Focus on Security

Ausgabe 03, März 2015

SECURITAS

Informationen zum Unternehmensschutz

Anschläge ... **3**
Arbeitsschutz ... **3**
Arzneimittelfälschung ... **4**
Betriebsschutz-Sachverständiger ... **4**
Betrug ... **4**
Biometrie ... **5**
Brandmeldesysteme ... **5**
Brandschutz ... **5**
Business Continuity Management ... **7**
Diebstahl ... **7**
Drohnen ... **8**
Einbruch ... **8**
Einzelhandelssicherheit ... **9**
Endgerätesicherheit ... **9**
Falschgeld ... **10**
Forensik ... **10**
Gefährdungslagebild Griechenland ... **10**
Gefahrstofflagerung ... **11**
Geschäftsgeheimnisse ... **11**
Geschäftsreisen ... **11**
IT-Sicherheit ... **12**
IuK-Kriminalität ... **13**
Juwelenraub ... **14**
Korruption ... **15**
Krisenregionen ... **15**
Ladungsdiebstahl ... **15**
Luftsicherheit ... **16**
Maschinensicherheit ... **16**
Mechatronik ... **17**
Mitarbeiterkriminalität ... **17**
Personennotruf ... **17**
Produkterpressung ... **18**
Produktpiraterie ... **18**
Schwarzarbeit ... **19**
Security LAN ... **19**
Shutdown industrieller Großanlagen ... **19**
Sicherheitssysteme ... **20**
Stromsicherheit ... **20**
Terrorismus ... **21**
Verfassungsschutz ... **22**
Verschlüsselung ... **22**
Videoüberwachung ... **22**
Zufahrtskontrolle ... **23**
Zutrittskontrolle ... **24**

Anschläge

Wie das BKA am 6. Februar mitteilt, setzten am 29. Januar unbekannte Täter in Berlin-Lichtenberg einen Kleintransporter der Firma **WISAG** in Brand. Die Flammen griffen auf einen davor stehenden VW Caddy über. In Berlin-Mitte wurde in derselben Nacht ein Kleintransporter der Firma **SODEXO** in Brand gesetzt. In einem Schreiben auf der Internetseite „linksunten.indymedia.org" bekannte sich eine „Autonome Gruppe Muslim H." zu den Brandstiftungen und stellte diese in den Begründungszusammenhang „Repression".

Die Selbstbezichtigung endete mit dem Aufruf „Am 18. März auf nach Frankfurt – EZB in Schutt und Asche legen". Am 18. März wird der Neubau der EZB eröffnet. Die linke Szene bzw. die Blockupy-Bewegung mobilisiert schon seit geraumer Zeit unter dem Rubrum der Kapitalismuskritik eine Blockadeaktion gegen die Veranstaltung. Die oben genannten Firmen werden von Angehörigen der linken Szene als „Handlanger des Repressionsapparates" angesehen.

Arbeitsschutz

80 Prozent der im Rahmen einer Arbeitsschutz-Studie von Messtechnik-Hersteller TSI befragten 210 Fachkräfte würden nicht für den Einsatz von **Atemschutz-Maßnahmen** trainiert, meldet die Zeitschrift GIT in der Ausgabe 1/2-2015 (S. 30). Trotz der kaum ausreichenden Trainingsmaßnahmen fühlten sich die Mitarbeiter sicher. 92 Prozent sähen den eigenen Arbeitsplatz als geschützt an. Von den 210 befragten Personen aus unterschiedlichen Unternehmen hätten 29 Prozent angegeben, dass innerhalb der letzten zwölf Monate Verstöße gegen den Arbeitsschutz vorkamen.

Die geplante **Reform der Arbeitsstättenverordnung** stecke voller Tücken, meint die FAZ am 18. Februar. Viele Empfangsbereiche, etwa in Hotels, Arztpraxen und Verwaltungsgebäuden könnten bald keine zulässigen Arbeitsplätze mehr sein. Denn die geplante VO würde nur wenige Ausnahmen von der verschärften Fensterpflicht („Sichtverbindung nach außen") zulassen: etwa für Verkaufsräume und Gaststätten, die sich in großen Kaufhäusern oder vollständig unter der Erde befinden; außerdem für Arbeitsräume, bei denen der Verzicht auf Fenster „betriebstechnisch" erforderlich ist, und für bestimmte Typen größerer Werkhallen. Die Arbeitsgeber hätten eine Liste an Vorschlägen zusammengestellt, was geändert werden müsste, damit die Nachteile für die Wirtschaft nicht zu groß würden. Die Kritik betrifft etwa die Baustellensicherheit, Bildschirm- und Telearbeit und die Pflicht, jedem Mitarbeiter eine abschließbare Kleiderablage zu stellen. Das Licht für Arbeitsräume, Bereitschaftsräume, Kantinen und Unterkünfte soll nicht – wie nach den bisherigen Vorschriften – „möglichst" Tageslicht sein, sondern „muss" durch ein Außenfenster hereinfallen. Andere Verschärfungen ergäben sich dadurch, dass der Begriff „Arbeitsplatz" über Dauerarbeitsplätze hinaus weiter gefasst werden soll.

Arzneimittelfälschung

Neben Italien entwickele sich **Rumänien** zunehmend zur Drehscheibe des illegalen Arzneimittelhandels, berichtet die WirtschaftsWoche am 14. Februar. Erst 2014 sei bekannt geworden, dass die Mafia in großem Stil Medikamente aus italienischen Kliniken stiehlt, über dunkle Kanäle lande die Arznei dann bei deutschen Apotheken und Großhändlern. Nun errege ein neuer Fall Aufsehen. Ende Januar seien aus dem Kreiskrankenhaus im rumänischen Braila große Mengen der Krebsmittel Avastin und Herceptin gestohlen worden. Wert: 400.000 Euro. Es bestehe die Gefahr, dass diese Medikamente ungekühlt gelagert und damit wirkungslos werden. Sie würden daher als Fälschungen gelten. Gleichzeitig stelle sich heraus, dass der Medikamentenklau in Italien noch größere Dimensionen habe als bisher angenommen. Das Bundesinstitut für Arzneimittel und Medizinprodukte spreche von weiteren 390 illegalen Transaktionen.

Betriebsschutz-Sachverständiger

Alexander Krause, Certified Protection Professional der ASIS International, geht in Security insight (Ausgabe 1-2015, S. 32–34) der Frage nach, warum es in der Sicherheitswirtschaft immer mehr Sachverständige gäbe, von denen die wenigsten sich der öffentlichen Bestellung unterziehen. Die Bezeichnung „Sachverständiger" dürfe in Deutschland jeder tragen. Die Nutzung sei nur dann unzulässig, wenn die Qualifikation, also das erforderliche Fachwissen und die ausreichende Berufserfahrung fehlen. Dann liege ein Verstoß gegen das UWG vor. Die besondere Sachkunde bei öffentlich bestellten und vereidigten Sachverständigen müsse dagegen nachgewiesen werden. Das geschehe vor den Ingenieur-, Architekten-, Handwerks- oder Industrie- und Handelskammern. Dieses Bestellungsverfahren dauere mehrere Monate. Wenn man externen Sachverstand benötigt, spreche sehr viel für die ausschließliche Beauftragung eines öffentlich bestellten und vereidigten Sachverständigen. Nur er biete die gesetzlich verankerte Gewähr für unabhängige, weisungsfreie, persönliche, gewissenhafte und unparteiische Gutachten. Der DIHK subsumiere den Security-Bereich unter dem Begriff „Betriebsschutz". Das Sachverständigenverzeichnis des DIHK kenne dazu fünf Einträge.

Betrug

Mit den Tricks der **Bankbetrüger** befasst sich die FAZ am 11. Februar. Sie versuchten, sich Zugänge zu Konten und Krediten zu verschaffen. Eines der spektakulärsten Fundstücke seien 52 französische Ausweise eines Betrügers, der in einer Bank überführt worden sei – 52-mal dasselbe Gesicht, 52-mal völlig unterschiedliche Identitäten. Durch das Internet werde es immer leichter, sich falsche Stempel mit den Originalemblemen zu besorgen. Führerscheine mit Hilfe von Farbdruckern, die 37 verschiedene Farbtöne unterscheiden, Prägemaschinen für Kreditkartenfälschungen, Foliermaschinen vom Elektrofachhandel – die Instrumente der professionellen Fälscher würden immer ausgefeilter. Gleichzeitig seien die meisten Banken nicht optimal auf solche Vergehen vorbereitet. Um die Täter zu fassen, die es nacheinander in verschiedenen Bankfilialen versuchten,

wollen einige Banken schon seit vielen Jahren miteinander Informationen austauschen. Datenschutzrechtliche Bedenken hätten aber den Start eines gemeinsamen „Fraud Pools" um eineinhalb Jahrzehnte verzögert. 2014 habe die Kreditauskunftei Schufa eine gemeinsame Datenbank gestartet, die derzeit 13 Banken nutzen. Mit Onlinebanking habe die Anfälligkeit für Betrug zugenommen. Zuletzt habe die deutsche Polizei jährlich 65.000 Urkundenfälschungen aufgedeckt. Es gebe 3.000 Direktbanken in Deutschland. Die ließen sich überwiegend Kopien vom Personalausweis schicken. Es bestünden Zweifel, dass die Banken die Prüfung akribisch genug vornehmen.

Biometrie

Eine Vorführung auf dem 31. Chaos Communication Congress in Hamburg habe gezeigt, dass man mittlerweile mit einer Digitalkamera an Fingerabdrücke Dritter gelangen könne, um biometrische Authentifizierungssysteme zu überwinden, schreibt die FAZ am 10. Februar. Dies solle man zum Anlass nehmen, sich mit der **Sprachbiometrie** zu beschäftigen. Sie basiere auf der Einzigartigkeit der menschlichen Stimme. Aus ihr seien rund 150 unterschiedliche Merkmale extrahierbar, dafür benötige man eine mehrminütige Aufzeichnung. Man könne die Stimme mit einem gewöhnlichen Kennwort kombinieren. Wer sich authentifizieren will, müsse dann zwei Bedingungen erfüllen: die richtige Stimme und die zugehörige Passphrase. Im Unterschied zu anderen Kennwortschutz-Verfahren arbeite die Sprachbiometrie mit Wahrscheinlichkeiten. Die Falschakzeptanzrate liege bei null. Der Wert gebe die Wahrscheinlichkeit an, mit der ein Sicherheitssystem den Zugang für Personen gewährt, die keine Zugangsberechtigung haben. Sprachbiometrie sei so sicher wie die Erkennung einer Person über ihren Fingerabdruck. Und im Unterschied zu einem Fingerabdruck lasse sich natürlich die Passphrase wechseln. Bislang kämen Sprachbiometriesysteme vor allem bei Banken und Mobilfunkanbietern zum Einsatz.

Brandmeldesysteme

Die Zeitschrift PROTECTOR enthält in der Ausgabe 1/2-2015 auf S. 28/29 eine **Marktübersicht** über 63 Brandmeldesysteme von 31 Anbietern. Abgefragt wurden 35 Kriterien aus den Bereichen Vernetzung, Fernbedienung, Löschanlagensteuerung, Datenschnittstellen, Lageplantableau, Zugriffsschutz und Ereignisspeicher.

Brandschutz

Mit Brandbekämpfung mittels **Hochdrucknebel** befasst sich Helmut Jung, K. A. Schmersal, in der Fachzeitschrift GIT (Ausgabe 1/2-2015 S. 82–84). Anders als bei einer Sprinkleranlage umgebe der Wassernebel die Gegenstände im Raum auch seitlich und von unten. Zudem werde die Bildung von Rauchgas und Ruß unterdrückt. Die Kühlwirkung sei aufgrund der sehr geringen Tröpfchengröße besser, und die peripheren Schäden würden im Vergleich zu traditionellen Spinkleranlagen deutlich vermindert. Aus diesen Gründen kämen die HDWN-Anlagen häufig in sensiblen Anwendungen zum Einsatz – etwa in Bibliotheken, Kliniken,

Chemieanlagen, Sicherheitslaboren, Entwicklungszentren und Produktionsbereichen. Ein zuverlässiger Betrieb von Löschanlagen – gerade in sensiblen Bereichen – erfordere, dass die Steuerung nicht nur alle Betriebszustände, sondern auch die Fehler im gesamten System erkennt, anzeigt und entsprechend weiterleitet. Dieselben Anforderungen würden auch für sichere Schaltsysteme im Maschinen- und Anlagenbau gelten und aus diesem Anwendungsbereich stammt die Steuerung, nämlich das Protect Select-System von Schmersal, das Callies, Hersteller von Hochdruck-Wassernebel-Löschsystemen, einsetzt.

Mehrere Brandschutzthemen enthält die Ausgabe 1/2-2015 der Fachzeitschrift PROTECTOR: Sie stellt ein **Brandschutzkonzept für Hochregallager** vor (S. 16–18). In einem Hochregallager müsse die vorgeschriebene Sprinkleranlage das Feuer weitestgehend selbstständig löschen. Die höhere Dichte an Stellplätzen in einem vollautomatisierten Kompaktlager erfordere eine entsprechend angepasste Besprinklerung, auch wenn die Rohstoffe und das fertige Produkt selbst eigentlich nicht brennbar sind. Brennbar seien aber die Paletten. Hinzu käme der „Kamineffekt". Nicht zuletzt deshalb forderten etwa die Sachversicherer für Lager ab einer bestimmten Höhe und Automationsgrad neben einer Deckensprinkleranlage zusätzlich ein Regalsprinklersystem. Die Anzahl der Sprinklerköpfe bemesse sich dabei nach der Dichte an Paletten und deren Material. Aufgrund der besonderen Konstruktion eines Hochregallagers sei bereits bei der Konzeption eine enge Zusammenarbeit aller Beteiligten, die für Sicherheit und Brandschutz verantwortlich sind, von Beginn sinnvoll und notwendig. Mark Egbers, Pfannenberg Europe GmbH, und Patrick Banholzer, Hekatron, behandeln **Auswirkungen der EN 54-23 auf optische Signalgeber** (S. 22/23). Die erhöhten Anforderungen dieser Produktnorm für optische Signalgeber führten dazu, dass besonderes Augenmerk auf die Auswahl der richtigen Produkte in der jeweiligen Anwendung gelegt werden müsse. Aktuell zeichne sich ab, dass es zwei Arten von optischen Signalgebern geben werde: zum einen Geräte mit LED-Technologie, die in den Kategorien W und C zugelassen sind. Diese Geräte würden ihren Einsatz speziell im Bereich von Verwaltungen mit kleinen Räumen finden. Alternativ seien auch Geräte mit Xenon-Technologie verfügbar, die vermehrt in der Kategorie O zugelassen sind. Diese Geräte fänden ihre Anwendung speziell in Produktionsstätten klassischer Industrie. Hier werde es zukünftig zugelassene Geräte geben, die Deckenhöhen bis 13,5 Meter mit einer Grundfläche von circa 27 x 25 Metern abdecken könnten. Vera Klopprogge, Siemens Building Technologies, stellt **intelligente Brandschutztechnik in Forschungseinrichtungen** vor (S. 24/25). Sensible Substanzen und aufwendige Prozesse, das bedeute auch spezielle Anforderungen an den technischen Brandschutz. In solchen Umgebungen kämen täuschungssichere Brandmelder zum Einsatz, die für ein optimales Gefahrenmanagement mit der Brandmelde- und Gebäudetechnik intelligent verknüpft werden könnten. Typische Brandursachen in solchen Umgebungen seien unter anderem Schwelbrände aufgrund von Elektrorisiken, die Selbstentzündung von Ablagerungen in Lüftungskanälen oder das Austreten leicht entzündlicher Flüssigkeiten und Gase. Zur zuverlässigen frühzeitigen Erkennung entstehender Brände komme in Forschungseinrichtungen das ganze Spektrum von Brand-, Wärme- und Flammenmeldern zum Einsatz. Brandmelder müssen auch die erfassten Werte korrekt interpretieren können. Neue Ansaugrauchmelder würden in der Messkammer die Größe von Partikeln und deren Konzentrationen erkennen. Dabei komme die optische Dualwellen-Detektion zum Einsatz. Das heiße, die Melder nutzen zur Erkennung zwei Lichtwellenlängen: blaue und infrarote. Damit könnten sie genau zwischen Rauch und Täuschungsgrößen unterscheiden. Neben Ansaugmeldern könnten auch lineare Wärmemelder spezielle Brandschutzaufgaben im Labor übernehmen. Sie würden erste Anzeichen eines Brandes schon innerhalb weniger Sekunden erkennen und böten außerdem häufig eine automatische Brandlöschung. Ein

weiterer Beitrag befasst sich mit der **Löschanlage im Rechenzentrum** (S. 26/27). Das Löschmittel Novec 1230 werde allen Anforderungen des Brandschutzes im Rechenzentrum gerecht. Es könne sehr platzsparend bevorratet werden – im direkten Vergleich benötige eine CO_2-Löschlösung die fünf- bis sechsfache Fläche. Einen weiteren Vorteil stelle vor diesem Hintergrund auch das geringere Gewicht und damit einhergehend die statische Belastung dar, die – je nach Standort der Löschflaschen – entscheidend sein könne. Zudem sei es aufgrund der geringeren Menge wesentlich wirtschaftlicher als andere Lösungen. Weitere Pluspunkte böten die human- und technikverträglichen Eigenschaften von Novec 1230, denn dieses sei für Personen ungefährlich und hinterlasse nahezu keine Schäden an den zu schützenden Objekten.

Business Continuity Management

Nicht alle Unternehmen haben ihre **Server-Räume und Rechenzentren** auf einen möglichen Ausfall oder Störfall vorbereitet, zeigt sich TECCHANNEL.de am 3. Februar überzeugt. Im Zeitalter von Big Data, Industrie 4.0 und Always-On reiche Verfügbarkeit „im Großen und Ganzen" nicht mehr aus. Eine HP-Studie von 2013 belege, dass in mittelständischen Unternehmen in Deutschland durch Ausfälle jährlich 380.000 Euro Kosten pro Jahr entstanden. 2014 hätten Unternehmen in Deutschland wegen „Downtime" Verluste von 11,6 Mrd. Euro hinnehmen müssen. Bei den Verfügbarkeitsoptionen werde zwischen „gut", „besser" und „optimal" unterschieden. Als gut gelte die Standardverfügbarkeit (99 Prozent Verfügbarkeit, durchschnittlich 87,5 Stunden Ausfall pro Jahr). Hier kämen in der Regel zuverlässige Server mit redundanten Lüftern, redundanter Stromversorgung und gespiegeltem Speicher zum Einsatz. Sie böten aber keinerlei Sicherheit bei der Datenübertragung. Besser sei da schon eine Datenreplikationssoftware. Die ständige Verfügbarkeit sei der höchste Level. Zu dieser Lösung gehörten zwei vollständig redundante Server sowie Software zur permanenten Überwachung der Systemkomponenten. Grundsätzlich sei zwischen Hochverfügbarkeitssoftware und einer Cluster-Lösung zu unterscheiden. Bei der Software-Lösung betrage die Ausfallzeit weniger als eine Stunde pro Jahr, bei Hochverfügbarkeits-Clustern hingegen fast neun Stunden. Das Cluster ziele auf eine möglichst schnelle Wiederherstellung nach einem Systemausfall ab, die Software hingegen könne Ausfallzeiten und Datenverluste automatisch erkennen und Fehler melden, bevor sie das gesamte System betreffen.

Diebstahl

2014 seien in London täglich durchschnittlich 17 schlüssellose Autos gestohlen worden, meldet heise.de am 4. Februar. 40 Prozent aller Kfz-Diebstähle betrafen **schlüssellose Fahrzeuge.** Die Londoner Polizei arbeite eigenen Angaben zufolge mit Autoherstellern zusammen, die besonders beklagten, dass Personal aus Autowerkstätten die Diagnose- und Reparaturtools für Diebstähle missbrauche. So würden die OBD-Ports angezapft und mit den heruntergeladenen Informationen der Autos die elektronischen Schlüssel kopiert. Laut Polizei werden auf diese Weise die meisten Diebstähle ausgeführt. Die Behörden raten für die Sicherung der smarten Autos zu Lenkradschlössern, Gangschaltungssperren, OBD-Schlössern und Peilsendern.

Die Deutsche Bahn wappnet sich gegen Diebe, meldet die FAZ am 11. Februar. Um Aufbrüchen vorzubeugen, rüste sie ihre **Fahrkartenautomaten** jetzt mit Farbpatronen aus. Die Farbkassetten seien von außen nicht zu sehen, Aufkleber wiesen aber auf die Sicherung hin. Werde die Geldkassette gekippt oder geschüttelt, platze eine Farbpatrone und spritze mit hohem Druck eine nicht ablösbare Farbe auf die Geldscheine. Das Geld werde wertlos. 390-mal seien 2014 Automaten aufgebrochen worden, der Bahn sei ein Schaden von 6,7 Mio. Euro entstanden.

Drohnen

Die Zahl der Drohnen wachse derzeit weltweit monatlich um etwa 300.000, berichtet die FAZ am 17. Februar. Sie könnten Hilfe bringen oder eine Bedrohung darstellen. Die Firma Dedrone GmbH befasse sich mit der Drohnenerkennung. Der **„Drone Tracker"** sei mit visuellen und akustischen Sensoren ausgestattet. Er sehe bei Tageslicht, im Infrarotbereich, erkenne Wärmestrahlen und könne bald auch bei Nebel mit Hilfe von Radarstrahlen sehen. Der Tracker detektiere die Flugobjekte in einem Umkreis von 100 Metern bei einer Abdeckung eines Winkels von 180 Grad. Er erfasse ein Flugobjekt, zeichne seinen Weg auf und gebe per SMS, E-Mail oder auf andere Weise Drohnenalarm an den Hausherrn, die Wache einer Kaserne oder die Sicherheitswarte eines Unternehmens.

Die private und **kommerzielle Nutzung von Drohnen** sei zurzeit in Deutschland im weltweiten Vergleich relativ liberal. In anderen europäischen Ländern benötige man eine spezielle Betreiberlizenz und eine Piloteneinweisung, betont Security insight in der Ausgabe 1-2015, S. 8–12. Kommerzielle Anwender benötigten Versicherungsnachweise und Aufstiegsgenehmigungen mit zahlreichen Auflagen. Ein Drohneneinsatz positiver Natur sei im Umfeld kleiner und mittelständischer Betriebe schon jetzt in vielfältiger Weise vorhersehbar. Besonders zur Kontrolle schlecht überschaubarer und unwegsamer Areale böten sich kamerabestückte UAVs (Unmanned Aerial Vehicels) geradezu an. So habe Securitas im Chemiepark Bitterfeld Drohnen getestet, die im Ernstfall zur Lagebeurteilung eingesetzt werden können. Das Nachtflugverbot und die Bestimmung, dass der Drohnenpilot immer Sichtkontakt zu seinem Fluggerät halten muss, seien die einzigen relevanten Einschränkungen bei ihrer Nutzung. Zu befürchten sei, dass bei großen Unfällen von Journalisten eingesetzte Drohnen über der Unglücksstelle kreisen und die Rettungskräfte behindern. Es gebe aber Abwehrmöglichkeiten. Steuersignale könnten gestört werden. Denkbar sei dies beim GPS-Signal oder bei der Datenverbindung zur Kontrollstation.

Einbruch

Die Zahl der Einbrüche in Hamburg steigt, aber Haus- und Wohnungsbesitzer rüsten mit zusätzlicher Technik auf, sodass bereits 42,4 Prozent aller Einbrüche im Ansatz stecken bleiben, berichtet abendblatt.de am 7. Februar. Im Interview rät der Leiter der Hamburger Kriminalpolizeilichen Beratungsstelle zu mechanischen Sicherungen, die sinnvoll aufeinander abgestimmt sind, an erster Stelle. Bewegungsmelder und durch sie gesteuerte Außenbeleuchtung spielten eine ganz wesentliche Rolle für den Schutz des Grundstücks. Ebenso empfehlenswert seien Zeitschaltuhren, die in der dunklen Jahreszeit

zu bestimmten Zeiten Licht anmachen. In 80 Prozent aller Wohnungseinbrüche hebelten die Täter ein Fenster auf. Im Erdgeschoss seien zur Fensterabsicherung Sicherungsbeschläge mit sogenannten Pilzköpfen zu empfehlen.

Einzelhandelssicherheit

In der Zeitschrift GIT (Ausgabe 1/2-2015, S. 28/29) wird **Sicherheitstechnik für den Handel** vorgestellt: Technologien zur Warensicherung, Geldbearbeitung, Geldaufbewahrung und -transport, Zutrittskontrolle und Überwachungsanlagen. Jährlich investiere der deutsche Handel rund 1,3 Mrd. Euro in Präventiv- und Sicherungsmaßnahmen. Trotzdem entgingen ihm jährlich rund 3,9 Mrd. Euro durch Inventurdifferenzen. Warenwirtschaftliche Auswertungen zur Erkennung von diebstahlgefährdeten Artikeln sowie Kassendatenanalyse-Tools zur Identifizierung von Schwachstellen im Kassenbereich würden weiter an Bedeutung gewinnen. Warensicherungssysteme hätten sich weiterentwickelt. Etiketten würden immer kleiner und die Erkennungsraten der Antennensysteme würden steigen. Die Antennensysteme würden auch für Kundenzählungen oder als Werbeflächen genutzt. Mit einem integrierten System könnten sämtliche Ereignisse wie Alarme, Deaktivierungen von Klebeetiketten oder das einfache Lösen von Hartetiketten registriert, dokumentiert und im Zusammenhang ausgewertet werden. Die stückgenaue Identifikation von Artikeln mit Hilfe des EPC (Electronic Product Code) und durch berührungslose Lesetechnik mittels RFID habe auch Auswirkung auf die Warensicherung. Obwohl EPC und RFID noch von einer echten Marktetablierung entfernt seien, gebe es eine Reihe von Konzepten, die die Nutzung dieser Technologie als Warensicherung oder in Kombination mit Warensicherungen vorsehen. Die RFID-Technologie ermögliche dabei den Zugriff auf produktspezifische Informationen oder die Rückverfolgung und Ortung von Waren in Echtzeit und unterstütze so einen reibungslosen, kontrollierbaren Warenfluss in der gesamten Supply Chain bis hin zum Point of Sale.

Endgerätesicherheit

In der Fachzeitschrift GIT (Ausgabe 1/2-2015, S. 75–77) stellt Klaus U. Klosa, Legic Identsystems, den RFID-Karten die modernen Mobiltelefone gegenüber. Die einfache Handhabung, die unterschiedlichen Kommunikationsschnittstellen, die starke Rechenleistung sowie attraktive Benutzeroberflächen machten mobile Endgeräte wie Smartphones zum bevorzugten Medium. Das Interesse an Mobile ID mit NFC und Bluetooth Low Energy (BLE) sei der große Trend im Jahr 2015. Smartcard versus Smartphone sei eine stetig andauernde Diskussion. Beide hätten ihre Vor- und Nachteile, die sie für die verschiedenen Anwendungsfälle zur bevorzugten Wahl machten.

Falschgeld

Um Fälschern die Arbeit zu erschweren, haben die Notenbanker für den **neuen 20 Euro-Schein** ein völlig neuartiges Sicherheitsmerkmal entwickelt, berichtet das Handelsblatt am 25. Februar. Rechts auf dem glänzenden Hologrammstreifen befinde sich bald ein kleines Fenster. Wer den Schein gegen das Licht hält, erblicke darin das Porträt der Figur Europa. Kippt man den Schein, erscheine die Ziffer 20 auf einer regenbogenfarbigen Fläche. Die Figur Europa sei auch im Wasserzeichen und im silbernen Hologrammband zu sehen. Auf der Vorderseite solle eine schimmernde Smaragdzahl das Fälschen erschweren. An den Rändern links und rechts auf der Vorderseite seien erhöhte Linien zu fühlen. 2014 sei in Deutschland so viel Falschgeld im Umlauf gewesen wie seit 2005 nicht mehr. Die Polizei habe rund 63.000 gefälschte Euro-Noten im Handel und bei Banken sichergestellt. Durch sie sei ein Schaden von 3,3 Mio. Euro entstanden. Rund ein Drittel der gefälschten Banknoten in Deutschland seien Zwanziger, nur der Fünfziger sei noch beliebter.

Forensik

Sofortmaßnahmen für das **Forensikverfahren bei unternehmensinternen Ermittlungen** beschreibt Marko Rogge, Conturn Analytical Intelligence Group, in Security insight (Ausgabe 1-2015, S. 54). Schädlich sei zunächst einmal Hektik, weil das für Innentäter ein Signal sein könnte, dass man ihnen auf die Schliche gekommen ist. Technisch sei es wichtig zu ermitteln, welche Systeme vom Ereignis betroffen sind und um welche Betriebssysteme es sich handelt. Bei Computersystemen sollte dringend nachgeprüft werden, ob und, wenn ja, wie und von wem ein System heruntergefahren wurde. Bei technischen Untersuchungen sei es für einen Forensiker ebenfalls wichtig zu wissen, ob und welche Logfiles bereits gesichert und/oder gesichtet wurden. Je umfangreicher und detaillierter die Informationen im Ereignisfall zusammengetragen, kommentiert und dem Forensiker zur Verfügung gestellt werden, desto besser stünden die Chancen, den Fall zu lösen.

Gefährdungslagebild Griechenland

Eine Gefährdungsbewertung deutscher Interessen in Griechenland durch das BKA vom 20. Februar kommt zu dem Ergebnis, es sei in Betracht zu ziehen, dass vereinzelt die Grenze legalen Protests überschritten wird und gewaltsam gegen deutsche Interessen und Personen vorgegangen werden könnte. Relevant sei insbesondere das linksextremistische/anarchistische Spektrum in Griechenland. Bereits 2013 habe die „Gruppe der Volkskämpfer" durch Anschläge auf die Residenz des deutschen Botschafters und die Mercedes-Benz Niederlassung in Athen belegt, dass die deutsche Haltung in der Finanzkrise als Legitimation für militantes Vorgehen genutzt wird. Nach wie vor stünden weitere vergleichbare Gewalttaten der „Gruppe der Volkskämpfer" zum Nachteil deutscher Interessen zu befürchten. Beachtenswert sei darüber hinaus, dass es in Griechenland aus dem sonstigen linken Spektrum immer wieder zu sogenannten Gazaki-Anschlägen bzw. Molotowanschlägen gekommen ist. Eine Fokussierung auf „internationale Gegner" sei zwar zunächst noch hypothetisch, aber dennoch möglich

Gefahrstofflagerung

Gefahrstofflagerung thematisiert Torben Eisberg, Denios AG, in der Fachzeitschrift GIT in der Ausgabe 1/2-2015, S. 96/97. **Gefahrstoffcontainer und -schränke** böten sich zur sicheren Lagerung brennbarer Flüssigkeiten und gefährlicher Stoffe an. Um den Schutz der Arbeitsmittel langfristig aufrechtzuerhalten, sei die Einhaltung regelmäßiger Wartungsintervalle notwendig. In Deutschland sei für Gefahrstofflager eine Feuerwiderstandsfähigkeit von 90 Minuten vorgeschrieben. Die Sicherheit des Containersystems basiere auf dem Zusammenspiel funktionaler Komponenten. Bei der Lagerung von umwelt- und gesundheitsgefährdenden Substanzen seien die Faktoren Raumklima und Belüftung von großer Relevanz für die Gesamtsicherheit des Lagersystems. Bei aktiver Lagerung von Gefahrstoffen sei ein fünffacher Luftwechsel pro Stunde vorgeschrieben.

Geschäftsgeheimnisse

Mit dem Schutz von Geschäftsgeheimnissen befasst sich Rechtsanwalt Michael Dorner in der FAZ am 18. Februar. In Deutschland gebe es gegenwärtig kein übergreifendes Gesetz zum Schutz von Geschäftsgeheimnissen. Die maßgeblichen Regelungen seien über verschiedene Rechtsgebiete und Normen hinweg verteilt. Die geplante Rechtsangleichung bestimme nicht nur, wann schutzfähige Geschäftsgeheimnisse vorliegen und wann deren Erwerb, Nutzung oder Offenlegung verboten sind. Es gehe auch darum, welche zivilrechtlichen Ansprüche dann zur Verfügung stünden und wie Geschäftsgeheimnisse im Gerichtsverfahren geschützt werden. Als „Zugangsschutz" schütze er lediglich die Geheimsphäre, die um die betreffenden Informationen herum besteht. Bislang halte das deutsche Recht in Streitfällen eine Vermutung für einen Geheimhaltungswillen des Schutzsuchenden bereit. Für Unternehmen, die bereits ein durchdachtes Know-how-Schutzkonzept etabliert haben, solle dieser Nachweis verhältnismäßig leicht zu führen sein. Am Ziel der Richtlinie, das Schutzniveau für Geschäftsgeheimnisse zu verbessern, ändere das Erfordernis der „angemessenen Schutzmaßnahmen" nichts. Die Regeln schützten zwar die unternehmerische Geheimsphäre, könnten das Offenkundigwerden von Geheimnissen aber weder verhindern noch rückgängig machen. Schadensbegrenzend und kompensatorisch wirkten sie nur, sofern die Schutzsuchenden sich nachweislich hinreichend um die Geheimsphäre gekümmert haben. Der Richtlinienentwurf mache insoweit klar: Know-how-Schutz gehöre zur unternehmerischen Compliance.

Geschäftsreisen

Arbeitgeber unterschätzen die Gefahren auf Geschäftsreisen, meint die FAZ am 21. Februar. Sicherheit sei zu einem brisanten Kernthema unter Geschäftsreisenden geworden. 83 Prozent der Manager achteten auf ihre Sicherheit – vor einem Jahr seien es 76 Prozent gewesen. Jeder dritte, der dienstlich regelmäßig ins Ausland aufbricht, habe es schon mal mit Einschränkungen wegen politischer Unruhen zu tun bekommen oder musste eine Reise absagen. Acht von neun Geschäftsreisende würden sich vor der Abreise detaillierte Angaben zur politischen Lage am Zielort wünschen, doch nur jeder

dritte will diese Informationen tatsächlich bekommen haben. Je höher das Reisevolumen, desto eher sei ein Bewusstsein über die Fürsorgepflicht vorhanden, die den Arbeitgeber verpflichtet, Vorkehrungen zum Schutz von Leben und Gesundheit der Arbeitnehmer zu treffen. Strukturen für die Kommunikation mit Reisenden in Gefahrensituationen haben drei von vier großen Unternehmen, aber nur jeder zweite kleine Betrieb. Sicherheitstrainings böten 44 Prozent der Großunternehmen an, unter den kleineren beschäftige sich nur jedes vierte damit. Spezielle Apps würden für Geschäftsreisende in Bezug auf Gesundheitsgefahren und Sicherheitsrisiken immer wichtiger.

IT-Sicherheit

Unternehmen müssten sich angesichts der steigenden Bedrohung stärker vor Cyberattacken schützen, argumentiert COMPUTERWOCHE.de am 12. Februar. Helfen könne ihnen eine Schutzbedarfsanalyse. 100.000 Hacker-Angriffen müssten die IT-Systeme der Deutschen Telekom jeden Tag standhalten. Eine Studie von BITKOM besage, dass ein Drittel der deutschen Unternehmen in den vergangenen zwei Jahren Opfer von Cyberattacken geworden sei. 50 Prozent der IT-Entscheider aus aller Welt seien davon überzeugt, dass politische Hackerangriffe und interne Gefährdungen im nächsten Jahr noch zunehmen werden. Den Verantwortlichen sei oft nicht bewusst, dass oder in welchen Dateien sensible Informationen enthalten sind. Ihnen falle es schwer, den virtuellen Daten einen realen Geldwert zuzuordnen. Mit der sogenannten Schutzbedarfsanalyse ließen sich schützenswerte Daten von Unternehmen erkennen und mit einem realen Angriffsrisiko verknüpfen. Die müsse man sich wie einen virtuellen Rundgang mit dem Werkschutz vorstellen, bei dem jeder Raum auf Wertgegenstände hin untersucht und gegen „Einbrecher" abgesichert wird.

Eine Studie von Convios Consulting mit einer Umfrage bei rund tausend Internetnutzern ab 14 Jahren zeigt nach einem Bericht in der FAZ am 23. Februar, dass der **Vertrauensverlust** wegen der Furcht durch Spähaktionen von Geheimdiensten andauere. 28 Prozent der Befragten habe Bedenken, Daten bei amerikanischen Unternehmen wie Google, Yahoo oder Microsoft zu speichern. Aber nur drei Prozent der Menschen, die bisher IP-basierte Netze überwiegend eines amerikanischen E-Mail-Dienstes nutzten, hätten wegen der Snowden-Enthüllungen diesen Anbieter gewechselt. Web.de und GMX wollten im Laufe diesen Jahres eine Ende-zu-Ende-Verschlüsselung für E-Mail anbieten. Die Herausforderung bestehe darin, diese Verschlüsselung massentauglich zu machen.

Dieter Fischer, Telefonbau Arthur Schwabe, thematisiert in der Zeitschrift GIT (Ausgabe 1/2-2015, S. 56/57) die Umstellung auf **IP-basierte Netze** und die Folgen für sicherheitstechnische Anwendungen. Die neuen Netze seien vollständig IP-basiert. Bei NGN (Next Generation Network)-Netzen handele es sich um sogenannte paketorientierte Netze. Das heißt, sämtliche Daten würden in Pakete gepackt und zusammen mit den Paketen anderer Netznutzer auf die Reise zum Ziel geschickt. Damit bestehende Endgeräte wie Telefone oder TK-Anlagen am neuen Netz weiterbetrieben werden können, würden Router angeboten, die die alten Schnittstellen „analog" und „ISDN" für Sprachdienste intern generieren und dem Kunden bereitstellen. Standard-Router seien jedoch nicht für den Abschluss von analogen oder ISDN-Übertragungsgeräten geeignet. Europäisch sei die Problematik bereits von den Kernrichtlinien für Übertragungstechnik erkannt und angepasst. EN 50136-1 beschreibe – unabhängig von den eingesetzten Netzen – ein Verfahren, bei dem die Übertragungswege abhängig von

der seitens der Anwendungsrichtlinien geforderten Klassen überwacht werden. Die neue europäische Norm für Alarmempfangsstellen EN 50518 fordere ausdrücklich zukünftig überwachte Alarmübertragungsstrecken nach den genannten EN 50136. Für den Fall, dass man gerade erst viel Geld für eine neue Alarmanlage mit alter Technik ausgegeben hat, gebe es ebenfalls eine Lösung: den IP-Converter.

Ein sicheres **Remote-Management und -Support in Unternehmen** gehöre zur Pflicht, betont TECCHANNEL.de am 18. Februar und gibt folgende sechs Tipps, die helfen sollen, die Fernwartung von IT-Systemen sicher zu betreiben: 1. Architektur von Remote-Management-Tools untersuchen; 2. Zuständigkeiten nachverfolgen; 3. Systemzugriffe unter Kontrolle halten; 4. alle Aktivitäten der Support-Sessions protokollieren; 5. Support-Technologie standardisieren; 6. gesamte Kommunikation verschlüsseln.

IuK-Kriminalität

Die Bedrohungen durch Cyberkriminalität und Wirtschaftsspionage nehmen laut aktuellem eco Report **„IT Sicherheit 2015"** weiterhin zu, berichtet itseccity.de am 6. Februar. 44 Prozent der von eco (Verband der deutschen Internetwirtschaft e. V.) befragten 280 Fachleute gingen davon aus. Dementsprechend rechneten 59 Prozent der Sicherheitsexperten in diesem Jahr mit steigenden Ausgaben für Datenschutz und IT-Sicherheit. Oliver Dehning, Leiter der eco Kompetenzgruppe Sicherheit, führe diese Entwicklung in erster Linie auf das gesteigerte Sicherheitsbewusstsein der deutschen Firmen zurück. Der Verein Deutscher Ingenieure (VDI) schätze den Schaden, der deutschen Firmen jährlich allein durch Wirtschaftsspionage entsteht, auf 100 Mrd. Euro. Laut Center for Strategic and International Studies (CSIS) sei in keinem anderen Land der durch Cyberkriminalität verursachte wirtschaftliche Schaden – gemessen an der Wirtschaftsleistung – größer als in Deutschland. Im eco Report ist der „Datenschutz" das wichtigste Sicherheitsthema für 2015 (88 Prozent der Befragten). Auf Platz zwei und drei folgten die „Verschlüsselung von Kommunikation" (81 Prozent) und die „Verschlüsselung von Daten" allgemein (80 Prozent). Es folgten im Ranking mit 78 Prozent die „Mitarbeitersensibilisierung", „Schadsoftware im Web" und „Mobile Device Security" (je 74 Prozent).

IT-Studenten aus Saarbrücken haben eine schwerwiegende Sicherheitslücke im Internet entdeckt, meldet ZEIT ONLINE am 10. Februar. Jedermann konnte mehrere Millionen Kundendaten mit Namen, Adressen, E-Mails und Kreditkartennummern im Internet abrufen oder gar verändern, habe die Universität Saarbrücken mitgeteilt. Ursache sei eine falsch konfigurierte, frei verfügbare Datenbanksoftware, auf der weltweit Millionen von Onlineshops und Plattformen ihre Dienste aufbauten. Bei dem falsch implementierten Programm handele es sich um die populäre Datenbank **MongoDB,** die als offene Software kostenlos verwendet werden könne. Die Lücke betreffe knapp 40.000 Datenbanken. Der Fehler sei nicht kompliziert, seine Wirkung jedoch katastrophal. Zu den betroffenen Websites gehöre auch die Kundendatenbank eines französischen Internetdienstanbieters und Mobiltelefonie-Betreibers, in der sich auch eine halbe Million deutscher Adressen befänden. Die Datenbank eines deutschen Onlinehändlers inklusive Zahlungsinformationen hätten die Studenten ebenfalls ungesichert vorgefunden.

Eine internationale Gang habe nach Auskunft von IT-Sicherheitsexperten in den vergangenen zwei Jahren bis zu einer Milliarde Dollar durch **Online-Attacken auf Banken** gestohlen, berichtet die FAZ am 16. Februar. Der

Online-Bankraub sei gemeinsam mit Interpol, Europol und Behörden verschiedener Länder aufgedeckt worden. Bis zu 100 Banken, Bezahldienste und andere Institute in rund 30 Ländern seien angegriffen worden, auch in Deutschland. Die Gang mit dem Namen „Carnak" habe sich zunächst über gezielte Attacken Zugang zu einem Angestellten-Computer verschafft und ihn mit ihrem Schadprogramm infiziert, erläuterte Kaspersky die gängige Methode. Dadurch sei sie in der Lage gewesen, im internen Netzwerk die für Videoüberwachung zuständigen Computer versteckt anzuzapfen. Danach hätten die Täter alles, was sich auf den Bildschirmen der für die Betreuung der Geldtransfersysteme verantwortlichen Mitarbeiter abspielte, einsehen und aufnehmen können. So hätten sie jedes Detail über die Arbeit der Angestellten imitieren können, um Geld zu überweisen oder bar auszuzahlen. Die größten Summen seien durch das Hacken von Banken erbeutet worden: bis zu zehn Mio. Dollar pro Überfall. Im Durchschnitt habe ein solcher Angriff zwischen zwei und vier Monate gedauert, von der Infizierung des ersten Computers im Unternehmensnetzwerk der Bank bis zum eigentlichen Diebstahl.

TECCHANNEL.de prognostiziert am 15. Februar **für das Jahr 2015 folgende fünf Trends:** 1. Botnets werden zur professionellen Dienstleistung; 2. neue Angriffsflächen durch Industrie 4.0 und das Internet der Dinge; 3. Sabotage nimmt einen höheren Stellenwert ein; 4. Angriffe erfolgen vermehrt aus der Lieferkette; 5. Smartphones und mobile Endgeräte werden noch unsicherer.

Die NSA sowie der britische GCHQ sollen sich Zugang zu unzähligen SIM-Karten verschafft haben, berichtet die FAZ am 21. Februar. Die beiden Dienste hätten Verschlüsselungscodes ergattert, indem sie die private Kommunikation von dem SIM-Karten-Hersteller **Gemalto** durchforsteten. Damit sei es ihnen möglich gewesen, ohne das Wissen der Kartenhersteller, der Mobilfunkunternehmen und der Kunden Telefongespräche und auch den Datenverkehr von Smartphones ausspähen zu können. Schon 2009 sei die NSA technisch in der Lage gewesen, bis zu 22 Mio. Verschlüsselungscodes je Sekunde zu knacken, um sie bei späteren Abhöraktionen einsetzen zu können. Giesecke & Devrient habe mitgeteilt, es sehe keine Anzeichen, dass es bei ihm zu einem ähnlichen Vorfall wie bei Gemalto gekommen sei. Die Deutsche Telekom habe nach eigenen Angaben ebenfalls Gemalto-Karten im Einsatz, habe aber darauf hingewiesen, dass sie den Standard-Verschlüsselungsalgorithmus der Karten geändert habe. Wie die FAZ am 25. Februar mitteilte, habe der Einbruch nicht zu einem massiven Diebstahl von SIM-Schlüsseln führen können, habe Gemalto jetzt berichtet. In der SIM-Infrastruktur sowie in den abgetrennten Bereichen, in denen Daten für Bankkarten, elektronische Dokumente oder Zugangskarten verarbeitet werden, sei kein Eindringen festgestellt worden.

Juwelenraub

Mit der Festnahme zweier Juwelenräuber in der Augsburger Altstadt habe die Polizei eine Überfallserie mit Millionenschaden geklärt, meldet die FAZ am 26. Februar. Die Männer sollen seit Dezember 2003 in Bayern, Hessen, Nordrhein-Westfalen und der Schweiz insgesamt sieben Juweliere überfallen und Schmuck im Wert von mehreren Millionen Euro erbeutet haben. Sie würden aus Russland stammen und seien offenbar nur für die Raubzüge nach Westeuropa gereist.

Korruption

Die **Korruptionsaffäre bei Ford** weite sich aus, meldet FOCUS am 14. Februar. So habe die Staatsanwaltschaft Köln inzwischen einen Riesenschwindel mit Ersatzteilen aufgedeckt. Offenbar habe Ford Zigtausende Verschleißteile bezahlt, die nie geliefert wurden. Die Masche sei durch Scheinrechnungen verschleiert worden. Im bisher größten Fall müssten sich zwei leitende Ford-Einkäufer und zwei Mitarbeiter eines Zulieferers wegen Untreue und bandenmäßiger Bestechung in bis zu 500 Fällen vor Gericht verantworten. Das Quartett solle durch seine Schiebereien zwischen 2006 und 2010 Ford um „mehrere Millionen Euro" geschädigt haben. Dafür hätten die korrupten Ford-Mitarbeiter Geschenke im Wert von einigen hunderttausend Euro erhalten. Insgesamt würden die Korruptionsfahnder in etlichen Ford-Komplexen gegen mehr als 100 Beschuldigte ermitteln.

Krisenregionen

Wegen der zunehmenden Spannungen zwischen Schiiten und Sunniten im Jemen haben mehrere westliche Staaten ihre Botschaften dort geschlossen, berichtet wiwo.de am 13. Februar. Großbritannien und Frankreich wären dem Beispiel der USA gefolgt und hätten ihr Personal aus Sanaa abgezogen sowie ihre Staatsbürger aufgerufen, das Land möglichst schnell zu verlassen. Auch Deutsche sollten ausreisen, habe das Auswärtige Amt in Berlin erklärt. In den südlichen und östlichen Teilen des Landes, die bislang nicht von den Huthi erobert worden seien, bewaffneten sich inzwischen sunnitische Stammesmitglieder und verbündeten sich zum Teil mit der Al-Qaida. Die Spannungen zwischen den Religionsgruppen hätten die Furcht vor dem Ausbruch eines Bürgerkriegs verstärkt.

Ladungsdiebstahl

Der ASW hat am 7. bzw. 14. Februar folgende Tatorte für Planen-Schlitzereien und Ladungsdiebstähle benannt:

- 26./27.1. Wismar, A 20, Autobahnparkplatz „Mölenbarg", Fahrtrichtung Lübeck
- 27./28.1. Wiesbaden, A 3, Rastanlage Medenbach Ost
- 28./29.1. Sinsheim, A 6, Rastanlage Kraichgau-Süd
- 3./4.2. Lehrte, A 2, Rastplatz Lehrter See Nord, Fahrtrichtung Dortmund
- 6./7.2. Recklinghausen, A 43, Parkplatz Speckhorn, Fahrtrichtung Münster
- 7./8.2. Tankrastanlage Spessart Nord, A 3, Parkplatz Fronberg und Birkenhain (Fahrtrichtung Frankfurt)
- 7./8.2. Goldberg, Gewerbegebiet „Neue Hoffnung"
- 10./11.2. Frankfurt/Main, A 3, Parkplatz „Stadtwald", Fahrtrichtung Würzburg
- 10./11.2. Weibersbrunn, A 3, Rastanlage Spessart-Süd, Fahrtrichtung Würzburg

Luftsicherheit

Nach der Überzeugung von Dirk Fischlein, Securitas Aviation Service International, wird auf absehbare Zeit der Terrorismus die virulenteste Bedrohung und eine der größten Herausforderungen bleiben. Securitas lege großen Wert auf die stetige und nachhaltige Verbesserung der individuellen Fähigkeiten der Beschäftigten und auf eine niedrige Personalfluktuation. Lokale, nationale und internationale Experten führten intern permanente Qualitätssicherungs- und Fortbildungsmaßnahmen durch. Securitas sei internationaler Spezialist für Luftsicherheit auf mehr als 200 Flughäfen in 25 Ländern mit insgesamt rund 25.000 spezialisierten Mitarbeiterinnen und Mitarbeitern. Als einer der personalstärksten Dienstleister für die Luftsicherheit im BDSW sei das Unternehmen mit rund 3.000 Experten in Deutschland an allen bedeutenden Flughäfen mit effektiven und effizienten Sicherheits- und Servicedienstleistungen im Einsatz (GIT, Ausgabe 1/2-2015, S. 22/23).

Körperscanner sollen genauer und schneller sein als bisherige Sicherheitskontrollen, argumentiert wiwo.de am 13. Februar. Seit November 2014 würden sie in Köln/Bonn und Düsseldorf auch für die allgemeinen Luftsicherheitskontrollen genutzt. Wer sie nicht benutzen möchte, muss es nicht. Die Kontrollen mit Körperscannern detektierten auch nicht-metallische Gegenstände. Sie arbeiteten mit einer Millimeterwellentechnologie, die für Menschen gesundheitlich unbedenklich sein soll. Außerdem zeige die Software, die in Deutschland zum Einsatz kommt, lediglich Piktogramme und nicht das Körperbild des kontrollierten Passagiers. 65 Prozent der Befragten in Deutschland, die selber noch nie ein solches Gerät genutzt haben, seien für den Einsatz von Körperscannern. Unter denen, die schon einmal in einer solchen Kabine standen, seien es sogar 77 Prozent.

Maschinensicherheit

Melanie Harke, Microsonic, befasst sich in der Zeitschrift GIT (Ausgabe 1/2-2015, S. 91/92) mit Sensoren, die den **Materialfluss** steuern. Ultraschallsensoren detektierten nahezu alle Materialien, unabhängig von ihrer Farbe. Auch glasklare Materialien oder transparente Objekte würden erkannt. Die Sensoren würden kontakt- und berührungslos in staubiger Luft genauso wie durch Farbnebel hindurch messen. Standard-Messprinzip für einen Ultraschallsensor sei die Echo-Laufzeitmessung. Der Sensor strahle zyklisch einen hochfrequenten Schallimpuls aus. Wenn er auf ein Objekt trifft, werde er reflektiert und das Echo kehre zum Sensor zurück. Aus der Zeitspanne zwischen dem Aussenden des Schalls und dem Empfang des Echos errechne der Ultraschallsensor die Entfernung zum Objekt.

In Logistik und Produktion überwachten Ultraschallsensoren zahlreiche Arbeitsvorgänge. Für die Messung des Füllstands von Produktionsstoffen beziehungsweise -hilfsmitteln aller Art hätten sich die chemiebeständigen crm+ Ultraschallsensoren von Microsonic bewährt. Die M30-Gewindehülse des Sensors bestehe aus rostfreiem Edelstahl, und seine Membran sei durch eine PEEK-Folie geschützt, sodass weder die abschließende Reinigung der Abfüllanlage, Milchsäurebakterien noch ausgehärtete Verschmutzungen dem Sensor schaden könnten. Mit einer Reichweite von bis zu acht Metern erschlössen die quaderförmigen Ics+ Ultraschallsensoren weite Einsatzmöglichkeiten zur Messung von Füllständen sowie Entfernungen und Abständen in Industrie und Landwirtschaft.

Mechatronik

Von einem „Siegeszug der Mechatronik" spricht Michael Zabler, Abus Security-Center GmbH & Co. KG, in der Fachzeitschrift GIT (Ausgabe 1/2-2015, S. 40/41). Die neue Secvest Zentrale kombiniere mechatronischen Einbruchschutz mit den klassischen Funktionen einer Alarmanlage: Schutz gegen Rauch, Wasser und im Notfall. Hinzu komme der bewährte Secvest Key-Türzylinder für komfortables Aktivieren bzw. Deaktivieren der Anlage über das Türschloss.

Mitarbeiterkriminalität

„Den Mitarbeitern auf der Spur", titelt die FAZ am 10. Januar. **Überwachungsmaßnahmen** durch den Arbeitgeber oder von ihm beauftragte Detektive seien nach dem BDSG nur zulässig, wenn bereits vor der Maßnahme ein konkreter Verdacht besteht, der sich gegen einen Einzelnen oder einen abgrenzbaren Personenkreis richtet. Weniger eingreifende Ermittlungsmethoden müsse der Arbeitgeber zuvor durchgeführt haben, ohne dass diese den Verdacht endgültig bestätigt oder ausgeräumt hätten. Schließlich müsse die Schwere des vermuteten Fehlverhaltens jene des Eingriffs in die Privatsphäre des Arbeitnehmers überwiegen. Gewisse Ermittlungsmethoden seien von vornherein ausgeschlossen. Dazu gehöre alles, was seinerseits eine Straftat darstellt, etwa das Hacken des (privaten) Rechners des Überwachten. Ebenfalls in diese Kategorie falle die bis vor einigen Jahren noch gebräuchliche Überwachung mittels GPS-Sendern am Fahrzeug. Im Öffnen des Spinds, in dem Angestellte oft auch persönliche Gegenstände verwahren, liegt nach einer Entscheidung des BAG ein Eingriff in die Privatsphäre des Verdächtigten. Der sei wegen des akuten Verdachts zwar womöglich gerechtfertigt, zumindest aber hätte er im Beisein des Mitarbeiters stattfinden müssen. Reiche der ermittelte Sachverhalt nicht aus oder ist er nicht verwertbar, so bleibe als Alternative zur Tat- noch die Verdachtskündigung, die stets eine Anhörung des Verdächtigten voraussetze. Gelingt die Verdachtskündigung, so stehe sie der Tatkündigung in nichts nach. Auch hier könne der Arbeitnehmer nicht nur fristlos entlassen werden, sondern es könnten ihm zudem die Kosten der Ermittlungen auferlegt werden.

Personennotruf

Personennotrufsysteme thematisiert Security insight in der Ausgabe 1-2015. Ein Alarmierungssystem bestehe im Wesentlichen aus einem aktiven Personen- oder Funkrufempfänger („Pager"), der unabhängig von der Person, die ihn trägt, einen Notruf an eine Zentrale absetze. Das Notsignal liefere gleichzeitig die genauen Koordinaten der Örtlichkeit an die Notrufzentrale. Dazu seien das Funkortungssystem GPS und das Mobilfunksystem GSM im Pager zusammengeführt worden. Für die präzise Positionsbestimmung seien im für die GPS-Ortung unzugänglichen Innenbereich intelligente Funkbaken installiert, die mittels Pop up-Signalen eine ständige Lokalisierung innerhalb der Werksräumlichkeiten durchführen (S. 46/47). Oliver Laube, Ascom Wireless Solutions, stellt ein System vor, bei dem als technische Grundlage ein multizellulares DECT (Digital Enhanced

Cordless Telecommunications)-Funknetz dient, das Sprach- und Datenkommunikation flexibel miteinander kombiniert. Einstellbar sei eine Steigerung der Funktionalitäten vom passiven Alarmieren eines mobilen Endgeräts über das Eskalations-Messaging mit erhöhter bis zum interaktiven Messaging. Hierbei könne der Nutzer nicht nur Alarme und Störungen weitergeben, sondern auch Prozesse anstoßen, Maschinen aktiv steuern oder standortbezogene Anweisungen und Funktionen übertragen (S. 48/49).

Produkterpressung

Karsten Holger Gennat befasst sich in der Ausgabe 1-2015 der Zeitschrift Security insight (S. 42/43) mit dem Phänomen Produkterpressung. Die Tathandlung bestehe aus drei Phasen, wobei jeder dieser Phasen ein höheres Risiko für den Erpresser mit sich bringe: die anfängliche Kontaktphase, die anschließende Verhandlungsphase, in der der Täter aus der Anonymität heraustreten müsse, und die Übergabephase, die das größte Entdeckungsrisiko beinhalte. Der Autor empfiehlt, immer und sofort die Polizei zu informieren. **Die größten Fehler,** die Unternehmen bei Produkterpressung begehen könnten, seien nach Aktionismus, Fehl-, Über- und Falschbewertung, nicht abgestimmtes Verhalten und Treffen von Maßnahmen, falsche Informationswege, Nichtbeachtung der Geheimhaltungserfordernisse und insbesondere fatale Entscheidungen im Hinblick auf den Alleingang des Unternehmens.

Produktpiraterie

Klaus Grigori, Wirtschaftsingenieur, empfiehlt in der Fachzeitschrift Security insight (Ausgabe 1-2015, S. 34–37) für die nachhaltige Bekämpfung der Marken- und Produktpiraterie einen **ganzheitlichen Ansatz,** konsequentes Vorgehen und viel Durchhaltevermögen. Die vorrangige organisatorische Maßnahme sei der rechtliche Schutz der Marken- und Patentrechte. Werde aus Gründen der Vertraulichkeit auf die Anmeldung verzichtet, sollte ein besonders effektiver Know-how-Schutz betrieben werden. Der Schutz der Kerninformationen gegen Industriespionage sei eine weitere wichtige organisatorische Maßnahme. Nach dem Markteintritt sollte eine aktive Marktüberwachung erfolgen. Wichtig sei auch die Schulung der Mitarbeiter zur Erkennung von Fälschungen. Das Grenzbeschlagnahmeverfahren sei grundsätzlich für den Rechteinhaber eine effektive und flächendeckende, aber doch kostengünstige Möglichkeit, den Markt zu beobachten und Schutzrechtsverletzungen aufzudecken. Bei der Formulierung der kommunikativen Maßnahmen, die auf den Absatzmarkt, also an den Verbraucher, gerichtet werden, sei Vorsicht und Fingerspitzengefühl geboten. Ein zu scharf formuliertes und aggressiv adressiertes Signal könne beim Kunden Unsicherheiten erzeugen und bewirken, dass er zu einem Konkurrenzprodukt wechselt.

Schwarzarbeit

Der Mindestlohn treibe die Schattenwirtschaft in Deutschland in diesem Jahr um 1,5 Mrd. Euro nach oben. Damit werde der jahrelange Rückgang der Schwarzarbeit in Deutschland gestoppt. Ihr Anteil am Bruttoinlandsprodukt bleibe unverändert bei 12,2 Prozent. Zu diesen Ergebnissen komme eine Studie des Tübinger Instituts für angewandte Wirtschaftsforschung (IAW) und der Universität Linz. Verglichen mit anderen Industrieländern liege Deutschlands Schattenwirtschaft im Mittelfeld. Am besten sei die Lage in den USA (5,9 Prozent) und in der Schweiz (6,5 Prozent). Düster sehe es in den Krisenländern Griechenland, Italien, Portugal und Spanien aus, mit Werten zwischen 18 und 22 Prozent (FAZ am 4. Februar).

Security LAN

Ulrich Leiner behandelt in Security insight (Ausgabe 1-2015, S. 38–41) die **Security LAN-Lösung für Sicherheitsleitstellen.** Die Anforderungen aus dem Konzept für die Sicherheitsleitstelle seien mit den „typischen" Anforderungen aus dem Unternehmensnetz für Office-Anwendungen nicht zu vergleichen. Der Autor beschreibt die typische Office-Anwendung, das Umfeld einer Sicherheitsleitstelle und die integrierten, vernetzten Leitstellensysteme. Durch die Migration der Sicherheitsgewerke in die IP-Technik entstünden Anforderungen, die beiden Welten „Office LAN" und „Security LAN" koordiniert zu planen. Zunächst müssten alle Komponenten der Systeme erfasst und in Kommunikationszonen zusammengefasst werden. Isoliert betrachtet sollten die Komponenten in einer Zone der sogenannten Demilitarisierten Zone (DMZ) ungehindert kommunizieren können. Die zunehmende Vernetzung der Sicherheitssysteme mache jedoch eine Kopplung der Systeme und Verbindungen zwischen den DMZ einzelner Systeme erforderlich. Die internationale Normenreihe IEC62443 beschreibe zum Beispiel Anforderungen und Regeln zum Schutz von IT-Systemen in industrieller Umgebung und sei speziell für die Steuerungs- und Leittechnik konzipiert. Die Beratung sollte aufgrund der Komplexität durch einen Fachplaner erfolgen.

Shutdown industrieller Großanlagen

Mirko Keeb, Securitas, bezeichnet im Interview mit Security insight (Ausgabe 1-2015, S. 44/45) die Sicherheits-Herausforderungen bei einem „Shutdown" industrieller Großanlagen, dem geplanten Herunterfahren von Großanlagen wie Raffinerien, petrochemischer Produktionsstätten oder Kraftwerke, um erneuert zu werden. Zu dem hochqualifizierten Sicherheitspersonal, das man dafür benötige, gehören Gas- und Brandposten, Fachkräfte für Sicherheit, Sicherungs- und Gefahrposten, Verkehrs- und Kranposten, Fachkundige zum Freimessen, Brandschutzbeauftragte, Sicherheitsaufsichten, Koordinatoren, Techniker sowie Safety-Projektleiter.

Sicherheitssysteme

Stefan Vogt, Honeywell Security Group, befasst sich in der Fachzeitschrift PROTECTOR (Ausgabe 1/2-2015, S. 36/37) mit Sicherheitssystemen für Mittelstandsunternehmen. In der Vergangenheit habe das Unternehmen die einzelnen Komponenten des Sicherheitssystems, also insbesondere Videoüberwachung, Einbruchschutz und Zugangskontrolle, aufwendig und relativ umständlich miteinander verbinden müssen. Um diesen Aufwand zu vermeiden, setze man nun auf die neue **Zentrale MB-Secure von Honeywell.** Die Lösung sei multifunktional, das heißt, die Zentrale bilde die Basis zur Integration von Einbruchmelde-, Zutrittskontroll- und Videoüberwachungslösungen in nur einem System. Die Lösung verbinde die verschiedenen Gewerke, was zahlreiche Vereinfachungen und sinnvolle Verknüpfungen erlaube. Auch die Verknüpfung mit der Gebäudesteuerung sei möglich und sinnvoll. Ausgangssituation für die Lösung sei ein vorkonfiguriertes MB-Secure Bundle, das der Errichter beim Unternehmen implementiert hat. Diese Vorkonfiguration mache es dem Errichter besonders einfach, da er alle wesentlichen Komponenten – Zentrale, Gehäuse, Netz- und Bedienteil sowie gegebenenfalls Sirenenmodul und Wählgerät – bereits eingerichtet erwerben könne.

In der Zeitschrift GIT (Ausgabe 1/2-2015, S. 45–47) wird die **Vernetzung von Zutrittssteuerung, Einbruchschutz, Videoüberwachung und Brandschutz** im Innovation Center der Rosen Gruppe in Lingen (Ems) vorgestellt. Das mit der Brandmeldeanlage verbundene Zutrittskontrollsystem sei äußerst umfangreich. Über 100 Türen im gesamten Gebäude seien mit Leser-, Türöffner- und Türschließeinheiten ausgestattet. Komplettiert werde das Sicherheitskonzept durch ein Videosystem. Das enge Zusammenspiel von Brandschutz- und Zugangskontrollsystem bringe klare Vorteile für das Schutzobjekt und zeige, was durch die intelligente Verknüpfung verschiedener Sicherheitssysteme mit dem Gebäudeleitsystem möglich ist. Komme es zum Brandfall, dann öffneten einzelne Türen, um die schnelle Flucht der Mitarbeiter sicherzustellen. Bei besonders sensiblen Bereichen hingegen schlössen sich die Brandschutztüren. Auch die Verbindung von Einbruchschutz und Gebäudeleitsystem schaffe Zusatznutzen, sowohl unter dem Aspekt der Sicherheit als auch hinsichtlich der Möglichkeit, Kosten zu senken. Signalisiert beispielsweise ein Fensterkontakt, dass dieses geöffnet ist, werde die Klima- beziehungsweise Belüftungsanlage automatisch herunter geregelt.

Stromsicherheit

Sorgen vor der **Sonnenfinsternis am 20. März** äußert die FAZ am 17. Februar. Wenn die Sonne plötzlich wegbleibt und die Solarstromerzeugung einbricht, müssten schnell Ersatzkapazitäten zur Verfügung stehen, die für Stabilität im Netz sorgen. Für die Vorbereitung sei es wichtig zu wissen, wie groß die Sonnenfinsternis ausfällt, wann und wie lange der Mond die Sonne verschattet, wo sie sich über der Erdkugel ausbreitet und wie das Wetter an dem Tag ist. Ein wolkenloser Himmel mache es schwieriger, das Stromnetz auszubalancieren. Nach Berechnungen der Berliner Hochschule für Technik und Wirtschaft erzeugten PV-Anlagen zu Beginn der Sonnenfinsternis am 20. März bei wolkenlosem Himmel 17.500 Megawatt. Dann breche sie binnen einer Stunde auf 6.200 Megawatt ein, um sich bis Ende der Sonnenfinsternis um 12 Uhr auf 25.000 Megawatt zu vervierfachen. Niemand wisse, was die Verbraucher tun. Schalten sie massenhaft das Licht ein,

wenn sich der Himmel am Vormittag verdunkelt und erhöhen damit die Nachfrage trotz gerade knapper Erzeugung, oder stehen alle draußen und betrachten das seltene Naturschauspiel? Die Netzbetreiber müssten sich auf den ungünstigsten Fall vorbereiten. Das Wirtschaftsministerium empfehle „die präventive Abregelung von PV-Anlagen". Europaweit sollten Anforderungen an die Sicherheit angehoben werden. Auf keinen Fall solle ein Black out in einer Region wie eine Lawine durchs Netz rasen und eine Abschaltung nach der anderen erzwingen.

Terrorismus

Die FAZ weist am 10. Februar auf die **Versicherung Extremus AG** hin, die Terrorschäden bis zu zwei Mrd. Euro trage. Oberhalb dieser Summe springe der Staat ein. Erfreuten sich die Deckungen in der Unsicherheit nach dem 11. September 2001 großer Beliebtheit, habe die Nachfrage inzwischen merklich nachgelassen. In den ersten 14 Monaten nach dem Start habe Extremus noch rund 90 Mio. Euro Prämie eingesammelt. 2014 sei dieser Wert auf 47 Mio. Euro gefallen. 7.500 Risiken in Deutschland seien versichert. Schließe ein Unternehmen eine Police ab, dann seien alle Standorte versichert. Zum Teil könnten Unternehmen heute auch wieder Schutz bei privaten Anbietern bekommen. Doch ein kontinuierliches Angebot sei in den besonders gefährlichen Ballungsräumen nur durch die Staatsgarantie möglich. Deckungen an ausländischen Standorten böten internationale Industrieversicherer wie Ace, AIG, der Lloyd`s Versicherungsmarkt und die Allianz-Tochter AGCS. Deckungssummen bis zu 1,4 Mrd. Euro könnten die Interessenten abschließen, wenn sich mehrere Versicherer zu einem Konsortium zusammenschließen. Die Extremus AG habe bisher noch nie einen Schaden begleichen müssen. Sehr viel mehr Bewegung sähen Marktteilnehmer heute bei der **Versicherung politischer Risiken.** Die Nachfrage nach ihnen steige kontinuierlich. Staatliche Beschlagnahmungen, Folgen von Embargos und Vertragsbruch von Staaten ließen sich damit versichern. In der Ukraine zahlten Versicherer, weil Betriebe wegen ausbleibender Stahllieferungen ihre Produktion unterbrechen müssten. Das Beispiel Ukraine habe gezeigt, dass es zu spät ist, sich eine Versicherung beschaffen zu wollen, wenn das Haus schon brennt. Vielmehr müssten Unternehmen antizipieren, wo in fünf Jahren Konflikte ausbrechen könnten.

Die EU soll im Kampf gegen den Terrorismus eine Reihe neuer gesetzlicher Vorkehrungen treffen sowie bestehende Vereinbarungen zur grenzüberschreitenden Zusammenarbeit besser nutzen. Dies hätten nach einer Meldung der FAZ vom 13. Februar die Staats- und Regierungschefs zugesichert. Die Blockade zur geplanten EU-Regelung zur **Erfassung und Speicherung der Daten von Flugpassagieren** soll aufgehoben werden. Die Rolle von Europol und der Vorläuferbehörde einer europäischen Staatsanwaltschaft solle gestärkt werden. Ziel der EU-Partner sei es ferner, durch bessere Aufklärung den auch über das Internet verbreiteten Botschaften radikaler Gruppierungen sowie der Anwerbung von Dschihadisten in Europa wirksamer als bisher zu begegnen. Schließlich verpflichteten sich die Staats- und Regierungschefs zu einer engeren Abstimmung und Zusammenarbeit bei der Terrorismusbekämpfung mit den Staaten Nordafrikas, im Nahen Osten und auf dem westlichen Balkan.

Verfassungsschutz

Die deutschen Verfassungsschutzbehörden sollen in Zukunft besser zusammenarbeiten. Auch der Einsatz von V-Leuten solle genauer geregelt werden. Das gehe aus dem Gesetzentwurf des BMI hervor, meldet die FAZ am 13. Februar. In Zukunft solle das BfV in Köln als Zentralstelle gestärkt und die Landesämter sollen „effektiv verzahnt" werden. Köln solle die Zusammenarbeit der Landesämter zudem koordinieren. Diese sollten unverzüglich die für ihre Aufgabenwahrnehmung relevanten Informationen übermitteln. Sie sollten in verschiedenen Bereichen gemeinsame Dateien führen. Informanten, die schon einmal zu einer Haftstrafe ohne Bewährung verurteilt wurden, sollten nicht mehr als V-Leute angeworben werden. Zudem müssten sie ein Einkommen haben, das sie von den Geldzahlungen unabhängig macht, die sie für ihre Informantentätigkeit erhalten.

Verschlüsselung

Mit seinem **Encrypted USB Flash Drive** präsentiere Toshiba einen USB 2.0-Stick mit integrierter Verschlüsselung nach AES 256 Bit und Sicherheitszertifizierung FIPS 140-2 Level 3, berichtet heise.de am 4. Februar. Um an die Daten des Sticks zu gelangen, sei vor dem Einstecken in einen USB-Port ein Passwort über die integrierte Tastatur einzugeben. Damit das funktioniere, versorge ein integrierter Akku den Stick abseits eines USB-Ports mit Strom.

Freie Verschlüsselungs-Software werde in industriellen Kreisen an allen Ecken und Enden verwendet, schreibt Constanze Kurz in der FAZ am 9. Februar. Natürlich enthielten bei allem Idealismus auch Open Source-Projekte Fehler. Die überwiegende Mehrheit seien Ungenauigkeiten, Schlampereien oder Denkfehler des Programmierers. Bei Projekten ohne Qualitätssicherungsdruck schlichen sich auch gern Abkürzungen und lose Enden ein. Dokumentiere und korrigiere man diese Kleinigkeiten frühzeitig, bestehe die Chance, dass Probleme entdeckt werden, bevor sie sich zu Sicherheitslücken auswachsen.

Videoüberwachung

Viktor Kaiser, Schirra IT, befasst sich in der Zeitschrift GIT (Ausgabe 1/2-2015, S. 60/61) mit **IP-Video in der Cloud.** Kein IP-Client werde ohne Weiteres Zugriff auf eine Mobilfunk-Kamera ermöglichen. Zudem sei eine für die direkte Kamera-Ansprache erforderliche feste IP-Adresse im Mobilfunk schwer realisierbar. Deshalb sei **ipvCloud** entwickelt worden. Vereinfacht gesagt werde für den wechselseitigen Datenaustausch zwischen Mobilfunk-Kamera und dem Internet ein Tunnel in Form eines privaten virtuellen Netzes gelegt. Diese Infrastruktur eröffne nicht nur den gezielten Zugriff auf das Endgerät, sondern gewährleiste noch dazu eine maximal mögliche Verschlüsselung. Mit der ipvCloud ließen sich verteilte Standorte und komplette Netzwerke und Leitstellen flexibel miteinander verbinden. Es gebe sie als gehostete Lösung im Rechenzentrum, als virtuelle Maschine oder direkt auf physikalischer Hardware. Dank der hohen Skalierbarkeit ließen sich von einer bis mehr als 1.000 Verbindungen pro Instanz herstellen. Zu Dokumentationszwecken lege ipvCloud ein sortiertes Bildarchiv an.

Netzwerkvideotechnik gewinnt weiter an Attraktivität und Fahrt, sind Martin Gren und Edwin Roobol, Axis Communications, überzeugt (GIT, Ausgabe 1/2-2015, S. 86–88). Die Absatzzahlen von Netzwerk-Kameras würden bis Ende 2018 um 22 Prozent jährlich steigen, nach Beurteilung von Techno System Research um 16 Prozent pro Jahr bis 2017. Gründe dafür sehen die Autoren in der Entwicklung von neuen Technologien, wie etwa 4K-Video, Video-Überwachungsservices via Cloud oder die einfache und schnelle Analyse von großen Mengen an Videodaten. Deshalb sei es erstaunlich, wie wenige Läden auf ein integriertes System setzten und sich dadurch viele Vorteile der IP-Technologie entgehen lassen. War früher eine Integration von Warensicherungsantennen, Kassen und Videosystemen nur über eine aufwendige Verkabelung zu erreichen, so biete die IP-Technologie heute völlig neue, intelligente und effiziente Möglichkeiten. Cloud Computing liege 2015 im Trend. Für die nächsten Jahre prognostiziere IHS (Innovative Handling Systeme) dem Video Surveillance as a Service Market ein durchschnittliches Wachstum von jährlich 17 Prozent und rechne 2017 mit fast 1,3 Mrd. Dollar Marktvolumen.

Die Herausforderung **Videoüberwachung am Flughafen** thematisiert GIT in der Ausgabe 1/2-2015, S. 69. Je flexibler die gewählte Videoüberwachungssoftware gegenüber der Einbindung anderer Systeme ist, desto mehr Funktionen könnten über ein einziges System gesteuert werden. Vorteilhaft seien hier Open Source-Plattformen wie die von Milestone Systems, die eine Vielzahl an Herstellern integriert hat. So könnten mit Hilfe einer Schnittstelle zur Zutrittskontrolleinheit Bereiche mit eingeschränktem Zugang detektiert werden. Werde eine Tür mit Zutrittskontroll-Terminal mittels einer Zugangskarte durchschritten, oder werde eine Bewegung in dem Bereich des Zugangs von der Kamera erfasst, starte die Aufnahme. Eine Loitering-Funktion helfe zusätzlich dabei, Personen anzuzeigen, die sich in bestimmten Bereichen verdächtig lange aufhalten. Die zusätzliche Einbindung von Kassensystemen in die Videomanagementsoftware könne dabei helfen, Ticketschalter oder Shops im Wartebereich des Flughafens zu überwachen und die Transaktionen zu detektieren.

Zufahrtskontrolle

In Security insight (Ausgabe 1-2015, S. 22/23) wird gezeigt, wie man softwaregesteuert die Be- und Entladung von Lkw auf dem Werksgelände sicher und effizient gestaltet. Moderne Systeme setzten bereits vor der Einfahrt an: Ein Zeitslot werde avisiert und eine Voranmeldung eingetragen. Bevor ein Lkw die Schranke zum Werksgelände passiert, würden die wesentlichen Daten des Fahrzeugs erfasst. Außerdem werde der Fahrer registriert. Eine lückenlose Dokumentation der einzelnen Stationen schaffe Transparenz. Mittels Einsatz eines Pager-Systems könne der Lkw-Verkehr auf dem Gelände weiter optimiert werden. Entscheide man sich für ein webbasiertes System mit zentraler Serverinstallation, ließen sich beliebig viele Standorte sicher verbinden und zentral verwalten.

Zutrittskontrolle

Allnet GmbH nennt in der Ausgabe 1/2-2015 (S. 64/65) der Fachzeitschrift GIT die 5 schlagendsten Gründe für IP-basierende Zutrittskontrolle:

- leichte Integration in Drittanbietersysteme
- zentralisiertes Management und Fernwartung
- mehr Sicherheit durch Echtzeit-Überwachung
- standardbasiert mit OSDP und daher herstellerunabhängig
- einfache Installation, anwenderfreundlich und kostensparend.

Marcus Heide, Chefredakteur von Security insight, zeigt in der Ausgabe 1-2015, S. 16/17, warum eine **„konvergente"** Lösung für Zutritts-, Zufahrts- und Zugriffskontrolle Betriebsprozesse effektiver macht und gleichzeitig mehr Sicherheit schafft. Die Vorteile der „Konvergenz" – also des Zusammenwachsens unterschiedlicher Systeme – lägen auf der Hand: Regelwerke ließen sich „geschmeidiger" durch Technik in die Organisation implementieren, die Abläufe seien reibungsloser. Der Nutzwert einer konvergenten Identity-Lösung steige natürlich mit der Zahl der möglichen Anwendungen. Das Smartphone werde den Zutritts-, Zufahrts- und Zugriffsausweis einmal ablösen.

Es sei nur eine Frage der Zeit, dass die Zutrittskontrolle auf IP aufsetzt, heißt es in Security insight (Ausgabe 1-2015, S. 21/22). Der Übergang zu ATCP/IP-basierten Systemen in der Zutrittskontrolle sei vergleichbar mit dem Wechsel von analoger zu digitaler Videotechnologie. Prinzipiell bestünden in einer standardisierten digitalen Umgebung unzählbar viele Möglichkeiten zur Integration weiterer Systeme, etwa Einbruchmelde- und Brandmeldesysteme. Ein IP-basiertes System sei auch weniger anfällig für Stromengpässe und Netzwerkausfälle.

Der Markttrend geht in Richtung mobile Identifikation („Mobile ID"), meint Klaus U. Klosa, Legic Identsystems AG, in Security insight (Ausgabe 1-2015, S. 24). Betreiber würden so Kosten sparen und den Komfort steigern, indem sie ihre ID-Vergabeprozesse verkürzen. Ein weiterer Vorteil von Mobile ID sei die temporäre Rechtevergabe. Und gehe das Smartphone verloren, könnten jegliche Rechte sofort gelöscht werden.

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