Focus on Security

Ausgabe 02, Februar 2017

SECURITAS

Inhalt

Arbeitsschutz

Die am 3. Dezember 2016 in Kraft getretene **Arbeitsstättenverordnung** bringe mehr Klarheit für Unternehmen, heißt es in der Ausgabe 1-2/2017 der Zeitschrift GIT, S. 84. Neu aufgenommen worden seien u. a. Regelungen zu Telearbeitsplätzen. Weiterhin habe eine Konkretisierung im Bereich der Arbeitsschutz-Unterweisung stattgefunden.

Brandschutz

Siemens habe bei den VdS-Brandschutztagen ein umfassendes Portfolio an technischen **Brandschutzlösungen aus einer ganzheitlichen und gewerkeübergreifenden Perspektive** präsentiert, meldet GIT in der Ausgabe 1-2/2017, S. 79. Zwei Neuentwicklungen hätten dabei besonders im Fokus gestanden: eine neue Brandschutzklappensteuerung und optische Signalgeber gemäß der neuen Norm EN54-23. Die von Brandschutz- und Lüftungsexperten des Siemens-Division Building Technologies gemeinsam entwickelte Brandschutzklappensteuerung sei Kernbestandteil des intelligenten, zuverlässigen Gesamtkonzeptes zum Brandschutz in Gebäuden. Sie lasse sich leicht in Brandschutzanlagen, Managementplattformen und Automatisierungsstationen von Siemens einbinden. Ebenfalls neu sei ein Zwischensockel-Sounder, der speziell die Anforderungen an eine optische Alarmierung gemäß der aktuellen Norm EN54-23 erfülle. Dieser loopgespeiste Zwischensockel-Sounder könne zwischen einem automatischen Brandmelder und dessen Anschlusssockel installiert werden. So werde aus einem „normalen" Brandmelder ein optisch-akustischer Signalgeber.

Christian Rahbari, Pyrexx, befasst sich in der Ausgabe 1-2/2017 der Zeitschrift GIT, S. 80/81, mit der **Wartung von Rauchwarnmeldern**. Spätestens ab Ende 2020 (Berlin und Brandenburg) sollten in jeder Wohnung im Bundesgebiet Rauchmelder vorhanden sein. Gebäudeversicherungen hätten angekündigt, nicht zu zahlen, wenn keine funktionierenden Rauchmelder installiert waren. Nur wer sich regelmäßig (einmal im Jahr nach DIN 14676) um die Rauchmelder kümmere, werde sie wohl auch zehn Jahre als funktionierende Geräte nutzen können. Nur das gesamte Paket auf DIN-konformer Installation der Melder, jährlicher Wartung, Brandschau auf den Fluchtwegen und schriftlicher Dokumentation über die durchgeführten Maßnahmen sorge für Sicherheit. Für Eigenheimbesitzer habe die Firma Pyrexx ein IP-Gateway mit Funkrauchwarnmeldern entwickelt, das mehrere Einsatzmöglichkeiten biete. Damit würden dem Nutzer weitere Möglichkeiten wie die Dokumentation und Nachweispflicht über die dazugehörige App für Versicherungen im Schadensfall oder die Weiterleitung des Alarmes an diverse Endgeräte gegeben. Grundsätzlich könne für Eigenheimbesitzer, die nicht über einen Fachdienstleister betreut werden, auch die Wartungs-Web-App empfehlenswert sein. Hier könnten mit Hilfe von Raumskizzen die Montageorte der Rauchmelder genau eingetragen werden. Zusätzlich frage die App alle wartungsrelevanten Handlungen nach DIN 14676 ab, die vom Nutzer eingetragen werden können. Einmal im Jahr melde sich die App und erinnere ihren Nutzer an die Wartung der Geräte.

Datenschutz

Die Bundesregierung müsse beim Datenschutz massiv nachbessern, sind der EU-Abgeordnete Till Steffen und der Hamburger Justizsenator Jan Philipp Albrecht in der FAZ am 29. Dezember 2016 überzeugt. Die vom BMI vorgelegten Regelungen zur Anpassung des Datenschutzrechts an die Vorgaben der Europäischen Datenschutz-Grundverordnung seien von dem Geist geprägt, die neuen europäischen Standards durch nationale

Gesetzesbestimmungen zu Lasten der Verbraucher zu unterlaufen. Zu diesem Zweck überdehne das BMI in unzulässiger Weise die in der Datenschutz-Grundverordnung vorgesehenen Grenzen für nationale Anpassungsmöglichkeiten. Das BMI wolle mit seinen Vorschlägen datenhungrigen Großkonzernen etwa erlauben, personenbezogene Daten zu völlig anderen Zwecken zu verarbeiten als die, für die sie ursprünglich erhoben wurden, zum Beispiel für Werbung, Kreditwürdigkeitsabschätzung oder zur Meinungsmanipulation in sozialen Medien. Der Referentenentwurf schränke darüber hinaus die in der Datenschutz-Grundverordnung vorgesehenen Informationspflichten von Internetunternehmen ein. Er schaffe ein Einfallstor für Unternehmen, Betroffene erst gar nicht zu informieren und damit auch eine Überprüfung der Datenverarbeitungspraxis gänzlich zu vermeiden. Datenschutz und Datensicherheit seien für die ganz große Mehrheit der Unternehmen von größter Bedeutung. Es seien allein die wenigen marktbeherrschenden Global Player, die mit ihren Big-Data-Geschäftsmodellen ein nachhaltiges Interesse an fehlenden Standards haben dürften.

Nach Einschätzung des DGB werde im Vergleich zu den geltenden Regeln im BDSG die **Videoüberwachung von öffentlich zugänglichen Räumen** nach den Vorgaben der EU-Datenschutzgrundverordnung in größerem Umfang und „nach zum Teil deutlich weniger strengen Voraussetzungen zulässig sein" (FAZ vom 29. Dezember 2016). Nach heutigem Recht sei die Videoüberwachung nur zulässig, wenn der Arbeitgeber sein Hausrecht wahrnehmen will oder wenn er berechtigte Interessen für konkret festgelegte Zwecke wahren will. Im neuen Recht gebe es dagegen Schutz nur gegen „systematische" und „umfangreiche" Videoüberwachung als Datenverarbeitung. Auch punktuelle Videoüberwachung in Betrieben und Ladenlokalen werde künftig häufiger erlaubt als bisher. Der DGB fordere das BMI nun auf, entsprechende Schutzvorschriften in den Entwurf aufzunehmen. Die Gewerkschaften würden für ein eigenständiges Beschäftigtendatenschutzgesetz werben.

Zeit.de meldet am 25. Januar, Microsoft müsse US-Behörden keinen Zugang zu **Nutzerdaten im Ausland** gewähren. Das habe ein Berufungsgericht in New York entschieden. Die Bundesrichter hätten damit ein vorheriges Urteil bestätigt und einen Antrag der US-Regierung gegen die Entscheidung abgelehnt. Hintergrund des Rechtsstreits sei eine Aufforderung der US-Behörden an Microsoft aus dem Jahr 2013 gewesen, E-Mails eines mutmaßlichen Drogenhändlers herauszugeben. Das Unternehmen habe jedoch nur die in den USA gespeicherten Accountdaten zur Verfügung gestellt. Die Freigabe der E-Mails selbst habe Microsoft mit der Begründung verweigert, diese seien auf einem Server in Irland abgelegt.

Drohnen

Die Bundesregierung verschärfe die Regeln für die Nutzung von privaten Drohnen, berichtet die FAZ am 19. Januar. Nach einer **Verordnung** von Bundesverkehrsminister Dobrindt, die das Kabinett **am 18. Januar beschlossen** habe, müssten solche unbemannten Fluggeräte künftig mit Namen und Adresse des Eigentümers gekennzeichnet werden, wenn sie mehr als 250 Gramm wiegen. Für schwerere Modelle würden künftig eine Art Führerschein und Betriebserlaubnis gefordert. Wer eine Drohne mit mindestens zwei Kilo Gewicht nutzt, müsse seine Kenntnisse über eine Pilotenlizenz oder die Einweisung durch einen Luftsportverein nachweisen. Für Drohnen mit mehr als fünf Kilo werde eine behördliche Betriebserlaubnis vorgeschrieben. Zurzeit sei die Nutzung in der Nähe von Flughäfen verboten. Mit der Verordnung werde das Verbot auf fremde Wohngrundstücke ausgeweitet. Für gewerbliche Nutzer werde das generelle Verbot aber

aufgehoben. Künftig könne ein Betrieb in mehr als 100 Meter Höhe von der Luftfahrtbehörde genehmigt werden.

Mehrere Autoren befassen sich in der Ausgabe 1-2017 der Fachzeitschrift Polizei Verkehr + Technik, S. 20–26, mit der **Drohnen-Problematik**. Achim Friedl weist auf eine repräsentative Umfrage des Bundesverbandes der Deutschen Luftverkehrswirtschaft e. V. im Juli 2016 hin. Danach akzeptieren 88 Prozent der Befragten den Einsatz zur Überwachung von Staatsgrenzen, 77 Prozent den Einsatz zur Überwachung von Industrieanlagen und 68 Prozent zur Überwachung der Sicherheit öffentlicher Räume. 84 Prozent benennen als Problem die Störung der Privatsphäre, 77 Prozent gezielte terroristische Anschläge und kriminelle Taten und 53 Prozent eine Lärmbelästigung. Prof. Dr. Wolfgang Koch vom Fraunhofer FKIE betont, dass der Multisensordatenfusion und dem Management der Sensoren bei der Drohnenabwehr eine Schlüsselrolle zufalle. Die Lösung der Problematik setze eine enge Kooperation der polizeilichen Nutzer, der Forschungsinstitute und der Industrie voraus. Wolfgang Strehmel, BKA, ist überzeugt, dass die Polizei einen hohen technischen Nachholbedarf bei der Detektion und Abwehr von Drohnen hat. Die komplexe und neue technische Herausforderung sei von einer hohen Asymmetrie geprägt. Die Polizeien der Länder und des Bundes hätten einen hohen administrativen, personellen und finanziellen Aufwand, um einem Bedrohungspotenzial zu begegnen, das mit geringem Aufwand realisiert werden könne. Christian Jäger, SG Elektroniksystem- und Logistik-GmbH, benennt Komponenten eines Drohnendetektions- und Abwehrsystems: Führungs- und Legedarstellungssystem, Drohnen-Detektionsradar, Akustiksensor, Fernbedienungsdetektion, Tag-/Nachtsicht-Kamera, Fernbedienungs-Jammer, GPS-Jammer, elektromagnetische Störquelle, Transport- und Integrationsplattform.

Einbruchschutz

Tresorverkäufer melden Absatzrekorde, meldet die FAZ am 21. Dezember. 2013 habe die Firma Eisenbach 11.800 Sicherheitsbehälter verkauft. Im aktuellen Geschäftsjahr dürften es fast dreimal so viele werden. Die große Nachfrage nach dem staatlichen Förderprogramm passe ins Bild. Für 2017 wolle die Bundesregierung das Programm noch einmal auf 50 Mio. Euro aufstocken. Wichtigster Grund für das gestiegene Sicherheitsbedürfnis dürften die immer weiter steigenden Einbruchzahlen sein. Hinzu komme, dass gerade auf dem Land immer mehr Bankfilialen schließen und mit ihnen jedes Mal eine Reihe von Schließfächern wegfällt. Wer einen Tresor kaufen will, solle in jedem Fall vorher mit seinem Versicherer reden. Denn die Hausratversicherung greife nicht automatisch. Bei der R+V-Versicherung zum Beispiel gelte der zusätzliche Schutz erst, wenn der Tresor mindestens 200 kg schwer ist. Leichtere Behälter würden in der Branche eher als zusätzliches Risiko gelten, weil der Einbrecher bei ihnen ohne großes Suchen alle Wertgegenstände gesammelt vorfinde. Außerdem müsse der Tresor mit einem sogenannten Zertifikat des VdS oder des ECB-S versehen sein.

Am 2. Februar berichtet auch die FAZ, die 10 Mio. Euro, die die Förderbank KfW in Form von Zuschüssen etwa zum Einbau neuer Türen und Fenster bereitgestellt habe, seien schon im Herbst aufgebraucht gewesen. 2017 stünden 50 Mio. Euro bereit, und die Nachfrage sei ungebrochen hoch. Interessenten könnten die Mittel nun direkt über ein Internetportal anfordern. Die Investitionen müssten mindestens 2.000 Euro umfassen. Zehn Prozent könnten dann von der KfW bezuschusst werden.

Ex- und Importkontrolle

Wie die Wochenzeitung DAS PARLAMENT am 23. Januar berichtet, hat der Bundestag am 19. Januar ein Gesetz zur Änderung des Zollverwaltungsgesetzes beschlossen. Ziel des Gesetzes sei es, die Ein- und Ausfuhr illegaler Waren auf dem Postweg besser zu kontrollieren und illegale Bargeldtransfers über die Grenze hinweg besser aufzuspüren. Die Neuregelungen räumten dem Zoll mehr Kontrollmöglichkeiten ein. **Änderungen** seien vor allem **im Postverkehr** vorgesehen, wo bislang nur die Deutsche Post verpflichtet sei, der Zollverwaltung Sendungen vorzulegen, bei denen Anhaltspunkte für einen Verstoß gegen ein Einfuhr-, Durchfuhr- oder Ausfuhrverbot bestehen. Diese Vorschrift werde auf alle Postdienstleister erweitert. Zudem sollten Mitarbeiter der Zollverwaltung in den Geschäftsräumen der Postdienstleister risikoorientierte und stichprobenartige Kontrollen vornehmen können.

Falschgeldkriminalität

Wie die Bundesbank mitteilt, hat sie **2016 82.200 falsche Euro-Banknoten** aus dem Verkehr gezogen (FAZ vom 28. Januar). Das waren 14 Prozent weniger als 2015. Auffällig sei der Rückgang bei den 20-Euro-Fälschungen, deren Anzahl sich fast halbiert habe. Die Bundesbank führe dies auf verbesserte Sicherheitsmerkmale der neuen 20-Euro-Serie zurück. Insgesamt hätten die sichergestellten Fälschungen 2016 einen Nennwert von 4,2 Mio. Euro nach 4,4 Mio. Euro 2015 gehabt. Damals seien so viele Fälschungen gefunden worden wie noch nie seit Euro-Einführung, nämlich 95.400. Auch im Euroraum sei die Zahl der Blüten 2016 zurückgegangen. Es seien 684.000 Fälschungen ermittelt worden, knapp ein Viertel weniger als 2015. Das Falschgeldaufkommen in Deutschland bleibe auf einem niedrigen Niveau. Rechnerisch seien 2016 zehn falsche Banknoten auf 10.000 Einwohner entfallen. Von April 2017 an würden neue 50-Euro-Scheine mit besseren Sicherheitsmerkmalen in Umlauf gebracht werden, unter anderem wie beim 20-Euro-Schein das durchsichtige Porträtfenster im Hologramm und die „Smaragdzahl". Der 50-Euro-Schein sei mit 50.000 Blüten 2016 das beliebteste Fälschungsobjekt gewesen.

Geldautomatensicherheit

Kriminelle haben mit dem Ausspähen sensibler Daten von Bankkunden auch 2016 einen Millionenschaden angerichtet, berichtet die FAZ am 10. Januar. Doch mit gut 1,9 Mio. Euro sei der Bruttoschaden durch „Skimming"-Angriffe auf ein Rekordtief gefallen, obwohl die Datendiebe 159 Geldautomaten manipuliert hätten, während 2015 nur 118 Fälle registriert worden seien. Ein größeres Problem stelle der Diebstahl und Verlust von Zahlungskarten dar: 12.373 seien 2016 gezählt worden (2015: 12.669). Offenbar bewahrten viele Verbraucher nach wie vor Karte und PIN zusammen auf – entgegen aller Warnungen.

Geldwäsche

Die Einführung eines sogenannten **Transparenzregisters im Kampf gegen Geldwäsche** und Terrorfinanzierung stoße bei Unternehmern auf große Sorge, schreibt die WirtschaftsWoche am 6. Januar. Dabei gehe es um die Eintragung der wirtschaftlich Berechtigten bei Firmen und Stiftungen in ein öffentliches Register. Familienunternehmer müssten sich durch Veröffentlichung privater Daten um Erpressung und Entführung sorgen, sage Lutz Goebel vom Verband „Die Familienunternehmer". Das BMF verliere mit seinem Entwurf zum Geldwäschebekämpfungsgesetz jegliches Augenmaß. Hier werde weder der grundrechtliche Schutz auf

informationelle Selbstbestimmung gewahrt noch jegliche Verhältnismäßigkeit im Hinblick auf das Ziel der Geldwäschebekämpfung. Das BMF weise dagegen darauf hin, dass auf Antrag die registerführende Stelle die Einsichtnahme in das Register beschränken könne. Allerdings müsse nachgewiesen werden, dass die Veröffentlichung unzumutbar ist.

Insiderhandel

Inkerman Fraud Weekly weist in der Ausgabe 190 auf einen Bericht der Sicherheitsanalysten von RedOwl und IntSights hin, der auf beispiellose Risiken im Kontext des Insiderhandels verweise. Mitarbeiter und Auftragnehmer vieler Firmen griffen nach dem Bericht immer häufiger auf das Darkweb zurück, um aus Unternehmensinformationen Geld zu machen. Gefunden worden seien illegale Foren, auf denen Firmenangehörige mit Insiderwissen aktiv dazu rekrutiert wurden, für eine Gewinnbeteiligung Daten zum Insiderhandel an der Börse oder zu anderen Arten des illegalen Handels zu stehlen. Ein besonders aktives Forum nenne sich „Kickass-Marketplace", wo Insiderinformationen über den generellen Aktienmarkt, Währungsgeschäfte und zum Rohstoffhandel ausgetauscht würden. Der Zugang zum Forum sei exklusiv und der Mitgliedsbeitrag von 1 Bitcoin recht hoch. Neben dem Beitrittsgeld hätten potenzielle Mitglieder zudem beweisen müssen, dass sie tatsächlich Zugang zu Unternehmensinformationen hatten.

Nach einem Bericht in der FAZ am 7. Februar bestätigt die Bafin einen **kontinuierlichen Anstieg von Verdachtsfällen** des Insiderhandels und der Marktmanipulation. 2016 hätten 713 Analysen stattgefunden, nach 570 im Jahr 2015. Insgesamt habe die Bafin 127 Anzeigen erstattet: 21 von ihnen, mit 49 betroffenen Personen, bezogen auf den Insiderhandel, 106 Anzeigen mit 275 Personen auf Marktmanipulation. Verurteilungen habe es aber 2016 kaum gegeben: zwei wegen Insiderhandel, 23 wegen Marktmanipulation. 2016 hätten sich aufgrund von EU-Direktiven auch in Deutschland die Bestimmungen verschärft. Schon der Versuch einer Marktmanipulation könne bestraft werden, schwere Fälle gelten als Verbrechen. Die Definition des Insiderhandels sei erweitert worden. Die Bafin verfüge auf ihrer Internetseite über ein anonymes Hinweisgebersystem und müsse Verstöße veröffentlichen. Leider komme es in vielen Fällen gar nicht zur Klärung der Rechtsfrage vor Gericht, weil Beschuldigte lieber mehrere hunderttausend Euro als Geldauflage zur Einstellung des Strafverfahrens zahlen würden. Die Reputation sei extrem wichtig für die persönliche Berufsperspektive.

Internet der Dinge (IoT)

Tillmann Braun berichtet am 27. Januar in silicon.de über die **„IoT Expo" in London**. Das US-Unternehmen Daqri habe einen neuen „Smart Helmet" präsentiert, der unter anderem mit einem Klarsicht-Display sowie diversen Sensoren und Kameras ausgestattet sei, darunter eine „Thermal Camera". Mit deren Hilfe würden unter anderem Gefahrenquellen wie heiße Rohre und andere Wärmequellen über das Display im Visier des Helms sichtbar, die mit dem bloßen Auge nicht ohne Weiteres erkannt werden könnten. Dass Daten auch auf anderen Wegen übertragen werden können als per Kabel, Wi-Fi oder Bluetooth, beweise das Unternehmen Chirp. Dessen Verfahren, bei denen Daten per Audio-Technologie übermittelt werden, würde unter anderem in einem KW von EDF in Frankreich eingesetzt. Chirp eigne sich vor allem dann, wenn altbekannte Ansätze keine Option sind. Dazu gehörten auch bestimmte Einsatzgebiete wie Kernkraftwerke. Denn in diesen dürften aus Sicherheitsgründen keine Funkfrequenzen eingesetzt werden, und damit auch kein Wi-Fi, Bluetooth und ähnliche Standards. Der Vorteil gegenüber Lösungen wie Infrarot sei, dass mit

Chirp Daten selbst dann übermittelt werden könnten, wenn sich Gegenstände zwischen Sender und Empfänger befinden.

IT-Sicherheit

Es gebe **weniger Schwachstellen in Softwareprogrammen**, meldet die FAZ am 12. Januar. Während im Internet nach wie vor massenhaft Viren, Würmer und Trojaner auftauchen und die Zahl der schweren Hackerangriffe unverändert hoch sei, sinke die Zahl der Schwachstellen in Softwareprogrammen. Wie das Hasso-Plattner-Institut (HPI) in Potsdam mitteilte, hätten die Forscher nach 7.310 Lücken 2014 und 6.354 Lücken 2015 im Jahr 2016 nur 5.577 Lücken registriert. Der wirtschaftliche Schaden, den kriminelle Hacker allein in Deutschland jedes Jahr verursachen, werde auf rund 50 Mrd. Euro beziffert. Dem stünden Investitionen im niedrigen einstelligen Milliardenbereich gegenüber, die hierzulande in Softwaresicherheit gesteckt würden.

Die Unternehmenswelt habe es nicht geschafft, eine funktionierende Sicherheitsarchitektur zu entwickeln, heißt es in der FAZ am 14. Januar. Niemand merke sich gerne Passwörter. **Zweifaktor-Authentifizierung müsse Standard werden**. Wer seine Identität in sicheren Händen wissen will, dürfe nicht nur auf die neuesten Entwicklungen der Sicherheitsbranche warten. Der verantwortungsbewusste Nutzer müsse schon offline entscheiden, welche Daten er mit wem und wo teilen möchte.

Peter Marwan berichtet in silicon.de am 25. Januar, die aktuellste Version von Firefox weise deutlicher auf potenziell unsichere Log-in-Seiten hin. Passwörter, die Nutzer in Formulare eingeben, könnten sich Nutzer nun vor der Speicherung anzeigen lassen. Der Passwortmanager des Browsers merke sich nun Eingaben auch dann, wenn ein Formular das „Submit"-Ereignis nicht unterstützt. Außerdem weise Firefox bei Websites, auf denen Passwörter eingegeben werden können, nun deutlicher auf potenzielle Sicherheitsrisiken hin. Von den mit Firefox 51 geschlossenen 24 Schwachstellen würden sechs als kritisch eingestuft. Von weiteren sechs gehe immerhin noch ein hohes Risiko aus.

Neue Paradigmen in der IT-Sicherheit seien unabdingbar, zeigt sich Peter Rost, Rohde & Schwarz Cybersecurity GmbH, in der Ausgabe 1-2/2017 der Fachzeitschrift GIT, S. 72/73, überzeugt. Die Cyberangriffe seien deshalb so gefährlich, weil auch die Anzahl der vernetzten Geräte weiter steige. Das liege nicht zuletzt am Internet der Dinge, das heißt der zunehmenden Vernetzung von Geräten, Sensoren etc. über IP-Netze. Täglich würden rund 360.000 neue Viren entdeckt. Das Erschreckende: 27 Prozent der Malware bleibe in den ersten drei Tagen nach dem Fund unentdeckt. Der Wechsel von reaktiven hin zu proaktiven Lösungen sei in der Cybersicherheit unabdingbar. Ein Beispiel sei der Endpoint-Schutz. Rund 70 Prozent der Malware würden über den Browser in das Netzwerk eindringen. Proaktive Endpoint-Lösungen arbeiteten mit dem Prinzip der Separierung. Der Browser werde im PC virtualisiert und von allen anderen Daten und Anwendungen im Endpoint und Intranet hermetisch getrennt. Das verkleinere die Angriffsfläche für Windows- und Linux-Malware enorm und Unternehmensdaten seien für Angreifer wie etwa Ransomware unsichtbar. Das Prinzip könne auch auf Smartphones und Tablets umfassenden Schutz bieten. Neue Sicherheitskonzepte basierten auf dem technologischen Ansatz **„Security by Design".** Der Paradigmenwechsel erfasse auch die Netzwerksicherheit. Während alte Firewall-Technologien reaktiv arbeiteten („Black-Lists"), setze die Next-Generation Firewalls um, bei denen Datenpakete proaktiv geprüft werden. Nur wenn diese sich als gutwillig identifizieren könnten, dürften sie passieren („Whitelisting").

IuK-Kriminalität

Silicon.de weist am 30. Dezember auf eine von PwC durchgeführte Umfrage hin, nach der 22 Prozent der Befragten angaben, schon Opfer von Identitätsdiebstahl geworden zu sein. Weitere 21 Prozent hätten angegeben, dass ihre E-Mail-Adresse für den Versand von Spam-Mails missbraucht worden sei. Wer den Verdacht habe, dass seine Daten von anderen verwendet werden, könne zum Beispiel das vom Potsdamer Hasso-Plattner-Institut angebotene, kostenlose Online-Tool Identity Leak Checker nutzen. Und ein sicheres Passwort helfe auch, zu verhindern, dass Fremde den eigenen Account übernehmen.

Android-Malware Switcher hackt WLAN-Router und ändert das DNS, titelt silicon.de am 1. Januar. Nutzer, die danach darüber ins Netz gehen, glaubten, auf der korrekten Website eines von ihnen genutzten Angebots zu sein. Sofern sie jedoch Log-in-Daten, Passwörter oder Kreditkarteninformationen eingeben, fielen diese Kriminellen in die Hände. Wie Kaspersky-Experte Alex Drozhzhin erkläre, ändert die Malware Switcher dazu die Einstellungen im Router. Für die Nutzer sei die neue Angriffsmethode nur schwer durchschaubar, denn letztendlich sei dabei dann die gefälschte Website auf einer legitimen Seite gehostet. Erreicht werde das dadurch, dass die Kriminellen ihren eigenen DNS-Server erstellen und mittels DNS-Hijacking Anfragen umleiten. Zunächst ahmten die Angreifer dazu bekannte und gängige Android-Apps nach. Sobald sich ein Nutzer diese Fake-App heruntergeladen habe und sich in einem WLAN befinde, kommuniziert der Schadcode mit einem Command and Control-Server. Ihm berichte er dann, dass der Trojaner in einem bestimmten Netzwerk aktiviert wurde und stellt eine Netzwerk-ID bereit. Dann versuche Switcher, den WLAN-Router zu hacken. Dazu teste er gängige Anmeldedaten, um sich einzuloggen. Habe der Trojaner die Anmeldedaten herausgefunden, rufe er die Einstellungsseite des Routers auf und ändere die Standard-DNS-Serveradresse zu einer von den Kriminellen genutzten. Kaspersky rate, bei der Einrichtung eines WLAN-Routers stets das Standardpasswort zu ändern und ein ausreichend komplexes, neues zu wählen.

Heise.de meldet am 10. Januar, über tausend deutsche Online-Shops seien laut BSI-Informationen so manipuliert, dass Kundendaten und Zahlungsinformationen beim Bestellvorgang an **Online-Kriminelle** weitergeleitet würden. Betroffen seien Shop-Betreiber, welche die Online-Shopsoftware Magento in veralteten und akut angreifbaren Versionen einsetzen: Darin würden kritische Sicherheitslücken klaffen, durch die sich die Angreifer mit beliebigen Codes in die Shops einschleusen könnten. Die von Angreifern ausgenutzten **Sicherheitslücken in Magento** seien von den Shop-Betreibern trotz vorhandener Softwareupdates offenbar nicht geschlossen worden. Das BSI weise darauf hin, dass Betreiber von Online-Shops nach § 13 Abs. 7 Telemediengesetz verpflichtet seien, ihre Systeme nach dem Stand der Technik gegen Angriffe zu schützen. Eine grundlegende und wirksame Maßnahme hierzu sei das regelmäßige und schnelle Einspielen von verfügbaren Sicherheitsupdates.

Die Bundesregierung wolle eine internationale Allianz schmieden, um Anschläge aus dem Internet auf einzelne Banken und den gesamten Geldkreislauf zu verhindern, berichtet die FAZ am 25. Januar. **Cyberattacken auf Finanzinstitute** seien nicht das Problem einzelner Institute. Sie seien ein Angriff auf die Integrität des internationalen Finanzsystems. Kriminellen eröffneten sich ganz neue Betätigungsfelder, wenn immer mehr Informationen über einzelne Menschen öffentlich werden könnten. Die internationalen Finanzmärkte seien eng miteinander vernetzt. Das führe dazu, dass eine Attacke auf ein einzelnes Institut immer auch Auswirkungen auf andere Institute und Staaten habe. In einem ersten Schritt wolle die Bundesregierung erreichen, dass die Finanzmärkte widerstandsfähiger

gegen Angriffe aus dem Internet werden. Dazu gehöre nach ihrer Einschätzung eine Art Bestandsaufnahme, um bestehende Sicherheitslücken zu identifizieren.

Katastrophen

Wie die FAZ am 5. Januar berichtet, haben **Stürme und Erdbeben 2016** zu den höchsten Schäden aus Naturkatastrophen seit vier Jahren geführt. Sie hätten sich auf 175 Mrd. Dollar summiert, gut zwei Drittel mehr als im eher schadensarmen, vorvergangenen Jahr, wie die Fachleute von München Re errechnet hätten. Wie so oft habe es die ärmsten Länder besonders schwer getroffen. Einige wetterbedingte Katastrophen des Jahres 2016 zeigen, wie sich „ein ungebremster Klimawandel auswirken" könne. Nach Einschätzung von Peter Höppe, Leiter der Georisikoforschung bei der Munich Re, träten extreme Wetterereignisse wie Hitzewellen, Überflutungen und Stürme häufiger auf. Die Erderwärmung mache solche Unwetter in bestimmten Regionen immer wahrscheinlicher. Ein Übriges leisteten Klimaphänomene wie die Warmwasser-Phase El Ninjo oder die Kaltwasser-Phase La Ninja, die meist Hurrikane entstehen ließen. Im vergangenen Jahr sei Nordamerika mit 160 Schadensereignissen so oft getroffen worden wie in keinem Jahr zuvor. Der größte Anteil aller registrierten Schadenssummen sei nicht versichert. Die Versicherer zahlten „nur" rund 50 Mrd. Dollar, weniger als ein Drittel der Gesamtsumme von 175 Mrd. Euro. Die Schadensbilanz der Munich Re weise als teuerste Naturkatastrophe des Jahres 2016 zwei Erdbeben aus, die sich im April auf der südjapanischen Insel Kyushi ereigneten. In Europa hätten die Gewitter und Sturzfluten im Frühsommer die größten Schäden mit sechs Mrd. Dollar ausgelöst. Bei den Naturkatastrophen seien insgesamt 8.700 Menschen ums Leben gekommen. Diese Zahl habe erheblich unter dem Zehn-Jahres-Durchschnitt von 60.600 Toten gelegen.

Korruption

Sorge über Bestechlichkeit wächst, titelt die FAZ am 26. Januar. Die Sorge in Unternehmen um eine Zunahme der Bestechungen gehe aus einem Index über die wahrgenommene Korruption hervor, den Transparency International (TI) veröffentlicht habe. Deutschland belege weiterhin den zehnten Platz. Führungskräfte in Deutschland nähmen es allerdings als „zunehmend normal wahr, dass irreguläre Zahlungen an Verwaltungen gemacht werden, um bestimmte Vorgänge zu beschleunigen oder erst möglich zu machen". Seit 2012 habe sich Deutschland beim sogenannten Executive Opinion Survey des World Economic Forum kontinuierlich verschlechtert. TI fordere Deutschland auf, die aktuelle Präsidentschaft der Gruppe G20 zu nutzen, um diese zur Unterzeichnung strengerer Leitlinien zu bewegen und globale Standards für den Hinweisgeberschutz zu schaffen. Insbesondere rate TI zur Einführung eines verpflichtenden Lobbyregisters in Deutschland. 2011 habe die vorige Regierungskoalition entsprechende Anträge abgelehnt. Kritisiert worden sei seinerzeit, dass das Vertreten von Einzelinteressen nicht stigmatisiert werden dürfe. Derzeit existiere in Deutschland nur ein freiwilliges Lobbyregister, in das sich zudem nur Verbände und ihre Vertreter eintragen lassen können.

Krisenregionen

Zwölf Länder mit nahezu nicht vorhandener Gesundheitsinfrastruktur lägen in Afrika, vier im Nahen Osten, dazu Afghanistan, Nordkorea, Haiti und Guyana, berichtet die FAZ am 30. Dezember. Durch die Globalisierung ließen sich aber Geschäftsreisen in solche Staaten oft nicht vermeiden. Der Dienstleister **International SLOS** profitiere davon. Von den 12.000 Mitarbeitern des von Franzosen in Singapur gegründeten Unternehmens seien 100 in Neu-Isenburg tätig. Hilfe bei Evaku-

ierungen seien der Ausnahmefall. In mehr als 85 Prozent der Fälle gehe es um medizinische Themen, in weniger als 15 Prozent um Sicherheitsthemen, für die es eine Kooperation mit dem Spezialunternehmen Control Risks gebe. Den wachsenden Beratungsbedarf spüre das Unternehmen an allen Ecken und Enden. Neben der zunehmenden wirtschaftlichen Verflechtung sei das Thema Fürsorgepflicht ein Treiber. Außerdem seien Betriebsunterbrechungen für Unternehmen im Ausland ein bedeutsames Risiko. Ein europäisches Unternehmen habe vor einiger Zeit 160 Mitarbeiter nach Westafrika geschickt. 40 von ihnen seien an Malaria erkrankt. 27 Assistance-Center auf der Welt sammelten Informationen über die Qualität von Ärzten und Krankenhäusern. Konzerneigene Assistance-Dienstleister der Versicherer seien die bedeutendsten Wettbewerber von International SOS. Auch der ADAC habe einen eigenen Assisteur als Teil seiner Auslandskrankenversicherung aufgebaut.

Terroranschläge gehörten in der **Türkei** zum Alltag, vermerkt die WirtschaftsWoche am 13. Januar. Kürzlich seien auch noch 380 Manager verhaftet worden. Deutsche Unternehmer seien alarmiert. Vor den Anschlägen könne sich kein Unternehmen schützen. Erste Rückzüge gebe es zu vermelden. Deutschen Unternehmen machten die Terroranschläge zumindest psychisch zu schaffen. Viele Beschäftigte wollten das Land verlassen oder zumindest ihre Familie nach Deutschland bringen. Terror und politische Unsicherheit führten dazu, dass deutsche Unternehmen ihre Reisen limitierten. 6.500 Unternehmen aus Deutschland, mehr als aus jedem anderen Land der Welt, seien in der Türkei tätig.

Lithium-Batterien

Lithium sei reaktionsfreudig, in Verbindung mit Feuchtigkeit entzünde sich das Metall, schreibt die FAZ am 10. Januar. In Lithium-Ionen-Batterien liege es zwar in gebundener Form und nur in geringer Menge vor, kritisch sei aber die Temperaturentwicklung durch die hohe Energiedichte. Wenn also zunehmend Lithium-Stromspeicher mit hoher Kapazität im Straßenverkehr in Elektrofahrzeugen oder auch in Flurförderfahrzeugen verbaut sind, stünden die Behörden nach einem Unfall vor dem Problem: Wie wird ein beschädigter Akku sicher transportiert und entsorgt? **Lithium-Stromspeicher gehörten zur Gefahrgutklasse 9** und könnten mit entsprechender Kennzeichnung versendet werden. Wenn sie eine mechanische Beschädigung haben, sei das indes nicht mehr der Fall. Dann sei der Transport in Deutschland nur unter den von der BAM festgelegten Bedingungen erlaubt. Er müsse dort angemeldet werden. Die Autoindustrie sei an einer Lösung dieses Transportproblems höchst interessiert. Die RLG Reverse Logistics GmbH habe in Zusammenarbeit mit den Herstellern spezielle gasdichte Behälter entwickelt, in denen die kritischen Akkus für den Transport auf der Straße gefahrlos untergebracht werden könnten. Die RLG biete auch ein gesamtes Entsorgungskonzept an. Beschädigte Lithium-Akkus würden unter hoher Temperatur verbrannt. Dazu gebe es in Deutschland eine Anlage der Accurec Recycling GmbH in Mülheim an der Ruhr sowie eine der Nickelhütte Aue GmbH.

Luftverkehrssicherheit

Martin Schindler berichtet in silicon.de am 25. Januar, am Hamburger Flughafen „Helmut Schmidt" hätten nach dem Update eines Servers für über eine halbe Stunde keine Flüge mehr starten und landen können. Durch das Update sei es zu Ausfällen im zentralen Rechnersystem des Flughafens gekommen. Dadurch sei es nicht möglich gewesen, mit der Flugsicherung zu kommunizieren. Die Betreibergesellschaft habe sich daher aus Sicherheitsgründen dafür entschieden, den Flugverkehr in der Zeit zwischen 8.31 Uhr und etwa 9.00 Uhr einzustellen.

Maschinensicherheit

„Safe Motion" thematisiert Holger Goergen, Pilz GmbH & Co. KG, in der Ausgabe 1-2/2017 der Zeitschrift GIT, S. 89. Die Funktion „Safe Limited Speed" (SLS) werde im Maschinenbau aktiviert, wenn ein Mitarbeiter sich im Gefahrenbereich aufhalte. Es müsse ein definierter Übergang von der Betriebsgeschwindigkeit im Automatikbetrieb auf die reduzierte Geschwindigkeit im Einrichtbetrieb gewährleistet sein. Erkennt die Überwachungsfunktion eine Verletzung des Grenzwertes, müsse der Antrieb sicher abgeschaltet werden.

Flexible Gestaltung der Sicherheitstechnik auf allen Ebenen ist das Thema von Franz Kaufleitner, B&R Ind.-Elektronik GmbH, in GIT (Ausgabe 1-2/2017, S. 96/97). B&R entwickle ein Konzept, das völlig neue sicherheitstechnische Lösungen ermöglichen werde: sich selbst organisierende Sicherheitsnetzwerke auf der Basis von OPC United Architecture – einem M2M Kommunikationsprotokoll – und dem quelloffenen Sicherheitsprotokoll openSafety. Mit dieser Technologie werde es möglich sein, Maschinenteile oder ganze Maschinen aus dem Maschinennetzwerk zu entfernen oder zu ergänzen, ohne dass die Sicherheitstechnik neu programmiert werden müsse. Sogar sich selbst validierende Maschinenlinien seien denkbar. Werde ein neues Gerät an ein Maschinennetzwerk angeschlossen, komme zuerst OPC UA ins Spiel. Mit Hilfe der OPC UA-Securitymechanismen werde eine sichere Verbindung hergestellt. Das Gerät suche nach weiteren Servern, die Safety-Funktionen anbieten. Zum Einsatz kämen dabei die OPC UA-Mechanismen Discovery und Server Capability. Anschließend werde mit den OPC UA-Browsing-Services festgestellt, welche Funktionen mit welchen Attributen diese Server anbieten. Auf diese Weise erlange jeder OPC UA-Server ein vollständiges Bild des Netzwerkes, ohne dass eine einzige Zeile Code programmiert werden müsse. Der Autor befasst sich dann mit der automatischen Überprüfung der neuen Komponenten, dem Test der Reaktionszeiten und der automatischen Reaktion der Geräte. Das quelloffene Sicherheitsprotokoll openSafety könne prinzipiell jeden Feldbus und jedes Industrie-Ethernet-Netzwerk als Transportmedium nutzen.

Mehr als eine reine **Schutztürabsicherung** sei die MGB2 von Euchner. Sie stelle die konsequente Weiterentwicklung der weltweit erfolgreichen Multifunctional Gatebox MGB dar. Sie ermögliche es, alle relevanten Funktionen rund um die Schutztür in einem Gerät zu integrieren (GIT, Ausgabe 1-2/2017, S. 100).

Netzsicherheit

Patrick Molck-Ude gibt in silicon.de am 29. Januar einen Überblick über **Firmennetz-Trends 2017**. Die Digitalisierung verändere die Geschäftsmodelle in fast allen Branchen. Immer mehr Unternehmen nutzten Cloud-Dienste, vernetzten Produktionsmaschinen und ermöglichten ihren Mitarbeitern mobiles Arbeiten. Die Folgen: Der Datenverkehr in den Firmennetzwerken steige drastisch und herkömmliche Netzkonzepte stießen in Sachen Bandbreite, Verfügbarkeit und Sicherheit an ihre Grenzen. Deswegen hätten viele Netzanbieter und Unternehmen schon die Grundlagen gelegt, um die Netze zu modernisieren. Netzbetreiber arbeiteten weltweit daran, ihre Infrastruktur auf Basis des Internet-Protokolls zu vereinheitlichen. „All-IP" bewältige nicht nur höhere Netzlasten, sondern trenne auch die Dienste von der Physik und ermögliche so, diese schneller und ortsunabhängig bereitzustellen – auch im Bereich der Telefonie. So würden zentrale Telekommunikationsanlagen 2017 ihren Siegeszug fortsetzen. Multinationale Unternehmen kämen 2017 nicht mehr umhin, in ihrem Corporate WAN verschiedene Netztechnologien zu kombinieren. Nur so

könnten sie die richtige Balance zwischen Übertragungsqualität und Wirtschaftlichkeit finden. Für den Zugang zur MPLS-Plattform nutzten immer mehr Unternehmen auch kostengünstigere Internet-Verbindungen oder optimierte Internet-Overlays, zum Beispiel für kleinere Standorte. Gleichzeitig würden die Trends zum Cloud Computing und zur All-IP-Technologie den Einsatz von Multi-Layer-Netzen vorantreiben. In Rechenzentren kämen die beiden Virtualisierungstechnologien „Software-Defined Networking" (SDN) und „Network Functions Virtualization" (NFV) erfolgreich zum Einsatz. Sie virtualisierten die Netzsteuerung bzw. Netzfunktionen, die bisher an Spezialhardware gebunden waren. Dadurch ließen sich Netze zentral programmieren und Funktionen wie Firewalls, Gateways und Load-Balance als Software bereitstellen. 2017 werde die Nachfrage nach durchgehend performanter Vernetzung bei Hybrid-Cloud-Ansätzen steigen. Mehr und mehr Public-Cloud-Anbieter würden MPLS-Zugangspunkte anbieten. Mit der stetig steigenden Zahl mobiler Endgeräte werde es besonders für multinationale Unternehmen noch komplexer, die mobilen Netzzugänge in verschiedenen Ländern zu managen. Denn für jedes Land gebe es unterschiedliche Dienste, würden eigene Verträge und andere Prozesse gelten. Telekommunikation und IT würden noch stärker zusammenwachsen. Erste Unternehmen würden daher endgültig aus der IT-Strategie eine ITK-Strategie machen. Das Bewusstsein für die Bedeutung von Netzwerksicherheit steige. Die Netzmodernisierung stelle Unternehmen 2017 vor eine Vielzahl an technischen, organisatorischen und wirtschaftlichen Herausforderungen. Um diese zu meistern, benötigten sie einen Partner mit Kompetenzen aus den vier Bereichen Festnetz, Mobilfunk, Security und Internet der Dinge.

Notfallplanung

Wenn der Chef plötzlich ausfällt, könnten die Folgen für ein Unternehmen dramatisch sein, heißt es in sicherheit.info am 24. Januar. Dennoch seien viele Firmen nur unzureichend für den Ernstfall vorbereitet. Ein „digitaler Notfallkoffer" sollte klare Stellvertretungsregelungen, Vollmachten für alle Konten, ein Unternehmer-Testament sowie eine Liste mit Lieferanten, Kunden und Geschäftspartnern enthalten. Darüber hinaus müssten konkrete Handlungsanweisungen zu den wichtigsten Aufgaben und Projekten sowie eine Liste mit sämtlichen IT-Passwörtern und Bank-Zugangsdaten hinterlegt werden. Zudem sollten wichtige Geschäftsunterlagen wie Gesellschaftervertrag, Versicherungspolicen und Kreditverträge gescannt sein. Und ein Vertrauter müsse wissen, wo die Schlüssel aufbewahrt werden. Eine sogenannte Existenz-Betriebsunterbrechungsversicherung (EBU) gewährleiste die finanzielle Stabilität, solange der Chef ausfällt. Sie übernehme die laufenden Fixkosten eines Betriebs wie Löhne und Gehälter, Miete und Pacht oder Zinsen für laufende Kredite. Wichtig sei eine passgenaue und firmenspezifische Gestaltung der Absicherung. Die EBU sollte bereits ab einer Arbeitsunfähigkeit von 70 Prozent greifen.

Öffentlicher Raum

Videoüberwachung biete keinen präventiven Schutz, schreibt sicherheit.info am 24. Januar. Der Trend gehe in allen Sicherheitsbereichen sinnvollerweise hin zur Kombination verschiedener Komponenten. Umfassender **Perimeterschutz auf öffentlichen Plätzen** könne nur durch eine Kombination von mechanischen und elektronischen Komponenten geschaffen werden. Dazu gehörten eine Außensicherung mit Crash-Pollern oder anderen zertifizierten, anprallast-getesteten Barrieren, gegebenenfalls Fahrzeugschleusen

mit Schnellfalttoren oder eine Schranken-Schiebetorkombination, Anlagen zur Personenvereinzelung sowie eine ergänzende Videoüberwachung. Die Auswahl der optimalen Kombination für einen bestimmten Anwendungsbereich sei von verschiedenen Kriterien abhängig. Neben der Risikoart, dem Schutzniveau, dem Täterprofil und der möglichen Bedrohung bildeten die Gebäude- bzw. Geländekontur oder -beschaffenheit die entscheidenden Faktoren. Die Absicherung innerstädtischer Bereiche stelle eine besondere Herausforderung aufgrund teilweise sehr enger Bebauung, fundamenttechnischer Einschränkungen durch unterirdische Rohre und Leitungen oder aufgrund starker Frequentierung durch Fahrzeuge oder Personen dar. Ein weiterer zentraler Faktor sei die optische Ausprägung eines Sicherheitskonzeptes in öffentlichen Bereichen. Hochsicherheitsprodukte mit Anpralllast seien eine ideale und präventive Ergänzung zur Absicherung von beispielsweise Fußgängerzonen oder anderen öffentlichen Bereichen, die von Fahrzeugen auf Zufahrtswegen erreicht werden können. Crash-getestete, hydraulische Poller wie die von Elkosta zum Beispiel, seien im abgesenkten Zustand bequem überfahrbar. Ein besonderes Merkmal von Elkosta-Durchfahrtssperren seien die besonders flachen Fundamente.

Onlineshop-Betrug

So werden Käufer in gefälschten Onlineshops betrogen, titelt die FAZ am 4. Januar. Die Masche sei immer gleich: Angezogen von den oft eigentlich unrealistisch niedrigen Preisen bestellten Ahnungslose ihren Artikel und bekämen kurz darauf den Hinweis, alles Weitere per Mail mit dem Verkäufer zu regeln statt über den Amazon-Warenkorb. „Sobald man die Umgebung verlassen soll, ist das schon ein Indikator dafür, dass etwa schief läuft", argumentiere die Verbraucherzentrale NRW. Die Polizei spreche von einem Massenphänomen. Das BKA habe 2016 74.421 Fälle von Warenbetrug im Internet registriert, wozu auch Fakeshops zählten. Von allen im Internet begangenen Straftaten mache Warenbetrug damit rund 30 Prozent aller Delikte aus. Das Ermitteln der Täter sei allerdings schwierig, manche Shops bestünden nur wenige Stunden. Gemeldete Shops würden von Amazon zwar nach und nach gelöscht, doch die Betrüger eröffneten einfach neue. Oder sie nutzten eine Methode, die für den Kunden noch schwieriger zu erkennen sei: Sie hackten sich in die Profile seriöser Händler und verkauften von dort aus ihre Scheinartikel.

Persönliche Schutzausrüstung

Mit der **Absturzsicherung an hoch gelegenen Arbeitsplätzen** befasst sich GIT in der Ausgabe 1-2/2017, S. 105/106. Um sich gegen einen möglicherweise tödlichen Sturz zu sichern, sei eine Persönliche Schutzausrüstung gegen Absturz (PSAgA) verpflichtend. Dabei sei die regelmäßige Teilnahme an Schulungen unumgänglich. Für Unternehmen, die ihrer Unterweisungspflicht nachkommen müssen, seien daher jene Hersteller von Absturzsicherungen die richtigen Ansprechpartner, die mehr bieten als nur ein vielfältiges Produktprogramm. Ausbilder sollten beispielsweise Ersthelfer sein, über theoretische Kenntnisse gesetzlicher Vorschriften verfügen und praxiserfahren sein. Das bedeute, dass sie ihre PSAgA mindestens 15 Tage im Jahr nutzen müssten. Theoretische Details zu Normen und Gesetzen, Unfallrisiken oder medizinischen Grundlagen gehörten ebenfalls zu den Schulungsinhalten. Die Übungen in der Praxis stünden jedoch im Mittelpunkt.

Personenschutz

GIT berichtet in der Ausgabe 1-2/2017, S. 98/99, die Schmerwal Gruppe sei damit beauftragt worden, Bahnsteige in U-Bahn-Stationen in Hongkong durch **Sicherheitsschaltmatten im Gleisbett** besser zu sichern. Eine Sicherheitsschaltmatte bestehe aus zwei voneinander getrennten, stromführenden Metallplatten, die durch isolierende Trennstreifen auf Abstand gehalten werden. Tritt eine Person auf die Schaltmatte, dann werde zwischen den Metallplatten ein elektrischer Querschuss hergestellt. Im Leitstand würden Signalleuchten aktiviert und eine Bewegung des Zuges gestoppt. Man habe sich für die Schaltmatten als Sicherheitslösung entschieden, da es sich um eine sehr robuste und widerstandsfähige Sicherheitslösung handele.

Produktpiraterie

Seit China vor mehr als 30 Jahren seine Wirtschaft öffnete, plagen chinesische Raubkopierer ausländische Unternehmen, schreibt die WirtschaftsWoche am 6. Januar. Die großen Traditionsunternehmen mit ihren Weltmarken wie Bosch oder Stihl hätten seither mühsam gelernt, sich gegen die Produktpiraten zu wehren. Nun seien die Digital Natives dran: Plattformen wie Indiegogo und Co. mutierten gerade zu unfreiwilligen Inspirationsquellen. Und die Kopisten überholten nun das Original oft, noch bevor dieses überhaupt fertig werden konnte. Dabei würden Crowdfunding-Seiten bei vielen Gründern als unkomplizierte Möglichkeit gelten, ihre Produktideen zu verwirklichen. Dafür müssten sie ihre Ideen möglichst detailliert ins Netz stellen. Denn je anschaulicher die Beschreibung, desto mehr Unterstützer fänden die Gründer in der Regel – aber inzwischen eben auch umso mehr Nachahmer aus China.

Mit dem Thema Produktpiraterie befasst sich der Behörden Spiegel in der Januar-Ausgabe. **Bei Lieferketten** gibt es nach Aussage von Thomas Franke vom „Forum Vernetzte Sicherheit" bisher **keine einheitlichen Standards**. Damit seien sie etwas sehr Fragiles und ein großes Einfallstor für Täter aus dem Bereich der OK. Die Kosten, die Zigarettenschmuggler für den Transport eines Containers aufbringen, lägen bei nur rund 60.000 Euro. Ihr Gewinn betrage pro Container etwa 1,8 Mio. Euro. Über sogenannte Track-and-Trace-Systeme könnten illegale Zigaretten leicht erkannt werden. Diese Lösungen, bei denen jede legal hergestellte Zigarettenstange und -packung eine individuelle Kennzeichnung erhalte, erlaubten eine lückenlose Rückverfolgung der Produkte. 2015 seien rund 1.200 „Grenzbeschlagnahmeanträge" beim Zoll gestellt worden. Insgesamt sei es hierdurch zu circa 23.300 Beanstandungen im Bereich des gewerblichen Rechtsschutzes gekommen. Damit rangiere Deutschland im europäischen Vergleich auf Platz eins. Im Bereich Arzneimittelfälschung sei das Internet die größte Herausforderung. Experten des Europäischen Patentamtes seien in einer Studie bereits 2014 davon ausgegangen, dass durch Produktpiraterie europaweit 4,7 Billionen Euro Umsatz und 77 Mio. Jobs gefährdet worden seien.

Reisesicherheit

Im ASW-Newsletter vom 6. Januar listet Pascal Michel, SmartRiskSolutions GmbH Punkte auf, die das **Reisesicherheitsmanagement von Firmen** umfassen sollte:
1. Informationen für Reisende mit Hinweisen zur Gefährdungslage am Reiseziel und Verhaltensempfehlungen, 2. unternehmensweites Reisesicherheitsmanagement, bei dem die Firma auf Knopfdruck Reisedaten abrufen kann, 3. aktuelle Kontaktdaten der Reisenden und Familienangehörigen vorhalten, 4. Sicherheitstraining für Geschäftsrei-

sende, 5. 24/7-Notfallhotline. 6. unternehmensweites Krisen- und Notfallmanagement mit einem Krisenstab, Krisenhandbuch und Notfallplänen, 7. Konzepte und Fähigkeiten zur Betreuung von betroffenen Mitarbeitern und Familien aufbauen, 8. Zusammenarbeit mit externen Sicherheits- und Krisenberatern, die auch vor Ort unterstützen können.

Schließsystem

Auf das PC-System eines Hotels in Österreich hätten Computerkriminelle in den vergangenen Monaten vier Attacken gestartet, meldet die FAZ am 2. Februar. Dreimal habe man nach der Attacke durch kriminelle Verschlüsselungssoftware das System selbstständig wieder zum Laufen gebracht. In einem Fall sei das nicht gelungen. Der Hotelier habe daraufhin den Erpressern 1.500 Euro in der virtuellen Währung Bitcoin gezahlt. In kürzester Zeit sei das System daraufhin wieder zugänglich gewesen. Der Hotelier erwäge nun Konsequenzen: „Wir denken wirklich darüber nach, wieder zu den Schlüsseln zurückzukehren."

GIT skizziert in der Ausgabe 1-2/2017, S. 44–46, das Schließsystem **Verso Cliq** der Assa Abloy Sicherheitstechnik für die RWTH Aachen, die mit ihren rund 350 Gebäuden zu den größten Universitäten Deutschlands zählt. Allein im sechsstöckigen Information-and-Communication-Technology-Cubes-Gebäude seien rund 300 Verso Cliq-Zylinder verbaut. In jedem Schlüssel sei ein Chip integriert, der individuell für jeden Nutzer programmiert werde. So habe jeder Schlüssel nur für festgelegte Türen eine Zutrittsberechtigung. Der größte Vorteil des Systems liege darin: Geht ein Schlüssel verloren, entstehe keine Sicherheitslücke. Die Energieversorgung für die Kommunikation mit dem Zylinder erfolge ausschließlich über eine Standardbatterie im Schlüssel.

GIT weist in der Ausgabe 1-2/2017, S. 70, auf das flexible Schließsystem **Dictamat 50** hin, das für kleine bis mittelgroße Schiebetüren zusätzliche Einsatzmöglichkeiten erschließe. Der Dictamat 50 WS sei als Baukastensystem mit einzelnen Komponenten konzipiert. Lediglich mit einem Wendeseil befestigt und gespannt sei es auch für Anwendungen geeignet, wo oberhalb der Tür sehr wenig Platz ist. Je nach Zusammenstellung seien drei verschiedene Betriebsarten des Schiebetürschließens möglich: Basisvariante mit reiner Schließfunktion, Freistellfunktion mithilfe eines Magneten und mit Freilauffunktion.

Schwarzarbeit

Der Bundestag hat weitere Maßnahmen zur Bekämpfung der Schwarzarbeit beschlossen, meldet die Wochenzeitung DAS PARLAMENT am 19. Dezember. Ausweispapiere müssten in Zukunft nicht nur der Zollverwaltung, sondern auch Bediensteten der zuständigen Landesbehörden vorgelegt werden. Die Landesbehörden erhielten zudem weitere Prüfungsbefugnisse. Zollbehörden dürften in Zukunft Daten aus dem Zentralen Fahrzeugregister des Kraftfahrt-Bundesamtes abfragen. Außerdem seien Verbesserungen in der behördlichen Informationstechnologie geplant. Zu weiteren Maßnahmen gehöre der Ausschluss von Bewerbern von der Teilnahme an Ausschreibungen, die mit Vorschriften zur Verhinderung von Schwarzarbeit in Konflikt gekommen sind.

Die Schattenwirtschaft schrumpft, titelt die FAZ am 8. Februar. Wie eine am 7. Februar vorgestellte Analyse des Tübinger Instituts für Angewandte Wirtschaftsforschung und der Universität Linz vorrechne, würden 2017 Leistungen im Wert von 330 Mrd. Euro in der Schattenwirtschaft erbracht. Das wären sechs Mrd. Euro weniger als 2016. Mehr als die Hälfte des Rückgangs gehe der Berechnung zufolge auf die günstige wirtschaftliche Situa-

tion zurück. Die Anhebung des gesetzlichen Mindestlohns zum 1. Januar 2017 werde die Schwarzarbeit hingegen leicht befördern. Der Anteil der Schattenwirtschaft an der offiziellen Wirtschaft werde 2017 im achten Jahr in Folge sinken, und zwar von 10,8 auf 10,4 Prozent. Damit sei ihr Anteil am Bruttoinlandsprodukt so niedrig wie noch nie seit Beginn der Auswertung 1985. Verglichen mit anderen OECD-Staaten liege Deutschland im Mittelfeld.

Sicherheitsgewerbe

In der Ausgabe 1-2/2017 der Zeitschrift GIT, S. 30/31, wird die Digitalisierung der Verwaltung des Sicherheitsdienstleisters Vigilat dargestellt. Mit dem **SequriX Softwaresystem** digitalisierten Sicherheitsdienste ihre Wach-, Empfangs- und Interventionsdienste. Das bedeute: Alle Daten über Objekte, Kunden, Örtlichkeiten, Fuhrpark und Verträge könnten in einem System verwaltet werden. Wachleute sähen direkt auf ihrem Smartphone Vorkommnisse, erhielten Alarmierungen oder registrierten, welcher Kollege schon auf dem Weg sei. Ziel der Software sei es, dass die Sicherheitsdienste ihre normalen Abläufe deutlich verbessern und dass dadurch auch die Berichterstattung gegenüber ihren Kunden genauer werde. Zum Dienstbeginn melde sich der Mitarbeiter mit seinem Smartphone an. In diesem sei sein Aufgabenpaket bereits vorbereitet. Jeder Kunde wiederum habe Zugriff darauf, was vom jeweiligen Wachmann erwartet wird. Er erhalte nach jeder Kontrolle durch das Wachpersonal automatisch ein PDF-Dokument mit allen relevanten Informationen, wer wann wo war und was dort passiert ist. SequirX sei ein Onlinesystem, Daten würden also auf einem gesicherten Server gespeichert.

Sicherheitsmarkt

Wie GIT in der Ausgabe 1-2/2017, S. 15, berichtet, zeigen sich die Facherrichter für Sicherheitstechnik weiterhin sehr zufrieden mit ihrer aktuellen Geschäftslage und bewerten diese durchschnittlich mit 1,81 auf der Schulnotenskala. Ihre künftige Geschäftslage beurteilten sie mit 1,92, dem besten Wert seit Beginn der Erhebungen. Die guten Ergebnisse seien unter anderem auf die **positive Nachfrageentwicklung im gewerblichen Bereich** zurückzuführen. Diese Kundengruppe sei durchschnittlich mit 1,88 benotet worden. In einzelnen Branchen seien die Werte geringfügig schwächer ausgefallen. Die führenden Sicherheitsdienstleister seien 2015 um durchschnittlich 17 Prozent gegenüber dem Vorjahr gewachsen. Ausschlaggebend hierfür seien Zukäufe, das Outsourcing der Bewachung von Bundeswehr-Standorten, die Neuvergabe von Großaufträgen mit hohen Umsatzvolumina, der Sicherungsbedarf von Flüchtlingsunterkünften sowie die Einführung des Mindestlohns gewesen.

Die Sicherheitsbranche profitiere vom **zunehmenden Schutzbedürfnis**, schreibt die Berliner Morgenpost am 22. Januar. Zwischen 2010 und 2015 sei der Branchenumsatz von Wach- und Sicherheitsdiensten um 37 Prozent auf 6,9 Mrd. Euro gewachsen. Allein 2015 sei der Umsatz um 14 Prozent gestiegen. Zwar falle das Wachstum 2016 etwas geringer aus. Der BDSW rechne jedoch weiter mit einem Umsatzplus von zwei bis drei Prozent. Das starke Wachstum stelle aber auch die Unternehmen vor große Probleme. Es fehle an genügend geeignetem Personal. Vom Objektschützer bis zum Sicherheitsmanager suche die Branche laut BDSW bundesweit knapp 11.000 Mitarbeiter. Den Arbeitskräftemangel spüre auch das Sicherheitsunternehmen Securitas. „Wir könnten gut 2.000 neue Kolleginnen und Kollegen einstellen", sagt Securitas-Sprecher Bernd Weiler. Ähnlich gehe es Unternehmen aus der

Sicherheitstechnik. Nach Schätzungen des BHE seien 2016 die Umsätze von Videoüberwachungssystemen in Deutschland um 6,6 Prozent auf 504 Mio. Euro gestiegen. Mit Alarmanlagen hätten die Unternehmen 800 Mio. Euro erwirtschaftet, ein Plus von 8,8 Prozent zum Vorjahr.

Social Engineering

Das BfV berichtet im Newsletter 4/2016 von **Cyberangriffen iranischer Gruppierungen**. Sie nutzten sehr häufig sogenannte Phishingmails, die das Opfer dazu verleiten sollen, Zugangsdaten zu E-Mail- oder Social-Media-Accounts auf einer Website einzugeben. Sie werde vom Angreifer betrieben und ahme die echte Website des vom Opfer genutzten Dienstes derart täuschend nach, dass viele Opfer nicht an deren Authentizität zweifeln. Die Angreifer flanierten ihre Ausspähungen oftmals mit Kontaktansprachen in sozialen Medien oder Telefonanrufen.

Im Visier einer vermutlich iranischen Cyberkampagne stünden besonders Unternehmen aus der Energiewirtschaft, heißt es in demselben Newsletter. Auch hier würde der Angriff durch ein hochprofessionelles Social Engineering vorbereitet. Das Opfer erhalte eine E-Mail mit dem Link zu einer nachgeahmten Website und den angeblichen Stellenangeboten. Der Download führe zu einer Schadsoftwareinfektion.

Terrorismus

Die Deutsche Telekom wolle eine europaweite Antiterrorinitiative starten, um den **Missbrauch von vorausbezahlten Mobilfunkkarten durch Terroristen** einzudämmen, berichtet die WirtschaftsWoche am 6. Januar. Die Täter legten nach jedem Anruf eine neue Prepaid-Karte ins Handy. So könnten sie mit Komplizen telefonieren, ohne dass das Gespräch abgehört werden könne. In einigen europäischen Ländern – etwa in Österreich, den Niederlanden und Rumänien – sei das besonders einfach. Denn dort könnten Prepaid-Karten ohne Vorlage des Personalausweises bestellt werden. Deutschland habe die Identitätsprüfung beschlossen. Das Gesetz trete aber erst am 1. Juli in Kraft. Aufgeschreckt worden sei Telekom-Vorstand Thomas Kremer durch einen drastischen Missbrauchsfall in Ungarn. Im Namen eines verstorbenen Obdachlosen hätten offenbar Hintermänner der Terrormiliz „IS" einen Vorrat von 20.000 Prepaid-Karten angelegt. Einzelne Karten hätten die Ermittler nach den Anschlägen in Paris und Brüssel in den Taschen der erschossenen Terroristen gefunden.

Überspannungsschutz

Anforderungen an eine hohe Dichte und Leistungsfähigkeit müsse der Überspannungsschutz für Rackmontage-Anwendungen erfüllen, heißt es in der Fachzeitschrift GIT (Ausgabe 1-2/2017, S. 100). Phoenix Contact habe nun die ersten steckbaren Überspannungsschutzgeräte für den Einsatz in Standard-Rackmount-Gehäusen entwickelt. Mit der neuen Positionierung in der Gehäusefront könne der Anwender die Statusanzeige kontrollieren, ohne die Abdeckung zu entfernen oder die Spannungsversorgung auszuschalten.

Unternehmens-Ordnungswidrigkeiten

Die Grünen wollen „zukunftsfähige Unternehmensverantwortung" gesetzlich festschreiben, berichtet DAS PARLAMENT am 30. Januar. In einem im Bundestag eingebrachten Antrag würden „wirksame Sanktionen bei Rechtsverstößen von Unternehmen" gefordert. Begründet sei dies damit worden, dass Unternehmen

gegen Gesetze, Umwelt- oder Sozialstandards verstießen, den Wettbewerb verzerren und damit den gesetzestreuen Unternehmen schaden. Allerdings wolle die Fraktion nicht Normen des StGB auf juristische Personen übertragen, sondern eine Verschärfung des Ordnungswidrigkeitenrechts. Auch Verstöße im Ausland sollten verfolgt und finanzielle Sanktionen erhöht werden. Die CSU kritisiere, das könne dazu führen, dass „Fließbandarbeiter oder Kleinaktionäre für das Fehlverhalten von Managern haften müssen". Mit einem zweiten Antrag sollten „menschenrechtliche Sorgfaltspflichten" verankert werden. Firmen sollten auf eine fortlaufende menschenrechtsbezogene Risikoanalyse, Präventionen zur Verhinderung von Menschenrechtsverletzungen und Abhilfen bei Menschenrechtsverstößen verpflichtet werden.

Videoüberwachung

Die Bundesregierung habe beschlossen, die **private Überwachung öffentlich zugänglicher Räume** zu erleichtern, berichtet die FAZ am 6. Januar. Länder und Kommunen diskutierten, ob die bestehenden Möglichkeiten ausreichen. Und auch Unternehmen setzten immer stärker auf Kameras. Die Deutsche Bahn etwa habe bereits im Frühjahr 2016 angekündigt 85 Mio. Euro in die Videoüberwachung in Zügen und Bahnhöfen zu stecken. Rechtlich gesehen sei die Videoüberwachung eine komplexe Materie. Es gebe diverse Normen im Landesrecht und im Bundesrecht, die die Aufstellung von Kameras erlaubten. Welche Norm Anwendung findet, hänge davon ab, wer die Kamera an welchem Ort zu welchem Zweck aufstelle. Aus Landesgesetzen ergebe sich, dass eine durch Tatsachen belegbare Gefahr für die Sicherheit drohen müsse, damit der Eingriff in die informationelle Selbstbestimmung gerechtfertigt ist. Größere Freiheit für den Einsatz von Kameras bestehe auf Grundlage des BDSG. Es erlaube allen privaten und öffentlichen Stellen, Kameras aufzustellen, um das Hausrecht wahrzunehmen oder „berechtigten Interessen für konkret festgelegte Zwecke" nachzukommen. Die Zwecke der Überwachung müssten gegen schutzwürdige Interessen der Betroffenen abgezogen werden. Hier komme der Beschluss des Bundeskabinetts ins Spiel. Bei der Frage, ob etwa ein Einkaufszentrum oder ein Parkhaus eine Kamera installieren darf, solle künftig „der Schutz von Leben, Gesundheit oder Freiheit" von Personen als „besonders wichtiges Interesse" berücksichtigt werden. Die Sicherheitsbelange sollten also höher gewichtet werden.

Die baden-württembergische CDU wolle sich für die Einrichtung eines nationalen „Kompetenz- und Entwicklungszentrums" zur Videoüberwachung in Stuttgart einsetzen, meldet die FAZ am 20. Januar. Es soll vor allem darum gehen, intelligente Systeme zur Videoüberwachung in einer neuen Zentrale zu steuern. Sie könnten verdächtige Personen oder Bombenkoffer automatisch erfassen.

Auch die Wochenzeitung DAS PARLAMENT berichtet am 30. Januar, das von der Bundesregierung im Entwurf beschlossene „Videoüberwachungsverbesserungsgesetz" (18/10941) ziele auf eine **Ausweitung der Videoüberwachung** ab. Es sehe Änderungen des BDSG vor mit dem Ziel, beim Einsatz von Videoüberwachung in Einrichtungen und Fahrzeugen des öffentlichen Schienen-, Schiffs- und Busverkehrs und öffentlich zugänglichen Anlagen wie Sportstätten oder Einkaufszentren festzuschreiben, „dass der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als besonders wichtiges Interesse gilt". Ziel eines zweiten Gesetzentwurfs sei „eine Stärkung der polizeilichen Befugnisse zum Einsatz von technischen Mitteln". So solle die Bundespolizei automatische Kennzeichenlesesysteme einsetzen können, um bei Gefahren für die öffentliche Sicherheit die Fahndung nach Fahrzeugen und deren Insassen sowie die Strafverfolgung zu verbessern. Ferner

sei unter anderem vorgesehen, durch mobile Videotechnik den Schutz von Polizeibeamten sowie die „Verfolgung von Straftaten und Ordnungswidrigkeiten von auch im Einzelfall erheblicher Bedeutung“ zu verbessern.

Die Fachzeitschrift GIT enthält in der Ausgabe 1-2/2017 mehrere Beiträge zur Videoüberwachung:

Auf S. 34 weist GIT in der Ausgabe 1-2/2017 auf das **Bosch Video-Managementsystem 7.0** hin, das das Sicherheitspersonal dabei unterstütze, hochauflösende Videostreams effektiv einzusetzen. Nutzer könnten jetzt mehrere Ultra High-Definition-Kameras gleichzeitig in Betrieb haben, ohne Sorge, dass sich die Anwendungen verlangsamen und/oder nicht mehr richtig laufen. Bosch VMS 7.0 nutze dazu die Technologie Streamlining. Dadurch sei das Video auf dem Bildschirm immer in der optimalen Auflösung zu sehen. Wenn das Sicherheitspersonal mehrere Kameras gleichzeitig im Blick haben müsse, schalte Bosch VMS 7.0 automatisch auf ein Streaming in geringerer Auflösung um. Eine weitere neue Funktion sei die verschlüsselte Kommunikation zwischen Bosch-Kameras und dem Video-Managementsystem.

Die **intelligente Video Analyse (IVA)** ist Thema in der Ausgabe 1-2/2017 der Fachzeitschrift GIT (S. 56/57). Die Funktion „virtueller Stolperdraht“ aktiviere in Ein- und Ausfahrten oder auf Parkplätzen bei auffälligen Ereignissen Sirenen oder Scheinwerfer. Die „Gesichtserkennung“ speichere an Sicherheitstüren automatisch ein Bild des Eintretenden und schaffe eine nachvollziehbare Zutrittsdokumentation. Auf Freiflächen, entlang von Zäunen, auf Parkverbotsbereichen oder Rettungswegen sichere die „Zonenüberwachung“ sensitive Punkte. Diese Funktion beobachte, interagiere, spreche an oder löse Alarm aus. Sie schicke beispielsweise Push-Nachrichten, sobald sie in „ihrer“ Zone Abweichungen von der Normalität registriert. In Lagerbereichen oder Produktionen registriere IVA das Entfernen von Teilen. Neben dem Sicherheitsaspekt liefere das System Facts für den Absatz. Stark frequentierte Gebäudebereiche ließen sich selektieren und Produktplatzierungen anpassen.

Rechtsfragen bei der Baustellenüberwachung und -dokumentation durch Videoüberwachung behandelt Rechtsanwalt Dr. Ulrich Dieckert in Ausgabe 1-2/2017 der Zeitschrift GIT, S. 62–64. Da die Bilderfassung nicht unverhältnismäßig in die Persönlichkeitsrechte der betroffenen Personen eingreifen darf, sollte stets geprüft werden, ob eine Überwachung wirklich „flächendeckend“ erfolgen muss, wenn auch eine Überwachung von Schwerpunkten bzw. in bestimmten Zeiträumen ausreicht. Aufnahmen in Sanitärbereichen oder Umkleidekabinen seien tabu. Gleiches gelte für Bereiche wie Raucherecken oder Imbissstände, in denen Kommunikation bzw. soziale Interaktion stattfindet. In der sogenannten Sozial- oder Geschäftssphäre, in der die Menschen ihren alltäglichen Verrichtungen nachgehen, seien Grundrechtskollisionen hingegen unvermeidbar. Insgesamt lasse sich festhalten, dass die Interessen des Betreibers in der Regel überwiegen dürften, soweit er die Bilderfassungssysteme auf Baustellen maßvoll einsetzt und dabei die Interessen der miterfassten Personen hinreichend berücksichtigt. Bilddaten sollten über ein von der sonstigen Unternehmens-EDV getrenntes Netz geleitet und in einem Server verwaltet werden, der sowohl physisch als auch elektronisch durch Passwörter gesichert ist. Die gemäß § 4d Absatz 5 BDSG erforderliche „Vorabkontrolle“ sollte hinreichend protokolliert werden, um die Erfüllung der Pflicht gegenüber den Datenschutzbehörden nachweisen zu können.

Über eine IP-Videosicherheitslösung für die Berliner CleanCar Filiale berichtet GIT in der Ausgabe 1-2/2017, S. 66/67. Um die Sicherheit von Kunden und Mitarbeitern zu gewährleisten und zur Vorbeugung von „klassischen“ Delikten im Umfeld von Tankstellen und

Waschstraßen – also Tankbetrug, Sachbeschädigung, Ladendiebstahl, illegale Müllentsorgung, Vortäuschung von Schäden – seien die Niederlassungen mit hochauflösenden Videoüberwachungssystemen ausgestattet worden. Eine Objektiventzerrungsfunktion (LDC) korrigiere optische Verzeichnungen und sorge auf diese Weise für akkurate Konturen. Atmosphärische Beeinträchtigungen der Bildqualität, z. B. durch Nebel, Nieselregen oder Smog, würden mittels Defog in Echtzeit korrigiert. Im Innenbereich der Filialshops seien fünf IP-Domes im Einsatz.

Impressum

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

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

Herausgeber:
Manfred Buhl, Vorsitzender der Geschäftsführung, Düsseldorf

Verantwortlicher Redakteur:
Bernd Weiler, Leiter Kommunikation und Marketing

Beratender Redakteur:
Reinhard Rupprecht, Bonn

focus.securitas.de

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

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

E-Mail: info@securitas.de