FOCUS ON SECURITY

AUSGABE 04, APRIL 2018

SECURITAS

Inhaltsverzeichnis

Alarmempfangstechnik

Dipl.-Ing. Günter Grundmann, VdS Schadenverhütung, befasst sich in s+s report, Ausgabe 1-2018, S. 40/41, mit der überarbeiteten Richtlinie **VdS 2466 und** der neuen **VdS 3500**. Die heutige Alarmtechnik werde ausschließlich über IP-basierte Netze realisiert, deren Empfangstechnik moderne digitale Datenverarbeitung nutzt. Mit den neu entwickelten Richtlinien VdS 3500, „Alarmempfangssoftware, Anforderungen und Prüfmethoden", werde die Möglichkeit eröffnet, auch ausschließlich die Softwarefunktionalität und deren Bediensicherheit von Alarmempfangseinrichtungen zu prüfen und zu zertifizieren. Für den VdS-konformen Betrieb der Alarmempfangseinrichtung in der Alarmempfangsstelle müssten Maßnahmen getroffen werden, die zum Beispiel Risiken durch Umwelteinflüsse in gleicher Weise minimieren, wie es für gerätetechnisch geprüfte Hardware gemäß VdS 2466 der Fall wäre. Außerdem sei für den Betrieb dieser Technik ein Gefahrenmanagementsystem nach VdS 3534 notwendig, um eine entsprechende Nutzerschnittstelle mit Darstellung der Informationen zu realisieren. Funktionell würden die Richtlinien insbesondere in Bezug auf die bestimmenden Kenngrößen für die Qualität der Alarmübertragung erweitert.

Arzneimittelsicherheit

Mit **SecuPharm** haben Apotheker, Großhändler und Hersteller ein gemeinsames System entwickelt, das die Einschleusung gefälschter Packungen in die legale Lieferkette nahezu unmöglich machen soll, berichtet die Apotheken Umschau in der Ausgabe vom 15. März. Jedes rezeptpflichtige Medikament werde mit einem 2-D-Code mit individueller Seriennummer versehen. Ein Erstöffnungsschutz solle zudem gewährleisten, dass die Packung auf dem Vertriebsweg nicht geöffnet wurde. Um sicherzugehen, dass eine Packung weder gefälscht noch gestohlen wurde, überprüften Apotheker vor der Abgabe den Sicherheitsverschluss, scannten den 2-D-Code und glichen die eingelesene Seriennummer mit einer zentralen Datenbank ab.

Bankensicherheit

Wie spiegel.de am 27. März berichtet, hat die schweizerische Finanzmarktaufsicht vor einer wachsenden Zahl von **Hackerangriffen in der Finanzwelt** gewarnt. Allein in der Schweiz würden jeden Tag hundert Angriffe auf E-Banking-Lösungen erfolgreich abgewehrt. Cyberangriffe seien inzwischen das größte operationelle Risiko außerhalb der typischen unternehmerischen Risiken für das Finanzsystem. Dass Banken zunehmend Dienstleistungen an IT-Infrastruktur auslagerten, verstärke die Cyberbedrohung.

Bis zu einer Milliarde Euro sollen die **„Cyberbankräuber" der Carbanak/Cobalt-Gruppe** in den vergangenen Jahren erbeutet haben, schreibt Martin Schindler am 27. März auf silicon.de. Neben Backdoor-Programmen für Spionage, Datendiebstahl und Remotezugriffen installierten die Hacker über die angegriffenen Personen auch eine Suche, die nach Finanztransaktionssystemen sucht. Dafür seien in manchen Fällen mehrere Hundert PCs infiziert worden, um schließlich an den Administrator der Banksysteme zu gelangen. Die Behörden gingen davon aus, dass seit 2013 die Gruppe mehr als 100 Banken, E-Payment-Systeme und andere Finanzorganisationen in mindestens 30 Ländern in Europa, Asien, Amerika sowie anderen Regionen attackiert habe. Über die angegriffenen Systeme hätten die Bankräuber entweder Geld auf eigene Konten überwiesen, die Beträge auf Bankkonten geändert oder Geldautomaten angewiesen, zu einem bestimmten Zeitpunkt Geld auszuspucken. Anschließend seien die Beträge in Kryptowährungen umgetauscht worden. Angesichts des internationalen Ausmaßes der Aktivitäten dieser Akteure gehe Kaspersky Lab davon aus, dass Dutzende von Menschen an dieser Cybercrime-Aktivität beteiligt sind. Es gebe Anzeichen dafür, dass die Urheber der Malware Carbanak russischsprachig sind.

Baustellendiebstahl

Laut LKA betrage der Schaden, der 2017 durch gemeldete Diebstähle auf Baustellen, in Rohbauten und Neubauten in Nordrhein-Westfalen entstanden ist, insgesamt 9,4 Mio. Euro, berichtet itipro.com am 26. März. Die Dunkelziffer liege weitaus höher. Nicht mitgerechnet seien Kosten für Beschädigungen, Folgekosten für die Wiederbeschaffung, Ausfallkosten

und Konventionalstrafen, wenn der Zeitplan nicht eingehalten wird. Für Schäden durch Diebstahl und Vandalismus würden selbst spezielle Bauversicherungen nicht aufkommen.

Betrug

Bayerns Innenminister Herrmann und Justizminister Prof. Dr. Bausback verstärken gemeinsam den Kampf gegen **Betrug im Gesundheitswesen**, meldet SecuPedia am 28. März. Laut Kriminalstatistik seien 2017 in Bayern 325 Fälle des Abrechnungsbetrugs im Gesundheitswesen mit einer Schadensumme von 5,9 Mio. Euro polizeilich angezeigt worden. Ein besonderes Problem sei hier das extrem große Dunkelfeld, habe Herrmann mit Blick auf den durch interne Kontrollen der Leistungsträger bundesweit festgestellten Schaden von rund 35 Mio. Euro erklärt, der auf nur rund 0,25 Prozent des tatsächlichen bundesweiten Schadens in Höhe von ca. 14 Mrd. Euro pro Jahr geschätzt werde.

Biometrie

Golem.de berichtet am 12. März über einen **Test biometrischer Systeme beim Boarding**. Flugkarte und Ausweis müssten Passagiere der British Airways an einigen Flughäfen in den USA am Gate nicht mehr vorzeigen. Stattdessen scanne die Fluglinie ihre Gesichter. Ein Blick in die Kamera, einen kurzen Moment warten, und schon könne der Fluggast passieren. Mit biometrischen Systemen wollten die Fluggesellschaften die Abfertigung effizienter machen. Es dauere 22 Minuten, 400 Passagiere in das Flugzeug einsteigen zu lassen. Das konventionelle Boarding nehme mehr als doppelt so lange in Anspruch, habe die Fluglinie mitgeteilt.

Gesichtserkennung ist in China auf dem Vormarsch, weil sie viele Vorteile biete, schreibt Frank Sieren auf dw.com am 29. März. Die Brille einer Polizistin sei mit einem Gesichtscanner ausgestattet, mit der sie die Massen am Ostbahnhof der zentralchinesischen Stadt Zhengzhou durchleuchtet. Verbunden mit einer riesigen Datenbank könne sie gesuchte Personen in Sekundenschnelle erkennen. Das Pilotprojekt in der Provinz Henan gelte schon jetzt als Erfolg: Seit Februar seien dank der Brillen mehr als sieben mit Haftbefehl gesuchte mutmaßliche Kriminelle verhaftet und 35 Menschen mit falschen Personalausweisen erwischt worden. In China sorgten um die 176 Mio. Kameras für eine engmaschige Überwachung im öffentlichen Raum. Bis 2020 sollen 450 Mio. weitere hinzukommen. Die Einsatzgebiete der Gesichtserkennung beschränkten sich nicht auf Überwachung. Als Authentifizierungsmethode sei die Technik deutlich sicherer als Passwörter oder PIN-Nummern. „Fotobetrug" sei durch „Lebendigkeitstests" ausgeschlossen, bei denen die Scanner Mundbewegungen und Muskelregungen einfangen. Auch schnellere Einlasskontrollen würden durch Gesichtserkennung möglich.

Brandschutz

Brandschutz in Kraftwerken thematisiert Dr. Günther Rossmann, GDV, in Ausgabe 1-2018 der Zeitschrift s+s report, S. 16–20. Die Betreiber von konventionellen Kraftwerken seien durch zahlreiche Bestimmungen aus unterschiedlichen Rechtsbereichen verpflichtet, jeweils rechtsbereichsbezogen die Risiken und Gefährdungen, die bei der Errichtung und dem Betrieb der Anlagen auftreten können, eigenverantwortlich zu ermitteln. Der Autor behandelt rechtliche Anforderungen, betriebswirtschaftliche Aspekte, Struktur und Inhaltsmerkmale der VdS 3132, den baulichen Brandschutz, Brandschutzanlagen und technischen Brandschutz sowie Explosionsschutz. Bei der Planung und Errichtung von Brandschutzanlagen sei darauf zu achten, dass dies nach den anerkannten Regeln der Technik erfolgt. Weiterhin dürfe die Installation grundsätzlich nur durch anerkannte Errichterfirmen durchgeführt werden. Für den Explosionsschutz sei die Explosionsgefährdung durch Gase, Dämpfe, Nebel und/oder Stäube systematisch wiederkehrend zu bewerten. Die formale Umsetzung der Anforderungen habe in den Unternehmen über das Explosionsschutzdokument zu erfolgen.

Alternative Löschsysteme für Siemens-Gasturbinen behandelt Dipl.-Ing. Wolfgang Hensel, Siemens AG, in s+s report, Ausgabe 1-2018, S. 22–25. Sein Beitrag beschäftigt sich mit der Frage, in welche Richtung das Brandschutzkonzept und das Löschkonzept für die Siemens-Gasturbinen großer Leistung (F- und H-Klasse) in nächster Zukunft tendieren könnten. Einschlägige Regelwerke, wie zum Beispiel die VGB R108 oder die NFPA 850, enthielten konkrete Vorgaben in Bezug auf Schutzmaßnahmen für Gasturbinen. Für alle Schutzkreise gelte der Grundsatz, dass mindes-

tens zwei Meldergruppen oder Meldertypen ausgelöst sein müssen. Beschrieben werden in dem Beitrag das Stickstoff/Wasser-Löschsystem von Siemens sowie die Wassernebel-Löschanlage von Minimax. Im Zusammenwirken der beiden Medien Stickstoff und Wasser werde eine vergleichbare Inertisierung und eine wesentlich bessere Kühlwirkung als mit einer CO2-Löschanlage erzielt. Für die Gasturbinen-Einhausung bestehe die Forderung, über eine vorgegebene Zeitspanne – i.d.R. ca. 20 Minuten – eine Mindestkonzentration aufrechtzuerhalten. Dazu würden eine Einsatzflutung und eine Halteflutung zur Anwendung gebracht. Beide werden vom Autor beschrieben. Die Wirkungsweise des von Minimax entwickelten Hochdruck-Wassernebelsystems sei ähnlich der einer Sprühwasserlöschanlage. Der wesentliche Unterschied bestehe in der viel feineren Zerstäubung des Wassers. Die insgesamt eingebrachte Wassermenge sei im Vergleich zu herkömmlichen Sprühwasserlöschanlagen wesentlich geringer.

Dipl.-Ing. Frank Bieber, VdS Schadenverhütung, beschäftigt sich in s+s report, Ausgabe 1-2018, S. 26–29, mit den Richtlinien **VdS 2109, 2108 und VdS CEA 4001**. Der Beitrag bietet einen Einblick in die Richtlinien-Fortschreibung und konkrete Ergebnisse am Beispiel der VdS CEA 4001. Anfang des letzten Jahrhunderts sei das gesamte Sprinklerwissen auf zehn Seiten dargestellt worden. Mit der aktuellen Version der VdS CEA 4001 sei die 300-Seiten-Marke durchbrochen worden; die Sprinklerwelt werde immer komplexer. Der Autor beschreibt redaktionelle Änderungen, Fehlerkorrekturen und Klarstellungen, ein alternatives Schutzkonzept für Regallager (Abschnitt 11.6), den Anschluss anderer Verbraucher an die Wasserversorgung (Abschnitt 7.2), Rohrhalterungen (Abschnitt 15.2), Gebäude mit Rauch- und Wärmeabzugsanlagen (Abschnitt 12.5.2) und Anforderungen an große Anlagen (Anhang M.2.6).

In der Zeitschrift s+s report, Ausgabe 1-2018, S. 33, wird auf die VdS-Publikation „**Galvanotechnische Betriebe – Gefahren, Risiken, Schutzmaßnahmen**" hingewiesen. Die Publikation enthalte Hinweise zur Vermeidung von Bränden und Explosionen sowie deren Auswirkungen und beschreibe mögliche bauliche, anlagentechnische sowie organisatorische Schutzmaßnahmen.

In Fortsetzung eines Beitrags in Ausgabe 4-2017 der Zeitschrift s+s report geben Stephanie Brandt, Siemens AG, Dr. Alexander Duric und Christian Lais, beide Siemens Schweiz AG, in der Ausgabe 1-2018, S. 34–38, eine Übersicht zu Technologien und Regelwerken der **Brandfrüherkennung durch CO-Melder**. Sie befassen sich mit der Messung des Ansprechverhaltens für Rauch, Wärme und CO-Konzentration, dem Test von Multikriterien-Meldern mit CO-Detektion, mit Kategorien für Mehrfachsensor-Brandmeldern mit CO-Detektion und mit der zusätzlichen Detektion toxischer CO-Konzentrationen. Je nach Anwendungsfall erfolge der Einsatz von CO-Meldern ausschließlich als Gasmelder entweder direkt zur Alarmierung vor dem Auftreten von toxischer Gaskonzentration – beispielsweise im Eigenheimbereich, in Hotels, Krankenhäusern und Seniorenheimen – oder zur Überwachung der CO-Konzentration. Auch wenn es sich bei der Branderkennung und der Detektion von toxischem CO-Gas um zwei unabhängige Schutzfunktionen handelt, so scheine die technische Integration von beiden in einem Melder interessant. Die beste Antwort auf die komplexen Herausforderungen des Schutzes vor Brandschäden und vor toxischem CO-Gas böten intelligente Mehrfachsensor-Brandmelder mit integrierter CO-Detektion. Eine logische Weiterentwicklung stellten Brandgasmelder dar. Auch wenn bei dieser Technologie noch einige Herausforderungen im Bereich der Sensorik bestünden, böte dieser Meldertyp einen interessanten Vorteil: Er benötige keine Messkammer und ermögliche damit eine deutlich kleinere Bauform als heute übliche Modelle.

Branddetektion mit **Meldern für jede Umgebung** bietet Securiton in der Ausgabe 4-2018 der Zeitschrift GIT, S. 64–68, an. Behandelt werden in dem Fachbeitrag Mehrfachsensormelder, Sonderbrandmeldetechnik für harte Umgebungsbedingungen, hochempfindliche Ansaugrauchmelder, linienförmige Wärmemelder, bei denen Fühlerrohre Luft und Druckanstieg auf einen Sensor in der Auswerteeinheit übertragen und Temperatursensorkabel, für die Staub, Hitze, Rauch oder Abgase kein Problem darstellen, weil ausgereifte Sensorkabel hochempfindliche adressierte Sensoren enthalten, deren Ansprechverhalten individuell programmiert werden könne, ebenso wie verschiedene Detektions- und Alarmschwellwerte in unterschiedlichen Abschnitten. Die Kabel überwachten Strecken von bis zu 3.200 Metern Länge oder bis zu 350 Sensoren.

Mit **CO-Warnmeldern** befasst sich GIT in der Ausgabe 4-2018, S. 68/69. Wer Öfen oder Gasthermen betreibt, sollte auf jeden Fall Kohlenmonoxid-Warnmelder (wie den Fire Angel DO-9D-DE) anbringen. Die elektrochemische Sensortechnologie der Kohlenmonoxid-Warnmelder warne nicht nur bei einer akuten Kohlenmonoxid-Gefahr, sondern auch, wenn sich über einen längeren Zeitraum eine gefährliche Kohlenmonoxid-Konzentration entwickelt.

Datenschutz

Der **Messengerdienst WhatsApp** gebe bereits eine ganze Reihe von Nutzerdaten an den Mutterkonzern Facebook weiter, meldet golem.de am 16. März. Dies gehe aus einem Bescheid der spanischen Datenschutzbehörde AEPD hervor, mit dem die beiden Firmen zur Zahlung eines Bußgeldes von jeweils 300.000 Euro verpflichtet werden. Die Weitergabe erfolge unabhängig davon, ob der WhatsApp-Nutzer auch ein Facebook-Konto hat, und diene den unternehmerischen Zwecken von Facebook, heißt es in dem Bescheid. Der Messengerdienst habe im August 2016 angekündigt, nach der Übernahme durch Facebook die Telefonnummern seiner Nutzer sowie Informationen zur Nutzungshäufigkeit an das weltgrößte soziale Netzwerk weiterzugeben. Dem Bescheid der Datenschutzbehörde zufolge teile WhatsApp zwar nicht die Telefonnummern seiner Nutzer mit, zu den übermittelten Daten gehörten jedoch neben der WhatsApp-Account-ID auch Informationen über das genutzte Gerät, bestimmte Nutzereinstellungen, die „zuletzt online"-Angaben sowie das Anmeldedatum des WhatsApp-Accounts. Der Hamburger Datenschutzbeauftragte habe die ursprünglich intendierte Datenweitergabe lediglich für unzulässig erklärt bzw. untersagt. Das OVG Hamburg habe diese Anordnung bestätigt, dass Facebook nicht massenhaft personenbezogene Daten seiner Tochterfirma WhatsApp für eigene Zwecke nutzen dürfe.

Es habe sich herausgestellt, dass Facebook jahrelang **Anrufmetadaten von Android-Nutzern gesammelt** habe, meldet golem.de. Wer die App in den vergangenen Jahren installiert hat und ihr die Rechte gab, auf Logdateien des Kurznachrichtenservice SMS sowie auf die Logs von Telefonaten zuzugreifen, finde diese Daten offenbar später auch in seinen Facebook-Daten. Diese Informationen würden an das soziale Netzwerk hochgeladen. Dies habe Facebook in einer Stellungnahme als normalen Vorgang dargestellt. Zum einen betone das Unternehmen, dass die Daten freiwillig von den Nutzern hochgeladen worden seien, da die App nach entsprechenden Zugriffsrechten frage. Zum anderen sei es „Gang und Gäbe", dass Kontaktdaten hochgeladen würden.

Drohnen

Ein Hobbypilot sei mit seiner Drohne am **Flughafen Köln/Bonn** den Flugzeugen so nahe gekommen, dass die große Start- und Landebahn mehrmals gesperrt werden musste, meldet die FAZ am 9. April. Ein Lufthansa-Flug aus München sei wegen der Sperrung schließlich nach Düsseldorf umgeleitet worden. In Nordrhein-Westfalen habe es 2017 nach Angaben der DFS 15 Zwischenfälle gegeben, bundesweit 70 Behinderungen an Flughäfen.

Extremismus

Die FAZ weist am 6. April darauf hin, dass die **Salafisten-Szene** in Deutschland nach Angaben des BMI in den vergangenen fünf Jahren enorm gewachsen ist: von 5.500 auf inzwischen bundesweit rund 11.000 Menschen, die sich zu dieser ultrakonservativen islamischen Strömung bekennen. Experten würden zwischen pietistischen, politischen und militanten Salafisten unterscheiden. Alle lebten nach strengen religiösen Regeln und lehnten die Werte westlicher Gesellschaften ab. Ein Teil der in Deutschland lebenden Salafisten akzeptierten Gewalt und Terror als Mittel zur Durchsetzung der Ziele der Bewegung.

In der April-Ausgabe von Veko-online.de befasst sich Dr. Stefan Goertz mit dem **islamistisch-terroristischen Personenpotenzial**, das er aktuell mit 1.830 quantifiziert. „Gefährder" und „relevante Person" seien nicht gesetzliche, sondern polizeilich abgestimmte Definitionen. Als **Gefährder** werde eine Person bezeichnet, zu der bestimmte Tatsachen die Annahme rechtfertigen, dass sie politisch motivierte Straftaten von erheblicher Bedeutung begehen werde, insbesondere i.S.v. § 100 a StPO. Eine Person ist nach der polizeilichen Definition als relevant anzusehen, wenn sie innerhalb des extremistisch/terroristischen Spektrums die Rolle einer Führungsperson, eines Unterstützers/Logistikers oder eines Akteurs einnimmt und objektive Hinweise vorliegen, die die Prognose zulassen, dass sie politisch motivierte Straftaten von erheblicher Bedeutung, insbesondere solche i.S.v. § 100 a StPO, fördert, unterstützt, begeht oder sich daran beteiligt, oder dass es sich um eine Kontakt- oder Begleitperson eines Gefährders, eines Beschuldigten oder eines Verdächtigen einer politisch motivierten Straftat von erheblicher

Bedeutung, insbesondere einer solchen nach § 100 a StPO handelt. Im Rahmen eines „Gefährderprogramms" wurden „Gefahrenermittlungen" durchgeführt, um das Gefahrenpotenzial bestimmter Personen festzustellen. Der Autor erklärt das Konzept RADAR-ITE, eine regelbasierte Analyse potenziell destruktiver Täter zur Einschätzung des aktuellen Risikos von islamistischem Terrorismus. In Deutschland seien derzeit über 570 Personen als Gefährder und rund 360 als **relevante Personen** eingestuft. Neben RADAR-ITE stünden der Polizei zwei weitere standardisierte Einstufungssysteme zur Verfügung. Während im klassischen Gefahrenabwehrrecht regelmäßig eine konkret bis hinreichend differenzierende Eintrittswahrscheinlichkeit erforderlich sei, gelte hiervor abweichend für eine Abschiebungsanordnung nach § 58 a AufenthG ein eigener Wahrscheinlichkeitsmaßstab. Für diese Anordnung müsse eine bestimmte Entwicklung nicht wahrscheinlicher sein als andere. Es genüge nach der Rechtsprechung des BVerwG vielmehr, dass sich aus den festgestellten Tatsachen ein beachtliches Risiko für eine terroristische Gefahr ergibt.

Fake-Shops

Die FAZ berichtet am 4. April von Shop-Besitzern auf der **Amazon-Plattform**, die von Fake-Shop-Betrügern heimgesucht worden seien. Die Gauner böten auf den eingeführten und meist sehr positiv bewerteten Plätzen qualitativ hochwertige Produkte zu besonders günstigen Konditionen an und lockten damit die Kunden. In Wirklichkeit aber existierten die attraktiven Offerten gar nicht. Die Kriminellen verlangten von den ahnungslosen Käufern oft über Konten im Ausland Vorkasse, doch der Versand der Ware finde nie statt. Oft werde mit gefälschten Bankkonten gearbeitet. Kunden, die von Betrügern für die Bestellung trickreich von der Amazon-Seite gelotst werden und zahlen, erhielten keine Rückerstattung. Fake-Shops trieben auch über eigens installierte Internetseiten ihr Unwesen. Typische Merkmale von Fake-Shops seien: auffällig niedrige Preise, fehlendes Impressum, fehlende Kontaktdaten. Und vor allem: die Forderung nach Vorkasse.

Frachtdiebstahl

Nach Angaben des GDV belaufen sich die direkten Schäden durch Frachtdiebstahl von Lkws in Deutschland auf rund 300 Mio. Euro im Jahr, berichtet die FAZ am 5. April. Die Dunkelziffer liege noch viel höher. Die volkswirtschaftlichen Folgeschäden beliefen sich auf ein Vielfaches der entwendeten Fracht. Den sogenannten „Planenschlitzern" habe die Alarmplane.de GmbH den Kampf angesagt. Das Unternehmen entwickele eine Vorrichtung, die Diebe abschrecken soll. Es habe ein Drahtnetz entwickelt, das an den Lkw-Planen angebracht wird. Die einzelnen Segmente würden auf die bisher verwendete Plane aufgeschweißt. Die Plane funktioniere mit einer separaten Stromversorgung über eine Batterie. Eine eigens entwickelte Software in dem Mikrocontroller führe dazu, dass der Stromverbrauch so gering sei, dass die Plane eine Laufzeit von etwa drei Jahren ohne Nachladen des Akkus habe. Sobald der separate Stromkreis durch das Zertrennen des Drahtnetzes unterbrochen wird, werde ein akustischer oder optischer Alarm ausgelöst. Der Stückpreis belaufe sich auf ca. 2.000 Euro. Die Kravag-Logistic Versicherungs AG biete einen Nachlass von zehn Prozent, wenn der **Auflieger mit der Alarmplane geschützt** wird. Spediteure erhielten auch eine Förderung vom Bundesamt für Güterverkehr über das Förderprogramm „De-minimis" (80 Prozent der Umbaukosten). Skeptiker glaubten, dass sich organisierte Banden durch die Alarmplane nicht abschrecken lassen und gegen sie nur Kofferzüge wirksam seien, die teilweise mit GPS ausgestattet sind.

Gaslagerung

Asecos befasst sich in der Ausgabe 3-2018 von GIT, S. 88/89, mit der sicheren Lagerung von brennbaren, brandfördernden und toxischen Gasen in der Industrie. **Sicherheitsschränke** mit 90 Minuten Feuerwiderstandsfähigkeit seien heute Stand der Technik und böten ein vergleichbares Schutzniveau wie Lagerräume. In dem Beitrag werden Vor- und Nachteile einer zentralen Lagerung im Außenbereich oder in Lagerräumen mit Vor- und Nachteilen einer dezentralen Lagerung in Druckgasflaschenschränken gemäß DIN EN 14470-2 gegenübergestellt. Bei einem zentralen System sorge ein Rohrleitungsnetz für die Gaszufuhr an die entsprechenden Verbraucherstellen. Im Gegensatz dazu seien bei einer dezentralen

Gasversorgung einzelne Versorgungseinheiten in unmittelbarer Nähe zum Arbeitsplatz aufgestellt. Behandelt werden in dem Beitrag ferner verbesserte Installationsmöglichkeiten.

Gefahrenmeldeanlagen

Christian Metzmacher, M.Sc., VdS Schadenverhütung, thematisiert in der Ausgabe 1-2018 der Zeitschrift s+s report, S. 48–50, die **Vernetzung von Gefahrenmeldeanlagen** in Unternehmen. Moderne netzwerkgestützte Gefahrenmeldeanlagen (GMA) würden immer häufiger in Unternehmensnetzwerke integriert. Cybersecurity spiele dabei oft noch eine untergeordnete Rolle. Der Autor beschreibt Beispiele für angreifbare Schwachstellen: Fehler in der Software als Einfallstor und zusätzliche Angriffsflächen, die zusätzliche Dienste bieten. Der Ansatz zur Entwicklung eines nachhaltigen und ganzheitlichen Sicherungskonzepts könne „Security by Design" darstellen. Der Autor stellt sieben Grundsätze dieses Ansatzes vor: Minimierung der Angriffsfläche, Vergabe von Minimalberechtigungen, Aufbau der Sicherheitsarchitektur nach dem „Zwiebelschalen"-Prinzip, Etablierung einer möglichst simplen Sicherheitsarchitektur, schnelle und umfassende Behandlung von Sicherheitslücken, Zugriff auf Fremd-Services und sichere Handhabung von Fehlfunktionen. Wichtig sei, dass immer die Sicherheit des gesamten Netzwerks im Blick behalten und regelmäßig die aktuelle Gefährdungslage auf Veränderungen überprüft wird.

Gefährliche Waren

Giftige Puppen, gefährliches Spielzeug, entzündliche Akkus: Europäische Verbraucherschutzbehörden haben 2017 mehr als 2.200 Mal wegen gefährlicher Produkte Alarm geschlagen, meldet die FAZ am 13. März. Fast 4.000 Rückrufaktionen, Verkaufs- oder Importstopps seien gefolgt. 29 Prozent der Meldungen habe Spielzeug betroffen, gefolgt von Kfz (20 Prozent) und Bekleidung (12 Prozent). Wie schon im Vorjahr sei mehr als die Hälfte der beanstandeten Produkte aus China gekommen.

Geldautomatensicherheit

Automatendiebe haben ihre **Methode verfeinert**, berichtet die FAZ am 13. März. Sie setzten jetzt Smartphones für den Überfall auf die automatisierte Bankfiliale ein und raubten über SMS. Amerikanische Sicherheitsbehörden nähmen an, dass Geldautomaten von 40 Herstellern in aller Welt nach dieser Methode ausgeraubt werden können. Europa stehe eine regelrechte **Welle von Automatenüberfällen** bevor, hätten die Spezialisten des Secret Service gewarnt. Die Bankräuber arbeiteten dabei meist in Dreiergruppen. Der „Installateur" begebe sich mit einem Endoskop und einem Smartphone zum GA. Mit dem Endoskop schaue er nach, wo die USB-Schnittstelle sitzt, um die mit dem Smartphone zu verbinden. Wenn sich die Schnittstelle im Innern des GA befindet, würden die Räuber Geld abheben und durch das geöffnete Geldausgabefach das Endoskop einführen, um damit die genaue Position der Schnittstelle zu finden. Nach Anschluss des Smartphones erhalte der „Dispatcher", der in einem entfernten Büro sitze, eine Nachricht. Er sende dann eine SMS an das Smartphone. Damit werde die Schadsoftware auf dem Automaten-PC installiert. Mit einer zweiten SMS werde die Auszahlung des gesamten im GA liegenden Geldes veranlasst. Ein großer Teil der in GA verbauten Computer laufe noch immer unter dem Betriebssystem Windows XP, für das es schon lange keine Sicherheitsupdates mehr gebe.

Geldtransportüberfall

Auf dem Weg von Hamburg nach Kiel sind am 24. Januar Geldkassetten mit rund 2,3 Mio. Euro aus dem Geldtransporter verschwunden. Jetzt meldet die FAZ am 31. März, dass als Verdächtige der Fahrer des Geldtransporters und dessen Bekannter festgenommen wurden. Bei Durchsuchungen seien zwei Mio. Euro aus der Beute sichergestellt worden.

Hotelsicherheit

Funkvernetzte Rauchwarnmelder als Brandschutz für kleinere Beherbergungsbetriebe, für die die Beherbergungsstättenverordnung nicht zwingend die Installation einer

BMA vorschreibt, werden von Hekatron in Ausgabe 3-2018 der Zeitschrift GIT, S. 72–74, vorgestellt. Bei einer Erweiterung des Funk-Rauchwarnmeldesystems um den „Genius Plus-Melder" könnten durch den zentralen Datenknoten alle Informationen der Rauchwarnmelder gebündelt und im Internet bereitgestellt werden. Alle Alarme und Störungen könnten auf mobile Endgeräte übertragen werden. Bleibe trotz Alarmierung die Ursache des Alarms bestehen, würden alle Melder erneut nach zehn Minuten in Alarmierung gesetzt.

Interne Ermittlungen

Rechtsanwalt Bernd Mayer, Skadden Deutschland, weist in der FAZ am 11. April darauf hin, dass der Koalitionsvertrag eine umfassende **Neuregelung des Sanktionsrechts für Unternehmen** vorsieht. Es sollen klare Verfahrensregelungen und spezifische Regelungen über die Verfahrenseinstellung geschaffen und das Sanktionsinstrumentarium für Unternehmen erweitert werden. Außerdem plane die große Koalition, gesetzliche Vorgaben zu „Internal Investigations" und Anreize zur Aufklärungshilfe zu schaffen. Unternehmen stünden bei der internen Aufarbeitung von Rechtsverstößen vor der Herausforderung, eine eigene umfassende Sachverhaltsaufklärung mit der umfassenden Wahrung ihrer Verteidigungsrechte sowie der ihrer Organe und Mitarbeiter in Einklang zu bringen. Unklar sei derzeit, ob und wann Verfahrensrechte der Organe und Mitarbeiter auch im Arbeits- oder Organverhältnis gelten und damit, unter welchen Voraussetzungen die Mithilfe und Aussage bei internen Untersuchungen verweigert werden könne. Bei der anvisierten Kooperation zwischen dem Unternehmen und der Ermittlungsbehörde sei praktisch besonders bedeutsam, dass eine Neuregelung eine einheitliche und transparente Verfahrenspraxis der Ermittlungsbehörden gewährleistet und die Eigenschaften der einzelnen Unternehmen sowie die Art und Intensität des Rechtsverstoßes angemessen berücksichtigt. Nur bei ausreichender Vorhersehbarkeit der Vorteile einer Kooperation könne die Geschäftsleitung sich für eine Verteidigungsstrategie entscheiden.

IT-Sicherheit

Nicht alle Firmen der mittelständisch geprägten **Maschinenbauindustrie** seien ausreichend auf Cyberattacken vorbereitet, gehe aus einer Umfrage des VDMA hervor, berichtet heise.de am 26. März. Demnach arbeite knapp die Hälfte der Unternehmen mit einem veralteten Schutz vor Angriffen aus dem Netz. Aus Sicht der Maschinenbauer seien Verwaltungsnetzwerke, zum Beispiel E-Mail-Accounts sowie die Produktions-IT besonders gefährdet. In die Haftung könnten die Unternehmen geraten, wenn sich Kriminelle bei der Attacke Zugang zu sensiblen Daten von Kunden oder personenbezogene Daten Dritter verschafften. Den Schaden durch Cyberattacken schätzten 60 Prozent der befragten Firmen auf 500.000 bis eine Million Euro. 88 Prozent der Befragten sei bislang noch nicht gegen Hackerangriffe versichert.

Peter Graß, GDV, und Thomas Packe, Riskpoint, ziehen in s+s report, Ausgabe 1-2018, S. 46/47, ein Resümee zu einem halben Jahr **GDV-Musterbedingungen für Cyberpolicen** („AVB Cyber"). Sie skizzieren die wesentlichen Inhalte einer Cyberrisiko-Versicherung nach diesem Konzept. Die unverbindlichen Musterbedingungen hätten sich als ein Ankerpunkt in der Diskussion um die Versicherung von Cyberrisiken etabliert. Ihr Aufbau erlaube es den Versicherungsnehmern und Maklern, die zuvor als potenziell gefährlich identifizierten Szenarien für das jeweilige Risiko an dem einzukaufenden Versicherungsschutz vorbeizuführen und Klarheit darüber zu erlangen, welche der identifizierten Cyberrisiken durch eine Cyberversicherung sinnvoll abgedeckt werden können.

IuK-Kriminalität

Wie die FAZ am 31. März meldet, hat der amerikanische Sportartikelhersteller Under Armour einen **Hackerangriff auf** seine **Kalorienzähler-App „MyFitnessPal"** veröffentlicht, der nach bisherigem Kenntnisstand etwa 150 Mio. Nutzerkonten betreffen soll. Das Unternehmen gehe davon aus, dass die Hacker Nutzernamen und E-Mail-Adressen sowie Passwörter erbeutet haben, aber keine sensibleren Informationen wie Kreditkartendaten. Nutzer der App sollten ihre Passwörter am besten sofort ändern.

Wie SecuPedia am 30. März meldet, hat iPass Inc., ein Anbieter weltweit verfügbarer mobiler Konnektivität, seinen **iPass Mobile Security Report 2018** veröffentlicht, aus dem hervorgehe, dass mehr als die Hälfte der befragten Unternehmen davon ausgehe, dass ihre „mobilen Mitarbeiter" in den letzten zwölf Monaten gehackt wurden oder dass es einen Sicherheitsvorfall auf deren mobilen Geräten gegeben habe. Insgesamt hätten 81 Prozent der Befragten angegeben, in den letzten zwölf Monaten Sicherheitsvorfälle im Zusammenhang mit Wi-Fi festgestellt zu haben, wobei Cafés/Coffeeshops (62 Prozent) als die Orte eingestuft worden seien, an denen solche Vorfälle am häufigsten aufgetreten waren, gefolgt von Flughäfen (60 Prozent), Hotels (52 Prozent), Bahnhöfen (30 Prozent), Messen (26 Prozent) und Flugzeugen (20 Prozent). Die Untersuchung sei von dem unabhängigen Marktforschungsunternehmen Vanson Bourne im Februar und März 2018 durchgeführt worden. Die Stichprobe habe 500 CIO- und IT-Entscheider aus den USA, Großbritannien, Deutschland und Frankreich umfasst.

Veko-online.de berichtet in der April-Ausgabe über die jährliche IT Security Risks-Studie von Kaspersky Lab 2017, bei der über 5.200 Entscheider aus der Wirtschaft in 29 Ländern zu IT-Sicherheitsthemen befragt wurden. Nach dieser Studie würden die **Kosten von DDoS-Attacken für Unternehmen** erheblich ansteigen. Sie beliefen sich pro Angriff auf KMU aktuell auf 123.000 Dollar, bei Großunternehmen sogar auf 2,3 Mio. Dollar. Dennoch verwende nur rund jedes fünfte Unternehmen eine spezielle Sicherheitslösung gegen DDoS-Attacken. Als Grund für fehlende Lösungen würden 20 Prozent die Kosten nennen, die durch die Risiken nicht aufgewogen würden. Sie seien aber vergleichsweise gering: bei KMU ca. 15.000 Dollar jährlich, bei Großunternehmen etwa 50.000 Dollar. DDoS-Botnetzbetreiber würden ihre Netzwerke für das Schürfen von Bitcoins, den Versand von Spam und politisch motivierte Sabotage nutzen. 71 Prozent der Botnetze, über die DDoS-Attacken gefahren werden, basierten auf Linux. Die längste DDoS-Attacke habe 146 Stunden angedauert.

Laut den Experten von Kaspersky-Lab wurden nach einem Bericht in der Ausgabe 4-2018 der Zeitschrift GIT, S. 72/73, 2017 insgesamt 2,7 Mio. Anwender von **schädlichen Minern** angegriffen. Das entspreche gegenüber dem Vorjahr einem Anstieg um fast 50 Prozent. Eine cyberkriminelle Bande verwende in ihrem Arsenal für die Infektion von Mining-Software erstmals Methoden der Prozess-Aushöhlung. Die Opfer würden zum Download und zur Installation von Adware verleitet, die einen versteckten Installer für Mining-Software in sich trage. Unternehmen empfehle Kaspersky-Lab die regelmäßige Durchführung von Sicherheits-Audits und die Installation von Sicherheitslösungen, möglichst auf allen Workstations und Servern. Die Lösungen müssten regelmäßig aktualisiert werden.

Krankenhaussicherheit

Veko-online.de befasst sich in der April-Ausgabe mit **intelligenten Sicherheitssystemen für Klinik und Pflege** gegen Feuer, Diebstahl und Gewalt. Mitarbeiter in Kliniken und Heimen hätten zu mehr als 56 Prozent verbale und zu 78 Prozent körperliche Angriffe erlebt. Zum Maßnahmenpaket zur Minderung dieser Angriffe gehörten geeignete Notruf- und Alarmierungssysteme mit akustischen Signalen zur Abschreckung, Videoüberwachung und Notruftaster sowie mobile Funksender für das Personal. Videobildanalysen trügen zum Schutz vor Diebstahl und zur Vermeidung von Unfällen bei, da sie Vorfälle automatisiert erkennen und blitzschnell informieren. Hohe Decken, Luftströmungen, Dämpfe oder extreme Temperaturen verhinderten bisweilen den Einsatz konventioneller Brandmelder und erforderten Sonderbrandmeldetechnik. Ansaugrauchmelder transportierten Luftproben über Ansaugleitungen zur Auswerteeinheit, sodass ein Anstieg der Rauchkonzentration sofort erkannt werden könne. In Patientenzimmern, Aufenthaltsräumen und Büros seien punktförmige automatische Brandmelder Standard. Sinnvoll für Bettenzimmer seien Melder, die in einem Raum die Kohlenmonoxid-Konzentration messen und schlafende Personen vor dem Erstickungstod bewahren. In punktförmige Brandmelder könnte Sprachalarmierung integriert werden. Für komplexe Objekte seien Sprachalarmierungsanlagen die bessere Wahl. Über ihr eigenes Lautsprechersystem sendeten sie gespeicherte oder aktuell eingesprochene Texte. Sie würden über Interfaces von Brandmeldesystemen direkt und intelligent gesteuert. Die Brandmeldezentrale kommuniziere mittels offener Schnittstellen mit externen und übergeordneten Systemen und übernehme die Steuerung der Gebäudetechnik. Eine ganzheitliche Lösung integriere alle Gewerke in einem System und binde vorhandene Fremdanlagen intelligent ein.

Kritische Infrastrukturen

Stromausfall legt Internetknoten in Frankfurt lahm, titelt die FAZ am 11. April. Durch den Internetknoten in Frankfurt fließen zu Hochzeiten mehr als 6 Terabit pro Sekunde, was etwa 60.000 DSL-Verbindungen mit 100 Megabit entspreche. Doch am 9. April abends habe der Knoten plötzlich „Schluckauf" gehabt, was 220 Kunden von De-Cix und noch viel mehr Internetnutzer merkten – und schuld sei ein Stromausfall gewesen. Zwar sei die Plattform in 21 Rechenzentren über die Stadt verteilt, doch ein bestimmter Teil der Infrastruktur stehe in einem Rechenzentrum des Anbieters Interxion. Im Rechenzentrum FRA-5, wo die De-Cix-Infrastruktur steht, seien nicht nur die normale Stromzufuhr, sondern auch die dann einspringenden Diesel-Stromaggregatoren ausgefallen. Vor allem betroffen sei das sogenannte Peering gewesen, das für das Zusammenschalten von Internet-Netzen zum Datenaustausch steht. Wie es zu dem Stromausfall kommen konnte, sei noch ungeklärt. Der 24-Stunden-Betrieb sei mehrfach abgesichert, mit doppelten Stromnetzen, Hunderten Batterien und als letzter Stufe mit Dieselgeneratoren, die bis zu drei Tage durchhalten könnten – in der Theorie.

Luftverkehrssicherheit

Unisys habe mit **Linesight** eine Software vorgestellt, die auf der Basis von Advanced Data Analytics und Machine Learning Sicherheitskontrollen im Personen- und Güterverkehr effizienter gestalten soll, heißt es auf lanline.de am 27. März. Die Lösung ermögliche es Zollbehörden oder der Sicherheitskontrolle am Flughafen, bei potenziellen Gefahrenquellen deutlich zielgerichteter einzugreifen und so letztlich Verzögerungen bei der Passagier- und Gepäckabfertigung zu minimieren. Dazu filtere sie aus einer großen Menge an Daten diejenigen Informationen heraus, die für die Sicherheitskontrolle relevant sind, und leite diese nahezu in Echtzeit an die entsprechenden Stellen weiter.

General Electric Security, die Sicherheitssparte des US-Konzerns, habe einen Scanner entwickelt, der es dem Sicherheitspersonal ermöglichen soll, verdächtige Gegenstände im Handgepäck aus verschiedenen Blickwinkeln zu betrachten. Das berichtet golem.de am 27. März. In dem Gerät mit der Bezeichnung CTX9800DSI seien unterschiedliche Produktlinien zusammengeführt worden. Es basiere auf Systemen für die Sprengstofferkennung. Diese Geräte, wie etwa der Vorgänger CTX9400, durchleuchten Gepäckstücke per Computertomografie und vergleichen die Eigenschaften der gescannten Gegenstände mit denen von Sprengstoffen. So sollen die Geräte automatisch erkennen, ob sich eine Bombe im Gepäck befindet. In das CTX9800 habe GE Security zusätzlich das **3-D-Bildgebungsverfahren Clarity** integriert, das ursprünglich von GE Healthcare für medizinische Anwendungen entwickelt worden sei. Clarity generiere aus den CT-Aufnahmen ein hochaufgelöstes 3-D-Bild. Das Sicherheitspersonal könne das Bild des Gepäckstückes in alle möglichen Richtungen drehen und so dessen Inhalt aus verschiedenen Blickwinkeln betrachten.

Maschinensicherheit

In der Zeitschrift GIT, Ausgabe 3-2018, S. 97, erklärt Torsten Singer, Georg Schlegel GmbH & Co. KG, wie ein herkömmlicher **Not-Halt** und wie die Selbstüberwachung funktionieren. Es sollte immer beachtet werden, dass die Not-Halt-Funktion eine ergänzende Schutzmaßnahme ist und nicht als Ersatz für Schutzmaßnahmen oder Sicherheitsfunktionen angewendet werden darf. Die Selbstüberwachung erfolge über einen zusätzlichen Schließerkontakt. Gehe die Verbindung zwischen Pilzknopf, der in einer Notsituation betätigt wird, und dem Kontaktgeber verloren, dann verhalte sich das Not-Halt-Gerät ähnlich einem Betätigen der Not-Halt-Taste und löse das Signal zum Anhalten der Anlage aus.

Benjamin Heimpel und Alexander Wiesler, Sick AG, stellen in der Ausgabe 3-2018 der Zeitschrift GIT, S. 100–102, das Sicherheitssystem **Safeguard Detector** als Komplettlösung für OEMs (Original Equipment Manufacter) vor, eine komplette Sicherheitslösung, die sich sehr gut in Verpackungsmaschinen einsetzen lasse, beispielsweise zur Überwachung von Materialzuführungen an Karton-Magazinen. Die Strategie einer produktionsgeführten Sicherheitstechnik verhindere das versehentliche Eingreifen in den Sicherheitsbereich. Hinter diesem Konzept verberge sich gleich ein doppelter Nutzen: mehr Tempo in der Produktion und mehr Raumgewinn durch kleinere Schutzzonen.

Jens Rothenburg, Euchner GmbH & Co. KG, erklärt in GIT, Ausgabe 3-2018, S. 104/105, die Faktoren, die das Risiko an einer Gefährdungsstelle in einer Maschine bestimmen, und die Risikoeinschätzung mit der EN ISO 13849-1.

Die **Beurteilung des Risikos** erfolge nach den Faktoren „Schwere der Verletzung", „Häufigkeit und Dauer der Exposition" und „Möglichkeit zur Vermeidung".

Carsten Hippler, Pfannenberg, stellt in GIT, Ausgabe 3-2018, S. 106/107, **Signalgeber für raue Umgebungsbedingungen** vor. In vielen Anwendungen in der Automobil-, Verpackungs-, Schüttgut- oder Bauindustrie sowie im Maschinenbau würden Signalgeräte extrem beansprucht. Um die Zertifizierung durch den Germanischen Lloyd (GL) zu erlangen, werde deren Leistungsfähigkeit in rauer Umgebung, bei Anwendungen im Außenbereich und unter schwersten Industriebedingungen geprüft. Vibrations-, Erschütterungs- und Stoßfestigkeit seien hierbei entscheidende Kriterien. Durch Verwendung flexibler Netzteile eigneten sich die GL-zertifizierten Signalgeräte besonders für Anwendungen mit „Energieversorgungsschwankungen". Verwindungssteife Kunststoffgehäuse mit Schlagfestigkeit IK08 und hohe Schutzarten wie IP66 oder IP67 gewährleisteten höchste Robustheit und Stoßfestigkeit. Dank der hohen IP-Schutzarten eigneten sich die Geräte auch für anspruchsvolle Anwendungen, wo Rohstoffe zerkleinert werden, wo in der Verarbeitung Staub, Dunst und Dämpfe entstehen und Arbeits- und Produktionsbereiche regelmäßig mit Wasser gereinigt werden. Die GL-zertifizierten Signalgeräte in Schutzart IP66 und IP67 seien absolut staubdicht und widerstünden auch starkem Strahlwasser und Überflutung.

Organisierte Kriminalität

Tschetschenische Banden breiten sich nach einem Bericht in der FAZ am 12. März in der organisierten Kriminalität in Deutschland immer stärker aus. Sie seien nicht mehr nur als „Söldner" für andere kriminelle Gruppierungen tätig, sondern übernähmen ganze Geschäftsfelder, etwa im Rauschgifthandel, aber auch bei Raub, Diebstahl und Fälschungen. Insgesamt hätten die Sicherheitsbehörden 200 bis 250 Personen aus Tschetschenien und dem Nordkaukasus im Blick, denen sie eine gewichtige Rolle in der OK in Deutschland zuschreiben. Mit Sorge sähen die Behörden, dass Tschetschenen ihre Gewinne aus kriminellen Geschäften zunehmend in legale Unternehmen investieren. Sie beobachten persönliche Kontakte und enge finanzielle Beziehungen zwischen tschetschenischen Kriminellen in Deutschland und dem Präsidenten der russischen Teilrepublik, Ramsan Kadyrow, in Grosny.

Die FAZ befasst sich am 27. März mit einem Strafverfahren gegen acht ehemalige Mitglieder der türkisch-nationalistischen **Rocker-Gang „Osmanen Germania BC".** Vorgeworfen werde den Beschuldigten gefährliche Körperverletzung, Zuhälterei, Unterstützung von Zwangsprostitution, versuchter Mord und versuchter Totschlag. Fünf der acht Angeklagten hätten die türkische Staatsbürgerschaft. Nicht das Strafverfahren, aber das Auftreten der nationalistischen Rocker-Gang in Deutschland habe eine enorme politische Dimension. Ermittler hätten schon lange den Verdacht gehabt, dass Funktionäre von Erdogans AKP die Rocker als Schläger auf deutschem Boden einsetzen. Sie hätten herausgefunden, dass es zwischen den Osmanen und der AKP-Auslandsorganisation UETD Verbindungen gegeben haben müsse. Bekannt geworden sei, dass die türkischen Osmanen-Mitglieder aus Stuttgart in der Hochphase der Flüchtlingskrise als Wachmänner gutes Geld verdienten. Sie sollen Subunternehmer von Subunternehmen gewesen sein.

Martin Vogler, Senstar, beschreibt in der Ausgabe 4-2018 der Zeitschrift GIT, S. 54/55, **sechs Schritte zur effektiven Zaunsicherung**: Grundsätzliche Überlegungen und Anforderungen; Einschätzung der Sicherheitslücken und des Risikos; Umfang und Anzahl der benötigten Materialien; Montage und Installation der Hardware; Einstellung und Funktionstest; Festlegung der Alarmausgänge und Inbetriebnahme. Natürlich gehöre zur erfolgreichen Projektrealisierung auch die Überlegung und letztendlich die Entscheidung, was im Falle eines Ereignisses überhaupt passieren soll und welche Mittel und Ressourcen zur Verfügung stehen, um den unerwünschten Zutritt zu verhindern.

Produktpiraterie

Lettische Zollbeamte haben im Hafen von Riga gut 17.000 Paar **gefälschte Markenturnschuhe** beschlagnahmt, meldet die FAZ am 27. März. Die in zwei Containern transportierte Ware stamme aus China und sei für einen Empfänger in Russland bestimmt gewesen. Es handele sich um Plagiate von Modellen eines amerikanischen Sportartikelherstellers.

Schließsysteme

Für den Einstieg in die **Welt der digitalen Schließsysteme** gebe es das Home & Office Set von CES (C. Ed. Schulte in der Ausgabe 3-2018 der Zeitschrift GIT, S. 56/57). Es bestehe aus einem Elektronik-Zylinder („Omega Flex") mit Elektronik-Schlüsseln für eine vierköpfige Familie und dem elektronischen Reserveschlüssel für den Nachbarn. Über ein Zusatz-Funkmodul könnten die Elektronik-Zylinder mit einer Alarmanlage kombiniert werden. Die Komponenten des Systems seien so gestaltet, dass sowohl Funktions- als auch Systemerweiterungen ohne Austausch der Hardware möglich sind. Alle Omega-Flex-Produkte seien mit einem internen Funkbaustein ausgestattet und grundsätzlich zur Integration in Smart-Home-Systeme verschiedener Hersteller geeignet und vorgerichtet. Der Autor behandelt ferner die cloudbasierte Schlüssel- und Schlossverwaltung, Softwaremodule für die häusliche Pflege und die Ausgabe digitaler Schlüssel für Ferienhäuser**.**

Fünf Gründe für IP-basierte Zutrittskontrollsysteme beschreibt Axis Communications in der Zeitschrift GIT, Ausgabe 3-2018, S. 58: Power over Ethernet; Fernwartung; Hardware-Migrationspfade; Software-Migrationspfade; integrierte Software.

Das Gebäudemanagement für eine Vielzahl städtischer Gebäude (in der französischen Gemeinde Vaureal) stellt die Paxton GmbH in GIT, Ausgabe 3-2018, S. 60/61, vor. Sämtliche Objekte seien mit dem **Zutrittssteuerungssystem Net2** von Paxton gesichert. Dabei ist jedes Einzelne in das Gesamtsystem eingebunden, könne aber auch unabhängig davon gesteuert werden. Dadurch könne der IT-Manager jede Einrichtung individuell verwalten, sodass die dort auftauchenden besonderen Anforderungen und Bedürfnisse berücksichtigt werden können. Seit Einführung von Net2 brauche man für den Zugang zu den kommunalen Gebäuden keine Schlüssel mehr.

Sicherheitsgewerbe

Aus- und Weiterbildung im Sicherheitsgewerbe thematisiert Gabriele Biesing, Securitas Holding GmbH, in der Ausgabe 1-2018 der Zeitschrift DSD, S. 24/25. Es werde zunehmend anspruchsvoller, geeignetes Personal und Nachwuchs für die Führungskräfte zu finden. In Zeiten des demografischen Wandels gelte es, das Bestandspersonal weiter zu qualifizieren und in dieses zu investieren. Verschiedenste Personalentwicklungskonzepte müssten erprobt werden. Das Sicherheitsgewerbe müsse die Arbeitswelt attraktiver gestalten und den Nachwuchs aus eigener Überzeugung entwickeln und optimal fördern. Nur mit „Klasse statt Masse" werde es gelingen, zukunftsfähig zu sein.

Frank Schimmel, Fachschule KG Protektor GmbH & Co., stellt in der Ausgabe 1-2018 der Zeitschrift DSD, S. 26/27, die „**Exzellenzinitiative"** – ein Pilotprojekt der BDSW-Landesgruppe Hamburg zur Verbesserung der Ausbildungsqualität und Situation der Auszubildenden, vor. Sie sehe einen Ombudsmann als niedrigschwellige Ansprechstelle bzw. als Gesprächsangebot für alle Auszubildenden an der Gewerbeschule vor. Der zweite Teil der Initiative befasse sich mit Exzellenzausbildungsbetrieben (EAB). Ein EAB verpflichte sich zu Standards, die der Autor im Einzelnen beschreibt. Ein EAB unterwerfe sich einer freiwilligen Selbstkontrolle. Die Überprüfung werde von zwei Mitgliedern eines Exzellenzprüfungsausschusses in regelmäßigen Abständen durchgeführt.

In einer Pressemitteilung vom 5. April erklärt der BDSW zu dem Berufsbildungsbericht der Bundesregierung, nach dem **50,6 Prozent aller Ausbildungsverträge im Sicherheitsgewerbe vorzeitig beendet** werden, die hohe Abbrecherquote habe den Verband leider nicht überrascht. Dazu trügen vor allem viele kleine Unternehmen bei, die ihre Auszubildenden regelrecht ausbeuteten. „Wenn ein 10-Mann-Sicherheitsunternehmen genauso viele Auszubildende habe, könne keine seriöse Ausbildung stattfinden. Die Industrie- und Handelskammern seien nun gefordert, den „schwarzen Schafen" unverzüglich die Ausbildereignung zu entziehen.

Sicherheitsmarkt

Der Umsatz der elektronischen Sicherungstechnik sei 2017 um 5,1 Prozent gestiegen, meldet s+s report in der Ausgabe 1-2018, S. 6, aufgrund von Schätzungen des BHE. Eine Steigerung von 7 Prozent werde für die Videoüberwachungstechnik prognostiziert. Für die Brandmeldetechnik würde ein Anstieg von 5,5 Prozent angenommen, für Einbruchmelder 4,8 Prozent, für die Zutrittssteuerung von 2 Prozent, für Sprachalarmsysteme und sonstige Gewerke 2,9 Prozent.

Sicherheitstechnik

Seit April 2017 legt die **EN 16763** Mindestanforderungen an Dienstleistungen von Unternehmen im Bereich Planung, Projektierung, Installation und Übergabe, Instandhaltung und Instandsetzung von Sicherheitsanlagen fest. Darauf weist s+s report in der Ausgabe 1-2018, S. 60, hin. Sie würden für jeden Betrieb aus der Branche gelten, unabhängig von seiner Größe. Die Forderungen beinhalteten u. a. spezifische Informationsprozesse zur Anlagendokumentation, das Vorhalten wichtiger Betriebsmittel, ein Qualitätsmanagementsystem und angemessene Aus- und Weiterbildung.

Spionage

Das Bundesamt für Verfassungsschutz warne vor **Wirtschaftsspionage durch Unternehmenskäufe,** meldet die FAZ am 12. April. Es gebe auch formal legale Möglichkeiten, um an Informationen zu kommen, habe Hans-Georg Maaßen, Präsident des BfV, am 11. April erklärt. „Man braucht keinen Spionageangriff mehr durchzuführen …, wenn man das Unternehmen aufkaufen kann." Maaßen habe besonders auf chinesische Konzerne hingewiesen.

Steuerhinterziehung

EU verschärft den Kampf gegen Steuerhinterziehung meldet die FAZ am 14. März. Künftig sollen nach einem Beschluss der EU-Finanzminister am 13. März auch Steuerberater, Anwälte, Wirtschaftsprüfer und Bankberater in diesen Kampf einbezogen werden. Die Berufsgruppen sollen verpflichtet werden, alle „potenziell aggressiven" Steuersparmodelle zu Gunsten ihrer Kunden sowie deren Namen an ihre nationalen Behörden zu melden. Diese sollen die Informationen anschließend in den grenzüberschreitenden Informationsaustausch der Behörden einbeziehen. Die Meldepflicht gelte für Steuersparmodelle, mit denen Geld in vermutete Steueroasen verschoben wird. Die EU-Staaten hätten nun bis Ende 2019 Zeit, die Vorgaben in nationales Recht zu gießen. Von Mitte 2020 an sollten die neuen Regelungen in der ganzen EU gelten.

Terrorismus

Hessens Polizei testet, wie die FAZ am 9. April berichtet, eine Analysesoftware des amerikanischen Anbieters Palantir Technologies zur Bekämpfung des islamistischen Terrorismus sowie der schweren und organisierten Kriminalität. Der Einsatz diene dazu, unterschiedliches Datenmaterial zusammenzuführen und auszuwerten. Dadurch könnten Gefahren rechtzeitiger erkannt und Ermittlungen zu einschlägigen Straftaten zielgerichteter und effizienter geführt werden. **Palantir Gotham** integriere strukturierte und unstrukturierte Daten und stelle sowohl Such- und Ermittlungsfunktionen als auch Wissensmanagement und sichere Zusammenarbeit unter verschiedenen Parteien zur Verfügung (Wikipedia).

Veranstaltungssicherheit

Sabine Funk, IBIT GmbH, befasst sich in der Ausgabe 1-2018 der Zeitschrift DSD, S. 4/5, mit der **Organisation von Ein- und Ausgangsbereichen** von Veranstaltungen: mit Faktoren für die Gestaltung von Einlassbereichen (Zu- und Ablauf; Warte- und Entlastungsflächen; mit infrastruktureller Gestaltung; Information & Kommunikation sowie Organisation), mit Zugangsflächen für öffentliche Veranstaltungen, mit Ausgängen und Auslassflächen sowie mit einer Betrachtung der Zu- und Abgangsbereiche unter dem Aspekt einer verstärkten terroristischen Bedrohung.

Die Sicherheit von Massenveranstaltungen in Zeiten realer terroristischer Bedrohungen thematisiert Dr. Harald Olschok, BDSW, in der Ausgabe 1-2018 von DSD. Er verweist auf die vom BDSW erarbeiteten Eckpunkte zur **Verbesserung des Veranstaltungsschutzes** insbesondere in Fußballstadien, plädiert für eine normative Abgrenzung von Ordnungs- und Sicherheitskräften und für eine Qualifizierung für Veranstaltungsordnungsdienste. Etablierte VDO-Dienstleister mahnten schon seit Jahren, dass Veranstaltungsdienstleistungen künftig nicht weiter auf Sicherheitstätigkeiten gem. § 34 a GewO reduziert werden dürfen. Sie hätten deshalb eigene Qualifizierungsmaßnahmen entwickelt, ein Schulungs- und Weiterbildungskonzept als Alternative zu § 34 a GewO in Qualifizierung und Zertifizierung von Mitarbeitern. Die Umsetzung werde vom AK VOD vorangetrieben. Eine entsprechende Online-Plattform sei erarbeitet worden. Auch das

Sicherheitsforschungsprogramm des BMBF enthalte wichtige Beiträge zum Schutz von Veranstaltungen: Im Projekt „BaSiGo" seien wichtige Bausteine für die Sicherheit von Großveranstaltungen erarbeitet worden. Das Projekt ProVOD zur Professionalisierung des Veranstaltungsordnungsdienstes laufe seit 2016. Benötigt würden weiterhin spezialgesetzliche Regelungen für private Sicherheitsdienste und die Ausbildung der bei Veranstaltungen eingesetzten Sicherheitskräfte.

Dr. Stephan Gundel, Gruner Gruppe, skizziert in der Ausgabe 1-2018 der Fachzeitschrift DSD, S. 9–11, **Entwicklungen und Trends** in der Veranstaltungssicherheit. Gundel listet Teilaspekte auf, die bei einem veranstaltungsspezifischen Sicherheitskonzept zu berücksichtigen seien. Für jede Versammlungsstätte bzw. Veranstaltung müsse eine Art Basissicherheit effizient und mit verhältnismäßigem Aufwand gewährleistet werden, die sich auf die anerkannten Regeln der Technik und die aktuellen Erfahrungen stützt. Ergänzend oder abweichend seien spezifische Maßnahmen zu treffen, die sich aus den besonderen Eigenschaften und Bedrohungsbildern des Veranstaltungstyps ergeben. Als Trends führt der Autor an: stark ausdifferenzierte Veranstaltungskonzepte; zunehmende Bedeutung klarer Organisation und Planung; moderne technische Hilfsmittel, die die Sicherheitsmaßnahmen erheblich vereinfachen; leistungsfähige Tools zur Bearbeitung von Checklisten, zur Erstellung von Plänen, Durchführung von Evakuierungs- und Personenstromsimulationen bis hin zu simulationsbasierten Entrauchungsnachweisen; Kommunikation und Information als kritische Erfolgsfaktoren.

Videoüberwachung

Über kritische Sicherheitslücken in der Cloud-Anbindung von **Samsung IP-Kameras** berichtet heise.de am 12. März. Mit dem Internet verbundene Kamera-Systeme enthielten immer wieder horrende Sicherheitslücken. Jetzt hätten Forscher der Firma Kaspersky Schwachstellen in einem weit verbreiteten Modell gefunden, das in Europa mit Samsung-Branding verkauft wird. Die Kamera SNH-V6410PN/PNW könne von Angreifern komplett übernommen werden, wenn sie aus dem Internet erreichbar ist. Um den Angriff auszuführen, bräuchten Angreifer allerdings die Seriennummer der Kamera, die sich aber mit relativ wenig Aufwand herausfinden lasse. Die Kaspersky-Forscher hätten weltweit fast 2.000 dieser Kameras gefunden. Die Dunkelziffer dürfte noch weit höher liegen, da wohl alle Geräte betroffen sind, die an den Cloud-Dienst des Herstellers angebunden sind. Habe ein Angreifer eine der Kameras im Web aufgespürt, könne er Video und Ton des Gerätes in Echtzeit abgreifen. Er könne auch selbst Töne über den eingebauten Lautsprecher abspielen. Die Sicherheitslücken der Kamera lägen in ihrer unsicheren Anbindung an den Cloud-Dienst des Herstellers begründet. Zusammen mit Unsicherheiten der mit PHP-Web-API auf den Kameras und beim Erstellen von Passwörtern bei der Cloud-Administration ergäben sich so eine große Anzahl von Angriffsmöglichkeiten bis hin zum Root-Zugriff auf das Linux.

Edge oder Server? Fragt Maximilian Busse, Moog Pieper, in der Ausgabe 4-2018 von GIT, S. 32/33. Intelligente Software – sogenannte Edge-basierte Videoanalyse – sei der Schlüssel für Analysen auf der Kamera. Dank leistungsfähiger Chips auf den Kameras ließen sich zahlreiche Kamerafunktionen in die Geräte selber integrieren. Unternehmen sparten Kosten, denn statt High Performance-Servern ließen sich kleinere preiswertere Modelle nutzen, die meist niedrigere Lizenzgebühren haben, weniger Strom- und Wartungskosten verursachen und bei zusätzlichen Kameras einfacher erweitert werden können. Edge-basierte Videoanalysen benötigten weniger Speicherkapazität. Darüber hinaus bestehe die Möglichkeit, dass ausschließlich relevantes Bildmaterial gespeichert wird. Edge-basierte Lösungen könnten grundsätzlich in allen Branchen eingesetzt werden und würden derzeit vor allem im Einzelhandel und ÖPNV Verwendung finden. Der Autor zeigt aber auch Grenzen der „On the Edge-Videoanalyse" auf. Beispielsweise reiche die Funktionalität und Leistungsfähigkeit noch nicht für die Nummernschilderkennung und die Gesichtserkennung aus.

Videoanalyse für intelligentes Verkehrsmanagement behandelt GIT in der Ausgabe 4-2018, S. 34/35. Hanwha Techwin und FF Group hätten ein umfangreiches Bundle an ANPR (automatic number plate recognition)-Lösungen für intelligentes Verkehrsmanagement eingeführt. Sie eigneten sich besonders für die Zufahrtskontrolle auf Parkplätzen für Geschäftsbereiche bis hin zu flächendeckenden Systemen für Städte, mit denen die lokalen Behörden die Anwohner beschützen sowie illegal geparkte Fahrzeuge und andere Verkehrsdelikte erkennen können. Anwender könnten bis zu 2.000 Kennzeichen in einer Freigabe- und Sperrliste definieren, um automatisch den Zugang zu einem Standort bzw. einem Parkplatz zu autorisieren bzw. zu verbieten, wobei jede Kamera bis zu drei Fahrbahnen überwachen könne.

Beschrieben werden in dem Fachbeitrag die Server-Lösung für die Kennzeichenerkennung und Cloud-Lösungen für mehrere Standorte.

Ingo Take, LunaHD, stellt in der Fachzeitschrift GIT, Ausgabe 4-2018. S. 36/37, die Frage: „Ist IP immer die erste Wahl?" Auf dem Überwachungsmarkt tummelten sich mittlerweile viele Alternativen zur IP-Technik: HD-CVI, HD-TVO oder AHD – kurz beschrieben als „HD über Koax". Der Hauptunterschied liege in der Übertragung der Bilder: **Netzwerkkabel versus Koaxialkabel**. Die HD-Videoüberwachung via Koax schlage zusammen mit dem richtigen Rekorder eine Brücke zwischen der analogen und der digitalen Welt. In einem weiteren Fachbeitrag (S. 42/43) wird ebenfalls dargestellt, wie sich mit der HDCVI-IoT-Technologie IoT-Anwendungen einfach umsetzen ließen. HDCVI 4.0 vergrößere den Anwendungsbereich von HD-Analog und diene dem Schutz der Investitionen von HDCVI-Kunden. Als eine Schlüsselkomponente von HDCVI 4.0 vereine HDCVI-IoT die Vorteile der Koaxialübertragung von HD-Videos und des Internet der Dinge. Informationserfassung, Video und HDCVI-IoT würden für eine umfassende Überwachung integriert. Sie funktioniere als Auge, als Alarmauslöser und sogar als Ersthelfer.

Holger Schmitz, Eizo, stellt in der Ausgabe 4-2018 der Zeitschrift GIT, S. 40/41, einen IP-**Decoder-Monitor mit integrierter Bildverbesserung** für den computerlosen Anschluss von Sicherheits- und Überwachungskameras vor. Mit der „Low Light Correction" ließen sich dunkle Bereiche besser darstellen. Die Web-API des Monitors unterstütze die Integration in das lokale Videomanagementsystem. Die Funktionseinstellung Outline Enhancer analysiere angezeigte Inhalte und korrigiere unscharfe Bereiche. Eine Overdrive-Schaltung verkürze den Grau/Grau-Wechsel auf 8 ms, wodurch bei sich schnell bewegenden Aufnahmen deutlich weniger Wischeffekte und Unschärfen aufträten. Bilder würden pixelgenau in bildschirmfüllender Full-HD-Auflösung dargestellt (1.920 x 1.080).

„Weniger Fehlalarme dank Deep Learning" verspricht ein Fachbeitrag in der Ausgabe 4-2018 von GIT, S. 56–58. In den letzten zwei Jahren habe die Technologie unter anderem im Bereich Spracherkennung, Interpretation von Bildern und sprachaktivierte Übersetzung enorme Fortschritte gemacht. So habe sie im Bereich der Gesichtserkennung und Bildklassifizierung sogar menschliche Fähigkeiten übertroffen. Statt manueller Eingriffe extrahiere ein Computer selbstständig die entsprechenden Merkmale. Auf diese Weise könne das System möglichst viele Merkmale des Ziels extrahieren. Zu den unmittelbaren Vorteilen der Deep-Learning-Algorithmen zähle eine hohe Genauigkeit bei der Mustererkennung, eine sehr hohe Unempfindlichkeit gegenüber Störungen sowie die Fähigkeit, tausende Merkmale zu erkennen und zu klassifizieren. Mit Hilfe einer Reihe von Experimenten habe die Erkennungsgenauigkeit der Lösungen mit dem Deep-Learning-Algorithmus um 38 Prozent verbessert werden können.

Wohnungseinbruch

Dr. Maike Meyer, LKA Nordrhein-Westfalen, vermittelt in der Ausgabe 1-2018 von s+s report, S. 42–45, Erkenntnisse aus dem **Forschungsprojekt Wohnungseinbruchdiebstahl** des LKA, das auf einer quantitativen Analyse von rund 7.500 staatsanwaltschaftlichen Ermittlungsakten in NRW aus den Jahren 2011 und 2012 beruht. Die Darlegungen beziehen sich nur auf ungeklärte Taten. Gemietete Tatobjekte seien schlechter mittels mechanischer Zusatzsicherungen gesichert als Eigentumsobjekte. Bei Mietobjekten sei in 10,1 Prozent von 721 Fällen eine Zusatzsicherung vorhanden gewesen, bei Eigentumsobjekten hingegen in 26,4 Prozent von 609 Fällen. Das Aufhebeln von Türen und Fenstern sei mit Abstand die häufigste Zugangsart zum Tatobjekt. In 82 Prozent der Fälle habe die Methode Anwendung gefunden. In 30,6 Prozent der Fälle seien die Tatverdächtigen beim Eindringen gescheitert. In 38,5 Prozent der Fälle seien die Täter an mechanischen Sicherheitseinrichtungen gescheitert, in 23,6 Prozent wegen einer Störung am Tatort, zumeist durch in der Wohnung anwesende Personen. Der Versuchsanteil, bei denen der Täter nicht in das Objekt gelangte, sei bei den Objekten mit Zusatzsicherung deutlich höher (79,8 Prozent) als bei den Objekten ohne zusätzliche Sicherung (68,1 Prozent). In 44,3 Prozent der Fälle seien Wohnungen, in 23,5 Prozent Häuser wiederholt Einbruchstatort gewesen.

Die FAZ weist am 11. April darauf hin, dass sich die **Zahl** der registrierten Wohnungseinbrüche in Deutschland 2017 **um mehr als ein Fünftel vermindert** hat. Die Polizei habe insgesamt 116.540 versuchte und vollendete Wohnungseinbrüche erfasst.

Zutrittskontrolle

Ernst Westerhoff, Axis Communications, stellt in der Ausgabe 4-2018 der Fachzeitschrift GIT, S. 20/21, die **nächste Stufe der digitalen Transformation** vor. Als Teil eines IoT (Internet of Things)-Systems könnten Netzwerk-Türstationen mit einem äußerst komplexen und hochwertigen Sicherheitsnetzwerk verbunden werden. Gleichzeitig würden aussagekräftige Business-Intelligence-Daten gesammelt und sicher an Smartphones oder Server gesendet. Die Vorteile von IoT und vernetzten Sicherheitssystemen zeige das Beispiel eines Parkplatzes, auf dem verschiedene Technologien über ein Netzwerk zusammenarbeiten und so die Zutrittskontrolle sichern. Die Förderung offener Systeme zwischen Hardware, Software und Anwendungstechnologien sowie Produkten berge spürbare Vorteile. Organisationen wie ONViF (Open Network Video Interface Forum), die sich für standardisierte Netzwerkprotokolle einsetzen, leiteten eine neue Ära der Zusammenarbeit in der Sicherheitsbranche ein. Dies bilde zusammen mit der Priorisierung von Cybersecurity die Grundlage für eine immer stärker vernetzte Welt.

Als **„funktionellen Quantensprung"** bezeichnet GIT in der Ausgabe 4-2018, S. 46–48, eine kartenbasierte und virtuelle Zutrittslösung. Erläutert wird der Systemwechsel von einer Offline-Anlage zur virtuell vernetzten Lösung. Einerseits könnten die Verantwortlichen nunmehr Zutrittsrechte vergeben oder ändern, ohne jede betroffene Tür aufsuchen zu müssen. Außerdem erlaube die Software die Bildung von Zutrittsgruppen, wodurch die Technik den Mitarbeitern nicht alle Türen und Zutrittspunkte einzeln zuweisen müsse. Technologisch basiere die Zutrittslösung auf dem Salto Virtual Network (SVN) mit patentierter Schreib/Lese-Funktionalität und verschlüsselter Datenübertragung. Im SVN würden die Informationen zu den Schließberechtigungen auf dem Identmedium gespeichert, wodurch eine Verkabelung der elektronischen Beschläge und Zylinder entfalle. Als Identifikationstechnologie fungiere Mifare DESFire EV1.

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

www.securitas.de/focus

Kontakt

Securitas Holding GmbH
Redaktion Focus on Security
Potsdamer Straße 88
10785 Berlin

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

E-Mail: info@securitas.de