FOCUS ON SECURITY

AUSGABE 10, OKTOBER 2017

SECURITAS

Inhaltsverzeichnis

Amoklauf

GIT-SICHERHEIT.de stellt in der Ausgabe 9-2017, S. 29, die Weiterentwicklung eines funkbasierten Zutrittssystems (eAccess) vor: Wird der Gebäudealarm aktiviert, dann verriegelten die Funkbeschläge ausgewählte Türen. Von innen könnten die Türen weiterhin jederzeit geöffnet werden, von außen nur mit speziellen Notöffnungsmedien.

Anschläge

Der Behörden Spiegel weist in seiner September-Ausgabe auf eine Warnung des BKA hin, nach der Anhänger von Terrororganisationen im Internet verstärkt über **Angriffe auf Züge** diskutierten. Als Vorbild werde von den Terroristen wiederholt das Unglück im bayerischen Bad Aibling genannt. Attacken und Geiselnahmen in Zügen seien keine neuen Phänomene. Bereits 1975 hätten bewaffnete Molukken in den Niederlanden einen Zug gekapert und bis zu 60 Geiseln festgehalten.

Arbeitnehmerüberwachung

Auch im Fall einer **Pflichtverletzung** ist die verdeckte Überwachung von Arbeitnehmern möglich. Auf diese Entscheidung des BAG (2 AZR 579/16) weist die FAZ am 1. September hin. Ansonsten wäre die Norm europarechtswidrig. Damit sei die schwer nachvollziehbare Meinung vom Tisch, nach der § 32 Abs.1 Satz 1 BDSG eine Sperrwirkung habe. Danach sollte die geheime Erhebung personenbezogener Daten nur möglich sein, wenn der Arbeitgeber dem Mitarbeiter den konkreten Verdacht einer Straftat im Beschäftigungsverhältnis aufklären will. Je transparenter, konkreter und detaillierter das Unternehmen geplante Datenerhebungen gegenüber seinen Mitarbeitern vorab kommuniziere, desto weniger angreifbar sei dies später von Klägern, Aufsichtsbehörden oder vor Gericht.

Arbeitsschutz

Wolfgang Quednau, BTTA GmbH, thematisiert in der GIT-Sonderausgabe PRO-4-PRO, S. 68–70, innovative Gewebe. Zwei Trends zeichneten sich ab: Erstens würden die innovativen Gewebe immer leichter in Abhängigkeit zur Schutzfunktion. Damit genügten sie den wachsenden ergonomischen Ansprüchen bei kontinuierlich verbesserter Schutzfunktion. Zweitens seien inzwischen Gewebe, die mehrere Schutzziele erfüllen, im rein präventiven Bereich Standard. Ein viel diskutiertes Thema heiße derzeit „Smart Textiles". Bereits jetzt reiche das Angebotsspektrum von Outfits mit heizbaren Elementen, die Arbeiten bei Kälte angenehmer machen, bis hin zu Feuerwehrkleidung mit Sensoren, die Vitalpunkte von Menschen erfassen und damit Rettungsaktionen unterstützen. An weiteren, immer komplexeren Lösungen werde mit Hochdruck gearbeitet.

Formen des Gehörschutzes listet GIT-SICHERHEIT.de in der Ausgabe 9-2017, S. 98–100, auf: Otoplastiken, Bügelgehörschützer (geeignet, wenn der Gehörschutz häufig abgelegt wird) und Kapselgehörschützer (für kurzfristige Arbeiten in Lärmbereichen). Sowohl 3M als auch Uvex böten eine Dezibel-App an, mit der sich via Smartphone feststellen lasse, ob ein Gehörschutz getragen werden sollte. Die Wahl des richtigen Lärmschutzes könne von einer Farbskala abgelesen werden.

Bankensicherheit

Der Bank-Verlag weist am 25. September auf ein **sicheres IP-Netzwerk** für Banken hin. SIPNET sei ein Service für die sichere Daten- und Transaktionsübertragung zur Abwicklung aller Kommunikationsanforderungen zwischen den Kopfstellen der privaten Kreditwirtschaft und den Banken bzw. ihren IT-Dienstleistern in Deutschland und den Nachbarstaaten. SIPNET habe entscheidende Vorteile gegenüber dem Internet. Die Funktionalität werde durch Service Level Agreements garantiert. Die Sicherheitsvorkehrungen entsprächen höchsten Anforderungen. Die Verfügbarkeit sei gewährleistet. Es handele sich um eine „State of the Art-Technologie" (MPLS-Plattform).

Betrug

Wie der ASW im Newsletter vom 14. September berichtet, senden seit März 2017 Betrüger vermehrt **E-Mails mit irreführenden Absenderangaben** an mittelständische Unternehmen der Metall-, Automobil- und Lebensmittelindustrie. Sie träten als Großkunden auf und würden unter dem Deckmantel seriöser britischer Unternehmen in großem Stil Bestellungen abgeben. Die Polizei bezeichne die Methode als **„Fake-Customer-Trick".** Die Anbahnung des Geschäfts erfolge mit Hilfe von E-Mail-Absenderadressen, die den Anschein erwecken, von Beschäftigten seriöser Unternehmen in Großbritannien zu stammen. Durch Fachbegriffe und branchenübliche Formulierungen unterstrichen die Betrüger diesen Eindruck. Sie signalisierten bei der Bestellung sofortige Zahlungsbereitschaft und belegten ihre Bonität mit gefälschten Bilanzen. Sie beauftragten über das Internet internationale Speditionen. Allein in Baden-Württemberg seien auf den Trick neun Firmen hereingefallen. Das baden-württembergische LKA empfehle: Verifizieren Sie den Kunden durch Telefonanruf oder E-Mail über Verbindungen, die auf der Homepage des Kunden hinterlegt sind. Benutzen Sie nicht die Kontaktdaten aus der E-Mail. Informieren Sie die Beschäftigten ihres Unternehmens über diesen Fake-Customer-Trick.

Brandmeldeanlage

Die **Integration von Brandmeldezentralen** beschreibt Bosch Sicherheitssysteme im Heft 9-2017 der Zeitschrift PROTECTOR, S. 46/47. Eine gemeinsame technische Plattform auf Basis von der IP, die Brandmeldeanlagen mit Evakuierungs-, Einbruchmelde- und Zutrittskontrollsystemen sowie der Videoüberwachung integriert, ermögliche den zentralen Betrieb und eine einheitliche Verwaltung der gesamten Sicherheitstechnik. Durch die Korrelation von Ereignissen ermögliche die Integration der einzelnen Gewerke auch eine schnellere und gezieltere Intervention. Einsatzkräfte wüssten im Alarmfall schon vor der Ankunft genau, was sie vor Ort erwartet. Des Weiteren ermögliche die Vernetzung auch den Einsatz von neuen Brandmeldetechniken, wie etwa die videobasierte Branderkennung. Vernetzte Systeme böten Planern und Bertreibern beim Brandschutz ein hohes Maß an Flexibilität. Die Vernetzung der einzelnen Gewerke sei auch eine unabdingbare Voraussetzung für eine Vielzahl neuer Anwendungen im Rahmen des IoT. Hierzu zählten insbesondere cloudbasierte Remote Services wie etwa Ferndiagnose. Über intelligente Algorithmen würden auf Basis der erhobenen Realdaten optimale Wartungsfenster kalkuliert. Nutzen könne die Vernetzung und das IoT nur, wer sich mit diesen Techniken und Konzepten intensiv auseinandersetzt und sein Personal auch entsprechend qualifiziert.

Frank Herstix, Honeywell Security and Fire/Novar GmbH, zeigt in der Ausgabe 9-2017 von PROTECTOR, S. 48/49, die **Vorteile modularer Brandmeldeanlagen.** Die Lebenszykluskosten eines Brandmeldesystems könnten Betreiber vor unerwartete Herausforderungen stellen. Unter Umständen seien Nutzungsänderungen eines Objektes oder Veränderungen in der Risikodefinition durch Sachversicherer oder Systemveränderungen nach kurzer Nutzungszeit gefordert, die dann zusätzliche Aufwendungen nach sich ziehen. Um diesen Zusatzkosten vorzubeugen, könne bereits im Vorfeld die Brandmeldeanlage in Form eines „Baukastensystems" geplant werden, um sich später wechselnden Objektanforderungen in der Liegenschaft anpassen zu können. Eine komplexe Brandmeldeanlage, die als modulares System aufgebaut ist, biete viele Vorteile sowohl für den Planer, den Errichter als auch für den Betreiber des Systems. Regionale Sonderanforderungen und Visualisierungseinrichtungen für Interventionskräfte sollten für eine Brandmeldeanlage verfügbar sein. Moderne und zukunftsorientierte Brandmeldesysteme könnten durch einen modularen Aufbau eine hohe Flexibilität erreichen. Wichtig sei, dass Sachverständige den ordnungsgemäßen Zustand prüfen und Fachfirmen die Instandhaltung gewährleisten.

Brandschutz

In dem Special Brandschutz 2017 befasst sich PROTECTOR mit der **Sprachalarmierung.** Ob Hotel, Flughafen, Einkaufszentrum oder Sportstadion – wenn sich im Brandfall Menschen in betroffenen Gebäuden aufhalten, gelte nur eines: so schnell wie möglich raus! Bei der Suche nach dem kürzesten Weg ins Freie zähle dann jede Sekunde. Nur wenn Brandmelde- und Sprachalarmanlage eine Einheit bilden, könne die umgehende Evakuierung sichergestellt werden. Es sei erwiesen, dass das Warnen durch eine menschliche Stimme eindeutiger und gleichzeitig beruhigender ist, als ein rein mechanisches Warnsignal. Im Zuge fortschreitender Entwicklungen in den Bereichen Digitalisierung und Vernetzung kämen Brandmelde- und Sprachalarmanlage immer häufiger gekoppelt zum Einsatz.

Eine Anwendungsrichtlinie für Errichter und Planer bilde hierbei die VDE 0833-4, die unter anderem die Planung sowie den Aufbau und Betrieb für Gefahrenmeldeanlagen und die Sprachverständlichkeit innerhalb des Sprachalarmkonzeptes kläre. Zusätzlich gelte die DIN 14675 für Errichter und Planer als Grundlage für die Zertifizierung der Firma und der nötigen Fachkraft. Die Ansteuerung der Sprachalarmanlage erfolge durch eine Brandmeldeanlage gemäß VDE 0833-2. Die einzelnen Komponenten der Sprachalarmanlage würden als zulässiges Gesamtsystem nach europäischem Standard gelten, wenn die harmonisierten Produktnormen DIN EN 54-4 (Energieversorgungseinrichtungen), DIN EN 54-16 (Sprachalarmzentralen) und DIN EN 54-24 (Lautsprecher) erfüllt sind.

Die GIT-Sonderausgabe PRO-4-PRO weist auf eine Statistik des Bundesverbandes Technischer Brandschutz zur **Effizienz von Löschanlagen** 2016 hin (S. 50). Demnach seien 2016 81 Prozent aller beim Verband gemeldeten Löscherfolge durch Sprinkleranlagen mit nur einem oder zwei Sprinklern erzielt worden. Bei 13 Prozent seien es 3–5 Sprinkler gewesen. 89 Prozent der eingesetzten Löschanlagen hätten automatisch ausgelöst.

Compliance

Helmut Sauro, Krolldiscovery, plädiert in der Ausgabe 9-2017 von PROTECTOR, S. 72, für Compliance-Checks für **Auslandsgeschäfte.** 79 Prozent der von Krolldiscovery befragten 296 Entscheider aus Vertriebs- und Einkaufsabteilungen zeigten trotz Regeldschungel für die nötige Sensibilität für internationale Compliance und hätten Prozesse und Regeln für grenzübergreifende Geschäftsbeziehungen definiert. Allerdings kontrollierten nur 57 Prozent der befragten Unternehmen die Einhaltung der internationalen Regelungen. 55 Prozent räumten ein, dass die Anpassung an lokale Gebräuche internationaler Geschäftspartner wichtiger ist als die Einhaltung von Compliance-Vorgaben. 37 Prozent gaben unumwunden zu, dass das Zahlen von Schmiergeldern oder der Austausch kleiner Gefälligkeiten für den Erfolg im internationalen Handel unverzichtbar sei. 67 Prozent der Entscheider stünden dazu, sich hin und wieder bewusst gegen das günstigste oder transparenteste Angebot zu entscheiden, um gute Beziehungen zu ausländischen Lieferanten aufrecht zu erhalten.

PROTECTOR befasst sich in der Ausgabe 9-2017, S. 72, mit einer aktuellen Befragung des Ediscovery-Anbieters Krolldiscovery von 256 Entscheidern aus Vertriebs- und Einkaufsabteilungen sowie Geschäftsführungen zum Thema internationale Geschäftsbeziehungen. 47 Prozent hätten eingeräumt, dass ihnen der Überblick über die Vielzahl der internationalen Gesetze fehlt. Die Befragung zeige Risiken im Umgang mit internationalen Compliance-Vorschriften. Nur 57 Prozent der befragten Unternehmen kontrollierten die Einhaltung internationaler Regelungen. 55 Prozent der Befragten räumten ein, dass die Anpassung an lokale Gebräuche internationaler Geschäftspartner für wichtiger gehalten werde als die Einhaltung von Compliance-Vorschriften. 37 Prozent hätten sogar unumwunden zugegeben, dass das Zahlen von Schmiergeldern oder der Austausch kleiner Gefälligkeiten für den Erfolg im internationalen Handel unverzichtbar sei. Dabei könne ein **Verstoß gegen Antikorruptionsrichtlinien** in Fernost bei der Anbahnung eines Geschäfts eine Kettenreaktion in Gang setzen, an deren Ende nicht nur das Geschäft im lokalen Markt in Gefahr ist. Ermittlungen in Deutschland könnten die Folge sein. Und das Unternehmen sehe sich im Rahmen des „Foreign Corrupt Practices Act" der Verfolgung durch die USA ausgesetzt.

Datenschutz

In der FAZ vom 6. September weist Rechtsanwalt Jörn Kuhn auf eine Entscheidung des BAG (2 AZR 681/16) hin, das zu der Frage ergangen ist, ob man die PC-Nutzung eines Arbeitnehmers mit Spähprogrammen ausforschen und ihm mit den so gewonnenen Daten kündigen darf. Das Gericht hat die Verwertung der vom Arbeitgeber derart erhobenen Informationen abgelehnt. Das Urteil bedeute aber nicht, dass der Einsatz solcher Software nun generell unrechtmäßig ist. **Keylogger** sollten nur in risikobehafteten Bereichen oder Tätigkeiten eingesetzt werden. Diese müssten von sonstiger Arbeit mit dem Computer abgegrenzt werden. Die Zweckbindung der Datenerhebung sei genauso darzustellen wie der Verwendungszweck der erhobenen Daten. Besteht im Unternehmen ein Betriebsrat, so seien die Regelungen zum Einsatz des Keyloggers mit ihm abzustimmen. Besteht kein Betriebsrat, müsse der Arbeitgeber eine transparente Anweisung zum Einsatz des Keyloggers vornehmen. Keylogger und Ähnliches könnten also weiterhin zulässig eingesetzt werden, wenn technische und organisatorische Vorgaben eingehalten werden. In derselben

Ausgabe wird über eine Entscheidung der Großen Kammer des Gerichtshofs für Menschenrechte (EGMR) berichtet (Az: 268 (2017)). Danach müssen Unternehmen ihre Belegschaft warnen, wenn sie beabsichtigen, private Chats mitzulesen. Im Fall eines Totalverbots der privaten Nutzung von Computer und Telefon am Arbeitsplatz habe der Arbeitgeber mehr Möglichkeiten, die **Kommunikation** zu **überwachen**. Dann könne er erwarten, dass keine Privatgespräche im Betrieb geführt werden. Ein Hinweis an den zu Überwachenden, dass einem Kollegen schon wegen privater Nutzung von Internet, Kopierer und Telefon gekündigt worden sei, genüge nicht. Vielmehr müssten Ausmaß und Art der Überwachung mitgeteilt werden.

Mehrheit der Unternehmen wird Datenschutzregeln verletzen, titelt die FAZ am 20. September. Die europäische Datenschutzgrundverordnung gilt ab Mai 2018. Von da an könnten die Aufsichtsbehörden Bußgelder verlangen, bis zu vier Prozent des konzernweiten Umsatzes. 54 Prozent der von Bitkom befragten Unternehmen würden jedoch angeben, die Regeln dann nur „teilweise umgesetzt" zu haben. Weitere acht Prozent hätten dann gerade erst begonnen. 13 Prozent hätten beantwortet, sie würden sich „bewusst" nicht mit den neuen Regeln beschäftigen. Die Behörden warnen: Die Unternehmen trügen die Verantwortung. Die „großen Unternehmen" seien in der Regel „gut unterwegs" – so die Datenschutzbeauftragte Niedersachsens. „Bei kleinen und mittelgroßen Unternehmen sei das Problem viel größer, wegen fehlender Ressourcen.

Datensicherheit

Die Zeitschrift Sicherheitsforum befasst sich in der Ausgabe 4-2017 mit Datensicherheit im Büro (S. 34). Nach einer Studie von Sharp gab ein Viertel der über 6.000 Befragten zu, Arbeitsinformationen in der öffentlich zugänglichen Cloud zu speichern und damit wissentlich gegen die Unternehmensrichtlinien zu verstoßen. 27 Prozent nutzten zudem **öffentliche File-Sharingdienste** ohne die Zustimmung ihres Arbeitgebers. Bieten Unternehmen flexible Arbeitsmodelle wie Homeoffice an, müssten sie den Mitarbeitern auch geeignete Mittel zum Schutz vertraulicher Informationen zur Verfügung stellen wie beispielsweise einen unternehmensinternen VPN-Anschluss.

Die FAZ berichtet am 21. September über Zahlen des sogenannten **Breach Level Index,** die das Unternehmen Gemalto veröffentlicht habe. Der Index registriere Verletzungen der Datensicherheit und deren Schweregrad im globalen Maßstab. Im Vergleich zur zweiten Jahreshälfte 2016 habe die Anzahl verlorener, gestohlener oder gefährdeter Informationen um 164 Prozent zugenommen. Der Sprung habe auch damit zu tun, dass die großen Fälle jeweils viele Mio. Datensicherheitsverletzungen umfassten. Allein 1,34 Mrd. Datensätze, vor allem E-Mail-Adressen in Verbindung mit Klarnamen und echten Wohnadressen, seien im ersten Halbjahr 2017 über ein Datenleck eines Marketing-Mailversenders bloßgelegt worden. Eine internationale Studie habe die Beziehung zwischen Börse und Cybersicherheit ermittelt. Demnach sei der Aktienkurs von zwei Drittel der Firmen, die eine Datensicherheitsverletzung erlitten, gesunken. Die Anteilsinhaber der 65 ausgewerteten Unternehmen hätten durch die Datensicherheitsverletzung 52,4 Mrd. Dollar verloren.

Einziehung krimineller Gewinne

Christian Schoop und Wolfgang Jäger, DLA Piper, weisen in der FAZ am 13. September darauf hin, dass seit 1. Juli 2017 Staatsanwaltschaften und Gerichte noch konsequenter als bisher alle **Erträge aus Straftaten** „einziehen" müssen. Für Unternehmen werde dies relevant, wenn Mitarbeiter zum vermeintlichen Wohl ihrer Firma Aufträge betrügerisch oder mit Schmiergeldern generiert haben. Für den Umfang der Einziehung gelte der Grundsatz: Was ein Unternehmen durch Verbotenes erlangt, soll an den Staat gehen, wobei allerdings für die Bestimmung des Erlangten legale Investitionen („Aufwendungen") abgezogen werden dürfen.

Endgerätesicherheit

Ildikó Bruhns, ESET Deutschland GmbH, erläutert in der September-Ausgabe des Behörden Spiegel, wie sich Sicherheit und Datenschutz bei Smartphones und Apps regeln lassen. Wer als Unternehmen private Mobilgeräte erlaubt, manövriere sich tief in datenschutzrechtliche und Sicherheitsrisiken. Spiele- und Spaß-Apps könnten sich einen Zugangsweg zu vertraulichen Geschäftsinformationen bahnen. Eine Absicherung ausschließlich auf Netzwerk- und Endpoint-Ebene greife standardmäßig zu kurz. Im Idealfall stellten Organisationen

betriebseigene Smartphones oder ein firmeninternes App-Portal zur Verfügung und vermieden so einen Gerätewildwuchs oder App-Dschungel. Wem es als kleines oder mittelständisches Unternehmen an Ressourcen fehlt, könne beispielsweise über Trennung von E-Mail-Konten, vereinbarte Richtlinien zum Einsatz einer Mobile-Device-Lösung inklusive App-Kontrolle auf privaten Smartphones im Doppeleinsatz Security und Datenschutz sicher steuern. ESET gebe **sieben Tipps,** um Sicherheit und Compliance zu verbessern: Mobile-Security-Lösung einsetzen; Betriebssysteme prüfen; Verschlüsselung nutzen; eigenes App-Portal einrichten; Mobile-Device Management-Lösung einsetzen; regelmäßige Updates und Tests; Handling vereinfachen.

Flughafensicherheit

Im Interview mit der Zeitschrift GIT-SICHERHEIT.de, Ausgabe 9-2017, S. 14–16, nimmt Friedhelm Jungbluth, Fraport AG, Stellung zur Unternehmenssicherheit am Luftverkehrsdrehkreuz **Frankfurt**. Zu den jährlich in der Sicherheitsleitstelle auflaufenden fast 100.000 Gefahrenmeldealarmen kämen etwa 25.000 Brandmeldealarme hinzu. Einer niedrigen Fehlalarmrate komme bei den automatischen Detektionssystemen eine immer höhere Bedeutung zu. Das Notfallmanagement umfasse grundsätzlich drei Themenkomplexe: Die Notfallplanung, die Krisenvorsorge rund um den Krisenstab und das sogenannte Care-Team für psycho-soziale Ersthilfe im Notfall. Im Rahmen der Notfallplanung würden Verfahren zur übergeordneten Gefahrenabwehr mit allen Beteiligten entwickelt. Es müsse gewährleistet sein, dass die Feuerwehr spätestens drei Minuten nach Alarmierung an jedem denkbaren Unfallort auf dem Start- und Landebahnsystem mit Lösch- und Rettungsmaßnahmen beginnen kann.

Gebäudesicherheit

Das **Zusammenwirken unterschiedlicher Gewerke** für Gebäudesicherheit thematisiert die GIT-Sonderausgabe PRO-4-PRO, S. 52/53. Vorgestellt wird eine neue Sprechstelle für Sprachalarmierung, Notbeleuchtung in hochmoderner OLED-Technologie (selbstleuchtende Pixel) und das Gefahrenmanagementsystem Winmag. Es verbinde eine hohe Integrationsfähigkeit der vorhandenen Systeme mit leichter Bedienbarkeit, intuitiver Steuerung und Automatisierung der Abläufe.

Das Münchner Startup Frogblue wolle das **intelligente Wohnen** revolutionieren, heißt es in der GIT-Sonderausgabe-PRO-4-PRO, S. 22/23. Kern der Innovation seien sogenannte Frogs, smarte Platinen, die in jede Unterputzdose einbaubar seien. Die intelligenten Frogs böten verschiedene Funktionen. Sie seien leicht zu programmieren und kommunizierten per Bluetooth Low Energy. Der Clou: Die Frogs kommunizierten untereinander und mit ihren Steuergeräten (Transponder, Smartphones, Tablets) per Bluetooth in der jüngsten Variante. Diese habe den entscheidenden Vorteil, dass sich nicht nur mehr Daten übertragen lassen. Auch die Reichweite sei deutlich erhöht.

Gefahrenmelder

Simon Foulkes, Honeywell, befasst sich in der Ausgabe 9-2017 der Zeitschrift GIT-SICHERHEIT.de, S. 72/73, mit Brandschutz- und **Notfallmeldelösungen.** Brandmeldeanlagen stellten ein zunehmend sicheres und zuverlässiges Rückgrat für die Integration anderer Anlagen wie etwa audiovisuelle Kommunikationssysteme dar. Der wesentliche Vorteil der Integration sei die Einhaltung der europäischen Richtlinien (EN54). Alle Notfallmeldevorrichtungen müssten analog dazu der EN 60849 entsprechen. Da Notfallmeldeanlagen immer mehr von den Möglichkeiten der drahtlosen Kommunikation Gebrauch machten, fügten sich Brandmeldeanlagen immer stärker in die Gebäudeautomation ein.

Das Fachmagazin DSD, Ausgabe 3-2017, weist auf Seite 25 darauf hin, dass die **überarbeitete ÜEA-Richtlinie** unter dem Titel „Bundeseinheitliche Richtlinie für Überfall-/Einbruchmeldeanlagen bzw. Anlagen für Notfälle/Gefahren mit Anschluss an die Polizei" (ÜEA-Richtlinie) – mit Stand Juli 2017 erschienen ist. Der Zeitpunkt der Umsetzung in den Bundesländern obliegt dem jeweiligen Bundesland. Eine Anpassung der VdS 2366 und die Anpassung der Anlagenbeschreibung für Videoüberwachungsanlagen an die neuen Auflösungklassen der DIN EN 62676-4 seien in Bearbeitung, ebenso eine Anpassung an die neue Ausgabe VdS 2311.2017-04(05).

Gefahrgutmanagement

Dipl.-Ing. (FH) Alexander Winkler, Neosys AG, stellt in der Ausgabe 4-2017 des Sicherheitsforum, S. 42–45, nützliche **Werkzeuge für den Gefahrgutbeauftragten** vor. Er erläutert das Vorgehen bei der Einführung eines Gefahrgutmanagements mit den drei Phasen Betroffenheitsabklärung, Einführung eines Gefahrgutmanagements und „Gefahrgutmanagement am Laufen halten". Als Elemente des Gefahrgutmanagements listet der Autor Vorschriften, Abläufe, das Vorgehen und Dokumente auf.

Gefahrstofflagerung

Sven Sievers, Asecos GmbH, stellt in der GIT-Sonderausgabe PRO-4-PRO den neuen **Asecos Sicherheitsschrank mit Vertikalauszug** vor (S. 63). In ihn seien neben den gesetzlich geforderten Sicherheitsmerkmalen weitere Sicherheitsaspekte integriert. Im Brandfall löse ein elektronischer Temperatursensor das Schließen des Vertikalauszuges ab einer Temperatur von über 40 Grand aus. Auch bei Stromausfall schließe der Auszug elektronisch. Für Mitarbeiterschutz sorge die inbegriffene Stoppfunktion. Der Vertikalauszug erkenne Widerstände während des Schließvorgangs und reagiere sofort darauf. Der Auszug werde ein Stück zurückgefahren, um ein Einklemmen zu verhindern. Der Auszug stoppe und melde optisch und akustisch, wenn ein Gegenstand ihn beim Öffnen blockiert.

Bei der Lagerung von **Druckgasflaschen** im Freien fordert der Gesetzgeber besondere Sicherheitsmaßnahmen in der TRGS 510. Neben einer ausreichenden Belüftung müssen die Druckgasflaschen gegen Umfallen gesichert sein und vor fremdem Zugriff geschützt werden. In der GIT-Sonderausgabe PRO-4-PRO (S. 66) werden die **SAFE Gasflaschen-Magazine** LIF von Säbu vorgestellt, deren Luftwechsel weit über dem geforderten Minimum läge. Die Sicherung der Gasflaschen erfolge durch verstellbare Haltevorrichtungen und Kettensicherungen. Der Gasflaschencontainer verfüge neben einer Statik nach Eurocode über eine langlebige, rundum verzinkte Konstruktion. Das Safe Gasmagazin verfüge über eine vom TÜV geprüfte konstruktive Eigenbelüftung, sei ausgestattet mit Lüftungskiemen an drei Seiten und einer Unterlüftung des Bodens. Die Zwangsbelüftung werde dann aktiviert, wenn zehn Prozent der Gaskonzentration der untersten Explosionsgrenze (ÜEG) überschritten werden. Übersteige die Gaskonzentration 20 Prozent, werde die Stromzufuhr zu allen elektrischen Geräten im Innenraum des Containers unterbrochen und es ertöne ein Warnsignal.

Hotelsicherheit

In der Ausgabe 9-2017 der Zeitschrift PROTECTOR wird gezeigt, wie im Sicherheitssystem eines Luxushotels das Management, die Sicherheit, das Marketing und der Betriebsablauf komplett vereinheitlicht wurden (S. 36/37). Im ersten Schritt seien 250 analoge Kameras durch lediglich 48 Vivotek Netzwerkkameras ersetzt worden. In der zweiten Phase sei eine Plattform installiert worden, auf der der Einsatz aller IP-Überwachungssysteme unter einer Oberfläche vereint wurden. Das Sicherheitssystem sei mit der Zutrittskontrolle und dem Brandschutzsystem integriert worden.

IT-Sicherheit

SAP-Kassensysteme einfach zu hacken, titelt silicon.de am 29. August. Voraussetzung sei aber, dass der Angreifer physischen Zugriff auf das Netz hatte, in dem das Kassensystem aufgestellt ist. Allerdings gebe es in vielen Ladengeschäften oder Einkaufshäusern Geräte, über die man sich unbemerkt einklinken kann. Ein Angreifer benötige dafür lediglich einen kleinen PC. Das Problem habe vor allem darin gelegen, dass der SAP POS Xpress Server keinerlei Authentifizierungsabfragen eingefordert habe. Das Leck sei inzwischen behoben. Viele POS-Systeme würden auf ähnlichen Architekturen basieren und könnten daher auch an ähnlichen Lecks leiden.

Die FAZ weist am 2. September auf die jüngste Mitteilung von Bitkom hin, nach der nur vier von zehn Unternehmen einen **Notfallplan** erarbeitet haben, der festlegt, welche Schritte im Fall eines erfolgreichen Cyberangriffs folgen. Unter Unternehmen mit mehr als 500 Mitarbeitern verfügten rund 68 Prozent über ein Notfallmanagement, bei Mittelständlern seien es 61 Prozent und bei kleineren Unternehmen mit bis zu 99 Mitarbeitern 40 Prozent. Auch von den Betreibern Kritischer Infrastrukturen hätte nur knapp über die Hälfte solche Pläne entworfen.

Im vernetzten Zuhause wird aufgerüstet, schreibt die FAZ am 4. September in einem Bericht über die Konsumelektronikmesse IFA in Berlin. Online angebundene Überwachungskameras gebe es für den Innenbereich, für den Außenbereich mit Schutz vor Wasser und Staub (Schutzklasse IP 65 beziehungsweise IP 67) oder als sogenannte Dome-Kamera. Besonders clevere Modelle nähmen nicht kontinuierlich auf, sondern dank integrierter Gesichtserkennung nur dann, wenn sie unbekannte Personen entdeckten. Wer sich generell nicht mit dem Gedanken an eine Alarmanlage anfreunden mag, für den verspreche das Start-up Mitipi eine Lösung. Ein **„virtueller Mitbewohner"** solle Aktivität vortäuschen, wo beispielsweise wegen Urlaubs keine mehr ist. Der Firmengründer Stylianou habe Patente auf Schatteneffekte angemeldet, die eine Schaltung durch ein Herauf- und Herunterdämmen der LEDs erzeugt. Und tagsüber, wenn die nicht gut zu sehen sind, solle die den Tagesablauf eines normalen Bewohners simulieren – einer, der kocht, Fernsehen schaut, duscht, Musik hört und sich auch mal mit seiner Freundin streitet. Die Akustik solle individuell anpassbar sein. Diese Kombination aus Licht und Akustik gebe es bislang noch nicht.

Managed Security Services (MSS) thematisiert Kevin Eisele, NTT Security, in der Ausgabe 9-2017 der Zeitschrift PROTECTOR, S. 44/45. Zu den Mindestleistungen, die Anbieter im MSS-Umfeld als wiederkehrende Betriebsleistungen im Infrastruktur-Management erbringen müssten, gehörten: Betriebsverantwortung durch den Dienstleister; präventive Wartung; Change Management; Support (Incident Management); Out-of-Band-Management und Service(Delivery) Management. Bei MSS stünden ganzheitliche Lösungskonzepte im Mittelpunkt, die den gesamten End-to-End-Sicherheitsservice abdecken. Bei MSS handle es sich nicht um Outtasking im klassischen Sinn, sondern viel umfassender um die Auslagerung von Risiken. Das Leistungsspektrum und Serviceangebot eines MSS-Providers sollte umfassen: Betrieb mehrerer Security Operation Center; Beschäftigung von Security-Analysten und Bereitstellung eines Computersecurity-Incident-Responseteams; Nutzung von Threat Intelligence Feeds; kundenübergreifende Erfahrungen und Korrelationen; Device Management; Security Monitoring; Vulnerability Management und SIEM as a Service. Die hohen Sicherheitsanforderungen seien für mittelständische Unternehmen ein Ding der Unmöglichkeit. Zu berücksichtigen sei, dass das auslagernde Unternehmen nicht durch eine extrem lange Vertragslaufzeit in Abhängigkeit eines bestimmten MSS-Anbieters gerät.

Die FAZ berichtet am 11. September über die Wandlung des Banknotendruckers **Giesecke + Devrient** zum **Software-Entwickler.** Dabei gehe es um die Sicherheit von Kredit- und Geldkarten sowie von Bezahlsystemen. Für die Sicherheit der Kommunikation sorgten „IoT Attach" und „IoT Advance". Die beiden SIM-Karten schützten vor unbefugten Zugriffen. Die steckbaren Karten hielten Einzug in das industrielle Internet. Die elektronische SIM-Karte (eSim) leite einen Umbruch ein. Seit zwei Jahren sei sie auf dem Markt. Sie erspare den Austausch der kleinen SIM-Karten bei einem Wechsel des Mobilfunkanbieters. Freischalten, Identifizieren, Einrichten der Benutzeroberfläche, Abrechnen – alles erfolge über das Internet und einen installierten Mini-Chip im Gerät. Der Wechsel von einem zum anderen Betreiber könne unkompliziert in wenigen Minuten erfolgen. Die digitale Offensive mobiler Bezahlsysteme sei nicht zu stoppen. Der ÖPNV biete mobiles Ticketing an. Alles müsse verbunden mit Softwarelösungen sein, welche die Transaktionen im Netz absichern und Informationen verschlüsseln. Im Frühjahr habe Giesecke ein Armband vorgestellt, mit dem etwa im Einzelhandel kontaktlos gezahlt werden kann. In drei bis sechs Monaten solle dieses „Wearable" von Finanzinstituten und Herstellern auf den Markt gebracht werden.

Mit dem **„Staatstrojaner"** befasst sich Michael Spehr, Redaktion FAZ, in der Ausgabe vom 12. September. Der Einsatz von Keyloggern und WLAN-Störern in privater Hand verstoße gegen geltende Gesetze. Für die Ermittlungsbehörden sei es indes wohl noch nie so einfach wie heute gewesen, verschlüsselte Kommunikation bereits an der Quelle anzuzapfen. Der sichere Datentransport zwischen Sender und Empfänger sei gut und schön. Wer jedoch seine IT-Infrastruktur nicht aufs penibelste abschottet, lasse Einfallstore für Angriffe von außen offen.

Reto Amstad, Siemens Schweiz, plädiert in der Ausgabe 4-2017 der Zeitschrift Sicherheitsforum, S. 30/31, für proaktive Maßnahmen, um einen optimalen Anlagenschutz zu erreichen. Mit **„Defense in Depth"** böte Siemens ein vielfältiges Konzept, das Anlagen sowohl rundum als auch in die Tiefe schützt. Das Konzept basiere auf Anlagen- und Netzwerksicherheit sowie Systemintegrität nach den Empfehlungen der ISA 99/IEC 62443, dem führenden Standard für Security in der industriellen Automatisierung. Das Konzept gliedere sich in drei große Schwerpunkte: Anlagensicherheit, Netzwerksicherheit und Systemintegrität. Das Konzept des „Plant Security Services" von Siemens basiere auf drei Säulen: Assess, Implement und Manage. Dabei beinhalte „Assess Security"

die umfassende Analyse von Bedrohungen, die Identifizierung der Risiken und die konkrete Empfehlung von Sicherheitsmaßnahmen. Mit „Implement Security" würden Schutzmaßnahmen umgesetzt, „Manage Security" bedeute eine regelmäßige Überwachung und Aktualisierung der implementierten Maßnahmen. Mit „MindApps" stelle das „MindSphere"-Ökosystem bereits eine Reihe von Applikationen für unterschiedliche Anwendungen zur Verfügung.

In der September-Ausgabe des Behörden Spiegel weist Oberstleutnant Volker Kozok, BMVg, darauf hin, dass das **TOR-Netzwerk** (The Onion Router) als datenstrombasierter Anonymisierungsdienst entwickelt worden sei. Die Nutzung sei dabei relativ einfach. Nutzer laden die Software runter und installieren den Browser auf ihrem PC. Mit dem Browser könne man neben den normalen Internetadressen auch Web-Seiten im sogenannten TOR-Netzwerk anwählen, die an der **Endung .onion** erkennbar seien. Diese Adressen seien kein Bestandteil der Domain Name Services. Die TOR-Technologie sei nicht entwickelt worden, um Kriminelle vor dem Zugriff der Ermittlungsbehörden zu schützen, sondern um eine geschützte und sichere Kommunikation ohne Überwachung sicherzustellen.

Der Behörden Spiegel befasst sich in der September-Ausgabe mit **simulierten Phishing-Versuchen.** Sie würden mit der Software Lucy durchgeführt. Damit ließen sich in kurzer Zeit E-Learning-Module erstellen oder Testkampagnen durchführen. Für den eigenen Phishing-Versuch könne aus anpassbaren Szenarien gewählt werden. Die Reaktionen der Mitarbeiter würden von Lucy selbständig überwacht und detailliert analysiert.

Jan Lindner, Panda Security plädiert in der September-Ausgabe des Behörden Spiegel dafür, den IT-Schutz als ein aktives System zu verstehen. Das bedeute, dass eine gute Endpoint Protection Plattform in der Lage sein müsse, jederzeit Veränderungen in den Datenmustern zu erkennen. Moderner IT-Schutz sollte nicht nur ausführbare Dateien klassifizieren, sondern müsse auch ihr Verhalten überwachen und analysieren. Mithilfe von **Data-Mining** und der Analyse mittels sogenannter **Big-Data-Analytik,** die fortschrittliche Algorithmen und künstliche Intelligenz nutzt, könne man in Echtzeit die Aktionen von möglicher Schadsoftware erkennen und auswerten sowie maßgeschneiderte Gegenmaßnahmen einleiten.

Nach einer Meldung von golem.de haben Forscher in den **Bluetooth-Implementierungen** fast aller gängigen Betriebssysteme zum Teil kritische Sicherheitslücken entdeckt. Diese ermöglichten einem Angreifer zum Teil, beliebigen Code auf dem Gerät auszuführen. Betroffen seien nach Angaben der Sicherheitsfirma Armis, die die Fehler gefunden habe, bis zu fünf Mrd. Geräte weltweit. Die Sicherheitslücken lägen nicht im Bluetooth-Protokoll, sondern in den jeweiligen Bluetooth-Stacks.

Nach Überzeugung des zuständigen EU-Kommissars gibt es zwei Arten von Unternehmen: solche, die Opfer von Cyberangriffen geworden seien, und solche, die nicht wüssten, dass sie Opfer von Cyberangriffen geworden sind (FAZ am 20. September). Die Zahlen sprächen eine deutliche Sprache: Mehr als 4.000 Angriffe mit Erpressungstrojanern wie „Wanna Cry" am Tag hätten die Statistiker 2016 gezählt. Das sei dreimal so viel wie ein Jahr zuvor. Den in der EU entstandenen Schaden schätze die Kommission auf jährlich 265 Mrd. Euro. Die zentrale Rolle zur Abwehr von Angriffen müssten Bürger und Unternehmen selbst spielen. Sie müssten sicherstellen, dass nicht nur ihre Computer, sondern auch alle anderen vernetzten Geräte vom Staubsauger bis zum Industrieroboter ausreichend geschützt sind. Cyberhygiene müsse genauso zum Alltag werden wie das Händewaschen vor dem Essen. Die Kommission dränge darauf, **einheitliche Sicherheitsstandards in der EU** einzuführen. Eine zentrale Rolle bei ihrer Erarbeitung solle die Europäische Agentur für Netz- und Informationssicherheit spielen.

GIT-SICHERHEIT.de geht in der Ausgabe 9-2017, S. 60/61, der Frage nach, wie verhindert werden kann, dass **Kameras und DVRs zu Bots** werden. Das seien „vernachlässigte Bereiche" eines Sicherheitssystems. Für Hersteller netzwerkfähiger Sicherheitsprodukte sei es eine Herausforderung, die richtige Balance zwischen einfacher Installation bzw. unaufwändigem Betrieb und dem Schutz des Geräts wie der angeschlossenen Infrastruktur zu finden. Arecont Vision setze auf Benutzererkennungen/Passwörter und auf eine eigene Architektur. Die Kameras des Unternehmens ließen die Einrichtung von Benutzerkennungen und 16-stelligen ASCII-Passwörtern für die grundlegende Cybersicherheit zu. In jeder Kamera werde die Bildverarbeitung von Arecont Vision auf einem integrierten Schaltkreis eines Field Programmable Gate Array durchgeführt. Damit werde sichergestellt, dass die Kamera nicht als Plattform für Cyberangriffe missbraucht werden kann.

Wie man sich vor Ransomware schützt, erklärt Kaspersky Lab GmbH in GIT-SICHERHEIT.de, Ausgabe 9-2017, S. 64/65. Endpoint-Sicherheitslösungen von Kaspersky Lab enthielten

ein spezielles Anti-Cryptomodul für die **Abwehr von Verschlüsselungstrojanern.** Die Einstiegsstufe Select verfüge neben Firewall und Anti-Malware über eine Programm-, Web- und Gerätekontrolle. Auch File-Server und Mobilgeräte seien in den IT-Schutz eingebunden. Bei der Stufe Advanced kämen Datenverschlüsselung sowie automatisiertes Patch-Management hinzu. Die höchste Stufe Total ergänze schließlich den Schutz von Collaboration- und Mail-Servern sowie Internet-Gateways.

Im Kampf gegen Hackerangriffe wolle **Baden-Württemberg** künftig kleine und mittlere Unternehmen unterstützen und schaffe dafür eine spezielle Anlaufstelle, meldet die FAZ am 21. September. Diese Cyberwehr genannte Einrichtung solle Firmen helfen, die keine eigenen IT-Spezialisten haben und mit der Abwehr von IT-Angriffen überfordert sind. Sie sei die Feuerwehr des 21. Jahrhunderts und sei dann unter einer einheitlichen Notfallnummer rund um die Uhr erreichbar. Für die Sofort- und Notfallmaßnahmen müssten die Unternehmen nichts bezahlen. Die Anlaufstelle gehe 2018 an den Start. Für weitergehende Maßnahmen solle sie Spezialisten vermitteln, für deren Dienstleistungen die Firmen dann allerdings zahlen müssten.

Der Bundesverband ASW hat ein Positionspapier zum Thema **„Handlungsfelder in der Cybersicherheit"** mit Stand 20. September 2017 veröffentlicht. Er kommentiert den aktuellen Status der Cybersicherheit in Deutschland und erarbeitet konkrete Handlungsempfehlungen in den drei Kategorien „Handlungsfelder für den Staat", „Handlungsfelder für die Wirtschaft" und „Gemeinsame Handlungsfelder für Staat und Wirtschaft". Handlungsfelder für die Wirtschaft sieht das Positionspapier in der Einführung von Grundsätzen und Standards für sichere IT-Systeme, die als Leitfaden für KMU dienen können, die klare Trennung von Cyber Security Governance und IT-Sicherheits-Umsetzungsverantwortlichkeit sowie Investitionen in die digitale Souveränität von Nationen. Als gemeinsame Handlungsfelder für Staat und Wirtschaft beschreibt das Positionspapier die Teilung von mehr Informationen, den Schutz kritischer Infrastrukturen, eine engere Verzahnung der Initiative Wirtschaftsschutz mit der Allianz für Cybersicherheit, eine Erhöhung der Bekanntheit der Initiativen zur Cybersicherheit, einen gemeinsamen Radar und gemeinsame Abwehr sowie die Förderung internationaler Standards und Gütesiegel.

IuK-Kriminalität

Wie die FAZ am 9. September berichtet, hat die amerikanische Wirtschaftsauskunftei **Equifax** mitgeteilt, Hacker hätten sich zwischen Mai und Juli 2017 durch das Ausnutzen einer Schwachstelle seiner Internetseite möglicherweise Zugang zu den Informationen von 143 Mio. amerikanischen Verbrauchern verschafft. Das ist annähernd die Hälfte der amerikanischen Bevölkerung. Gemessen an der Zahl der betroffenen Personen zähle der Angriff auf Equifax zu den größten, die es je gab. Zwei Cyberattacken auf Yahoo hätten zwar noch deutlich mehr Menschen getroffen, aber bei dem Angriff auf Equifax gehe es um viel sensiblere Daten. Der Sicherheitsforscher Brian Krebs vermute, Equifax habe seine Internetseite nicht ausreichend mit Sicherheits-Updates geschützt. David Emm, Kaspersky, rate Nutzern, sie sollten, wo immer es möglich ist, die sogenannte Zweifaktor-Authentifizierung einrichten. Damit sei auch gesichert, dass selbst im Fall eines Passwortdiebstahls Kriminelle nicht auf Konten von Internetdiensten zugreifen können, weil jeder Login über ein zweites Gerät autorisiert werden muss.

Krankenhaussicherheit

Hagen Zumpe, Salto Systems GmbH, beschreibt in der Ausgabe 9-2017 der Zeitschrift PROTECTOR, S. 26–28, das **elektronische Schließsystems des Isar-Klinikums München.** Der elektronische Kurzbeschlag XS4 Mini von Salto erfülle die Anforderung nach einfacher Installation in gleichem Maße wie ein Zylinder, weil er auf der DIN-Lochgruppe für Türrosetten ohne zusätzliche Bohrung installiert werden kann. Darüber hinaus passe er mit seiner Bedienung in den Klinikalltag. Technologisch basiere die Zutrittslösung auf dem Salto Virtual Network (SVN) mit patentierter Schreib-/Lese-Funktionalität und verschlüsselter Datenübertragung. Im SVN würden die Informationen zu den Schließberechtigungen auf dem Identmedium gespeichert, wodurch eine Verkabelung der elektronischen Beschläge und Zylinder entfalle. Gleichzeitig würden auch Informationen über gesperrte Identmedien auf die Identmedien geschrieben und somit weitergegeben. Die Online-Wandleser würden die ausgelesenen Daten an den zentralen Server übertragen und gleichzeitig die aktuellen Schließberechtigungen auf die Identmedien übermitteln. Ergänzt werde das SVN im Isar Klinikum an einigen Stellen um

Wireless-Zutrittspunkte, die per Funk in Echtzeit überwacht werden, Hinzu kämen relativ viele online verkabelte Türen. Neben den Türen seien Schranken, das Tiefgaragentor sowie die Lasten- und die OP-Aufzüge in die elektronische Zutrittslösung integriert. Bei der Rechtevergabe erfolge eine Plausibilitätsprüfung.

Die **Videobildanalyse** im Krankenhaus thematisiert PROTECTOR im Special Videoüberwachung, September 2017, S. 45. Um Klinik-Mitarbeiter vor Übergriffen durch Patienten oder deren Angehörigen zu schützen würde neben geeigneten Notruf- und Alarmierungssystemen mit akustischen Signalen zur Abschreckung Videoüberwachung eingesetzt. Die Kameras lokalisierten automatisiert den Alarmort und stellten die Bilder in Echtzeit dem Sicherheitspersonal zur Verfügung. Das Eindringen in bestimmte Bereiche wie etwa in ein Medikamentenlager könne mit Videobildanalyse-Modulen überwacht werden.

Krisenkommunikation

Dr. Richard Werner, Risk Control RCC GmbH, befasst sich in der Ausgabe 4-2017 der Zeitschrift Sicherheitsforum, S. 59–63, mit Krisenkommunikation. **Kommunikationsfehler** seien die Einnahme einer Opferrolle, Zorn als Reaktion, zweifelhafte Argumente und eingeschränktes Bedauern. Der Autor behandelt den öffentlichen Auftritt des Krisenkommunikators und das Problem „Shitstorm" (lawinenartiges Auftreten negativer Kritik). Es sei heute für jedes Unternehmen mit mehr als den Dimensionen eines Start-up nötig, die Kommentare und Geschichten, die zum eigenen Brand oder den Produkten geschrieben werden, zu monitoren und zwar rund um die Uhr. Wird auf einem Social-Media-Kanal berechtigte Kritik laut, dann müsse auch darauf reagiert werden.

Der ASW weist in seinem Newsletter vom 22. September darauf hin, dass er einen Leitfaden zu **Krisenmanagement und Krisenkommunikation bei Terroranschlag oder Amoklauf** veröffentlicht hat. Er gebe Hilfestellung, wie sich Unternehmen auf solche Fälle hinsichtlich Krisenmanagement, Krisenstabsarbeit und Krisenkommunikation vorbereiten können. Der Leitfaden behandelt vor allem, was während und nach einem Terroranschlag zu erwarten ist, wie Unternehmen sich vorbereiten sollten und wie die Entwicklung nach der Krise verläuft.

Ladendiebstahl

Die häufigsten Ladendiebstahl-Tricks beschreibt Buchautor Hans Günter Lemke in der Ausgabe 4-2017 der Zeitschrift Sicherheitsforum, S. 48–50: das Verschwindenlassen in großen Taschen; den Ablenkungstrick; „Teuer gegen billig", den Zupacken-Trick, den Einkaufswagen-Trick, den Zusatzkauf-Trick; den „Zeitschrift in Zeitschrift"-Trick; den Umetikettier-Trick; den Zusammensteck-Trick, den Vertrauenstrick; den Kinderwagen-Trick, den „Alt gegen Neu"-Trick und den Helm-Trick. Und er gibt trick-spezifische Vorbeugungsempfehlungen.

Maschinensicherheit

Zertifizierte Signalgeber stellt sicherheit.info am 28. August vor. Pfannenberg präsentiere mit den DNV-GL-zertifizierten Signalgebern passende Lösungen für raue Industrieanwendungen, bei denen Signalgeräte starken Erschütterungen, andauernden Vibrationen oder harten Stößen ausgesetzt werden. Zu den Anwendungsbereichen zählten unter anderem die Schwer- und Automobil-Industrie, Hafenanlagen und Werften.

Stefen Hensel, BetR, thematisiert in der GIT-Sonderausgabe PRO-4-PRO, S. 74/75, die **flexible Gestaltung von Sicherheitstechnik auf Linienebene.** Wenn während des Betriebes an den Maschinen etwas verändert wird, Maschinen entfernt werden oder neue hinzukommen, müsste jedes Mal die Sicherheitstechnik neu programmiert werden. Daher entwickle BetR ein Konzept, das völlig neue sicherheitstechnische Lösungen ermöglichen werde: **sich selbst organisierende Sicherheitsnetzwerke** auf der Basis von OPC UA (industrielles Kommunikationsprotokoll) und dem quelloffenen Sicherheitsprotokoll openSafety. Mit dieser Technologie werde es möglich sein, Maschinenteile oder ganze Maschinen aus dem Maschinennetzwerk zu entfernen oder zu ergänzen, ohne dass die Sicherheitstechnik neu programmiert werden muss. Mit Hilfe der OPC UA-Securitymechanismen werde eine sichere Verbindung hergestellt. Das neue Gerät suche nach weiteren Servern, die Safety-Funktionen anbieten. Die Sicherheitsapplikation prüfe, ob die neue Komponente bereits bekannt ist oder ob alle Eigenschaften aus sicherheitstechnischer Sicht gleichwertig zu einer zuvor validierten Konfiguration sind. Falls relevante Unterschiede erkannt werden, werde der Anwender aufgefordert, die Richtigkeit der Konfiguration zu bestätigen.

Im Interview mit GIT-Sonderausgabe PRO-4-PRO, S. 76–78, nimmt Frank Hagendorff, Berufsgenossenschaft Holz und Metall, Stellung zur Manipulation von **Schutzeinrichtungen an Maschinen.** Dieser Aspekt sei im gesamten Lebenszyklus einer Maschine relevant. Das beginne beim Einkauf des Kunden, der mit dem Lastenheft das gewünschte Einsatzspektrum definiert. Besteht im Betrieb ein klares Konzept zur sicheren Fehlersuche und Störungsbeseitigung, beuge man Manipulationen erfolgreich vor. Der Autor klassifiziert die verschiedenen Maßnahmen gegen Manipulation in drei Stufen: Das Ziel der ersten Stufe sei, Anreize zur Manipulation zu vermeiden. Manipulationen zu erschweren bilde die zweite Stufe der Methode. Die dritte Stufe nutze die Möglichkeiten, die sich durch die zunehmende elektronische Ausstattung der Maschinen anbiete. Ziel sei hier, vorgenommene Manipulationen zu erkennen.

Mehrere Aspekte der Maschinensicherheit behandelt die Zeitschrift GIT-SICHERHEIT.de in der Ausgabe 9-2017.

Vorgestellt werden in der Ausgabe 9-2017 von GIT-SICHERHEIT.de, S. 80–82, der **Sicherheitssensor RSS36 und die Sicherheitszuhaltung AZM300** von Schmersal. Beide Komponenten erreichten aufgrund der integrierten RFID-Technologie die Codestufe „hoch" gemäß der Norm EN ISO 14119, die höchste Anforderungen an den Manipulationsschutz stelle. Beide Einrichtungen seien mit einer integrierten AS-i Safety at Work Schnittstelle (zum Verkabelungssystem für die untere Ebene der Industriekommunikation) ausgestattet. Damit seien ein geringer Verdrahtungsaufwand und gute Diagnosemöglichkeiten verbunden.

Ein **„Functional Safety Management System"** umfasse Methoden und Verfahren, mit denen systematische Fehler bei der Entwicklung vermieden werden, d. h. Planung, Änderungs- und Modifikationsmanagement, alle Fragen des Hardware-Designs sowie Validierungs- und Verifizierungs-Aktivitäten und die Definition der hardwarebezogenen Anwendungs-, Installations- und Wartungsanforderungen (GIT-SICHERHEIT.de, Ausgabe 9-2017, S. 83).

Sicherheitsschaltgeräte für **Anwendungen unter extremen Bedingungen** (Offshore-Anlagen, extreme Kälte bis 60 Grad) stellt Dipl.-Ing. Rainer Lumme, Steute Schaltgeräte GmbH & Co. KG, in der Ausgabe 9-2017 von GIT-SICHERHEIT.de, S. 84/85, vor, zum Beispiel Positionsschalter, die auch für sicherheitsgerichtete Einsätze entwickelt worden seien und den Abmessungen der DIN EN 50041 entsprächen. Der Autor befasst sich mit den hohen Anforderungen an Gehäusekonstruktion und -abdichtung, mit der Sicherheit bei Minusgraden, bewährter Elektromechanik in robuster Bauform und der berührungslosen Schaltung in Extrembereichen.

Sichere Bewegungsüberwachung thematisiert GIT-SICHERHEIT.de in der Ausgabe 9-2017, S. 86/87. Die spiele in der modernen Fabrik- und Prozessautomation eine immer größere Rolle. Das neueste Produkt der Firma Bihl+Wiedemann sei das AS-i 3.0 EtherCAT Gateway, Safety over EtherCAT(FSoE), das Antriebe ohne zusätzliche Sicherheits-SPS (speicherprogrammierbare Steuerung) auf direktem Weg sicher steuern und überwachen könne. Ethercat gelte als schnellster Industrial-Ethernet-Standard. Zudem sorgten die kurzen Zykluszeiten von maximal 100 Mikrosekunden und der geringe Jitter (Taktzittern bei der Übertragung von Digitalsignalen) von höchstens einer Mikrosekunde für eine exakte Synchronisation.

Max Boehme und Michael Bangert, Sick AG, erläutern in der Ausgabe 9-2017 der Zeitschrift GIT-SICHERHEIT.de, S.88/89, warum die Scantechnologie SafeHDDM Sicherheits-Laserscanner im Einsatz bei der industriellen Parkettherstellung **immun** macht **gegen Holzspäne.** SafeHDDM (high definition distance measurement) sei ein durch die Sick AG patentiertes Verfahren, das durch intelligente Filterung und Auswertung ein für Sicherheits-Laserscanner einzigartiges Messergebnis liefere. Durch eine digitale Filterung der Remissionen zu einer Histogramm-Akkumulation würden zufällige Einzelremissionen ausgeblendet, während die Remissionen codierter Impulssequenzen des Scanners auch bei den geforderten geringen Signalstärken sicher erkannt und ausgewertet würden. Dadurch würden Staubpartikel die Erfassungssicherheit und zuverlässige Schutzfunktion erheblich weniger beeinträchtigen.

Um Prozesse – beispielsweise in modular aufgebauten Fertigungsstraßen – zuverlässig und sicher steuern sowie überwachen zu können, müssten Bedienpanels sämtliche Zustandsinformationen sofort erfassbar und intuitiv bereitstellen. Nur so könne der Mitarbeiter auch im Notfall seiner Überwachungstätigkeit gegenüber dem automatisierten System gerecht werden und schnell eingreifen. **Beleuchtbare Betätiger** erhöhten die Arbeitssicherheit in hochautomatisierten Produktionsumgebungen. Um die Normanforderungen der DIN EN ISO 13850:2015 im Zusammenhang mit steckbaren oder kabellosen Bedienstationen bzw. modularen Anlagenteilen zu erfüllen, müsse gleichzeitig immer mindestens ein herkömmlicher, aktiver Not-Halt-Schalter direkt an der Maschine vorhanden

sein. Für größtmögliche Sicherheit dürfe die Not-Halt-Taste nur bei Lichtverhältnissen verwendet werden, bei denen eine klare und eindeutige Erkennbarkeit des rot beleuchteten Pilzknopfs gewährleistet ist (GIT-SICHERHEIT.de, Ausgabe 9-2017, S. 92/93).

Notruf

Peter Niggl, Security insight, befasst sich in der Ausgabe 3-2017 des Fachmagazins DSD, S. 21–24, mit der Notrufproblematik. Von rund 1,3 Mio. Notrufen pro Jahr gebe es laut Polizei bei 300.000 keinen Grund für einen Polizeieinsatz. Zwei gegenläufige Tendenzen seien zu konstatieren: zum einen die Versuche, die Anzahl der öffentlichen NSL, vor allem für Notrufe auf der 112, zu reduzieren, zum anderen eine ständig wachsende Zahl von NSL privater Anbieter, die unter einem enormen Kostendruck arbeiteten. Es sei angezeigt, das Thema NSL umfassender zu regulieren, um einem Wildwuchs Grenzen zu setzen.

Perimeterschutz

Perimeterschutz zur Sicherung von Infrastruktureinrichtungen behandelt Martin Vogler, Senstar, in GIT-SICHERHEIT.de, Ausgabe 9-2017, S. 56/57. Er beschreibt elektronische Sensoren und Bodendetektionssysteme. Beide Systeme würden Durchdringungsversuche metergenau detektieren und darstellen. Sie könnten jahrelang beinahe wartungsfrei betrieben werden und würden bei einer Störung der definierten Grundstücksgrenzen den benötigten Zeitgewinn zur Intervention erzielen.

Rechenzentrumssicherheit

Wenn das Management komplexer IT-Prozesse die Kernkompetenz eines Unternehmens ist, werde die Sicherheit und Hochverfügbarkeit der eigenen IT-Infrastruktur eine unabdingbare Voraussetzung (PROTECTOR, Ausgabe 9-2017, S. 43). Kernstück des vorgestellten Unternehmens sei mit 70 qm der IT-Sicherheitsraum. Die Indoor-Lösung sei als modulares, hochverfügbares **Raum in Raum-System ECB*S-zertifiziert nach DIN 1047-2.** Für zusätzliche Sicherheit würden die Technikflächen, der Serverraum sowie der Hallenbereich überwacht und durch Zutrittskontrollen geschützt. Letztere authentifizierten Berechtigte mittels neuester Handflächenerkennungstechnologie und Code-Eingabe. Zudem sei der Technikbereich unterteilt in drei getrennte Brandabschnitte mit eigenen Zugangstüren, in denen sich die USV-Anlage sowie der Niederspannungshauptverteiler befinden. Der Serverraum werde mittels Kühleinheiten durch EC-Ventilatorentechnik gekühlt. Zusätzlich werde die IT indirekt dynamisch von außen gekühlt. Für den Brandfall seien flächendeckend eine Löschanlage sowie Rauchansaugsysteme installiert.

Brandfrüherkennung mit einem Aktivlöschsystem im Rechenzentrum thematisiert GIT-SICHERHEIT.de in der Ausgabe 9-2017, S. 68/69. Bei kleinen IT-Anwendungen mit einer geringen Anzahl an Serverschränken sei es sinnvoll, den Brandschutz auf Ebene der IT-Racks zu implementieren. Hierfür seien eine Reihe von Brandmelde- und Löschsystemen am Markt verfügbar. Diese Lösungen bestünden meist aus einer Brandfrüherkennungsanlage sowie einem Aktivlöschsystem und ließen sich in der 19-Zoll-Ebene des IT-Racks montieren. Im Rechenzentrum kämen nicht Wasser oder Aerosollöschmittel zum Einsatz, sondern Inertgase oder chemische Löschmittel wie Novec 1230. Letzteres ermögliche eine Bevorratung auf kleinem Raum im IT-Rack. Die Trennung der elektrischen Komponenten von der Energieversorgung, die innerhalb der Zeit erfolgen müsse, in der eine löschfähige Konzentration aufrecht zu erhalten ist, könne automatisiert mit einer schaltbaren Power Distribution Unit in Kombination mit einem Monitoring-System erfolgen. Den Schutz der IT-Komponenten könnten Unternehmen auf Rack-Ebene weiter erhöhen, indem sie Sicherheits-Safes verwenden.

Sicherheitsgewerbe

Die **Position führender Politiker** der im Bundestag vertretenen Parteien zum Sicherheitsgewerbe wird im Fachmagazin DSD, Ausgabe 3-2017, S. 3–10, wiedergegeben. Nach Überzeugung des Bundesinnenministers **de Maizière** sind private Sicherheitsunternehmen „fester Bestandteil unserer Sicherheitsarchitektur. Sie leisten einen wichtigen Beitrag zur Gefahrenvorsorge, sie sichern die privaten Rechte von Unternehmen und Bürgerinnen und Bürgern und sie stärken das all-

gemeine Sicherheitsgefühl. Große Events, aber auch Projekte der Wirtschaft, wie zum Beispiel Bauvorhaben, sind ohne die Mitwirkung von privaten Sicherheitsdienstleistern kaum noch vorstellbar." Dennoch sieht de Maizière für ein Gesetz mit speziellen Befugnissen für die Sicherheitswirtschaft „weder Raum noch Bedarf. Darin bin ich mir als zuständiger Bundesminister mit meinen Länderkollegen in der Innenministerkonferenz einig." Für einen Beauftragten oder ein zusätzliches Gremium für den Wirtschaftsschutz sehe er derzeit keine Notwendigkeit. Besonderen Wert lege er auf „die Weiterentwicklung und Vertiefung der strukturierten Kooperation von Staat und Wirtschaft und die Fortsetzung der guten Zusammenarbeit". Der Bayerische Innenminister Joachim **Herrmann** betont: „Welch tragende Rolle Sicherheits- und Ordnungsdienste in unserer Sicherheitsarchitektur haben, zeigt sich vor allem an den Beispielen Veranstaltungsschutz, Luftsicherheit sowie Sicherheit in und im Umfeld von Asylbewerberunterkünften." Vor dem Hintergrund der geänderten Sicherheitslage komme dem Einsatz der Sicherheitsdienste bei Veranstaltungen insbesondere hinsichtlich Zugangskontrollen, eine immer größere Bedeutung zu. Wichtig sei es, die Organisation der Luftsicherheit ständig kritisch zu hinterfragen. In der Diskussion um eine effizientere Gestaltung der Luftsicherheit könne das bayerische Modell mit staatlicher Mehrheitsbeteiligung Lösungsansätze aufzeigen. Im Lichte des Anspruchs auf zertifizierte und qualifizierte Sicherheitsdienste im Zusammenhang mit deren vielfältigen Aufgaben sei das Gesetz zur Änderung bewachungsrechtlicher Vorschriften vom 1. Dezember 2016 der richtige Schritt. Der Ausbau von Sicherheitskooperationen müsse bundesweit die Sicherheitsarchitektur verstärken. Dagegen bleiben nach Auffassung von MdB Irene **Mihalic** die geschaffenen gesetzlichen Bestimmungen hinter den tatsächlichen Anforderungen der verschiedenen betroffenen Aufgabenfelder zurück. Der eingeschlagene Weg einer Qualifizierung der privaten Sicherheitsdienste sei fortzusetzen. Einheitliche Standards und eine aussagekräftige Zertifizierung dienten einer besseren Zusammenarbeit. MdL Wolfgang **Kubicki** sieht eine klare Aufgabenteilung zwischen der privaten Sicherheitswirtschaft und der Polizei. „Alles, was grundrechtssensibel ist, fällt in den Bereich der Polizei. Die weiteren Bereiche können von der Sicherheitswirtschaft wahrgenommen werden." Diese klare Trennlinie sollte „auch nicht durch Hilfspolizei oder ähnliche Modelle, wie sie leider schon in einigen Bundesländern bestehen, verwischt werden." Hinsichtlich der Auftragsvergabe teilt die FDP „die Einschätzung des BDSW, dass Billigstvergaben beendet und Qualitätskriterien Teil der öffentlichen Auftragsvergabe werden müssen. Vorbild können andere Bereiche des Vergaberechts sein, wo es ähnliche Standards bereits gibt."

Christina Perzl, Aarcon GbR Unternehmensberatung, stellt in der Ausgabe 3-2017 des Fachmagazins DSD, S. 27/28 die **Frage nach IT-Sicherheit und digitaler Technik** im Sicherheitsgewerbe. Dienstleister sollten ihre Erfahrungen im IT-Bereich ausbauen, denn die einzelnen Schnittstellen und Gewerke ließen sich mittlerweile durch die Digitalisierung optimal vernetzen. In der Sicherheitstechnik müsse vom „Handwerksbetrieb" zum modernen „IT-Unternehmen" umgedacht werden und dementsprechend eine neue Personalausrichtung stattfinden. Die Mitarbeiter müssten zwingend im Umgang mit digitaler Technik geschult werden, damit man den Kundenanforderungen gerecht werden kann.

Software und Integration im Sicherheitsunternehmen thematisiert Walter Rijk, SequriX, im DSD, Ausgabe 3-2017, S. 29. Software könne zu vielversprechender totaler Integration führen, wenn mehrere Disziplinen der Sicherheit digitalisiert werden. Wenn Daten beispielsweise von Empfangsdiensten, Werk- und Objektschutz, Revierwachdiensten und Interventionsdiensten vollständig integriert und von einem System aus gesteuert werden, dann bringe das enorme Vorteile. Sicherungsprozesse würden schneller durchlaufen, und Kunden könnten besser mit vollständigen Berichten und Wachbüchern versorgt werden.

Sicherheitstechnik

GIT-SICHERHEIT.de weist am 30. August darauf hin, dass der BHE unter dem Titel **„Haftungsrisiken bei der Integration von Sicherheitstechnik in kundeneigene Netzwerke"** über die Risiken eines notwendigen Eingriffs in das vorhandene kundeneigene Netzwerk informiert und Tipps zur Haftungsvermeidung gibt. Zusätzlich sei im Hinblick auf Möglichkeiten der Haftungsbegrenzung eine BHE-Mustervorlage „Bedenkenanzeige und Kostenübernahmeerklärung" erstellt worden.

Wie sicherheit.de am 31. August berichtet, hat die Firma Pyronix einen **Passiv-Infrarotsensor für große Bereiche** auf den Markt gebracht. Dazu nutze der Octopus DQ einen Quad-Element Passiv-Infrarotsensor, der eine bessere Erkennungsleistung biete als herkömmliche deckenmontierte PIR-Sensoren mit zwei Elementen. Der Octopus DQ bestehe

aus hochwertigem Kunststoff, lasse sich optimal installieren und biete eine 360-Grad-Abdeckung in den Gängen von Geschäften, Büros und Lagerhallen.

Über den **Umsatzzuwachs elektronischer Sicherheitstechnik 2016** berichtet die GIT-Sonderausgabe PRO-4-PRO, S. 14/15. Er ist um 6,2 Prozent auf knapp 3,95 Mrd. Euro gestiegen. Die langfristige Wachstumsperspektive sieht Uwe Bartmann, ZVEI, in der Digitalisierung und Vernetzung mit anderen Gewerken. Die Videotechnik habe mit acht Prozent auf 511 Mio. Euro am stärksten zugelegt. Die Brandmeldetechnik sei nach wie vor das größte Segment der Sicherheitstechnik. Der Umsatz sei hier stark von der Baukonjunktur abhängig. Er ist 2016 um 6,8 Prozent auf knapp über 1,8 Mrd. Euro gestiegen. Ein hohes Wachstum habe auch die Überfall- und Einbruchmeldetechnik mit acht Prozent auf 800 Mio. Euro verzeichnet. Die Umsatzzahlen im Bereich Zutrittskontrolle hätten 307 Mio. Euro erreicht (+ 4,8 Prozent). Etwas abgeschwächt habe sich das Umsatzwachstum bei Sprachalarmierungstechnik mit 5,3 Prozent auf 100 Mio. Euro. Rauch- und Wärmeabzugsanlagen und Rufanlagen nach DIN VDE 0834 zeigten eine stabile Entwicklung.

Terrorismus

Deutschland im Fokus des internationalen Terrorismus lautet der Titel einer Ausarbeitung von Dr. Peter Roell vom ISPSW, die im September 2017 erschienen ist. Der islamistische Terrorismus sei in Syrien und im Irak noch nicht geschlagen. Er werde in den Untergrund abtauchen, sich dislozieren und im Rahmen des globalen Dschihad weiterhin Terroranschläge durchführen, auch in Deutschland. Der Autor beschreibt die Bedrohungslage auf der Basis dokumentierter Anschläge und terroristische Methoden, auf die man sich einstellen müsse. Die deutsche und europäische Politik müsse geeignete Abwehrmaßnahmen umsetzen und die Bevölkerung, die Industrie und die Wissenschaft in diesen Prozess einbinden.

Unternehmenssicherheit

Manuel Bohé, Concepture, erläutert in der Zeitschrift Sicherheitsforum, Ausgabe 4-2017, S. 21–23, weshalb die meisten Unternehmen ihre **Werk- und Gebäudesicherheit falsch dimensionieren.** Es seien im wesentlichen fünf Gründe: Reaktives statt vorausschauendes Handeln; die Wahl bekannter, aber im Einzelfall nicht geeigneter Mittel; mangelnde Risikoanalyse; das Übersehen des „Faktors Mensch"; falsche Beratung.

Der Arbeitskreis Integrierte Sicherheit BDSW/VfS gibt in der Ausgabe 3-2017 des Fachmagazins DSD, S. 17–20, Erläuterungen und **Handlungsempfehlungen zur integrierten Sicherheit** für Anwender, Sicherheitsdienstleister, Systemlieferanten, Errichter und Fachplaner. Entstanden ist eine kompakte Zusammenstellung von Strategien, die wichtige Anregungen und Hilfestellungen geben können. Behandelt werden in dem Fachbeitrag Herausforderungen im Wirtschaftsschutz, die Darstellung integrierter Sicherheit am Beispiel Objektschutz, Gründe für die integrierte Sicherheit, Zielsetzung und Nutzen für den Anwender, Optimierung des Prozesses, Planungssicherheit für das Budget, Schonung der Kundenressourcen und Zielgruppen (Branchenlösungen). BDSW und VfS planten als weiteren Schritt einen Leitfaden zur Vorgehensweise bei der integrierten Sicherheit.

Videoüberwachung

Eine Reihe von Beiträgen zur Thematik Videoüberwachung enthält die GIT-Sonderausgabe PRO-4-PRO:

Visualisierungstechnologie in modernen Kontrollräumen thematisiert Eyevis S. 16/17. Die heute gängigste Variante sei die Verwendung stegloser LCD-Bildschirme zum Aufbau von Bildwänden mit nur wenigen Millimetern Steg zwischen zwei Displays. Für größere Anlagen sei der Aufbau der Bildwand mit Rückprojektions-Cubes zu bevorzugen. Ihr Vorteil liege in der Verfügbarkeit in verschiedenen Größen und Auflösungen, eine ununterbrochene Betriebszeit von bis zu 100.000 Stunden und eine garantierte Unempfindlichkeit gegenüber Einbrenneffekten. Mit den Controllern aus der NetPix Reihe biete Eyevis verschiedene auf Server-Technologie basierende Hochleistungsrechner. Mit Software könnten mehrere Videowände und Einzeldisplays über die Grenzen einer einzelnen Grafik-Controllers hinaus zu einer Bedienoberfläche zusammengeschaltet werden.

Timo Sachse, Axis Communications, stellt die **Zipstream-Technology** von Axis zur **Videokompression** vor (S. 28–30).

Die Komprimierungstechnologie sei jetzt auch für die neuen 360-Grad-Fisheye-Kameras sowie Modelle mit 4K-Auflösung verfügbar. Da nicht vorhersehbar sei, wie komplex eine Szene werden kann, seien Technologien erforderlich, die dynamisch sind und ohne wiederkehrenden Konfigurationsaufwand auskommen. Der Ansatz von Axis Zipstream sei es, das Bild zu jedem Zeitpunkt vollständig und dynamisch zu analysieren und irrelevante Bildinhalte stärker zu komprimieren. Videokompression sei nicht verlustfrei. Einmal komprimiert seien die unkomprimierten Ursprungsinformationen nicht wiederherstellbar. H.264 und H.265 seien Sammlungen von Methoden, mit denen Videomaterial komprimiert werden kann. Je höher der Anspruch an die Bildqualität, desto vorsichtiger sollten diese Methoden eingesetzt werden, und je größer der Wunsch nach Reduzierung des Datenvolumens, desto optimistischer könne vorgegangen werden. In der Videoüberwachung müsse in Echtzeit komprimiert werden, und zwar direkt in der Kamera. Die Zipstream-Technologie analysiere das Bild vor der Komprimierung. Der Encoder in der Kamera werde mit diesen Informationen gefüttert und könne auf dieser Basis entscheiden, wo mehr und wo weniger komprimiert werden darf. Grundsätzlich gelte, dass ohne Prüfung der jeweiligen Szene keine Bitrate fundiert prognostiziert werden kann.

Fragt Ingo Take, Luna HD GmbH, in der GIT-Sonderausgabe PRO-4-PRO, S. 32/33. Viele Videoüberwachungsanlagen seien veraltet und brächten nur einen geringen Mehrwert. Der Wechsel auf ein neues System werde häufig aus Kostengründen gescheut. Die HD-CVI-Technologie sei jedoch in der Lage, die bestehende Infrastruktur weiterhin zu nutzen und gleichzeitig alle Vorteile moderner Videoüberwachung zu bieten. HD-CVI steht für High Definition Composite Video Interface. Mit dieser Schnittstelle sei es möglich, hochauflösende Signale über Koaxialkabel zu übertragen. Fernzugriff, Steuerung über mobile App, intelligente Suchfunktion und Instant Replay seien auch ohne IP-Kamera möglich.

Antworten des Technologieunternehmens Dahua auf IoT-Fragen enthält ein Beitrag auf S. 34/35. Die zukünftige **Entwicklung von HD-Analogvideo** müsse an die Anforderungen von IoT und Big Data-Anwendungen angepasst werden. Deep Learning mit KI werde dafür eine zentrale Technologiekomponente darstellen. Die HDCVI 4.0-Technologie von Dahua umfasse drei Schlüsselkomponenten: 4K-HDCVI für überlegene Videoaufnahmen, IoT-HDCVI für die mehrdimensionale Sensierung und AI-HDCVI zur Umwandlung HDCVI-Video in durchsuchbare Boolesche Daten. Die IoT-HDCVI-Technologie ermögliche es, Kameras in Kombination mit der **IoT-Sensierungstechnologie** zu beziehen. Mit Hilfe von IoT-Sensoren könnten Koaxialkabel nicht nur Videosignale übertragen, sondern auch Informationen wie Alarm, Temperatur und Feuchtigkeit. Die HDCVI-Technologiearchitektur unterstütze die komplexe Datenübertragung zwischen Kamera und DVR.

Die **automatische Verfolgung von Eindringlingen** mit intelligenter Videotechnik thematisiert Securiton in der GIT-Sonderausgabe PRO-4-PRO, S. 38. Eine nützliche Funktion sei die 3-D-Georeferenzierung des Videosicherheitssystems IPS VideoManager von Securiton. Kopple man automatisch steuerbare Kameras mit dem IPS VideoManager, ergäben sich mächtige Werkzeuge für die Objektsicherung. Strecke und Position von Eindringlingen könnten punktgenau im Lageplan visualisiert werden.

HTL. Ing. Elektrotechnik Guido Simak befasst sich in der Zeitschrift Sicherheitsforum, Ausgabe 4-2017, S. 18/19, mit der **Video Security-Norm EN 62676.** Er weist auf die neuen Abschnitte EN 62676-2-3 (Videoübertragungsprotokolle, IP-Interoperabilität) und EN 62676-5 (Standard für die Bewertung der Bildqualität) hin. Bisher hätten keine einheitlichen Standardisierungsvorschriften existiert, was dazu geführt habe, dass die von Herstellern an ihren eigenen Produkten durchgeführten Messungen und deren Ergebnisse oft nicht objektiv vergleichbar waren.

Nach einer Meldung in der September-Ausgabe des Behörden Spiegel plant **Bayern** eine deutliche Intensivierung der kameragestützten Beobachtung des öffentlichen Raumes. Demnach solle es sowohl mehr festinstallierte Videoüberwachungsanlagen der Polizei an Kriminalitätsschwerpunkten als auch eine verstärkte mobile Beobachtung der Sicherheitsbehörden geben. Des Weiteren sei ein Ausbau der kommunalen Videoüberwachung vorgesehen, vor allem im Bereich des ÖPNV. Gleiches gelte für öffentlich zugängliche Gebäude, Einkaufspassagen oder Veranstaltungshallen. Schließlich solle auch die eingesetzte Technik optimiert werden.

Nach einem Bericht in der Ausgabe 9-2017 der Zeitschrift GIT-SICHERHEIT.de, S. 34, erweitert Geutebrück sein Portfolio mit einer kamerabasierten Video-Contentanalyse. Die Video-Bewegungserkennung werde vom Kunden freigeschaltet. Hauptfeatures seien herrenlose oder fehlende Objekte, Objektzählung, Perimetersicherung, Loitering, Geschwindigkeit, Eindringen, Verlassen, zu lange Unbeweglichkeit, Abstandserkennung und Manipulationserkennung.

Videotechnologie in der Logistik 4.0 thematisiert GIT-SICHERHEIT.de in der Ausgabe 9-2017, S. 44/45. Mithilfe einer hochwertigen Videoanlage könne der Weg jedes einzelnen Containers lückenlos dokumentiert werden. Die Waren würden am Eingang eines Umschlagspunktes gescannt, während ihres gesamten Durchlaufs lückenlos verfolgt und beim Ausgang noch einmal elektronisch erfasst. Die erfassten Vorgangsdaten würden anschließend zusammen mit den Bilddaten vom digitalen Aufzeichnungssystem gespeichert. Der eingescannte Barcode sei der Schlüssel zu jedem einzelnen Packstück. Auch die Zusammenstellung ganzer Paletten oder Container könnten in allen Handlingsphasen überwacht werden.

Epko van Nisselrooij, Axis Communications Middle Europe, zeigt in der Ausgabe 9-2017 von GIT-SICHERHEIT.de, S. 58/59, wie **Netzwerk-Kameras in intelligenten Städten** die Lebensqualität verbessern. Die intelligente Stadt der Zukunft basiere auf einer Systemstruktur, die auf vier unterschiedlichen Technologieschichten beruhe. Die erste bildeten Sensoren, wie von Maschine zu Maschine kommunizierende Endgeräte, kabellose und mobile Sensoren, Kameras, die Video und Audio aufzeichnen. Alle Sensoren seien von einem Städtenetzwerk über die Kommunikationsinfrastruktur angeschlossen und bildeten die zweite Schicht des IoT. Die gemeinsame Betriebsplattform der Daten und Anwendungen bilde die dritte Schicht. In der vierten Schicht schließlich gehe es um die Einbindung der aktuellen wie der historischen Daten in Anwendungen für die intelligente Stadt. Die Kameras dienten als Knotenpunkt für den Anschluss anderer Sensoren an ein Netzwerk intelligenter Geräte, beispielsweise Verkehrs- und Zutrittskontrollsysteme. Viele Netzwerk-Kameras verfügten außerdem über integrierte multifunktionale Anwendungen wie Nummernschilderkennung, Personenzählung und Fahrzeugverfolgung.

Auch die Zeitschrift PROTECTOR hat im September ein Special zur Videoüberwachung herausgebracht:

Das von PROTECTOR & WiK zum 13. Mal veranstaltete **Forum Videosicherheit** 2017 wird zusammenfassend dokumentiert (S. 8–33). Die Diskussionsrunden fokussierten sich auf den Trend zur Wärmebildtechnik (S. 16–20), auf die Fragen, ob sich Qualität in der Videobranche heute überhaupt noch verkaufen lässt (S. 8–14), wie Videosysteme als Teil von übergeordneten Sicherheitslösungen verstanden und umgesetzt werden können (S. 22–27) und welche Auswirkungen die Entwicklung von Netzwerkbandbreiten und Speicherkapazitäten auf die Effizienz von professionellen Videosystemen haben (S. 28–33). Die Bandbreite an vernetzbaren Systemen sei extrem groß, vom einzelnen Smart Home über digitalisierte Industriekomplexe bis hin zur vollkommen vernetzten Stadt. Der Effizienzgedanke spiele in nahezu allen Anwendungen eine Rolle. Höhere Auflösungen und steigende Kamerazahlen forderten einerseits stärkere Kompression und smarte Codecs sowie andererseits optimale Nutzung von Bandbreiten und Speichern.

Die Beliebtheit von Videoanalyse sei eng mit dem **Wachstum in der cloudbasierten Sicherheit** verbunden, heißt es in einem weiteren Fachbeitrag (S. 34/35). Ein Internetbrowser könne die vom Videoüberwachungssystem gesammelten und ausgewerteten Daten in Grafiken und statistischen Reports aufbereiten und anzeigen. Die Cloudtechnik biete zahlreiche Vorteile. Zunächst würden keine speziellen Server-Spezifikationen benötigt, kein SQL und kein komplexes Netzwerk-Routing. Fernwartung und -diagnose könnten einfach über einen PC oder Smartphone ausgeführt werden. Die Cloud biete höhere Sicherheit und Widerstandsfähigkeit, komfortablen und mobilen Support, erhöhte Flexibilität und eine insgesamt angenehmere Bedienung.

Umfassende Sicherheitslösungen für **Smart Citys** erläutert Zhejiang Dahua Technology Co., Ltd. (S. 36/37). Die Smart City-Lösung nutze eine hochintegrierte Plattform und künstliche Intelligenz. Die Videoplattform nutze Deep Learning, um eine schnelle und effektive Risikoerkennung durchzuführen. Deep Learning ermögliche zudem eine unmittelbare Klassifizierung von Personen und Fahrzeugen im Video und eine Extraktion von detaillierten Merkmalen wie beispielsweise Kleidungsfarbe, Geschlecht, Kopfbedeckung, Nummernschild, Fahrzeugfarbe, Größe, Modell/Marke, Handynutzung. Die integrierte Plattform ermögliche eine einheitliche und zentralisierte Datenspeicherung.

Vorzüge des Live-Streamings mit Bodycams beschreibt Marie Clutterbuck, Digital Barriers plc. (S. 38/39). Es sei relativ anspruchsvoll, Videos verlässlich über Mobilfunknetze zu übertragen. Digital Barriers nutze für die Übertragung einen speziellen Edgevis-Codec, der auch bei sehr kleiner Bandbreite noch zuverlässig arbeite und so in schwachen Netzwerken operieren könne.

Nick D'hoedt, Genetec Deutschland GmbH, weist auf S. 42–44 darauf hin, dass Unternehmen, die Videoüberwachung in ganz oder teilweise öffentlichen Bereichen einsetzen, sich jetzt auf die GDPR vorbereiten müssten. Durch Verpixelung und

Maskierung könnten Risiken für den **Datenschutz** an der Quelle eliminiert werden, wenn die eingesetzte Technologie nachweisbar den Compliance-Anforderungen entspricht und ein striktes Zugriffsmanagement implementiert ist.

Mit der **Zukunft der Datenspeicherung** befasst sich Stephen Jones, Seagate Technology LLC, S. 48/49. Cloud Storage sei auch für die Videoüberwachung ein wichtiges Thema, das viele Vorteile biete. Zum einen würden die Daten in einem zentralen, gemeinsam genutzten System gespeichert, sodass Benutzer schnell und einfach von überall auf den Inhalt zugreifen könnten. Zum anderen sei es möglich, ein cloudbasiertes Produkt kontinuierlich und oft sogar in Echtzeit zu verbessern. Wenn Sicherheitskräfte und Notdienste Daten, die mittels künstlicher Intelligenz erzeugt werden, nutzen könnten, um intelligente Vorhersagen zu machen, würden diese dazu beitragen, präventive und Echtzeit-Taktiken aus Überwachungsaktivitäten zu verbessern, anstatt Daten in erster Linie als einen Berichterstattungsprozess für forensische Einsichten zu verstehen.

Die **videobasierte Intelligenz** zu erhöhen, sollte ein branchenweites Ziel sein. **Deep Learning** könne dabei helfen (S. 50/51). Deep Learning sei grundsätzlich anders als sonstige Algorithmen. Es überwinde die Unzulänglichkeiten der klassischen Algorithmen durch diverse Maßnahmen. Eine bestehe in der wesentlich tieferen Struktur. Die Zahl der Ebenen könne auf bis über 100 ansteigen, was eine komplexe Klassifizierung großer Datenmengen ermögliche. Es ähnele dem menschlichen Lernen und setze auf einen ebenenweisen Merkmalabstraktionsprozess. Als Simulation des menschlichen Gehirns durchlaufe das Signal im Deep Learning zunächst eine Ebene der Verarbeitung, als nächste finde ein teilweises Verstehen statt, schließlich folge eine übergeordnete Abstraktion. Einer der unmittelbaren Vorteile von Deep Learning liege in einer vergleichbaren oder sogar besseren Erkennungsrate, als sie ein Mensch erzielen würde. Hinzu kämen Fähigkeiten zur Erfassung und Klassifizierung tausender Merkmale. In den letzten beiden Jahren habe die Deep Learning-Technologie bei Spracherkennung, Computersehen, Stimmübersetzung und in vielen weiteren Anwendungen neue Maßstäbe gesetzt. Beim Einsatz intelligenter Videotechnik für die Zieldetektion, -verfolgung und -erkennung spiele der Aufstieg des Deep Learning eine große Rolle.

Freiflächenüberwachung mit **Laserscanner und Kamera** thematisiert Christian Jagusch, Lase Peco Systemtechnik GmbH, S. 54/55. Ein zweidimensionaler Laserscanner übernehme die Flächenüberwachung. Durch das lückenlose Netz der Laserstrahlen werde das gesamte Feld soweit wie möglich in der Horizontalebene abgedeckt, jede Bewegung sofort erfasst. Registriere der Laserscanner ein unerwünschtes Objekt, dann steuere er automatisch die Dome-Kamera und fokussiere sie zentimetergenau, damit diese ein scharfes Bild vom Eindringling machen könne und so die Identifikation gewährleiste. Dank neuester Lasertechnik und spezieller Algorithmen in der Programmierung eigne sich diese Technologie auch für den Einsatz bei widrigen Wetterverhältnissen. Unerwünschte Alarme würden auf einen Bruchteil der herkömmlichen Technologie verringert.

PROTECTOR enthält in dem Special Videoüberwachung **Marktübersichten** über 155 Nerzwerkkameras von 53 Anbietern, über 115 Produkte der Videomanagement-Software von 54 Anbietern und über 162 Produkte digitaler Speichersysteme von 65 Anbietern (S. 56–61).

Zutrittskontrolle

GIT-SICHERHEIT.de weist am 21. August auf das **SmartIntego Wireless-Schließsystem** von SimonsVoss und Axis hin. Die batteriebetriebenen digitalen SmartIntego-Schlösser würden sich in Form von Schließzylindern, Vorhängeschlössern oder SmartHandle-Türklinken per Funk über ihren GatewayNode und die Axis Entry Manager-Software mit dem Tür-Controller Axis A1001 verbinden. Die Lösung sei ein komplettes, skalierbares, vollständig integriertes Zutrittskontrollsystem. Die integrierte Lösung erlaube die Steuerung verdrahteter und drahtloser Türen, mit in Echtzeit überwachtem Zutritt und detaillierten Prüfpfaden.

Vorgestellt wird in PROTECTOR, Ausgabe 9-2017, S. 22/23, das Zutrittskontrollsystem der **Universität Hafencity (HCU) in Hamburg,** das den Verwaltungsaufwand minimiere und kurzfristige Änderungen ermögliche. Ausgewählt worden sei eine innovative elektronische Zutrittskontrolle von Siemens, deren Anlage mit Aperio-Komponenten der Assa Abloy Sicherheitstechnik ausgestattet ist. Im Einsatz seien 500 Offline-Elektronikzylinder. Die Aperio-Zylinder hätten den Vorteil, dass sie sich nachträglich verlängern lassen. Über das Online-Zutrittskontrollsystem ließen sich alle Zutrittsberechtigungen in RFID-Autorisierungen speichern. Die Nutzer benötigten nur noch ein Schließsystem und könnten auf den mechanischen Schlüssel verzichten.

Petra Eisenbeis-Trinkle, Dormakaba Deutschland GmbH, zeigt in der Ausgabe 9-2017 der Zeitschrift PROTECTOR, S. 24/25, wie das **Wohnungsunternehmen Vonovia** in Kooperation mit Insitech diverse Schließanlagen ausgetauscht und durch eine einheitliche Anlage ersetzt hat. Der Austausch von etwa 22.000 Profilzylindern in Hauseingangstüren habe ein detailliertes Konzept, gute Planung und sorgfältige Vorbereitungen vorausgesetzt. Bundesweit seien rund 8.000 Zugänge zu Heizungsräumen und Kellern mit den neuen Schließzylindern ausgestattet worden. Inzwischen seien deutschlandweit über 130.000 Zylinder geliefert und eingebaut worden.

Die Zeitschrift PROTECTOR enthält in Ausgabe 9-2017, S. 32/33, eine **Marktübersicht** über 27 Zutrittskontrollzentralen von 26 Anbietern. Abgefragt worden seien 29 Kriterien aus den Bereichen ZK-Hardware, ZK-Funktionen, Schnittstellen & Zusatzfunktionen und IT-Basis.

Markus Baba, HID Global, behandelt in der Ausgabe 4-2017 der Zeitschrift Sicherheitsforum, S. 64/65, den **digitalen Schlüsselbund auf dem Smartphone.** Smartphones seien immer häufiger Bestandteil der Zugangskontroll-Infrastruktur von Unternehmen. Durch den Einsatz von Mobile Access-Technologien mit NFC und Bluetooth würden sie zunehmend als universage digitale Ausweise verwendet, sowohl für den Zutritt zu Gebäuden wie für den Zugang zu IT-Systemen und Applikationen. Um Mobilgeräte im Rahmen einer Zugangskontrolle zu verwenden, müssten sie selbst umfassend geschützt werden. Um sicherzustellen, dass keine anderen Anwendungen auf sensitive Berechtigungsinformationen zugreifen können, sollte die Zugangs-App in einer dedizierten Sandbox laufen. Welche Kommunikationstechnik konkret zum Einsatz kommt, müsse sich am jeweiligen Einsatzszenario entscheiden. NFC habe nur eine Reichweite von wenigen Zentimetern. Der zentrale Vorteil kontaktloser und mobiler Technologie bestehe darin, dass sie auch für den Zugang zu IT-Systemen und Applikationen genutzt werden können und die Bereiche Sicherheitstechnik und IT immer weiter miteinander verschmelzen.

Lisa Abolt, Kentix GmbH, behandelt im Special Videoüberwachung der Fachzeitschrift PROTECTOR, September 2017, S. 40/41, **Zutrittskontrolle mit integrierter Videoüberwachung.** Sie bringe einen besonders deutlichen Mehrwert. Biete die Online-Zutrittskontrolle zusätzlich die Integration von Verzeichnisdiensten wie Microsoft Active Directory und LDAP, dann werde die Verwaltung des Systems noch einfacher. Jede beliebige Tür im System werde mit einer IP-Kamera verknüpft, die bei einer Buchung am Türöffner angesteuert wird und eine Bildserie aufnimmt. Nicht autorisierte Zugriffsversuche oder Sabotage würden direkt per Mail und mit Videoanhang an die Verantwortlichen weitergeleitet.

Impressum

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

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

Herausgeber
Manfred Buhl, Vorsitzender der Geschäftsführung, Düsseldorf

Verantwortlicher Redakteur
Bernd Weiler, Leiter Kommunikation und Marketing

Beratender Redakteur
Reinhard Rupprecht, Bonn

www.securitas.de/focus

Kontakt

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

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

E-Mail: info@securitas.de