. Mit Hilfe von Simulationen ließen sich in der Dynamik eines Systems Indikatoren und Trends aufzeigen. Schon bestehende Simulationen sollten technisch zusammengeschaltet werden und zu einem entsprechend aussagekräftigen Analyseergebnis kommen.

In derselben Ausgabe von PROTECTOR werden Lösungen für die **Sicherheit der Wasserversorgung** behandelt (S. 52/53). Die Firma Turck habe für die Rheinisch-Westfälischen Wasserwerke eine Lösung für die Sicherheit von Brunnen entwickelt: Am äußeren Rand von Brunnendeckeln sitze ein induktiver Näherungsschalter, der den Metallrand des Brunnens erfasst, solange der Deckel geschlossen ist. Wird er geöffnet, „sehe" der Sensor ins Leere und ändere sein Signal. Der Status von mehr als 50 Brunnen werde erfasst und kabellos an die zentrale Leitwarte des Wasserwerks übermittelt. Der Schlüssel zum vorbeugenden Diebstahlschutz bei Außenanlagen liege in der Kombination aufeinander abgestimmter Komponenten: Bewegungsmelder könnten jeden Eindringling Tag und Nacht melden. Sehr wichtig für für einen autarken Einsatz solcher Systeme sei die netzunabhängige Gewährleistung der Energieversorgung.

Ladendiebstahl

Nach einer aktuellen **Studie des Kölner EHI Retail Institute** sind die Inventurdifferenzen 2014 mit 3,9 Mrd. Euro (bewertet zu Verkaufspreisen) unverändert hoch geblieben, berichtet die FAZ am 18. Juni. Besonders große Sorge bereite der Branche, dass zwar der einfache Ladendiebstahl eher stagniert, schwere Diebstähle auch von gesicherter Ware aber dramatisch zugenommen haben. In den vergangenen sieben Jahren hätten sie sich nach Beobachtungen des EHI mehr als verdoppelt, wobei offensichtlich zunehmend organisierte Banden am Werk seien. Nehme man den Aufwand von rund 1,3 Mrd. Euro, den die Ladenbesitzer jährlich in Technik und Personal zum Diebstahlschutz stecken, zu den festgestellten Inventurdifferenzen hinzu, habe der Handel insgesamt rund 5,2 Mrd. Euro rund um das Thema Inventurdifferenzen zu stemmen. Das entspreche etwa 1,3 Prozent des Branchenumsatzes. Die Dunkelziffer werde auf über 98 Prozent veranschlagt. Daraus sei abzuleiten, dass alljährlich mehr als 26 Mio. Ladendiebstähle unentdeckt blieben. Die Unternehmen wollten sowohl die speziellen Schulungen des Kassenpersonals verbessern als auch die technische Überwachung durch Kameras verstärken.

Leitstelle

Die Zeitschrift PROTECTOR enthält in der Ausgabe 6-2015 (S. 48/49) eine Marktübersicht über 44 Leitstellenausstatter. Abgefragt wurden Kriterien zur Einrichtung, zur Leittechnik und zu Dienstleistungen.

Luftverkehrssicherheit

Mit Passagierkontrollen an Flughäfen befasst sich inforadio.de am 4. Juni. Die EU-Kommission habe ein Vertragsverletzungsverfahren gegen Deutschland wegen vermeintlicher Verstöße gegen die Qualitätskontrolle bei den Sicherheitsschecks eingeleitet. Wie könne man bei einem vollgepackten Koffer auf einen Röntgen-Blick erkennen, ob verbotene Dinge darin sind? Diesen „Durchblick" könne man erlernen, etwa im Schönefelder Ausbildungszentrum der Sicherheitsfirma Securitas Aviation. 2014 habe das Unternehmen 250 Luftsicherheitsassistenten ausgebildet. Voraussetzung für den Job sei eine abgeschlossene Berufsausbildung. Zu dem Vertragsverletzungsverfahren habe das Bundesinnenministerium klargestellt, dass sich die Kritik der EU gegen die Aufsicht der Kontrolleure, nicht aber gegen die Art und Weise ihrer Sicherheitschecks selbst richte.

Mobile Endgeräte

Sebastian Hönig, Hewlett Packard Deutschland GmbH, beschreibt im Tagungsband zum 14. Deutschen IT-Sicherheitskongress (S. 11–22), wie **Near Field Communication (NFC)** die mobile Sicherheit vereinfacht. Das Passwort bzw. der Schlüssel zur Benutzerauthentifizierung oder Verschlüsselung von Daten werde auf einem NFC-Tag hinterlegt. Um zu funktionieren, müsse sich dieser NFC-Tag in der Nähe des Smartphones befinden. Sobald der NFC-Tag vom Smartphone entfernt wird, seien Daten und Anwendungen automatisch für Änderungen und Ansicht gesperrt.

In demselben Tagungsband empfehlen Kristoffer Braun und Philipp Rack, TU Darmstadt, eine **Blickschutzfolie** mit positionsunabhängigen Authentisierungsverfahren, also zufällig angeordneten Eingabefeldern, zum Schutz vor dem „Shoulder-Surfing", bei dem ein Angreifer versucht, dem Nutzer eines Smartphones „über die Schulter zu schauen", um an sensible Daten zu gelangen (S. 45–56). Das sei jedenfalls im geschäftlichen Kontext empfehlenswert, weil ein Smartphone hier äußerst sensible Daten enthält und der zusätzliche Aufwand durch einen höheren Schutz aufgewogen werde.

Mit der systematischen Risikobewertung von mobilen Endgeräten im Unternehmenseinsatz befassen sich in dem Tagungsband zum 14. Deutschen IT-Sicherheitskongress Jörn Störling und Dr. Sven Wenzel vom Fraunhofer-Institut für Software und Systemtechnik (S. 329–341). Sie beschreiben einen Ansatz, um **Schwachstellen systematisch zu identifizieren** und passende Maßnahmen zu empfehlen. Für die Modellierung von IT-Systemen, Infrastrukturen und Datenflüssen sowie Risiken mit passenden Gegenmaßnahmen entwickeln sie einen grafischen Editor, der unter Nutzung einer eigenen domänenspezifischen, grafischen Sprache Risikoanalysen auf modellierten Infrastrukturen erlaube und die Ergebnisse einer solchen Analyse als Bericht aufbereite. Es gelinge so leicht und schnell einen Überblick über die aktuelle Situation einer Infrastruktur zu erlangen, was besonders im Kontext des Einsatzes von mobilen Endgeräten, die einem schnellen Wandel unterliegen, wichtig sei.

COMPUTERWOCHE.de stellt am 31. Mai einige Lösungen für die **Verschlüsselung** von Daten auf mobilen Geräten vor. Dabei werde das Hauptaugenmerk auf die einfache und sichere Bedienung gelegt. Am konsequentesten seien die Entwickler von Apple vorgegangen, die Betriebssystem und Geräte unter anderem mit einer hardwaregestützten Verschlüsselung und mit einer als File Data Protection bezeichneten Technik ausgestattet haben. Für alle anderen Smartphone- und Tablet-Nutzer sei es wichtig, zusätzliche Apps und Programme auf ihren mobilen Systemen zur Sicherung der Daten zu installieren. Die Sophos Mobile Encryption-App sei einfach zu installieren und zu verwenden. Sie ermögliche es auch, recht unkompliziert Dateien zu verschlüsseln und auf verschiedenen Cloud-Speichern abzulegen. Die Boxcryptor-App sei kostenlos und stehe auf sehr vielen mobilen Plattformen zur Verfügung. Alle gängigen Cloud-Anbieter würden von ihr unterstützt. Die App TextSecure biete alle die Sicherheitseinstellungen und -möglichkeiten, die bekannte Apps wie WhatsApp vermissen ließen. Eine sehr gute freie Lösung, bei der auch alle wichtigen Hintergrunddaten und der Source-Code offengelegt werden, sei SecurStick. Mit ihr könnten Nutzer verschiedene Datenträger und USB-Sticks verschlüsseln. DiskCryptor biete unter anderem folgende Möglichkeiten: Es könne die Systempartition mit den Verschlüsselungs-Algorithmen AES, Serpent oder Twofish sichern. Auch alle anderen Partitionen sowie Volumen auf externen Datenträgern könnten verschlüsselt werden. Und er stehe unter GNU GPLv3 offen zur Verfügung.

Mobiler Zugriff auf Sicherheits- und **Gebäudemanagementsysteme** ist ein Thema in der Ausgabe 6-2015 der Zeitschrift GIT (S. 98/99). Hochentwickelte mobile Lösungen böten die Möglichkeit, über die vom Personal mitgeführten Endgeräte auch Ereignisinformationen flexibel zu erfassen und zur Bearbeitung an die Leitstelle zu übermitteln. Die Übermittlung mobiler Meldungen beinhalte die automatische Weitergabe der Geo-Koordinaten des Ereignisorts. Die mobilen Lösungen seien in der Regel nicht nur plattformübergreifend mit allen Betriebssystemen verwendbar, sondern darüber hinaus auch endgeräteunabhängig. Die Bereitstellung mobiler Lösungen sei heutzutage eine der wettbewerbsentscheidenden Faktoren, da sich kontinuierlich neue Möglichkeiten zur Flexibilitätssteigerung und für den Bedienkomfort ergäben.

Objektfunkversorgung

Den Digitalfunk für Behörden und Organisationen mit Sicherheitsaufgaben **(BOS) innerhalb von Gebäuden** thematisiert die Zeitschrift GIT in der Ausgabe 6-2015, S. 56–58). Die Eigentümer oder Betreiber von Gebäuden seien verpflichtet, für eine funktionsfähige Funkversorgung in Gebäuden zu sorgen. Der „Leitfaden zur Planung und Realisierung von Objektversorgungen (L-OV)" sei für das digitale Sprech- und Datenfunksystem BOS und beschreibe die rechtlichen Vorgaben und Bedingungen sowie die Anforderungen an die technische Umsetzung. Über diese Leitlinien hinaus existierten in den Bundesländern und Kommunen Richtlinien und Konzepte zur Objektversorgung. Dazu gehörten auch die Bauordnungen der Bundesländer. Die Anforderungen an die Objektversorgung seien oftmals schon in der Baubeschreibung bzw. Baugenehmigung enthalten. Die Versorgung aus dem Freifeld reiche dann aus, wenn 96 Prozent des Gebäudes ohne besondere Maßnahmen bereits funktechnisch versorgt sind. Zertifizierte Planungsunternehmen könnten die Bauherren durch alle technischen Verfahrensschritte begleiten. Für Objekte, die heute bereits über eine Funkversorgung für den analogen BOS-Funk verfügen, bedürfe es eines technischen Konzepts für die „Migration" der analogen in eine digitale Inhouse-Netzstruktur.

Organisierte Kriminalität

Prof. Dr. Arndt Sinn, Universität Osnabrück, nimmt in der Ausgabe 3-2015 der Zeitschrift WiK Stellung zu dem aktuellen **EUROPOL-Report „Exploring Tomorrow".** Danach sei mit einer dramatischen Änderung der „kriminellen Landschaft" zu rechnen – mit Auswirkungen auf die Wirtschaft. Für die neue Dynamik der OK identifiziere Europol mehrere Schüsselfaktoren, die eine Neuorientierung der OK begünstigen, darunter Big Data und der Handel mit Ressourcen. Auch sehe die Studie ein Zusammenwachsen von OK und Terrorismus. „Crime as a Service" sei ein Teil des modernen OK-Bildes. Es bedeute, dass die traditionellen Strukturen krimineller Netzwerke durch Modelle von individuellen Dienstleistungen abgelöst werden. So kämen etwa Hacker für kurzzeitige Aufträge zusammen und bilden somit keine festen und hierarchisch strukturierten großen Netzwerke mehr. Die Straftat werde als Dienstleistung angeboten. Und so könnten sich mehrere Personen für eine bestimmte „große Sache" zusammenschließen und sich danach wieder voneinander lösen. EUROPOL benennt folgende „Key Driver" für die OK: 1. Entwicklungen und Neuerungen in der Transport- und Logistik-Branche; 2. Nanotechnologie und Robotik; 3. Big Data; 4. Illegaler Handel mit E-Abfällen; 5. Mehr gesellschaftliche Akzeptanz; 6. Einfluss auf die immer wichtiger und zugleich knapper werdenden natürlichen Ressourcen; 7. Virtuelle Währungen; 8. Gesundheitsmarkt.

Personenschutz

Der Aufklärung müsse im Personenschutz eine größere Rolle zukommen, schreibt Thilo Ohrmundt, DISEO, in der Ausgabe 3-2015 von Security insight (S. 36/37). Heute existierten Schutzkonzepte, die ausschließlich auf Aufklärung basieren. Hier gelte die direkte Sicherheitsbegleitung bereits als Maßnahme des erweiterten Personenschutzes, und nur dort, wo die Aufklärung nicht mehr als ausreichend angesehen wird, greife man „notgedrungen" auf die Begleitung zurück.

Rechenzentrumssicherheit

Jörg Kreiling, Rittal, zeigt in der Ausgabe 6-2015 der Zeitschrift GIT (S. 105–107), wie ein Rechenzentrum aufgebaut ist und welche Sicherheitsanforderungen erfüllt werden müssen. Die Abhängigkeit der Unternehmen von Rechenzentren werde durch die Digitalisierung der Arbeitswelt weiter zunehmen. Damit rückten Themen wie Ausfallsicherheit, Redundanz, Datensicherheit und Zugangskontrollen immer stärker in den Vordergrund. Bei der standardisierten Rechenzentrumslösung **RiMatrix** erhielten Kunden ein vorkonfiguriertes Rechenzentrum inklusive Racks, Klimatisierung, Stromversorgung und Sicherheitstechnik. Durch einen garantierten PUE-Wert von bis zu 1,15 bekämen sie eine klare Kalkulationsgrundlage für die Wirtschaftlichkeitsberechnung. Das Konzept eines modularen Rechenzentrums mache das IT-Budget für mittelständische Unternehmen besser planbar.

Reisesicherheit

Die Zeitschrift WiK weist in der Ausgabe 3-2015 (S. 31) auf einen neuen ASW-Leitfaden zur Sicherheit auf Geschäftsreisen hin, der über www.asw-bundesverband.de bezogen werden könne. Er gebe in Form von Checklisten einen geordneten Überblick, wie man sich entsprechend vorbereiten könne.

Schulsicherheit

In der Zeitschrift Security insight (Ausgabe 3-2015, S. 40) wird darauf hingewiesen, dass es seit Anfang 2015 eine neue **technische Norm für Notrufsysteme** in Schulen gibt. Die unter Federführung des VDE entwickelte Richtlinie beschreibe ganz konkret jene Anforderungen, die neue Kommunikationsanlagen in Not- und Gefahrenfällen künftig zu erfüllen haben. Neu sei die Position des technischen Risikomanagers, der innerhalb einer Organisation bestimmt, welcher Sicherheitsgrad umgesetzt werden muss. Er sei es auch, der entscheiden könne, ob eventuell von den Vorgaben der Norm abgewichen werden kann. Die Norm gebe Planungsstellen bessere Orientierungsmöglichkeiten bei der Bewertung bestehender sowie beim Kauf neuer Notfall- und Gefahrenreaktionssysteme.

Sicherheitssysteme

In der Zeitschrift PROTECTOR (Ausgabe 6-2015, S. 38/39) wird die **Planung von Sicherheitssystemen** thematisiert. Der beste Ansatzpunkt für die Planung sei die Vision eines Unternehmens. Ein relativ offenes System sei eine wichtige Voraussetzung. Ein modulares, softwarebasiertes System bedeute, einfacher auf zukünftige Entwicklungen reagieren zu können. Das Hinzufügen von Hardware, wie biometrische Systeme, sei dann ohne die Installation eines komplett neuen Systems möglich. Wenn man bei der Ausschreibung Sicherheit als einen Zyklus mit Prozessen begreift, bekäme man ein System, das gemäß Strategie und Vision einfacher modifiziert werden kann.

Bosch Sicherheitssysteme befasst sich in der Ausgabe 6-2015 von PROTECTOR (S. 50/51) mit neuen Möglichkeiten von IP-Anwendungen. Ethernet und das IP-Protokoll gewännen in der gesamten Sicherheitstechnik immer mehr an Bedeutung. Sie ermöglichten die einfache Vernetzung mehrerer Alarmzentralen, die Integration unterschiedlicher Gewerke und einen kosteneffizienten Betrieb der gesamten Sicherheitstechnik. Zudem bildeten IP-basierte Lösungen die Basis einer Vielzahl von Remote Services sowie ganz neue Geschäftsmodelle in der Cloud. Die Integration unterschiedlicher Gewerke erhöhe das gesamte Sicherheitsniveau, da Ereignisse und Alarme unterschiedlicher Systeme automatisch korreliert werden könnten, was sehr schnelle und gezielte Maßnahmen ermögliche. Die Flexibilität und die Skalierbarkeit seien weitere große Pluspunkte vernetzter Systeme. Das Bosch-System Effilink sei eine umfassende, IP-basierte Plattform für Remote Services, mit der durch Dienste wie Ferndiagnose und -parametrierung der Einsatz eines Technikers vor Ort in etwa zwei Drittel aller Fälle überflüssig werde. Bei Effilink ermögliche Bosch keinerlei Fernzugriffe, die von außen initiiert werden.

Sicherheitstechnik

Der Markt für elektronische Sicherheitstechnik erzielte laut Angaben auf bdsw.de am 17. Juni im Jahr 2014 einen neuen Spitzenwert. Der Erhebung des BHE (Bundesverband Sicherheitstechnik e. V.) zufolge belief sich der Gesamtumsatz auf rund 3,18 Mrd. Euro – das beste Ergebnis seit Beginn der Messungen und ein deutliches Wachstum von 3,7 Prozent gegenüber dem Vorjahr. Besonders deutlich sei der Zuwachs in der Videoüberwachungstechnik ausgefallen. Hier sei eine Umsatzsteigerung von 4,2 Prozent auf 448 Mio. Euro erreicht worden. Spürbare Zugewinne hätten auch die Brandmeldetechnik (+ 4 Prozent auf 1,42 Mrd. Euro), die Sprachalarmsysteme (+ 3,7 Prozent auf 84 Mio. Euro) und die Zutrittssteuerung (+ 3,3 Prozent auf 282 Mio. Euro) erzielt. Die Einbruchmeldetechnik habe ihre Umsätze auf 693 Mio. Euro gesteigert (+ 3 Prozent). Sonstige elektronische Sicherungssysteme wie Rauch- und Wärmeabzugsanlagen oder Flucht- und Rettungswege hätten den Umsatz um 3,6 Prozent auf 258 Mio. Euro gesteigert.

Mit Ausgabedatum Juli 2015 erscheint nach einer Meldung von bdsw.de vom 17. Juni der deutsche Entwurf der DIN EN 16763 – Dienstleistungen für Sicherheitsanlagen. Die Norm lege Mindestanforderungen an die Dienstleistungsorganisation sowie an die Kompetenz, das Wissen und die Erfahrungen für die mit der Planung, Projektierung, Montage, Inbetriebnahme, Anlagenüberprüfung, Abnahme oder Instandhaltung von Sicherheitsanlagen betrauten Beschäftigten fest, unabhängig davon, ob die Dienstleistungen am Installationsort oder durch Fernzugriff erbracht werden.

Stadionsicherheit

Stadionwelt-business.de berichtet am 17. Juni über den **Hightech-Schutz** für das Stadion des 1. FC Union Berlin. Der Lösungsintegrator globits konzipiere und installiere eine Videoüberwachungsanlage mit Kameras des IP-Videoherstellers Axis Communications unter Beratung der Berliner Polizei und des Sicherheitsunternehmens Securitas. Globits installiere 19 moderne PTZ-Dome-Netzwerk-Kameras sowie zwei Thermal-Kameras, die Tag und Nacht das Stadion und das Vereinsgelände scannen und einen besonders hohen Schutz während der laufenden Spiele sowie beim Einlass und Abgang der Fans bieten. Mit ihren Funktionen zum Schwenken, Neigen und Zoomen eigneten sich die IP-Kameras ideal zum Überblicken von Menschenmengen und Warteschlangen. Die unauffällige kuppelartige Bauform des Kameragehäuses biete

nicht nur einen wirksamen Schutz vor einer Verdrehung oder Defokussierung, sondern mache es auch Einbrechern oder sonstigen Straftätern schwer, die Aufnahmerichtung zu erkennen.

Transportdiebstahl

Der ASW-Bundesverband meldet folgende Tatorte von Planen-Schlitzereien und sonstiger Ladungs-Diebstähle auf Fahrstrecken im Bundesgebiet:

- 26./27.5., A 6, St. Leon-Rot, Parkplatz „Weißer Stock"
- Nacht zum 27.5., A 4, Hainichen, Parkplatz „Rossauer Wald"
- 27./28.5., Leipzig, Wiesenstraße
- 30.5., A 2, Auetal-Wiersen, Parkplatz „Schafstrift", Fahrtrichtung Dortmund
- 9./10.6., A 7, Autobahnparkplatz Stauffenberg, Fahrtrichtung Norden
- 18./19.6., A 2, Ziesar, Lkw-Rastplatz an der Raststätte Buckautal-Süd
- 18./19.6., A 2, Brandenburg an der Havel, Parkplatz Temnitz zwischen Wollin und Brandenburg
- 18./19.6., A 9, Beelitz, Parkplatz Zauche zwischen Brück und Beelitz
- 18./19.6., A 7, Northeim, Parkplatz „Schlochau", Fahrtrichtung Hannover, zwischen Anschlussstelle Northeim-West und Northeim-Nord

In der Juni-Ausgabe von Veko-online befasst sich Henning Glitza, Fachjournalist, mit dem Transportdiebstahl. Der geschätzte jährliche Schaden allein für die deutsche Transportwirtschaft betrage laut Verband Spedition und Logistik NRW 1,5 Mrd. Euro. Die Aufklärungsquote bei Frachtdiebstählen liege deutlich unter 10 Prozent. Nach seriösen Schätzungen würden europaweit jährlich etwa 200.000 Diebstähle von Ladungen oder kompletten Lkw gemeldet. Laut einer Studie des Verkehrsausschusses des Europäischen Parlaments würden dabei Güter im Wert von 8,2 Mrd. Euro gestohlen. Diese gewaltige Summe markiere indessen noch lange nicht den tatsächlichen Gesamtschaden. So blieben die Kollateralschäden der Transportwirtschaft, wie erforderliche Reparaturen, längerfristige Fahrzeugausfälle, erneute Lieferungen beziehungsweise Auftragsstornierungen und gestiegene Versicherungsprämien, unberücksichtigt. Wie das BAG in einer 2013 vorgelegten Untersuchung konstatiere, würden von hiesigen Unternehmen jährlich schätzungsweise 6.000 Ladungsdiebstähle gemeldet. 2013 seien laut BAG 1.798 Lkw komplett gestohlen worden, viele mitsamt Ladung. Auf einem mindestens „mittleren vierstelligen Niveau" bewegten sich die Fälle von Kraftstoffdiebstählen. 39 Prozent aller Vorfälle ereigneten sich auf Raststätten und Autohöfen, 35 Prozent auf Betriebsgeländen.

Die einfachste Art des Angriffs auf Lkw sei das sogenannte Planenschlitzen. In der Dunkelheit gingen die oft als Lkw-Fahrer getarnten Kriminellen auf Parkplätzen von Lkw zu Lkw. Sie tasteten zunächst die Planen ab und stellten dadurch fest, ob sich überhaupt Ladung auf dem Lkw befindet. Ist dies der Fall, dann schlitzten sie etwa 20 Zentimeter der Plane sichel- oder rechteckförmig auf. Der sogenannte Kontrollschnitt sei gerade so groß, dass die „Lkw-Marder" die Plane umklappen und einen Blick ins Innere werfen können. Sie rufen dann meist per Handy Komplizen herbei, die irgendwo in der Nähe in einem Transportfahrzeug auf ihren Einsatz warten. Dann werde die Plane circa 1 x 1 Meter aufgeschlitzt und das Gut umgeladen. Von der unmittelbaren Tatbegehung bis hin zur Zwischenlagerung und der Verwertung des Diebesguts liege alles quasi in einer Hand. Die Entwendung abgestellter Zugmaschinen und Auflieger habe seit 2012 enorm zugenommen. Regionale Schwerpunkte seien Nordbayern, Thüringen, Sachsen und Sachsen-Anhalt. Zumeist würden internationale Banden tätig. Auch Baumaschinen von nahezu ungesicherten Baustellen stünden

auf der Top-Liste der Täter. Der Autor geht auch auf die sogenannten **Sicherheitsparkplätze** ein. Sie seien gut ausgeleuchtet, videografisch überwacht und mit Zäunen und Toren gesichert. Es gebe aber erst vier dieser Parkplätze in Deutschland. Die Aufenthaltspreise lägen zwischen 25 und 120 Euro. Die TRASPAL Deutschland GmbH wolle ein flächendeckendes Netz von 80 bis 100 solcher Parkstationen in den nächsten 5–7 Jahren schaffen. Die Firma fordert eine bundeseinheitliche Zertifizierung solcher Parkplätze mit der Pflicht zur jährlichen Erneuerung.

Unternehmenssicherheit

Die Zeitschrift Security insight stellt in Ausgabe 3-2015 (S. 16–19) die branchenübergreifende Studie **„Corporate Security 2030: Challenges & Opportunities"** vor, die der VSW NW veröffentlicht hat. Die Studie zeige, dass das Management Projektionen, die sich mit dem Informationsschutz beschäftigen, grundsätzlich höher bewertet als die Sicherheitsexperten, die Projektionen, denen eine Governance-Kompetente zugrunde liegt, im Durchschnitt höher bewerten. Deutliche Differenzen zeigten sich bei den Themen Resilienz und Unternehmenskultur. Sicherheitsexperten sähen im BCM einen zentralen Aufgabenbereich der Corporate Security. Das Management hingegen glaube an eine der Organisation inhärente Resilienz: Flexibilität und Kreativität der Belegschaft würden massive Ausfälle bei Störereignissen verhindern.

Den dritten Teil des Ergebnisberichts der WiK-Sicherheitsenquete 2014/2015 enthält die Zeitschrift in Ausgabe 3-2015 (S. 12–15). Er bezieht sich auf die Aussagen von Experten der Unternehmenssicherheit und von Sicherheitsdienstleistern zum **Outsourcing** von Funktionen der Unternehmenssicherheit. 84 Prozent der befragten Unternehmen hatten 2014 mindestens eine Sicherheitsaufgabe an externe Anbieter vergeben. An der Spitze standen Objektschutz/Streifendienst (57,1 Prozent), Wartung von Sicherheitstechnik (55,1 Prozent) und Alarm-/Notrufzentrale (49 Prozent). In nahezu allen Outsourcing-Bereichen wird künftig ein Zuwachs erwartet, am stärksten beim Facility-Management (16,3 Prozent), der Alarm-/Notrufzentrale und bei Awareness-Schulungen (je 14,3 Prozent). Dass bereits fremdvergebene Aufgaben wieder selbst erledigt werden, kommt zwar vor (bei 19 Prozent der befragten Unternehmen in den letzten zwei Jahren), spielt aber bei der Planung so gut wie keine Rolle. Die Begründung der Auftraggeber für Vertragskündigung oder Nichtverlängerung sind vielfältig. Am meisten wurden genannt: Mängel in der Leistungserbringung (62,5 Prozent; vor zwei Jahren waren es noch 49,2 Prozent) und Ersatz der personellen Dienstleistung durch Technik (40 Prozent). Die überwiegende Zahl der Kunden ist mit den von ihnen beauftragten Sicherheitsdienstleistern zufrieden. Als Kriterien für die Fremdvergabe wurden an den ersten vier Rängen genannt: Ausbildung des Dienstleistungspersonals, Sprachkenntnisse (deutsch) des Personals, kein Einsatz von Subunternehmen und Berufserfahrung des Dienstleisterpersonals. An letzter (21.) Stelle steht die „Paketlösung mit Sicherheitstechnik". Gefragt wurde auch nach den „skills", die besonders günstige Voraussetzungen für eine leitende Tätigkeit in der Unternehmenssicherheit sein sollen. Bei den Antworten nehmen die ersten sechs Plätze ein: Branchenerfahrung, Erfahrung in Sicherheitsbehörden, allgemeine Technikkenntnisse, Kenntnisse der IT-Sicherheit, Auslandserfahrung und Studium des Sicherheitsmanagements.

In derselben Ausgabe berichtet WiK über Ergebnisse der branchenübergreifenden Studie **„Corporate Entrepreneurship (SIIE)** der EBS Business School und des Beratungsunternehmens Z_punkt. Befragt wurden 66 Sicherheitsexperten und 34 Manager ohne Sicherheitsbezug (S. 32). Beide Gruppen sähen im Schutz von Know-how, von Informationen und Daten die wichtigste Aufgabe

für die Unternehmenssicherheit der Zukunft. Als wichtigste Maßnahme werde dabei neben rein technologischen Lösungen gesehen, den Faktor Mensch stärker einzubeziehen. So sollten Wissensträger langfristig an das eigene Unternehmen gebunden werden. Outsourcing und der für die Innovation bedeutsame Informationsaustausch würden wichtiger, müssten aber so geregelt werden können, dass die für das Unternehmen wichtigen Informationen geschützt werden können.

Veranstaltungsschutz

Thomas Semmler, M.A., Fachjournalist, stellt in der Ausgabe 3-2015 der Zeitschrift WiK das **Forschungsprojekt MultikOSi** (Multikriterielle Vernetzung für Offenheit und Sicherheit) vor, das den Weg zu mehr Sicherheit bei Events ebnen soll. Es verbinde Hochschulkompetenzen mit dem Know-how mehrerer Unternehmen mit dem Ziel, bis Mitte 2016 eine leicht zu nutzende Planungshilfe in einem exemplarisch implementierten Online-Tool zur Verfügung zu stellen. Neben Masken zur Erhebung von Grunddaten und organisatorischen Rahmenparametern würde auch die Integration von OpenStreetMap-Karten und CAD-Plänen, also interaktive Kartenmaterialien nutzbar sein. Auf diesen Materialien ließen sich Haltestellen für Busse ebenso wie Essens- und andere Stände variabel platzieren, bis der perfekte Stellplatz gefunden sei. Auch Warteschlangen im Einlass und das Verhalten der Besucher könnten simuliert werden, vom Schlendern über Anstehen bis zur Entfluchtung.

In der Juni-Ausgabe des Behörden Spiegel äußert sich Olaf Jastrob, Sicherheitsberater, zur neuen **Muster-Verordnung,** die der Bund 2014 eingeführt hat. Zu den wichtigsten Änderungen zählt der Autor folgende Bereiche:

1. Um problematische Wartezeiten bei Räumungen zu vermeiden, müssten Versammlungsräume für mehr als 100 Besucher künftig zwei möglichst weit auseinanderliegende Ausgänge vorweisen.

2. Bei der Berechnung zur Breite der Rettungswege entstehe fortan mehr Spielraum, wenn Veranstalter nachweisen können, dass sich Räumungszeiten entsprechend verringern.

3. Versammlungs- und Aufenthaltsräume müssten zur Unterstützung der Brandbekämpfung durch die Feuerwehr entraucht werden können. Hier gebe es umfängliche Anforderungen an die Rauchableitung.

4. Unter bestimmten Voraussetzungen müsse künftig ein Räumungskonzept erstellt werden.

Die gravierendste Änderung, der geänderte Anwendungsbereich der Verordnung bei sogenannten Open Air-Veranstaltungen, sei ein Rückschritt. Künftig würden Versammlungsstätten im Freien nur noch dann zur MVStättVO zählen, wenn sie Szenenflächen und Tribünen besitzen, die keine fliegenden Bauten sind und mehr als 1.000 Besucher fassen. Somit fielen Open Air-Veranstaltungen, die von einem Bauzaun umgeben sind, aus dem Geltungsbereich der MVStättVO.

Carsten Laube, Doris Dobranic und Philipp Kuschewski, Deutsche Hochschule der Polizei, stellen in der Juniausgabe des Behörden Spiegel **Polizeiliche Handlungsempfehlungen** zum Management von Großveranstaltungen vor. Bundesweit seien einsatztaktische Erfahrungen unmittelbar aus der Praxis hinsichtlich der Vorbereitung, Durchführung und Nachbereitung polizeilicher Einsätze bei Großveranstaltungen gewonnen und ausgewertet worden. Die Handlungsempfehlungen seien 17 unterschiedlichen Themenfeldern zugeordnet, welche die wesentlichen Aspekte des polizeilichen Einsatzhandelns

abdeckten. Dieser Bogen spanne sich, angefangen von der Gefährdungsbewertung, dem Genehmigungsverfahren oder der Erstellung des Sicherheitskonzepts, über die Strukturierung einer besonderen Aufbauorganisation, die szenarienabhängige Maßnahmenplanung, das Krisenmanagement im Ereignisfall oder ein zielgerichtetes Besucher- und Crowd-Management bis hin zur Einsatznachbereitung. Ein besonderes Augenmerk liege dabei auch auf dem Aspekt der interorganisationalen Zusammenarbeit mit nichtpolizeilichen Akteuren.

Verschlüsselung

Zwei Drittel der mittelständischen Unternehmen haben laut einer aktuellen Studie von QSC Tools zur E-Mail-Verschlüsselung im Einsatz, meldet die Zeitschrift WiK in der Ausgabe 3-2015 (S. 9). Allerdings würden diese nur von der Hälfte der Mitarbeiter genutzt, obwohl der große Teil dieser Daten als unternehmenskritisch eingestuft werde. Als Hindernisse würden die befragten Unternehmen Lizenzkosten und Akzeptanzprobleme bei den Anwendern nennen.

Verschlüsselungsverfahren

Tobias Elsner, yet GmbH, befasst sich in der Juni-Ausgabe des Behörden Spiegel mit der Sicherheit von Verschlüsselungsverfahren. Bei der **Auswahl von Kryptosoftware** sollte darauf geachtet werden, dass allgemein anerkannte Standardverfahren eingesetzt werden. Ein Anbieter, der ein Produkt als besonders sicher, weil mit brandneuen und geheimen Verfahren arbeitend, anpreist, sei unseriös. Idealerweise sollte auch die Implementierung öffentlich zugänglich sein (freie Software) und einen intensiven Reviewprozess durchlaufen haben. Abgesehen von der Auswahl des Verfahrens spiele auch die Schlüssellänge eine entscheidende Rolle. AES gelte mit 256 Bit Schlüssellänge als ausreichend sicher, während asymmetrische Verfahren wie RSA deutlich mehr, nämlich 2.048 Bit, benötigten. Entscheidend sei weiterhin eine sichere Erzeugung und Verwaltung der Schlüssel. Für ersteres sei ein kryptografisch sicherer Zufallszahlengenerator notwendig. Für Anwendungen mit hohem Schutzbedarf sollte auf Hardware-Zufallsgeneratoren zurückgegriffen werden, die auf quantenphysikalischen Effekten basieren. Schlüssel sollten dort erzeugt bzw. gespeichert werden, wo sie zum Einsatz kommen, also zum Beispiel auf den Endgeräten von Anwendern bei Ende-zu-Ende-Verschlüsselung. Als Zugeständnis an die Verwaltbarkeit sei der Einsatz von Hardware Security Modulen denkbar. Nicht zu empfehlen seien Cloudlösungen, bei denen die Schlüssel beim Anbieter erzeugt und/oder gespeichert werden. Bei der Verschlüsselung von Datenströmen sollte außerdem darauf geachtet werden, dass stets neue Sitzungsschlüssel erzeugt werden (Forward Secrecy).

Videoüberwachung

IP-Video im Einzelhandel thematisiert Silke Stumvoll, Axis Communications GmbH, in der Ausgabe 6-2015 der Fachzeitschrift GIT (S. 78/79). Eine Einsatzmöglichkeit finde sich im Bereich Point of Sale (POS). Netzwerkvideolösungen würden schnell und effizient helfen, häufig vorkommende Fehler aufzudecken, Missstände aufzuklären und innovative Manipulationen des POS-Systems nachzuweisen. Zusatzapplikationen wie die Personenzählung oder das sogenannte Heat-Mapping würden immer wichtiger für Erfolgsmessung von Sonderaktionen, aber auch für die Frage, ob sich die Kunden im Geschäft wohlfühlen. In Kombination mit einer Personenzählung für den Laden insgesamt und in speziellen Zonen sowie einer Anbindung an die Kassendaten könne der Einzelhändler ein exaktes Bild des Kaufverhaltens sehen.

Vorgestellt wird in der Ausgabe 6-2015 der Zeitschrift GIT (S. 82/83) von der Securiton GmbH ein Videoüberwachungssystem zum **Schutz Kritischer Infrastrukturen.** Die Kernfunktion des Systems sei ein Drei-Zonen-Konzept, das Erfassungs-, Alarm- und Prioritätszone unterscheide. Alarm werde ausgelöst, wenn sich eine Person aus der Erfassungszone heraus und in die Alarmzone hinein begibt oder sich in der Prioritätszone bewegt. Die intelligente Analyse-Software könne auch Manipulationsversuche wie zum Beispiel das Zusprühen mit einer Spraydose, das Blenden und Verdrehen der Kamera sowie die Trennung der Stromzufuhr bemerken. Die intelligente Software spiele ihre Stärken in Verbindung mit Wärmebildkameras aus: Diese lieferten klare und kontrastreiche Aufnahmen bei jeder Witterung und bräuchten keine künstliche Beleuchtung.

In der Juni-Ausgabe von Veko-online wird die neueste **Version 6.0 des IPS VideoManagers** von Securiton vorgestellt. Im Vordergrund stünden eine deutliche Steigerung der Leistungsfähigkeit durch 64-Bit-Versionen von Multi Site Management, Device Server und aller Analysemodule sowie neue Funktionen, unter anderen die Ergänzung der Analyse IPS Outdoor Detection um einen weiteren leistungsstarken Filter zur Erkennung von Scheinwerferlicht und die Weiterentwicklung des IPS Dome Tracker zur Verfolgung von Objekten über große Liegenschaften hinweg trotz schwieriger Umgebungsbedingungen.

Wohnungseinbruchdiebstahl

Die Zeitschrift WiK weist in der Ausgabe 3-2015 (S. 11) auf zwei Neuerungen hin: Ein neuer, **vom Fraunhofer IMS entwickelter Funkchip,** der sich per Solarzelle selbst für bis zu 30 Stunden mit Energie versorge, solle künftig Hausbewohner darüber informieren, wenn Fenster geöffnet sind. Das System unterscheide zwischen verschiedenen Schwingungen – beispielsweise zwischen einem Ball, der die Scheibe trifft, oder dem Stemmeisen eines Einbrechers. Montiert werde der Chip direkt zwischen die Glasscheiben auf das Aluminiumprofil, das die Scheiben auf Abstand hält. ComfyLight nenne sich eine Glühbirne, die mittels eingebauter Sensoren auch als Einbruchmelder fungieren solle. Per WLAN sei sie zudem mit dem Internet verbunden und könne per App einen Alarm- oder Statusbericht senden. Mehrere Birnen könnten vernetzt werden. Per Dauerblinken solle sie im Alarmfall den Einbrecher in die Flucht jagen. Zudem solle sie sich während der Abwesenheit der Bewohner in einem bestimmten Muster ein- und ausschalten. Anbieter des ab Oktober 2015 verfügbaren LED-Leuchtkörpers mit E27-Sockel (99 Euro) sei Comfy.

Zahlungskartenkriminalität

Nach dem vom BKA veröffentlichten **Bundeslagebild** Zahlungskartenkriminalität wurde 2014 in Deutschland mit insgesamt 222 Angriffen auf Geldautomaten zur Erlangung von Kartendaten und PIN erneut ein Rückgang der Skimming-Straftaten um rund 54 Prozent registriert. Durch die sicherheitstechnische Aufrüstung von Türöffnern zu Bankfoyers seien Kartendatenabgriffe in diesem Bereich nahezu bedeutungslos geworden. Es bleibe abzuwarten, ob Zahlungskartenkriminalität in Deutschland dauerhaft an Bedeutung verliert. Eine Zusammenfassung des BKA-Lagebildes ist auf der Securitas-Webseite unter www.securitas.com/de/de/news/sicherheitslage/zahlungskartenkriminalitaet enthalten.

Zutrittskontrolle

Wie bewährte Zutrittstechnologie für die Zukunft fit gemacht werde, erklärt Ralf Grammel, Sympatron, in Ausgabe 6-2015 der Zeitschrift GIT (S. 86–88). Die multifunktionale und modulare **Sicherheitsplattform Patronum** integriere auch herstellerübergreifende Anwendungen auf einer Plattform. Der Anwender nutze mit Patronum weitere Funktionen und Systeme wie Videokontrolle, Payment, Biometrie, Alarme, Einbruchmeldetechnik usw. in einem System. Nicht nur die Zutrittslösungen von Siemens seien in die Plattform integriert, auch Zutrittssysteme von Salto und Payton oder die Videotechnik von Milestone, biometrische Systeme von TBS seien voll nutzbar.

Die Zeitschrift Sicherheitsforum hat im Juni 2015 eine Sonderausgabe Zutrittskontrolle veröffentlicht, die eine **Marktübersicht** über Zutrittskontrollsysteme von 34 Anbietern enthält (S. 37–71). Sie umfasst Angaben der Hersteller zur Serviceorganisation, dem Tätigkeitsgebiet, der Instandhaltung, Instandsetzung, Software-Updates, Software-Upgrades, Benutzerschulung und Migration. Roland Hunkeler, Siemens Building Technologies, befasst sich mit dem **Identity Access Management.** Global tätige Unternehmen mit mehreren Standorten sähen sich vermehrt mit Zutrittskontrollsystemen unterschiedlicher Hersteller konfrontiert. Das erschwere die standortübergreifende Zutrittsvergabe und erhöhe Risiken und Kosten. Eine prozessautomatisierte Zutrittskontrolle wirke dem entgegen und erleichtere die täglichen Bewilligungsprozesse. Die aktuellen Trends zeigten eine steigende Nachfrage nach IAM-Lösungen (S. 6/7).

Dipl.-Ing. Lutz Kirberg geht auf **Near Field Communication (NFC)** ein. Mehrwerte ließen sich mittels NFC über den Übertragungswert generieren, aber auch durch die Möglichkeit der interaktiven Kommunikation und Informationsdarstellung auf dem Display des Smartphones. Doch trotz des potenziellen Mehrwerts würden die herkömmlichen Chipkarten und Badges dem Smartphone mit NFC vorgezogen. Dies liege sicherlich auch an dem finanziellen Unterschied, den die Anschaffung eines Smartphones gegenüber einer Chipkarte ausmacht. Ob NFC in einem Unternehmen Berücksichtigung finden sollte, könne im Rahmen der Anforderungsdefinition an das Zutrittskontrollsystem identifiziert werden (S. 9).

Dipl.-Ing. Klaus Behling, von zur Mühlen'sche GmbH, erläutert die **System-Implementierung.** Zunächst gelte es, die Nutzerbedürfnisse zu identifizieren. Es müssten aber auch Projektgrenzen definiert werden. Im nächsten Schritt gelte es, allgemein gültige Standards für alle genutzten Gebäude und deren Teilbereiche zu entwickeln. Bearbeitet werden müssten: Risikoanalyse und -bewertung für unterschiedliche Gebäudekategorien, Definition allgemeiner Schutzziele für unterschiedliche Gebäudekategorien, Erarbeiten eines allgemein gültigen Schutzzonenmodells und Definition von schutzzonenbezogenen Zielen. Daraus ergäben sich automatisch die Anforderungen an die Zutrittssicherheit der einzelnen Zonenübergänge (S. 11–13).

Almut Eger, 4m2s – 4 Management 2 Security GmbH, behandelt die **ISO-Norm 27001** im Zusammenhang mit Zutrittskontrollsystemen. Vor der Implementierung eines Zutrittskontrollsystems, das mit einem Sicherheits- und Gebäude-Managementleitsystem verbunden wird, müssten die entsprechenden Prozesse genau definiert werden. Und sie erforderten eine umfassende Planung im Sinne eines echten Integrierten Managementsystems. Die Betriebsdaten für komplexe Systeme könnten unter anderem bei der Zutrittskontrolle gesammelt werden. Sie dienten der Prozesssteuerung in Bezug auf Qualität, Arbeitssicherheit und Informationssicherheit. Die entsprechenden ISO-Normen würden als methodischer Hintergrund gelten.

Best Practice liege in der pragmatischen Umsetzung. Die Herausforderung bestehe darin, die Anforderungen aller drei Aspekte zu integrieren, in einem unternehmensweiten integrierten Konzept. Bei einer praxisgerechten Umsetzung der Normen könnten diese Abläufe und Prozesse kontinuierlich verbessert und im Rahmen eines Integrierten Managementsystems gepflegt und weiterentwickelt werden (S. 22–25).

Die Fachzeitschrift PROTECTOR hat im Juni ein **Special Zutrittskontrolle** veröffentlicht. Berichtet wird zunächst über Ergebnisse des 9. PROTECTOR-Forums Zutrittskontrolle (S. 8–31). Vor dem Hintergrund aktueller Trends und Entwicklungen hätten die Forumsteilnehmer intensiv den Stellenwert von Zertifizierungen diskutiert. Wenn es um die Einschätzung der Bedeutung von Zertifizierungs- und Regelungsinstanzen für die Branche ging, sei der Begriff BSI, das verstärkt auf IT-Standards setze, in aller Munde gewesen. Vom VdS habe in diesem Zusammenhang kaum jemand gesprochen. Weitere Themen seien unter anderen die Annäherung von Online- und Offlinesystemen, Planung und Beratung sowie aktuelle Entwicklungen in der Frage nach den Standardisierungsbemühungen durch NFC, SOAA (Standard Offline Access Application) oder auch Onvif (offenes Industrieforum) gewesen. Letztlich müssten Anwender Standards einfordern und bereit sein, mit Pilotprojekten voranzugehen, damit die Verbreitung Fahrt aufnehmen könne. Axel Schmidt, Salto Systems GmbH, plädiert für kabellose elektronische Systeme (S. 36–38). Bei der Auswahl des Systems sei es wichtig, auf folgende vier Aspekte zu achten: Erstens sollten die Daten nicht nur von der Karte zum Beschlag oder Zylinder transportiert werden, sondern auch vom Beschlag oder Zylinder zur Karte. Die Identifikationstechnologie auf der Karte sollte zudem hochsicher sein. Empfehlen würden sich RFID-Lösungen mit 13,56 Megahertz, die eine AES 128 Bit-Verschlüsselung bieten. Bei der Systemauswahl sollte man auch bedenken, dass jeder elektronische Ausweis eine einmalige Identifikationsnummer besitzt. Zudem sollte der Anbieter der Zutrittslösung eine große Auswahl an Komponenten und deren Varianten liefern können.

Thomas Lang, Axis Communications GmbH, sieht einen Trend zu offenen Systemen (S. 40/41). Nach Schätzungen des Analysten IHS werde der Markt für Zutrittskontrolle bis 2017 auf einen Wert von 4,2 Mrd. US-Dollar ansteigen. Dabei werde die Zutrittskontrolle zunehmend auch in die Videoüberwachung integriert. Mit einem IP-basierten System werde jede Zutrittskontrolleinheit zu einem intelligenten, unabhängigen Gerät. Da IP-basierte Zutrittskontrolleinheiten mit offener API eine integrationsfreundliche offene Plattform darstellen, könnten mehrere Arten von Software parallel laufen.

Julian Lovelock, HID Global, stellt die Frage „Karte oder Smartphone?". Es sei davon auszugehen, dass künftig beide Medien in einem zentralisierten Identitätsmanagementsystem nahtlos zusammenarbeiten. Neben mehr Komfort und Sicherheit verspreche die Bereitstellung verschiedener IDs für IT-Datenzugriff und Zutrittskontrolle auf einer Smartcard oder einem Smartphone mittels einheitlicher Prozesse auch niedrigere Betriebskosten (S. 42). Die Nachfrage nach Zutrittskontrollsystemen, die gemeinsam mit Kamera-, Brandmelde- und Einbruchmeldesystemen in einer Plattform integriert sind, über die sie gesteuert und verwaltet werden können, nehme laut einer Marktanalyse ständig zu (S. 43).

Matthias Daszenies, Plasticard-ZFT GmbH, befasst sich mit der Multiapplikationsfähigkeit, einem Standardmerkmal moderner RFID-Chips, die in der Sicherheits- und Zugangsbranche verwendet werden (S. 44/45). In Ausweiskarten für aktuelle Projekte werde diese Funktionalität als Selbstverständlichkeit genutzt. Chipentwickler und Systemhäuser würden alles dafür tun, dass die vielfältigen Anwendungen in einem Unternehmen mit genau einem Medium bedient werden

können. Der Autor erläutert die technischen Voraussetzungen der aktuell verbreitetsten multifunktionsfähigen ID-Chipsysteme Legic Advant und Mifare Disfire.

Dipl.-Phys. Bernd Schöne befürchtet, dass hochauflösende Kameras Biometrie aushebeln (S. 48–50). Bei der hohen Auflösung moderner Kameras reiche dem Hacker eine Daumenkuppe oder ein Auge am Bildrand aus. Gegen leichte Unschärfen würden moderne Bildbearbeitungsprogramme helfen.

In dem Special hat PROTECTOR auch **Marktübersichten** zu Stand-alone-Terminals für Zutrittskontrollsysteme (77 Anbieter mit 160 Systemen), für Biometrielösungen (59 Anbieter mit 109 Systemen), Zutrittskontrollsoftware (91 Anbieter mit 131 Systemen) und Zutrittskontrollzentralen (82 Anbieter mit 138 Systemen) zusammengestellt (S. 51–59).

Impressum

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

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

Herausgeber:
Manfred Buhl, Vorsitzender der Geschäftsführung, Düsseldorf

Verantwortlicher Redakteur:
Bernd Weiler, Leiter Kommunikation und Marketing

Beratender Redakteur:
Reinhard Rupprecht, Bonn

focus.securitas.de

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

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

E-Mail: info@securitas.de