FOCUS ON SECURITY

AUSGABE 03, MÄRZ 2018

SECURITAS

Inhaltsverzeichnis

Bahnsicherheit

Die Zahl der Übergriffe auf Bahn**-Mitarbeiter** ist 2017 abermals gestiegen, meldet die FAZ am 21. Februar. Es seien 2.550 Fälle von Körperverletzung gemeldet worden, 7,4 Prozent mehr als 2016. Meist seien Sicherheitskräfte angegriffen worden, oft in Zusammenhang mit Fußballspielen, Volksfesten und anderen Großveranstaltungen. Der Prävention dienten Schulungen für Konfliktfälle und Body-Cams.

Biometrie

Die biometrische Zutrittskontrolle im Stadion thematisiert die Zeitschrift PROTECTOR in der Ausgabe 3-2018, S. 30/31. Vorgestellt wird die biometrische Identifizierungslösung „BioSec LifePass". Im Ticketverkaufsbüro würden die biometrischen Profile (Handvenenmuster beider Hände) der Besucher angelegt und in einer zentralen und gesicherten Datenbank gespeichert. Für den Zutritt halte der Besucher seine Fan-Karte an das RFID-Lesegerät. Anhand der Mitglieds-ID überprüfe das System die folgenden Informationen: Besitzt die Person ein gültiges Ticket? Falls ja, befindet sich die Person auch am richtigen Eingang? Im Gegensatz zu anderen biometrischen Technologien wie der Gesichtserkennung bestehe keine Möglichkeit, den **Handvenenscanner** zu täuschen. Die BioSec-LifePass-Lösung basiere auf der PalmSecure-Technologie von Fujitsu. Mit Nahinfrarotlicht scanne PalmSecure das Muster des sauerstoffarmen Bluts, das in den Venen fließt. Ein speziell von Fujitsu entwickelter Algorithmus erstelle anhand dieser Daten dann ein individuelles biometrisches Muster.

Blockchain

Die Anwendung der Blockchain-Technologie beschreibt Hendrick Lehmann in der Ausgabe 3-2018 von PROTECTOR, S. 20–22. Er geht insbesondere auf die Funktionsweise ein, der auf viele Teilnehmer verteilten Datenstruktur, die für alle gleichermaßen einsehbar ist. Die Dezentralität der Blockchain sei ein Aspekt, der sie in den Augen vieler **sicherer** mache **als zentral verwaltete Systeme**. Die Blöcke würden von allen Teilnehmern gleichermaßen verwaltet, was das System redundant und ausfallsicher mache. Ferner gebe es damit keine zentrale, angreifbare Stelle. Auch die Art der verwendeten asymmetrischen Verschlüsselungstechnologien gelte als weitgehend sicher. Eine rückwirkende Veränderung der Hashwerte sei bislang mit vertretbarem Aufwand nicht möglich, weshalb die Blockchain unveränderlich sei und damit als besonders revisionssicher gelte. Trotz der starken kryptografischen Sicherheit sei die Blockchain-Technologie nicht gänzlich frei von Risiken und Problemen. Zu letzteren gehörten etwa die notwendige Rechenleistung für das Mining und der damit verbundene Zeitaufwand. Da die Validierung der Transaktionen auf Konsens im Netzwerk beruhe, könne ein Angreifer Transaktionen in einem Block verändern, wenn er mehr als 50 Prozent der Rechenleistung kontrolliert und den veränderten Wert erneut in den „Proof of Work"(PoW)-Kreislauf bringt.

Brandschutz

Dipl.-Ing. Matthias Siemon, Gruner AG, befasst sich in der Ausgabe 1-2018 der Fachzeitschrift Sicherheitsforum, S. 14–17, mit **Ingenieurmethoden im Brandschutz**. Zu ihnen würden üblicherweise gezählt: Brand- und Entrauchungssimulationen, Heißbemessung/Naturbrandverfahren, Evakuierungsberechnungen und Warmrauchversuche. Ihre Anwendung habe grundsätzlich in Kombination mit einem ganzheitlichen Brandschutzkonzept zu erfolgen. Nachweise auf Grundlage von Ingenieurmethoden würden im Regelfall angewendet, wenn präskriptive Anforderungen der entsprechenden Brandschutzvorschriften nicht eingehalten werden können. Die häufigsten Gründe seien den Brandschutzanforderungen widersprechende Nutzerbedürfnisse, architektonische Anforderungen, Randbedingungen einer baulichen Situation im Bestandsbau oder denkmalpflegerische Aspekte. Der Autor behandelt in dem Fachbeitrag im Einzelnen die vier Anwendungsbereiche. Aktuelle Entwicklungen wie Building Information Modeling (BIM) führten dazu, dass der Modellierungsaufwand für die numerischen Simulationsmodelle stetig sinkt. Die weit über die dreidimensionale Planung und Kollisionsprüfung hinausgehenden Möglichkeiten von BIM böten auch den Ingenieurmethoden im Brandschutz ein hohes Potenzial an Steigerung von Qualität und Effizienz.

BCM

Security insight befasst sich in der Ausgabe 1-2018, S. 22–23, mit Business Continuity Management. Schwerpunkte bildeten die Definition, welche Zwischenfälle für das Unternehmen die stärksten negativen Auswirkungen haben, das Ordnen möglicher Zwischenfälle nach Prioritäten und das Bestimmen der zu ergreifenden Maßnahmen. Mit der Erweiterung des Managementsystems um den Aspekt Gesundheit werde eine vitale Unternehmenskultur gefördert, die sich deutlich auf ein positives Image und den Unternehmenserfolg auswirke. Nach Einführung des BCM sei die erfolgreiche Zertifizierung nach ISO 9001 die ideale Grundlage für den Aufbau von Business Continuity. Die Definition der Unternehmensprozesse sei die Basis, um Risiken zu identifizieren. Das vereinfache die Definition von Kernprozessen – ein Schlüsselfaktor für den Aufbau eines BCM.

Datenschutz

Richard Werner, Trend Micro, behandelt in der Februar-Ausgabe des Behörden Spiegel den **„Stand der Technik" in der IT- Sicherheit**. Die DSGVO definiere den Begriff mit Absicht nicht genauer, denn die Verordnung sei längerfristig ausgelegt und die Entwicklung in der IT sei sehr schnelllebig. Sicherheit müsse auf verschiedenen Ebenen angegangen werden, wobei zum Schutz der Daten an deren Speicherort mehrere – traditionelle wie neue Sicherheitstechniken gleichzeitig angewendet werden. Nur so lasse sich jedem Angriff grundsätzlich mit den wirksamsten Schutzmethoden und letztendlich nach dem „Stand der Technik" begegnen. Komme ein Angriff „an der Verteidigung vorbei", so bedeute „Stand der Technik" auch, einen Plan für die Reaktion darauf zu haben. Externe Forensiker mit der Beantwortung dieser Fragen zu beauftragen, sei bei der kurzen Reaktionszeit von 72 Stunden nicht mehr „Stand der Technik". Schnelle, moderne Lösungen müssten die Analyse übernehmen und vollständige Transparenz für die gesamte Infrastruktur und über die gesamte Dauer des Angriffs bieten. Schließlich gehöre noch Schadensminderung zu einer zeitgemäßen IT-Sicherheit. Organisationen müssten automatisch Angriffsvektoren unterbinden können, Bedrohungsinformationen auf allen Infrastrukturebenen verteilen und proaktiv Schwachstellen in allen Bereichen schützen, in denen personenbezogene Daten vorhanden sind.

Rechtsanwalt Stefan Drewes empfiehlt in der Februar-Ausgabe des Behörden Spiegel allen Unternehmen dringend die Einführung eines **Datenschutz-Governancemodells**, in dem sämtliche Datenverarbeitungen dokumentiert werden. Zusätzlich müssten Arbeitsrichtlinien zum Umgang mit Daten und im Falle von Datenverlust aufgestellt werden. Die Beratungsfirma McKinsey empfehle, im Arbeitsalltag vermehrt Messenger statt E-Mails zu verwenden, da die neue Technik die Mitarbeiterproduktivität um etwa 35 Prozent steigere. Mit dem Messenger SimsMe business, der von der Deutschen Post entwickelt wurde, solle die Unternehmenskommunikation auf bewährte Art und Weise normaler Messenger funktionieren. Der Messenger funktioniere komfortabel und einfach, aber gleichzeitig mit der Sicherheit, die die neue DSGVO voraussetzt. Dazu gehöre eine moderne Ende-zu-Ende-Verschlüsselung aller Nachrichten und Daten, die auf deutschen Servern bearbeitet und nicht in andere Rechtsgebiete ausgelagert werden. Durch ein sogenanntes Management Cockpit könnten zentral vom Administrator Lizenzen vergeben und gelöscht, Gruppen organisiert und betreut und Kanäle mit bis zu 1.000 Teilnehmern erstellt werden, um Mitarbeiter gebündelt zu unterrichten.Ulrich Pontes, Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB, zeigt in der Ausgabe 1-2018 des Sicherheitsforum, S. 28, wie **intelligente Verfahren der Videoanalyse** in der Lage sind, erhöhte Sicherheit mit verbessertem Schutz der Persönlichkeitsrechte zu kombinieren. Nur wenn ein Algorithmus Verdächtiges entdeckt, stelle das System bei der intelligenten Videoüberwachung mit der Möglichkeit der „kaskadierten Anonymisierung" das Bild scharf und alarmiere den Operator. Die Software sei darauf ausgerichtet, Handlungsmuster zu erkennen. Die automatisierte Suche nach „soft biometrischen Merkmalen" (bestimmte Accessoires, Haarfarbe oder Körpergröße) in Videodaten könnten Ermittlern helfen. Eine solche Software sei bei manchen Landeskriminalämtern bereits im Einsatz.

Ein Beitrag von Dipl.-Wirtschaftsinformatiker Markus Pfister, MAS Information Security Hochschule Luzern, in der Fachzeitschrift Sicherheitsforum, Ausgabe 1-2018, S. 45–50, befasst sich mit **Verschlüsselung und Pseudonymisierung**, zentralen Elementen, um der EU-Datenschutzgrundverordnung gerecht zu werden. In einem Krypto-System sei die Komponente, die Schlüssel erzeugt, speichert und verwaltet, das Herzstück. Ein Hardware-Securitymodul (HSM) sei ein Device, der diese Aufgaben übernehmen könne. Der Autor geht näher auf HSM, Pseudonymisierung, Verschlüsselung, Verschlüsselung von Nachrichten mit einem Businesspartner, Disk-, File- und Fileshare-Verschlüsselung

und Rights Management System (RMS) sowie auf Datenbankverschlüsselung ein und gibt dazu Praxistipps.

Die Kritik an Apples China-Gebaren wächst, berichtet heise.de am 27. Februar. Der Umzug von **iCloud-Daten auf die Server einer chinesischen Firma** löse große Bedenken aus, dass Behörden Apple-Nutzer in China nun unbeschränkt überwachen können, betone Amnesty International. Da Apple die für den Zugriff nötigen Schlüssel auf chinesischen Servern speichere, sei es praktisch unumgänglich, dass der Konzern gezwungen sein wird, entschlüsselte Daten herauszugeben. Ebenso wie Reporter ohne Grenzen rate auch Amnesty International chinesischen iCloud-Nutzern dringend dazu, ihre Landeseinstellungen zu ändern. Apple solle chinesische Nutzer dadurch schützen, iCloud standardmäßig nicht zu aktivieren.

Drohnen

Neues Abwehrsystem gegen gefährliche Drohnen, titelt die FAZ am 1. März. Mit einem neu entwickelten Sensor könnten unerwünschte und gefährliche Drohnen schneller als bisher geortet werden. Die Technik komme vom Unternehmen Dedrone. Das Peilgerät spüre erstmals anhand der Radiosignale auch die Fernbedienung auf und bestimme zudem ihre genaue Position. Sicherheitskräfte erhielten damit nicht nur Echtzeit-Informationen zur Flugroute und zum Gefahrenpotenzial der Drohne, sondern könnten den **Standort des Drohnenpiloten** ausmachen. Die Deutsche Flugsicherung (DFS) und die Deutsche Telekom arbeiteten an einem Drohnen-Prototyp, der mittels SIM-Karte wie ein „fliegendes Handy" Signale sende und auf Radarschirmen sichtbar werde.

Einbruchschutz

Die FAZ weist am 1. März auf eine vom Unternehmen Ring – und nach Übernahme dieses Unternehmens jetzt von Amazon – vertriebene intelligente **Türklingel mit integrierter Videokamera** hin. Diese Klingel erlaube es ihren Besitzern, auf ihren Smartphones zu sehen, wer vor der Tür steht, auch wenn sie gerade unterwegs sind. Sie könnten auch mit der betreffenden Person sprechen und damit zum Beispiel gegenüber etwaigen Einbrechern den Eindruck erwecken, sie seien zu Hause.

Endgerätesicherheit

Nach einer Meldung von focus.de am 15. Februar sehen laut dem US-amerikanischen Nachrichtensender CNBC die Chefs von sechs Geheimdiensten die Verwendung von chinesischen **Handys der Marken Huawei und ZTE** kritisch. Gründe für das Misstrauen seien vor allem angebliche Spionage und Datenmanipulation. FBI-Direktor Cris Wrey habe erklärt, dass beim Markteintritt von Huawei oder ZTE die Gefahr bestehe, dass Informationen böswillig modifiziert oder gestohlen werden könnten und unerkannte Spionage durchgeführt werde.

Erpressung

Nach einer Meldung von veko-online schätzten Experten der Result Group die Zahl der **Produkterpressungen** auf ca. 100 bis 150 pro Jahr in Deutschland. Die Täter wählten primär die bekannten Markennamen von finanzkräftigen Unternehmen mit herausgehobener Marktstellung aus. Die Täter seien zumeist nicht vorbestraft und sähen sich mit finanziellen Problemen konfrontiert. Aus der Erfahrung ergäbe sich eine Vielzahl an Hinweisen, auf die geachtet werden sollte: Ist die Absenderadresse unbekannt oder gar anonym? Ist die Adresse richtig und vollständig? Ist der adressierte Empfängerkreis limitiert? Hat das Paket eine ungewöhnliche Form, einen seltsamen Geruch, ölige Flecken an der Außenseite, verrutscht der Inhalt oder hat das Paket einen ungewöhnlichen Schwerpunkt? Ist der Empfänger nicht sicher, solle das Paket isoliert in einem ungenutzten Raum abgelegt und fotografiert werden. Es werde geraten, umgehend für alle weiteren Schritte die Polizei zu verständigen. Zudem solle sich derjenige, der das Paket in den Händen gehalten hat, gründlichst die Hände mit Seife waschen.

Evakuierung

Dr. Lukas Arnold, Forschungszentrum Jülich GmbH, stellt in der Fachzeitschrift Crisis Prevention, Ausgabe 4-2017, S. 24–27, Experimente und Simulationen für eine sichere **Evakuierung von U-Bahnstationen** im Brandfall vor. Die Rauchausbreitung in unterirdischen Verkehrsstationen stelle eine Herausforderung für den Brandschutz dar. Kompakte, verwinkelte Stationen mit mehreren Ebenen zeigten im Brandfall ein komplexes strömungsdynamisches Verhalten. Besonders die Dynamik der Rauchausbreitung während der sogenannten Selbstrettungsphase sei kritisch. Das Projekt ORPHEUS untersuche neben der Personensicherheit und dem Einfluss des Tunnelsystems auf die Branddynamik auch psychologische Aspekte der Evakuierung und die interorganisationale Zusammenarbeit von Rettungskräften und Betreibern. Im Rahmen von ORPHEUS seien Experimente zu verschiedenen Aspekten durchgeführt worden. Aus neu gewonnenen experimentellen Daten seien numerische Modelle erstellt worden. Die Kopplung der numerischen Berechnungen der Strömungsdynamik an ein Evakuierungsmodell ermögliche es, den Verlauf des Verrauchungszustands bei der Evakuierungssimulation zu berücksichtigen. Die entwickelten Werkzeuge und Konzepte seien auch auf andere Infrastrukturen übertragbar. Durch die umfangreichen Arbeiten im ORPHEUS-Projekt könnten Fluchtwege in U-Bahnstationen besser geplant werden.

Gefahrenmanagementsystem

Integration von Sicherheitsanlagen in übergeordnete Gefahrenmanagement-Systeme (GMS) thematisiert Thomas Stretz, euromicron Deutschland GmbH, in der Ausgabe 1-2018 von Security insight, S. 44/45. Es handele sich um Softwareplattformen, die auf einem zentralen Security-Server betrieben werden und alle sicherheitstechnischen Gewerke über definierte Schnittstellen auf einer einheitlichen, intuitiv bedienbaren Benutzeroberfläche zusammenführen. Physical- und IT-Security müssten eng vernetzt werden, wenn für jeden Krisenfall eine optimale Reaktion ermöglicht werden soll. Es sei ratsam, auch andere sicherheitsrelevante Systeme eines Gebäudes, wie etwa Systeme zur unterbrechungsfreien Stromversorgung oder die Licht- und Heizungssteuerung, in das GMS zu integrieren. Standardprotokolle wie Onvif oder Bacnet würden von GMS-Plattformen ebenso zuverlässig verarbeitet wie offene Bus-Protokolle oder proprietäre Protokolle verschiedenster Hersteller. Schon die bloße Existenz einer einheitlichen Benutzeroberfläche schaffe ein bislang ungekanntes Maß an Struktur und Übersichtlichkeit. Ist das GMS an die Einsatzleitsysteme von Polizei und Sicherheitsdienst angebunden, werde der Einbruchalarm direkt an diese weitergegeben. Feuerwehr und Rettungsdienste würden nicht nur über den Brand informiert und mit der Leitstelle verbunden, sondern erhielten automatisch detaillierte Angaben darüber, in welchen Gebäudebereichen sich das Feuer ausbreitet und ob Personen eingeschlossen sind. Zugleich könnten Sprinkleranlagen aktiviert und Feuertüren geschlossen werden. Ein wichtiger Aspekt von GMS sei, dass sie auch Systeme zur IT-Sicherheit integrieren. Cyberattacken könnten stets schnell beantwortet werden, auch durch das zeitweilige Abschalten von Online-Zugängen oder einen Shutdown hochgradig gefährdeter Teilsysteme der Gebäudetechnik. Umfassende GMS-Lösungen seien auch für Mittelständler technisch wie wirtschaftlich interessant. Die marktführenden Systeme seien modular aufgebaut und ermöglichten für Unternehmen jeder Größenordnung die Konfiguration der passenden Managementanwendung.

Interne Revision/Interne Untersuchungen

Elmar Schwager, The Audit Factory, befasst sich in Ausgabe 3-2018 von PROTECTOR, S. 64/65 mit **Massendatenanalysen** durch die Interne Revision. Werden auffällige Rechnungen in einem Unternehmen entdeckt, müsse abgeklärt werden, ob es sich eventuell um Korruptionszahlungen handelt. Dabei müssten die Unternehmensdaten untersucht werden, was ohne computergestützte Werkzeuge nicht zu bewältigen sei. Diese Werkzeuge würden in der Sprache der Internen Revision CAATs (Computer Aided Audit Tools) heißen. Häufig handele es sich dabei um Spezialsoftware, die Daten nach bestimmten Schlüsseln durchsuchen könne oder große Datenmengen unter einer oder mehreren Fragestellungen strukturiere. Der Autor geht auf die forensische Ausgangslage, auf Massendaten ohne Analyse, auf die Aufarbeitung des Betrugsfalles, auf unzulässige Rasteruntersuchungen und die Massendatenanalysen bei Regelprüfungen ein. In forensischen Prüfungen könne man bei bekanntem Betrugsschema sehr gezielt große Datenmengen analysieren. Im Bereich der Regelprüfungen gebe es ebenfalls erhebliche Vorteile der Massendatenanalyse: Fokussieren auf die

richtigen Risikobereiche; Ermöglichen des Testens von 100 Prozent der Datenpopulation; Ersatz für aufwendige Einzelfallprüfungen.

Rechtsanwalt Burkhard Fassbach und Steuerberater Frank Hülsberg weisen in der FAZ am 7. März darauf hin, dass unternehmensinterne Untersuchungen hohe Kosten verursachen können, vor allem durch externe Rechtsanwälte oder Wirtschaftsprüfer. Diese ließen sich durch die richtige **Manager-Haftpflichtversicherung** (D&O-Versicherung) abfedern. Zuständig für die Mandatierung externer Ermittlungen sei der Vorstand oder – sofern der Vorstand betroffen ist – der Aufsichtsrat. Solche „Internal Investigations" seien elementare Bestandteile eines Compliance Management Systems (CMS). Die Verantwortung verbleibe beim Vorstand oder Aufsichtsrat, auch wenn sie externe Rechtsanwälte und Wirtschaftsprüfer hinzuziehen. Der D&O-Versicherungsschutz entfalle bei Vorsatz und vorvertraglichen Obliegenheitsverletzungen. Eine Compliance-Versicherung knüpfe als Unternehmensdeckung an das vom Wirtschaftsprüfer geprüfte CMS an. So werde beurteilt, ob das eingerichtete System geeignet ist, um mit hinreichender Sicherheit Risiken wesentlicher Regelverstöße zu erkennen und diese zu verhindern (Angemessenheitsprüfung).

IoT (Internet der Dinge)

Stefan Strobel, sirosec GmbH, behandelt in der Ausgabe 3-2018 der Zeitschrift PROTECTOR, S. 38/39, **Sicherheitslücken im IoT**. Die Vernetzung von immer mehr Geräten mit Schnittstellen bedeute auch eine Vervielfachung potenzieller Sicherheitslücken. Häufig führten Softwareschwachstellen in IoT-Geräten und insbesondere in Kameras dazu, dass ein Unbefugter nicht nur lesenden Zugriff auf die Kameras hat, sondern auch die Software der Kamera manipulieren oder komplett austauschen kann. Ein anderes typisches Problem von IoT-Geräten sei neben der Überwachung des Besitzers der Zugang zum privaten Netzwerk des Anwenders. Um den Hintertüren und Sicherheitslücken der Geräte nicht hilflos ausgeliefert zu sein, sollte man die Geräte als Käufer/Anwender nicht einfach in sein privates WLAN/internes Netzwerk integrieren, sondern in ein eigenes, durch eine Firewall abgeschottetes WLAN/Netzwerksegment. In Unternehmen sollte in jedem Fall eine solche Abschottung erfolgen.

Veit Mathauer, Telent GmbH, befasst sich in PROTECTOR, Ausgabe 3-2018, S. 42/43, mit dem **Funknetz für das IoT**. Damit sich die Daten, die Sensoren in unterschiedlichsten Anwendungen erfassen, auswerten lassen, müssten sie zunächst an zentraler Stelle zusammengeführt werden. Low-Power-Netzwerke bildeten hierfür eine ideale Infrastruktur. Für das IoT typische Anwendungen bestünden im Wesentlichen aus drei Teilen: den Sensoren, dem Funknetz und der Plattform. Der Autor beschreibt diese Komponenten im Einzelnen. Um konkreten Nutzen aus der Fülle der erfassten Daten zu ziehen, stelle Telent die Plattform „evaIorIQ" zur Verfügung. Sie verbinde Sensoren, Applikationen und weitere Plattformen und stelle sicher, dass Ende-zu-Ende-Kommunikation oder Asset-Tracking genau auf die Bedürfnisse des Kunden angepasst werden können.

IT-Sicherheit

Der **TÜV Informationstechnik**, ein Tochterunternehmen der TÜV Nord, greift in einem Industriegebiet in Essen Chips und Software an, um Schwachstellen zu finden, berichtet die FAZ am 12. Februar. Mit einem Analyseprogramm schicke ein Hacker Tausende Codes, die zufällig generiert werden, an den Chip. Diese Daten würden vom Chip mit dem 16-stelligen PIN-Code verschlüsselt. Mit einem Oszilloskop, also einem Messgerät, das Spannung über einen gewissen Zeitraum misst, überprüfe der Hacker die Rechnung des Chips, er erstelle praktisch ein Stromprofil. Denn in dem Moment, in dem der Chip überprüft, ob der eingegebene PIN-Code der richtige ist, ließen sich höhere Stromwerte ablesen, wenn man genau diesen Prozess stört. So tauchten im Analyseprogramm des Angreifers nach wenigen Minuten 16 Graphen auf, mit jeweils neun Balken, acht davon seien blau und einer verräterisch rot. Die zufällig ausgewählten Zahlen, um den Chip zu verschlüsseln, würden offen auf dem Bildschirm angezeigt. Die Verschlüsselung sei geknackt. Mehr als 600 verschiedene Prüfungen gebe es. Gut zwei Wochen dauere ein einzelner Durchlauf eines Tests. Für Hochsicherheitschips, wie sie in Bankkarten oder neuen Personalausweisen verbaut sind, dauere die Prüfung bis zu einem Jahr. So ein Langzeittest koste dann auch schon siebenstellige Beträge. Mit dem BSI arbeite der TÜV IT zusammen, auch um die Sicherheit in Unternehmen zu erhöhen.

Führende Vertreter der Industrie gründen eine Initiative gegen weltumspannende Cyberkriminalität, meldet die FAZ am 17. Februar. Knapp 70 Prozent der deutschen Unternehmen und Institutionen seien 2016 und 2017 Ziel von Cyberangriffen geworden. Nach Angaben des BSI habe es 2016 rund 350.000 Schadprogramme gegeben – täglich. Laut Enisa Threat Landscape Report richteten Angriffe auf die Netzsicherheit 2016 Schäden in Höhe von 560 Mrd. Euro an und das Gefahrenpotenzial wachse dramatisch. Auf der Münchner Sicherheitskonferenz sei nun eine **Charta für mehr Cybersicherheit** unterzeichnet worden. Neben Siemens – wo dem Chief Information Security Officer (Ciso) 1.300 Cyberexperten zur Seite stünden – hätten Airbus, Daimler, Allianz, IBM, NXP, Deutsche Telekom, SGS und die Münchner Sicherheitskonferenz die „Charter of Trust" unterzeichnet. Sie zeige zehn Handlungsfelder für Politik und Industrie auf. Die Verantwortung für Cybersicherheit müsse wegen der Bedeutung auf höchster Ebene von Unternehmen und Regierungsorganen angesiedelt werden. Für Kritische Infrastrukturen sollten verpflichtende unabhängige Zertifizierungen durch Dritte vorgenommen werden. Sicherheits- und Datenschutzfunktionen sollten automatisch in angebotenen neuen Technologien als Werkseinstellung konfiguriert sein. Sicherheitsregeln müssten Bestandteil der Freihandelsabkommen sein, eine multilaterale Zusammenarbeit bei Regulierung und Standardisierung gefördert werden. Vertraglich vereinbarte Partnerschaften von Staat und Privatwirtschaft seien zu unterstützen.

Silicon.de meldet am 20. Februar, der Sicherheitsanbieter Avetco habe Daten von Microsoft Security Update Guide analysiert und dabei herausgefunden, dass sich die Zahl der in **Windows 10** gepatchten Kritischen **Sicherheitslücken** zwischen 2016 und 2017 um 64 Prozent erhöht habe. Insgesamt habe der Softwarekonzern im vergangen Jahr 587 Anfälligkeiten in Windows Vista, Windows 7, Windows 8.1 sowie Windows 10 gemeldet. Die Zunahme der Sicherheitslücken bewerte Avetco als Zeichen dafür, dass Windows unsicherer geworden sei. Avetco habe aber nicht nur Windows-Lücken, sondern auch Bugs in anderen Microsoft-Anwendungen analysiert. Demnach habe sich die Zahl der Office-Schwachstellen zwischen 2013 und 2017 um 89 Prozent erhöht. Kritische Löcher in den Microsoft-Browsern hätten indes nur um 46 Prozent zugenommen.

Die FAZ weist am 21. Februar auf einen neuen **Cybersicherheitsbericht des Netzwerkausrüsters Cisco** hin, der Ergebnisse einer Befragung von 3.600 Sicherheitsverantwortlichen in 26 Ländern enthält. Während früher vor allem die klassische IT ein Ziel von Kriminellen gewesen sei, werde nun vermehrt auch die für Unternehmen Kritische Infrastruktur angegriffen, weil sie nun vernetzt ist. Fachleute rieten daher davon ab, industrielle Kontrollsysteme mit dem Internet zu verbinden. Neun von zehn Befragten nutzten inzwischen sogenannte Behaviour Analytics: Das bedeute, dass ein Algorithmus automatisch anormales Verhalten über alle Benutzer und angeschlossenen Endgeräte überprüft. Im Schnitt stocke der Verkauf von Produkten nach einem Sicherheitsvorfall in Unternehmen fast acht Wochen, zwei Drittel der befragten Manager hätten Verzögerungen bereits erlebt. Unternehmen nähmen sich keine Zeit, um festzustellen, wie viele Geräte aus dem Internet der Dinge eigentlich mit ihren Netzwerken verbunden sind. Besonders angreifbar seien Sensoren, weil sie rund um die Uhr angeschlossen sind und häufiger schlechter geschützt als Computer. Wenn die Einschätzung der Analysten von Gartner stimme, wonach es in zwei Jahren 20,4 Mrd. und damit mehr als doppelt so viele vernetzte Geräte wie heute gebe, könne das unmöglich von Menschen überprüft werden. Gebraucht werde ein Netz, das hochgradig automatisiert ist und Angriffe selbstständig stoppt. Die Sicherheitsforscher gingen davon aus, dass Angriffe „ohne menschliches Zutun" wie die Computerwürmer „WannaCry" und „NotPetya" 2018 zunehmen werden.

Nach Befragung von rund 1.000 Unternehmen ergibt sich aus einer **Studie der Gothaer Versicherung**, dass 40 Prozent der KMU Cyberrisiken als eine der bedrohlichsten Gefahren für ihren Betrieb einschätzen, berichtet die FAZ am 26. Februar. 2016 waren es erst 32 Prozent gewesen. Dennoch verzichte ein Fünftel auf Virenschutzprogramme, fast ein Drittel führe keine regelmäßigen Sicherheitskopien durch. Eine Umfrage des BMWi zeige, dass ein Viertel der KMU keine Verschlüsselungstechnik nutzt. Unter den Großunternehmen seien es weniger als 10 Prozent. Im Handel seien Verschlüsselungstechniken bislang wenig verbreitet. Als größte Hürde würden die meisten der 140 befragten Unternehmen den technischen Aufwand angeben. Auch der finanzielle Aufwand werde immer wieder als Grund genannt. Das BMWi veröffentliche einen Leitfaden, mit welchen technischen Maßnahmen Unternehmen ihre Daten schützen können.

Wie eine Umfrage des BMWi zeige, nutzt ein Viertel der **KMU noch keine Verschlüsselungstechnik**. Unter den Großunternehmen sei dieser Anteil deutlich geringer und liege dort bei weniger als 10 Prozent. Interessant seien die Branchenunterschiede: Während nahezu alle mittelständischen IT- und Telekommunikationsunternehmen ihre Daten nur noch

verschlüsselt speicherten und mit Dritten austauschten, würden dies in der Autobranche und auch im Maschinenbau nur rund zwei Drittel der Unternehmen tun. Dabei würden die Daten in diesen Branchen als ähnlich sensibel gelten (faz.net am 26. Februar).

Timo Sachse, Axis Communications, benennt in der Ausgabe 1-2018 der Zeitschrift Security insight, S. 40/41, **IT-Trends für das Jahr 2018**: Edge Computing (dezentrale Datenverarbeitung am Rande des Netzwerks); Integration zwischen einzelnen Cloud-Diensten (Einsparungspotenzial), Deep-Learning und maschinelles Lernen; Plattformen zur Nutzung sämtlicher Vorteile des IoT; nichtvisuelle Sensoren, die neue Dimensionen erschließen; virtuelle Assistenten und Augmented Reality.

Fünf Faktoren einer **optimal gelebten Informationssicherheit** beschreiben Almut Eger, Auditorin für TÜV Rheinland Cert, und Walter Rüegg, Lead Auditor ISO 27001 Informationssicherheit, in der Ausgabe 1-2018 des Sicherheitsforum, S. 32–35, nämlich: Sicherheit unter der Kosten- und Effizienz-Lupe; Einsatz von Tools zur Wahrung der Informationssicherheit; Überprüfung der Informationssicherheit intern/extern; Informationssicherheit im Benchmark und Leistungsfähigkeit des ISMS. Mit der Implementierung eines ISMS nach ISO 27001 sei ein wesentlicher Schritt in die richtige Richtung getan: ein kontrollierter Umgang mit Informationen im ganzen Unternehmen. Die integrierte Sicherheit zu Daten, Dokumenten, Informationen und Wissen generell werde erreicht, wenn Informationssicherheit in allen Leistungseinheiten einer Organisation implementiert ist.

Die digitale Welt sicherer machen, titelt die FAZ am 5. März im Verlagsspezial „Zukunft Elektrotechnik". In der Automationsbranche sei nach dem Ergebnis der **ZVEI-Studie „Sicherheitslagebild im Fachverband Automation"** nahezu jedes Unternehmen mit kleineren und mittleren Angriffen konfrontiert. Drei von zehn Betrieben registrierten regelmäßig schwere Vorfälle. Der ZVEI verfolge im Beirat der **Allianz für Cybersicherheit** – mit 2.100 teilnehmenden Unternehmen das größte deutsche Informations- und Austauschnetzwerk zu dieser Thematik – drei langfristige Ziele: Etablierung einer Sicherheitskultur in der Industrie, industrietaugliche Sicherheitsregulierung und Stärkung der Kernkompetenz „Industrial Security" in der Öffentlichkeit. Software- und Hardwarehersteller müssten sich um Security by Design kümmern und Transparenz bei der Verfügbarkeit von Updates schaffen. Rohde & Schwarz habe über seine eigenen fünf Fertigungsstandorte, in denen Produkte für den Wireless-Markt, die Industrieelektronik, für Luftfahrt und Verteidigung, Informationssicherheit, Broadcast und Medientechnik gefertigt werden, elektronische „Schutzhüllen" gestülpt und biete dies auch anderen Unternehmen an. Das Prinzip: Bevor ein Programm oder ein Datenfragment von außen ins Haus gelangt, werde es in einer isolierten Umgebung – der Sandbox – auf Herz und Nieren geprüft.

Vertrauenswürdige Identitäten behandelt Markus Baba, HID Global, in PROTECTOR, Ausgabe 3-2018, S. 24/25. Der Bedarf steige, denn sie seien die Basis für einen besseren Komfort, eine höhere Sicherheit sowie eine gesteigerte Produktivität und Effizienz. Seit Kurzem könnten auch Smartphones als vertrauenswürdige Credential-Lösungen mit Zutrittskontrollsystem über die Cloud verknüpft werden. Eine logische Weiterentwicklung sei die Verbindung der mobilen Geräte mit der Authentifizierung im Bereich IoT. Dadurch werde es möglich, eine Verknüpfung von physischen Gegenständen und einem vertrauenswürdigen ID-Ökosystem herzustellen, sodass IoT-Applikationen sicherer und einfacher zu nutzen sind. Mobile Geräte könnten in Kombination mit vertrauenswürdigen Tags und Cloud-Authentifizierungsservices sowie unter Verwendung von Cloud-Maintenance Management-Software (CMMS) für die Wartung von Geräten genutzt werden.

IuK-Kriminalität

Momentan würden in vielen E-Mail-Postfächern gefälschte Nachrichten unter dem Namen des Bezahldienstes Klarna landen, meldet spiegel.online am 6. März. Angeblich habe der Angeschriebene eine Rechnung nicht bezahlt. Das LKA Niedersachsen warne jedoch: Auf keinen Fall sollten Betroffene den Anhang öffnen, nicht einmal dann, wenn der Kunde mit dem korrekten Namen und der korrekten Postadresse angeschrieben worden sei. Er enthalte Schadsoftware, die derzeit nur von wenigen Antivirenprogrammen erkannt werde. Die E-Mail stamme auch nicht von Klarna.

Kommunale Sicherheit

Schutz des öffentlichen Raumes ist nicht nur Aufgabe der Polizei, betont der Innenminister von NRW, Herbert Reul, in der Februar-Ausgabe des Behörden Spiegel. Die EU-Kommission habe einen Aktionsplan vorgelegt und wolle mit 18,5 Mio. Euro aus dem Fond für Innere Sicherheit die Mitgliedstaaten bei grenzübergreifenden Projekten zum Schutz von öffentlichen Räumen unterstützen. Dieser Schutz gelinge nur gemeinsam mit den Kommunen sowie mit den Veranstaltern von Großereignissen. Für Städte, die in Sicherheitslösungen investieren, stünden 2018 weitere 100 Mio. Euro aus der EU-Initiative „innovative Maßnahmen für eine nachhaltige Stadtentwicklung" bereit. Ein Forum zu öffentlich-privaten Partnerschaften im Sicherheitsbereich, in dem ein aktiver Erfahrungsaustausch stattfindet und in dem lokale und regionale Behörden zum „Best Practice" für den Schutz des öffentlichen Raumes informieren können, sei wichtig.

Krankenhaussicherheit

Jens Seeliger, Bosch Energy and Building Solutions, stellt in der Ausgabe 1-2018 der Zeitschrift Security insight, S. 36–38, ganzheitliche und vernetzte Lösungen zur präventiven **Gefahrenerkennung und -vermeidung in Krankenhäusern** vor. Neue Herausforderungen entstünden zum Beispiel durch die wachsende Gewaltbereitschaft, Substanz-Missbrauch und Auftragsdiebstähle von Medizingeräten. Dazu kämen die immer strengeren Brandschutz- und Hygiene-Vorschriften sowie der zunehmende Kostendruck. Die Anzahl der Fälle von „Hospital Violence" habe sich laut der Suchmaschine „PubMed" in den letzten zehn Jahren mehr als verdoppelt. Der Autor präsentiert personelle und organisatorische Lösungsansätze und technische Ansätze. Kameras würden um komplementäre Techniken ergänzt, die Gefahren erkennen, bevor es zum Gewaltausbruch kommt. Laut einer Studie von Roland Berger arbeiteten knapp 90 Prozent aller Krankenhäuser an einer Digitalisierungsstrategie. Der Weg zum „Smart Hospital" sei aber für die meisten noch weit. Schon heute seien aber in einem Gesamtkonzept folgende installierte Lösungen denkbar: Sensoren an Türen und Fenstern, vernetzte Bewegungsmelder oder EMA, Sprachalarmierung und intelligent gesteuerte Beleuchtungslösungen.

Kriminalität

Nach den bisher von einigen Bundesländern veröffentlichten Kriminalstatistiken ist die **polizeilich registrierte Kriminalität 2017** im Vergleich zu 2016 insgesamt und in vielen Deliktsarten gesunken. So war zum Beispiel die gemessene Gesamtkriminalität in Hessen 2017 auf dem niedrigsten Stand seit fast 40 Jahren und lag fast neun Prozent niedriger als 2016. Zugleich wurde eine Aufklärungsrate von 62,8 Prozent erreicht. Das ist der höchste jemals gemessene Wert (innen.hessen.de vom 15. Februar). Wie der hessische Innenminister bei der Vorstellung des Berichts ausführte, habe sich die Straßenkriminalität in den letzten 20 Jahren halbiert. Neben einer starken polizeilichen Präsenz im öffentlichen Raum bildeten moderne Videoüberwachungsanlagen einen wichtigen Baustein für mehr Sicherheit auf Hessens Straßen. In 16 Städten seien 20 Anlagen mit insgesamt 148 Kameras zur Überwachung öffentlicher Räume in Betrieb. An den videoüberwachten Örtlichkeiten würden jährlich über 2.100 Straftaten registriert, bei denen die Aufzeichnungen zur Klärung der Straftaten beitragen könnten. In Niedersachsen ist die Zahl der gemeldeten Straftaten 2017 im Vergleich zum Vorjahr nach einem Bericht in der FAZ am 27. Februar um 6,4 Prozent gesunken. Der Rückgang bei Wohnungseinbrüchen betrage 17 Prozent. Deutlich gestiegen sei hingegen die Furcht vor Kriminalität. Binnen zwei Jahren sei, wie sich aus einer „Dunkelfeldstudie" ergebe, der Anteil der Menschen mit geringem Sicherheitsgefühl von 9,1 Prozent auf 12,3 Prozent gestiegen. Hamburg meldet einen Rückgang der Gesamtkriminalität gegenüber 2016 um 5,6 Prozent, bei Wohnungseinbrüchen um 23,2 Prozent. Dabei sei der Anteil der vor allem aufgrund technischer Sicherheitsmaßnahmen im Versuchsstadium stecken gebliebener Wohnungseinbrüche von 43,2 Prozent auf 46,2 Prozent angestiegen. Gefallen sei auch der Diebstahl aus gewerblichen Objekten und Büros (um 27,1 Prozent).

Krisenmanagement

Veko-online.de berichtet in der Februar-Ausgabe, das **Forschungsprojekt TEAMWORK** werde im Zuge der Bekanntmachung „Zivile Sicherheit – Erhöhung der Resilienz im Krisen- und Katastrophenfall" des BMBF über einen Zeitraum von drei Jahren mit rund 2,1 Mio. Euro gefördert. Koordiniert werde das Verbundprojekt „Krisensimulation für

die Zusammenarbeit von Einsatzkräften und Bevölkerung" vom Institut C.I.K. an der Universität Paderborn. Verfolgt würden Forschungsziele in den drei Bereichen Formalisierung, Simulation und Auswertung. Bei der Formalisierung gehe es darum, im Team realistische Szenarien zu entwickeln und in eine virtuelle Umgebung umzusetzen. Mit einem kollaborativen Szenario-Editor könne jeder Akteur dazu beitragen, die virtuelle Umgebung noch realistischer zu gestalten. Die Grundlage dafür bildeten importierte Daten, beispielsweise Geodaten. Eine webbasierte Plattform ermögliche die Kommunikation und Zusammenarbeit zwischen den Akteuren. In der Simulation könnten unterschiedliche Krisenszenarien in einer virtuellen Umgebung in Echtzeit gemeinsam bewältigt werden. Die Daten aus der Simulation würden in einer Auswertung automatisiert aufbereitet und anhand eines Zeitstrahls, Lagefilmen sowie Diagrammen auf einer webbasierten Plattform visualisiert.

Dominic Gißler, M.Sc., und Prof. Dr.-Ing. Frank Fiedrich, Bergische Universität Wuppertal, beschreiben in der Ausgabe 4-2017 der Zeitschrift CRISIS Prevention, S. 20–23, **standardisierte Methoden für die Einsatzführung** bei Hilfsorganisationen und im Krisenmanagement. Die wichtigsten Techniken bildeten quasi den „Werkzeugkasten" der Stabsarbeit: **– Organisation –** Ein Organigramm mit typischer Arbeitsteilung könne bereits vorbereitend erstellt werden. **– Modell des Ereignisses –** Ereigniskonten könnten mit Metaplankarten auf einem Schreibblock oder in einer Tabellenkalkulation geführt werden. **– Analyse und Beurteilung –** Es habe sich bewährt, wenn die Leitung des Stabes und die Aufgabenbereiche Lagedarstellung und Einsatz abseits des Stabsgeschehens das Ereignis analysieren. **– Zeitstrahl und Vorhersage –** Das Werkzeug diene dazu, die zeitlichen Beschränkungen der möglichen Handlungen sowie Wendepunkte des Ereignisses zu erkennen sowie um die bestmögliche und schlechtmöglichste Entwicklung einschätzen zu können. **– Strategie –** Die Effizienz und Effektivität der Stabsarbeit könne deutlich erhöht werden, wenn die Stabsleitung ihren Handlungsplan in einer Strategie formuliert. **– Maßnahmenplanung & Aufgabennachverfolgung –** Das Werkzeug könne bereits vorbeugend angelegt werden. **– Lagebesprechung –** Es habe sich in unübersichtlichen Situationen bewährt, dass die Stabsleitung in kurzen Vorbesprechungen mit den Verantwortlichen der Aufgabenbereiche des Fokus auf wichtige Punkte lenkt. **– Stabsablauf –** Die Agenda von Lagebesprechungen könne aufgebaut sein wie der Stabsablauf. Hierdurch werde die Besprechung zu einer logischen Abfolge geordnet. Die Werkzeuge könnten in Einzelübungen ausprobiert, in Planbesprechungen gemeinsam angewendet und in umfassenderen Stabsrahmenübungen an einem simulierten Ereignis erprobt werden.

Kritische Infrastrukturen

Burkhard Dregger, MdA Berlin, sieht in der Abwehrfähigkeit Kritischer Infrastrukturen eine Kernaufgabe moderner Sicherheitspolitik (Behörden Spiegel, Februar-Ausgabe). Die **Netzökonomie** – das heißt die durch und über das Internet erwirtschafteten volkswirtschaftlichen Vermögenswerte und die Verknüpfung der Offline-Welt mit der Digitalwelt – erhielten aufgrund ihres Wachstums eine immer größere, ja existenzielle Bedeutung für die Funktionsfähigkeit unseres Staates. Durch die Digitalisierung der Strom-Lieferkette entstünden weitere Angriffspunkte. Denn die IT helfe bei der Steuerung der gesamten Lieferkette, und diese Steuerung könne nicht mehr nur physisch gestört werden, sondern per Fernzugriff von jedem Ort der Welt aus. Eine Fokussierung auf den Angreifer allein könne die Angriffe nicht stoppen. Die Gefahrenabwehr müsse früher ansetzen. Wir müssten vor allem verstehen, von welchen Voraussetzungen die Funktionsfähigkeit unserer lebenswichtigen Infrastrukturen abhängt. Das Schließen der Einfallstore in der Verwundbarkeit in der Lieferkette müsse aufgrund der fortschreitenden technischen Entwicklung von möglichen Angriffswegen ein kontinuierlicher Prozess der „Best Practices" sein. Die Anpassung der technischen Schutzmechanismen an den sich permanent weiterentwickelnden Stand der Technik müsse höchste Priorität für die Betreiber Kritischer Infrastrukturen haben.

Ist die Security einer Kritischen Infrastruktur überwunden, dann bedarf es nach der Überzeugung von Jürgen Kolb, iQSol GmbH, eines **geordneten Shutdowns** mit nachfolgendem Restart aller relevanten Geräte in der IT-Infrastruktur (Behörden Spiegel, Februar-Ausgabe). Mithilfe des Power Managements könne in solchen Fällen bewahrt werden, was wichtig ist: Daten werden per Live-Migration in sichere Ausfall-Rechenzentren verschoben, Server und Systeme durch einen geordneten Shutdown und Restart nach Logik und auf Knopfdruck gerettet. Eine solche Lösung sei die PowerApp von iQSol. Die Hardware-Appliance werde vor Ort oder per Managed Security Service in die IT integriert und mit den entsprechenden Knotenpunkten verbunden. Auch die sogenannte Disaster Recovery müsse bedacht werden.

Damit diese gelingt, sei zunächst wichtig, per Notfallhandbuch klar zu definieren, welche Prozesse aufrechterhalten werden müssen und welche Maßnahmen dies erfordere. Es definiere, wo sich Backups befinden, wie diese nach einem Crash wieder eingespielt werden können, welche Systeme welche Passwörter erfordern, wo eventuell benötigte Ersatzcomputer stehen und dergleichen mehr. Übungen sollten durchgeführt werden. Um ein technisches Business-Continuity-Management auch als Prozess durchzuführen, werde von iQSol das Log Management vorgeschaltet und die Enterprise-Alarmierung nachgelagert.

Konstantin Rogalas, Honeywell Industrial Cyber Security Zentral- und Südeuropa, skizziert in der Ausgabe 1-2018 der Zeitschrift Security insight, S. 18–21, industrielle Cyber Security und die **schleppende Umsetzung des IT-Sicherheitsgesetzes**. Bis zum 3. Mai 2018 müssten die Betreiber Kritischer Infrastrukturen IT-Sicherheit nach dem „Stand der Technik" umsetzen und deren Einhaltung fortan regelmäßig gegenüber dem BSI nachweisen. Aber viele Unternehmen seien noch längst nicht so weit, die Vorgaben im Bereich Automation Security erfüllen zu können. Eine neue Studie von LNS Research und Honeywell habe belegt, dass mit 53 Prozent gut die Hälfte aller befragten Anlagenbetreiber regelmäßig Cyberangriffe feststellen und berichten könnten. Gleichzeitig hätten aber nur etwas mehr als die Hälfte dieser Befragten eine Firewall zwischen Office-Netz und dem Dateiformat PLS installiert (59 Prozent).

Ladungsdiebstahl

In Ausgabe 1-2018 von Security insight, S. 46/47, wird der **Schutz von Lkw-Transporten** vor Ladungsdiebstählen thematisiert. Der wirtschaftliche Schaden solcher Ladungs- und Kraftstoffdiebstähle sei enorm. Euro Rastpark mache sich daran, zusammen mit anderen Mitgliedern der Vereinigung Deutscher Autohöfe e.V. (VEDA) diese Probleme durch die Entwicklung eines praxisnahen Sicherheitskonzepts abzustellen und habe Premium-Parkplätze eingerichtet. Euro Rastpark GmbH & Co. KG betreibe an 18 Standorten komfortabel ausgestattete Rastanlagen, viele davon entlang wichtiger Routen der Transportlogistik. Man setze auf kurzfristig wirkende Aufklärungs- und Abschreckungsmaßnahmen wie beschränkte Zufahrten, optimale Beleuchtung und lückenlose Dokumentation aller Fahrzeug- und Personen-Bewegungen.

Gernot Dähne, DeDeNet GmbH, stellt in der Ausgabe 3-2018 von PROTECTOR, S. 68/69, **Telematik-Lösungen** gegen Fahrzeug- und Maschinendiebstahl vor. Schon jetzt kämen in nahezu allen Lkw Telematik-Lösungen zum Einsatz, allerdings meist nur mit Standardfunktionen. Ein zusätzliches Modul zur Echtzeitortung hätte gleich mehrere Vorteile. Telematik-Lösungen mit Streckenplanung, Zeiterfassung und Tankbericht seien eine solide Grundlage, um Daten zu verwalten. Lösungen mit umfassenderen Funktionen verfügten über Funktionalitäten wie Diebstahlschutz, Echtzeitortung und die Kontrolle der Lenk- und Ruhezeiten. Über ein Webportal könne der Unternehmer zudem die gesamte Route unter Berücksichtigung von Besuchszeiten beim Kunden planen und verfolgen. Einsatzbereiche für die moderne Telematik-Technologie seien Fahrzeuge jeder Art wie Lkw, Transporter und andere Nutzfahrzeuge, aber auch Pkw sowie Bau- und Landmaschinen. Flotten und Fuhrparks könnten mit der Fuhrparkverwaltungssoftware größenunabhängig überwacht und kontrolliert werden. In der Regel ließen sich Telematik-Lösungen einfach per Schnittstelle in die meist schon vorhandene Standard-Transportmanagement-Lösung integrieren.

Luftverkehrssicherheit

Das Weiße Haus habe vorgeschlagen, die Bundesluftfahrtbehörde FAA und ihre Controller unter dem Dach einer staatlich gecharterten gemeinnützigen Gesellschaft zusammenzuführen, meldet Security insight in der Ausgabe 1-2018, S. 20. Sie würde durch Steuern auf Flugtickets und Flugbenzin finanziert werden. Viele Industrieländer hätten ähnliche Vereinbarungen, darunter Kanada, Großbritannien und Australien.

Auf Seite 49 der Zeitschrift Security insight, Ausgabe 1-2018, erläutert der neu gegründete Bundesverband der Luftsicherheitsunternehmen (**BDLS**) seine ersten Schritte: Vereinheitlichung und Vereinfachung der gesetzlichen und behördlichen Regelungen im Bereich der Luftsicherheit; Erarbeitung einheitlicher nationaler und europäischer Standards für den Aufgabenvollzug; verbindliche Festlegung dieser Standards durch entsprechende Normen und Zertifikate; Vereinheitlichung aller Schulungs-, Prüfungs- und Auditierungsverfahren; Erarbeitung gesetzlicher und tariflicher Regelungen; ständige Weiterentwicklung der Kontrollverfahren.

Persönlichkeitsrechtsverletzung

Google haftet als Betreiber einer Suchmaschine nicht dafür, wenn es Websites mit Inhalten anzeigt, die die Persönlichkeitsrechte von Dritten verletzten. Dies habe der BGH in einem Berufungsprozess entschieden, meldet zeit.de am 27. Februar. In dem Fall sei es darum gegangen, ob Google Links auf Websites sperren muss, auf denen die Kläger aus ihrer Sicht diffamiert und bloßgestellt werden. Auch die Vorinstanz – das OLG Köln – habe entschieden, dass ein Suchmaschinenbetreiber nur dann zur Sperrung von Links verpflichtet werden kann, wenn die behauptete Rechtsverletzung offensichtlich erkennbar ist. Hierfür müsse der Betroffene detailliert über die Rechtsverletzung informieren. Die bloße Auflistung von fraglichen Links mit dem Hinweis der Persönlichkeitsrechtsverletzung genüge dafür nicht.Pharmasicherheit

Peter Niggl befasst sich in der Ausgabe 1-2018 von Security insight, S. 16–18, mit der **Belastung der Pharmaindustrie durch Fälschungen und Diebstahl**. Mit einem Umsatz zwischen 150 Mrd. und 200 Mrd. Euro seien illegal hergestellte Pharmaprodukte das lukrativste Segment des weltweiten Handels mit illegal in Verkehr gebrachter Waren. Gefälschte und minderwertige Medikamente verursachten in Deutschland jährlich eine Mrd. Euro Schaden. Ab 9. Februar 2019 müssten Arzneimittelpackungen, die vom Hersteller in den Verkehr gegeben werden, Sicherheitsmarkmale tragen. Kernelemente des Systems seien zum einen die Verwendung von Packungen mit Erstöffnungsschutz, zum anderen die Kennzeichnung jeder Packung mit einer individuellen Seriennummer. In der Lieferkette lauerten für Pharmaunternehmen Risiken: Diebstahl, Manipulationen und falsche Temperaturen. Die Gefahr, dass ein Spediteur den Auftrag an ein Subunternehmen vergibt, sollte ausgeschlossen und der Logistikprozess gemäß der EU-Richtlinie Good Distribution Practice vom European Institute for Pharma Logistics zertifiziert sein. Beim Lagern und Transport der sensiblen Waren seien zahlreiche Vorschriften zu berücksichtigen, die vor Fälschungen, Verwechslungen und unbefugtem Zugriff schützen.

Produktpiraterie

Der **Negativpreis „Plagiarius"** sei am 9. Februar 2018 zum 42. Mal vergeben worden, meldet Security insight in der Ausgabe 1-2018, S. 47. Der 1. Preis sei an die Fälschung des Küchen-Schneidgeräts „Nicer Dicer Plus" gegangen, das vom chinesischen Unternehmen Pingyang County Leyi Gift Co. kopiert worden sei. Allein 2016 hätten die EU-Zollbehörden mehr als 41 Mio. rechtsverletzende Produkte im Wert von 670 Mio. Euro an den EU-Außengrenzen beschlagnahmt. China sei Herkunftsland Nummer eins für Fälschungen. An den Kunden gelangten die Fälschungen oftmals über den Online-Handel. Für eine bestmögliche Abwehr von Produkt- und Markenpiraterie rate die Aktion Plagiarius Firmen, auf eine ganzheitliche Strategie aus juristischen, organisatorischen und technischen Maßnahmen zu setzen.

Unterlassungsverfügungen gegen Produktpiraterie thematisiert Rechtsanwalt Hartwig Schmidt-Hollburg in der FAZ am 7. März. Allein europäischen Unternehmen entstünden durch Produktpiraterie jährlich Schäden in Höhe eines zweistelligen Milliardenbetrags. Aufgrund der im internationalen Vergleich besonders schnellen und effizienten einstweiligen Verfügungsverfahren seien deutsche Gerichte wichtige Anlaufstellen für das Vorgehen gegen Produktpiraterie aus aller Welt. Der BHG habe in einem Beschluss vom Oktober 2017 klargestellt: Eine Unterlassungsverfügung, die dem Antragsgegner den rechtsverletzenden Vertrieb bestimmter Produkte verbietet, verpflichtet den Antragsgegner nicht nur dazu, dass er selbst den Absatz dieser Erzeugnisse unverzüglich unterlässt. Sondern nach den Ausführungen des Gerichtshofs muss der Antragsgegner zugleich aktiv sämtliche möglichen, erforderlichen und zumutbaren Maßnahmen ergreifen, um zu verhindern, dass seine Abnehmer die betroffenen Produkte ihrerseits weitervertreiben. Bei Weitergabe der Produkte an Dritte könne aus einer einstweiligen Unterlassungsverfügung sogar eine Verpflichtung des Antragsgegners zu einem Rückruf bereits ausgelieferter Waren folgen.

Rechenzentrumssicherheit

Bernd Hanstein und Christian Abels, Rittal GmbH & Co. KG, befassen sich in der Ausgabe 3-2018 der Zeitschrift PROTECTOR, S. 44/45, mit der **Sicherheit von Serverschränken**. Ein

IT-Rack sollte mit einer abschließbaren Tür ausgerüstet sein. Elektronische Schlösser mit Zugangscode sollten protokollieren, welche Person zu welchem Zeitpunkt auf den Schrank zugegriffen hat. Stehe der Serverschrank in einer weniger geschützten Umgebung, dann müsse das IT-System gegen die Umweltbedingungen gesichert sein. Die IP-Schutzart gebe durch eine einfache Zahlenkombination an, wogegen das Gehäuse seinen Inhalt schützt. Die Zahlen der ersten Kennziffer definierten den Schutz vor festen Gegenständen und Staub, die Zahlen der zweiten den Schutz vor Wasser. Für industrietaugliche Installationen kämen Schutzarten bis IP 55 zum Einsatz. Mit Sicherheitssafes ließen sich noch höhere Schutzmaßnahmen implementieren als beim Standard-IT-Rack. Gerade für Unternehmen mit nur zwei bis drei Serverschränken böten die Safes eine schnell realisierbare Option für mehr IT-Sicherheit. Je nach Sicherheitsklasse schütze der Safe die IT-Komponenten vor Bränden, Rauch und Wasser. Die Lösung Micro Data Center von Rittal sei in verschiedenen Sicherheitsstufen verfügbar und ermögliche es, die IT in einem Schutzraum bis zur Widerstandsklasse 4 zu betreiben.

PROTECTOR plädiert in der Ausgabe 3-2018, S. 46, dafür, nicht nur Wartung und Service, sondern auch die **Reinigung eines Rechenzentrums** Profis zu überlassen. Vielfach fehle das Bewusstsein oder es sei nicht bekannt, dass Rechenzentrum-Verantwortliche nach der DIN ISO Norm 14644-1 Klasse 8 die Einhaltung der Luftreinheit sicherstellen müssen. Während bei geschlossenen Systemen eine jährliche Reinigung ausreiche, empfehle es sich, bei offenen Systemen vorab eine Feinstaubanalyse durchführen zu lassen.

Sicherheitsgewerbe

Andreas Paulick, BDSW, befasst sich in der Februar-Ausgabe des Behörden Spiegel mit dem **Bewacherregister**, das bis zum Jahresende eingeführt werden soll. Er listet die personenbezogenen Daten auf, die im Register gespeichert werden. Nutzer seien vor allem Ordnungsbehörden, die vor der Erteilung einer Gewerbeerlaubnis das Vorliegen der Voraussetzungen zu prüfen haben. Das BAFA sei die Registerbehörde. Es sei für die Sicherstellung des technischen und fachlichen Betriebs und für die Weiterentwicklung verantwortlich. Ein Konzept zur Erstregistrierung sehe einen dreistufigen Prozess vor (Registrierung der Ordnungsbehörden vor der Aufnahme der lokalen Bewacherdaten).

Manfred Buhl, Securitas Deutschland, zeigt in der Ausgabe 3-2018 von PROTECTOR, S. 66/67, in welchem Maße Sicherheitsunternehmen zur **Sicherheit des öffentlichen Raumes** beitragen und welche Möglichkeiten noch nicht ausgeschöpft sind: Streifendienste im Auftrag der Kommunen im Rahmen der Aufgabenstellung des Ordnungsamtes (am effizientesten mit gesetzlicher Beleihung der hoheitlichen Befugnis zur Anhaltung, Personalienfeststellung und Platzverweis); Unterstützung von Einzelhandelsgeschäften in städtischen Geschäftsvierteln in kritischen Situationen durch Alarmierung von Interventionskräften, die sich mobil in dem Geschäftsviertel aufhalten; konsequentere Umsetzung der bestehenden Sicherheitspartnerschaften mit der Polizei; Erarbeitung von Konzeptionen kommunaler Sicherheit zusammen mit der Kommune, ihrem Präventiven Rat und der Polizei.

Sicherheitstechnik

Jürgen Rumeney und Carsten Meissner, Siemens AG, befassen sich in der Ausgabe 3-2018 der Zeitschrift PROTECTOR, S. 6–9, mit der **Digitalisierung in der Sicherheitstechnik**. In Bezug auf Planung und Betrieb sicherheitstechnischer Systeme biete „Building Information Modeling" (BIM) vor allem im Bereich der passiven Sicherheit große Potenziale. So könne beispielsweise mit der Evakuierungssimulationssoftware von Siemens ein Digital Twin aus einer BIM-Planung nahtlos für eine Simulation der Gebäudeentfluchtung verwendet werden. Auch bei Brandmeldern erschließe die Digitalisierung immer neue Potenziale. Algorithmenbasierte und parametergestützte Detektionsverfahren hätten sich längst durchgesetzt. Ein Beispiel für einen holistischen – also ganzheitlichen – Ansatz sei das One-Card-Konzept für die unternehmensweite Zutrittskontrolle. Eine multifunktionale ID-Karte erfülle dabei sämtliche Anforderungen von Besuchern, Mitarbeitern und Lieferanten. Als konkrete Lösung zur Umsetzung integrierter Konzepte stelle Siemens aktuell das System „Transliner Pro" vor: Speziell für Hochsicherheitsanwendungen und größere Industrieanlagen konzipiert erweitere es die Funktionen einer klassischen EMZ um Zutrittskontrollfunktionen und ermögliche die Einbindung von Videotechnik. Ein weiteres Beispiel für einen holistischen, integrierten Ansatz in der Sicherheitstechnik sei das Gefahrenleitsystem „Siveillance Viewpoint". Es vereine Gefahrenmanagement und ausgewählte Einsatzleitfunktionen erstmals in einer integrierten Plattform. Die Software korreliere Informationen aus allen Subsystemen und liefere

damit eine klare, strukturierte Übersicht über die Ereignisse sowie die gesamte Melderlandschaft. In der Sicherheits- und Brandmeldetechnik setze sich der Einsatz digitaler Technologien und Konzepte mit guten Gründen zunehmend durch.

Spionage

Christian Schaaf, Corporate Trust, Business Risk & Crisis Management GmbH, warnt in der Ausgabe 3-2018 der Zeitschrift PROTECTOR, S. 70/71, vor Betriebsspionage. Nach dem von Corporate Trust zusammen mit dem BVSW und der Brainloop AG herausgegebenen **Future Report** hätten etwa 30 Prozent aller befragten Unternehmen angegeben, Opfer von Spionage oder Informationsabfluss geworden zu sein. 83,9 Prozent der befragten 4.738 Vorstände und leitenden Manager hätten angegeben, dass sie Cyberattacken in Zukunft für die größte Bedrohung für die deutsche Wirtschaft halten. Konkret für das eigene Unternehmen hätten dies jedoch nur 66,5 Prozent als Bedrohung eingeschätzt. Längst seien moderne IT-Systeme und Firewalls so gut, dass sie Spionageattacken rechtzeitig erkennen und in der Regel verhindern können. Um die unternehmenseigenen „Kronjuwelen" in Zukunft effektiver vor digitalen Spionageattacken zu schützen, sei es notwendig, die Präventionsmaßnahmen mit allen in diesen Bereichen involvierten Abteilungen abzustimmen.

Steuerbetrug

„Milliardenschaden durch Steuerbetrug" thematisiert die FAZ am 14. Februar unter Hinweis auf einen Bericht im Handelsblatt. Steueranwälte als „Goldfinger"-Berater seien im Visier der Staatsanwaltschaft. Das Modell „Goldfinger" funktioniere so: Ein Unternehmer erzielt einen hohen Gewinn, etwa durch den Verkauf von Firmenanteilen. Dazu gründet er etwa in Großbritannien ein Unternehmen. Dieses erwirbt Gold oder ähnliche Edelmetalle, um sie wieder zu verkaufen. So kann man das Metall dem Umlaufvermögen zurechnen. Das Geld, das für den Ankauf des Goldes ausgegeben wurde, führte zu Verlusten. In der Regel lag der Steuersatz für das Gesamteinkommen daher aufgrund eines Doppelbesteuerungsabkommens mit Großbritannien bei Null. Im zweiten Schritt verkauft das Unternehmen das Gold ein Jahr später. Das zuständige Finanzamt muss die Gewinne nun über den „Progressionsvorbehalt" berücksichtigen. Das Unternehmen zahle aber ohnehin den Spitzensteuersatz. Nach heute geltender Rechtslage dürfe Umlaufvermögen erst als Ausgabe berücksichtigt werden, wenn das Unternehmen Einnahmen erzielt oder das Gold ins Privatvermögen überführt.

Terrorismusbekämpfung

Auf **Reformen im Kampf gegen den Terror** weist die FAZ am 20. Februar hin. In den vergangenen fünf Jahren habe sich die Zahl der salafistischen Extremisten in Deutschland nahezu verdreifacht. Sie liege bei derzeit bei knapp 11.000 Personen. Die Anzahl islamistischer Gefährder habe sich in den letzten fünf Jahren von 140 auf 750 erhöht. Nach Überzeugung des BKA-Präsidenten Holger Münch sei es nötig, die Überwachung auszubauen. Insbesondere müssten in den Bundesländern einheitliche Standards herrschen. In einigen Bundesländern zähle zu den wichtigsten neuen Befugnissen die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ). Damit könnten auch verschlüsselte Nachrichten überwacht werden. Bayern habe die Quellen-TKÜ sogar für den Verfassungsschutz eingeführt. Der Präsident des BfV, Georg Maaßen, fordere ebenfalls die Quellen-TKÜ.

BKA sieht **Terrorgefahr bei Fußball-WM in Russland**, meldet rp.online am 6. März. Dem BKA-Papier zufolge thematisiere die Dschihadistenmiliz Islamischer Staat seit Mitte Oktober 2017 zunehmend die WM 2018.

Bisher Unbekannte haben am 6. März – wie welt.de am 7. März berichtet – Bernard Günther, Finanzvorstand des Energieversorgungsunternehmens Innogy, **mit Säure übergossen** und schwer verletzt. Er sei in eine Spezialklinik gebracht worden. Über die Hintergründe gebe es nach Angaben von Innogy bislang keine Informationen. Laut Bildzeitung werde geprüft, ob es einen Zusammenhang mit den Auseinandersetzungen um den Tagebau „Hambacher Forst" gebe. Mit welcher Flüssigkeit das Opfer übergossen wurde, werde noch geprüft.

Unternehmenssicherheit

Das Indoor Positioning System (IPS) erlaubt es Großunternehmen und Krankenhäusern, die Sicherheit in ihren Gebäuden zu erhöhen, ist Marc Maurer, Siemens Schweiz AG, überzeugt (Sicherheitsforum, Ausgabe 1-2018, S. 56/57). Besonders wirksam sei der **IPS-Einsatz in unübersichtlichen Gebäuden**. Mit einem „Asset Tracking" könne man die Position wichtiger Gegenstände wie etwa Diagnosegeräte in einem Krankenhaus ermitteln. Mit einem solchen „Locator Tag", der Signale an ein zentrales Serversystem aussendet, seien teure Medizinalgeräte auch gegen Diebstahl besser geschützt. In Form einer Armbinde könne so auch die Sicherheit von dementen/unzurechnungsfähigen Patienten oder von Mitarbeitern auf risikoreichen Arbeitsplätzen wie Labors besser gewährleistet werden. Besuchern eines Firmengebäudes könne ein Badge ausgehändigt werden, um sie orten zu können. So könne man verhindern, dass sie unbemerkt sensible Bereiche aufsuchen. Im Fall eines Sicherheitsvorfalls zeige das Gerät den schnellsten und unverstellten Fluchtweg an.

Verschlüsselung

Golem.de meldet, Google wolle mehr Webseitenbetreiber unter Druck setzen, auf HTTPS-Verbindungen umzusteigen. Ab Sommer 2018 sollen Webseiten ohne Verschlüsselung generell als unsicher markiert werden. Googles Chrome-Browser werde ab Juli alle Webseiten ohne HTTPS-Verschlüsselung in der Adressleiste mit dem „Unsicher"-Tag versehen. Nach Angaben von Google sind mittlerweile 68 Prozent des Chrome-Traffics unter Android und Windows verschlüsselt, unter MacOS und Chrome OS sollen es sogar über 78 Prozent sein. Außerdem verwendeten mittlerweile 81 der Top 100-Seiten standardmäßig HTTPS.

Videoüberwachung

heise.de meldet am 19. Februar, das „**Bündnis für mehr Videoüberwachung in Berlin"** versuche mit 25.083 Unterschriften ein Volksbegehren zu erzwingen. Ihr Ziel: 50 öffentliche Plätze der Hauptstadt sollen künftig per Kameras rund um die Uhr überwacht werden. Darüber hinaus sei die Überwachung von Fahrradabstellplätzen und Großveranstaltungen im Gespräch – mit insgesamt 2.000 bis 2.500 zusätzlichen Kameras im Stadtgebiet. Laut einer Forsa-Umfrage im Auftrag der Berliner Zeitung wünschten sich 80 Prozent der Berliner eine stärkere Videoüberwachung an Bahnhöfen und öffentlichen Plätzen. Als Beweggründe würden die Befragten ihr Sicherheitsempfinden anführen.

Einsatzgebiete der Wärmebildtechnik beleuchtet Dahua in PROTECTOR, Ausgabe 3-2018, S. 34/35. Dahua habe Wärmebildkameras mit neuartigen Funktionen entwickelt. Diese seien geeignet, sichtbares Licht mit Infrarotlicht zu kombinieren und so eine effektive Überwachung unter allen Lichtbedingungen zu ermöglichen. Zum Perimeterschutz könne im Abstand von einem Kilometer jeweils eine „Termal Dome Camera" mit 30-fachem Zoom montiert werden. Sie könne Bedrohungen mit Bildern aus dem sichtbaren Spektrum verifizieren. Ein intelligentes Waldbrand-Detektionssystem von Dahua überwache automatisch die gesamte Waldfläche und biete dazu „intelligente Wächterrundgänge". Ein weiteres intelligentes System diene der Überwachung von Umspannwerken.

Wohnungseinbruch

In einem Aufsatz über den **Modus operandi bei „reisenden und zugereisten" Tätern** des Wohnungseinbruchs in der Fachzeitschrift DIE POLIZEI, Ausgabe 2-2018, S. 42–49, ziehen die Soziologin Gina Rosa Wollinger und die Kulturwissenschaftlerin Dr. Nadine Jukschat, beide Kriminologisches Forschungsinstitut Niedersachsen e.V., aus qualitativen Interviews mit 30 verurteilten Tätern Konsequenzen für die Prävention. Hilfreich seien vor allem mechanische Sicherungsmechanismen wie zusätzliche Tür- und Fenstersicherungen. Die Einfachheit, Türen und Fenster von außen zu öffnen, sei in den Interviews oftmals mit als Tatanreiz genannt worden. Vermehrt seien Kunststofftüren als Schwachstelle genannt worden. Alarmanlagen und die Installation von Videokameras hätten eine Abschreckungswirkung auf eher unprofessionelle und vorsichtige Täter. Bei den routinierten Tätern laufe diese Maßnahme allerdings ins Leere. Generell abschreckend hingegen wirkten Anzeichen dafür, dass sich Bewohner im Haus bzw. der Wohnung aufhalten, aber auch nachbarschaftliche Kontrolle. In Interviews sei eine deutliche Skepsis hinsichtlich der Abschreckungswirkung hoher Strafen gezeigt worden.

Zutrittskontrolle

Hagen Zumpe, SALTO Systems GmbH, erläutert in der Ausgabe 3-2018 von PROTECTOR, S. 26/27, **Bluetooth als Basis funkvernetzter Systeme**. Es finde für die Übertragung mobiler Schlüssel in Zutrittslösungen bereits breite Verwendung. Doch die Technologie werde inzwischen auch als Basis für die Funkvernetzung von kabellosen Zutrittskomponenten genutzt. Die Bluetooth-Technologie biete in erster Linie eine stabile Kommunikation zwischen den Hardwarekomponenten. Denn die Chips wählten permanent die besten Übertragungskanäle abhängig von den Umgebungsbedingungen und der Belegung. Zugleich punkte Bluetooth mit hoher Übertragungsgeschwindigkeit, großer Datenrate und geringer Latenz, was wesentlich zu einem zuverlässigen Betrieb beitrage. Bereits mit dem Standard ab 4.0 (Bluetooth Low Energy) hätten die Chips erstmals sinnvoll in Offline-Türkomponenten eingesetzt werden können. Die Version 5.0 reduziere den Energieverbrauch noch einmal. Auch für das Produktdesign bringe der Einsatz einer Funkvernetzung über Bluetooth eine Reihe von Vorteilen. Bluetooth als Übertragungstechnologie in Wireless-Systemen weise insbesondere gegenüber einer Vernetzung über WLAN deutliche Vorteile auf.

PROTECTOR enthält in der Ausgabe 3-2018, S. 32–33, eine **Marktübersicht** über 83 Systeme von **Vereinzelungsanlagen** von 21 Anbietern. Zu den in der Übersicht ausgewiesenen Kriterien zählen: Sicherheitsniveau, Durchgangsfrequenz, Maße, Schnittstellen, Steuerung, Vereinzelung mechanisch oder elektronisch, Mögliche Fluchtwegintegration, Stromausfallverhalten, Erweiterungsmöglichkeiten.

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