Focus on Security

Ausgabe 04, April 2017

SECURITAS

Inhalt

Anschläge

Anhänger der linksmilitanten Szene haben nach einer Meldung der Berliner Morgenpost vom 2. März in Berlin **sechs Fahrzeuge des Sicherheitsunternehmens Securitas** angezündet. Auch wenn es kein Bekennerschreiben gebe, gehe die Polizei von einem politischen Hintergrund aus. Die Formel, die Security-Branche bedeute Repression und sei damit ein legitimes Ziel für Gewalt, gehöre im militanten Teil der Szene zum „kleinen Einmaleins". Das Thema angezündeter Autos beschäftige Berlin schon lange. Laut Innensenator Andreas Geisel gab es in den vergangenen Jahren jährlich zwischen 200 und 400 Brandstiftungen. Ein Viertel davon seien politisch motiviert. 2009 habe die Berliner Polizei den Höchstwert von 145 politisch motivierten Brandstiftungen registriert.

Wie die FAZ am 17. März berichtet, ist bei einer Explosion einer **Briefbombe** im Pariser Büro des IWF am 16. März eine Mitarbeiterin im Gesicht und am Arm verletzt worden. Inzwischen habe sich eine Gruppe von Linksterroristen aus Griechenland zu dem an das BMF in Berlin gesendeten Sprengstoffpakets bekannt, das dort in der Poststelle am 16. März abgefangen worden sei. Die Sendung sei an Finanzminister Schäuble adressiert gewesen und sei nach Angaben der griechischen Regierung in Athen verschickt worden. Die Selbstbezichtigung der Gruppe „Verschwörung der Feuerzellen" ist nach Angabe der griechischen Polizei glaubwürdig. Das Paket wäre laut deutscher Polizei geeignet gewesen, erhebliche Verletzungen beim Öffnen zu verursachen.

Bankensicherheit

Stephan Gorek befasst sich in Ausgabe 3-2017 der Zeitschrift PROTECTOR, S. 20–22, mit Sicherheit von **IT-Infrastrukturen und Prozessen** bei Banken. 2014 hätten Kriminelle mit der Schadsoftware Carbanak bei Angriffen auf bis zu hundert Banken, E-Payment-Systeme und andere Finanzinstitute zwischen 300 Mio. und einer Milliarde US-Dollar erbeutet. Bei der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse sei grundsätzlich auf gängige Standards abzustellen. Insbesondere seien Prozesse für eine angemessene IT-Berechtigungsvergabe einzurichten, die sicherstellen, dass jeder Mitarbeiter nur über die Rechte verfügt, die er für seine Tätigkeit benötigt. Die Zusammenfassung von Berechtigungen in einem Rollenmodell sei möglich.

Es gibt fast täglich **Angriffe von Hackern** auf die Computersysteme deutscher Banken, berichtet die FAZ am 17. März. Die Gefahr werde umso größer, da die IT-Sicherheitssysteme der Banken nach den Worten des BaFin-Exekutivdirektors für Bankenaufsicht, Raimund Röseler, schwerwiegende Mängel aufweisen. Immer mehr kriminelle Organisationen versuchten, sich in die IT-Systeme der Banken einzuhacken und würden zunächst über Monate hinweg nichts unternehmen. Erst wenn sie die Abläufe in der Bank genau kennen würden, schlügen sie zu. Die Zugangsmöglichkeiten zu den Systemen der Banken vergrößerten sich, weil die Banken immer mehr IT-Bereiche auf spezialisierte Anbieter übertragen würden. Die Zahl der Software-Anbieter habe sich deutlich verringert, wodurch sich Programmierfehler oder Sicherheitslücken schneller über das gesamte Bankensystem verbreiten könnten.

Bankräuber räumen in Deutschland jedes Jahr 5.000 Online-Konten leer, titelt die FAZ am 23. März. Die Digitalisierung ändere das Geschäftsmodell der Banken, könne aber auch ihre Existenz bedrohen. Denn die Angriffe von Hackern nähmen zu, sie erfolgten fast täglich. Und die erfolgreichen Attacken bemerkten die Banken oftmals nur, wenn es schon zu spät ist. Noch immer müssten Bankenaufseher das mangelnde

Risikobewusstsein der Banken rügen. Denn die meisten Cyberattacken bemerkten die Banken nicht selbst, sondern nach Hinweisen von Kunden oder Aufsehern. Die EZB dürfte nun nach einem Pilotprojekt eine Datenbank für Cyberrisiken einrichten. Alle 126 von ihr direkt beaufsichtigten Institute müssten dort Attacken melden, wenn diese eine bestimmte Verlusthöhe erreicht haben oder öffentlich bekannt werden. BaFin und Bundesbank hätten nun ein Rundschreiben zu ihren Anforderungen verfasst. Darin werde von den Banken eine IT-Strategie verlangt, was der Tatsache geschuldet sei, dass diese in vielen Instituten noch gar nicht vorhanden ist. Schwere IT-Mängel deutscher Banken stelle der oberste Bankenaufseher der BaFin, Raimund Röseler, fest. Gemessen an Schulnoten schneide kein Institut besser ab als vier. Ein durch Hacker ausgelöster großer Schadensfall könne zu einer neuen Finanzkrise führen, wenn die Kunden der Banken-IT nicht mehr vertrauen. 2016 hätten Hacker von 9.000 Kundenkonten der Bank des britischen Einzelhändlers Tesco 2,5 Mio. Pfund gestohlen. Es gebe auch Fälle, bei denen Mitarbeiter der Bank beteiligt waren. Das Risiko undichter Stellen nehme zu, weil die Banken immer mehr IT-Bereiche auf externe Dienstleister wie zum Beispiel IBM übertragen. Diese wiederum lagerten bestimmte Teilbereiche an weitere Dienstleister aus. Nach Angaben der EZB hätten die Banken aus dem Euroraum 2016 42 Prozent ihres IT-Budgets für Outsourcing ausgegeben.

Bodycam

DB-Sicherheitschef Hans-Hilmar Rischke plädiert in der Ausgabe 1-2017 des DSD, S. 63, für die Bodycam auch für Einsatzkräfte von Sicherheitsunternehmen. Mit der Bodycam werde nicht nur Beweismaterial bei Straftaten gesichert. Sie schrecke auch Angreifer ab. Gegen die Sicherheits-Teams mit Bodycams seien seit Beginn des Tests in den Bahnhöfen keine Angriffe und deutlich weniger Pöbeleien registriert. Neben der Aufzeichnungsfunktion sei vor allem der eingebaute Monitor sehr wirkungsvoll. Ist er eingeschaltet, würden sich Angreifer auf dem Bild selbst erkennen und von ihren Taten ablassen.

Brandschutz

Rauchmeldungen per Browser oder App thematisiert GIT in der Ausgabe 3-2017, S. 70/71. Mit dem Wi-Safe Gateway WG-1EU habe Fire Angel eine Internetanwendung entwickelt, die Alarmmeldungen überträgt und ein cloudbasiertes und kostengünstiges Monitoring zur unterstützenden Wartung von Rauchwarnmeldesystemen ermöglicht. Das Monitoring der Internetbrowser und Smartphone-App biete besonders Kleingewerbetreibenden wie Arztpraxen, Bürogebäuden, Apotheken, Kindertagesstätten oder Ferienunterkünften einen Mehrwert. Zudem erreiche eine Alarmmeldung im Brandfall genau die Person, die informiert werden soll. Das Gateway biete zudem Errichtern, Schornsteinfegern und Brandschutzfachhändlern ein intelligentes Diagnosetool, um die Funktion und Zustände ganzer Rauchwarnmelder-Netzwerke zu überwachen und die Funktionsfähigkeit zu gewährleisten. Es ermögliche Dienstleistern zudem, alle systemrelevanten Netzwerkparameter abzufragen.

Compliance

Kenan Tur, Business Keeper AG, plädiert in PROTECTOR 3-2017, S. 70/71, für **das richtige Compliance-Lösungssystem.** Deutsche Versicherungsunternehmen seien seit Juni 2016 dazu verpflichtet, bestimmte Compliance-Prozesse einzuführen. Unter anderem müsse es Mitarbeitern erlaubt sein, unter Wahrung der Vertraulichkeit ihrer Identität potenzielle oder tatsächliche Verstöße

gegen die Marktmissbrauchsverordnung (MAR)EU 596/2014 oder das Versicherungsaufsichtsgesetz (VAG) zu melden. Seit Januar 2017 seien börsennotierte Unternehmen mit mehr als 500 Mitarbeitern erstmals in der Pflicht, Maßnahmen und Umsetzung von „Softfacts" in ihre Berichterstattung mit aufzunehmen. Relevant seien zum Beispiel auch Arbeitnehmer-, Sozial- und Umweltbelange und Konzepte zur Korruptionsbekämpfung. Unternehmen, die gegen die Vorgaben verstoßen, müssten mit Strafgeldzahlungen bis zu zehn Mio. Euro beziehungsweise fünf Prozent des jährlichen Gesamtumsatzes der Kapitalgesellschaft rechnen. Experten würden Verantwortlichen empfehlen, sich im Rahmen der Nachhaltigkeitsberichterstattung an den Leitlinien der Global Reporting Initiative zu orientieren. Potenzielle Hinweisgeber könnten zukünftig nicht länger auf die zuvor von Ombudsleuten garantierte Anonymität vertrauen. Denn das LG Bochum habe entschieden, dass zwischen Ombudsleuten und Hinweisgebern kein „mandatsähnliches" Verhältnis bestehe. Hinweisgebersysteme seien ein wertvolles Instrument zur Risikoreduzierung und Minimierung von Haftungsrisiken. Als webbasierte Anwendung seien sie flexibel einsetzbar, ermöglichten eine zeit- und ortsunabhängige Meldung und könnten in jeder beliebigen Sprache aufgesetzt werden. Wichtig sei die Wahl des richtigen Hinweisgebersystems. Es sollte zertifiziert und auditierbar sein, sodass es auch zukünftigen normativen, sicherheits- und datenschutzrechtlichen Anforderungen gerecht wird. Bei Bedarf müsse die Anonymität des Hinweisgebers sichergestellt werden können. Dazu verlange es einer autarken Anwendung und spezieller Verschlüsselungsverfahren.

Auf einen Gesetzesentwurf des Bundesjustizministeriums zur Androhung von Sanktionen gegenüber sozialen Medien, die **Hassbotschaften** verbreiten, geht die FAZ am 15. März ein. Der Entwurf schaffe eigene „Compliance-Anforderungen", die die Autoren zielgruppengerecht genau so bezeichnen. Betreiber wie Facebook und Twitter sollen ein Beschwerdemanagement einrichten, um rechtswidrige Inhalte in offensichtlichen Fällen innerhalb von 24 Stunden zu löschen, innerhalb von klärungsbedürftigen Fällen innerhalb von sieben Tagen. Auf 28 Mio. Euro im Jahr schätzten die Autoren den Aufwand für die Unternehmen. Eine Million koste bereits der einzurichtende „Zustellbevollmächtigte", also eine Stelle im Unternehmen, die für jedes Zivil- und Bußgeldverfahren in Deutschland die Post entgegennimmt. Nur Netzwerke mit zwei Mio. Nutzern oder mehr im Inland sollen betroffen sein. Die Definition des „Sozialen Netzwerks" sei denkbar weit: Es komme nur darauf an, dass Nutzer beliebige Inhalte mit anderen Nutzern tauschen können. Thematisch und personell eingegrenzte Netzwerke sollen keiner Regelung unterliegen. Damit solle wohl das deutsche Geschäftsnetzwerk XING herausgeschält werden.

Datenschutz

In der Ausgabe 3-2017 der Fachzeitschrift GIT, S. 80/81, zeigt Veli Kirim, Hikvision Europe, wie datenschutzrechtlich unbedenkliche **Videoüberwachung** gelingt. Es gebe drei Dinge zu beachten: Personen dürfen nicht zu erkennen sein, das Datenmaterial muss verschlüsselt und die Datensicherheit durch das „Vier Augen-Prinzip" gewährleistet sein. Bei diesem Prinzip gebe es zwei individuelle Passwörter, die man benötigt, um Daten einsehen zu können. Die „Verschleierung" könnten Unternehmen im Fall eines kriminellen Vorfalls wieder aufheben, sofern es der Betriebsrat genehmigt. Um Videomaterial vor dem Zugriff Dritter wirksam zu schützen, sollte es bereits vor der Übertragung von der Kamera zum Rekorder Ende-zu-Ende verschlüsselt sein.

Digitalisierung

Digitalisierung meine mehr als nur intelligente, webbasierte Produkte und Systeme, schreiben Dr. Peter Fey und Jean-Francois Pauly, Dr. Wieselhuber und Partner GmbH, in der Zeitschrift PROTECTOR, Ausgabe 3-2017, S. 6/7. Die F&E-Quote sei mit 4,9 Prozent eher im Mittelfeld anzusiedeln. In der Elektrotechnik-Industrie habe sie 2013 bei 8,6 Prozent gelegen, im Maschinenbau bei 2,9 Prozent. Merkmale und Zustände von Komponenten und ganzheitlichen sicherheitstechnischen Systemen, zum Beispiel zum Perimeterschutz, seien in Echtzeit verfügbar. Immer leistungsfähigere Algorithmen sowie künstliche Intelligenz machten nutzbare Informationen daraus, ein wahrer Datenschatz, der häufig noch völlig brach liege. Die Kernfrage laute, welche Daten von wem auf welche Weise genutzt werden. Werde der Betreiber künftig bereit sein, dem Komponentenhersteller beziehungsweise Systemanbieter online Zugriff auf seine Daten zu gestatten, um „automatisiert" Serviceleistungen oder Vorschläge zur Systemoptimierung und damit zur Steigerung der Sicherheit bereitzustellen?

Der Behörden Spiegel weist in seiner März-Ausgabe auf ein von den Autoren Müller-Quade, Waidner und Backes erarbeitetes Positionspapier zur **IT-Sicherheitsforschung** hin. Danach nähmen die Herausforderungen schneller zu als politische Maßnahmen greifen könnten, weil Komplexität und Dynamik bei IKT stiegen. Beim überwiegenden Teil heutiger IT-Systeme sei Sicherheit nicht ausreichend im Entwicklungsprozess berücksichtigt worden. Zunehmende Komplexität und Verbreitung von IKT und immer mehr datenzentrierte Geschäftsmodelle würden die Angriffsfläche noch vergrößern. Es sei notwendig, eine Strategie für Cybersicherheit auf den Weg zu bringen, durch die Stärken besser erkannt und ausgebaut werden könnten. Große Bedeutung messen die Autoren Regularien zu Sicherheit, Datenschutz und Haftung bei.

Zum **Zusammenhang von Digitalisierung und Cybersicherheit** nimmt Arne Schönbohm, Präsident des BSI, in der Beilage ITK 2014 der FAZ am 17. März Stellung. Digitalisierung, Vernetzung und zunehmende Komplexität der IT böten Cyberangreifern weitreichende Möglichkeiten, Informationen auszuspähen und Geschäftsprozesse zu sabotieren. Das BSI stelle auf Wunsch Informationen über Risiken, Angriffsformen und Schutzmaßnahmen zur Verfügung und berate bei der Auswahl und Umsetzung von Sicherheitsmaßnahmen, insbesondere zur Härtung von IT-Systemen und IT-Netzen. Es gelte, Akteure aus Staat, Wirtschaft und Gesellschaft zu verzahnen, da nur ein gemeinsamer Ansatz zum Erfolg führen könne. Der Schutz von Deutschlands Kritischen Infrastrukturen müsse weiter konsequent verbessert werden. Dazu kooperiere das BSI im Rahmen des UP KRITIS mit den KRITIS-Betreibern. Zentrales Ziel des UP KRITIS mit seinen rund 400 Mitgliedern sei es, die Versorgung mit lebensnotwendigen Dienstleistungen möglichst uneingeschränkt aufrechtzuerhalten. Auch bilateral sowie im Rahmen der Allianz für Cybersicherheit, der mehr als 2.000 Institutionen angehörten, treibe das BSI die Zusammenarbeit mit der Wirtschaft voran. So leiste das BSI seinen Beitrag zum Gelingen der Energiewende durch die Erarbeitung von Sicherheitskriterien für die Infrastruktur der intelligenten Stromzähler und unterstütze bei der Erarbeitung der Sicherheitsaspekte einer digitalisierten Verkehrsinfrastruktur, in der autonomes Fahren möglich wäre. Die Wirtschaft bleibe in der Verantwortung, die Cybersicherheit für Unternehmen und deren Kunden zu verbessern und die eigenen Maßnahmen zur Prävention und Sensibilisierung auszubauen. Das BSI stehe bereit, um bei der Gestaltung der einzelnen Maßnahmen zu unterstützen.

Einzelhandelssicherheit

Martin Hildebrandt weist in der Ausgabe 1-2017 des DSD, S. 30, auf den Neustart der **„Sicherheitskraft Handel"** hin. Derzeit bedürften die ca. 15.000 in Deutschland eingesetzten Einzelhandelsdetektive nach der Ansicht des Handels dringend einer über die Regelungen der Sachkundeprüfung hinausgehenden Qualifizierung. In zwei Modulen zu je 40 Unterrichtseinheiten würde eine Reihe von handelsspezifischer Themen im neuen Zertifikatslehrgang behandelt, die in den regulären, allgemeinen Qualifikationen nicht oder nur am Rande thematisiert würden. Auf die Teilnahme an den Unterrichtseinheiten folge je Modul eine Abschlussprüfung.

Endgeräte

Wie golem.de am 2. März meldet, hat das australische Unternehmen Cog Systems auf dem Mobile World Congress in Barcelona ein Smartphone vorgestellt, das vor allem mit **Sicherheitsfunktionen** punkten soll. Zur Absicherung des Android-Systems verwende Cog Systems einen Hypervisor, der verschiedene Bereiche wie das Betriebssystem und einige der Schnittstellen in verschiedenen Domänen betreibe. Ebenfalls integriert sei ein fest verbauter und immer aktiver VPN-Dienst, der den ausgehenden Datenverkehr auf Wunsch nach auffälligen Mustern durchsuche, um Nutzer vor Gefahren zu warnen. Auch der Key Store sei mit einem Hypervisor vom Rest des Systems isoliert. Mit der Abschottung der verschiedenen Bereiche wolle Cog Systems die Sicherheit des Telefons verbessern.

Standard-Smartphones wie das iPhone oder Systeme mit den Betriebssystemen Android und Windows Phone verfügten immer noch nicht über ausreichende Sicherheitsvorkehrungen, betont Erwin Schöndlinger, Atos IT Solutions and Services GmbH, in der Ausgabe 3-2017 von PROTECTOR, S. 34. Eine Alternative seien spezielle **Mobilsysteme,** die **gegen Cyberangriffe „gehärtet"** seien. Solche Spezialsysteme verschlüsselten die gesamte Kommunikation mithilfe von sogenannten starken Verfahren wie AES 256. Eine sichere Authentifizierung könne mittels biometrischer Verfahren wie dem Scannen des Fingerabdrucks oder kryptografischer Authentifizierung erfolgen. Zudem verfügten Hochsicherheits-Smartphones im Allgemeinen über weitere Sicherheitsfunktionen. Ein Weg, um Risiken durch unsichere Apps zu minimieren, bestehe darin, nur Apps zur Installation freizugeben, die zuvor einer Prüfung unterzogen wurden und die im Einklang mit der Security-Policy des Unternehmens stehen.

Energiesicherheit

Niklaus Blaser und Mario Wolf, Keymile, befassen sich in der Ausgabe 1-2017 des Sicherheitsforum, S. 60/61, mit Problemen der **Notstromversorgung.** Bei den Notstromaggregaten ließen sich drei Varianten unterscheiden: Anlagen, die mit einem Dieselaggregat arbeiten, Wasserstoff- und Methanol-Brennstoffzellen. Eine Direkt-Methanol-Brennstoffzelle werde mit Methanol und Sauerstoff aus der Umgebungsluft versorgt. Diese Lösung biete eine leistungsfähige Möglichkeit, um einen von der Stromversorgung unabhängigen mehrtägigen Betrieb von „Mission Critical-Systemen und -Komponenten" sicherzustellen. Methanol ermögliche eine umweltfreundliche Energieversorgung, da es aus erneuerbaren Ressourcen wie Biomasse oder Abfällen aus der Landwirtschaft hergestellt werden kann. Es gebe auch keine beweglichen Teile, die einem natürlichen Verschleiß unterliegen.

Fensterschutz

Eine weniger als einen halben Millimeter dünne **Polyesterfolie** könne die Druckwelle nach einem Sprengstoffanschlag aushalten, berichtet die FAZ am 2. März. Die auf Sicherheitstechnik spezialisierte Haverkamp GmbH stelle nach eigenen Angaben als einziges Unternehmen in Deutschland solche Sicherheitsfolien her. Bewährt hätten sich die Folien bei dem Bombenanschlag auf das Regierungsviertel in Oslo 2011. Vier Jahre vor dem Anschlag sei begonnen worden, dort 15.000 qm Sicherheitsfolie zu montieren. Dadurch seien siebzig Menschenleben gerettet worden. Vor 15 Jahren sei damit begonnen worden, eine Spezialfolie zu entwickeln, die vor Industriespionage schützt. Der Schutz werde durch Metallisierungen in den Folien erreicht, die Infrarot- und Hochfrequenzsignale reflektieren. Der Hauptgrund für den Kauf einer Folie sei der Einbruchschutz. Die mit Folie versehene Scheibe halte auch wiederholten Einschlägen einer Axt stand. Der Preis für eine Folie, die diesen Anforderungen gerecht werde, liege zwischen 120 und 130 Euro pro qm inklusive Montage.

Gebäudesicherheit

Die wichtigsten Erkenntnisse einer Veranstaltung „Presse Round Table" von Honeywell Building Solutions zur vernetzten Gebäudetechnologie sind laut GIT, Ausgabe 3-2017, S. 24–26: vollintegriertes Managementsystem statt Inselbetrieb installieren; Prozessdefinition muss vor Technologieauswahl stehen; Betriebskosten bereits in die Planung einbeziehen; den Umgang mit der Technik vereinfachen und Informationen veranschaulichen; IT und Gebäudetechnik nähern sich an; Erfahrung von Planern und Beratern nutzen; moderne Tools helfen, komplexe Vorgänge zu verstehen.

Jochen Sauer, Axis Communications, berichtet in der Ausgabe 3-2017 der Fachzeitschrift GIT, S. 52–54, über die Entwicklung des **„Smart Building"** mit integrierten Systemen in der Praxis. Heutzutage übernehme meist derjenige den Part der Systemintegration, der den größten Anteil an dem System hat. Einen speziell beauftragten, gewerke- und systemübergreifenden Integrator gebe es nicht. Die Digitalisierung habe zwar den Gebäudebereich erreicht, trotzdem seien „smarte" gewerkeübergreifende Lösungen noch die Ausnahme, denn viele Hersteller versuchten, ihre proprietäre Systeme zu schützen. Funkwege seien meist unsicher und leicht manipulierbar. So sei es zum Beispiel mit einfachen Mitteln möglich, Infrarotmelder unter bestimmten Voraussetzungen zu umgehen. Bei einer korrekten Planung müssten die mechanische, die organisatorische und die personelle Sicherheit berücksichtigt werden. Hersteller müssten anfangen, mehr in Lösungen zu denken anstatt an einzelne passende Produkte. Ein gutes Sicherheitskonzept sollte im Vorhinein klären, wie das System mit anderen vernetzt ist, mit welchen Gewerken kommuniziert werden soll und mit welchen nicht. Beim Thema zukunftsorientierte Planung sollten sich Planer am Positionspapier des VDE orientieren. Für die heutigen Bauherren bedeute das, dass sie bereits an Technologien denken sollten, die erst in ein paar Jahren in die Gebäudesicherheit einfließen. Bauherren sollten anwenderneutrale, intelligente Netze für eine Zweit- oder Drittnutzung in Gebäude integrieren. Glasfaser beispielsweise stelle einen Zukunftstrend dar. Besondere Gefahr drohe von kostengünstigeren Plug-and-Play-Lösungen. Anders als Deutschland hätten andere Länder wie Dänemark und Singapur erste „selbstlernende" Häuser implementiert.

Gefahrstofflagerung

Roger Strässle, Chefredakteur Sicherheitsforum, behandelt in der Ausgabe 1-2017, S. 53–55, die Gefahrstofflagerung. Als gefährliche Stoffe im Sinne des Brandschutzes würden Stoffe und Zubereitungen gelten, die einen Brand verursachen können oder solche, die im Brand- oder Explosionsfall eine besondere Gefahr für Mensch, Tier und Umwelt darstellen. Für die Gefahrstofflagerung in feuerwiderstandsfähigen Sicherheitsschränken gelte die Norm EN 14470-1. Gefahrstofflager außerhalb der Produktionshalle sollten möglichst in Randbereichen des Industrieareals angesiedelt werden. Sie müssten zudem oberhalb des höchsten Grundwasserspiegels erstellt werden. Auch an Hochwasser sei zu denken, denn dringt dieses in den Lagerraum ein, könnten Gebäude zerstört werden und giftige Substanzen gelangten ins Wasser und in den Boden. Die Räumlichkeiten müssten flüssigkeitsdicht und mit Rückhalteeinrichtungen versehen sein, um auslaufendes Lagergut aufzufangen. Werden mehr als 100 Liter gelagert, müsse der Raum belüftet sein. Grundsätzlich würden Räume als genügend belüftet gelten, wenn sie über dem Erdboden liegen und mindestens zwei einander gegenüberliegende, nicht verschließbare Öffnungen aufweisen, die ins Freie führen.

Geo-Informationssystem (GIS)

GIS-Daten im Dienst der Sicherheit ist das Thema von Almut Eger, 4m2s – 4 Management 2 Security GmbH, und Martin Probst, bbp geomatik AG, in der Ausgabe 1-2017 der Zeitschrift Sicherheitsforum, S. 20–23. Die Autoren gehen auf die Verknüpfung der Informationen, die unterschiedliche Genauigkeit der Geodaten sowie auf Richtigkeit und Sicherheit von Geodaten ein und bringen Praxisbeispiele, die die Sicherheitsrelevanz aufzeigen. Entscheidend für eine sicherheitsrelevante Verwendung von Geodaten und Verbindung mit Fachinformationen seiendie Daten und Fachinformationen an sich und das Wissen darüber, wie genau und wie richtig diese Informationen sind die Verbindung von raumbezogenen Geodaten mit Fachinformationen und Kriterien zur Klassifizierung und Darstellung. Auch hier sei entscheidend zu wissen, um welche Genauigkeit, Aktualität und Richtigkeit es sich handelt und welche Nutzung möglich respektive sinnvoll ist.

Gesichtserkennung

Bei der Verwendung der Gesichtserkennungstechnik sei nach Überzeugung der Berliner Datenschutzbeauftragten mit hoher Sensibilität vorzugehen, berichtet der Behörden Spiegel in der März-Ausgabe. Der europäische Gesetzgeber habe die enormen Risiken biometrischer Gesichtserkennung für die Privatsphäre erkannt und die Erhebung dieser Daten in der ab Mai 2018 geltenden EU-Datenschutzgrundverordnung grundsätzlich verboten. Ausnahmen seien zulässig, wenn der Betroffene ausdrücklich eingewilligt habe oder wenn die Identifizierung aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist.

Industrie 4.0

Industrie 4.0 sei deutlich mehr **als ein Marketingbegriff,** argumentiert Burkhard Röhrig, GFOS mbH, in der Ausgabe 3-2017 der Zeitschrift PROTECTOR, S. 32/33. Eine zentrale Herausforderung bei der Digitalisierung und Industrie 4.0 bestehe darin, neue Entwicklungen und Technologien aus der IT wie Cloud Computing, Big Data, Apps, Virtual Reality, Smart Devices oder das Internet of Things gezielt zu nutzen, um darauf

aufbauend smarte Produkte und innovative Geschäftsmodelle zu entwickeln. Die Motivation und die Zufriedenheit der Mitarbeiter würden künftig noch stärker zum Schlüsselfaktor für unternehmerischen Erfolg. Bei aller Dezentralität, die Teil des Industrie 4.0-Konzeptes sei, sei es dennoch sinnvoll, eine zentrale Instanz zur Koordinierung und Synchronisation einzurichten.

Mikrokerne für mehr Sicherheit stellt Bernd Schöne, Journalist, in PROTECTOR, Ausgabe 3-2017, S. 36/37, vor. Statt auf Büro-IT würden immer mehr Anwender auf extrem abgespeckte, aber garantiert sichere Mini-Betriebssysteme setzen. Die schlanke Ware sei inzwischen in Milliarden Geräten verbaut. Die Produzenten von Malware hätten leichtes Spiel, immer neue Einfallstüren zu finden, denn Betriebssysteme würden nicht nur immer leistungsfähiger, sondern auch immer komplexer. Hacker müssten nur eine der in die Zehntausende gehenden Schwachstellen finden, und sie dann ausnutzen. Eine „Gegenbewegung" setze nun auf das genaue Gegenteil: Betriebssysteme mit so wenig Umfang wie möglich. Statt mit 40 Mio. kämen sie mit 20.000 Zeilen Code aus. Extrem kompakte Betriebssysteme würden Mikrokerne oder Mikrokernels genannt. Sie hätten eigentlich überhaupt keine Funktionalität, sondern böten starke Isolation und kontrollierte Kommunikation zwischen ansonsten isolierten Komponenten. Jüngstes Mitglied der Familie sei der Mikrokern „sel.4", der für besonders sensible Systeme gedacht sei. Er sei einer formalen Verifikation unterzogen worden. Mathematiker würden bei diesem Vorgang nachweisen, dass sich keine formalen Fehler in der Software eingeschlichen haben. Auch das neue Betriebssystem „KasperskyOS", das vor kurzem vorgestellt wurde, basiere auf Mikrokernel-Architektur.

Mit dem Ziel, verbesserte Technologien, Schnittstellen und Infrastrukturen für die Realisierung einer **digitalen industriellen Produktion** zu entwickeln, beteilige sich Siemens mit drei Partnern an einem Förderprojekt des Bayerischen Staatsministeriums für Wirtschaft und Medien, Energie und Technologie. Seit September 2016 arbeite das interdisziplinäre Expertenteam daran, die Prozesslandschaft der industriellen Massenproduktion bis auf die Werkstattebene digital zu erfassen und zu integrieren (PROTECTOR, Ausgabe 3-2017, S. 39). Die Forschungs- und Entwicklungsergebnisse sollten zeigen, dass durch die Digitalisierung sowohl Effizienzsteigerung als auch optimale Qualitätssicherung möglich sind. Um die Wertschöpfungskette innerhalb der Produktion zu digitalisieren, werde ein intelligenter Werkstückträger mit Kommunikations- und Ortungsfunktionalität im Rahmen eines sogenannten Cyber-Physischen Systems (CPS) ein zu fertigendes Produkt durch den gesamten Produktionsprozess begleiten. Anhand der mitgeführten Produktdaten und der gewonnenen Kontextinformationen solle der intelligente Werkstückträger eigenständig Prozessschritte erkennen, protokollieren und steuern. Das gewonnene Know-how solle nach Projektabschluss die Erweiterung und Übertragung des Konzeptes auf weitere Produktionslinien, Werke und Unternehmen ermöglichen.

IT-Sicherheit

Nach einer Umfrage von PwC unter mehr als 2.000 Führungskräften auf der ganzen Welt stuften nur noch 52 Prozent die Digitalkompetenz ihres Unternehmens als hoch ein. Das sei deutlich weniger als in den beiden Umfragen 2014 und 2015. Damals seien es noch 67 bzw. 66 Prozent gewesen. Nur 55 Prozent der befragten Entscheidungsträger meinten, dass Digitalprojekte in ihrem Unternehmen im Regelfall erfolgreich umgesetzt würden. Sogar 63 Prozent hätten einen Mangel an ausreichend qualifizierten Mitarbeitern beklagt (FAZ am 2. März).

Wie golem.de am 2. März meldet, hat das südkoreanische Telekommunikationsunternehmen SK Telecom einen **serienreifen Chip für Quantenverschlüsselung** entwickelt. Der nur 5 x 5 mm große Chip generiere nichtdeterministische Zufallszahlen, die die Grundlage für sichere Verschlüsselungssysteme bilden. Eingesetzt werden solle der Chip vor allem für Anwendungen im Internet der Dinge. Die Zufallszahlen würden per „Schrotrauschen" generiert.

Die Umsetzung des IT-Sicherheitsgesetzes laufe an, berichtet heise.de am 1. März. Betreiber Kritischer Infrastruktur der Sektoren Energie, IT+TK, Ernährung und Wasser müssten die ersten Prüfungsnachweise bereits zum 3. Mai 2018 beim BSI einreichen. In einem „Multiplikatoren-Workshop" habe das BSI die Schulungsinhalte und -konzepte festgelegt, nach denen Prüfer fortgebildet werden sollen. Das wiederum definiere, was und vor allem wie letztlich geprüft werden soll. Die Wirtschaftlichkeit gelte nur noch sehr begrenzt als Entschuldigung, eine eigentlich erforderliche Maßnahme nicht umzusetzen. Ein Problem wie etwa Mängel an der Speicherprogrammierbaren Steuerung (SPS) führe nicht zur Stelllegung der Anlage. Man bemühe sich eher um einen Dialog mit der Wirtschaft, statt auf formale Vorgaben und Strafen zu setzen.

IuK-Kriminalität

Einen gefährlichen **Schwarzmarkt für Cyberattacken,** auf dem Geheimdienste, Hacker und Kriminelle mit Informationen über Sicherheitslücken in Unternehmen handeln, sieht die FAZ am 9. März. Nach Meinung von Fachleuten gerate vor allem der Umgang mit Informationen über Sicherheitslücken außer Kontrolle. Die Geheimdienste vieler Länder suchten seit Jahren gezielt selbst nach systematisch ausnutzbaren Schwachstellen in IT-Systemen. Hierzu gebe es diverse Anbieter am Markt. Die sogenannten Zero Day Exploits, die den Betroffenen nicht bekannt seien, würden zum Eindringen in Unternehmensnetzwerke genutzt. Die Gerätehersteller wüssten nicht Bescheid über ihre Schwachstellen. Sechs- bis siebenstellige Summen würden auf dem Schwarzmarkt für Zero Day Exploits gezahlt. Zum Beispiel sollten Fernseher von Samsung in Abhörgeräte umfunktioniert worden sein. Dabei würden die Mikrofone so manipuliert, dass sie Unterhaltungen aufzeichneten, obwohl das Gerät scheinbar ausgeschaltet sei. Das BSI habe betont, dass es Erkenntnisse zu Sicherheitslücken, die öffentlich bekannt seien, auf eigenen Analysen beruhten oder sonst gewonnen würden, mit den jeweiligen betroffenen Herstellern diskutiere.

Peter Marwan berichtet in silicon.de am 9. März über eine Warnung der Polizei vor **betrügerischen Support-Anrufen** angeblicher Microsoft-Mitarbeiter. Den Behörden zufolge arbeiteten die Betrüger nach der bekannten Masche: Sie stellen sich am Telefon als Microsoft-Mitarbeiter vor und behaupten, der Rechner des Nutzers sei von Viren befallen. Dann bieten sie Software an, die es ihnen angeblich erlaube, das Problem zu beheben. Im Zuge der Installation der angeblichen Fernwartungssoftware werde allerdings entweder Malware auf den Rechner gespielt, über die die Betrüger auf das Gerät zugreifen und Daten ausspähen können oder, wie die Polizei Koblenz jetzt mitgeteilt hat, der PC gesperrt und erst nach Zahlung eines Lösegeldes wieder freigegeben. Nachdem Firmen wie Dell und Microsoft, deren Namen für solche betrügerischen Aktivitäten seit Jahren missbraucht werden, das Problem zunächst versucht hätten totzuschweigen, sei Microsoft im Herbst 2016 in die Offensive gegangen. Das Unternehmen habe damals eine Untersuchung vorgestellt, der zufolge immer mehr Nutzer Betrugsversuche durch Personen melden, die sich als Support-Mitarbeiter großer Firmen ausgeben.

Über **Hackerangriffe auf Autos** berichtet die FAZ am 10. März. Es gehe dem Geheimdienst um gezielte Attacken auf Smartphones und Computer von einzelnen Personen oder Organisationen. So könnten etwa der Standort des Nutzers ausgelesen, Telefone abgehört, Textnachrichten mitgelesen und Kamera und Mikrofone ferngesteuert werden. Wohl von der CIA gehackt worden seien auch Fernseher von Samsung aus den Jahren 2012 und 2013, auf denen die älteren Software-Versionen 1111, 1112 und 1116 liefen. Nachdem die Schadsoftware in das Zielsystem eingedrungen und den Zahlungscode namens „Weeping Angel" dort platziert hatte, seien die Fernseher in den sogenannten Fake-Off-Modus versetzt worden. Die Nutzer hätten geglaubt, das Gerät sei ausgeschaltet. Tatsächlich aber hätten die Mikrofone Gespräche im Raum aufgezeichnet und an die CIA übermittelt. Um Schadsoftware einzuschleusen, habe der Geheimdienst bis dahin unbekannte Sicherheitslücken direkt in den Betriebssystemen und Programmen genutzt. Ob und wie die CIA diese Sicherheitslücken missbrauche, sei unklar. Wer sich schützen wolle, solle generell mit gesundem Misstrauen im Netz surfen: keine Mailanhänge von unbekannten Absendern öffnen, nicht auf unbekannte Links klicken. Außerdem würden starke und vor allem viele Passwörter helfen. Denn wer dieselbe Zeichenfolge für alle Logins benutzt, gebe Hackern einen Universalschlüssel in die Hand. Sehr hilfreich sei auch die sogenannte Zwei-Faktor-Authentifizierung: Neben einem Passwort loggt man sich noch mit einer zweiten Komponente ein, beispielsweise einem speziellen USB-Stick.

Die Schattenseite des Internets – das **Darknet** – behandelt der Behörden Spiegel in der März-Ausgabe. Das bekannteste Darknet sei das Tor-Netzwerk. Eine mehrfach verschlüsselte Umleitung des Datenverkehrs über Server des Tor-Netzwerks mache eine Rückverfolgung praktisch unmöglich. Der Nutzer könne so im Prinzip das gesamte World Wide Web anonym erreichen. Doch das Tor-Netzwerk ermögliche es auch, Webseiten anonym zu betreiben. Solche sogenannten Hidden Services seien über normale Suchmaschinen nicht auffindbar. Um sie zu erreichen, müsse man ihre Adressen-Kombinationen von Buchstaben und Zahlen mit der Endung „onion" direkt im Tor-Browser eingeben. Es gebe im Darknet illegale Waren aller Art zu kaufen: Falschgeld und gefälschte Dokumente nach Wunsch; gestohlene Ausweise, Kreditkartendaten oder ganze virtuelle Identitäten; Pharmaka und Drogen; einsatzbereite Trojaner, Viren und andere Malware; Waffen und Gewaltvideos. Genauso floriere der Markt für Dienstleistungen im Darknet: Crime as a Service. Botnetze könnten für Cyberattacken stundenweise gemietet werden. Wem das Know-how dafür fehlt, selbst Angriffe durchzuführen, der könne auch einen Dienstleister beauftragen. In den letzten Jahren seien die kriminellen Angebote zunehmend professioneller und zugänglicher geworden. Bezahlt werde mit digitalen Währungen, vor allem Bitcoin, die komfortable, direkte und vor allem anonyme Zahlungsvorgänge ermöglichten.

Wie das Sicherheitsforum in der Ausgabe 1-2017, S. 37, berichtet, gehe aus einer KMU-Umfrage der Zurich 2016 hervor, dass kein Risiko derart an Bedeutung gewonnen habe wie die Cyberkriminalität. Inzwischen gingen zwölf Prozent der KMU in der Schweiz davon aus, dass Hacker ein Schlüsselrisiko für sie darstellen (2013: 2,8 Prozent).

Wie der Bundesverband ASW in seinem Newsletter am 24. März berichtet, fälschen **Phishing-Angreifer** immer öfter E-Mails und Internetseiten, um auf diesem Weg in den Besitz vertraulicher Daten wie Passwörter, Zugangsdaten, Kontoinformationen oder Kreditkartennummern zu gelangen. Noch viel zu häufig gäben Nutzer dann ihre Daten freiwillig preis und machten damit den Weg frei für Betrug und den Verlust schützenswerter Informationen und Daten. Wie solche Angriffe erkannt werden können und wie man richtig darauf reagiert, erfahre man in einer Videoserie der exploqii library SECURITY.

Im Newsletter vom 24. März meldet der Bundesverband ASW, das **Mobilbetriebssystem Android** werde sicherer. Das melde Google in dem jährlichen Sicherheitsbericht. Demnach habe sich die Verbreitung von potenziell gefährlichen Apps zwischen 2014 und 2016 deutlich reduziert.

Korruption

Das seit Juli 2011 in **Großbritannien** geltende neue Antikorruptionsgesetz enthalte nicht nur Straftatbestände für Einzelpersonen, sondern auch einen Unternehmensstraftatbestand der unterlassenen Verhinderung von Bestechung, so die FAZ am 15. März. Danach könnten sich auch deutsche Unternehmen mit einem Geschäftsbezug zu Großbritannien strafbar machen, wenn eine diesem Unternehmen nahestehende Person eine andere Person in der Privatwirtschaft oder im öffentlichen Sektor besticht und dabei zugunsten des Unternehmens handelt. Ein Verfahren durch Verständigung auszusetzen sei seit 2014 möglich – nicht nur in Korruptionsfällen, sondern auch bei Betrug oder Geldwäsche. Den möglichen Inhalt solcher Verständigungen und den Ablauf von Verhandlungen dazu regele im Wesentlichen ein von britischen Strafverfolgungsbehörden veröffentlichter Leitfaden. Voraussetzung für Verhandlungen sei danach, dass dem öffentlichen Interesse bereits durch eine Verständigung hinreichend genügt werden könne. Neben einer frühen Selbstanzeige und einer vollständigen Kooperation spielten Kriterien wie etwa frühere Verstöße des Unternehmens, die Schwere des Verstoßes und der entstandene Schaden eine Rolle. In Deutschland gebe es bei Ermittlungsverfahren wegen Straftaten oder Ordnungswidrigkeiten mit Unternehmensbezug bisher kein vergleichbares formales Prozedere.

Krisenregionen

In einem Hintergrundbericht beschreibt SmartRiskSolutions GmbH Risiken für Unternehmensaktivitäten in der **Türkei** und gibt unter anderem folgende Empfehlungen: Überprüfung bzw. Erweiterung bestehender Notfallpläne, insbesondere zu den Themen der Festnahme von Mitarbeitern, Durchsuchungen von Büroräumen durch Ermittlungsbehörden sowie dem Notfallmanagement bei einem Terroranschlag und Evakuierungspläne; due diligence zu Geschäfts- und Joint Venture-Partnern, um nicht ungewollt durch Partnerschaften ins Visier von Ermittlungsbehörden zu geraten; Überprüfung gemeinsam mit den betroffenen Mitarbeitern, ob es besondere Risiken im Profil und durch Aktivitäten des Mitarbeiters bei Türkeireisen gibt; Prüfung, ob es eine indirekte Gefährdung durch Terroranschläge gibt, zum Beispiel durch potenzielle Anschlagsziele in der Nähe der eigenen Liegenschaften oder nahegelegenen Orten von Demonstrationen (Newsletter des Bundesverbandes ASW vom 24. März).

Künstliche Intelligenz (KI)

Mit der zunehmenden Bedeutung KI für die Sicherheitstechnik und möglichen Auswirkungen auf das Sicherheitsgewerbe befasst sich Manfred Buhl, Securitas Deutschland, in der Ausgabe 3-2017 des PROTECTOR, S. 66–68. Der Autor beschreibt Möglichkeiten von KI in den Bereichen der Entwicklung von Robotern und von Drohnen, in der Biometrie und der Analysesoftware in Videokameras. Er zeigt, wie KI Planung und Strategie bei Sicherheitsunternehmen unterstützt: durch Data Mining, bei Predictive Analytics und in der Prognose der Entwicklung des Sicherheitsmarktes unter Verwendung der „Szenariomethode". Fazit: KI werde Märkte und Geschäftsmodelle verändern, aber das

Sicherheitsgewerbe brauche die fortschreitende Anwendung von KI nicht zu fürchten. Die in immer kürzeren Innovationszyklen fortschreitende Intelligenzfähigkeit der Sicherheitstechnik ermögliche es Sicherheitsunternehmen, immer leistungsfähigere Sicherheitslösungen anzubieten: in der Sensortechnologie, in der Bildanalyse, in der Biometrie und in der intelligenten Auswertung von „Big Data".

Luftverkehrssicherheit

Rechtsanwältin Juliane Holtz behandelt in der Ausgabe 1-2017 des DSD, S. 12–14, die **Novellierung des Luftsicherheitsgesetzes** (LuftSiG) vom November 2016. Neben der Verhängung von Einflug-, Überflug-, Start- oder Frachtbeförderungsverboten für einzelne Luftfahrzeuge oder eine näher bestimmte Gruppe von Luftfahrzeugen beträfen grundlegende Änderungen des LuftSiG insbesondere die sichere Lieferkette, die Zuverlässigkeitsüberprüfung und die Beleihungsmöglichkeit. Nach § 9a LuftSiG benötigten lediglich Transporteure – im Gegensatz zum europäischen Recht – nun auf nationaler Ebene eine Genehmigung. Probleme bereite die im neuen § 9a enthaltene Verpflichtung von reglementierten Beauftragten oder Luftfahrtunternehmern zur Feststellung der Identität einer Person, die eine Sendung übergibt. Die geforderte Dokumentationspflicht gehe über die europäischen Bestimmungen weit hinaus. Nach dem neuen LuftSiG sei auch für Beschäftigte der sicheren Lieferkette, die außerhalb des Flugplatzgeländes tätig sind, stets eine Zuverlässigkeitsüberprüfung durchzuführen. Dies betreffe vor allem Beschäftigte bekannter Versender, reglementierter Beauftragter oder anderer Beteiligter der sicheren Lieferkette, sofern sie aufgrund ihrer Tätigkeit unmittelbaren Einfluss auf die Sicherheit des Luftverkehrs haben. Zur Passagierkontrolle seien zusätzlich Beleihungstatbestände eingeführt worden, die z. B. die Zulassung von Luftsicherheitsplänen, die Zulassung von reglementierten Beauftragten und die Zertifizierung sowie die Zulassung und Überwachung von Sicherheitsausrüstung betreffen.

Maschinensicherheit

Mit der **Absicherung komplexerer Maschinen** und Anlagen befasst sich Udo Weber, Schmersal, in der Ausgabe 3-2017 der Zeitschrift GIT, S. 74/75. Auf der Wunschliste der Konstrukteure im Maschinen- und Anlagenbau stehe die Flexibilität der eingesetzten Komponenten und Systeme ganz obenan, gefolgt von dem Wunsch nach einfacher Montage der Maschine und umfassender Diagnoseinformation. Diese Trends beträfen auch die Maschinensicherheit. Grundprinzip der Installationssysteme sei es, dass der Maschinenbauer die Sicherheitsschaltgeräte nicht mit der jeweiligen Sicherheitssteuerung bzw. dem zugehörigen Sicherheitsrelaisbaustein verbindet, sondern mit einer separaten Einheit, die im Schaltschrank oder im Feld installiert werden kann. Dort würden die Signale gebündelt und an die Auswerteeinheit oder die Sicherheitssteuerung weitergeleitet. Die Sicherheitsschaltgeräte würden einfach in Reihe geschaltet. Ein besonderer Vorteil bestehe darin, dass unterschiedliche elektronische Sicherheitsschaltgeräte wie Sicherheitssensoren und -zuhaltungen gemischt in der jeweiligen Anwendung anschließbar sind. Für Anwendungen mit ausschließlich elektronischen Sicherheitsschaltgeräten stünden zwei Installationssysteme zur Verfügung: mit passivem Verteilermodul und mit passiver Feldbox. Eine dritte und aktive Variante gebe es für Sicherheitsschalter und Sicherheitssensoren.

Holger Unger, Pepperl+Fuchs, zeigt in der Ausgabe 3-2017 der Zeitschrift GIT, S. 87/88, wie ein innovatives Sensorkonzept und der Kommunikationsstandard IO-Link vielseitige **Integrationsmöglichkeiten**

eröffnen. Alle optoelektronischen Funktionsprinzipien im jeweils identischen Kleingehäuse, IO-Link-Konnektivität als Standard, intuitive Integration und Bedienung – die zukunftsorientierte Produktarchitektur der Lichtschrankenserien R100, R101 und R103 von Pepperl+Fuchs böte alle Optionen für die smarte Automation. Darüber hinaus überzeuge die neue Lichtschranken-Generation immer mehr Anwender durch die Vielzahl innovativer Technologien. IO-Link und SmartBridge ermöglichten Konnektivität und Kommunikation bis in die Cloud. Die neue Lichtschrankengeneration stehe erst am Anfang ihres Produktlebenszyklus.

Netzwerksicherheit

Siegfried Becker-Ullmann, Siemens AG, präsentiert in der Ausgabe 3-2017 der Zeitschrift GIT, S. 84/85, **Automatisierungstechnik und Netzwerksicherheit** aus einer Hand. Industrielle Netzwerksicherheit und IT-Sicherheit seien zwei Sprachen – als würden die einen portugiesisch und die anderen spanisch sprechen. Bilfinger GreyLogix habe Pakete entwickelt, durch die die beiden Bereiche problemlos kommunizieren können. Aufgrund der erstklassigen technologischen Ausrüstung mit Siemens-Komponenten könnten auch umfangreiche sicherheitstechnische Dienstleistungen für Kunden direkt im IT-Securitylabor angeboten werden. Das Spektrum reiche von der Analyse von Kundennetzwerken über die Entwicklung kundenspezifischer Lösungen bis hin zur Abnahme von Site bzw. Factory Acceptance Tests. Es gelte, eine hohe Sicherheit beim Anlagenbetrieb in einem digitalisierten Umfeld zu schaffen.

Perimeterschutz

Michael Luckey und Kira Lichte, Perimeter Protection Germany, befassen sich in der Ausgabe 3-2017 von GIT, S. 60/61, mit Problemen der **Sicherheit im öffentlichen Raum.** Der Trend in allen Sicherheitsbereichen gehe hin zur Kombination verschiedener Komponenten. Umfassender Perimeterschutz auf öffentlichen Plätzen könne nur durch eine Kombination von mechanischen und elektronischen Komponenten geschaffen werden. Dazu gehörten, je nach Art des Perimeters, eine Außensicherung mit Crash-Pollern oder anderen zertifizierten, Anpralllast-getesteten Barrieren, gegebenenfalls Fahrzeugschleusen mit Schnellfalttoren oder einer Schranken-Schiebetorkombination, Anlagen zur Personenvereinzelung und Zutrittskontrollsystemen sowie eine ergänzende Videoüberwachung.

Produktpiraterie

Lösungen zur Bekämpfung von Schmuggel und Produktfälschung wurden beim Europäischen Polizeikongress im Februar in Berlin erörtert. Auf über 460 Mrd. US-Dollar hätten sich allein die Profite durch Plagiate belaufen, habe Thomas Franke vom Forum Vernetzte Sicherheit ausgeführt. Prof. Blind, TU Berlin, habe als erstes bessere Kooperationen der Institutionen gefordert. Vor allem brauche man den Einsatz von Technologien, die ein Tracking und Tracing auch von Standardprodukten ermöglichten. Nur zwei Prozent der Container könnten aufgrund von Personalmangel beim Zoll im Hamburger Hafen kontrolliert werden.

Der deutsche Zoll hat auf der Frankfurter **Sanitär- und Klimamesse ISH** mutmaßliche Produktfälscher gestellt, meldet das Hauptzollamt Darmstadt. Insgesamt habe man 169 verdächtige Artikel sichergestellt.

Die Nachahmer geschützter Markenprodukte stammten meistens aus China und der Türkei. (FAZ am 25. März)

Das Sicherheitsforum weist in der Ausgabe 1-2017, S. 68, auf das ganzheitliche Überwachungssystem **„Packet Power"** hin. Diese über die Firma Daxten erhältliche Lösung funktioniere via Funktechnologie und führe verschiedene Monitoring-Funktionen auf nur einer Systemebene zusammen. Mit dem Sensormodul zur Detektion von Wasserleckagen sei das Packet Power Monitoring um einen wichtigen Baustein erweitert worden. Neben Stromwerten und Umgebungsbedingungen (Temperatur, Feuchte, Differenzdruck) könnten auch von Leckagen bedrohte Areale im Rechenzentrum zuverlässig überwacht werden. Funkmessmodule, die Stromwerte auf jeder Verteilungsebene (Raum, Abzweigung, Rack, PDU, IT-Gerät) erfassten, komplettierten die Monitoring-Familie.

Erhöhten Schutz durch **kompakte IT-Safes** stellt Simon Federle, freier Journalist, in der Ausgabe 3-2017 von PROTECTOR, S. 38, vor. Das Rack im Kompaktrechenzentrum „DC-ITSafe" biete vollen Zugriffsschutz und sei nachweislich das feuerbeständigste Mini Data Center der Welt. Den Schutz vor Einbrüchen und unautorisiertem Zugriff gewährleisteten eine nicht aushebelbare Schwenkriegeltechnik und die selbstverriegelnden Türen. Darüber hinaus sei das Gehäuse so konzipiert, dass es Sicherheit vor Lauschangriffen respektive Abstrahlung biete. Zusätzlich würde das Rack einen Einbruchsschutz RC 2 für Werkzeugangriff nach EN 1630 aufweisen. Der DC-ITSafe sei EI90 feuerbeständig nach EN 1363-1 und erfülle als einziger über 40 Minuten lang die Grenzwerte nach EN 1047-2. Das Mini Data Center halte auch allen anderen wesentlichen Gefahren wie Gas, Explosion sowie Löschwasser stand. Die eingebaute Klimatisierung sei redundant und als DX-Invertertechnologie, mit Leistungsstufen von 1,6 bis 8,1 Kilowatt, modifizierbar individuell als Kaltwasserersatzlösung.

Patricia Späth und Bernd Hanstein, Rittal, stellen in der Ausgabe 3-2017 der Zeitschrift GIT, S. 62–65, das **Micro Data Center von Rittal** vor. Es sei in verschiedenen Sicherheitsstufen verfügbar und ermögliche es, IT-Komponenten wie Server, Storage oder Netzwerk in einem Schutzraum bis zur Widerstandsklasse 4 zu betreiben. Das Umhausungssystem richte einen vollständigen Sicherheitsbereich um ein 19-Zoll-Rack ein. Darin fände IT-Hardware auf 42 oder 47 Höheneinheiten ihren Platz. Somit biete das System einen hohen Grundschutz gegen physikalische Bedrohungspotenziale wie Diebstahl, Feuer, Fremdzugriff, Staub, Vandalismus, korrosive Gase und Löschwasser. Je nach individuellen Anforderungen lasse sich die Lösung zu einem kompakten Rechenzentrum ausbauen. Die Sicherheitsfunktionen sorgten dafür, dass im Fall eines Feuers die garantierten Brandschutzwerte von 90 Minuten nach DIN 4102 (F90) eingehalten werden. Rauchgase könnten nicht eindringen. Es bestehe die Möglichkeit, bis zu vier Micro Data Center aneinanderzureihen.

Risikomanagement

Dr. Ing. Ralf Mock und Dr. sc. nat. ETH Christian Zipper, ZHAW, befassen sich in der Ausgabe 1-2017 der Zeitschrift Sicherheitsforum, S. 45–47, mit dem Management-Werkzeug für Organisation und Kontrolle smarter Produktions- und Dienstleistungssysteme. Ein **smartes System** sei eine Infrastruktur mit erweiterter technischer Leistungsfähigkeit, die dafür ausgelegt sei und betrieben und unterhalten werde, um zur nachhaltigen Entwicklung und Resilienz beizutragen. Die Erwartungen an solche smarten Systeme seien neben ökonomischen Vorteilen eine ausgewiesene Resilienz und Nachhaltigkeit. Die ISO/TS 37151:2015 kläre die Begrifflichkeiten. Resilienz bedeute, dass Systeme dafür ausgelegt seien, Dienste in Notfällen weiterhin zu erbringen und sich

rasch von Schäden und der Einstellung von Diensten zu erholen. Funktion und Aufbau smarter Systeme seien mehrschichtig und erforderten die Analyse mindestens dreier Ebenen: Software-Ebene, Kontroll-Ebene und physische Ebene. Vor allem die Kontrollebene sei einem massiven Wandel unterworfen. Nach Meinung der Autoren bedeutet der Einzug von Smartness in Unternehmen und Organisationen, dass das gewohnte Risikokonzept als Basis für das technische Risikomanagement möglicherweise unzureichend ist. Umfassende konzeptionelle und methodische Änderungen und Neuerungen, wie man die neuen Systeme handhaben solle, deuteten sich an.

Schließsysteme

Schließ- und Schlosslösungen für gewerbliche und private Gebäude stellt Assa Abloy in der Ausgabe 3-2017 von GIT vor (S. 42/43). Die **Alarmsicherung Exitalarm** biete eine visuelle und akustische Hemmschwelle gegen missbräuchliche Türbenutzung. Der elektromechanische Beschlag Code Handle Window verhindere, dass Fenster und Terrassen- sowie Balkontüren, die sich ausschließlich von innen verriegeln lassen, unkontrolliert geöffnet werden. Einbrecher könnten den Griff selbst bei gekippter Terrassentür nicht bewegen. Bei wiederholt falscher Eingabe blockiere der Griff für drei Minuten. Mit der elektronischen Schließlösung „Entr" der Marke Yale könne die Haustür per Fernbedienung, Smartphone, Fingerabdruck oder durch PIN-Eingabe geöffnet werden – und auch weiterhin gewohnt mit einem normalen Hausschlüssel. Der elektronische Zylinder verriegele die Haus- oder Wohnungstür automatisch, wenn der Bewohner sie zuzieht. Der Zylinder biete keine Angriffsfläche für Manipulationen und somit optimalen Schutz gegen Lockpicking-Versuche. Mit Scala habe der Hersteller ein skalierbares Zutrittskontrollsystem entwickelt, das sich stufenlos anpasse. Es erlaube die Einbindung von über 2.000 Türen. Mit ESA500 zeige das Unternehmen eine kabellose Stand Alone-Lösung für private und innerbetriebliche Bereiche wie Lager- und Personalräume.

Sensortechnologie

Professor Harald Giessens habe zusammen mit seinen Kollegen ein **exklusives Linsensystem** entwickelt, quasi elektronische Augen, die scharf seien wie Adleraugen und kleiner als ein Sandkorn – und verbunden mit dem Internet, berichtet die FAZ am 2. März. Das System, in eine Brille implantiert, die mit einem Wi-Fi-Transmitter ausgestattet ist, wäre eine mögliche Anwendung für dieses Linsensystem. Das „Adlerauge" erkenne eine Maus aus drei Kilometern Höhe, weil es im Bereich des schärfsten Sehens extrem viele Sehzellen habe und weil außerdem eine zweite Fovea am Augenrand für scharfe Sicht nach den Seiten sorge. Das ganze Linsensystem werde mit einem 3-D-Drucker hergestellt. Natürlich habe man schon eine Minidrohne gekauft, um dort das Sensorsystem einzubauen Das weite Feld der Spionage wäre eine Einsatzmöglichkeit. Künftig könnten Objekte in der Größe einer Biene oder einer Fliege alles Mögliche ausspionieren.

Sicherheitsgewerbe

Wie die neue DIN 77200-1 den **Versicherungsmarkt für Sicherheitsunternehmen** verändere, thematisiert Bernd M. Schäfer, ATLAS, in der Ausgabe 1-2017 des DSD, S. 47/48. Zum einen werde für Unternehmen viel klarer als bisher erkennbar sein, welchen Schutz sie warum bieten müssen, und zum anderen würden die Mogelpackungen einer ganzen Reihe von Versicherern nicht mehr marktgängig sein. Einer Million Euro für Personenschäden und 250.000 Euro für

Sachschäden der Bewachungsverordnung stehen nach neuem Standard 2,5 Mio. Euro pauschal für Personen- und sonstige Schäden gegenüber. Schlüsselverluste sollten nun mit 250.000 Euro nachgewiesen werden. Bewachte Sachen würden nun mit wenigstens 250.000 Euro versichert sein. Dass viele Versicherer den zunächst in Millionenhöhe gebotenen Versicherungsschutz für Sachschäden durch die Einführung eines Sublimits für Beschädigung und Vernichtung bewachter Sachen auf Beträge von nur 260.000 Euro einschränken, sei zwar in allen Verträgen und Versicherungsbestätigungen nachlesbar, werde aber mangels Abfrage in Ausschreibungen von niemandem hinterfragt. Der neue Standard schreibe vor, dass Beschädigung und Vernichtung bewachter Sachen eindeutig zu den Sachschäden zu zählen sind und dass deshalb auch hierfür 2,5 Mio. Euro als Versicherungssumme zur Anwendung kommen müssen. Auch bei einem Diebstahl durch einen Mitarbeiter gelte die Vertragsdeckungssumme für Abhandenkommen bewachter Sachen oder bei Brandstiftung in Höhe von 2,5 Mio. Euro. Durch die Verwendung eines standardisierten Formulars gebe es nun einen Paradigmenwechsel: Nicht, was der Versicherer bestätigt sei entscheidend, sondern das, was der Auftraggeber abfragt. Wenn Versicherer ein Sicherheitsunternehmen versichern, müssten sie den Mindeststandard bieten und könnten nicht von sich aus den Deckungsumfang willkürlich einschränken. Zum Versicherungsschutz für die Bewachung von Landfahrzeugen gebe es im neuen Standard leider keine Vorgabe.

Sicherheitsmarkt

Der **Home-Security-Markt** sei noch ein schlafender Riese, ergebe die Marktstudie „Home Security 2016" von Bbw Marketing (GIT, Ausgabe 3-2017, S. 56–59). Eine Verbraucherbefragung von Home Security 2015 habe bei elektronischen Sicherheitsprodukten folgende Prioritäten ergeben: Funktionalität (66,5 Prozent), Robustheit der Produkte (44,9 Prozent), niedriger Preis mit ausreichender Qualität (40,7 Prozent), Fachberatung (39,4 Prozent), Angebot hochwertiger qualitativer Produkte (38 Prozent). Die geringsten Prioritäten wiesen Warenpräsentation (2,3 Prozent) und hoher Preis mit Superqualität (3,2 Prozent) auf. Ein Ass im Ärmel der Home-Security-Wirtschaft sei aktuell die Brandmeldetechnik, die mit knapp 1,7 Mrd. Euro nicht nur einen sehr hohen Umsatz aufweise, sondern auch mit zweistelligen Zuwachsraten aufwarten könne. Auch bei anderen Produktbereichen spreche nichts dafür, dass die überaus positive Entwicklung in den Produktfeldern von Home Security ein abruptes Ende nehmen werde.

Openpr.com meldet am 21. März, nach einer Prognose von Stratistics MRC werde der Weltmarkt für Fingerabdruck-Sensoren auf 2,96 Billionen US-Dollar für 2015 berechnet und erwartet, dass er 2022 auf 8,98 Billionen US-Dollar steigt. Ursächlich sei die wachsende Nachfrage für Sicherheitskontrollen auf Flughäfen und schnelles Wachstum an elektronischen Geräten.

Spionage

Die **neueste Enthüllung von Wikileaks** offenbare, dass die Zukunftsszenarien von Datenspezialisten längst Gegenwart sind, schreibt die FAZ am 9 März. Jedes nur erdenkliche digitale Gerät solle potenziell als Abhör- und Überwachungsvehikel genutzt werden können. Das Internet der Dinge mit denkenden Kühlschränken, mit vernetzten Thermostaten, Stromzählern, Fernsehern, Aktiv-Lautsprechern, vor allem aber mit Kommunikationsboxen wie Amazons Echo werde zu einem gigantischen Netz für Überwachung, Spionage, Sabotage – einsetzbar bis hin zur gezielten Tötung.

Mehr als 80 Prozent der Digitalkommunikation seien schon verschlüsselt. Google, WhatsApp und Spezialdienste wie Signal und Telegram hätten Dutzende von Millionen in die Überwachungssicherheit von Mails und Messages investiert. Folgerichtig seien die Dienste ausgewichen und bemächtigten sich der Endgeräte – ein Weg, der mittlerweile in Ländern wie Großbritannien gesetzlich sanktioniert worden sei.

Die EU-Kommission habe 2016 die **Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Informationen** erlassen, die bis zum 9. Juni 2018 die EU-Mitgliedstaaten umsetzen müssten, berichten Udo Kornheimer und Ramon Glassi, Rechtsanwälte bei Schalast, in der FAZ am 15. März. Nicht nur Patente, Marken-, Urheber- und sonstige gewerbliche Schutzrechte seien zentrale Unternehmenswerte. Oft seien es auch Kundenlisten, Kalkulationen, Marketing- und Vertriebsstrategien, geplante Innovationen oder Rezepturen. Die Richtlinie läute einen Paradigmenwechsel ein: Geschäftsgeheimnisse erhielten erweiterten Schutz, der jedoch nur greife, wenn Unternehmen ihre Geheimnisse aktiv schützen. Auch die Sperrung von USB-Anschlüssen, die Installation von Kopierschutz, Schulungen, Geheimhaltungsvereinbarungen und Wettbewerbsverbote sowie ein Compliance-Management könnten Schutzmaßnahmen sein. Eine Besonderheit enthalte die Richtlinie in Artikel 3: Rechtmäßig handelt, wer ein Geschäftsgeheimnis durch sogenanntes Reverse Engineering erlangt – also durch eine Nachkonstruktion durch eingehende Produktanalyse. Dies gelte nur dann nicht, wenn der Erwerber eines Produkts vom Hersteller vertraglichen Beschränkungen unterworfen wird. Mit den angemessenen Schutzmaßnahmen entstehe nach der Richtlinie quasi ein gewerbliches Schutzrecht. Denn sie sehe einen umfangreichen Maßnahmenkatalog zur Durchsetzung des Geheimnisschutzes vor.

Sprengstoff

In einem Beitrag in der Zeitschrift CRISIS PREVENTION stellen Dominik Wild von der Hochschule Bonn-Rhein-Sieg, Lukas Pschyklenk, Cathrin Theiß und Gerhard Holl ein neuartiges Konzept zur Detektion von verborgenen Explosiv- und Gefahrstoffen vor, zum Beispiel in verlassenen Gepäckstücken an öffentlichen Orten. Ein mobiles, intelligentes und sensorgesteuertes Laserbohrverfahren sei das Kernelement der aktuellen Forschung des vom BMBF geförderten Projekts „Lasertechniken zur Beurteilung von Gefahrenlagen mit Objekten mit chemischen und explosiven Gefahrstoffen **(LAGEF)**". Zunächst werde mittels eines gepulsten Lasersystems die äußere Umhüllung bzw. Verpackung des Objektes durchdrungen. Daraufhin finde die Wechselwirkung zwischen Laserstrahlung und dem eigentlichen Zielstoff statt, bei dem ein Austrag von Material erfolgt. Der zu identifizierende Stoff werde anschließend durch das Probenahmesystem aufgenommen und könne mit verschiedenen chemischen Detektoren untersucht werden. Die Energieversorgung des Lasers könne über eine Glasfaser erfolgen, wodurch das System in größerer Distanz von der Bedien- und Steuereinheit einsetzbar sei. Die Anwendung der LAGEF-Technologie sehe vor, dass im Vorfeld eine Analyse des Bildes vom Objektinneren durch z. B. Röntgentechnik erfolgt. Im Verdachtsfall lasse sich das Laserbohrverfahren dann gezielt an der richtigen Stelle der USBV als Verifikationssensor einsetzen. Der Einsatz der Technik sei für die Anwendung auf ferngelenkten Roboterplattformen vorgesehen. Im Hinblick auf eine robuste Einsatzfähigkeit solle das System bedienungsfreundlich aufgebaut sein und selbstständig den Bohr- und Probenahmeprozess steuern und überwachen. Anschließend kehre das Robotersystem mit den sichergestellten Proben zum Bediener zurück.

Tunnelsicherheit

Edi Lehmann, Siemens Building Technologies, behandelt in der Ausgabe 1-2017 der Zeitschrift Sicherheitsforum, S. 42/43, Tunnelsicherheit. In der Schweiz würden erstmals Videokameras mit Radar kombiniert. Vor allem im Portalbereich eines Tunnels könnten unterschiedliche Wetterbedingungen für eine erschwerte Detektion per Video sorgen. Siemens Schweiz habe nun eine Lösung entwickelt, die das intelligente Videosystem „Tunnel Automatic Incident Detection (AID)" mit Radar kombiniert. Der Radar übernehme die Detektionsfunktion, die Videokamera die visuelle Überprüfung. Denn im Ernstfall müsse es schnell gehen.

Unternehmenssicherheit

Im März 2017 hat der Bundesverband ASW zusammen mit dem BfV und dem BSI als Baustein zum Wirtschaftsgrundschutz einen Leitfaden zum Sicherheitsvorfallmanagement herausgegeben. Beschrieben wird ein Verfahren zum zeitnahen Erkennen und angemessener Reaktion auf Vorfälle, um die schutzwürdigen Werte eines Unternehmens abzusichern. Aufgrund der Vielfältigkeit besitze das **Sicherheitsvorfallmanagement** oftmals Schnittstellen zu diversen anderen Managementsystemen, z. B. Notfallmanagement und Krisenmanagement. Das Sicherheitsvorfallmanagement stelle das steuernde Bindeglied zwischen dem Regelbetrieb und dem Reaktionsmanagement, bestehend aus Vorfall-, erweitertem Vorfall-, Notfall- und Krisenmanagement, zur Verfügung.

Der DSD weist in der Ausgabe 1-2017 auf folgende Analysen und Hilfestellungen zum **Wirtschaftsschutz** hin:

- Wirtschaftsgrundschutz-Handbuch (BfV/BSI/ASW, www.wirtschaftsschutz.info)
- Soziale Netzwerke – Sicherheitsrisiko für Unternehmen? (CAZ, www.verfassungsschutz.bayern.de)
- Analysebericht Radikalisierungshintergründe und -verläufe (BKA/BfV/HKE, www.wirtschaftsschutz.info)
- IT-Sicherheitstrends 2017 (NIFIS, www.nifis.de)

Videoüberwachung

Mit **Kameranetzwerken** befasst sich Dipl. Ing. FH Rudolf Rohr, Barox Kommunikation GmbH, auf S. 44 der Zeitschrift PROTECTOR, Ausgabe 3-2017. Netzwerke, speziell im Videobereich, würden immer komplexer. Dazu komme die Verbindung von Daten mit PoE (Power over Ethernet), welche nochmals mehr Parameter in die Anlagen bringen. Netzwerke sollten ohne einen Stab von IT-Leuten im Hintergrund aufgesetzt und betrieben werden können. Gleichzeitig sollten sie aus der Ferne analysiert werden können. Im Umkehrschluss bedeute dies, dass Switche mit einer Sensorik mit Analysefunktionalitäten ausgestattet werden müssten. Dies erfolge mit einem speziell für Video optimierten Chipsatz. Ziel sei es, bis zu 120 Watt über Datenkabel zu bringen. Somit könnten Laptops und Bildschirme direkt bequem mit einem Kabel versorgt werden. Mit den Normen IEEE 802.3af und at seien Sicherheitsstandards eingeführt worden. Die Sicherheitsbestimmungen seien dafür gedacht, die beteiligten Geräte – Energieversorger und Energieverbraucher – zu schützen, wenn z. B. ein Kurzschluss beim Verbraucher vorliege. Dies bedeute zwingend, dass Energieversorger und Energieverbraucher miteinander kommunizieren könnten.

Die **Problematik des Datenaufkommens** bei Videolösungen thematisiert PROTECTOR in der Ausgabe 3-2017, S. 45. Synology

habe es sich als Netzwerk- und Datenspezialist zur Aufgabe gemacht, auch die Verwendung und Verarbeitung der auftretenden Bildmaterialien zu optimieren und somit intelligenter zu gestalten. Die Surveillance-Station des Herstellers biete aus diesem Grund verschiedene Funktionen, die die benötigte Festplattenkapazität der Aufzeichnungen wie auch die erforderliche Bandbreite zur Live-Ansicht den individuellen Anforderungen jedes Projekts anpasst und somit minimiert. In der Live-Ansicht ließen sich die Kamerabilder in einer konfigurierten Auflösung und Bildwiederholrate anzeigen. Erst beim Auslösen entsprechender Alarme würden die hochauflösenden Bildmaterialien aufgezeichnet und der Speicherplatz somit effizient genutzt. Zu den neuen Funktionen der Surveillance Station 8.0 zählten: Surveillance Station Client, Axis ACAP-Integration und CMS N+M Failover.

Für **mehr Videoüberwachung im öffentlichen Raum** plädiert Manfred Buhl, Securitas Deutschland, in der Ausgabe 3-2017 der Zeitschrift GIT, S. 20–22. Sie habe einen dreifachen Effekt: höheres Sicherheitsgefühl, mögliche erweiterte Öffentlichkeitsfahndung und bessere Tataufklärung. Der Bundesinnenminister fordere zu Recht eine verstärkte Videoüberwachung durch Hausrechtsinhaber an öffentlich begehbaren Plätzen, zumal sich islamistische Terroristen „weiche Ziele" suchen und diese am leichtesten in öffentlich zugänglichen Räumen finden. Der Autor beschreibt die für den öffentlichen Raum geeignete Kameratechnik, die Videoanalysetechnik und speziell die Problematik der Gesichtserkennung. Securitas biete im Rahmen ganzheitlicher Sicherheitslösungen Videoüberwachungssysteme an, die entsprechend den Kundenwünschen, dem Überwachungszweck und den Umgebungsbedingungen die geeignetsten Kameratypen mit intelligenter Detektions- und Bildanalysesoftware umfassen. Durch die Verknüpfung von Video- und Audiotechnik sei im Alarmfall eine sofortige Einwirkung auf den Ereignisbereich möglich.

Wie GIT in seiner Ausgabe 3-2017, S. 23, berichtet, führt UTC Fire & Security Deutschland die **Truvision Netzwerkrekorderserie TVN22** mit dem neuen H.265 Kompressionsstandard ein. H.265 reduziere die Datengröße um bis zu 50 Prozent im Vergleich zu H.264, was gleichermaßen eine höhere Bandbreite und auch eine bessere Aufzeichnungsqualität bei geringerem Speicherbedarf bedeute. Der TVN22-Rekorder könne mit beiden Kompressionsverfahren arbeiten, sodass die volle Kompatibilität zu den H.264-Kameras garantiert sei.

Kameras mit automatischer Kennzeichenerkennung von Dahua stellt GIT in der Ausgabe 3-2017, S. 45, vor. Nach der Einfahrt auf einen Parkplatz brauche der Fahrer nun nicht mehr auszusteigen und einen Parkschein oder eine Karte zu lösen, um die Parkdauer und -gebühr zu berechnen. Stattdessen könne jeder Wagen direkt einfahren, denn eine 2MP-LPR-Kamera zeichne Parkdauer und Kfz-Kennzeichen automatisch auf. Anschließend ermittle die Spot-Detection-Kamera, die drei oder sechs Parkplätze simultan erfassen könne, die Parkplatzverfügbarkeit und leite die Daten an den Informationsanzeiger weiter, der die verfügbare Platzzahl für verschiedene Zonen in unterschiedlichen Farben angibt. Die Lösung des Herstellers biete nach eigenen Angaben eine Erfassungsrate von bis zu 98 Prozent und eine Genauigkeit von bis zu 95 Prozent. Außerdem biete sie Funktionen wie Kennzeichensuche und Videoverknüpfung, White List/Black List, Verbindung mit Schrankensystemen und so weiter.

Intelligente IP Video- und Thermaltechnologie thematisiert GIT in der Ausgabe 3-2017, S. 47/48. Aus sicherheitstechnischer Sicht sei ein System ideal, bei dem möglichst viel Intelligenz in jeder einzelnen Kamera steckt, und das somit ohne einen zentralen Server zur Bildverarbeitung und -analyse auskommt. Eine intelligente Kamera trete nur dann in Aktion, wenn es wirklich darauf

ankommt. Dringt jemand zum Beispiel innerhalb eines definierten Zeitfensters auf das Betriebsgelände ein, starte die Kamera automatisch eine Lautsprecheransage und schalte eine Zusatzbeleuchtung ein. Erst mit einer gewissen Intelligenz des Kamerasystems, einer intelligenten Software zur Bewegungserkennung und einem aktiven Alarmmanagement, lasse sich eine leistungsfähige, präventive Sicherheitslösung aufbauen. Mit Hilfe von Dualkameras, die mit einem optischen Sensor und mit einem Thermalsensor ausgestattet sind, könnten sich bewegende Objekte auch anhand ihrer Wärmestrahlung selbst bei absoluter Dunkelheit über lange Distanzen sicher erkannt werden. Das Wärmebild zeige ein Temperaturprofil, das Personen nicht im Detail erkennen lässt. Video- und Thermaltechnologie werde von Unternehmen zunehmend auch zur Erfassung von Gefahrensituationen im Produktionsprozess genutzt. In Produktionsbetrieben seien robuste, qualitativ hochwertige Outdoor-Kameras gefragt. Dualkameras könnten zudem temperaturkritische Prozesse überwachen. Auch diese Anwendung zur Prävention von Schäden durch Überhitzung oder Brand mache erst die Intelligenz des Kamerasystems möglich. Bei Über- oder Unterschreiten von definierten Temperaturgrenzen sowie bei einem schnellen Temperaturanstieg erfolge eine automatische Alarmierung. Ein intelligentes Kamerasystem verursache geringere Gesamtkosten als eine herkömmliche Videolösung. Denn wenn die Bildverarbeitung und -analyse auf der Kamera selbst sowie die Aufzeichnung auf einem Netzwerkspeicher nicht permanent, sondern ereignisgesteuert erfolgt und die Kamera zudem bei Netzwerkausfall Daten selbst speichert, seien die Anforderungen an die erforderliche Bandbreite und die weitere IT-Infrastruktur gering.

Nach einer Meldung von golem.de können Überwachungskameras des Smarthome-Herstellers Nest in ihrer Funktion gezielt gestört werden. Für ein bis zwei Minuten gebe es dann keinerlei Aufnahmen – genug Zeit, um unentdeckt in die Wohnung einzusteigen. Die Dropcam und die Dropcam Pro des zum Konzern Alphabet gehörenden Smarthome-Herstellers Nest könnten offenbar von Angreifern ohne Authentifizierung deaktiviert werden. Sicherheitsforscher hätten in der Firmware mit der Versionsnummer 5.2.1 drei Sicherheitslücken gefunden. Nest habe angekündigt, ein Update zu verteilen.

Wettbewerbsregister

Mit Hilfe eines zentralen Wettbewerbsregisters will die Bundesregierung kriminelle Unternehmen künftig von öffentlichen Aufträgen ausschließen, meldet die FAZ am 30. März. Diese „Schwarze Liste" solle von 2019 an dazu beitragen, Korruption und andere Arten der Wirtschaftskriminalität einzudämmen. Das Vergaberecht regele den Ausschluss solcher Unternehmen schon heute. In einigen Bundesländern existierten Korruptionsregister, sie folgten aber sehr unterschiedlichen Regeln. Das **zentrale Wettbewerbsregister,** das beim Bundeskartellamt geführt wird, solle nun Abhilfe schaffen. Nach den Gesetzesplänen müsse die öffentliche Hand von einem Auftragswert von 30.000 Euro an vor Erteilung des Zuschlags elektronisch abfragen, ob das Unternehmen im Register geführt ist. Nach drei bis fünf Jahren würden Eintragungen gelöscht. Die Unternehmen hätten darüber hinaus die Möglichkeit, eine vorzeitige Löschung zu erreichen, wenn sie sich wieder als zuverlässig erweisen. Dazu müssten sie personelle und organisatorische Maßnahmen treffen, die weitere Rechtsverstöße verhindern.

Wohnungseinbruch

Der **Rückgang** der Anzahl an Wohnungseinbruchdiebstahls-Fällen sei nach Überzeugung von Norbert Schaaf, BHE Bundesverband

Sicherheitstechnik, auch auf die höheren Investitionen in Sicherheitsmaßnahmen zurückzuführen (FAZ am 17. März). Er schätze, dass vier Prozent der Haushalte mit Alarmanlagen ausgestattet sind. In Frankreich seien es zehn Prozent, in den USA etwa 20 Prozent. Elektronische Überwachungssysteme seien auf dem Vormarsch, wichtigster Einbruchschutz und größter Markt bleibe aber die weite Palette mechanischer Schutzeinrichtungen: einbruchhemmende Fenster und Türen, Verriegelungen mit Pilzkopfzapfen, Sicherheitsbeschläge, abschließbare Fensterschlösser, Riegel, Zylinderschlösser, Schließbleche, Rollläden und Gitter. Die Erfahrung zeige: Wenn ein Einbrecher lange braucht, gibt er auf. Trotz Lobbyarbeit sei es der Sicherheitsbranche bislang nicht gelungen, Mindestanforderungen für Einbruchschutz in die Bundesbauordnung zu bringen.

Zutrittskontrolle

Dr. Jörg Wissdorf, Interflex Datensysteme GmbH, befasst sich im Sicherheitsforum, Ausgabe 1-2017, S. 62, mit **„Zutritt 5.0"**. Im Hinblick auf Industrie 4.0 sollten Anbieter für Zutrittslösungen drei Kriterien erfüllen: den ganzheitlichen Lösungsansatz, die Vernetzbarkeit der Komponenten und die Möglichkeit für den Anwender, selbst im Sinne von Industrie 4.0 zu agieren. Bei der Vernetzung von Software und Produktionsabläufen seien eine globale Zutrittskontrolle, flexible Arbeitszeitmodelle sowie eine effiziente Personaleinsatzplanung erforderlich. Beim Thema „Zutritt 5.0" gingen Unternehmen noch einen Schritt weiter. Zukünftig würden Zutrittslösungen nicht mehr als Schleuse wahrgenommen, sondern als flüssige Interaktion von Maschinen und Menschen. Die Lösungen würden zunehmend intelligenter miteinander vernetzt.

Kabellose Zutrittssysteme thematisiert PROTECTOR in der Ausgabe 3-2017, S. 28/29. Die optimale Lösung für den elektronischen Zutritt kombiniere mechatronische und mechanische Komponenten. Online-Systeme seien permanent vernetzt; Administratoren verwalteten und vergeben Berechtigungen zentral. Offline-Systeme seien dagegen wesentlich einfacher und kostengünstiger zu installieren. Sie erforderten bei der Vergabe neuer Berechtigungen jedoch deutlich mehr Aufwand. In naher Zukunft werde eine Statusüberwachung der Türöffnung per App möglich sein, dann erfülle das System nahezu alle Funktionen einer Online-Lösung. „eAccess" bestehe zum einen aus bewährten mechanischen Elementen. Zum anderen erleichterten Technologien wie Funk und RFID das Programmieren und die tägliche Benutzung. Neue Kabel müssten nur sehr selten verlegt werden, etwa bei Motorschlössern. Da Berechtigungen in der Tür und nicht im Chip gespeichert werden, bleibe das System auch in der Anwendung mit vielen Nutzern und in großen Gebäuden flexibel. Dank einer Funk-Onlinelösung kämen Anwender in den Genuss fast aller Funktionen einer verkabelten Online-Lösung. Mit einem Repeater könnten bis zu 20 Türen in rund 30 Metern Entfernung vom Funkstick erreicht werden, sodass auch größere Gebäude und mehrere Etagen einfach per Funk verwaltet werden könnten. Dank einer Triple-DES-Verschlüsselung sei der Sicherheitsfaktor besonders hoch.

Eine **Marktübersicht** über 207 Systeme von Lesegeräten für Zutrittskontrollsysteme von 98 Anbietern enthält Ausgabe 3-2017 der Zeitschrift PROTECTOR (S. 30/31). Abgefragte Kriterien sind unter anderen: Display, Tastatur, optische und akustische Signalisierung, maximale Anschlussdistanz, Netzausfall-Datenerhalt, Speichergröße, Schnittstellen, Offline-Fähigkeit, Türsteuerung, Datenübertragung, Identifikationsmerkmal, physische Sicherung von Gehäuse und Datenleitung, Kartentechnologie, Lesedistanz, biometrische Merkmale.

Impressum

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

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

Herausgeber:
Manfred Buhl, Vorsitzender der Geschäftsführung, Düsseldorf

Verantwortlicher Redakteur:
Bernd Weiler, Leiter Kommunikation und Marketing

Beratender Redakteur:
Reinhard Rupprecht, Bonn

focus.securitas.de

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

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

E-Mail: info@securitas.de