Focus on Security

Ausgabe 06, Juni 2017

SECURITAS

Inhalt

Anschläge

In den Morgenstunden des 5. Mai wurden nach IBWS-Informationen vom 11. Mai auf dem Hof eines fischverarbeitenden Betriebes in Hamburg drei Kleintransporter und zwei Pkw durch Brandanschläge beschädigt. Die Fahrzeuge trugen ein Firmenlogo. Dazu gebe es ein Selbstbezichtigungsschreiben von „g20fischen". Darin heiße es: „G20 anzugreifen bedeutet auch, die Nutznießer/innen der Vernichtung weltweiter Fischvorkommen anzugreifen."

Brandschutz

Richtig ausgeführte **Holzkonstruktionen** sind bei einem Brand sehr robust, schreibt Holzbauingenieur David Sauser, Gebäudeversicherung Bern, in der Ausgabe 2-2017 der Zeitschrift Sicherheitsforum, S. 23–25. Die Ausführung einer Konstruktion habe einen wesentlich größeren Einfluss auf das Brandverhalten eines Gebäudes als die Brennbarkeit des verwendeten Baustoffs. Grundsätzlich gelte das Schutzziel bei Holzfassaden: Ein Brand darf sich höchstens über zwei Stockwerke oberhalb des Brandgeschosses ausbreiten, bevor die Feuerwehr eintrifft. Die Fassade müsse horizontal konstruktiv unterteilt werden. Der Autor erläutert notwendige Maßnahmen je nach Fassadentyp: Lochfassade, Fensterbandfassade, Schindelfassade. Anstelle von Schürzen oder Abschottungen könnten auch durchgehende Balkonbänder als Brandschutzmaßnahme wirken.

Mit der **Wartung von Rauchmeldern mit Echtheitsprüfung** befasst sich die Redakteurin Iris Gehard in der Ausgabe 2-2017 der Zeitschrift Sicherheitsforum, S. 64/65. Um bei der Überprüfung möglichst schnell und eindeutig zu erkennen, ob es sich um einen Originalrauchmelder handelt und dieser an der richtigen Stelle verbaut ist, könne eine Sicherheitsmarkierung angebracht werden: Das Label bestehe aus einer Tiefeneffektfolie, einer individuellen Nummerierung, einer Markierung mit der fälschungssicheren Substanz sowie einem Near-Frequence-Chip (NFC). Die am Rauchwarnmelder angebrachte Sicherheitsmarkierung lasse sich auch mit einem NFC-fähigen Smartphone auslesen.

Cloud Computing

Die Cloud ist in Deutschland angekommen, titelt die FAZ am 8. Mai. Betreiber von Rechenzentren investierten allein am Standort Frankfurt eine halbe Milliarde Euro. Hinein komme man in diese wie **Hochsicherheitstrakte** bewachten Gebäude kaum. Ohne Anmeldung ohnehin nicht, nach der Personalausweiskontrolle müsse noch eine Schleuse durchquert werden, die mit einer PIN-Nummer und einem Handrückenscanner gesichert ist. Denn der Rücken der Hand sei nicht so leicht kopierbar wie die Handinnenfläche. Im Innern der Rechenzentren seien die einzelnen Unternehmen durch abgeschlossene Käfige voneinander getrennt. Will jemand mit seiner Zugangskarte in einen Bereich, in dem er nichts zu suchen hat, gehe sofort eine Kamera an und ein Alarm los. Manch einer sichere seine Daten noch mit einem sogenannten Venenscanner: Der messe die Durchblutung, und so könnten Kriminelle selbst dann nicht eindringen, wenn sie einem Mitarbeiter die Hand abhacken würden, um den Handrückenscanner zu überlisten.

Digitale Gesellschaft zwischen Risikobereitschaft und Sicherheitsbedürfnis lautete der Titel des **15. Deutschen Sicherheitskongresses**, der vom 16. bis 18. Mai in Bonn

stattfand. Unter dem Aspekt des Cloud Computing werden folgende Referate hervorgehoben: Prof. Dr. Georg Borges, Universität des Saarlandes, befasst sich mit der **Datenschutz-Zertifizierung für Cloud-Dienste** (S. 23–38). Das Datenschutzrecht stelle den Nutzer von Cloud-Diensten vor eine schwierige Herausforderung. Gemäß § 11 Abs. 2 BDSG müsse der Cloud-Nutzer die organisatorischen und technischen Maßnahmen des Cloud-Anbieters zur IT-Sicherheit überprüfen. Diese Prüfung könne durch ein Datenschutz-Zertifikat entscheidend erleichtert werden. Dies gelte jedoch nur, wenn der zugrundeliegende Prüfstandard die gesetzlichen Anforderungen abdeckt. Die Zertifizierung nach dem Prüfstandard „Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP)" – Version 1.0 – und die begleitenden Konzepte setzen die Anforderungen an die Datenschutz-Zertifizierung in praxistauglicher Weise um. Thomas Niessen, Kompetenznetzwerk Trusted Cloud e. V. (S. 87–94), beschreibt Mindestanforderungen für **vertrauenswürdiges Cloud Computing**. Das Label **Trusted Cloud** für vertrauenswürdige Cloud Services sei die Umsetzung eines der Ergebnisse des 2015 abgeschlossenen Technologieprogramms Trusted Cloud des BMWi. Mit dem Label sollen Vertrauen und Transparenz im Hinblick auf Cloud-Angebote geschaffen werden. Die rund 160 Trusted-Cloud-Kriterien für Cloud Services nähmen insbesondere Aspekte wie Sicherheit und Datenschutz, Transparenz und Qualität sowie Rechtskonformität in den Blick. Robin Fa, Universität Siegen stellt zusammen mit Studierenden am Lehrstuhl für Digitale Kommunikationssysteme ein Sicherheitskonzept für das **Fog-Computing** vor (S. 95–108). Beim Cloud Computing würden aufwendige Berechnungen und große Datenmengen auf externe Recheneinheiten ausgelagert. Im Gegensatz dazu würden die Daten beim Fog-Computing von vielen kleinen Quellen wie Sensoren erfasst und dann lokal aggregiert und verarbeitet. So könnten zum einen die Datenmengen reduziert und zum anderen Informationen durch die lokale Vorverarbeitung dort genutzt werden, wo sie erforderlich sind. Im Rahmen der Arbeit werde eine sichere Architektur für das Fog-Computing entworfen und deren prototypische Umsetzung vorgestellt. Außerdem wird auf die für den Anwender transparente Integration der Sicherheitsmechanismen, die eine fehlerfreie Verwendung der kryptografischen Verfahren sicherstellt, eingegangen.

Compliance

Im ASW-Newsletter vom 12. Mai wird auf den **Control Risks Compliance Survey 2017** mit folgenden zentralen Ergebnissen hingewiesen: Die Compliancefunktionen großer Unternehmen (über 10.000 Mitarbeiter) seien unterbesetzt. Die Compliance-Teams von 28 Prozent der großen Unternehmen bestünden aus fünf oder weniger Personen. Nur 27 Prozent der für Compliance zuständigen Führungskräfte nähmen an allen Vorstandssitzungen teil. Compliance-Beauftragten stünden ungenutzte technologische Möglichkeiten zur Verfügung, um effektiver arbeiten zu können. Sie müssten aktiver agieren. Zwei Drittel verließen sich auf Whistleblowing, anstatt Prüfungen zur Aufdeckung von Korruptions- und Fraud-Fällen durchzuführen. Compliance-Richtlinien weltweit tätiger Unternehmen seien uneinheitlich.

Die **Entlassung von CEOs wegen unethischen Verhaltens** nehme deutlich zu, berichtet die FAZ am 15. Mai. 2016 seien insgesamt 18 Vorstandsvorsitzende der 2.500 größten börsennotierten Unternehmen der Welt wegen unethischen Verhaltens

zurückgetreten. Zu diesem Ergebnis komme eine Studie der Unternehmensberatung Strategy&. Während in den Jahren von 2007 bis 2011 nur 52 (oder 3,9 Prozent) aller Chefwechsel in den 2.500 Konzernen durch unethische Fehltritte ausgelöst worden seien, seien es 2012 bis 2016 insgesamt 86 (oder 5,3 Prozent) gewesen. Zu den ethischen Verfehlungen zähle die Studie etwa Betrug, Bestechung, Insiderhandel, das Auslösen von Umweltkatastrophen, gefälschte Lebensläufe oder sexuelle Indiskretionen. Früher hätten größere Skandale nur selten zur Entlassung eines Konzernchefs geführt. Für die grundlegende Änderung gebe es mehrere Gründe. Die Politik habe auf Druck der Öffentlichkeit viele Gesetze verschärft. Gefängnisstrafen für Manager hätten zugenommen. Aber auch die finanziellen Strafen für Unternehmen hätten sich drastisch erhöht. Durch die digitale Kommunikation sei außerdem die Wahrscheinlichkeit des „Erwischtwerdens" deutlich gestiegen. Nicht zuletzt habe mit dem Aufkommen des Internets, von Online-Finanznachrichten und der sozialen Netzwerke der mediale Druck stark zugenommen. Und am 27. Mai ergänzt die FAZ: Vor allem bei systematischer Manipulation seien Spitzenmanager entweder beteiligt oder duldeten das Vorgehen.

Mehr als drohende Strafen zählten für Mitarbeiter Anerkennung und Lob für ihre Erfolge im Unternehmen sowie das Gefühl, zum innersten Kreis zu gehören. Zudem fehle es in vielen Fällen an Unrechtsbewusstsein. Klaus Moosmayer, Chief Compliance Officer von Siemens: „Mitarbeiter lassen sich mit Compliance nicht kontrollieren, sie müssen dafür gewonnen werden", vor allem mit dem Argument, dass ethisch korrektes Verhalten einen wirtschaftlichen Mehrwert bringt und Compliance nicht Gegner, sondern Treiber des Geschäftserfolges ist. Mit einer festgeschriebenen Unternehmensethik, einer Digitalisierung der Abläufe und einer Whistleblower-Hotline allein sei es keineswegs getan. Vielmehr müsse Compliance auch die innere Haltung der Manager bestimmen. Um für saubere Geschäftspraktiken in politisch schwierigen Ländern zu werben, würden viele Unternehmen auf branchenübergreifende Aktionen wie etwa die internationale Initiative „Collective Action" setzen.

Mit **„Due Diligence" im Auslandsgeschäft** befasst sich Frank Schurgers, Integris International LLC., in der Mai-Ausgabe von PROTECTOR, S. 62/63. Due Diligence solle eher als ein wesentliches Instrument der Risikoerkennung und -bewertung in einem gesamtheitlichen Konzept verstanden werden, in dem neben Compliance und Rechtsabteilung auch die Unternehmenssicherheit einen wesentlichen Beitrag liefern könne. Nahezu alle Unternehmen, die im Ausland tätig sind, hätten schon negative Erfahrungen mit Geschäftspartnern gemacht und erhebliche Verluste erlitten, die bei einer sorgfältigen Due Diligence vor Geschäftsabschluss vermeidbar gewesen wären. Zielgerichtete Recherchen vor Ort von Experten, die die lokalen und nationalen Gegebenheiten im Detail kennen und nach Möglichkeit den Besuch der Geschäftsadressen eines potenziellen Partners einschließen, seien der beste Weg, relevante Fakten und Informationen für die konkrete Bewertung eines Geschäftsrisikos zu liefern. Gerade ein interdisziplinärer Ansatz, der neben kaufmännischen, rechtlichen und Compliance-Aspekten auch die Sicherheitsbelange im Sinne eines ganzheitlichen Risikomanagements in den Due-Diligence-Prozess integriert, könne einen wesentlichen Beitrag für die umfassende Bewertung und Minimierung von Geschäftsrisiken leisten.

Datenschutz

Das **Verhältnis von Informationssicherheit und Datenschutz** betrachten Bettina Weßelmann, Beraterin, und Dr. Johannes Wiele, Berater, in der Ausgabe 2-2017 der Fachzeitschrift <kes>, S. 48–55. Informationssicherheit und Datenschutz arbeiteten in zu vielen Organisationen nebeneinander her. Notwendig sei ein Schwenk hin zu einer Kommunikationskultur, die über abteilungsinterne Verständigung unter Gleichgesinnten hinaus immer auch den vollwertigen Austausch mit fachfremden Kollegen zum Ziel hat. Wie gut dies in einer Organisation gelingt, hänge oft auch von der jeweiligen Unternehmenskultur ab. Langfristig würde eine Weiterentwicklung der jeweiligen Ausbildungsgänge weiterhelfen, die Technikern mehr Einblicke in das Recht und Datenschützern eine intensivere Auseinandersetzung mit der Technik vermittelt.

Eine **Checkliste für die Datenschutz-Grundverordnung** (DS-GVO) stellt Dr. Niels Lepperhoff, Xamit Bewertungsgesellschaft mbH, in der Ausgabe 2-2017 der Zeitschrift <kes>, S. 56–59, vor. Zu den neuen Pflichten für IT-Führungskräfte, Administratoren und Sicherheitsbeauftragten gehörten unter anderem die Erstellung eines Sicherheitskonzepts, die dokumentierte Durchführung umfassender Wirksamkeitstests, die Meldung von Sicherheitsvorfällen an die Datenschutzaufsichtsbehörde, umfassende Informationspflichten gegenüber Mitarbeitern, Kunden und Lieferanten sowie die Pflicht, jederzeit die Einhaltung der Datenschutzgesetze mittels Dokumentation nachweisen zu können. Aufgelistet werden Fragen, mit denen ergründet werden soll, wie groß der eigene Handlungsbedarf im IT-Bereich noch ist.

Die Mehrheit der deutschen Unternehmen sei noch nicht ausreichend auf die **DS-GVO** vorbereitet, schreibt Martin Schindler am 19. Mai in silicon.de. Vor allem Organisationen, die komplexe Daten verarbeiten, hätten derzeit noch selten Antworten darauf, wie sie sicherstellen können, zu jeder Zeit angeben zu können, wo sich Daten befinden. Nur 59 Prozent der Unternehmen könnten sämtliche Daten zu einer Person schnell lokalisieren. Das aber sei eine wichtige Voraussetzung für die Gewährleistung des „Rechts auf Vergessenwerden", das die DS-GVO vorschreibe. Etwa ein Drittel der Unternehmen könne nicht garantieren, dass sie alle Kundendaten finden können. Unternehmen drohen bei Verstößen gegen die Verordnung vier Prozent des weltweiten Umsatzes, mindestens jedoch 20 Mio. Euro.

Datensicherheit

Die FAZ berichtet am 22. Mai, Forscher des Fraunhofer-Instituts für Experimentelles Software Engineering (IESE) hätten mit der **„Datennutzungskontrolle"** eine Lösung gefunden, nach der Daten ausgetauscht werden können, der Dateneigentümer aber über Möglichkeiten verfügt, deren Nutzung einzuschränken. Die Software-Umsetzung „Ind2uce" (Integrated Data Usage Control Enforcement) funktioniere mit Hilfe von Sicherheitsrichtlinien. In ihnen sei beschrieben, was erlaubt ist. Und vor allem, was nicht. Datenproduzenten und -besitzer könnten dabei ziemlich viel festlegen. Dazu gehöre, welche Daten wie oft gelesen, kopiert oder weitergeleitet werden dürfen; ob sie auf Smartphones gelesen werden könnten und ob dies nur auf dem Firmengelände oder auch auf öffentlichen Plätzen möglich sein soll. Prototypen dieser Sicherheitslösung würden gegenwärtig in der Industrie erprobt. Namen wolle man nicht nennen.

Sabine Sülberg, AKTEN-EX GmbH, erläutert in <kes> special vom Mai 2017, S. 35/36, wie Akten und **Datenträger sicher entsorgt** werden. Der Weg sei seit 2012 in Form der DIN 66399 „Büro- und Datentechnik – Vernichten von Datenträgern" festgelegt. Die Norm beschreibe drei Schutzklassen und sieben Sicherheitsstufen und setze diese in Beziehung zueinander. Ebenso unterscheide die Norm zwischen drei Prozessvarianten: Datenträgervernichtung durch die verantwortliche Stelle, Datenträgervernichtung vor Ort durch Dienstleister und extern durch Dienstleister. Weil es nur wenige Unternehmen gebe, die in der Lage seien, die höchsten Sicherheitsstandards bei der Vernichtung zu erfüllen, sei 2017 die Ultimate Shredding GmbH mit dem Ziel gegründet worden, eine nicht reproduzierbare Vernichtung von Akten und Datenträgern sowie eine individuelle Lösung anzubieten. Das System von MAX-XeGUARD vernichte alle Arten von digitalen Datenträgern wie Festplatten, CDs, DVDs, Disketten, Bänder PDAs, Mobiltelefone und elektronische Karten nach dem höchsten Stand der Technik.

Diebstahl

Innerhalb von drei Stunden habe eine Frau in einem Supermarkt in Hagen 156 Artikel gestohlen, meldet die FAZ am 2. Mai. Ein Beutestück nach dem anderen habe sie in ihrer Handtasche und einem Rollkoffer verschwinden lassen.

Der Staat ist untätig bei **Ladendieben**, titelt die FAZ am 31. Mai unter Bezugnahme auf scharfe Kritik des HDE an der Politik. Registriert würden laut HDE jährlich insgesamt knapp 400.000 Diebstähle bei einer geschätzten Dunkelziffer von 95 Prozent. Der jährliche Schaden liege bei zwei Mrd. Euro. Um sich zu schützen, investierten die Einzelhandelsunternehmen in Deutschland zudem etwa 1,2 Mrd. Euro in Maßnahmen gegen Diebstahl, Betrug und Raub. Die Zahl der schweren Diebstähle im Einzelhandel sei laut PKS seit 2013 kontinuierlich um fast 30 Prozent gestiegen. Der Einzelhandel erwarte strafrechtliche Rahmenbedingungen, die konsequente repressive Maßnahmen der Justiz und Polizei sicherstellen. Eine „Verschärfung des Strafrahmens" sei für „alle schweren Diebstahldelikte" geboten und nicht nur beim Einbruchdiebstahl. Der Verband fordere nun für schwere Diebstahldelikte nach § 244 Abs. 1 StGB eine Ahndung mit einer Freiheitsstrafe von mindestens einem Jahr. Damit würde die Einstellungspraxis der Staatsanwaltschaften und Gerichte ausgeschlossen. Weiterhin sollte „gewerbsmäßiger Diebstahl" in den Tatbestand aufgenommen werden. Auch die Möglichkeit zur Strafmilderung sollte komplett gestrichen werden.

Rund 1.500 gestohlene **Fahrräder** haben nach einem Bericht der FAZ vom 2. Mai Polizeibeamte in vier Lagerhallen und im Freien im Hamburger Stadtteil Rothenburgsort sichergestellt. Im Fokus stünden drei mutmaßliche Hehler, deren Aktionsradius sich auf ganz Norddeutschland erstreckte. Das Beutegut sollte in Kleintransportern nach Osteuropa gebracht werden. Nach den Zahlen der PKS 2016 würden in Deutschland täglich durchschnittlich fast 1.000 Fahrräder gestohlen. Aber nur jeder zweite oder dritte Fahrraddiebstahl komme zur Anzeige. Die Aufklärungsquote betrage nur knapp neun Prozent. Der durchschnittliche Schaden betrage laut Auskunft der Versicherer 520 Euro. Wichtigste Schutzmaßnahme sei der robuste Schutz durch Schlösser, hochwertige Bügelschlösser, Panzerkabel- oder Kettenschlösser, die möglichst Rahmen und Reifen umfassen. Und man sollte das Rad stets fest anketten.

Einbruch

GIT weist in der Ausgabe 5-2017, S. 8, darauf hin, dass die in der **NSL von Securitas** erfassten Einbruchszahlen 2016 deutschlandweit um rund 20 Prozent zurückgegangen sind. Die Zahl der versuchten Einbrüche steige dagegen tendenziell. Mit 31 Prozent würden Unternehmen des Lebensmittel- und Einzelhandels am häufigsten Opfer von Einbrüchen.

Golem.de berichtet am 29. Mai, dass bei allen Einbruchsdelikten die Polizei **Funkzellen- und Standortdaten** abfragen dürfe. Schon jetzt erlaube die im Oktober 2015 vom Bundestag beschlossene Vorratsdatenspeicherung eine Abfrage bei schwerem Bandendiebstahl. Die Polizei könne mit dem technischen Start der Vorratsdatenspeicherung am 1. Juli die Standortdaten konkreter Verdächtiger abrufen, wenn diese mutmaßlich einer Bande angehören.

Energiesicherheit

Das **Smart Meter-Gateway** stellt Dennis Laupichler, BSI, in der Ausgabe 2-2017 der Zeitschrift <kes>, S. 39/40, vor. Es ermögliche als zentrale Kommunikationsplattform in einem intelligenten Messsystem die sichere Umsetzung vielfältigster Anwendungsfälle und werde zum Treiber für Innovationen der Digitalisierung. Im Zusammenhang mit den technischen Standards des BSI schaffe das Gesetz zur Digitalisierung der Energiewende verbindliche Rahmenbedingungen für den sicheren und datenschutzkonformen Einsatz von intelligenten Messsystemen in verschiedenen Bereichen. Im Auftrag des BMWi entwickle das BSI daher Anforderungen an vertrauenswürdige Produktkomponenten (Smart-Meter-Gateway mit integriertem Sicherheitsmodul), deren sicheren IT-Betrieb und an die vertrauenswürdige Kommunikationsinfrastruktur (Smart Metering – Public Key-Infrastruktur).

Falschgeld

Falschgeldhersteller nutzen vermehrt das sogenannte **Darknet** im Internet, um ihre Blüten zu produzieren und zu vertreiben, meldet die FAZ am 16. Mai. Deutschland sei in der Vergangenheit vor allem Umschlagplatz für Blüten gewesen. Inzwischen würden aber vermehrt Blüten hier produziert. 2016 habe es gut 60 Prozent mehr Ermittlungsverfahren wegen Herstellung von Falschgeld gegeben. Die Bundesbank habe 2016 rund 82.200 falsche Euro-Banknoten im Nennwert von 4,2 Mio. Euro registriert. Dies sei ein Rückgang um rund 14 Prozent zum Vorjahr gewesen. Die Bundesbank führe das Zurückdrängen von Falschgeld vor allem auf die höheren Sicherheitsstandards der neuen Banknoten der Europaserie zurück.

Gefahrenmanagement

Für eine **einzige Schnittstelle für Gebäude- und Sicherheitsmanagement** plädiert UTC Fire & Security Deutschland in der Ausgabe 5-2017 der Zeitschrift GIT, S. 14/15. Die UTC-Einbruchmeldezentrale Advisor Master sei eine integrierte Lösung für Einbruchmeldung, Zutrittskontrolle, Videoüberwachung und Brandschutz. Im Falle eines Feueralarms sorge die grafische Benutzeroberfläche mit Lageplänen für eine schnelle Lokalisierung der Ereignisse. Wenn ein Feuer bestätigt wurde, könnten Türen entriegelt, Signalgeber aktiviert und Aufzüge in das Erdgeschoss

geschickt werden, während die Ereignisabläufe durch das Videosystem verifiziert werden.

PROTECTOR enthält in der Mai-Ausgabe, S. 29, eine **Marktübersicht** über 62 Gefahrenmanagementsystemen von 34 Anbietern. Abgefragt wurden unter anderen folgende Kriterien: Systemarchitektur, Schnittstellen, Übertragungsprotokolle und Service.

Gefahrenmeldeanlage

GIT weist in der Ausgabe 5-2017, S. 21, darauf hin, dass die Planung von Gefahrenmeldeanlagen – und somit auch Einbruchmeldeanlagen – nach DIN VDE 0833-1 generell nur von sogenannten „Elektrofachkräften GMA" vorgenommen werden dürfe. Beschrieben wird in dem Beitrag, welche Fragestellungen im Rahmen der Planung zu beantworten sind und welche Faktoren bei der Auswahl der Überwachungsmaßnahmen berücksichtigt werden sollten.

Das Management der **Ab- und Zuschaltung von Meldern** behandelt die Zeitschrift PROTECTOR in der Mai-Ausgabe, S. 24/25. In Verbindung mit einem Gefahrenmanagementsystem könnten Schaltungen sowie deren Dokumentation über ein neues Konzept einfach parallel zum normalen Meldungsbetrieb erfolgen. Dabei beschränke sich das neue Konzept nicht auf die Bedürfnisse bei der Abschaltung von Brandmeldern. Mit Hilfe eines Software-Moduls zum Management von Schaltvorgängen ließen sich Zeiträume einzeln oder zyklisch festlegen, in denen bestimmte angeschlossene Sensoren und Aktoren (Datenpunkte) in einem definierten Zielzustand versetzt werden sollen. Zu Beginn beziehungsweise Ende eines derart definierten Zeitraums würden hierzu Steuerbefehle, vollautomatisch oder nach Rückfrage, an die betroffenen Datenpunkte geschickt. Zusätzlich zur Planung und Automatisierung von Schaltzeiten übernehme ein Schaltvorgänge-Modul auch deren Verwaltung und Dokumentation.

Gefahrstofflagerung

Sicherheitsschränke seien für die Lagerung von Gefahrstoffen gegenüber baulichen Lösungen oft im Vorteil, argumentiert die Zeitschrift GIT in der Ausgabe 5-2017, S. 66/67. Sicherheitsschränke nach DIN EN 14470-1 könnten in vielen Fällen eine wirtschaftlichere und deutlich flexiblere Alternative sein. Bauliche Lösungen müssten eine Vielzahl strenger Vorgaben erfüllen. Heute seien Typ-90 Sicherheitsschränke in Deutschland und vielen Ländern Europas Stand der Technik. Sie böten genug Zeit, um Evakuierungs-, Lösch- und Rettungsmaßnahmen einzuleiten. Auslaufende brennbare Flüssigkeiten müssten noch im Sicherheitsschrank aufgefangen und beseitigt werden können.

Chemanager-online.com beschreibt am 25. Mai die Entwicklung von Sicherheitsstandards im Umgang mit **Chemikalien am Arbeitsplatz**. Die DIN EN 14470-1 beschreibe Kriterien für die Bauweise und Beschaffenheit des Sicherheitsschranks, wie zum Beispiel die Selbstschließung der Türen im Brandfall oder die Anforderungen an die Feuerwiderstandsfähigkeit des Schranks. Je nach Konstruktionsweise und immer in Verbindung mit einer erfolgreichen Brandprüfung würden Schränke in die Typklassen 15, 30, 60 oder 90 eingeteilt. Die Typklasse beschreibe die Zeitspanne, in der im Brandfall im Innenraum des Schranks keine Temperaturerhöhung auf mehr als 200 °C stattfindet. Asecos habe vor über 20 Jahren den ersten Sicherheitsschrank

mit 90 Minuten Feuerwiderstandsfähigkeit entwickelt. In den USA setze beispielsweise FM Global maßgeblich den Sicherheitsstandard. Dessen Geschäftszweig FM-Approvals sei ein qualifizierter Prüfservice für Anlagen und Produkte mit höchsten Qualitäts- und Sicherheitsstandards. Die Anforderungen an Lagerschränke für entzündliche Flüssigkeiten seien in der FM-Norm 6050 definiert. Ein Sicherheitsschrank müsse demnach so beschaffen sein, dass bei einem Brand die Innentemperatur des Schranks über die Dauer von lediglich zehn Minuten nicht über 163 °C ansteigt. Dies gelte in den USA in Verbindung mit einer geforderten Sprinkleranlage als ausreichend, um notwendige Evakuierungsmaßnahmen einzuleiten. Gezielte Experimentalvorträge verdeutlichten, wie wichtig das ständige Sensibilisieren ist. Denn so paradox es klinge, gerade der routinierte Umgang berge Gefahren.

Geldwäsche

Die Wochenzeitung DAS PARLAMENT berichtet am 2. Mai, die Bundesregierung habe den Entwurf eines Gesetzes zur Umsetzung der 4. EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen im Bundestag eingebracht. Danach müssten die geldwäscherechtlich Verpflichteten strengere Vorgaben beachten. Außerdem werde eine **Zentralstelle für Finanztransaktionsuntersuchungen** bei der Generalzolldirektion eingerichtet. Sie solle geldwäscherechtliche Meldungen entgegennehmen, analysieren und bei einem Verdacht auf Geldwäsche oder Terrorismusfinanzierung an die zuständigen Stellen weiterleiten. Alle wirtschaftlich Berechtigten sollten in einem elektronischen Transparenzregister erfasst werden.

Güterhändler, also Händler von beweglichen und nicht beweglichen Sachen, die Barzahlungen über 10.000 Euro entgegennehmen, sollten ebenfalls in die Regeln einbezogen werden. Der BDI befürchte, dass jeder gewerbliche Verkäufer von Gütern in den Anwendungsbereich des Geldwäschegesetzes fallen könnte. Aus dem Anwendungsbereich der Geldwäscherichtlinie herausgenommen würden Geldspielgeräte. Aufgrund der geringen Einsatzhöhe und der niedrigen Gewinnhöhe im einstelligen Eurobereich bestehe auf der Spielerseite ein nur sehr geringes Geldwäscherisiko.

Illegales Glücksspiel

Deutschland gelinge es im internationalen Vergleich besonders schlecht, den Glücksspielmarkt in geordnete Bahnen zu lenken. Die Regulierung sei gescheitert. Alle Ziele des Glücksspielstaatsvertrages würden verfehlt – darunter die Schwarzmarktbekämpfung sowie der Jugend- und Spielerschutz, berichtet die FAZ am 29. Mai. Es floriere ein riesiger Schwarzmarkt mit einer Abdeckung von mehr als 95 Prozent. Dieser Bereich ohne staatliche Kontrolle soll inzwischen ein Jahresvolumen von mehr als 30 Mio. Euro haben, schätze das Hessische Innenministerium.

Industrie 4.0

„Die **disruptive Kraft von Industrie 4.0**" thematisiert Bernhard Müller, Sick AG, in der Zeitschrift GIT, Ausgabe 5-2017, S. 58/59. Sensoren müssten mit den Datenwelten kommunizieren können und damit liege in der Kommunikationsfähigkeit der Sensoren das Hauptmerkmal für Industrie 4.0.

Das „Disruptive" sei, dass ein Sensor die Datenwelt bedienen kann und mit eben dieser Datenwelt umgehen kann.

Mit industrieller Sicherheit befassten sich mehrere Referate im Rahmen des 15. Deutschen IT-Sicherheitskongresses vom 16.–18. Mai in Bonn. Prof. Dr.-Ing. Reiner Anderl und Kollegen von der Technischen Universität Darmstadt stellten das **Projekt IUNO**, ein nationales Referenzprojekt zur IT-Sicherheit in Industrie 4.0 vor (S. 109–120 im Tagungsband). In diesem Projekt würden Bedrohungen und Risiken für die intelligente Fabrik identifiziert und Schutzmaßnahmen entwickelt sowie exemplarisch umgesetzt. Ziel sei es, Sicherheitsrisiken im Kontext von Industrie 4.0 ganzheitlich zu erforschen und möglichst allgemein verwendbare Lösungen für Herausforderungen der IT-Sicherheit im industriellen Anwendungsfeld zu entwickeln, die auf alle produzierenden Unternehmen übertragbar sind und als Blaupausen für eine sichere Implementierung von Industrie 4.0 herangezogen werden können. David Meier, Steffen Pfrang, Jörg Kipper und Dr.-Ing. Christian Haas, Fraunhofer Institut IOSB, erläutern den Entwurf und Einsatzszenarien eines **Sicherheitslabors für Industrie 4.0** (Tagungsband S. 137–150). Mit Hilfe des IT-Sicherheitslabors sei es möglich, auf der einen Seite die notwendigen Konsequenzen im Bereich IT-Sicherheit aufzubauen und im täglichen Einsatz zu erproben, als auch in Forschungs- und Entwicklungsprojekten Technologien und Lösungen zu testen. Das IT-Sicherheitslabor werde auch in Zukunft an aktuelle Technologien und Anforderungen angepasst bzw. um diese erweitert werden.

Industrial Control Systems (ICS), die unmittelbar mit dem Internet verbunden sind, würden in nahezu allen Infrastrukturen eingesetzt – von der Fabrikautomation über die Wasserversorgung bis hin zur Verkehrsleittechnik, schreibt Ernst Lehmhofer, Westermo Data Communications GmbH, in der Ausgabe <kes> special vom Mai 2017, S. 38/39. Mit dem IT-Sicherheitsgesetz seien Betreiber einer Kritischen Infrastruktur verpflichtet, IT-Sicherheit auf dem aktuellen Stand der Technik vorzuhalten. Für eine sichere und hochverfügbare Datenkommunikation mit entsprechender Verschlüsselung wäre es sinnvoll, eine „Ende-zu-Ende-Lösung" für das Informationssicherheitsmanagementsystem (ISMS) zu implementieren. Einen weiteren Schutz böten Tools wie „Irma" von Videc zur Angriffserkennung. Das abgeschottete System sei für potenzielle Angreifer wie auch für eingeschleuste Schad-Software unsichtbar.

IT-Sicherheit

Im Auftrag des BSI wurde im September/Oktober 2016 eine jetzt veröffentlichte **„Cybersicherheitsumfrage"** anonym durchgeführt. Von den befragten Institutionen in zahlreichen Wirtschaftsfeldern sind 21 Prozent IT-Dienstleister. 331 Datensätze gingen in die Auswertung ein. 65,6 Prozent der Institutionen waren Ziel erfolgreicher oder erfolgloser Cyberangriffe (2015: 58,5 Prozent). 47 Prozent der Institutionen (2015: 43 Prozent) waren Opfer eines erfolgreichen Cyberangriffs, 12 Prozent mit relevanten Folgen. Die meisten gemeldeten Angriffsarten (fast 140) waren Infektionen mit Ransomware (gezielt oder ungezielt), gefolgt von ungezielten Infektionen mit sonstiger Malware (über 120). 32 Prozent der Institutionen waren in den letzten 6 Monaten durch eine Ransomware-Infektion betroffen. Von 169 Befragten gaben 54 einen Produktions-/Betriebsausfall, 44 erhebliche Kosten für die Aufklärung und Wiederherstellung als Schaden an. Auf die Frage „Stellen Cyberangriffe eine relevante Gefährdung für die Betriebsfähigkeit der Institution dar?" antworteten 47 Prozent mit

„ja", 42 Prozent mit „ja, aber der Betrieb kann mittels Ersatzmaßnahmen aufrechterhalten werden". 62 Prozent der Befragten gehen von einer Zunahme der Cyberrisiken aus; 19 Prozent sehen keine Veränderung. In 73 Prozent der befragten Institutionen gibt es einen Gesamtverantwortlichen für das Thema IT-Sicherheit. Bei 14 Prozent verteilt sich die Zuständigkeit auf mehrere Personen. Sechs Prozent beauftragen einen Externen. Unter den zum Schutz vor Cyberangriffen umgesetzten Maßnahmen wurden vorrangig genannt: Absicherung von Netzübergängen (fast 300 der 331 Befragten), zentraler oder dezentraler AV-Scan (ca. 250 bzw. 240) und regelmäßige Sensibilisierungsmaßnahmen (über 200).

Die **Back-up-Infrastruktur** behandelt Dipl.-Ing. Andreas Wisler, goSecurity GmbH, in der Ausgabe 2-2017 der Zeitschrift Sicherheitsforum, S. 34/35. Es gebe sogar Firmen, die lieber bei Ransomware bezahlen, als auf das Back-up zurückzugreifen, da dies teurer wäre. Die Dauer eines Back-ups benötige bei den stetig wachsenden Daten zudem immer länger. In einer repräsentativen aktuellen Umfrage von <kes>/Microsoft hätten 13 Prozent der befragten IT-Leiter ausdrücklich angegeben, kein Back-up von Servern, Clients oder mobilen Geräten zu tätigen. Vor dem Einsatz eines Back-ups sei zu überlegen, welche Daten für das Überleben der Firma notwendig sind oder wo gesetzliche, respektive regulative Anforderungen bestehen. Als Zweites müssten die verschiedenen Abteilungen und Personen für ihren Bereich angeben, auf welche Daten sie in welcher Zeit wieder zugreifen müssen. Um genügend Reserven einzuplanen, müsse die Back-up-Infrastruktur auf die Verarbeitung von mindestens der vierfachen Datenmenge gegenüber dem Stichdatum ausgelegt werden. Das heiße nicht, dass dieses Datenvolumen ab der Einführung zur Verfügung stehen muss. Der Autor beschreibt die Sicherungsmethoden „Speicherung auf Tape(s)", „Back-up auf Wechsel-Harddisk" und „Erstellung eines Images". Auch wenn Back-ups und Archivierung ähnlich sind und häufig die gleichen Hilfsmittel verwendet würden, hätten sie doch unterschiedliche Anforderungen. Deshalb werde empfohlen, die Archivierung in einem eigenen Konzept zu bearbeiten. Der Sicherungsrhythmus der Datenbestände sei entsprechend ihrer Wichtigkeit und ihrer Dynamik unterschiedlich. Nach jeder Sicherung sollte das Ergebnis kontrolliert werden. Mindestens nach einer Anpassung des Back-up-Plans sollte ein Desaster-Recovery, d. h. eine vollständige Wiederherstellung aller Daten, durchgeführt werden.

An einer **VdS-Studie zur Cyber-Security** haben 2.000 Unternehmen teilgenommen, meldet GIT in der Ausgabe 5-2017, S. 48/49. Eines der vielen Hilfsmittel, mit denen VdS die digitale Absicherung speziell von Mittelständlern unterstützt, sei der kostenlose **Quick-Check**. Auf www.vds-quick-check.de erhalten Firmenverantwortliche in nur 20 Minuten eine individuelle Übersicht über den Status ihrer Cyber-Security in allen relevanten Handlungsfeldern – inklusive möglicher Optimierungsvorschläge. Auf die Widerstandsfähigkeit ihrer eigenen Netzwerke verließen sich 67 Prozent der Teilnehmer. Starke Schwächen existierten gemäß der Auswertung beim Umgang mit Sicherheitsvorfällen, beim allgemeinen Managementansatz sowie bei der Integration externer Dienstleister. Zudem führten nur die wenigsten Firmen systematische Risikoanalysen durch. Informationssicherheit werde vom Management vieler Unternehmen noch immer nicht ausreichend thematisiert.

Mit einem „Generalschlüssel fürs Internet" meine eine Allianz deutscher Unternehmen keine Backdoor in Krypto, sondern ein **Single-**

Sign-on-Verfahren, heißt es im ASW-Newsletter vom 12. Mai. Dies solle besonders sicher sein, technische Details gebe es bislang aber nicht. An der Partnerschaft nähmen Daimler, die Deutsche Bank, der Versicherungskonzern Allianz, der Axel Springer-Verlag und das Karten-Startup Here teil.

Der Behörden Spiegel weist in der Mai-Ausgabe darauf hin, dass das BSI den neuen **BSI-Standard 200-2** zur IT-Grundschutz-vorgehensweise vorgestellt habe. Der neue Standard etabliere drei Vorgehensweisen. Neu sei die Möglichkeit einer Basisabsicherung als Einstieg zur Initiierung eines ISMS. Mit der Standardabsicherung könne ein komplettes Sicherungsprogramm implementiert werden. Diese Absicherung sei kompatibel zur ISO 27001-Zertifizierung. Neu sei die Schaffung einer Kernabsicherung. Hier würden zunächst die jeweils wichtigsten Daten auf Standard-Niveau abgesichert. Auch hier sei das Ziel die vollständige Umsetzung des IT-Grundschutzes.

Die Widerstandsfähigkeit gegen Cybergefahren müsse erhöht werden, zeigt sich Arne Schönbohm, Präsident des BSI, in der Mai-Ausgabe des Behörden Spiegel überzeugt. Ein Lösungsansatz bestehe darin, bei aktuellen Entwicklungen in Bereichen wie Automotive, Industrie 4.0 oder mobilen Anwendungen bereits jetzt IT-Sicherheitsstandards zu formulieren, die etablierte Vorgehensweisen und Erkenntnisse in die Produktentwicklung mit einfließen lassen.

Bundesverkehrsminister Dobrindt fordere ein **schärferes IT-Sicherheitsgesetz**, berichtet die FAZ am 16. Mai. Das IT-Sicherheitsniveau müsse erhöht werden und zwar im Hinblick auf die Verkehrsinfrastruktur oder das Gesundheits- und Finanzwesen, habe er in einem Zeitungsinterview gesagt. Derzeit befinde sich eine wichtige Verordnung zur IT-Sicherheit in der Ressortabstimmung, mit der weitere Bereiche der Wirtschaft, etwa Versicherungen und bestimmte Logistikdienste, als „Kritische Infrastruktur" einbezogen werden sollen. Der netzpolitische Sprecher der SPD, Lars Klingbeil, fordere Investitionen in mehr Sicherheit und neue Technologien sowie schärfere Haftungsregeln für die Unternehmen. Matthias Kammer vom Deutschen Institut für Vertrauen und Sicherheit im Internet: „Wir beobachten, dass Komfort die Sicherheit im Zweifel aussticht." Sicherheit müsse bequemer werden.

Im Gespräch mit der FAZ (vom 16. Mai) weist Arne Schönbohm, Präsident des BSI, darauf hin, dass es heute knapp **600 Mio. Schadprogramme** gebe. Cybercrime sei ein größeres Geschäft als Drogenkriminalität. Eine der wichtigsten Aufgaben des BSI sei die Zertifizierung. Keine Behörde rund um die Welt stelle so viele Zertifikate aus wie das BSI. Das Amt habe eine Art GSG9 für die Cyberabwehr geschaffen und MIRT genannt. Das stehe für Mobile Incident Response Team, eine mobile Truppe, die zu Vorfällen ausschwärmt. Vor allem kleine und mittelgroße Unternehmen würden davor zurückschrecken, Erpressungen anzuzeigen: Sie treibe die Angst, damit den eigenen Ruf zu ruinieren. Dabei gebe es mehrere Untersuchungen, die zeigten, dass ein transparenter Umgang mit Sicherheitslücken Unternehmen eher nutzt, weil Kunden die Ehrlichkeit schätzen.

Digitale Gesellschaft zwischen Risikobereitschaft und Sicherheitsbedürfnis lautete der Titel des **15. Deutschen Sicherheitskongresses**, der vom 16. bis 18. Mai in Bonn stattfand. Unter dem Aspekt der Unternehmenssicherheit werden folgende Referate hervorgehoben: Christian Horn und Max Klein, Fraunhofer Institut für Produktionsanlagen und Konstruktionstechnik, thematisieren **Detektion von Advanced Persistent**

Threats durch kausalitätsbasierte Erkennung anomalen Verhaltens in Prozessen verteilter Automatisierungsnetzwerke, S. 255–268. Bisherige Systeme zur Angriffserkennung seien üblicherweise nicht in der Lage, die Grenzen zwischen den einzelnen Systemebenen der technologischen Infrastruktur zu überwinden, in denen sich ATPs verstecken könnten. Die Arbeit dieses Beitrags nutze ein neuartiges Verfahren zur kausalitätsbasierten Anomalie-Detektion als Grundlage einfacher Klassifikatoren von Prozessdaten in komplexen Kritischen Infrastrukturen, um Manipulationen an Prozesswerten über Systemebenen der Infrastruktur hinweg erkennen zu können. Dazu würden andere Prozessdaten genutzt, um über zugrunde liegende physikalische Kausalitäten eine Validierung durchzuführen. Eine realitätsnahe Simulations- und Testumgebung in Kombination mit Daten aus realen Prozessen diene als Grundlage für eine Evaluation des Verfahrens. Dr. Robert Koch und Teo Kühn, Universität der Bundeswehr, München, stellen ein neues **stromverbrauchbasiertes System zur Einbruchs- und Innentätererkennung** vor: Dr. WATTson (S. 269–284). Im Gegensatz zu Businessnetzen seien industrielle Steuerungssysteme (ICS) über lange Zeit hinweg abgeschlossene Einheiten gewesen, ohne Verbindung zur Außenwelt. Die Sicherheit der Systeme habe oftmals eine untergeordnete Rolle gespielt. Andererseits würden heutzutage mehr und mehr dieser Systeme mit dem Internet verbunden. Die Sicherheitssituation verbleibe in diesem Bereich auf einem unzureichenden Niveau. Gerade im Bereich der industriellen Steuerungssysteme seien viele ältere Anlagen im Einsatz, die nicht einfach mit Sicherheitstechnik nachgerüstet werden könnten. Dagegen könne ein auf der Messung von Stromverbrauch basiertes, leichtgewichtiges Sicherheitssystem auch in bestehende und eigentlich nicht nachrüstbare Anlagen integriert werden. Hierfür würden im Prototyp „Dr. WATTson" verschiedene Detektionsverfahren kombiniert und auf Basis von kostengünstigen Einplatinenrechnern umgesetzt. Die Evaluation zeige, dass es hohe Detektionsraten unter gleichzeitig niedrigen Fehlalarmraten ermögliche. Karsten U. Bartels, Merlin Backer und Michael Schramm, Rechtsanwälte, befassen sich mit dem **„Stand der Technik" im IT-Sicherheitsrecht**. Zur Feststellung des Standes der Technik biete der Gesetzgeber nichts an. Eine Möglichkeit stellt ein dreigliedriges Verfahren dar. Zunächst sind die technischen Einrichtungen im Rahmen einer limitierten Schutzbedarfsanalyse zu erfassen. Dann sind die branchenweit typischerweise genutzten technischen und organisatorischen Vorkehrungen sowie bestehende Sicherheitsstandards zu ermitteln. Schließlich sind Informationen zu branchenübergreifenden Technologien einzuholen. Der Erlass einer Verordnung sowie die Einführung eines Zertifizierungsverfahrens wären sinnvoll (S. 503–514). Stefan Zink, Net at work GmbH, plädiert für **Sender- und Empfängeridentifikation** als zentralen Schlüssel zu höherer E-Mail-Sicherheit (S. 451–461). Der Autor gibt fünf Soforttipps für jedes Unternehmen: Die Konfiguration der eigenen Mail-Infrastruktur mit kostenlosen Tools wie ssl-tools.net testen. Sofern nicht vorhanden, Sender Policy Framework-/DomainCase Identified Mail (SPF-/DKIM) und Domain-based Message Identification, Reporting and Conformance (DMARC-)Records einrichten. Verschlüsselung von Verbindungen zu einem Server zum Schutz vor Mithören bei der Kommunikation mit bekannten Partnern erzwingen. DNS-based Authentification of Named Entities (DANE) nutzen. Prüfen, ob der Hersteller der eingesetzten Mail-Securitylösung DANE nutzt. Andernfalls alternative Produkte in Betracht ziehen.

Friedhelm Greis befasst sich am 18. Mai in ZEIT-ONLINE mit der Absicht der Großen

Koalition, in den kommenden Monaten Grundlagen für einen umfangreichen Einsatz von Überwachungsprogrammen auf Endgeräten von Verdächtigen zu schaffen. Mit Hilfe von gehackten Smartphones oder Computern solle eine verschlüsselte Kommunikation überwacht oder sollen Dateien ausgelesen werden können (Quellen-TKÜ bzw. Online-Durchsuchung). Der Einsatz dieser **„Staatstrojaner"** solle der Polizei nicht nur zur Gefahrenabwehr, sondern bei Ermittlungen zu 38 bzw. 27 Straftaten erlaubt sein.

Dr. Sebastian Schmerl, Computacenter, stellt in der Ausgabe 2-2017 der Zeitschrift <kes>, S. 24–29, das Konzept eines **Cyber Defence Centre** (CDC) vor. Um Reaktionsmechanismen organisationsweit zu verankern, brauche es menschliche Expertise, definierte Prozesse und eine klare Aufgabenverteilung. Ein CDC verbessere den proaktiven Schutz der gesamten IT-Infrastruktur einer Organisation durch einen ganzheitlichen Ansatz: Ausgehend vom Echtzeitlagebild lasse sich ein CDC schrittweise aufbauen und gleichsam evolutionär nach Maßgabe der jeweils vorhandenen Ressourcen bis zum vollen Funktionsumfang erweitern. Rollenverteilung und Prozesse im CDC sowie der damit einhergehende Informationsfluss müssten so definiert werden, dass sich das CDC permanent selbst optimiert und das Zusammenspiel mit den Resolvern und anderen Stakeholdern eines CDC im Unternehmen verbessert.

In der Ausgabe 2-2017 der Zeitschrift <kes>, S. 35–39, befassen sich Dr. Heike Hagemeier und Dr. Manfred Lochter, BSI, mit dem **Quantencomputer**. Die Idee stamme von Richard Feynman (Anfang der 1980er-Jahre) und beruhe auf den Gesetzen der Quantenmechanik. Er unterscheide sich von den heutigen Computern dadurch, dass er nicht mit Bits, sondern mit Quantenbits rechnet. Sie könnten im Gegensatz zu klassischen Bits zwei Zustände (mit gewissen Wahrscheinlichkeiten) gleichzeitig annehmen (Superposition). Ein Quantencomputer könne mit verschränkten Qubits in einem Schritt Berechnungen durchführen, für die ein herkömmlicher Rechner zwei Operationen benötigt. Bisher sei noch kein Quantencomputer verfügbar, der zum Brechen kryptografischer Verfahren geeignet wäre. Es gäbe jedoch große Fortschritte bei der Realisierung der dafür benötigten Grundbausteine. In der Kryptografie entwickele sich ein neues Forschungsgebiet: die Post-Quantum-Kryptografie. Der Einsatz quantencomputerresistenter Verfahren werde früher oder später für die meisten kryptografischen Verfahren zum Standard werden. Ein kurzfristiger Einsatz sei allerdings nicht realistisch. Das BSI empfehle daher, vorerst „hybride" Lösungen einzusetzen, also eine Kombination der klassischen Verfahren mit quantencomputerresistenten Lösungen.

Die **SINA Workstation** für sicheres Surfen im Internet stellt Jan Leduc, secunet Security Networks AG, im <kes> special vom Mai 2017 vor. Es seien lokale (Browser) Anwendungen, die enorme Angriffsflächen bieten. Wirksame Abhilfe schaffe hier ein sogenanntes Remote-Controlled Browser System (ReCoBS). Der Internetbrowser des Mitarbeiters werde nicht auf seinem lokalen System ausgeführt, sondern auf einem Terminalserver außerhalb des sensiblen Netzwerkbereichs. Der secunet safe surfer sei eine Lösung, die auf der ReCoBS-Architektur aufbaut. Eine weitere Lösung, die zuverlässig vor Cyberbedrohungen schützt, sei die SINA Workstation. Deren Sicherheitsphilosophie umfasse Smartcard-basierte Kryptografie und eine sichere Systemplattform).

Die **biometrische Unterschrift auf dem Smartphone** thematisiert Dr. Roman Schmidt, Intelligent Insights GmbH, in der

Ausgabe <kes> special vom Mai 2017, S. 8/9. Im Gegensatz zu traditionellen Verfahren extrahiere der neuartige Algorithmus jedes einzelne Pixel aus dem digitalisierten Unterschriftenbild und reichere dieses mit biometrischen Merkmalen des Schreibers an. Insbesondere würden die Geschwindigkeit und die Beschleunigung der Unterschrift zu jedem Zeitpunkt der Unterzeichnung berechnet. Zum Vergleich zweier Unterschriften würden die Pixel der Unterschriften durch einen Optimierungsalgorithmus aufeinander abgebildet. Nur wenn eine Abbildung möglich ist, die keine zu starke Modifikation der Unterschriften erforderlich macht, werde eine gegebene Unterschrift positiv verifiziert.

DocSetMinder sei ein idealer Nachfolger für das Grundschutz (GS-)Tool, schreibt Krysztof Paschke, GRC Partner GmbH, in <kes> special vom Mai 2017, S. 18/19. Die Software bilde die BSI-Standards 100-1 bis 100-4 und den Datenschutz (DS-GVO) vollständig ab. Ab Mai 2017 stünden auch die BSI Standards 200-2 und 200-3 zur Verfügung. Der Funktionsumfang der Software mache den Einsatz weiterer Tools oder Office-Anwendungen für die Dokumentation und Zertifizierung des umgesetzten Standards überflüssig. In DocSetMinder stünden diverse Module, Schnittstellen und standardisierte Maßnahmenkataloge zur Verfügung. Der Autor beschreibt die Module Organisation, Dokumentation, IT-Grundschutz, Datenschutz, (IT-) Notfallmanagement, Katastrophenschutzplan und Risikoanalyse.

Die Computing Technology Industry Association (CompTIA) habe einen **Karrierepfad für IT-Sicherheitsfachkräfte** entwickelt, den Christina Allmeroth, CompTIA, in <kes> special vom Mai 2017, S. 20/21, vorstellt, Er baue systematisch auf grundlegenden Zertifizierungen auf, die mit einem eigens für den Bereich Cybersicherheit entwickelten Nachweis abgeschlossen werden. Der Pfad bestehe aus sechs Stufen: IT-Fundamentals, A+, Network+, Security+, CSA+ und CASP. Ganz neu sei die internationale, herstellerneutrale Zertifizierung Cybersecurity Analyst+(CSA+), die die Ausbildungslücke zwischen CompTIA Security+ und CompTIA Advanced Security Practitioner (CASP) schließe. Zielgruppe hierfür seien IT-Profis mit drei bis vier Jahren Praxiserfahrung.

Traditionellen IT-Sicherheitssystemen fehlt die Schwarmintelligenz, meint Michael Veit, Sophos, in <kes> special vom Mai 2017, S. 26/27. Die Netzwerkgrenzen würden immer durchlässiger und die Verantwortlichen für IT-Sicherheit müssten neue Werkzeuge an die Hand bekommen, um auf die zunehmende Mobilität der Arbeitswelt reagieren zu können. Die Flexibilität der Hacker mache den traditionellen Sicherheitssystemen zu schaffen, da ihnen die Schwarmintelligenz fehle. Entscheidend für das Funktionieren sei heute, dass alle Systeme intelligent miteinander verknüpft sind und miteinander kommunizieren. Ein gutes Beispiel für eine intelligente Verknüpfung sei **Malicious-Traffic-Detection**. Die Funktion enttarne kompromittierte Computer, während sie mit den „Command and Control"-Servern der Angreifer kommunizieren. Indem das Feature in den Endpoint integriert wird, könnten Kompromittierungen nicht nur innerhalb, sondern auch außerhalb des Netzwerks erkannt, die spezifische Schaddatei identifiziert und die Infektion beseitigt werden. Letztendlich sei die Verschlüsselung der Daten der perfekte Schutz, selbst wenn es Hacker bis ins System geschafft haben sollten.

Einige Wirtschaftsprüfungsgesellschaften haben sich darauf spezialisiert, für die große Mehrheit der Mittelständler mit begrenzten Ressourcen eine moderne, umfassende

Sicherheitsarchitektur aufzubauen und zu unterhalten, heißt es in der FAZ, Verlags Special Zukunft Mittelstand, vom 23. Mai. Sie würden zudem bei der Anwendung eines entsprechenden Sicherheitsstandards beraten. Der **Vorteil mittelständisch geprägter Prüfungsgesellschaften** sei zusätzlich, dass sie keine Mono-Spezialisierung betreiben. Die Mitarbeiter seien nicht zu kleinteilig spezialisiert und könnten gerade dadurch ein Konzept erarbeiten, das für Mittelständler auch praktikabel ist.

IuK-Kriminalität

Einige deutsche Kunden von Telefonica seien im Januar Opfer eines Hackerangriffs geworden, der dazu benutzt worden sei, Geld von Bankkonten zu stehlen, berichtet die FAZ am 4. Mai. Ausgeführt worden sei die Hacker-Attacke mit dem sogenannten **mTAN-Verfahren**. Das BSI rate schon länger von der mobilen TAN ab und empfehle stattdessen die sogenannten TAN-Generatoren für das Online-Banking. Die Schwachstelle, die von den Hackern ausgenutzt wurde, liege im **SS7-Netzwerk**. Das gelte nach heutigen Sicherheitsstandards nicht mehr als zeitgemäß, werde aber trotzdem weiterhin rund um die Welt eingesetzt. Am 6. Mai titelt aber die FAZ mit „Die Mär über das unsichere Online-Banking". Panikmache sei fehl am Platz. Die Hacker müssten Zugriff sowohl auf die Zugangsdaten zum Online-Konto wie auf die TAN bekommen. Schützen könne man sich sehr einfach: den Virenscanner aktualisieren, keine Anhänge von Mails aus unbekannten Quellen öffnen und vor allem, bloß nicht vertrauliche Bankdaten auf Internetseiten eingeben, selbst wenn sie täuschend echt aussehen. Halte man sich an diese einfachen Regeln, sei das Onlinebanking auch sicher.

Nach einem Bericht in der FAZ am 4. Mai über eine Cybercrime Conference sei 2016 in Deutschland ein **Gesamtschaden von 51 Mio. Euro** durch Internetkriminalität entstanden. Der BKA-Präsident Holger Münch habe auf den Zusammenhang zwischen der Zunahme von Internetkriminalität und dem enormen Anwachsen der globalen Datenmenge hingewiesen. In den vorigen beiden Jahren seien weltweit so viele Daten produziert worden wie zuvor in der gesamten Menschheitsgeschichte. Die Polizei müsse sich dieser Herausforderung dadurch stellen, dass klassische Polizeiarbeit wie Streifengänge und Kontrollen künftig im übertragenen Sinne auch im Internet stattfinden sollte. Weil Deutschland ein hochentwickeltes Land sei, das viel Angriffsfläche biete, gebe es Schätzungen, die den Gesamtschaden auf 1,6 Prozent des deutschen Bruttoinlandsproduktes bezifferten.

Martin Schindler weist in silicon.de am 28. April darauf hin, dass immer häufiger Unternehmen gezielt mit **Ransomware** angegriffen würden. Laut Symantecs Internet Security Threat Report haben sich die Forderungen der Cyberkriminellen 2016 in den USA mehr als verdreifacht. 64 Prozent der Betroffenen hätten in den USA die Forderungen von Cybererpressern beglichen, weltweit 34 Prozent. Insgesamt habe Symantec 2016 463.841 Ransomware-Angriffe registriert, 27 Prozent mehr als 2015. Kostenlose Tools gegen Ransomware gebe es unter anderem von No More Ransom, einem Zusammenschluss von Behörden und Unternehmen. Aber auch andere Organisationen und Unternehmen lieferten kostenlose Tools, um die Verschlüsselung wieder loszuwerden.

Der Behörden Spiegel weist in der Mai-Ausgabe auf den **Internet Security Threat Report 2016 von Symantec** hin, demzufolge Kriminelle offenkundig öffentlich

wahrnehmbare Organisationen und Staaten angreifen, um diese zu destabilisieren. Zum ersten Mal, so scheine es, würden auch Nationalstaaten in Cyberangriffe involviert sein. Symantec habe Belege, die Nordkorea mit Attacken auf Banken in anderen Ländern in Verbindung brächten. In Deutschland sei eine von 94 E-Mails mit einem bösartigen Link oder verseuchten Anhang versehen. Außerdem würden durch sogenannte **Business E-Mail Compromise Betrugsfälle** über die letzten drei Jahre mehr als drei Mrd. Dollar erbeutet und dabei 400 Unternehmen pro Tag angegriffen. Viele CIOs hätten den Überblick darüber verloren, wie viele cloudbasierte Programme in ihrem Unternehmen genutzt werden. Die meisten vermuteten, dass es nicht mehr als vierzig Applikationen sind. Dagegen hätten die Recherchen von Symantec ergeben, dass es durchschnittlich sogar beinahe Tausend sind.

In etwa 150 Ländern seien etwa 75.000 Computer mit sogenannter **Ransomware** angegriffen worden, meldet die FAZ am 15. Mai. In Deutschland habe der Angriff nicht das Gesundheits-, sondern das Transportwesen getroffen. Viele Bahnreisende hätten auf den elektronischen Anzeigentafeln nicht mehr sehen können, wann welcher Zug wohin fährt, sondern hätten die Botschaft der Erpresser gelesen. Alle Angriffe seien mit der Ransomware „WannaCry" ausgeführt worden. Nach Darstellung des BSI sei das Besondere an „WannaCry", dass sie sich selbst verbreiten könne. Betroffen sind nach Angaben des BSI Computer, die mit dem Betriebssystem Microsoft Windows arbeiten. Verhindern könne man die Weiterverbreitung mit dem Patch MSI17-010 aus dem März 2017. Ende 2015 hätte das BSI schon vor einer Zunahme der zur Lösegelderpressung verwendeten Verschlüsselungstrojaner gewarnt. In den zurückliegenden sechs Monaten sei ein Drittel befragter Firmen in Kontakt mit solcher Software gekommen. In 75 Prozent der Fälle sei die Infektion über E-Mail-Anhänge erfolgt. Weiter heißt es dazu in der FAZ am 23. Mai: Im täglichen Umgang mit Rechner, E-Mail und Internet gelten jene Hinweise, die man nicht oft genug wiederholen kann: Man öffne keine verdächtigen Dateianhänge in der elektronischen Post, selbst wenn sie von bekannten Adressen stammen. Man stelle sein Microsoft Office so ein, dass keine Makros ausgeführt werden und verwende einen PDF-Betrachter, der keine Mini-Programme (Skripte) ausführt. Software installierte man nur aus einer vertrauenswürdigen Quelle, und man lasse keine Unbekannten zu Wartungszwecken aus der Ferne auf den Rechner zugreifen. Besteht der Verdacht, dass ein Rechner von Schadsoftware befallen wurde, trenne man ihn sofort vom Internet. Man versuche anschließend, ihn mit einem bootfähigen USB-Stick oder einer Wiederherstellungs-DVD hochzufahren, und kann anschließend, falls das gelingt, die eigenen Daten auf ein anderes Medium sichern.

Mit **Distributed Denial of Service-Attacken (DDoS)** befasst sich Guido Erroi, Corero Network Security, in der Ausgabe 2-2017 der Zeitschrift <kes>, S. 12–15. Das Bild dieser Bedrohungen habe sich von rein volumetrischen Angriffen inzwischen zu Multivektor-Attacken gewandelt. Aktuelle Toolkits seien in der Lage, DDoS-Angriffe sowohl gegen die Infrastruktur als auch gegen die Anwendungsebene zu richten. Ziel sei zunehmend, einen zweiten Angriff zu initiieren. Vor allem komplexe und zielgerichtete Angriffe gelängen besser, wenn sie sich mit DDoS quasi tarnen. In Zukunft würden DDoS-Attacken wohl komplett automatisiert ablaufen. So könnten so lange verschiedene der zur Verfügung stehenden Möglichkeiten getestet werden, bis eine von ihnen zum Erfolg führt. Menschliche Intervention könne mit solchen Geschwindigkeiten nicht mehr konkurrieren.

Das Kapern ganzer Geschäftsprozesse oder **„Businessprocess-Compromise" (BPC)** behandelt auch Richard Werner, Trend Micro Deutschland, in der Ausgabe 2-2017 der Zeitschrift <kes>, S. 16–18. Das BPC laufe in mehreren Phasen ab und unterscheide sich zunächst nicht sehr von anderen fortgeschrittenen Angriffen. Wie der finale Schlag letztlich aussieht, müsse bei der Erstinfektion und während der Ausspähphase noch gar nicht feststehen. Das Ziel der Täter sei aber stets Geld. Die häufigeren Fälle mit enormer Dunkelziffer seien Attacken, die einem Parasitenbefall ähneln. Zumeist verfolgten sie einfach nur zufällig auftretende Gelegenheiten. Das wirksamste Mittel, um sich vor BPC-Attacken zu schützen, seien funktionierende Prozesse: Schöpfen Mitarbeiter Verdacht, sollten sie sich an den internen Sicherheitsbeauftragten wenden.

Kreditkartensicherheit

Unter Berufung auf den Datenschutz geben Banken in Fällen des Kreditkartenbetrugs den Betroffenen **wenig Auskünfte**, berichtet die FAZ am 10. Mai. Nach Ansicht von Datenschutzbeauftragten sei aber die Kreditkartennummer ein personenbezogenes Datum. Wenn Kreditkartendaten also an Kriminelle gelangen, müsse der Händler oder die Bank dies dem Kreditkarteninhaber mitteilen. Seit der flächendeckenden Einführung der Chip- und PIN-Technologie sei die Betrugsrate bei Kartenzahlungen deutlich gesunken, um mehr als die Hälfte. Neue Karten für kontaktloses Zahlen, ausgerüstet mit sogenannten NFC-Chips, ließen sich auch aus wenigen Zentimetern Entfernung auslesen. Dazu müsse man unbemerkt aber schon sehr nah an die Person treten, außerdem gebe es Schutzhüllen für Geldbörsen, die das verhindern.

Kritische Infrastrukturen

Guido Müller, Stadtwerke Bayreuth Energie und Wasser GmbH, und Matthias Hofherr, atsec information security GmbH, beschreiben im Tagungsband zum **15. Deutschen IT-Sicherheitskongress**, S. 231–238, gesammelte Erfahrungen bei der Implementierung der Vorgaben des IT-Sicherheitskatalogs der Bundesnetzagentur am **Beispiel der Stadtwerke Bayreuth**. Auch wenn sich grundsätzlich eine Zertifizierung nach ISO/IEC 27001 von einer Zertifizierung nach IT-Sicherheitskatalog nur in wenigen Punkten unterscheide, führten zusätzliche Anforderungen der Bundesnetzagentur doch zu erheblichem Mehraufwand. Bei entsprechender Aufgeschlossenheit und dem Willen, die Vorgaben auch als Chance für das Unternehmen zu begreifen, werde aber ein echter langfristiger Mehrwert generiert. Tamara Gurschler, Universität der Bundeswehr München, analysiert die **Risikobeurteilung** im Förderschwerpunkt ITS/KRITIS (S. 395–409). Besonders kleinere und mittlere Betreiber von KRITIS stießen bei der Anwendung bestehender Risikobeurteilungsmethoden an die personellen und finanziellen Grenzen. Die ausgearbeiteten Methoden des Beitrags nähmen sich ihrer Probleme an. MoSaIK entwickele auf Basis von identifizierten Stärken und Schwächen bisheriger Risikobeurteilungsmethoden ein eigenes, modellbasiertes Vorgehensmodell für die KRITIS-Sektoren Energie, Wasser, Staat und Verwaltung sowie unterstützende Werkzeuge, um die Auswirkungen der IT-basierten Risiken im operationalen Umfeld eines Bankensystems bewerten zu können.

Mit einem Referentenentwurf zur Änderung der BSI-KritisV zur Anpassung an neue EU-Vorgaben befasst sich Ingrid Dubois, zugelassene Auditorin für ISO 27001, in der Zeitschrift <kes>, Ausgabe 2-2017,

S. 60–65. BSI-KritisV beschränke sich auf die Sektoren Energie, Wasser, Informations- und Kommunikationstechnik sowie Ernährung. Der nun veröffentlichte Referentenentwurf umfasse Festlegungen zur Bestimmung Kritischer Infrastrukturen für die noch ausstehenden Sektoren Gesundheit (medizinische Versorgung, Versorgung mit Medizinprodukten als Gebrauchsgüter, Versorgung mit verschreibungspflichtigen Arzneimitteln, Laboratoriumsdiagnostik), Finanz- und Versicherungswesen (Bargeldversorgung, kartengestützter Zahlungsverkehr, konventioneller Zahlungsverkehr, Verrechnung und Abwicklung von Wertpapier- und Derivatgeschäften) und Transport und Verkehr (Luftverkehr, Schienenverkehr, See- und Binnenschifffahrt, Straßenverkehr, Öffentlicher Personenverkehr, Logistik, sonstige Anlagenkategorien).

Die FAZ befasst sich am 29. Mai mit einem Fehler in einem Computersystem von **British Airways**, durch den am 27./28. Mai das gesamte IT-Netz der Gesellschaft lahmgelegt wurde. Offenbar habe die Fluggesellschaft bestimmte IT-Systeme nicht redundant gebaut. Die Robustheit von Computersystemen sei besonders für Kritische Infrastrukturen zwingend notwendig. Es sei unerlässlich, dass es gespiegelte Systeme und redundante Strukturen von IT-Systemen bei solchen Unternehmen gebe. Durch IT-Ausfälle sei Unternehmen 2016 rund um die Welt im Durchschnitt ein Schaden von 22 Mio. Dollar entstanden. Nach einer Umfrage des IT-Unternehmens Veeam finden gut 77 Prozent der deutschen Unternehmen ihre eigenen Prozesse für Datensicherheit nicht ausreichend.

Lüftungssicherheit

Frauke Petzold, Slat GmbH, befasst sich in der Mai-Ausgabe von PROTECTOR, S. 28, mit der unterbrechungsfreien Stromversorgung (USV) für **CO-Warnanlagen in Tiefgaragen**. Gemäß Garagenverordnung der Länder und der VDI 2053 (basierend auf DIN EN 50545-1) müssen maschinelle Lüftungssysteme an notstromgepufferte CO-Warnanlagen zur ständigen Überwachung und rechtzeitigen Warnung vor toxischen Gasen angeschlossen sein. Die Warnanlage steuere Lüfter und Signalanlagen (optische und akustische Melder) an und überwache per Messfühler die CO-Konzentration in der Tiefgarage. Bei Stromausfall garantiere eine DC-USV der Reihe SDC-M von Slat mit stabiler Ausgangsspannung den reibungslosen Weiterbetrieb von Warnanlagen und Signalgebern für mindestens eine Stunde.

Maschinensicherheit

Mit den Voraussetzungen des Inverkehrbringens und der Inbetriebnahme von Maschinen nach Art. 5 der MRL befasst sich Dipl.-Ing. (FH) Alexander Winkler, Neosys, in der Ausgabe 2-2017 der Zeitschrift Sicherheitsforum, S. 45–47. Er geht insbesondere auf Konformitätserklärung, Betriebsanleitung und Risikoanalyse ein. Die systematische Risikoeinschätzung und -bewertung stelle den aufwendigsten Teil der **Risikoanalyse** dar. Als Ergebnis der Risikoanalyse seien folgende Aspekte umzusetzen: Signalisierung, Originalbetriebsanleitung und Not-Aus-Einrichtung sowie Instruktion des Personals.

In der Ausgabe 5-2017 der Zeitschrift GIT erklärt Klaus Schuster, K.A. Schmersal GmbH & Co. KG, was unter einer **berührungslos wirkenden Schutzeinrichtung – BWS –** zu verstehen ist. Sie erkenne das Eindringen einer Person oder eines Körperteils in einen geschützten Bereich mit Hilfe von Sensoren und wirkt ohne unmittelbaren mechanischen Kontakt. Die Vorteile der BWS längen auf der Hand: Der Bediener habe den Arbeitsraum im Blick und man könne auf Schutztüren oder andere trennende Vorrichtungen verzichten.

Für die Materiallogistik mit Prozessanforderungen wie etwa dem Ein- und Ausschleusen von Paketen oder Paletten böte die BWS Funktionen, die einen Materialtransport in einen Gefahrbereich nur dann zulässt, wenn Zeitpunkt und Kontur mit der zuvor definierten Anforderung übereinstimmen. Eine Palette mit unregelmäßiger Beladung, Lücken im Transportgut oder Überständen könne eine BWS mit bestimmten Parametern tolerieren. Ganz neu im Programm von Schmersal seien die Sicherheitslichtschranken der Baureihe SLB 240/440, die sich durch eine extrem kleine Bauform auszeichnen und über eine integrierte Auswertung verfügen.

Multifunktionsgeräte

„Angriffsziel Multifunktionsgeräte" titelt der Behörden Spiegel in der Mai-Ausgabe. Das Bewusstsein für dieses „Randthema" werde durch Angriffe auf Webserver, Datenbanken und Router überlagert. Drucker, Multifunktionsgeräte, Faxgeräte und die damit verbundene Software seien gegen Manipulation zu sichern. Die Härtung der Endgeräte und der mit ihnen verbundenen IT-Systeme sei unerlässlich.

Museumssicherheit

Den **Diebstahl eines wertvollen Diadems** aus dem Badischen Landesmuseum in Karlsruhe meldet die FAZ am 9. Mai. Das Anfang des 20. Jahrhunderts gefertigte Diadem im Wert von ca. 1,2 Mio. Euro habe sich in einer verschlossenen Vitrine im Thronsaal, einem öffentlich zugänglichen Ausstellungsraum im Obergeschoss des Museums im Karlsruher Schloss befunden. Die Großraumvitrine – ein Glaskasten mit mehreren Ausstellungsstücken – sei „mit einem geeigneten Gegenstand" geöffnet worden und unversehrt geblieben, habe eine Museumssprecherin gesagt.

Die **Sicherung von Fahrzeugen in Museen** und Sammlungen thematisiert die Zeitschrift PROTECTOR in der Mai-Ausgabe, S. 26. Vorgestellt wird das Sicherungssystem „Human Detector": In einem kompakten und leicht zu versteckenden Gehäuse seien mehrere intelligente Sensoren untergebracht. Die Hauptarbeit verrichte ein kapazitiver Detektor, der ohne den sonst notwendigen Massebezug arbeite. Das löse die üblichen Probleme beim Einsatz von Feldänderungssensoren wie Fehlalarme durch Störungen des Massepotenzials oder ein Übersprechen zwischen den Exponaten. Die Empfindlichkeit könne bei vielen Exponaten so eingestellt werden, dass die Alarmierung schon vor der eigentlichen Berührung erfolgt. Zusätzlich könne ein Hochfrequenzsensor angeschlossen werden. Er überwache zum Beispiel den Innenraum von Cabriolets.

Personenschutz

Markus Strübel, Securiton GmbH, stellt in der Mai-Ausgabe von PROTECTOR, S. 30/31, integrative Lösungen mit einem Höchstmaß an **Sicherheit für Hausbewohner** vor. Securiton habe mit Premium Private ein Rundum-Sicherheitsportfolio mit flexibel anpassbaren Lösungen geschaffen. Das Security-Level-Modell hinter Premium Private biete bedarfsorientiert die Peripheriesicherung, die Gebäudesicherung und die Einrichtung und Ausstattung von Rückzugsräumlichkeiten. Jede zum Einsatz kommende Technologie werde individuell auf das jeweilige Schutzbedürfnis abgestimmt und garantiere rund um die Uhr maximale Sicherheit. Die technisch-baulichen Leistungen umfassten beispielsweise Videosicherheitssysteme mit intelligenter Bildanalyse, Einbruchmeldung, Zutrittskontrolle, unsichtbare Branddetektion, Gefahrenmanagement und nicht zuletzt auch mechanische Ausstattungen. Beim Überschreiten der Grundstücksgrenze werde ein akustischer Alarm inner- und außerhalb

des Hauses ausgelöst und eine umgehende Meldung an die Service- und Notrufleitstelle weitergeleitet. Rückzugsräumlichkeiten seien mit zusätzlicher Sicherheits- und Kommunikationstechnik ausgestattet.

Wolfgang Merken, ZDF, thematisiert in der Zeitschrift PROTECTOR, Mai-Ausgabe, S. 66, Sicherheitsmaßnahmen zum **Schutz vor Stalking** im Medienbereich. Die klassische Post diene nach wie vor als das zentrale Medium, bei dem sich Tendenzen zum Stalking abzeichnen. Elektronische Medien spielten noch eine untergeordnete Rolle. Das Sicherheitsmanagement des ZDF versuche, die Sicherheitsmaßnahmen so zu konzipieren, dass sie verzahnt und ineinander übergreifend die erforderliche Sicherheit erzielen.

Rechenzentrumssicherheit

Performanceeinbußen bei Harddisks infolge der **Geräuschentwicklung bei Löschungen mit Inertgas** thematisiert in der Ausgabe 2-2017 der Zeitschrift Sicherheitsforum, S. 48–51, Roland Matthes, Siemens Building Technologies. Bei einer Inertgas-Löschanlage könnten während einer Auslösung Geräuschemissionen von bis zu 130 Dezibel (dB) entstehen. Dadurch könne es zu Performanceeinbußen oder im Extremfall sogar zu einem Defekt kommen. Ziel einer von Siemens entwickelten **„Silent Extinguishing"-Löschtechnologie** sei eine deutliche Verringerung des Geräuschpegels bei gleicher Löschleistung. Bei der entwickelten „Flüsterdüse" entweiche das Gas nicht über mehrere Löcher, sondern über zwei längliche Rohre mit vielen kleinen Löchern. Dadurch könne die Strömungsgeschwindigkeit bei den Austrittsöffnungen der Röhre verkleinert werden. Auf die „Flüsterdüsen" könne auch ein Schalldämpfer montiert werden. Dadurch werde der Ausströmungsprozess gedämpft und habe gleichzeitig die positive Eigenschaft, dass die hochfrequenten Töne herausgefiltert werden.

Risikomanagement

Den **Faktor Mensch** im Risikomanagement behandelt Dr. Eric Montagne, i-Risk GmbH, in der Zeitschrift Sicherheitsforum, Ausgabe 2-2017, S. 18–21. Aussagen von komplexen quantitativen Risikomanagementsystemen seien mit Vorsicht zu genießen. In der Industrie sei für die Bewertung der meisten Risiken ein qualitativer Ansatz zur Priorisierung der Risiken besser geeignet. **Das qualitative Risikomanagement** baue auf der Intuition und dem Wissen der Mitarbeitenden auf. Untersuchungen der 50 größten Firmenpleiten der letzten Jahre zeigten: Sämtliche Abstürze basierten auf internen Risiken. Der Autor geht auf Interessenkonflikte, auf blindes Vertrauen in Experten, die Beeinflussung durch die Gruppe, irrationale Bewertung von Risiken, Erfahrung des Beurteilenden und auf ein vorgegebenes Werteintervall ein. Für jedes Risiko sollten mehrere Personen in den Bewertungsprozess mit einbezogen werden, denn die Gruppe sei schlauer als der Einzelne. Eine heterogene Gruppenzusammensetzung mit unabhängigen Gruppenmitgliedern helfe, das Know-how jedes Einzelnen zu nutzen.

Schließsysteme

Sylvia Lambach, C.Ed. Schulte GmbH, stellt in der Mai-Ausgabe von PROTECTOR, S. 40/41, die **Schließanlage in der Elbphilharmoni** vor. Sie beherberge nicht nur den Konzertbetrieb, sondern zugleich einen Hotel- und Gastronomiebereich, einen Verwaltungs- und Techniktrakt, private Apartments sowie ein Parkhaus und eine öffentlich zugängliche laza. Diese Vielfalt an Funktions- und Organisationseinheiten und die damit verbundenen unterschiedlichen Zutrittsrechte hätten im Schließsystem abgebildet werden müssen. Es sei eine mehr als 20 DIN A3 Seiten umfassende Schließplanmatrix entstanden, eine Art Konstruktionsvorlage für die spätere Tür-

Schließanlage für rund 2.500 Türen.

Florian Flade berichtet in welt.de am 4. Mai, dass die Bundesanwaltschaft in Karlsruhe einen Schweizer Ex-Polizist in Frankfurt a. M. festgenommen hat, weil er verdächtigt werde, für den **Schweizer Geheimdienst** in Deutschland spioniert zu haben. Konkret gehe es um die Bespitzelung von Steuerfahndern aus Nordrhein-Westfalen. Der Festgenommene soll dabei geholfen haben, deutsche Steuerfahnder ausfindig zu machen, die sich am Ankauf von Schweizer Steuer-CDs beteiligt haben. Möglicherweise habe er sogar einen Informanten in der nordrhein-westfälischen Finanzverwaltung platziert. Sein Auftrag sei es gewesen, eine lückenhafte Liste mit persönlichen Daten von Steuerfahndern aus NRW zu vervollständigen. Die Berner Bundesanwaltschaft ermittele seit zwei Jahren gegen ihn wegen des Verdachts des wirtschaftlichen Nachrichtendienstes. Er soll mehrfach Bankdaten an deutsche Auftraggeber verkauft haben. Die Informationen hätten sich später als gefälscht erwiesen.

Terrorismus

Was tun gegen „schmutzige Bomben"? titelt Dr. Wolfgang Koch, FKIE, in der Mai-Ausgabe des Behörden Spiegel. Der Bundesinnenminister warne immer wieder vor Terroranschlägen mit „schmutzigen Bomben". Im Vergleich zu Nuklearwaffen seien sie leicht herzustellen. Fachleute sprächen von „Improvised Radiological Dispersion Devices", für die sich etwa radioaktive Isotope von Cäsium, Kobalt oder Strontium eignen. Gemäß der Nuclear Threat Initiative vom März 2016 würden viele Anlagen dieser Art als schlecht gesichert und anfällig für Diebstähle gelten. Allein die monetären Folgen radiologischer „Beschaffungskriminalität" betrügen Milliarden Euro. Man spreche von Massenverunsicherungswaffen (Weapons of Mass Disruption). Ein Experimentalsystem, das radiologische Gefährder in einem Personenstrom erkennt und das Sicherheitspersonal auf sie aufmerksam macht, sei der Beitrag des Fraunhofer Instituts FKIE zum deutsch-französischen Vorhaben **REHSTRAIN** (Resilence of the Franco-German High Speed Train Network). Angesichts der terroristischen Bedrohung erforsche dieses Verbundprojekt die Verwundbarkeit des transnationalen Hochgeschwindigkeitssystems. Angestrebt werde ein Assistenzsystem, das die Aufmerksamkeit des Sicherheitspersonals weckt und auf eine radiologische Gefahr lenkt. Die Zuordnung einer radiologischen Gefahr zu einer bestimmten Person gelinge erst durch einen multisensoriellen Ansatz: Mehrere verteilte Gamma-Sensoren werden mit Kameras vernetzt und ermöglichen so eine raum-zeitliche Fusion des durch die Passanten erzeugten Sensordatenstroms. In dichter Folge lieferten alle Gamma-Sensoren Messdaten. Damit werde der Gefahrstoffträger identifiziert. Die Information gehe entsprechend aufbereitet an das Sicherheitspersonal. Bahnhofsszenarien seien nur Beispiele für diese Technologie. Drohnengetragen könne sie radiologische Gefahrstoffe auch in größeren Arealen aufspüren.

Umsatzsteuerbetrug

Die Länder dringen auf Maßnahmen zur Bekämpfung des Umsatzsteuerbetrugs, meldet die FAZ am 17. Mai. Nach Schätzungen von Fachleuten entgingen den deutschen Finanzämtern pro Jahr Einnahmen in Höhe von 800 Mio. Euro, weil beispielsweise Kunden Waren über große Internetplattformen wie ebay oder Amazon bestellen, die Ware aber von chinesischen Händlern versandt wird. Diese umgingen die deutsche Steuergesetzgebung, verschicken die Ware ohne Rechnung und zahlen keine Umsatzsteuer. Firmen aus China sowie aus Hongkong führten Waren mittlerweile im großen Stil zu diesem Zweck in die EU ein. Die Länderfi-

nanzminister wollten das Problem auf ihrer Konferenz am 26. Mai behandeln.

Veranstaltungssicherheit

Dr. rer. pol. Stephan Gundel, Gruner Gruppe, thematisiert in der Zeitschrift Sicherheitsforum, Ausgabe 2-2017, S. 10–13, **Entwicklung und Trends der Veranstaltungssicherheit**. Nur mit einem veranstaltungsspezifischen Sicherheitskonzept sei es möglich, auf die besonderen Eigenschaften, Rahmenbedingungen und Gefährdungen einzugehen. Die zwingende Basissicherheit umfasse grundlegende Maßnahmen zur Arbeitssicherheit und dem Gesundheitsschutz des eingesetzten Personals, zum Brandschutz, Crowd Management und zur Besucherbetreuung, Security sowie Notfallmanagement. Als Trends der Veranstaltungssicherheit bezeichnet der Autor: stark ausdifferenzierte Veranstaltungskonzepte, die zunehmende Bedeutung klarer Organisation und Planung, Vereinfachung durch moderne technische Hilfsmittel sowie Kommunikation und Information als kritische Erfolgsfaktoren.

Videoüberwachung

Modernste Kompressionstechnologie bringt Videoüberwachung in die **4K-Ära**, titelt Hikvision Europe in der Zeitschrift GIT, Ausgabe 5-2017, S. 26–28. Das größte Problem bestehe darin, die Bitrate von Ultra-HD-Videoübertragungen zu senken, ohne die Qualität der 4K-Bilder zu beeinträchtigen. Bei der Videoübertragung müsse ein Gleichgewicht zwischen Bildqualität, Übertragungskapazitäten und Datenanforderungen gefunden werden. H.265+ verwende einen intelligenten Algorithmus, dessen Kodierungstechnologie auf dem Standard H.265/High Efficiency Video Coding (HEVC) basiere. H.265+ optimiere den existierenden Codec besonders bei Videoübertragungen, die bestimmte – im Einzelnen beschriebene – Kriterien erfüllen. H.265+ steigere den Komprimierungsgrad mithilfe von drei Schlüsseltechnologien: prädiktive Kodierung, basierend auf einem Hintergrund- oder Referenzbild, digitale Rauschunterdrückung und langfristige Bitratensteuerung. Diese Technologien werden in dem Beitrag näher beschrieben. H.265+ nutze jedes Bit voll und ganz aus. H.265+ verbessere die Bildübertragung. Ein Netzwerk, das H.265+ einsetzt, besitze zu jedem Zeitpunkt mehr Bandbreite. Mit H.265+ bleibe die Videoqualität gegenüber H.265/HEVC praktisch unverändert. Die notwenige Übertragungsbandbreite und Speicherkapazität würden jedoch erheblich gesenkt.

Hardo Naumann, Accellence Technologies GmbH, befasst sich in der Mai-Ausgabe von PROTECTOR, S. 32/33, mit der **Videoaufschaltung in Leitstellen** für optimalen Service aus der Ferne. In Kundenobjekten seien heute Videoanlagen vieler verschiedener Hersteller verbaut, die oft nicht miteinander kompatibel sind. Mehr als drei bis fünf verschiedene Videosysteme könnten von den Mitarbeitern in der Leistelle nicht mehr effektiv bedient werden. Aus diesem Grund sei auf Initiative der Polizei, des ZVEI, BDSW und BHE die integrative Videomanagementsoftware Ebüs entwickelt worden. Damit würden nicht nur IP-Kameras, sondern auch digitale Videorekorder, Netzwerk-Videorekorder, andere Videomanagementsysteme sowie neuartige Cloud-Lösungen und alle anderen Arten von bildgebenden Systemen integriert.

Wirtschaftsschutz

Wirtschaftsgrundschutz auf Basis des IT-Grundschutzgedankens behandelt Prof. Dr. Timo Kob, HiSolutions AG, in der Ausgabe 2-2017 der Zeitschrift <kes>, S. 6–11. Die grundlegende Idee des Wirtschaftsgrund-

schutzes beruhe auf einem ganzheitlichen Schutzmodell, das nicht nur sämtliche Werte einer Institution abdeckt, sondern für deren Schutz auch alle erforderlichen Funktionen und Bereiche unter einer zentralen Funktion zusammenfasst und steuert. Der Autor stellt die themenübergreifenden Prozesse des Sicherheitsmanagements, des Berechtigungsmanagements und des Sicherheitsvorfallmanagements im Wirtschaftsgrundschutz vor. Geplant oder bereits erstellt seien die Bausteine Basismaßnahmen, Standardmaßnahmen und erweiterte Maßnahmen. Jeder dieser Bausteine sei in die Kapitel Relevanzentscheidung, Gefährdungsübersicht und Maßnahmenbeschreibung unterteilt.

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