Focus on Security

Ausgabe 11, November 2016

SECURITAS

Inhalt

Arbeitsschutz

Die Autoren Thomas Lange R.A. und Dipl.-Ing. Wolfgang Quednau, BTTA GmbH, weisen in GIT, Ausgabe 10-2016, S. 114–116, darauf hin, dass mit der neuen **PSA-Verordnung (EU) 2016/425** die alte Richtlinie 89/686/EWG dem „neuen Rechtsrahmen" angepasst wurde. Sie gelte unmittelbar in allen Mitgliedsländern der EU. Sie belasse zwar weiterhin die Hauptverantwortung beim Hersteller persönlicher Schutzausrüstung, implementiere aber weitere Hauptverantwortliche und reduzierte Pflichten für nachgelagerte Wirtschaftsakteure. Die Autoren beschreiben die Pflichten des Herstellers, des Einführers, des Händlers und des „Quasiherstellers". Jedes Unternehmen, das Produkte eines anderen mit seinem Namen und seiner Marke versieht und dann erstmals in der EU in den Verkehr bringt, werde wie ein Hersteller behandelt. Der Beitrag geht auch ein auf die beschränkte Gültigkeit der Baumusterprüfbescheinigung, auf die Gültigkeit „technischer Unterlagen" für alle PSA-Kategorien, auf die Zuordnung bestimmter Produktgruppen zur Kategorie III, auf die Änderung der Anforderung „Für die Signalisierung des Nutzers geeignete PSA" (Warnschutz), auf grundlegende Anforderungen für Schutzkleidung mit abnehmbaren Protektoren, auf Konformitätsbewertungsmodule und auf Übergangsvorschriften.

Bankensicherheit

Die meisten Banken unterschätzten die Auswirkungen der Digitalisierung, schreibt die FAZ am 13. Oktober. Das mag an der konservativen Kundschaft in Deutschland liegen. Zudem werde ein unglaublicher Investitionsstau in der IT der Banken beobachtet. Im Vergleich zu anderen Branchen sei die Finanzbranche untertechnisiert.

Betrug

CEO-Betrug sei eine der häufigsten Betrugsformen in Unternehmen, wobei Betrüger mit dieser Masche in E-Mails täglich Tausende Unternehmen ins Visier nähmen, schreibt Inkerman Fraud Weekly in der Ausgabe 181. Seit Januar 2015 sei der CEO-Betrug um 270 Prozent gestiegen und habe Unternehmen weltweit in den letzten drei Jahren schätzungsweise 2,3 Mrd. GBP gekostet. Damit verhindert wird, dass Unternehmen Opfer eines CEO-Betrugs werden, seien von einigen Unternehmen spezielle Sicherheitsmaßnahmen getroffen worden. In Deutschland sei ein kriminelles Netzwerk, das sich als Werbeunternehmen ausgegeben habe, Ziel polizeilicher Ermittlungen gewesen. Dabei sei aufgedeckt worden, dass die Daten von 1,5 Mio. deutscher Bürgern gehackt und ihre persönlichen Daten gestohlen wurden. Im Anschluss hätten die Betrüger ihre Opfer angerufen und ihnen eine hundertprozentige Gewinnchance bei Lotteriespielen versprochen. Von 95.000 Anrufen hätten sie 4.443 Leute überzeugt, 69 Euro für einen Zeitraum von zwölf Monaten in das „Lottospiel" zu investieren. Beamte der Betrugsbekämpfung hätten geschätzt, dass durch die Masche insgesamt rund eine Mio. Euro erbeutet wurden.

Betrugsversuche über falschen Support: Das ist das Thema von Martin Schindler in silicon.de am 25. Oktober. Immer mehr Nutzer meldeten laut einer Studie von Microsoft Betrugsversuche durch Personen, die sich als Support-Mitarbeiter großer Firmen ausgeben. Den Kontakt zu den potenziellen Opfern stellten sie über E-Mail, Telefon oder über Pop-up-Nachrichten auf Webseiten her. Auf diesen Wegen gaukelten die Betrüger den Anwendern vor, dass der Rechner von Viren befallen ist. Dann werde dem Nutzer eine Software angeboten, die angeblich das Gerät von dem Schädling befreien soll. Die Fernwartungssoftware sei aber tatsächlich ein Trojaner, über den die Kriminellen den

Rechner ausspähen können. Auf diesem Weg würden die Angreifer zum Beispiel versuchen, an Passwörter für das Online-Banking zu kommen. Die Betrüger ließen sich jedoch relativ einfach erkennen: Microsoft führe unter keinen Umständen unaufgeforderte Telefonanrufe durch, in denen das Unternehmen anbietet, ein schadhaftes Gerät zu reparieren. Microsoft schicke unaufgefordert weder E-Mails, noch fordere das Unternehmen per Telefonanruf persönliche oder finanzielle Daten an. Gibt sich der Anrufer als Mitarbeiter der Microsoft-Lotterie aus, dann stimme dies nicht. Es gebe keine Microsoft-Lotterie. Microsoft frage niemals nach Kreditkarteninformationen. Und es kontaktiere Nutzer nicht ungefragt, um über neue Sicherheits-Updates zu informieren.

Brandschutz

Dipl. Haustechnikplanerin Andrea Cottier, BDS Security Design AG, behandelt in Ausgabe 5-2016 der Zeitschrift Sicherheitsforum, S. 16–19, den **organisatorischen Brandschutz**. Dazu gehörten das Freihalten von Flucht- und Rettungswegen, eine brandschutztechnisch einwandfreie Ordnung, die Durchführung periodischer Betriebskontrollen und die Mängelbehebung. Organisatorische Maßnahmen im Brandschutz seien in der Regel personalintensiv. Es sei daher zwingend, die organisatorischen Strukturen für die Brandschutz- und Evakuations-Organisationen so knapp wie möglich zu gestalten. Andererseits funktioniert die Organisation während der Betriebsphase einfacher. In den einzelnen Pflichtenheften werde klar definiert, welche Aufgaben im Normalbetrieb zu erfüllen sind. Wichtig sei aber auch das Pflichtenheft für den Ereignisfall. Organisatorischer Brandschutz sei nur so gut, wie er im Alltag gelebt wird. Jeden Organigramm, jedes Pflichtenheft und jede Checkliste sei unnütz, wenn die jeweiligen Mitarbeiter ihre Pflichten nicht ernst nehmen. Eine gute und regelmäßige Übungspraxis sei besser als dicke schriftliche Dokumente. Die sollten übersichtlich und einfach auszufüllen sein.

Chemikalienrecht

Dr. sc. nat. chem. Lukas Felix und Dr.-Ing. Mathias Breimesser, Neosys AG, befassen sich in der Ausgabe 5-2016 der Zeitschrift Sicherheitsforum, S. 21–23, mit **Reach** (Registration, Evaluation, Authorization and Restriction of Chemicals) **und Chemikalien in Erzeugnissen**. Von Reach betroffen seien alle Erzeugnisse und Gemische, welche in der EU in Verkehr gebracht werden. Für Stoffe und Gemische würden Forderungen gelten, die für Erzeugnisse nicht gelten. Stoffe in Erzeugnissen müssten beim Import in die EU oder Herstellen ab einer Menge von mehr als einer Tonne pro Jahr in der EU nach Art. 7 Abs. 1 in Reach bei der europäischen Chemikalienagentur (Echa) registriert werden. Wenn die Stoffe unter vorhersehbaren Verwendungsbedingungen aus den Erzeugnissen freigesetzt werden. Als Sonderfall definiere die Echa im Leitfaden Erzeugnisse mit Gemischen als integralen Bestandteil. Für die Klassifizierung von Grenzfällen sei der Leitfaden der Echa eine gute Entscheidungshilfe. Der Beitrag zeigt, wann genau aus Gemischen ein Erzeugnis wird. Die Autoren weisen auch auf den wichtigen Grundsatzentscheid des Europäischen Gerichtshofes 2015 hin. Um die Sicherheit in der Lieferkette zu gewährleisten, gelte der Grenzwert für jeden einzelnen, individuell hergestellten Bestandteil eines Produkts. Der Entscheidungsprozess solle möglichst genau dokumentiert sein. Lieferanten sollten angefragt werden, ob und wie viel Kandidatenstoffe in den von ihnen gelieferten Produkten enthalten sind. Sollte ein Lieferant aus einem Staat außerhalb der EU die erforderlichen Daten zur Erfüllung der Reach-Pflichten nicht bereitstellen, empfehle die Echa, sich nach einem Lieferanten mit Sitz in der Gemeinschaft umzusehen.

Compliance

Nikolaus C. Krenzel und Daniel Kautenburger-Behr, Ebner Stolz, weisen in dem Verlagsspezial Zukunft Mittelstand der FAZ vom 20. Oktober auf eine aktuelle Studie der Prüfungs- und Beratungsgesellschaft Ebner Stolz und des F.A.Z.-Instituts hin, in der mittelständische Unternehmen aus unterschiedlichen Branchen mit einem Jahresumsatz bis zu maximal 750 Mio. Euro zum Thema Compliance befragt wurden. Am meisten fürchteten sich die Mittelständler vor einem Reputationsverlust (86 Prozent) durch Compliance-Verstöße. 75 Prozent scheuten sich vor den wirtschaftlichen Einbußen und strafrechtlichen Sanktionen. 68 Prozent der befragten Unternehmen hätten angegeben, dass sie mit Compliance-Verstößen Wettbewerbsnachteile erleiden könnten. 85 Prozent hätten angegeben, dass vermehrt Kunden und Geschäftspartner die Einhaltung von Compliance-Strukturen verlangen. Eindeutig sei das Votum auf die Frage, ob die Einführung von Compliance-Strukturen bloße Pflichterfüllung sei oder einen Mehrwert erbringe. 90 Prozent der Befragten sähen als Zusatznutzen mehr Sicherheit, 83 Prozent eine Transparenzsteigerung. Der größte Handlungsbedarf werde beim Datenschutz (98 Prozent) und der IT-Sicherheit (92 Prozent) gesehen, dicht gefolgt vom Arbeits- und Steuerrecht (86 und 82 Prozent). Umfassende Compliance-Managementsysteme bestünden in weniger als der Hälfte der Unternehmen. Einzelmaßnahmen, deren sich in erster Linie die Geschäftsführung oder Abteilungsleiter annähmen, würden überwiegen. Sie würden je nach Risikograd schrittweise in einzelnen Modulen implementiert. 58 Prozent der mittelständischen Unternehmen hätten angegeben, dass die Compliance-Investitionen in Zukunft steigen würden.

Dipl.- Umwelt-Natw. ETH Niklaus Renner, IPSO ECO AG, zeigt in Ausgabe 5-2016 der Zeitschrift Sicherheitsforum, S. 34-36, die Vorteile von **Legal Compliance-Softwares**. Sie unterstützen Unternehmen dabei, sich auf die Vielzahl an regulatorischen Anforderungen einzustellen. Sie seien in Form thematisch gegliederter Fragebögen aufbereitet. So könne die Nachweispflicht unternehmensspezifisch und entsprechend der einschlägigen INO-Normen erfüllt werden. Vorteile der Softwares seien Praxisnähe und Benutzerfreundlichkeit, verständliche Infos, Zeit- und Kostenersparnis, übersichtliche Gliederung der Anforderungen, Konformitätsnachweis per Mausklick und MS/Outlook-Schnittstelle. Der Beitrag geht näher ein auf die Rechtskonformität in einem dynamischen Umfeld, auf die Schaffung von Bewusstsein und Transparenz, auf die die Implementierungsphase und die personenzentrierte Zuordnung.

Einbruchmeldetechnik

GIT bringt in der Ausgabe 10-2016, S. 29, einen Überblick über die im Zusammenhang mit einer EMA zu beachtenden Normen und Richtlinien: DIN VDE 0833-1 und 0833-3, DIN EN 50131-1, VdS 2311 und Richtlinien ÜEA. Nach wie vor gelte grundsätzlich die Aussage, dass unter Einbeziehung der Richtlinie VdS 2311 auch die DIN VDE 0833-3 eingehalten ist. Doch sind die VdS-Klasse und der Grad aus der DIN VDE 0833-3 zu berücksichtigen. So deckt z. B. die VdS Klasse A den Grad 1 vollständig und den überwiegenden Teil des Grades 2 ab. Gleiches gelte für die VdS Klasse B in Bezug auf die Grade 2 und 3 und für die VdS Klasse C in Bezug auf die Grade 3 und 4.

Gebäudesicherheit

Die **Integration von Gebäudeautomation und Sicherheitstechnik** behandelt GIT in der Ausgabe 10-2016, S. 20-22. Bei der Sicherheitstechnik geht es dabei um Videotechnik,

die Zutrittskontrolle, die Einbruch- und Brandmeldetechnik, die Alarmierung und die Löschtechnik. Ein gelungenes Zusammenspiel von Sicherheitstechnik, IT-Security und Gebäudetechnik lasse sich durch fünf Kernaspekte erreichen: Kommunikation während aller Projektphasen, Engagement und Offenheit aller Beteiligten, gemeinsames Verständnis, auch von der Sonderrolle der IT-Sicherheit. Im Vordergrund der Integration müssten die gleichberechtigte Kooperation sowie der permanente Austausch von Erfahrung und Wissen stehen.

Gefahrstoffe

GIT stellt in der Ausgabe 10-2016, S. 122, die **Flameflex- bzw. Chemflex-Sicherheitsschränke** von Asecos vor, die mit dem Konzept „Flexibilität" viele Vorteile böten: Zusammenlagerung unterschiedlichster Gefahrstoffe, Absaugung sowie Filtration der entstehenden gesundheitsgefährdenden Dämpfe. Dieses Konzept gebe es für die Lagerung entzündbarer Flüssigkeiten, schwach aggressive Gefahr- und Giftstoffe sowie für Säure und Laugen. Die Feuerwiderstandfähigkeit von 90 Minuten gemäß EN-Norm 14470-1 sei bei Typ 90-Schränken der FX-Linie für entzündbare Flüssigkeiten serienmäßig. Die Flameflex- und Chemflex-Sicherheitsschränke verfügten über eine Überwachungselektronik mit hochmodernem 4,7-Zoll-Grafikdisplay mit Touch-Steuerung. Hier lasse sich die aktuelle Luftwechselrate anzeigen, überwachen und einstellen Ebenfalls angezeigt werde die Restlaufzeit bis zum nächsten anstehenden Filterwechsel.

Internet der Dinge (IoT)

Jan-Peter Kleinhans, Think Tank Stiftung Neue Verantwortung, behandelt in der FAZ am 30. September Verbrechen im „Internet der Dinge". DDoS-Angriffe seien als Angebot auf Bestellung in den letzten Jahren immer günstiger, professioneller und leistungsfähiger geworden. Für verhältnismäßig kleines Geld könne sich jeder diese Dienste einkaufen und beliebige Websites attackieren. Die Kriminellen rekrutierten vor allem im Internet der Dinge – Internetrouter, Überwachungskameras und Digitale Video Recorder. Aus Sicht der Kriminellen sei es durchaus sinnvoll, sich auf IoT-Geräte zu spezialisieren. In Deutschland, Österreich und der Schweiz gebe es mittlerweile **pro Tag durchschnittlich 100 DDoS-Attacken** auf Unternehmen. Die Kriminellen profitierten davon, dass in der digitalen Welt erst vernetzt und nachträglich gesichert wird – wenn überhaupt. Gerade im Konsumbereich hätten Unternehmen wenig Anreize, auf Sicherheit wert zu legen. Dadurch seien Webinterfaces zur Wartung und Konfiguration des Gerätes oft unübersichtlich und wenig verständlich. Standard-Einstellungen zielten auf Komfort statt Sicherheit. Nutzer hätten wenig Interesse daran, Zeit und Energie in die sichere Konfiguration und Wartung ihrer vernetzten Geräte zu stecken. Es brauche einen **Dialog zwischen IoT-Herstellern und Betreibern, Infrastrukturprovidern und Konsumenten**, um effektive und nachhaltige Lösungen zu finden.

SANS (SysAdmin, Networking and Security) warnt vor neuen **IoT-Botnets**, schreibt Martin Schindler am 4. Oktober in silicon.de. Das SANS Institute rufe Systemadministratoren dazu auf, bei der Sicherung von mit dem Internet verbundenen Geräten zu helfen. In der Vergangenheit habe es prominente Fälle gegeben, bei denen Angreifer über ungesicherte Geräte wie digitale Video-Rekorder (DVR) ein riesiges Botnet aufsetzen konnten. Den Experten von SANS zufolge sei der Angriff recht trivial gewesen: Die Hacker hätten schlicht das Default-Passwort eines Videorekorders xc3511 geknackt und damit mehr als 100.000 Geräte unter Kontrolle gebracht.

Schöner parken mit der Deutschen Telekom, titelt die FAZ am 31. Oktober. Mit „normalem" Mobilfunk sei im IoT nichts zu machen. Der Energieverbrauch wäre viel zu hoch, und die Netze würden unter der Last rasch zusammenbrechen. Der Weg in die vernetzte Welt führe über einen neuen Standard-IoT , im Fachjargon NB-IoT genannt (Narrowband Internet of Things). Diese Schmalband-Kommunikation arbeite mit Funkwellen, die eine besonders großflächige Abdeckung ermöglichen. Zugleich seien sie in der Lage, dicke Betonmauern zu durchdringen und so auch entlegene Winkel zu erreichen. Am Unternehmenssitz in Bonn und in den Niederlanden liefen erste Tests, in denen er Autofahrern freie Parkplätze anzeigt. Die Parkgebühren könnten gestaffelt werden, nach Tageszeit oder dem genauen Standort in einem Parkhaus. Seit einigen Wochen würde die Telekom KMU standardisierte Basislösungen für die Vernetzung von Geräten und Anlagen anbieten. Die Preise für einen Sensor samt Funkverbindung und Cloud-Service begännen bei weniger als zehn Euro im Monat. Typische Anwendungsbeispiele seien die Überwachung von Leistungsdaten oder die Temperaturkontrolle. Üblicherweise würden Normbereiche mit Schwellenwerten definiert, bei deren Über- oder Unterschreitung das System Alarm schlage. Ein für T-Systems besonders lohnendes Segment seien Fahrstühle. Mit vorbeugender Datenanalyse in der Cloud ließen sich die Fahrstuhlwartungskosten um bis zu 30 Prozent reduzieren. Der Konzern habe zusammen mit Microsoft einen vorbeugenden Wartungsservice entwickelt. Die Telekom-Lösung lasse sich ohne großen Aufwand und teure Verkabelung nicht nur in neuen Aufzügen einsetzen, sondern auch in den vielen Mio. älteren Bestandsanlagen. Alle Fachleute seien sich darüber einig, dass das IOT zu einem Multi-Milliarden-Markt werden würde. Europa habe bei der Digitalisierung der Industrie sehr viel bessere Karten als in den von amerikanischen Internetkonzernen dominierten verbrauchernahen Diensten. Mit dem Schmalband-Funk gebe es von Anfang an einen global akzeptierten Standard.

IT-Sicherheit

Die FAZ widmet am 18. Oktober ein Verlagsspezial Themen der IT-Sicherheit. Helge Denker konzentriert sich auf **Erpresserprogramme**. Robert Carolina von der Universität London, berichtet, dass über 15 Prozent aller Unternehmen im vergangenen Jahr mindestens ein Sicherheitsproblem hatten. 42 Prozent davon seien auf Ransomware zurückzuführen. Laut einer Checkpoint-Studie hat sich die Anzahl der Malware-Programme, die Unternehmen angreifen, innerhalb eines Jahres verneunfacht. Auch die Leiter von Unternehmen würden immer mehr zu einem lohnenden Angriffsziel, da sie meist viele Zugriffsrechte in der IT des Unternehmens besäßen. Zukünftig solle Windows 10 mit einer Maschine-Learning-Technik bei aggressiven Schädlingen und arglosen Mitarbeitern dagegenhalten. Arne Schönbohm, Präsident des BSI, ist überzeugt, die **Chancen der Digitalisierung** der Wirtschaft überwiegen die Risiken. Big Data bezeichne die Verarbeitung und Analyse umfangreicher strukturierter und unstrukturierter Datenmengen in Echtzeit. Entscheidende Charakteristika der Datenanalyse seien dabei, dass Zusammenhänge sichtbar werden, die längst von Menschen kognitiv nicht mehr erkannt werden könnten. Denn die Datenmenge, die Datenvariabilität und Komplexität erforderten sowohl eine enorme Verarbeitungsgeschwindigkeit wie auch eine weitgehend automatisierte Auswertung. Notwendig sei ein zwischen Politik, Wirtschaft, Wissenschaft und Gesellschaft koordinierter Ansatz, um über Maßnahmen zum Schutz vor Datenmissbrauch und -manipulation und über die Chancen und Risiken von Big Data in der digitalisierten Gesellschaft zu diskutieren. Das BSI verfolge hier einen ausgeprägten kooperativen Ansatz. Martin Stemplinger,

BT, nimmt im Interview Stellung zu Geldgeschäften, Ransomware-Trojanern und Ethical Hackern. Potentiell gefährdet seien vor allem solche Finanzdienstleister, die vernetzt sind und Bankgeschäfte mobil oder online anbieten. Zu den Zielen der Angreifer zählten zunehmend auch Investment-, Geschäftskunden- und Zentralbanken. Mit dem unerlässlichen Grundschutz wie dem Management von Softwareupdates allein sei es nicht getan. Selbst wenn man noch so sorgfältig sei, nicht alle Angriffe ließen sich verhindern. Aus diesem Grund sollten Unternehmen ihren Schwerpunkt eher darauf legen, Prozesse zu definieren und einzuüben, um Cyberattacken schnellstmöglich zu erkennen und entsprechende Gegenmaßnahmen einzuleiten.
Hadi Stiel, Sicherheitsberater, beschreibt das **„Wagnis Cloud-Dienste".** Vor allem mit Blick auf Compliance und den Datenschutz erachte er die Auslagerung von Daten als „problematisch". Auch für diese Daten stehe nicht der Cloud-Dienstleister, sondern weiterhin das Unternehmen als Eigentümer der Daten in der Verantwortung, dass die gesetzlichen Vorschriften nachweislich eingehalten werden. Der Autor sieht dennoch in der Wolke Sicherheitsvorteile gegenüber der IT im Unternehmen. Oft seien die eingesetzten Sicherheitsmechanismen bei Cloud-Anbietern höher standardisiert, die Prozesse besser integriert und die Berechtigungskonzepte für die Daten konsequenter umgesetzt. Mirco Rohr, Bitdefender, ist überzeugt, **selbstlernende Maschinen** könnten enorm hilfreich sein, zum Beispiel indem sie Unternehmen mit hochintelligenten Analysen im Kampf gegen die zunehmend gefährliche Internetkriminalität unterstützen. Nach aktuellen Untersuchungen ließen sich mit diesen sogenannten Maschine-Learning-Technologien 99,97 Prozent der Bedrohungen erkennen, die von traditionellen Sicherheitsmechanismen nicht registriert würden. Algorithmen analysierten Schadprogramme und würden – ähnlich wie das menschliche Gehirn – gemeinsame Muster und Strukturen erkennen. Ihre Intelligenz bestehe darin, aus diesen Mustern Prognosen für potenzielle Angriffsmethoden abzuleiten. Zu den besten Ergebnissen hätten hybride Ansätze geführt, bei denen maschinelles Lernen durch menschliche Analysten überwacht werde. In fünf Schritten zu mehr IT-Sicherheit, lautet der Ratschlag von Anja Steinbuch: Schwachstellen erkennen durch IT-Landschaftsanalyse; Verknüpfen der IT-Sicherheitsrisiken mit Geschäftsrisiken; technische Unterstützung der Maßnahmen durch Software; alles im Griff mit managed endpoint security und Versicherungen gegen Cyber-Angriffe abschließen und Mitarbeiter einbeziehen.

Die FAZ kritisiert am 17. Oktober die **Wohnungsbaugesellschaften**. Sie versprächen Verschlüsselung für die Daten Tausender Interessenten, hielten sich aber nicht daran. Das Fehlen einer Verschlüsselung sei teilweise seit Jahren nicht bemerkt worden. Ein Datenpaket laufe auf seinem Weg von Frankfurt nach Düsseldorf über mehrere Knotenpunkte, manchmal sogar über ausländische Server. Die Anzahl der potenziellen Mitleser sei deshalb unüberschaubar. Eine Verschlüsselung einzurichten, sei weder besonders aufwendig noch teuer. Laut Bundesdatenschutzgesetz sei eine sogenannte Transportversicherung Pflicht, und zwar „entsprechend dem Stand der Technik". Verstöße technischer Art seien derzeit nicht bußgeldbewehrt. Seit einigen Monaten gehe das Bayerische Landesamt für die Datenschutzaufsicht in Einzelfällen gegen Unternehmen vor, deren Websites unverschlüsselte Kontaktformulare enthalten.

Der Newsletter des Bundesverbandes ASW vom 21. Oktober weist auf den **DsiN-Sicherheitsmonitor** 2016 hin, der in seiner diesjährigen Erhebung zum Teil die Stagnation bei IT-Schutzvorkehrungen in KMU bestätige. Auch zum Thema Social Engineering werde nur rund ein Viertel der Mitarbeiter geschult. Die an der Umfrage beteiligten KMU ließen weiterhin ganzheitliche Ansätze von Sicherheitskonzepten vermissen. Im Hinblick auf den sich verstärkenden Digitalisierungspro-

zess bedürfe die Notwendigkeit der Benutzerverwaltung bei den Unternehmen einer deutlicheren Platzierung. Bei den Themen Cloud Computing und E-Mail zeichne sich bei vielen Unternehmen ebenfalls Unsicherheit darüber ab, ob getroffene Maßnahmen ausreichend sind und ob sie umfassend genug über die rechtlichen Anforderungen Bescheid wissen. Es seien aber auch positive Entwicklungen zu mehr Sensibilität und ganzheitlichen Sicherheitskonzepten im Ansatz erkennbar. Der DsiN-Sicherheitsmonitor Mittelstand untersucht seit 2011 die IT-Sicherheitslage in KMU und ermittelt Schwachstellen, um wirksame Aufklärungsmaßnahmen für den digitalen Schutz zu entwickeln. Grundlage für die Untersuchung sei der DsiN-Sicherheitscheck, mit dem sich KMU einen Überblick über ihren IT-Sicherheitsstatus verschaffen können und mittels eines Online-Fragebogens Auskunft über ihr Sicherheitsniveau erhalten.

Focus.de berichtet am 19. Oktober über eine **Sicherheitslücke bei Photo-TAN**. Sie gelte derzeit als eines der sichersten Verfahren im Online-Banking. Mit der Photo-TAN werde als Passwort ein ungefähr drei mal drei cm großes Bild aus kleinen Punkten generiert, das die Transaktionsdaten enthält. Diese Grafik solle der User mit dem Smartphone von seinem Computerbildschirm abfotografieren. Nun hätten Forscher der Universität Nürnberg-Erlangen das System überlistet. Die Transaktionen hätten allerdings nur manipuliert werden können, wenn Banking-App und Photo-TAN-App auf demselben Gerät installiert seien. Betroffen seien Anwendungen der Deutschen Bank, der Norisbank und der Commerzbank.

Kai Grunwitz, NTT Security, berichtet in dem Verlagsspezial Zukunft Mittelstand der FAZ vom 20. Oktober über das Ergebnis einer Befragung von 1.000 Business-Entscheidern aus sieben Ländern (darunter 200 aus Deutschland), unterschiedlichen Branchen und Unternehmen jeder Größe zum Thema IT-Sicherheit. Die Befragten schätzten, dass die Behebung des durch einen Cyberangriff entstandenen Schadens rund neun Wochen dauert und durchschnittlich Kosten in Höhe von mehr als 800.000 Euro verursache. Mit 65 Prozent der befragten Firmen vertrete eine deutliche Mehrheit die Auffassung, dass sie in der Zukunft selbst Opfer einer Sicherheitsverletzung wird. Dennoch agierten die meisten Unternehmen eindeutig zu zurückhaltend und investierten angesichts der massiven Bedrohung noch immer zu wenig, um die kritischen Assets ihres Unternehmens zu schützen. Nur erschreckend geringe 13 Prozent des gesamten IT-Budgets würden bei den Befragten überhaupt in den Bereich IT-Sicherheit investiert.

Ammar Alkassar, Rohde & Schwarz Cybersecurity GmbH, fordert in der Oktober-Ausgabe des Behörden Spiegel einen Paradigmenwechsel, nämlich **proaktive Sicherheit durch Separation**. Zudem brauche man ein „Whitelisting", welches klar definiere, welche Protokolle Zugang haben sollen. Ein weiteres Umdenken forderte Alkassar bei der Zugriffskontrolle, nämlich „Informationsflusskontrolle statt einer Zugriffskontrolle". Zudem müssten die Anbieter Lösungen entwickeln, welche den Benutzer von der Verantwortung für die IT-Sicherheit weitestgehend entlasten.

Jan Lindner, Panda Security, mahnt in der Oktober-Ausgabe des Behörden Spiegel eine bessere Zusammenarbeit von Firmen und Behörden an. Die klassischen Mittel wie eine Firewall und ein Antivirenschutz reichten nicht mehr aus, um mit aktuellen Bedrohungen wie Zero-Day-Angriffen zurechtzukommen. Der Schlüssel sei ein Mix aus den „Klassikern" und innovativeren Technologien wie z. B. „Adaptive Defense".

Isabel Münch, BSI, berichtet in der Oktober-Ausgabe des Behörden Spiegel über die **Modernisierung des BSI-Grundschutzes**. Das BSI sehe in den Grundschutzkatalogen generell nicht die Notwendigkeit, dass sie vollständig umgesetzt werden müssten.

Vielmehr seien sie als Nachschlagewerk und Hilfestellung zu verstehen. Statt auf je 100 Seiten sollten die einzelnen Bausteine des IT-Grundschutzes künftig mit einem Zehntel dessen auskommen. Neben der Neuausrichtung der Bausteine gebe es zwei weitere Neuerungen: den Basisschutz als vereinfachten Einstieg in den BSI-Grundschutz und eine Kernabsicherung, die darauf abziele, dass die wertvollsten Daten besonders geschützt würden.

Markus Baumgartner, Helvetia Versicherungen AG, gibt in der Ausgabe 5-2016 der Zeitschrift Sicherheitsforum, S. 24–27, Antworten auf die Frage **„Hat die integrale Sicherheit noch eine Chance?"**. Die Unternehmenssicherheit von morgen basiere in vielen Firmen auf der Erkenntnis, dass der Schutz von außen gegen Innen nicht mehr genügt. Sowohl die Mitarbeiter als auch die Netzwerke, Systeme und Applikationen müssten vermehrt von innen nach außen geschützt werden. Die eingangs gestellte Frage beantwortet der Autor mit einem klaren Ja. Mit der Einführung des Internets und seinem dazugehörenden Übermittlungsprotokoll TCP/IP (Transmission Control Protocol/Internet Protocol) könnten Hausleitkomponenten mit Fabrikationsprozessen oder mit Anwenderapplikationen „sprechen". Computer, die Fertigungs- und Überwachungsprozesse steuern, seien im Netzwerk des Unternehmens eingebettet, über das auch Personaldaten und Finanzkennzahlen übermittelt werden. Dass Mitarbeiter auch Privatpersonen sind, würden Internetkriminelle immer raffinierter ausnutzen und E-Mails an die private Adresse schicken, weil sich die Mitarbeiter möglicherweise in Firmenblogs, in sozialen Medien und Suchmaschinen mit ihrem privaten Account angemeldet haben. Auf die Frage „Was können Unternehmen tun?" plädiert der Autor dafür, dass technische Netzwerke zwingend von den Datennetzwerken des Business getrennt werden. Nach Möglichkeit sogar physisch und wo immer möglich sollten Anschlussbuchsen an das Firmennetzwerk sowie sämtliche Verkabelungen in verschlossenen Umgebungen geführt werden. Stockwerkverteiler, Abteilungsserver und Kabelkanäle müssten stets verschlossen sein. Ebenso müsse eine Erkennungssoftware im Unternehmen etabliert sein, die allfällige physische Manipulationen melden könne. Zudem sollten Überwachungsprogramme dafür sorgen, dass sämtliche Netzwerke laufend überwacht werden. Es brauche vermehrt selbstlernende Softwareelemente, welche die Flut von Log- und Nutzdaten analysieren, korrelieren und Anomalien melden können.

Die FAZ thematisiert am 22. Oktober die **Speicherung von IP-Adressen**. Sie sei grob vergleichbar mit einer Telefonnummer. Diese werde in aller Regel gespeichert. Ein „Logfile" liste dann die Zugriffe aller Computer auf. Das diene der Sicherheit. Auf diese Weise ließen sich nämlich etwa wiederholte Aufrufe in kurzer Zeit erkennen oder ungewohnte Muster, mögliche Spuren eines Hackerangriffs. Manchmal diene es der Abrechnung von Diensten. Der EuGH habe in einem salomonischen Urteil festgelegt, dass auch die meist variable IP-Adresse eines Nutzers datenschutzrechtlich geschützt sein kann, wenn sich mit weiteren Informationen die Identität des Nutzers erkennen lasse. Im Telemediengesetz solle nun festgelegt werden, dass IP-Adressen nur für eine bestimmte Zeit gespeichert werden dürfen, nämlich sieben Tage lang. Diese sieben Tage reichten nach Ansicht von Computerfachleuten nicht immer aus, um die erforderliche Sicherheit in einem Kommunikationssystem herzustellen. Das gelte insbesondere bei Hackerangriffen. Sieben Tage sei besser als nichts, aber dennoch zu wenig, so Marc Fliehe von Bitkom. Aus Sicht der IT-Sicherheit könnten auch 200 Tage nötig sein, um Hackerangriffe zu erkennen.

Sicherheitsforscher von Cisco Talos haben ein Tool namens MBRFilter veröffentlicht, das Windows-Computer bis zu einem gewissen Grad vor bestimmten Verschlüsselungs-Trojanern beschützen soll, heißt es in heise.de am

25. Oktober. Dabei verhindere das Tool aber nicht das Verschlüsseln von Daten, sondern schütze den Master Boot Record (MBR) und das GUID Partition Table (GPT) davor, überschrieben zu werden. Ransomware wie z. B. HDD Petya versuche, den Zugriff auf infizierte Computer zu sperren. MBRFilter verbiete das Schreiben auf den Sektor 0 von allen an einen Computer angeschlossenen Festplatten. So könne etwa ein Schädling nicht auf den MBR zugreifen. Um das zu erreichen, setzten die Entwickler unter anderem auf Microsofts Windows-Bordmittel Diskperf.

Peter Marwan beschreibt in silicon.de am 24. Oktober eine gefährliche Sicherheitslücke in Speicherbausteinen. Die Lücke an sich sei schon bekannt gewesen. Neu sei, dass sie sich nun durch einen in einer App versteckten Exploit systematisch ausnutzen lasse. Unter Android benötige sie keinerlei Berechtigungen und könne sich trotzdem Root-Rechte verschaffen. Da der Fehler in der Hardware steckt, könnten auch iOS-Geräte und Windows Phones betroffen sein. Die als Rowhammer bezeichnete Sicherheitslücke könne ausgenutzt werden, um Daten im Random Access Memory (RAM) zu manipulieren. Wie Ars Technica berichtet, sei es den Forschern nun jedoch gelungen, eine App zu entwickeln, die keinerlei Berechtigungen benötigt und nicht auf Sicherheitslücken in Android angewiesen ist. Den von den Forschern als Drammer bezeichneten Exploit hätten sie bereits erfolgreich eingesetzt. Die Erfolgsquote sei dabei recht hoch gewesen: Root-Zugriff hätten die Forscher bei 12 von 15 getesteten Nexus 5 und bei einem von zwei Galaxy55.

Nach wiederholten Denial-of-Service-Angriffen über Botnetze fordere das BSI höhere **Sicherheitsstandards bei vernetzten Geräten**, berichtet golem.de am 25. Oktober. Viele Geräte ließen sich vor allem deshalb so leicht kapern, weil sie mit einheitlich voreingestellten Zugangsdaten ausgeliefert werden. „Sind die voreingestellten Passwörter nicht für jedes Gerät individualisiert, so sei bei der Inbetriebnahme ein Passwortwechsel zu erzwingen", verlange das BSI. Nicht zwingend benötigte Dienste müssten nach Ansicht des BSI durch den Benutzer deaktiviert werden können. Zudem sollte die ein- und ausgehende Kommunikation des IoT-Geräts nur mittels kryptografisch geschützter Protokolle wie TLS erfolgen. Dem Forderungskatalog des BSI zufolge sollten Netzwerkgeräte nicht automatisiert über Universal Plug and Play eine unsichere Konfiguration im Router herstellen, etwa Verbindungen zu unsicheren Diensten erlauben. Die Hersteller sollten „regelmäßig, schnell und über einen hinreichenden Nutzungszeitraum hinweg Sicherungsupdates für die Geräte zur Verfügung stellen".

IuK-Kriminalität

Peter Marwan berichtet in silicon.de am 18. Oktober, dass sich Polizeibehörden aus 13 Ländern der von der niederländischen Polizei, Kaspersky und Intel Security ins Leben gerufenen Initiative **„No more Ransom"** angeschlossen haben. Im Wesentlichen biete die Initiative eine zentrale Anlaufstelle für Opfer von Ransomware: Sie fänden dort Entschlüsselungstools und Informationen, wo und wie sie ihren Fall den Behörden melden und zur Anzeige bringen können. Aber auch Informationen zur Prävention stünden dort bereit. In den ersten zwei Monaten konnten durch die Bereitstellung von Entschlüsselungstools Kaspersky zufolge Lösegeldzahlungen in Höhe von rund einer Mio. Dollar vermieden werden.

Unternehmen müssten Delikte aus dem digitalen Raum verstärkt zur Anzeige bringen, mahnt der Behörden Spiegel in der Oktober-Ausgabe. Sie hätten Angst vor einem Reputationsverlust. Sie seien unsicher in der Zusammenarbeit mit den Behörden oder bemerkten die Attacke erst spät.

Reinhold Zurfluh, InfoGuard AG, plädiert in der Ausgabe 5-2016 der Zeitschrift Sicherheitsforum, S. 28/29, dafür, dass Unternehmen fähig sein müssten, Infiltrationen zu erkennen, schnell darauf zu reagieren und nicht nur die Sicherheitsmauer zu erhöhen, denn die Gefahrensituation habe sich in den letzten 24 Monaten dramatisch verändert. Betrachte man die TOP 15 Cyberbedrohungen der ENISA, so finde man Malware-Attacken, Phishing, Bot-Netze, Insiderattacken, Cyberspionage, Identitätsdiebstahl, DDoS-Attacken, Spam, Gerätediebstahl und Online-Erpressung auf den vordersten Rängen. Um Zugang zu fremden Computern zu erhalten, nutzten „Exploit Kits" oftmals Schwachstellen im Browser aus. Cyber Defence sei mehr als eine Sicherheitsmauer. Zur Verteidigung sei technologische Unterstützung in Form einer zentralen **Security-Intelligence-Plattform** und entsprechender Agenten auf den Endgeräten erforderlich. Sie sammle automatisch alle Informationen aus den Infrastrukturkomponenten, vergleiche diese mit externen Threat Feeds und untersuche sie in Echtzeit auf Angriffe. Ergänzt werde dieses System mit **Breach-Detection-Systemen**, welche den Datenverkehr mithilfe von Data Science, maschinellem Lernen und Verhaltensanalysen durchsuchen und auswerten.

Im ASW-Newsletter vom 28. Oktober nimmt Sam Fox, Control Risks, Stellung zur **Bedrohung von Unternehmen „von innen".** Kaspersky Lab habe kürzlich bekannt gegeben, dass mittlerweile an 28 Prozent aller Cyberangriffen Täter aus den eigenen Reihen beteiligt seien. Sie seien schwer zu erkennen, da ihre Aktivitäten im Netzwerk völlig im Rahmen des normalen Arbeitsalltags lägen. Während Fehler von Mitarbeitern häufig vorkommen und großen Schaden anrichten könnten, gehe die größere Gefahr für Unternehmen von Insidern aus, die ihren Zugang zum Netzwerk nutzen, um Geld zu stehlen, Daten zu beschädigen oder an vertrauliche Geschäftsinformationen zu kommen. Um bösartige Angriffe und unbeabsichtigte Vorfälle zu verringern, sollten die Unternehmen mit der Identifizierung der wichtigsten Vermögenswerte beginnen, um festzulegen, was überwacht und geschützt werden muss. Sie sollten ferner den Zugriff von Mitarbeitern auf Daten beschränken, die sie für ihre Arbeit benötigen. Darüber hinaus sollten Unternehmen Technologien zur Kontrolle von Datenverlust einsetzen. Firmeneigene Laptops sollten verschlüsselt werden, damit kein Fremdzugriff auf die Daten möglich ist.

Krisenmanagement

Problemstellungen des Krisenstabs skizziert Marc Brandner, SmartRiskSolutions GmbH, im Newsletter des ASW am 7. Oktober. Er habe sich im Rahmen einer Konferenzschaltung einmal unversehens in einem virtuellen Krisenstab wiedergefunden. Dieser sei dadurch gekennzeichnet gewesen, dass der Krisenstabsleiter zu keinem Zeitpunkt wusste, wer überhaupt gerade in der Leitung war. Auch die Funktionen und Aufgaben der einzelnen Stabsmitglieder blieben völlig unklar. Auch in Krisenstäben treffe man auf Führungskräfte, die ungern Entschlüsse fassen oder keine klaren Aufträge erteilen. Im zumeist zeitkritischen Krisenmanagement seien die negativen Auswirkungen einer derartigen Führungsschwäche leider sofort greifbar und könnten schnell zur Zuspitzung einer Krise führen. Gerade die ersten Phasen einer Krise seien für Krisenstäbe häufig körperlich und seelisch sehr kräftezehrend. Eine unzureichende Krisenstabslogistik könne diese Belastungen unnötig verschärfen. Erfahrungsgemäß würden diejenigen Krisenstäbe in einer akuten Krise schwimmen, die auf unklaren Strukturen fußen. Dazu gehörten insbesondere zuvor nicht definierte Rollen, Abläufe und Befugnisse.

Kritische Infrastrukturen

Andreas Reisen, BMI, berichtet in der Oktober-Ausgabe des Behörden Spiegel, dass sich bislang nur zehn Prozent, nämlich 73 von 730 der als Kritische Infrastrukturen eingestuften Einrichtungen aus den Sektoren ITK, Energie, Wasser und Ernährung beim BSI gemeldet hätten. Die Betreiber müssten innerhalb von zwei Jahren ein Sicherheitskonzept vorgelegt und umgesetzt haben. Letztlich ziele das Erfassen der KRITIS-Betreiber darauf, gemeinsame Standards zu etablieren, die durch Zertifikate belegt und danach Benchmarks unterzogen werden könnten.

Maschinensicherheit

GIT weist in der Ausgabe 10-2016, S. 86–88, darauf hin, dass es Argumente für einen zentralen Aufbau des Systems der gesamten Sicherheitstechnik, aber auch für dezentrale Strukturen gibt. Es gebe ein entscheidendes Kriterium für die Wahl des zu favorisierenden Aufbaus: die Anlagengröße. Mit zunehmender Komplexität der Applikation würden die Vorteile der dezentralen Strategie an Bedeutung gewinnen. Dazu gehörten neben der höheren Verfügbarkeit auch Kostenaspekte und die überlegene Flexibilität. Mit dem neuen **AS-i Safety Gateway Profisafe** über Profinet mit Safe Link von Bihl+Wiedemann könnten nun auch Systeme mit sicheren Antrieben von Siemens absolut flexibel miteinander vernetzt und mit einem dezentralen Konzept betrieben werden. Jeder Anlagenteil habe seine eigene kleine oder mittelgroße Steuerung, das Sicherheitsprogramm werde in vielen Fällen komplett im AS-i Gateway abgearbeitet. Die Kopplung der einzelnen Segmente erfolge über Safe Link.

Anforderungen an die **sichere Steuerungstechnik** beschreibt die Zeitschrift GIT in der Ausgabe 10-2016, S. 90/91. In ganz unterschiedlichen Aufgabenfeldern der industriellen Produktion werde die Flexibilität zur immer wichtigeren Eigenschaft von Maschinen und Anlagen. Die Losgrößen würden kleiner, die Maschinen sollten sich einfach und schnell an veränderte Produkte und Marktgegebenheiten anpassen lassen. Daraus ergäben sich auch besondere Anforderungen an die sichere Steuerungstechnik. Eine neue Generation von programmierbaren modularen Sicherheitssteuerungen sei bestens eingestellt auf diese Anforderung. Der Beitrag befasst sich mit der Integration der sicheren Antriebsüberwachung, mit den integrierten Diagnosefunktionen und enthält Anwendungsbeispiele (Fleischereimaschine, Abfüllmaschine sowie komplexe Abfüll- und Verpackungsanlage).

Ein **„Safety Evaluation Tool"** stellt Mathias Rebling, Siemens, in der Zeitschrift GIT, Ausgabe 10-2016, S. 92/93, vor. In Verbindung mit umfangreichen Kennwertbibliotheken biete es eine schnelle und einfache Möglichkeit, normenkonforme Anlagendokumentationen zu erstellen. Elektronische Komponenten zur Realisierung von Sicherheitsfunktionen seien aus modernen Automatisierungslösungen nicht mehr wegzudenken. Dabei spiele die funktionale Sicherheit sowohl bei der Auslegung dieser Funktionen als auch bei deren Dokumentation eine entscheidende Rolle. Die Robustheit solcher Systeme werde durch einen Performance- bzw. Safety-Integrity-Level ausgedrückt, welchen es zu berechnen und zu dokumentieren gelte – und zwar pro Sicherheitsfunktion. Diese Berechnungsverfahren seien durch die Normen ISO 138491 und IEC 62061 vorgegeben. Das Safety Evaluation Tool führe den Anwender schrittweise von der Festlegung der Struktur eines Sicherheitssystems über die Auswahl der Komponenten bis hin zur Ermittlung der erreichten Sicherheitsintegrität. Der Autor geht besonders ein auf das standardisierte Austauschformat für Sicherheitskennwerte, auf den Import von Sicherheitskennwerten, auf das Erstellen von Anlagendokumentationen

und auf den Aufbau und die Dokumentation von Sicherheitslösungen.

Zur **Manipulation von Schutzeinrichtungen** an Maschinen nimmt Frank Hagendorff von der Berufsgenossenschaft Holz und Metall, BGHM, im Interview in GIT, Ausgabe 10-2016, S. 94–96, Stellung. Die Welt der Schutzeinrichtungen an Maschinen sei technisch ausdifferenziert wie nie. Sie reiche von feststehenden und beweglichen trennenden bis zu nicht trennenden Schutzeinrichtungen, die durch Berührung oder berührungslos wirken. Nur bei der Akzeptanz scheine es zu hapern. In einem Arbeitskreis auf DGUV-Ebene sei ein Dreistufenkonzept gegen die Manipulation von Schutzeinrichtungen entwickelt worden. Das Ziel der ersten Stufe sei es, Anreize zur Manipulation zu vermeiden. Hierzu dienten geeignete Schutzkonzepte und -einrichtungen, die nicht behindern und leicht angewendet werden können. Manipulationen zu erschweren bilde die zweite Stufe der Methode. Positionsschalter mit kodierten oder unlösbaren Betätigern gehörten dazu. Die dritte Stufe nutze die Möglichkeiten, die sich durch die zunehmende elektronische Ausstattung der Maschinen anbiete. Hier bestehe das Ziel darin, vorgenommene Manipulationen zu erkennen.

Wie Schutzschaltungen zur Bedienersicherheit, besseren Maschinenlaufzeiten und der Wirtschaftlichkeit von „Original Equipment Manufacturer" beitragen, zeigt in der Zeitschrift GIT, S. 102–105, Dr. Peter Terhoeven, Eaton Electric GmbH. Die Auswahl und Beschaffung der richtigen Schutzbaugruppen und ihre Abstimmung untereinander innerhalb eines Stromversorgungsnetzes stelle eine sehr komplexe Aufgabe dar. Der Autor beschreibt die möglichen elektrischen Probleme sowie deren Folgen. Weltweit lägen heute keine einheitliche Qualität der Stromversorgung und der Installationsbedingungen vor. Auch die Verfügbarkeit von ausgebildeten Technikern sei international nicht überall gewährleistet. Um eine optimale Leistung liefern zu können, müsse eine Maschine über einen geeigneten elektrischen Stromkreisschutz gegen vor allem **folgende mögliche Fehlerarten** verfügen: Überströme, Fehlerströme und gefährliche Berührungsspannungen und Lichtbögen einschließlich der durch Blitzeinschlag oder benachbarte Ausrüstungen verursachte Überspannungen. Demgemäß behandelt der Autor Überströme (Überlast- oder Kurzschlussstrom), Fehlerströme, Fehlerlichtbögen und den Bedarf an Überspannungsschutzeinrichtungen.

GIT zeigt in seiner Ausgabe 10-2016, S. 110/111, wie ein **stationärer Sicherheitsaufstieg** Arbeitsunfällen auf Tankfahrzeugen und Containern vorbeugt. Da Kesselwagen oder Container häufig nicht ausreichend abgesichert sind, sei der Aufstieg oft mit hohen Sicherheitsrisiken verbunden. Bei betriebsmäßigen Begehungen, insbesondere bei Arbeiten am Mannloch, komme es daher immer wieder zu Stürzen und Verletzungen der Mitarbeiter. Abhilfe würden bisher nur Schutzgeländer schaffen, die allerdings erst ab einer Fahrzeughöhe von zwei Metern vorgeschrieben seien, und mit denen jeder Lkw einzeln ausgestattet werden müsse. Anders bei stationären Klapptreppen. Die seien bei jedem Fahrzeug auf die richtige Höhe positionierbar – integriert entweder in Zugangsplattformen für Kesselwagen oder als klapp- oder verstellbare Arbeitsbühnen. Sie würden aus Stahl hergestellt und seien TÜV-zertifiziert.

Organisierte Kriminalität (OK)

Die OK in Deutschland werde immer mehr geprägt durch **international agierende**, sehr **mobile Tätergruppen**, berichtet die FAZ am 15. Oktober. 80 Prozent der 566 Ermittlungsverfahren im Jahre 2015 hätten internationale Bezüge aufgewiesen. Etwa zwei Drittel der insgesamt 8.675 Tatverdächtigen seien ausländische Staatsangehörige. Der Bundesinnenminister und der Präsident

des BKA hätten bei der Vorstellung des „Bundeslagebildes OK" darauf hingewiesen, dass der Anteil der deutschen Staatsangehörigen auf etwa 3.000 leicht gesunken sei. Es folgten Litauer (990), Türken (841), Polen (445) und Rumänen (413). Als „wesentliches Instrument" zur Bekämpfung der OK habe der Bundesinnenminister die Abschöpfung von Vermögen bezeichnet. Vermögen unklarer Herkunft könnte künftig eingezogen werden, auch wenn die konkrete Straftat, aus der die Gelder gewonnen wurden, nicht nachweisbar sei. 2015 seien insgesamt 65 Mio. Euro gesichert worden. Auf etwa 230 Mio. Euro seien die kriminellen Erträge geschätzt worden. Insgesamt seien durch OK 2015 etwa 424 Mio. Euro Schaden verursacht worden. Dabei müsse man von einer hohen Dunkelziffer ausgehen. BKA-Präsident Münch habe bekräftigt, dass man sich nicht mehr nur an der klassischen Definition von OK orientieren dürfe. Kriminelle würden immer stärker in Netzwerken agieren. In mehr als einem Drittel der Verfahren gehe es um Rauschgiftkriminalität, gefolgt von Eigentumskriminalität (14,8 Prozent) und Wirtschaftskriminalität (11,8 Prozent). Ein Schwerpunkt im Kampf gegen die OK sei das Internet als Tatort und auch als Kommunikationsmittel.

Outsourcing

Jürgen Kempf, Result Group GmbH, stellt im Newsletter des ASW die Frage: **Outsourcing – Chance oder Risiko**? und beantwortet sie mit „Sicher Beides!". Positive Aspekte seien: Kosteneinsparungen, Wissensverbreiterung, Flexibilität, Spezialisierung und Fokussierung, Transparenz und Leistungseffizienz sowie optimiertes Prozess- und Technologie-Outsourcing. Aus der Sicht der Sicherheitsverantwortlichen könnten aber auch Risiken beinhaltet sein: Kontroll- und Einflussverlust; „you get what you pay for" (durch niedrigere Löhne könne es zu Qualitätsverlust kommen); Verlust der Bindung an den Arbeitgeber – Loyalitätsverlust (Mitarbeiter eines Dienstleisters spürten selten eine Verbundenheit zum Unternehmen, in dem sie eingesetzt sind.); Informations- und Kompetenzverlust (Dienstleister würden manchmal vorgeschriebene Zuverlässigkeitsprüfungen umgehen); Verfügbarkeit des Personals; Repräsentation des Arbeitgebers (ein eigener Mitarbeiter werde sein Unternehmen meist anders vertreten als der Mitarbeiter eines Dienstleisters); Weisungsverlust (keine Weisungsbefugnis des Auftraggebers direkt gegenüber Mitarbeitern des Dienstleisters).

Jürgen Kempf rät, sich beim Oursourcing den Auftragnehmer genau anzuschauen und vor Ort zu prüfen, ob alle Anforderungen erfüllt werden. Er rät ferner, sich mit dem Management des Dienstleisters zusammenzusetzen und festzulegen, wie in einzelnen Situationen, z. B. in Notfällen oder bei kritischen Prozessschritten, zu verfahren ist.

Parkflächensicherheit für Lkw

Allein an deutschen Autobahnen fehlten 14.000 Lkw-Stellplätze, berichtet die FAZ am 13. Oktober. Bosch starte nun ein Geschäftsmodell, das diesem Mangel abhelfen will und gleichzeitig ein anderes Problem lösen solle, nämlich den Frachtdiebstahl zu begrenzen. „Wir bringen Autohöfe ins Internet und machen sie zu einem vernetzten Dienstleister", erklärt Bosch-Projektleiter Jan-Philipp Weers das Prinzip von **Secure Truck Parking**. Der erste angeschlossene Kunde sei der Autohof Thiersheim an der A 93 kurz vor der tschechischen Grenze, wo 50 sichere Lastwagen-Parkplätze angeboten werden sollen. Geplant sei, Parkflächen auf Autohöfen, aber auch Firmenparkplätze in Autobahnnähe, auf einer Plattform zu vernetzen. Ob sie belegt seien oder ob freie Stellplätze verfügbar seien, werde über eine App oder ein Online-Portal in Echtzeit zu sehen sein. So könnten Lkw-

Fahrer passend zu ihrer Route schon vorab oder auch während der Fahrt Stellplätze für ihre Ruhezeiten reservieren. Zudem seien alle Parkflächen mit Sicherheitstechnik ausgestattet und per Videoanlage überwacht. Den Betreibern des jeweiligen Parkraums biete Bosch auch virtuelle Wächterrundgänge an. Allein durch den Diebstahl von Fracht entstehe in Deutschland jährlich ein Schaden von drei Mrd. Euro, in der EU seien es sogar 16 Mrd. Euro. Jedes Jahr würden in der EU 90.000 Überfälle auf parkende Lkw gemeldet.

Perimeterschutz

Zeitgemäßen Perimeterschutz gegen neue Bedrohungslagen stellt GIT in der Ausgabe 10-2016, S. 44/45, vor. Von mikrowellenbasierten Volumensensoren wie Wavesec zur weitläufigen Freigeländeüberwachung, seismischen ortungsfreien Bodendetektionssystemen wie Groundsec bis hin zu Zaundetektionssystemen – die Bandbreite an Systemen biete eine Vielzahl an Möglichkeiten. Die Auswahl des passenden Systems und der optimalen Kombination 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 Kombination von Systemen zur Freigelände- oder Zaundetektion, z. B. mit moderner Videotechnik, bilde nahezu lückenlose, zuverlässige Sicherheitskonzepte.

Rechenzentrumssicherheit

Branddetektion und Löschen im Rechenzentrum behandelt GIT in der Ausgabe 10-2016, S. 64/65. Für die Raumüberwachung in den Kaltgängen mit den Racks kommen im neuen Hochverfügbarkeits-Datacenter bei der Sto SE punktförmige Mehrfachsensormelder MTD 533X von Hekatron zum Einsatz. Sie seien in Zweimeldungsabhängigkeit Typ B geschaltet, sodass der Löschvorgang normgerecht erst bei Ansprechen zweier Melder ausgelöst wird. Den Doppelboden darunter sichere ein mit zwei Ansaugrohren ausgerüsteter Ansaugrauchmelder ASD 535-2 . Dank seiner hochdynamischen HD-Sensoren könne der ASD äußerst geringe Mengen von Rauchgasen bereits in der frühesten Phase der Brandentstehung detektieren. Die messbare Rauchkonzentration liege dabei in einem Bereich von 0,002 bis 10 Prozent pro Meter.

Security Fabric

Antwort auf die Frage „Wie lässt sich heute ein Unternehmensnetzwerk umfassend schützen?“ gibt Franz Kaiser, Fortinet, in der Ausgabe 5-2016 des Sicherheitsforum, S. 32/33: durch die „Security Fabric“ als Lösungsweg. Nur ein ganzheitlicher Ansatz könne Abhilfe schaffen, eine „Sicherheitsfabrik“, die Hardware, Software und Kommunikationsprotokolle mit interner Segmentierung in einer einzigen Architektur vereint. Sie adressiere Cloud-Applikationen, die Bedrohung durch Advanced Persistent Threats, das Event Management, Compliance und Investitionsschutz. Eine solche Architektur werde von Grund auf so entwickelt, dass sie mit den wesentlichen Bestandteilen eines Netzwerks arbeite. Auch wenn sich die einzelnen Netzwerkkomponenten verändern, bleibe die solide Grundlage der „Security Fabric“ relevant.

Signaltechnologie

In der Ausgabe 10-2016, S. 72–74, thematisiert GIT die **Leistung von Signalgebern im Raum**. Eine neue praxisorientierte Darstellungsmethode des Unternehmens Pfannenberg mache erstmals die tatsächliche

Leistung von Signalgebern im Raum unter den realen Umgebungsbedingungen der Applikation sichtbar und helfe Planungsverantwortlichen so, Signalisierungslösungen optimal auszulegen. Nicht jeder Signalgeber erfülle die Kriterien eines Alarmierungsgerätes. Um den passenden Signalgeber auswählen zu können, müssten in der Planungsphase unbedingt die Umgebungsbedingungen am Einsatzort berücksichtigt werden. Bei vielen günstigen Schallgebern komme die Piezo-Technologie zum Einsatz. Ihre geringe Stromaufnahme mache sie insbesondere in der Brandalarmierung auf dem Papier attraktiv. Betrachte man jedoch ihre Leistung, so lasse sich ein weitaus geringerer Signalisierungsbereich als bei der elektrodynamischen Schallerzeugung feststellen.

Sprachalarmierung

GIT stellt in der Ausgabe 10-2016, S. 78/79, das Sprachalarmierungssystem Multives von NSC vor. Es sei ein System zur Übertragung von Alarm-, Sprach- und Werbedurchsagen. Die Komponenten des Systems seien zertifiziert nach EN 54-16 bzw. EN 54-4. Es bestehe aus System-Controllern, Mehrkanalverstärkern sowie Feuerwehr-Mikrofonen und Systemsprechstellen. Den Kern bilde eine Plattform, die eine digitale Kommunikation zwischen den einzelnen Systemkomponenten sowie mit anderen Sicherheits- oder Leitsystemen ermöglicht. Die Verbindung zwischen diesem und dem Brandmeldetechniksystem des Herstellers erfolge über die RS485-Schnittstelle und ermögliche neben der Ansteuerung nach VDE 0833-4 auch eine komfortable Programmierung gewünschter Alarmierungsbereiche.

Terrorismus

Flughäfen gehörten wie **Bahnhöfe** zu den bevorzugten Zielen von Terroristen, betont sueddeutsche.de am 11. Oktober. Es handele sich um sogenannte „weiche Ziele" mit vielen potenziellen Opfern, die vor entschlossenen und zum Selbstmord bereiten Einzeltätern kaum zu schützen seien. Am Brüsseler Flughafen kämen Reisende und Besucher nicht mehr ohne Sicherheitscheck und Gepäckdurchleuchtung ins Gebäude. Verdächtige Fahrzeuge würden bereits auf der Zufahrtsstraße kontrolliert. Die Haltezone vor der Abflughalle sei gesperrt worden. Bei den Personenkontrollen vor den Flugsteigen hätten die Flughäfen in den vergangenen Jahren technisch enorm aufgerüstet, während es an den Bahnhöfen nichts Vergleichbares gebe. Im Zusammenhang mit möglichen Direktzügen nach London werde in Frankfurt geprüft, die Fahrgäste vor Betreten des Zuges zu kontrollieren. Im Luftverkehr sähen Experten noch Sicherheitslücken bei der Fracht, die anders als das Passagiergepäck nicht komplett durchleuchtet werde. „Terrorgeplagte" Länder hätten weit schärfere Sicherheitsvorkehrungen installiert. An russischen oder türkischen Flughäfen seien Kontrollen an den Eingängen üblich. In Afghanistan oder Israel seien zudem Checkpoints schon weit vor den Flughäfen eingerichtet. Am Flughafen Ben Gurion in Tel Aviv setzten die Sicherheitskräfte zudem auf Social Profiling, das videogestützt nach möglicherweise verhaltensauffälligen Gefährdern suche. Die vorsortierten Reisenden würden gezielt und in unterschiedlicher Intensität befragt. Die deutschen Flughafenbetreiber argumentierten gegen vorverlagerte Kontrollstellen. Bei den meisten Flughäfen fehle es schon allein an dem notwendigen Platz. Damit würden nur neue Anschlagsziele geschaffen, aber keine zusätzliche Sicherheit, wie der Istanbuler Anschlag im Juni auf die Eingangskontrollen belege.

Videoüberwachung

Stefan Palm, Moxa Europe GmbH, befasst sich in der Zeitschrift GIT, Ausgabe 10-2016, S. 50/51, mit der **Videotechnik im Schienenverkehr**. Er geht besonders auf die Temperaturabhängigkeit der LED-Leistung ein und skizziert die Auswirkungen auf Infrarot-LED. Kann die auf eine LED einwirkende Hitze nicht angemessen abgeleitet werden, beeinflussten hohe Temperaturen sowohl die Lichtemission, als auch die Lebensdauer der LED. Die folgenden grundlegenden Tipps für das Design seien ein wichtiger Aspekt der LED-Entwicklung: Die Auswahl eines passenden LED-Materials, des Materials für das LED-Substrat und der Art der Befestigung der Chips auf der Systemplatine beeinflussten die Wärmeableitung. Die Auswahl eines Materials mit hohem thermischem Leitfähigkeitskoeffizienten sei ebenfalls ein wichtiger Aspekt.

GIT befasst sich in der Ausgabe 52/53 mit **hochentwickelten Wärmebildkameras** für visuell schwierige Anwendungsgebiete. Die in einem von dem Unternehmen Hikvision selbst entwickelten Imaging-Modul integrierten Wärmebildkameras lieferten plastische, hochauflösende HD-Videos von sich bewegenden Objekten mit einer Auflösung von bis zu 640 x 512 Pixeln ohne Beeinträchtigung durch Dunkelheit oder schlechtes Wetter. Diese Wärmebildkameras besäßen drei innovative Funktionen für optimale Bildqualität: Automatische Verstärkungsregelung, digitale Detailoptimierung und mehrdimensionale digitale Rauschunterdrückung. Die digitale Detailoptimierung basiere auf einem Algorithmus für einen Zielbereich und sorge dafür, dass mehr Details im Bild sichtbar bleiben. Wärmebildverfahren spielten bei der Sicherung offener, großflächiger Bereiche eine wichtige Rolle. Besonders häufig werde die Technologie für Sicherheitsanwendungen an Perimetern, Häfen, kritischer Infrastruktur, Verarbeitungs- und Fertigungsanlagen eingesetzt.

Wie die FAZ am 19. Oktober berichtet, stellt das deutsche Startup Smartfrog Überwachungskameras her und verkauft sie in einem Abonnement-Modell. Wer knapp sechs Euro im Monat zahlt, bekomme die Kamera und könne 24 Stunden Video speichern und damit etwa nachschauen, ob sich Einbrecher an der Terrassentür zu schaffen machen. Das Unternehmen habe unter anderem mit Amazon, Otto, Mediamarkt oder Conrad ein Vertriebsnetzwerk aufgebaut. Andreas Rudyk, einer der Gründer von Smartfrog, habe gegenüber der Zeitung versichert, dass das Unternehmen keinen Zugriff auf die Videodaten habe. Je nach Abo-Modell könnten Aufnahmen von Kunden bis zu 30 Tage gespeichert werden.

Mit der **Analyse von digitalen Videobildern**, der Sicherung und Auswertung von Bild- und Videoaufnahmen als optische Spuren, befasst sich in der Ausgabe 5-2016 des Sicherheitsforums, S. 10–13, Roland Bachofner vom Forensischen Institut Zürich. Die Vorgabe einer Pixeldichte entscheide schließlich über die Auswertbarkeit der Bilder und die effektive Tauglichkeit des gesamten Systems. Da das Videobild nur zweidimensional aufgenommen wird, lasse sich die Frage nach der Körpergröße eines aufgenommenen Tatverdächtigen nicht direkt beantworten. In solchen Fällen werde der Tatort nachträglich mit einem 3D-Scanner räumlich erfasst und dann das Videobild mit dem dreidimensionalen Raumbild rechnerisch verbunden. Der Beitrag geht auf eine Reihe von Methoden der forensischen Bildbearbeitung ein: Entpixeln, Integrieren und Pixelberechnung mittels Filtertechniken.

Wohnungseinbruch

Kaum eine „Branche" wachse hierzulande so stark wie die der Einbrecher, betont die TÜV Rheinland Akademie in GIT, Ausgabe 2016, S. 36/37. Laut PKS 2015 sei die Zahl der

Wohnungseinbrüche auf gut 167.000 gestiegen. Das sind fast zehn Prozent mehr als 2014 und sogar 50 Prozent mehr als 2005. Wer wirksamen Schutz vor Einbrüchen in die privaten vier Wände sucht, sichere die baulichen Schwachstellen, z. B. durch geprüfte einbruchhemmende Türen und Fenster und mit einer Alarmanlage. Einbruchhemmende Produkte hätten spezielle Pilzkopfverriegelungen, die sich nur schwer aufhebeln lassen. Einbruchhemmende Produkte könnten jedoch ihre Schutzfunktion nur erfüllen, wenn sie von Fachleuten eingebaut würden. Der Beitrag skizziert die Vielzahl von Regelwerken, Errichterlisten der Landeskriminalämter und die Bedeutung der Außenbeleuchtung. Er weist ferner auf die staatliche Förderung für Einbruchschutz seit November 2015 hin.

Auch die FAZ befasst sich am 1. Oktober mit der Entwicklung des Wohnungseinbruchs in Deutschland. Er habe im letzten Jahrzehnt um 58 Prozent zugenommen. Dabei sei die Aufklärungsquote mit 15 Prozent erschreckend niedrig. Das Bundesbauministerium habe im November 2015 der Förderbank KfW zehn Mio. Euro zur Verfügung gestellt, um damit den Einbau einbruchhemmender Türen, sicherer Fenster und von Alarmanlagen zu bezuschussen. Investiert der Eigentümer mindestens 2.000 Euro, könne er einen Zuschuss von bis zu zehn Prozent erhalten. 2017 werde die Bundesregierung die Mittel verfünffachen. 68 Prozent der Hausbesitzer hätten in einer bundesweiten Umfrage des Verbands Wohnungseigentum NRW auf eine Außenbeleuchtung als wichtigste Sicherung verwiesen, 62 Prozent hätten Bewegungsmelder, 54 Prozent abschließbare Fenstergriffe genannt. Nur 17 Prozent vertrauten auf Empfehlungen von Versicherern, 57 Prozent auf den Fachhandel, aber 80 Prozent der Polizei. Obwohl im Herbst mehr Taten festzustellen seien, suchten Täter nicht unbedingt den Schutz der Dunkelheit. 58 Prozent der Einbrüche würden zwischen 10 und 18 Uhr verübt, die meisten zwischen 12 und 14 Uhr sowie zwischen 16 und 18 Uhr. Die Versicherer hätten ermittelt, dass die Einbrecher Gegenstände im Wert von durchschnittlich 3.250 Euro erbeuteten. Am beliebtesten seien Schmuck, Bargeld und Handys.

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
Vorsitzender des Aufsichtsrates: Dr. Carl A. Schade

E-Mail: info@securitas.de