Focus on Security

Ausgabe 12, Dezember 2015

SECURITAS

Inhalt

Aufzugssicherheit

Thyssen-Krupp stellt ein neues Aufzugssystem vor, berichtet die FAZ am 29. Oktober. Die Technologie mit dem Namen „Max" markiere den Einstieg der Aufzugssparte in das „industrielle Internet". Durch die Verknüpfung mit dem Internet sollen Fahrstühle in die Lage versetzt werden, zu signalisieren, wann es Zeit für eine vorsorgliche Wartung ist und wann sie repariert werden müssen. Allein in Deutschland blieben nach Angaben von Thyssen-Krupp jedes Jahr 18.000 Menschen in einem Aufzug stecken. Für die Technologie habe sich Thyssen-Krupp mit Microsoft zusammengetan. Microsoft werde Daten der mit dem Internet verbundenen Fahrstühle sammeln und analysieren, woraus dann Rückschlüsse auf etwaige Wartung oder Reparatur gezogen würden. Thyssen-Krupp sei der erste Aufzughersteller mit einer Technologie, die den Wartungsbedarf voraussehen kann.

Business Continuity Management (BCM)

Mit Grundlagen zur Einführung eines **Business Continuity Management (BCM) in mittelständischen Unternehmen** befasst sich Sicherheitsingenieurin (M. Sc.) Sophie Charlotte Schwarz, Provinzial Rheinland Versicherung AG, in der Ausgabe 4-2015 von s+s report, S. 48–51. Die Notwendigkeit eines BCMs für mittelständische Unternehmen sei mit mehreren Aspekten zu begründen. Insbesondere diene ein BCM der Existenzsicherung und Aufrechterhaltung der Wettbewerbsfähigkeit. Im Rahmen der Globalisierung würden Wertschöpfungsprozesse vermehrt verknüpft, wodurch verstärkt Abhängigkeiten und somit höhere Risiken entstünden. Dabei seien besonders mittelständische Unternehmen im Fokus, denn sie seien oftmals nicht ausreichend auf Vorfälle vorbereitet, die eine Betriebsunterbrechung nach sich ziehen. Der Beitrag geht vor allem auf rechtliche Grundlagen für die Durchführung eines BCMs und relevante Standards – DIN EN ISO 22301 und 22313, Good Practice Guidelines und BSI Standard 100-4 – ein.

Brandschutz

Dipl.-Ing. Bernhard Tschöpe, AG Betrieblicher Brandschutz Berlin e. V., nimmt in der Ausgabe 4-2015 von s+s report (S. 8/9) zur **Verwendung fluorhaltiger Schaumlöschmittel** Stellung. Die in ihnen enthaltenen poly- und perfluorierten Chemikalien (PFC) seien in der Natur nur sehr schwer bis gar nicht abbaubar. Dies habe bereits zum fast vollständigen Verbot von Perfluoroctansulfonat (PFOS) geführt. Ein Verzicht auf fluorhaltige Schaummittel würde aber bedeuten, dass bestimmte Problemstoffe nicht mehr effektiv gelöscht werden können. Einen Blick in die Zukunft der fluorhaltigen Schaummittel zu wagen sei schwierig. Hoffnungsträger als eine Alternative zu den fluorhaltigen Schaummitteln seien derzeit die Siloxantenside. Für Tankanlagen seien fluorhaltige Schaumlöschmittel – abhängig von der gelagerten Flüssigkeit – momentan absolut unersetzbar.

Dipl.-Ing. Heike Menna Siefkes, VdS Schadenverhütung, erläutert in der Ausgabe 4-2015 von s+s report, S. 20/21, neue VdS-Richtlinien für die Planung und den Einbau von **Sauerstoffreduzierungsanlagen.** Sie beschreibt die wesentlichen Änderungen in den Richtlinien VdS 3527. Als grundlegende Änderung habe VdS durch ein Klassifizierungssystem die Flexibilität der Richtlinien erhöht. Die Autorin geht auf Besonderheiten der Klasse 2-Anlagen ein. Jetzt könne die Stickstoffversorgung im Schutzbereich erfolgen und das Verteilerrohrnetz könne innerhalb des zu schützenden Bereichs in Kunststoffausführung installiert werden. Außerdem könne auf die selbsttätige Überwachung verzichtet werden, wenn die gemin-

derte Betriebsbereitschaft durch die höhere Ausfallwahrscheinlichkeit und die verzögerte Störungsbehebung in einem Notfallkonzept entsprechend berücksichtigt wird.

Ulrich Schwieger, Heitel Digital Video GmbH, weist in der Ausgabe 4-2015 von s+s report (S. 24–27) darauf hin, dass das Bundeskartellamt entschieden hat, künftig dürfe es keine exklusive **Konzessionierung** über sämtliche Einzelleistungen der Brandalarmübertragung mehr geben. Der Autor stellt die möglichen Verantwortungsbereiche und Konstellationen dar, die sich unter Betrachtung des Kartellamtsbeschlusses ergeben können. Die Reduzierung des Verantwortungsbereichs der Konzessionäre führe zu mehr Wettbewerb. Die Kosten für eine Konzession könnten reduziert werden, weil derzeit ein Großteil der Investitionen und der laufenden Kosten durch die Übertragungseinrichtung verursacht würden.

Felix Flörke, VdS Schadenverhütung, befasst sich in der Ausgabe 4-2015 von s+s report, S. 28–31, mit der **Gefährdungsbeurteilung für Gaslöschanlagen.** Insbesondere stellt er Gefahren und Gefährdungsklassen dar. Der Betreiber einer Gaslöschanlage habe gemäß § 5 Arbeitsschutzgesetz für jede Gaslöschanlage eine Gefährdungsbeurteilung für die sich im Gefährdungsbereich befindenden Personen durchzuführen. Der Betreiber habe auch die Auswirkungen einer Auslösung seiner Löschanlage zu betrachten und ein an seine Bedürfnisse angepasstes Schutzkonzept zu erstellen, durch das eine Personengefährdung aufgrund der Gastechnik ausgeschlossen werden soll.

Cloud Computing

TECCHANNEL.de betont am 27. Oktober, dass die im August 2014 verabschiedete **ISO-Norm ISO 27018** für Anwender bei der Auswahl von Cloud-Anbietern besonders wichtig sei. Um ihren Kunden Sicherheit personenbezogener Daten gemäß dieser Vorgabe gewährleisten zu können, müssten Dienstleister ihr „Information Security Management System" (ISMS) im Rahmen von ISO 27001 nach der neuen Norm zertifizieren lassen. Doch um diesen Wettbewerbsvorteil zu erlangen, sei die technische Umsetzung der ISO 27018-Vorgaben zu bewältigen. TECCHANNEL skizziert die aus der ISO-Norm folgenden Verpflichtungen für Cloud-Anbieter. Aus den Vorgaben ergebe sich auch das Erfordernis der aktiven Produktion von Anbieter-eigenen Tools, die den Cloud-Kunden helfen sollen, deren Endkunden Zugang zu persönlichen Daten zu gewähren. TECCHANNEL geht insbesondere auf automatisierte Tests, die Betriebssicherung und die Zertifizierung ein.

Silicon.de berichtet am 3. November über neue Sicherheitsprodukte von Cisco. Angreifer würden immer häufiger den Weg über das erweiterte Netzwerk, auf Router, Switches, angeschlossene Datenzentren oder Cloud-Dienste gehen. Denn auf diese Komponenten hätten IT-Sicherheitsadministratoren meist keine Sicht. Dafür stelle Cisco jetzt die Lösung **Cloud Access Security** (CAS) vor. Zusammen mit dem Anbieter Elastica könne Cisco hier für Cloud-basierte Anwendungen Datensicherheit und Transparenz sicherstellen. Daneben habe Cisco auch die Cisco Cloud Web Security mit CAX integriert. Damit könnten verteilte Niederlassungen über Integrated Service Router direkt auf das Internet zugreifen und damit Bandbreiten einsparen. Und in die Identity Services Engine (ISE), eine Verwaltung für Sicherheitsregeln, die automatisch den Zugriff zu Netzwerkressourcen verwaltet, integriere Cisco nun die Cisco Mobility Services Engine. Damit könnten Administratoren ortsbasierte Regeln erzwingen und beispielsweise nur gewissen Personengruppen in bestimmten Räumen des Unternehmens Zugriff auf bestimmte Daten gewähren. Inbound- und Outbound-Netzwerktraffic lasse sich mit dem neuen Cisco-Dienst Threat

Awareness Service überwachen. Die Lösung könne dann auch mögliche Bedrohungen hervorheben.

Microsoft will mit einer **Art neuer deutscher Cloud** Datenschutzbedenken wegwischen, berichtet die FAZ am 12. November. Dafür kooperierten die Amerikaner mit der Telekom-Tochter T-Systems und nutzten deren Rechenzentren in Frankfurt und in Magdeburg. Dort laufen dann Microsoft-Dienste wie die Cloud-Computingplattform Azure, die Bürosoftware Office 365 und die Unternehmenssoftware Dynamics CRM Online. Für die Sicherheit der Daten stehe T-Systems, das als ein sogenannter Datentreuhänder auftrete. Ohne Zustimmung der Telekom-Tochtergesellschaft oder des Kunden habe Microsoft keinerlei Zugang zu Kundendaten, werde versichert.

Silicon.de weist am 26. November auf die IDC-Studie „**Hybrid Cloud** in Deutschland 2015/16" hin, nach der Komplexität, Sicherheitsbedenken und mangelnde Kenntnis eine stärkere Verbreitung von Cloud-Technologien bei Unternehmen ausbremsen. Dennoch setzten immer mehr deutsche Unternehmen auf das hybride Modell. Das sei in der IDC-Definition die Verknüpfung verschiedener Sourcing-Varianten aus unternehmenseigener herkömmlicher IT-Umgebung mit Private, Hosted oder Public Cloud Services. Gerade unter dem nach wie vor als sehr wichtig erachteten Sicherheitsaspekt sei es wenig verwunderlich, dass die Private Cloud mit 57 Prozent der Unternehmen noch immer die am meisten verbreitete Variante sei. Im Vergleich zu 2014 steige der Anteil der Unternehmen, die Hybrid Clouds nutzen, von 15 auf jetzt 20 Prozent an. Als wichtigste Bereiche nenne IDC die Geschäftsprozessautomatisierung, Big Data Analytics und Kunden-Self Services zur Verbesserung der Customer Experience sowie die Entwicklung neuer Geschäftsmodelle. Etwa 75 Prozent der Unternehmen planten derzeit bis 2017 den Einsatz von Hosted Private Clouds und mehr als 60 Prozent den Einsatz von Public Clouds. Allerdings blieben Personaldaten, Kundendaten, Finanz- und Buchhaltungsdaten sowie Forschungs- und Entwicklungsdaten nach Angaben der befragten IT-Entscheider zumeist im eigenen Unternehmen. Deutsche Firmen seien nach wie vor sehr konservativ und entschieden sich vor allem für Public Cloud-Anbieter mit deutschem Vertragsrecht (57 Prozent) und Rechenzentren auf deutschem Boden (47 Prozent).

Datenschutz

Laut Bitkom drohen durch das **Safe Harbor-Urteil** negative Konsequenzen für den Standort Europa, berichtet heise.de am 10. November. Eine politische Einigung mit den USA sei daher notwendig. Es bestehe die Gefahr, dass als Folge des EuGH-Urteils in Zukunft keine personenbezogenen Daten mehr in die USA übertragen werden dürfen. Zudem drohe den Unternehmen ein hoher finanzieller und organisatorischer Aufwand, wenn sie die Datenverarbeitung nach Europa verlegen müssen. Alternativen für neue Regeln seien die Standardvertragsklauseln der EU-Kommission, von den Datenschutzbehörden genehmigte verbindliche Unternehmensregelungen oder die Einwilligung der Betroffenen.

Die Fachzeitschrift GIT befasst sich in der Ausgabe 11-2015 (S. 66/67) mit der **sicheren Zerstörung von digitalen Datenträgern.** Zwar gebe es dafür spezielle Softwareprogramme. Doch sei das mehrmalige Überschreiben sehr zeitaufwendig. Die neue DIN 66399 beschreibe anhand von drei Schutzklassen und sieben Sicherheitsstufen, wie besonders sensible Daten zu vernichten sind und welche Anforderungen die dafür eingesetzten Maschinen erfüllen müssen. Der Festplattenvernichter HDS 230 der Firma HSM GmbH + Co. KG biete hohen Durchsatz. Dank der speziellen Schneidwerkzeuge könnten mehr als 400 Festplatten pro Stunde zerkleinert werden.

Drohnen

s+s report weist in der Ausgabe 4-2015 (S. 6) darauf hin, dass sich das Unternehmen Dedrone der Bedrohung durch zivile Drohnen widmet und dafür das Drohnen-Erkennungs- und Warnsystem **„DroneTracker"** entwickelt habe, das in einer neuen Version verfügbar sei. Es sei mit verbesserter Hardware inklusive einer industriellen HD-Kamera ausgestattet. Alle Alarmvideos würden zwecks Beweissicherung gespeichert. Softwareverbesserungen und -erweiterungen sowie eine erhöhte akustische Erkennung steigerten die Leistung bei der Detektion von Drohnen deutlich. Neue Schnittstellen ermöglichten außerdem eine einfachere Integration in bestehende Sicherheitssysteme.

EMA

In der Fachzeitschrift s+s report (Ausgabe 4-2015, S. 36/37) erläutert Dipl.-Wirtschaftsjurist (FH) Sebastian Brose, VdS Schadenverhütung, dass in der Praxis mitunter Fälle auftreten, bei denen aus technischen Gründen die vollständige Umsetzung der Anforderungen aus den Richtlinien VdS 2311 für **Planung und Einbau von EMA** nicht möglich ist. Deshalb sei mit der Ergänzung S2 zu den Richtlinien eine neue Kategorie von Abweichungen – „kompensierbare Abweichungen" – eingeführt worden. VdS 2311-S2, Abschnitt 13.11.2 regele die zu kompensierenden Abweichungen in EMA. VdS 3465-1 beschreibe das Prüfungsverfahren und enthalte das Auftragsformular. VdS 3465-2 beinhalte die Tabelle der geprüften Kompensationsmaßnahmen.

Endgerätesicherheit

TECCHANNEL.de weist am 22. November auf das Ergebnis einer Umfrage hin, nach dem 44 Prozent der befragten 500 IT-Entscheider angeben, dass in den letzten zwölf Monaten eine leitende Führungskraft ein **Mobilgerät verloren** habe. 39 Prozent hätten erklärt, dass ihrem Management ein Gerät gestohlen wurde. Zugleich habe die Studie ergeben, dass fast ein Drittel der IT-Entscheider nicht vorschreiben, dass Geräte, die außerhalb des Arbeitsplatzes verwendet werden, durch Verschlüsselung oder Passwörter geschützt sein müssen. Und ein Viertel verlange nicht, dass digitale Dateien außerhalb des Büros mit Verschlüsselung oder Passwörter geschützt werden müssen.

International Data Corporation (IDC) gibt laut TECCHANNEL.de vom 24. November sechs Tipps zur Sicherheit im **Umgang mit mobilen Endgeräten im Unternehmen:**
1. Betrachten Sie Mobile Security nicht isoliert, sondern als wichtigen Teil Ihres IE-Sicherheitskonzepts. 2. Finden Sie die richtige Balance aus Produktivität und Sicherheit. 3. Sensibilisieren Sie Anwender für die Risiken im Umgang mit mobiler IT. 4. Verschaffen Sie sich Transparenz in einem unübersichtlichen Markt. 5. Holen Sie sich externe Unterstützung. 6. Setzen Sie sich mit den Auswirkungen von Wearables auf Ihre IT-Sicherheit auseinander.

Evakuierung

Um Personen unterschiedlicher Herkunftsländer im Brandfall möglichst sicher aus einem Gebäude zu leiten, sollte neben den technischen Möglichkeiten im Bereich der Brandmeldetechnik und der Sprachalarmierung auch ein Konzept für die Gebäudeevakuierung existieren, betont die Zeitschrift GIT in der Ausgabe 11-2015 (S. 70/71). Falls

baurechtliche Vorgaben nicht dagegen sprechen, könnten statt einer Sprachalarmanlage auch **Brandmelder mit sprachunterstützter Alarmierung** eingesetzt werden. Inzwischen hätten sich Melder bewährt, die wahlweise über integrierte akustische Signalgeber, Blitzleuchte und Sprachausgabe verfügen. Auf diese Weise könne mit der Alarmierung, wenn gewünscht, gleichzeitig die Evakuierung eingeleitet werden. Da verschiedene Sprachdurchsagen multilingual generiert werden können, böten solche Melder gerade in Gebäuden, in denen sich internationales Publikum aufhält, entscheidende Vorteile.

Falschgeld

Im Darknet, dem nicht über allgemeine Suchmaschinen zugänglichen Teil des Internets, sollen aus Italien stammende, hochwertig gefälschte 20- und 50 Euro-Scheine angeboten worden sein, die nach einem Fälscherkreis **„Bologna"-Blüten** genannt werden, berichtet die FAZ am 13. November. Man hätte sie im Netz gegen digitale Währung wie Bitcoin zu einem Preis unter dem Nennwert erwerben können, etwa 25 bis 50 Prozent billiger. Die Scheine würden dann per Post verschickt. Nach Einschätzung der Bundesbank gehörten die „Bologna"-Fälschungen zu den größten Fällen von Falschgeld in Europa. 2014 seien in Deutschland gefälschte Euroscheine im Wert von 3,3 Mio. Euro entdeckt worden, eine Zunahme um 63 Prozent. Die gefälschten 20-er und 50-er aus Italien sollen 52 Prozent des Falschgeldes nach Stückzahlen ausgemacht haben und 36 Prozent nach Nennwert. Im ersten Halbjahr 2015 seien die Falschgeldzahlen abermals gestiegen, um 31 Prozent auf 50.500 Scheine im Wert von 2,2 Mio. Euro.

Frachtdiebstahl

In der Ausgabe 11-2015 von PROTECTOR nimmt Joerg Schib, Mitglied in der Tapa (Transport Asset Protection Association) Stellung zur Problematik des Frachtdiebstahls (S. 20/21). Allein in Europa werde der jährliche Verlust an Waren mit 8,2 Mrd. Euro beziffert. 2014 seien 1.102 Fälle gemeldet worden. Die Dunkelziffer dürfte allerdings um ein Vielfaches höher liegen. Besonders dramatisch sei die wachsende Gewalt und Gefahr für Leib und Leben. Längst seien normale Lkw fahrende Tresore geworden. Das Spektrum reiche von lückenloser GPS- und Satellitenüberwachung über verstärkte Bordwände und Türen bis hin zu ferngesteuerter Motorelektronik.

Gefahrenmeldeanlagen (GMA)

Mögliche **Fallstricke bei Fernzugriff und Fernwartung von GMA** behandelt in s+s report (Ausgabe 4-2015, S. 56–58) Rechtsanwältin Petra Menge. Sie schildert einen interessanten Praxisfall und gibt Tipps zum Datenschutz und zur allgemeinen Schadenprävention. Errichter sollten mit ihren Kunden genau besprechen, was diese brauchen und wollen. Der vorausschauende Errichter müsse dabei genau abwägen, was für ihn aus haftungstechnischer Sicht vertretbar und sinnvoll ist.

Geldautomatensicherheit

Kriminelle sprengen derzeit vor allem in Nordrhein-Westfalen reihenweise Geldautomaten (GA), meldet handelsblatt.com am 3. November. Während 2006 vier Geldautomaten in dem Bundesland gesprengt worden seien, seien es 2015 bisher bereits 38. Dabei

gingen die Täter stets nach dem gleichen Prinzip vor. Sie dichten die GA so ab, dass keine Luft mehr durchkommt und leiten dann Gas hinein.

Wer GA der Sparkasse bei ihren regelmäßigen Software-Updates erwischt, könne mit einem Trick in eine **Windows-Kommandozeile** gelangen und auf dem GA eigene Befehle ausführen, berichtet heise.de am 3. November. Neben Manipulationen am GA selbst ergebe sich so die Möglichkeit für einen Angriff auf das Netzwerk der Bank. Betroffen seien GA der Firma Wincor Nixdorf, die nicht nur bei der Sparkasse im Einsatz sind.

Geldwäsche

Wie die FAZ am 13. November berichtet, ziehen sich die Banken aus westlichen Ländern von Partnerbanken in der Karibik, in Osteuropa, in Asien und in Afrika zurück, weil sie Angst hätten, in den USA hohe Milliardenstrafen verhängt zu bekommen. Denn das könne passieren, wenn die Geschäftsbeziehung einer Partnerbank in einem Drittland mehr als zweifelhaft sei und ein Vergehen wegen Geldwäsche oder Terrorismusfinanzierung nachgewiesen werden könne. Auch der stärkere Austausch von Steuerdaten zwischen den Staaten mit dem Ziel der gemeinsamen Bekämpfung von Steuerhinterziehung zwinge die Banken westlicher Industrieländer, ihre Beziehungen zu den Partnerinstituten, den sogenannten Korrespondenzbanken, zu prüfen. Die Regeln, die von dem bei der OECD in Paris angesiedelten Arbeitskreis zur Geldwäschebekämpfung, der Financial Action Task Force, entwickelt werden, verunsicherten die Banken. Die Vorgabe, die Kunden der Korrespondenzbanken zu kennen, sorge unter dem Anglizismus „know your customer's customer" für enorme Verunsicherung in den Banken der Industrieländer.

Industrie 4.0

In der vernetzten Welt der Industrie 4.0 würden neue Herausforderungen auf das IT-Sicherheitsmanagement zukommen, schreibt die FAZ in einem Verlagsspezial **„Innovationstreiber IKT"** (Informations- und Kommunikationstechnik) am 19. November. In dieser vernetzten Umgebung bildeten sich unweigerlich Sicherheitslücken, die möglichst schnell zu identifizieren sind. „Das Unternehmen muss sich öffnen und schützen. Der klassische Werkschutz muss in die digitale Transformation", erkläre Alexander Pilger vom Systemhaus Controlware die Herausforderung. Zudem sei zu klären, welche Auswirkungen es auf den Produktionsprozess habe, wenn etwa manipulierte Daten in den Fertigungsstationen ankommen. Prävention sei gefragt. Eine Methode sei der **Schutz durch IT-Komponenten für die Produktionskontrolle,** wie sie etwa das Fraunhofer SIT als Prototyp entwickelt habe. Der Prototyp der Schutz-Konfiguration setze auf die genaue Identifizierung einzelner Komponenten über das Netzwerk. So ließen sich die Informationen derartig chiffrieren, dass nur eine zugelassene Werkzeugmaschine die Daten verarbeiten kann. Dafür sorge ein Digital-Rights-Management (DRM)-System. Hierbei würden Hardwaremodule zur Verschlüsselung der Daten direkt in den Maschinen angebracht. Mit der Blackbox sei zudem eine exakte Kontrolle über die Stückzahl der hergestellten Bauteile machbar. Wer sich selbst ein solches Konzept zusammenstellen will, müsse mit hohen Investitionen rechnen. Alternativ könne man auch mit einem Minimalstandard für IT- und Produktionssicherheit über die Runden kommen – dem sogenannten Notfallmanagement. Die Bereitschaft, ein solches einzusetzen, sei zurzeit allerdings gering. Gerade einmal die Hälfte aller deutschen Unternehmen greife darauf bei digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl zurück. Bei den Betrieben mit mehr als 500 Mitarbeitern seien es einer Umfrage

von Bitkom zufolge zwei Drittel der Firmen, bei denen mit 100 bis 499 Mitarbeitern die Hälfte, bei 10 bis 99 Beschäftigten 46 Prozent.

Wie IT-Abteilungen künftig von **militärischen Sicherheitsstandards** profitieren könnten, erläutert Gianluca De Lorenzis, FGND Group, im Verlagsspezial „Innovationstreiber IKT" der FAZ vom 19. November. Die Grundschutzkataloge des BSI umfassten mehrere Tausend Seiten. Wer sich mindestens an den wertvollen Hinweisen des BSI-Standards 100-2 orientiere, stoße dann schnell auf die Frage, wo man überhaupt ansetzen soll. Hilfe böten inzwischen immer mehr IT-Dienstleister mit Hard- oder Softwarelösungen an, die nach Standards von Militär und Geheimdiensten geprüft sind. Bei deren Auswahl sollten Unternehmen in erster Linie simulieren, ob die Lösung in der vorhandenen IT-Infrastruktur einsetzbar und skalierbar ist. Entscheidender Dreh- und Angelpunkt für die IT-Sicherheit sei stets die Authentisierung und der Umgang damit in der Lösung. Hier sollte man die Vor- und Nachteile eines zentralen Schlüsselservers, von Smart-Cards oder Token prüfen. Verschlüsselungstechnologien mit militärischen Wurzeln seien auch für das Firmen-Smartphone erhältlich. Dazu werde das Telefon zum Beispiel mit einer MicroSD-Karte aufgerüstet, auf der ein Smartchip Sitzungsschlüssel mit eingebautem Zufallszahlengenerator erstellt. Die Karte weise sich gegenüber einem speziell gesicherten VME-VoIP-Server aus, der die Verbindung zwischen zwei Endgeräten herstellt und kontrolliert. Erst dann starteten Gespräche und E-Mail-Versand. Bei der Auswahl dieser oder ähnlicher Technologien sollte man allerdings die Usability im Auge behalten.

In einem Verlagsspezial Industrie 4.0 der FAZ am 17. November erläutert Wolf Lichtenstein, SAS, wie man die **digitale Fabrik** schützt. Entscheidend sei ein ganzheitlicher Ansatz: Wer die digitale Fabrik absichern will, dürfe sich nicht einfach auf einzelne Komponenten stützen, sondern müsse das Zusammenspiel diverser Bereiche betrachten. Die potenziellen Angriffszonen im Hardware-Design erstreckten sich über drei Ebenen: das Gehäusedesign, das Platinen-Layout und die Firmware. Es gelte, den Blick auf die Daten zu richten. Welche Daten seien eigentlich in den eigenen Produktionsmaschinen vorhanden, und welche wolle und könne man rausgeben? RFID Tags könnten als Informationsträger an einzelne Maschinenkomponenten angebracht werden, mittels derer sich eine Maschinen-/Prozess-/Produkt-Einheit als sicher im Gesamtsystem ausweise. Das würde auch die Migration von 3.0 auf 4.0 „versichern". Wenn dann noch die entsprechende Netzwerksicherheit und Firewalls eingebaut sind, hätten alle beim Thema Sicherheit einen riesigen Schritt nach vorne getan. Alles münde in einen internen Change-Managementprozess. Denn die Mitarbeiter müssten die Konzepte auch mittragen. Die Cloud sei wichtig, kostengünstig und flexibel. Sie sei aber teilweise noch ein schwieriges Thema bei Industrieunternehmen. Noch gehörten Absatzzahlen, Produktions- und Maschinendaten nicht in die Cloud.

Hannes Schwaderer, Intel GmbH & EMEA Energy Sector, befasst sich im Verlagsspezial Industrie 4.0 der FAZ am 17. November mit der **Verschmelzung der beiden Faktoren Big Data und Industrie 4.0.** Sie erfordere ein neues Denken. Beachte man die Menge und Relevanz der Daten, so müsse Sicherheit an erster Stelle stehen. In Zukunft würden herkömmliche Sicherheitssysteme nicht mehr ausreichen, Unternehmen vor IT-Angriffen zu schützen. Wichtig sei, dass es einen Ausgangspunkt gibt, der sicher und unveränderbar ist. Diese „Root of Trust" sei idealerweise direkt in der Hardware verankert, denn Silizium könne im Nachhinein nicht mehr geändert werden.

Schritt für Schritt zum sauberen Netzwerk nach einem Cyberangriff ist das Thema eines Beitrags von Thomas Uhlemann, ESET, im

Verlagsspezial Industrie 4.0 am 17. November. Komme es zu einem Zwischenfall, sollte man zunächst einmal das Ausmaß des Angriffs ermitteln. Ein funktionierendes **IT-Notfallmanagement** liefere schnelle und umfassende Antworten. Hat das IT-System stärkeren Schaden genommen, sollten nun Reservesysteme und redundante Netzwerkverbindungen aktiviert werden. Netzwerke, in denen sich die befallenen Rechner befinden, müssten abgekoppelt werden. So werde den Angreifern der Zugang versperrt und sie könnten keine weiteren verwertbaren Daten abgreifen. Anschließend sollte man versuchen, den eventuell verschlüsselten Datenverkehr zwischen den infizierten IT-Systemen im eigenen Netzwerk und den Rechnern der Angreifer zu decodieren. Es folge das große Aufräumen. Die befallenen IT-Systeme müssten von sämtlicher Schadsoftware gesäubert, die Einfallstore gesichert werden. Zusätzlichen Schutz biete eine Analyse der Datenpakete, die über das Netzwerk transportiert werden. Zu überprüfen sei, ob hier Verkehrsmuster und Befehle zu erkennen sind, die von den Angreifern verwendet wurden. War der Angriff Teil eines „Advanced Persistent Threat", dann sei davon auszugehen, dass ähnliche Attacken folgen.

Ingo M. Rübenach, UL International Germany GmbH, thematisiert in der FAZ am 27. November **Sicherheit als Herausforderung für eine Industrie 4.0-Welt.** Entwicklungen von der Smart Factory über Connected Car, Connected Home und Smart Metering bis hin zu Smart Watches und anderen Wearables stellten ganz neue Ansprüche an die Sicherheit. Für Hersteller und Anbieter werde Sicherheit ein Kernbestand des Umsetzungsprozesses von Industrie 4.0. Eine extrem dynamische Arbeitsumgebung habe gravierende Konsequenzen für die Arbeitssicherheit. Gemeinsam müssten die Industrie und die Sicherheits- und Zertifizierungsunternehmen erforschen, wie Sicherheit in diesem Kontext definiert und gewährleistet werden kann. Cyberphysische Systeme vor unautorisierten Zugriffen und Fehlsteuerungen zu bewahren, sei aufgrund ihrer Vernetzung eine enorme Herausforderung. Es gelte daher, ein völlig neues Zusammenspiel von Betriebssicherheit, Datenschutz und Informationssicherheit zu realisieren und diese Sicherheitsaspekte in den Komponenten und Systemen zu integrieren. Es werde die große Aufgabe von Forschung, Wirtschaft sowie Normierungs- und Zertifizierungsunternehmen sein, gemeinsam geeignete Sicherheitsanforderungen an die dynamische Industrie 4.0-Welt und das Internet of Things zu definieren.

IT-Sicherheit

heise.de meldet am 10. November, SAP habe 21 Sicherheitslücken in der In-Memory-Plattform HANA geschlossen. SAP empfehle allen Nutzern, die Updates zügig einzuspielen. Sechs der acht als kritisch eingestuften Lücken ließen sich nicht patchen. Nutzer müssten ihre Systeme rekonfigurieren, um sich abzusichern. Denn in der Standardeinstellung könnten Angreifer das TrexNet-Interface aus der Ferne attackieren.

Auf die **Reformierung des Grundschutzes** durch das BSI weist der Behörden Spiegel in seiner November-Ausgabe hin. Ein vorrangiges Ziel sei die Flexibilisierung und Verschlankung, womit vor allem eine bessere Skalierbarkeit erreicht werden soll. Der erste Schritt zur Implementierung des Grundschutzkatalogs solle künftig ein Basisschutz sein, der vor allem auf kleine und mittelständische Unternehmen sowie auf kleine Behörden zugeschnitten sei. Aufbauend auf dem Basisschutz erfolge bei Bedarf eine Standardabsicherung, die hohen Sicherheitsanforderungen genügt. Im Gegensatz zum neuen Basisschutz solle die Standardvariante unverändert bleiben. So sei zum Beispiel weiterhin eine ISO 27001-Zertifizierung auf der Basis von BSI-Grundschutz vorgesehen. Neu sei ein Konzept, mit dem der jeweilige

Reifegrad der IZT-Security bestimmt werden soll. Insgesamt sechs Reifegrade würden durch das BSI näher beschrieben. Für die Risikoanalyse würden in Zukunft die hierfür nötigen Arbeitsschritte in dem neuen BSI Standard 200-x gebündelt, der unter anderem eine Anleitung für einen Risikoentscheidungsprozess enthalten werde.

In seiner November-Ausgabe berichtet der Behörden Spiegel über einen Vortrag von Martin Schallbruch, BMI, zu den **Auswirkungen des IT-Sicherheitsgesetzes.** Bei der Durchführung der Meldepflicht bedürfe es einer namentlichen Nennung von Unternehmen nur dann, wenn die Funktionsfähigkeit des gesamten Unternehmens gefährdet sei oder wenn Folgen für eine gesamte Branche zu befürchten seien. Da das BSI nicht dem Legalitätsprinzip unterliege, werde es in der Mehrzahl der IT-Angriffe, die dem BSI gemeldet werden, nicht zu einer Namensnennung kommen.

Nemanja Malisevic, Microsoft, plädiert nach einer Meldung des Behörden Spiegel in seiner November-Ausgabe für international geltende Cybersicherheitsnormen. Staaten sollten nicht versuchen, Backdoors in Software einzubauen und sie sollten es unterlassen, Schwachstellen in IT-Produkten zu lagern und zu verkaufen, sondern stattdessen den Herstellern Schwachstellen melden.

Silicon.de weist am 26. November auf ein Grundsatzurteil des BGH hin, nach dem Access Provider den Zugang zu **Webseiten mit urheberrechtsverletzenden Inhalten** unter gewissen Umständen sperren müssen. Das sei dann der Fall, wenn es keinen anderen Weg gibt, die Urheberrechtsverletzung auszuschalten. Bevor die sogenannten Access-Provider in die Störerhaftung genommen werden können, müssten die Rechteinhaber zunächst gegen die „Host Provider" und die Betreiber der Webseite vorgehen. Dazu gehörten auch zumutbare Nachforschungen, wenn die korrekte Adresse des Betreibers nicht zu erfahren ist.

IuK-Kriminalität

Das BfV weist im „Cyber-Brief Nr. 01/2015" auf eine aktuelle Bedrohung von Unternehmen hin: Seit spätestens Juni sei eine Angreifergruppierung aktiv, die weltweit Wirtschaftskonzerne angreife. Sie versende eine E-Mail an die Abteilung für Öffentlichkeitsarbeit eines Unternehmens, in der mit der Presseveröffentlichung eines kompromittierenden Videos gedroht wird, das zu einem Imageverlust des Unternehmens führen könne, sodass sich der Empfänger gezwungen sieht, einen in der E-Mail angegebenen Link zu öffnen, um das Video auf seine Echtheit zu überprüfen. Durch das Aufrufen des Links installiere sich das Schadprogramm PlugX auf den Rechnern des Unternehmens. Um festzustellen, ob ein Unternehmen von dieser Angriffskampagne betroffen ist, empfiehlt das BfV, in den E-Mail-Eingängen nach einer möglichen E-Mail vom Absender hnn.hk mit dem Betreff: "Urgent: Confirmation needed regarding a tip-off video of your company staff" oder einer ähnlichen E-Mail zu suchen.

heise.de meldet am 26. Oktober, dass Betrüger einen im Jahr 2010 als Proof of Concept vorgeführten **Angriff auf die PIN-Prüfung von Kreditkarten** ausgebaut und so Transaktionen im Wert von 600.000 Euro getätigt hätten. Mit einem selbst entwickelten Chip sollen Betrüger die Kommunikation zwischen Kreditkarte und Terminal als „Man-in-the-middle" beeinflussen können. Sie sollen den Chip mit Original-Chips von gestohlenen Kreditkarten verlöten. Der aufgelötete Chip klinke sich in die Kommunikation zwischen Kreditkarte und Terminal ein. Dabei versichere der „Man-in-the-middle"-Chip dem Chip auf der Kreditkarte, dass sich der Karteninhaber über eine Unterschrift ausgewiesen habe. Dem Terminal gegenüber signalisiere er hingegen, dass die PIN-Prüfung erfolgreich war.

Die ICT-Welt werde gefährlicher, betont Prof. Dr. Hannes P. Lubich, Fachhochschule

Nordwestschweiz, in der Ausgabe 5-2015 der Zeitschrift Sicherheitsforum, S. 40–43. Probleme und Herausforderungen der Informationssicherheit seien in der Regel additiv und asymmetrisch. Additiv, da ständig neue Angriffsformen, Schwachstellen usw. zu einer bereits übermäßig komplexen ICT hinzukommen, die alten Schwachstellen und Angriffsformen aber nicht wegfallen. Asymmetrisch, da Angreifer meist den Weg des geringsten Widerstands gehen und dafür nur eine bekannte Sicherheitslücke kennen und ausnutzen, der Verteidiger jedoch möglichst alle Sicherheitslücken kennen und schließen müsse. Treiber seien im derzeitigen Lagebild insbesondere: Advanced Persistent Threats, Blended Attacks (Angriffe, die aus dynamisch und oft situativ miteinander kombinierbaren Teilschritten bestehen, die für den Angreifer wie aus einem Baukasten wählbar, für den Betroffenen in ihrem Zusammenhang jedoch kaum rechtzeitig als Angriffsmuster erkennbar sind) und Cybercrime as a Service (vom organisierten Verbrechen teilweise in die Cloud verlegte Dienstleistungen). Der Autor sieht auf lange Sicht sechs sich abzeichnende Trends: Quanten-, Bio- und Neurocomputing werden die Rechenleistung massiv beschleunigen; software-definierte IT-Infrastrukturen; Big Data-Analysen; Systeme werden ihre „Resilience" verbessern, das heißt, sie werden auch angesichts eines laufenden Angriffs ihre Basisdienste noch aufrechterhalten können; Schutzmechanismen werden von den Gesamtsystemen hin zu einzelnen Anwendungen oder Datensätzen mit jeweilig spezifischem Schutzanspruch migrieren; aktive Verteidigung.

Zwei Studien von KPMG und Bitkom, die **E-Crime-Studie 2015** und der Studienbericht Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter, belegen nach einem Bericht von TECCHANNEL.de vom 12. November für die QGroup, dass mittlerweile rund die Hälfte der deutschen Unternehmen von der Cyberkriminalität betroffen seien. Doch die Gefahren würden noch immer unterschätzt. Webseiten von Unternehmen aus dem Bereich Medien stellten ein besonders begehrtes Ziel für Hacker dar.

TECCHANNEL.de berichtet am 15. November, eine Studie von Blue Coat zeige, dass einige neue **Top-Level-Domains** (TLDs) bis zu 100 Prozent verdächtige Webseiten aufweisen. Der Hauptgrund dafür seien nachlässige Vergabekriterien. Das Ranking der TLDs mit zweifelhaften Sites im Internet werde angeführt von .zip, .review und .country. Die zweifelhaften TLDs bildeten eine hervorragende Basis für kriminelle Aktivitäten. Die meisten würden für Spam- und Scam-Angriffe sowie die Verteilung von unerwünschter Software genutzt. Eine zunehmend beliebte Masche von Scam-Betrügern sei es, Besucher auf eine Seite zu locken, die so ähnlich aussieht wie YouTube. Folgende Tipps sollten als Grundschutz beachtet werden: Unternehmen sollten die riskantesten TLDs generell blockieren. Nutzer sollten mit höchster Vorsicht auf Links in Suchergebnissen, E-Mails oder sozialen Netzwerken klicken, vor allem, wenn sie zu Webseiten mit diesen TLDs führen. Um zu verifizieren, wohin genau ein Link führt, sollten Nutzer mit der Maus den Link berühren, ohne ihn anzuklicken. Auf mobilen Endgeräten lasse sich ein Link verifizieren, indem der Nutzer ihn berührt und anschließend kurz hält, anstatt ihn nur anzutippen.

Sicherheitsforscher warnen davor, dass Cyberkriminelle mit vergleichsweise einfachen Methoden einen Großteil der weltweiten Öl-Produktion kontrollieren könnten, berichtet heise.de am 17. November. Kryptologen der Sicherheitsfirma ERPScan würden aufzeigen, wie es um die Sicherheit der **IT- und Operational Technology-Systeme (OT-Systeme) der Gas- und Öl-Industrie** stehe. Dabei beschreiben sie vielfältige Angriffspunkte, um in ERP (Enterprise Resource Planning)-Systeme einzusteigen. Hacker könnten so etwa im schlimmsten Fall 75 Prozent der weltweiten Ölproduktion kontrollieren. Das Problem sei, dass viele OT-Systeme eng mit IT-Systemen

verzahnt sind. Gelangen Hacker über ein IT-System in kritische Steuerungssysteme, könnten sie Schwachstellen ausnutzen. Dabei beziehen sich die Forscher unter anderem auf jüngst aufgedeckte Speicherfehler in SAP HANA.

Sicherheitsforscher haben wieder einmal **Lücken in Barcode-Verarbeitungssystemen** dokumentiert, meldet heise.de am 18. November. Sie hätten entdeckt, dass man mit bestimmten Scannern angeschlossene Systeme dazu bringen kann, Schadcodes auszuführen, allein durch das Scannen eines oder mehrerer Badcodes. Den Angriff würden sie BadBarcode nennen. Dabei nutzten sie aus, dass die Scanner gegenüber dem Host-System als USB-Tastaturen fungieren und man mit speziellen ASCII-Kontrollzeichen Hotkeys aktivieren und so etwa unter Windows ein Ausführen-Fenster öffnen kann. Da die Sicherheitslücken in vielen verschiedenen Scannern auftauchen, werde es lange dauern, alle Lücken zu schließen. Momentan könne man wohl nur versuchen, keine Scanner zu verwenden, die sich gegenüber dem Host-System wie eine Tastatur verhalten. Ist ein solches Gerät im Einsatz, könne man Hotkeys deaktivieren und sollte grundsätzlich dafür sorgen, dass das Betriebssystem mit den neuesten Sicherheitsupdates versorgt wurde.

Nach einem Bericht in der FAZ am 20. November hat Bundesinnenminister Thomas de Maizière auf dem Nationalen IT-Gipfel in Berlin eine schärfere Anwendung der bestehenden Gesetze gegenüber lückenhafter Software gefordert. Die Sicherheitslücken in diesen Programmen verursachten Jahr für Jahr Schäden in zweistelliger Millionenhöhe. Der Schutz der IT-Systeme durch die Anwender könne mit den oft hoch entwickelten Werkzeugen zur Ausnutzung von Sicherheitslücken nicht immer Schritt halten. Einige Softwarehersteller tendierten dazu, für die aus ihrer Sicht weniger schwerwiegenden Sicherheitslücken in ihren Produkten keine Sicherheitsupdates mehr bereitzustellen.

Beunruhigt habe sich der Minister daneben über die wachsende Zahl von Angriffen auf industrielle Produktionsanlagen gezeigt. Hierdurch entstünden neue betriebs- und volkswirtschaftliche Risiken. Die Kritik des Ministers werde durch den aktuellen **Lagebericht des BSI** unterfüttert. (Eine zusammenfassende Bewertung aus diesem Lagebericht findet sich auf der Webseite von Securitas Deutschland unter „Sicherheitslage".) Dutzende deutsche Unternehmen seien von einer Gruppe namens **Dragonfly mit dem Schadprogramm Havex** angegriffen worden. Das Ziel: die Kontrollen über industrielle Steuerungsanlagen. Mit Blick auf Schwachstellen schneiden dem BSI zufolge populäre Softwareprodukte schlecht ab. Dies seien Adobes Flash, Microsofts Internet Explorer sowie die Betriebssysteme Apple Mac OS X und Microsoft Windows. Bei ihnen seien bis September mehr als 100 kritische Schwachstellen registriert worden. Das BSI poche darauf, dass Hersteller über den gesamten Lebenszyklus ihrer Produkte Verantwortung für die Sicherheit übernehmen müssen.

Spiegel.de berichtet am 24. November von einer Malware, mit der **Kreditkartenterminals infiziert** werden können. iSight habe die Schadsoftware bereits 2014 entdeckt. Nach Angaben dieser Firma sei es schwierig, das Programm zu analysieren, weil es so komplex und ausgeklügelt sei. iSight zufolge besteht das Programm aus Modulen, einige davon sollten bereits in den Jahren 2012–2014 eingesetzt worden sein. Die Experten der Sicherheitsfirma vermuteten, die ModPOS getaufte Malware könnte in Osteuropa entwickelt worden sein.

Korruption

Das **„Gesetz zur Bekämpfung der Korruption"**, das der Bundesrat gebilligt hat, sei ein weiterer Schritt zur Eindämmung internationaler Korruption, ist die FAZ am 18. Novem-

ber überzeugt. Es überführe Bestechungsvorschriften aus Nebengesetzen in das Strafgesetzbuch und verschärfe bestehende Bestimmungen. Die Verfolgung von Korruption im Ausland werde wesentlich erleichtert, die Ermittlungen von Staatsanwaltschaften und Gerichten würden vereinfacht. Wer in Zukunft einem europäischen Amtsträger Vorteile gewährt, riskiere Ermittlungen und eine Bestrafung. Nach der Neufassung der entsprechenden Norm sei kein Bezug zum internationalen geschäftlichen Verkehr oder eine erstrebte Auftragserlangung mehr notwendig. Die Neuregelung werde erhebliche Bedeutung für Unternehmen erlangen, die international mit Amtsträgern zusammenarbeiten, etwa bei der Forschung und Entwicklung im medizinischen Sektor, oder die Geschäftsbeziehungen zu ausländischen Dienststellen unterhalten. Auch die exportierende Industrie werde sich auf die neuen Regeln einstellen müssen. Der Tatbestand der Bestechung von Angestellten sei nunmehr auch dann erfüllt, wenn der Mitarbeiter als Gegenleistung für die Zuwendung eine Handlung vornimmt und dabei seine Pflichten verletzt. Auf einen nachweisbaren Schaden des Unternehmens komme es für eine Bestrafung nicht mehr an. Auch steuerrechtlich würden die neuen Strafvorschriften eine erhebliche Bedeutung bekommen. Korruptionszahlungen dürften nicht als Betriebsausgabe gebucht werden.

Maschinensicherheit

Elektromechanische Zuhaltungen, mit denen sich GIT in der Ausgabe 11-2015, S. 78–80, befasst, seien bewährte Sicherheitsbauteile, um Gefahrenstellen an einer Maschine abzusichern. Da mit diesen Sicherheitsbauteilen der Zugang zur Gefährdung verhindert, und zudem auch noch die Bearbeitung in der Maschine gegen eine Unterbrechung geschützt wird, sei die klassische Zuhaltung auch heute noch eine gern und häufig genutzte Sicherheitsmaßnahme für Maschinen und Anlagen. Ein Prinzip, das für eine Zuhaltung mit Personenschutzfunktion möglich ist, laute „Energie ein entsperrt, Energie ein zugehalten". Bei dieser Art Zuhaltungen verbleibe das Sperrmittel in der Stellung, in der es bei Abschalten der Spannungsversorgung ist und ändere den Status nicht. Solche Zuhaltungen seien als sogenannte bistabile Versionen bereits seit Jahren erhältlich. Mit einer elektromechanischen Zuhaltung für den Personenschutz lasse sich eine Schutztür in jedem gewünschten und benötigten Performance Level (PL) nach EN ISO 13849-1 absichern. Der Beitrag behandelt ferner die Auflistung der Fehlerausschlüsse, die Kategorie 3 ohne Fehlerausschluss, die Zuhaltung in Kategorie 4, die Zuhaltung für den Personenschutz und die Überwachung der Zuhaltestellung.

Peter Stoevesand, Phoenix Contact Electronics, beschreibt in der Ausgabe 11-2015 der Zeitschrift GIT die **funktionale Sicherheit in der Prozesstechnik** (S. 86–88). Eine der wichtigsten Aufgaben in der produzierenden Industrie liege darin, das Risiko, dass Mensch und Umwelt während des Fertigungsprozesses einen Schaden erleiden, auf ein Minimum zu reduzieren. Während in der Prozessindustrie überwiegend die internationalen Standards IEC 61511 und IEC 61508 maßgeblich sind, werde im Maschinenbau auf Basis der EN ISO 13849-1 sicher automatisiert. Hatten viele Anlagenerrichter und -betreiber bisher kaum Berührungspunkte mit der funktionalen Sicherheit, müssten ihre Applikationen nun auch die Anforderungen der Maschinenrichtlinie erfüllen. Der Autor behandelt mV-Werte und Explosionsschutz als begrenzendes Auswahlkriterium für Sicherheitssteuerungen und zeigt an zwei Anwendungsbeispielen, wie sich die sicheren Interfaces in der Industrie einsetzen lassen.

Mit der Frage, welche **Option für die Kopplung der Komponenten und Signale** von Anlagen der Maschinensicherheit vorzuziehen ist – parallele Verdrahtung, sichere

Ethernetsysteme oder flexibel mit „Safe Link" der Firma Bihl+Wiedemann GmbH – befasst sich die Ausgabe 11-2015 der Zeitschrift GIT (S. 80–82). Zur Beantwortung der Frage lägen inzwischen genügend Erfahrungswerte vor. Die sichere Kopplung durch konventionelle Verdrahtung sei flexibel, aber unnötig aufwändig und extrem unübersichtlich. Die Anwendung der sicheren Ethernetsysteme sei eher unflexibel und oft relativ teuer. Safe Link sei eine Technologie, die es ermöglicht, sichere Steuerungen ganz einfach, unschlagbar effizient und höchst flexibel miteinander zu verbinden.

Dr. Volker Rohbeck, Leuze electronic, behandelt in der Ausgabe 11-2015 der Zeitschrift GIT (S. 93–95) das **Trendthema Muting** – die bestimmungsgemäße Überbrückung einer Schutzeinrichtung. Diese bestimmungsmäßige Unterbrechung einer Sicherheitsfunktion habe ihre Tücken, zumal die relevanten Normen EN ISO 13855, IEC/EN 61496-1 und IEC/TS 62046 neu sind oder geändert wurden. Der Autor beschreibt neue normative Anforderungen, grundlegende Muting-Varianten sowie mögliche Alternativen und vermittelt konkrete Entscheidungshilfen. Auch eine Muting-Funktion dürfe das Sicherheitsniveau nicht absenken. Dazu seien geeignete Muting-Sensoren bzw. -signale und Auswerteverfahren zu verwenden.

Parkhaussicherheit

Sicherheit in Parkhäusern thematisiert Hendrick Lehmann, Redaktion PROTECTOR in der Ausgabe 11-2015 (S. 22–24). Das Wichtigste sei die ausreichende **Beleuchtung** der Parkräume im Sinne der Normen DIN EN 13201 und DIN EN 12665 sowie der jeweils geltenden Garagenverordnung. Danach sei unter anderem an Stellen der Nutzfläche eine Beleuchtungsstärke von mindestens 20 Lux zu erreichen. Parkhäuser und Tiefgaragen stellten aufgrund ihrer Konstruktion besondere Anforderungen an den Brandschutz. Immer häufiger kämen in Parkhäusern Sprinkleranlagen zum Einsatz. In Tiefgaragen seien sie vorgeschrieben, wenn der Fußboden der Geschosse mehr als vier Meter unter der Geländeoberfläche liegt und das Gebäude nicht allein der Garagennutzung dient.

Parkhausbetreiber sollten auf ein individuelles und **umfassendes Sicherheitskonzept** setzen, bestehend auf intelligenter Branddetektion und Videoüberwachung, betont die Zeitschrift GIT in der Ausgabe 11-2015, S. 22–24). Der linienförmige Wärmemelder SecuriSens ADW 535 basiere auf einem einfachen physikalischen Prinzip, setze dieses aber komplex um: Bei Feuer steige die Umgebungstemperatur und gleichzeitig erhöhe sich der Luftdruck. Dieser Druckanstieg werde von luftgefüllten Fühlerrohren auf einen empfindlichen Sensor in der Auswerteeinheit übertragen. Sobald ein definiertes Limit überschritten wird, schlage das System Alarm. Täuschungsalarme blende der Brandwächter dank eines intelligenten Algorithmus aus.

Politisch motivierte Kriminalität

Das BKA hat am 13. November über **Auswirkungen der Flüchtlingsthematik** auf die Gefährdungslage Politisch motivierte Kriminalität informiert. Die Flüchtlingssituation in ihrer gegenwärtigen Ausprägung stelle sowohl für die Innen- und Europapolitik als auch für den gesellschaftlichen Raum das herausragende Thema dar. Die weitere Entwicklung der Flüchtlingssituation sei von einer unbestimmten Zahl weltweiter Einflussfaktoren abhängig und lasse sich hinsichtlich der Auswirkungen auf die Innere Sicherheit Deutschlands polizeilich nur bedingt prognostizieren. Eine Beruhigung der Lage sei kurz- und mittelfristig nicht zu erwarten. Einzukalkulieren sei, dass Wirtschaftsunternehmen ins Zielspektrum linker Agitation geraten, die beispielsweise als

Profiteure einer negativ bewerteten Unterbringungssituation der Flüchtlinge, oder aber als mittelbare oder unmittelbare Verantwortliche hierfür, ausgemacht werden.

Qualitätsmanagement

Markus Edel, VdS Schadenverhütung, weist in s+s report (Ausgabe 4-2015, S. 46/47) darauf hin, dass der weltweit führende Standard für Qualitätsmanagementsysteme, die ISO 9001, als ISO 9001:2015 neu erschienen ist und nach siebenjähriger Gültigkeit die Version ISO 9001:2008 abgelöst hat. Er gibt Tipps zur Dokumentationsstrukturierung, zur Kontextbestimmung, zur Risikoanalyse, zu Rollen und Verantwortlichkeiten, zur Planung und Durchführung von Änderungen, zum prozessorientierten Denken, zur Anwendbarkeit der Prozessumgebung und zur Vermeidung menschlicher Fehler.

Sicherheitsgewerbe

Die 2015 erschienene **Lünendonk-Studie „Sicherheitsdienstleister in Deutschland 2014“** enthält folgendes Management Summary: „Zum zweiten Mal in Folge steigerten die Unternehmen ihr Wachstum auf aktuell 5,3 Prozent. Besonders stark wuchsen die Security-Spezialisten mit 6,6 Prozent. Die FS-Multidienstleister kommen auf 5,1 Prozent. Die Übernahmen des vergangenen Jahres hinterlassen ihre Spuren: Kötter übernahm 2014 OSD Schäfer und Teile des Sicherheitsgeschäfts der ISS. Securitas ist erneut als Marktführer bestätigt. Mit ESD, Stölting, Secura Protect und IWS sind vier neue Unternehmen in der Lünendonk-Liste platziert. Die erwirtschafteten Margen verbessern sich: Zwischen zwei und fünf Prozent EBIT sind marktüblich. Der Mindestlohn wird von den Anbietern begrüßt. Die Hälfte wünscht sich gleiche Lohnverhältnisse in Ost und West. Im Mittel halten die Anbieter 9,70 Euro pro Stunde im Westen und 9,30 im Osten für eine angemessene Lohnuntergrenze. Die Industrie ist der wichtigste Kundensektor. Sie steht für mehr als 40 Prozent des Umsatzes im Markt. Für die Anbieter ist die öffentliche Hand als Auftraggeber genauso wichtig wie die Industrie mit je knapp 30 Prozent Umsatzanteil. Die Stimmung in der Branche ist gut. Kein Unternehmen gab an, pessimistisch in die Zukunft zu blicken. Das Branchenimage verbessert sich: Immer weniger Dienstleister geben an, dadurch behindert zu werden. Aktuell behindert das Preisniveau die Unternehmen am stärksten, mittelfristig sehen sie sich durch den Personalmangel noch stärker eingeschränkt.“ „Die Sicherheitstechnik wird wichtiger für die Dienstleister. Hier besteht Umsatzpotenzial. 2015 wurden 40 Unternehmen in die Studie einbezogen, die zusammen drei Mrd. Euro oder 56,6 Prozent des vom Branchenverband BDSW taxierten Marktvolumens erwirtschafteten. Insgesamt wurden drei Unternehmen mehr als im Vorjahr analysiert. Für 2016 erwarten die analysierten Unternehmen ein stabiles Wachstum von 5,2 Prozent. Der deutliche Anstieg an zu sichernden Unterkünften wird zu Sonderkonjunktureffekten im Geschäftsjahr 2015 führen.

Sicherheitstechnik

Änderungen des Errichteranerkennungsverfahrens von VdS erläutert Dipl.-Wirtschaftsjurist (FH) Sebastian Brose, VdS Schadenverhütung, in Ausgabe 4-2015 von s+s report, S. 43–45. Die zentrale Neuerung bestehe darin, dass es zukünftig in den Fachgebieten BMA, EMA und VÜA nur noch ein Errichteranerkennungsverfahren geben werde. Dabei handele es sich dann um „den VdS-Errichter“, der zukünftig unterschiedliche Fachrichtungen (EMA, BMA, VÜA) haben werde. Damit einher gehe eine Stärkung des VdS-Errichters und damit auch des VdS-Gütesiegels insge-

samt. Um zukünftig noch effizienter zu kommunizieren, werde vieles im neuen Verfahren auf elektronischem Wege abgewickelt.

Smart Home

Günther Ohland, SmartHome Initiative Deutschland e. V., befasst sich in Ausgabe 11-2015 von PROTECTOR, S. 56/57, mit der Problematik von **Standards** für Smart Home. Es gebe eine Vielzahl von Standards im Smart Home, die den unterschiedlichen Aufgaben und Sub-Systemen geschuldet seien. Das eine, allumfassende System über alle Anwendungen sei nicht notwendig und auch nicht sinnvoll, dazu seien die Anforderungen an die Subsysteme zu heterogen. Nahezu alle Systeme könnten über das Internetprotokoll IP und das lokale Netzwerk miteinander kommunizieren. Eine Interoperabilität zwischen den Subsystemen entstehe dadurch jedoch noch nicht. Erst umfassende Software-Produkte oder die Middleware EEBUS oder die neutrale Qivicon-Plattform ermöglichten den sinnvollen Austausch von Daten zwischen den einzelnen Subsystemen.

Spionage

Oft schon habe die Kanzlerin das Thema Computerspionage bei ihren Besuchen in **China** angesprochen, bisher ohne großen Erfolg, meint die FAZ am 31. Oktober. Nun tue sich etwas: Bis 2016 wollten beide Länder einen Verzicht auf Cyberattacken im Wirtschaftsbereich aushandeln, habe Premier Li angekündigt. Ein „offenes und sicheres Internet" wolle China nach den Worten Lis, und einen „harten Kampf gegen den Diebstahl von Geschäftsgeheimnissen". Zudem wolle China „energisch" gegen den „Diebstahl geistigen Eigentums" vorgehen.

silicon.de stellt am 2. November die **Telekom-Dienstleistung gegen Spionage in Unternehmen** vor. Neben Angriffen auf die IT eines Unternehmens versuchten Spione auch nach wie vor gern über Telefone, Yucca-Palmen oder andere Gegenstände im Büro vertrauliche Gespräche abzuhören. Kleine Wanzen oder andere Überwachungsgeräte könnten sich auch in Kaffeekannen oder Steckdosen befinden. Die Methoden würden immer ausgefeilter. Industriespione versteckten in Büros oder Konferenzräumen zum Beispiel SIM-Karten mit Funktechnik in verschiedenen alltäglichen Dingen wie etwa PC-Mäusen. Inzwischen könnten auch über größere Entfernungen akustische Schwingungen von Fensterscheiben über Laser gemessen werden. Daher rieten die Experten der Telekom, geheime Besprechungen mit heruntergelassenen Außenjalousien abzusichern oder die Konferenz in ein Zimmer mit Blick zum Innenhof zu verlagern. Die Experten der Telekom zeigten Unternehmen, wie sie Informations- und Abhörschutz verbessern könnten und erarbeiteten individuelle Schutzkonzepte. Darüber hinaus biete die Telekom Schulungen zum Umgang mit Top-Geschäftsgeheimnissen und dem Bewusstsein für Angriffsstrategien an und berate bei Bauvorhaben.

Steuerhinterziehung

Der illegale Handel mit Produkten sei ein globales Problem, durch das weltweit jährlich Steuereinnahmen in Milliardenhöhe verlorengehen, betont der Behörden Spiegel in seiner November-Ausgabe. Insbesondere der Zigarettenschmuggel stelle die Sicherheitsbehörden regelmäßig vor erhebliche Herausforderungen. Abhilfe könne nun die auf einer Smartphone-App basierende **Technologie „Codentify"** schaffen. Dieses sogenannte Tracking & Tracing-System scanne und entschlüssele einen auf jeder Zigarettenschachtel angebrachten, individuellen Code.

So könnten Informationen zum kompletten Herstellungs- und Versandprozess der Ware ausgelesen und mit Hinweisen, die in einer speziellen Datenbank hinterlegt sind, abgeglichen werden. Dies ermögliche das Nachvollziehen der gesamten Lieferkette (Tracking) sowie die Echtheits-Verifizierung jeder einzelnen Zigarettenpackung. Außerdem könne „Codentify" dazu beitragen, zu bestimmen, wann und an welchem Ort die Zigaretten in illegale Kanäle geleitet wurden (Tracing).

Unternehmenssicherheit

Wie der Bundesverband ASW am 13. November mitteilt, hat Control Risks die Studie **„The State of Organisational Resilience"** veröffentlicht. Resilience werde definiert als die Fähigkeit einer Organisation, disruptive Einflüsse zu identifizieren, ihr Eintreten vorherzusehen und bei deren Eintritt die Auswirkungen auf die Organisation zu minimieren und schnellstmöglich wieder in das Tagesgeschäft zurückzukehren. Die wichtigsten Ergebnisse der Studie: Es gebe Abweichungen zwischen der gefühlten Widerstandsfähigkeit und der realen Situation in der Organisation. 86 Prozent der befragten Unternehmen hätten in den letzten fünf Jahren eine Betriebsunterbrechung zu verzeichnen, 28 Prozent sogar mehr als sieben. Unternehmen fürchteten mehr den langfristigen Reputationsschaden als kurzfristige finanzielle Verluste. Politische Instabilität werde als relevanteste externe Bedrohung angesehen. Eine höhere Widerstandsfähigkeit zu erreichen sei schwierig. Bessere Risikoanalysen anstelle von reiner Risikobeobachtung, klare Verantwortlichkeiten und umfassende Einbindung von Zulieferern führten zu einer höheren Resilience.

Das **Kompetenzzentrum für internationale Sicherheit** an der Rheinischen Fachhochschule Köln stellt der Leiter dieses Zentrums Holger Berens in der Ausgabe 4-2015 von s+s report (S. 32–34) vor. Es bündele Expertenwissen im Bereich der Unternehmenssicherheit, Aus- und Weiterbildung, interdisziplinäre Auftragsforschung, Implementierung von Sicherheitssystemen und solle ein führender „Think Tank" im Bereich Wirtschaftsschutz werden. Unter dem Stichwort „Security-Themenpaten" biete das KIS außerdem für KMU einen Zugang zu einer ganzheitlichen Sicherheitsberatung. Der Autor behandelt die wirtschaftliche, die gesellschaftspolitische, die mediale und die wissenschaftliche Dimension des Beratungsangebots und veranschaulicht am Beispiel Reisesicherheit, vor welchen Herausforderungen gerade KMU in Sachen Compliance und Security stehen.

Corporate Security als Konzept thematisiert in s+s report, Ausgabe 4-2015, S. 40–42, Michael Bouché, Siemens Building Technologies. Sicherheitskonzepte für Unternehmen müssten so vielfältig sein wie die Firmen, Märkte und Branchen, in denen sie tätig sind. Bei der Umsetzung dieser Lösungen sei ihnen jedoch eines gemeinsam: Der Faktor Mensch spiele eine entscheidende Rolle für den Erfolg der verwendeten Technologie. Je mehr Menschen sich im Unternehmen bewegen, desto relevanter werde dieser Aspekt. Physische Sicherheitsvorkehrungen einerseits und organisatorisch und technische Maßnahmen andererseits müssten also so zusammenspielen, dass sie von allen Personen im Unternehmen akzeptiert werden und den Betriebsalltag in keiner Weise behindern. Der Autor behandelt insbesondere den Aspekt der Globalisierung, Cyberkriminalität und IT-Sicherheit, den Wettbewerbsdruck, Image und Compliance, den Faktor Mensch, die notwendige Alltagstauglichkeit der Technik, Corporate Security als Konzept und zentrale Sicherheitsstrukturen.

Videoüberwachung

Dipl. Telematik-Engineer Giray Aybet, Bosch Sicherheitssysteme, befasst sich in Ausgabe 5-2015 der Zeitschrift Sicherheitsforum, S. 19/20, mit **intelligenten Algorithmen.** Jede IVA (Intelligente Videoüberwachung)-Kamera von Bosch erstelle laufend Metadaten, die der IVA als Grundlage dienen. Diese Metadaten enthielten die Details zu allen Objekten innerhalb des überwachten Bereichs sowie zu allen Objekten, die in den überwachten Bereich hinein- bzw. aus diesem herausgelangen. Da Metadaten auch abgespeichert werden, könne die Analyse auch über beliebige Zeiträume in der Vergangenheit laufen und in Sekunden alle gesuchten Ereignisse liefern. Die Suche sei deshalb so effizient, weil die Metadaten ein wesentlich geringeres Datenvolumen als die zugehörigen Videobildaufzeichnungen aufweisen und weil die Rechenregeln sehr viel einfacher ausfallen. Die intelligente Videoanalyse nutze eine spezielle Methode für die Video-Contentanalyse und stelle die benötigte Bild-Rechenleistung direkt in der Kamera bzw. im Video-Encoder zur Verfügung. Natürlich gehöre auch zur IVA, dass sie sich automatisch an schwierige Bedingungen anpasst. Bei Sicherheitssystemen sei selbstverständlich, dass Alarme automatisch von einer integrierten Manipulationserkennung ausgegeben werden, wenn die Kamera abgedeckt, geblendet, verdreht oder der Fokus verstellt wird.

Dieter Jöcker, Bosch Sicherheitssysteme GmbH, erörtert in Ausgabe 11-2015 der Zeitschrift PROTECTOR, S. 26/27, die Möglichkeit der **Bildmanipulation** bei Videoaufnahmen. Selbst bei Live-Videos bestünden Möglichkeiten der Manipulation. Die klassische Man-in-the-Middle-Attacke funktioniere heute auch mit sehr viel datenintensiveren Videos. Dabei leite der Hacker den Datenstrom auf einen eigenen Rechner um, auf dem das Video bearbeitet werde, und sende die manipulierten Daten weiter an den ursprünglichen Empfänger. Ein heute sehr praktikabler Weg zum Nachweis der Authentizität von Videoaufnahmen sei die Implementierung von Verschlüsselungsmechanismen und digitalen Signaturen in der Kamera. Sei der generierte Hashwert identisch mit dem übertragenen Schlüssel, handele es sich um die Originalaufnahme. Zudem diene der Key zur eindeutigen Identifizierung der Kamera, sodass auch die Authentizität der Kamera jederzeit nachgewiesen werden könne. In einem weiteren Beitrag (S. 32/33) wird die Vorbeugung vor IP-Manipulationen erörtert. Der Einsatz von externen IP-Kameras setze die Bereitstellung eines externen Netzwerkanschlusses zur IP-Kamera voraus. Diese externen Anschlüsse könnten böswillig manipuliert werden, um Zugriff auf das unternehmensinterne Netzwerk zu erhalten. Es gebe eine technologische Lösung: **Linklock des britischen Unternehmens Veracity.** Es blockiere die Verbindungen zu allen Kabeln oder Geräten, die manipuliert bzw. abgekoppelt wurden, vollständig. Das Funktionsprinzip basiere auf der vollständigen Trennung des Daten- und Stromflusses von der Koaxialkabelverbindung und der sich ergebenden vollständigen Isolation der betroffenen Verbindung. Bei einer Standard-Videoüberwachungsanlage sei eine verschlüsselte Verbindung über ein Koaxialkabel unzureichend zur Verhinderung von unbefugten externen Zugriffen, da die Ethernetverbindung zur Kamera weiterhin offen und ungesichert bleibe. Jedoch erkenne die Linklock-Basiseinheit jeden Anzapf- und Trennungsversuch über das Koaxialkabel oder über die Netzwerkverbindungen und deaktiviere den POE- und Datenfluss sofort.

Analog HD als Alternative zu IP empfiehlt Florian Lauw, Abus Security-Center GmbH & Co KG, in Ausgabe 11-2015 der Zeitschrift PROTECTOR, S. 28/29. Bei vergleichbarer Leistungsfähigkeit lägen die Kosten für die Modernisierung eines vorhandenen analogen Videoüberwachungssystems mit Analog HD nur bei einem Bruchteil der Kosten, die für den Komplettaustausch auf IP-Technik an-

fielen. Aufgrund der überlegenen Auflösung gegenüber Analogtechnik seien bei Analog HD zudem insgesamt weniger Kameras notwendig, um ein Areal zu überwachen. Smarte Software, wie zum Beispiel die Tripwire-Detection-Funktion von Abus, spare durch selektive Datenspeicherung Speicherplatz, da die Aufzeichnung nicht kontinuierlich mitlaufe, sondern nur starte, wenn bewegliche Objekte eine zuvor definierte imaginäre Linie im Aufzeichnungsbereich in eine vorgegebene Richtung überqueren. Mit der zeitsparenden „Smart Search"-Funktion könnten alle Aufzeichnungen am Recorder nachträglich auf Bewegungsinformationen durchsucht werden.

Redundanz thematisiert PROTECTOR in Ausgabe 11-2015 (S. 30/31). Beim Hersteller Geutebrück würden je nach Recorderserie die Komponenten Netzteil, Lüfter, Netzwerkanbindung, Festplatten, RAID-Controller sowie für das Betriebssystem „Solid State Disks" standardmäßig oder optional in redundanter Ausführung angeboten. Sollten einmal ein oder mehrere Geräte komplett ausfallen, beugten sogenannte „Failover Konzepte" vor, die dank intelligenter Steuerung durch die Software die Verfügbarkeit sicherten. In Serverräumen seien Energieeffizienz und Platzbedarf ein Thema. Parallel werde meist die Verfügbarkeit hochprofessioneller Server-Hardware gefordert. Alle diese Herausforderungen ließen sich mit Virtualisierung meistern. Bei diesem Ansatz würden auf einem größeren physikalischen Rechnerverbund aus meist hochredundanten Servern „virtuelle Recorder" installiert, die für das Videosicherheitssystem wie eigenständige Geräte arbeiten. Falle ein Teil der Hardware – also ein physikalischer Server – aus, so zögen die virtuellen Maschinen von dieser Hardware um, und zwar auf einen anderen Teil der Hardware.

Die **Bildqualität** bleibe weiterhin das entscheidende Kriterium bei der Anschaffung einer Videoüberwachungslösung, ist Dirk Brand, Canon Deutschland, überzeugt (GIT, Ausgabe 11-2015, S. 38/39). Mit der 4K-Technologie stehe der nächste Technologiesprung bevor. Mit einer Auflösung von 3.840 x 2.160 Pixel produzierten 4K-Netzwerkkameras Bilder, die über die Auflösung von rund acht Megapixeln verfügten. Diese Verbesserung der Bildqualität und der Auflösung führe zu deutlicheren Livestream-Bildern, klareren Zoom-Bildern und einem breiteren Sichtfeld. Es gäbe aber auch Hindernisse. Die größte Hürde bestehe in den Kosten der zusätzlichen Komponenten. Für die Installation einer voll funktionsfähigen 4K-Überwachungslösung müsse die Netzwerkbandbreite und die Videospeicherung in der Kaufentscheidung Berücksichtigung finden. Und bei der Installation müssten die Auswirkungen bedacht werden, die mehrere 4K-Kameras auf das IT-Netzwerk haben. Daher würden einige Hersteller Unternehmen empfehlen, den Livestream in HD zu betrachten und die Vorteile von 4K für eine detaillierte Analyse zu nutzen.

Ludwig Bergschneider, ASP AG, erläutert in Ausgabe 11-2015 der Zeitschrift GIT (S. 40/41), warum **4K** zum neuen Auflösungsstandard in der Sicherheitsbranche werde. 4K biete einen außergewöhnlichen Szenenabdeckungsbereich, große Schärfe und Detailgenauigkeit. Die Kosten für eine 4K-Lösung erhöhten sich nicht zwangsläufig. 4K-Kameras könnten mit gleicher Detailgenauigkeit eine größere Szene abdecken als Full HD-Kameras. Die realen Kosteneinsparungen ergäben sich aus dem Bedarf an weniger Kameras vor Ort. Der Autor behandelt die Empfindlichkeit bei schwachen Lichtverhältnissen, die Objektiv-Kompatibilität und Verfügbarkeit, Auflösung, Bildrate und Netzwerkbandbreite sowie Upgrade und Kompatibilität. Das Zusammenwachsen der neuen Technologien trage dazu bei, dass der frühe Durchbruch der 4K-Technologie möglich werde.

Zutrittskontrolle

Franz Erni, Interflex-Allegion International AG, beschreibt in der Ausgabe 5-2015 der Zeitschrift Sicherheitsforum, S. 78–81, verschiedene Möglichkeiten des Zutrittskontrollsystems. Bei Zutritten in Sicherheitszonen sollte darauf geachtet werden, dass diese nicht allein mit dem Ausweis, sondern nur mit einem zusätzlichen Merkmal (PIN oder Biometrie) gewährt werden. Viele Firmen seien bestrebt, immer weniger Personen einen Schlüssel auszuhändigen und möglichst viele Türen mit Ausweisen zu bedienen. Hier lägen sogenannte Offline-Komponenten im Trend, die sich ohne Verkabelungsaufwand als ausweislesender Türbeschlag/Zylinder an Bürotüren montieren lassen. Immer wichtiger werde die Integration eines Videosystems sowie die Einbindung der Zutrittskontrolle in einen Sicherheitsleitstand bzw. in ein Gebäudemanagementsystem. Bei der Beschaffung eines Zutrittssystems gelte es generell darauf zu achten, dass das System mit den Anforderungen und Bedürfnissen mitwachsen kann.

Impressum

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

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

Herausgeber:
Manfred Buhl, Vorsitzender der Geschäftsführung, Düsseldorf

Verantwortlicher Redakteur:
Bernd Weiler, Leiter Kommunikation und Marketing

Beratender Redakteur:
Reinhard Rupprecht, Bonn

focus.securitas.de

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

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

E-Mail: info@securitas.de