Focus on Security

Ausgabe 04, April 2016

SECURITAS

Inhalt

Anschläge

Am 7. März setzten Unbekannte an zwei Kabelkanälen an der **Bahnstrecke Berlin Hbf–Spandau** die darin befindlichen Kabel mittels derzeit unbekannten Tatmitteln in Brand, berichtet das BKA in der Wochenlage am 11. März. Unbekannte hätten unter der Gruppenbezeichnung „Vulkangruppe Festung Europa sabotieren" auf der Internetseite „linksunten.indymedia.org" ein Selbstbezichtigungsschreiben verfasst, in dem sie angeben, dass das Ziel der Aktion gewesen sei, den Personen- und Güterzugverkehr empfindlich zu stören und die Festung Europa von innen zu erschüttern und zu sabotieren. Wie das BKA ausführt, hat es unter der Bezeichnung „Vulkangruppe" in Berlin bereits mehrere Brandanschläge auf Bahnanlagen und auf eine Funkverteileranlage von Vodafone 2013 gegeben.

Wie das BKA in der Wochenlage am 18. März mitteilt, setzten Unbekannte am 15. März an drei verschiedenen Orten in Berlin jeweils ein Fahrzeug der Firma **Bosch** in Brand. Auf der Internetseite „linksunten.indymedia.org" sei ein Selbstbezichtigungsschreiben zu den Taten veröffentlicht worden, in dem der Anschlag in die Begründungszusammenhänge „Antirassismus" und „Antirepression" gestellt worden sei. Am 3. März setzten Unbekannte in Berlin einen Kleintransporter der Firma **Vattenfall** in Brand. Unter der Bezeichnung „ag-hambi love" sei am 8. März auf der Internetseite „linksunten.indymedia.org" ein Selbstbezichtigungsschreiben erschienen, in dem Vattenfall für das „Ausbremsen" des Atomausstiegs in Schweden, den Braunkohletagebau in der Lausitz sowie die „horrenden Strompreise in Berlin" verantwortlich gemacht werde.

Arbeitsschutz

Zum richtigen **Gehörschutz** äußert sich Thomas Ulmer, Berufsgenossenschaft Holz und Metall, in der Zeitschrift GIT, Ausgabe 3-2016, S. 102/103. Die Verantwortlichkeiten eines Arbeitgebers zur Sicherstellung der Schutzwirkung geeigneter Gehörschützer sind in § 8 der LärmVibrationsArbSchV festgelegt. Den jeweils am Ohr vorliegenden Schallpegel unter dem Gehörschutz könne man grob abschätzen. Er errechne sich aus dem Tages-Lärmexpositionspegel, dem Spitzenschalldruckpegel, den Herstellerangaben zur Dämmwirkung und dem zugehörigen Praxisabschlag. Detailinformationen fänden sich im Anhang 1 der DGUV-Regel 112-194. Eine verminderte Dämmwirkung könne verschiedene Ursachen haben: Die Kapsel umschließt das Ohr nicht vollständig. Der Gehörschutz wird nicht genau nach Anweisung eingesetzt. Oder die Otoplastik wird nicht richtig eingesetzt oder sie sitzt schlecht und es treten dadurch Leckagen auf. Derzeit gebe es nur für Gehörschutz-Otoplastiken eine Regelung zur Funktionsprüfung. Anderweitige Verfahren würden zurzeit auf ihre Eignung in mehreren Studien und Projekten untersucht.

Bankingsicherheit

Dirk Losse, HID Global GmbH, befasst sich in der Ausgabe 3-2016 von PROTECTOR, S. 44/45, mit **Sicherheitslösungen für das Online- und Mobile-Banking**. Sichere Authentifizierung des Kunden sei zwar wichtig, sie müsse aber in ein erweitertes, mehrschichtiges Sicherheitsmodell eingebunden werden. Für verschiedene Aktionen sollten unterschiedliche Risikoklassen definiert werden. Parameter, die in eine Risikobewertung eingehen könnten, seien auch der Ort, von dem aus sich der Kunde verbindet, das genutzte Endgerät oder das Verhalten des Internet-Browsers. In Abhängigkeit vom Ergebnis der Risikoanalyse müsse ein geeignetes Sicherheitsmodell dann unterschiedliche Authentifizierungsverfahren unterstützen. Auf mobilen Geräten sollte auch der Einsatz von Soft-Token zur Einmal-Passworterzeu-

gung möglich sein, die auf iOS, Android, Windows 10 Mobile oder anderen Betriebssystemen basieren. Auch die Geräteauthentifizierung sei möglich. Ein weiterer „Layer" betreffe die Transaktionsauthentifizierung, die die Sicherheit für besonders kritische Transaktionen erhöhe. Eine effiziente Implementierung unterschiedlicher Security-Layer erfordere auch eine integrierte und flexible Authentifizierungsplattform mit Threat/Detection-Funktionalität in Echtzeit.

Betriebsausflug-Sicherheit

Mit Sicherheitsfragen im Zusammenhang mit dem Betriebsausflug befasst sich Security insight in der Ausgabe 1-2016, S. 12–15. Nach einem Urteil des BGH vom 8. Oktober 2002 (VI ZR 182/01) muss der Arbeitgeber die Personen, die die Veranstaltung durchführen, „gewissenhaft" auswählen und überwachen. Passiert etwas auf dem Firmenfest, dann greife im Regelfall die gesetzliche Unfallversicherung. Sei aber die Teilnahme an der Veranstaltung nicht für alle Mitarbeiter offen, z. B. bei „incentive events", dann sei allerdings keine automatische Abdeckung des Schadens durch diese Versicherung gegeben. Der Versicherungsschutz ende im übrigen, wenn die Unternehmensleitung oder eine von ihr beauftragte Person den Betriebsausflug für beendet erklärt.

Betriebsanleitung

Mit dem systematischen **Zusammenspiel von Risikoanalyse und Betriebsanleitung** befasst sich Tomislav Matievíc, Tanner Italien, im Sicherheitsforum (Ausgabe 1-2016, S.57–59). Präzise, knapp und zielgruppenorientiert formuliert, seien bereits die ersten Schritte in Richtung einer sicherheitsorientierten Anleitung zurückgelegt. Der Hersteller müsse die Restrisiken, die er nicht konstruktiv oder mithilfe von Schutzmaßnahmen mindern kann, durch die Benutzer-Instruktion auffangen. Ohne Risikobeurteilung sei die Erstellung einer CE-konformen Betriebsanleitung unmöglich. Eine CE-konform erstellte Risikobeurteilung liste zu jeder Gefährdung die zu ergreifenden Schutzmaßnahmen konkret auf. Zwischen Sicherheits- und Warnhinweisen müsse klar unterschieden werden. Sicherheitshinweise zielten auf eine Schulung des Anwenders. Warnhinweise dagegen warnen vor Gefahren. Es habe sich bewährt, Sicherheitshinweise mit allen Restrisiken komplett am Anfang der Anleitung oder in einem separaten Sicherheitshandbuch zusammenzufassen. Um eine „warning pollution" zu vermeiden, sollten Warnhinweise nur dann erfolgen, wenn der Anwender in dieser Situation nicht mit einer Gefahr rechnet oder die Gefahr nicht kennt.

Betrug

Mit **manipulierten Ladenkassen** als einem Massenphänomen befasst sich das Handelsblatt am 2. März. Die Manipulationen seien längst systematisch in allen Bargeld-Branchen. Das sei längst ein Wettbewerbsnachteil für ehrliche Ladentreiber. Im Gastronomiebereich hätten der Steuerfahnder Edo Diekmann und seine Kollegen 2014 in Niedersachsen in 17 Prozent der geprüften Restaurants und Eissalons Manipulationen festgestellt. Im Schnitt aller Betriebsprüfungen habe die Quote bei 3,3 Prozent gelegen. Typisch sei etwa der Fall eines gutbürgerlichen Restaurants in NRW: Für den Gast ziehe der Kellner aus der Kasse eine „Proforma-Rechnung", während in der Kasse ein niedrigerer Betrag für die Buchführung gespeichert wird. Aufwändiger seien Systeme, in denen der Manager am Ende des Tages die Eingaben per Knopfdruck nachträglich ändert und die Kasse neue Tagesendbons erzeuge. 2015 habe das Problem für den Bundesrechnungshof das Stadium eines „systematischen Vollzugsdefizits" erreicht.

Dies – so der Grünen-Finanzexperte Thomas Gambke – verpflichte den Gesetzgeber einzuschreiten. 2008 hätten die Physikalisch-Technische Bundesanstalt und Kassenhersteller das Projekt Insika gestartet. Entwickelt werde ein Smartcard-System, das Umsätze automatisch fälschungssicher speichert. Alle Kassenhersteller könnten es lizenzfrei nutzen. Das BMF habe vorgeschrieben, dass ab 1. Januar 2017 alle Kassensysteme die Umsätze digital aufzeichnen müssen. Manipulierte Registrierkassen fänden sich in allen Bargeldbranchen: Einzelhändler, Tankstellen, Bäcker, Friseure und Taxen, neben Hotels, Gaststätten und Imbissen. Aber auch Akademiker erlägen der Versuchung, Apotheker zum Beispiel.

Der Bundesjustizminister habe den Entwurf für ein „Gesetz zur Reform der strafrechtlichen Vermögensabschöpfung" präsentiert, meldet die WirtschaftsWoche am 18. März. Es solle dafür sorgen, dass **Privatvermögen von Anlagebetrügern** in Zukunft gleichmäßig unter den Geschädigten verteilt wird – in einem klassischen Insolvenzverfahren. Konkret bedeute das: Sobald das Urteil wegen Anlagebetrugs rechtskräftig ist, werden gesicherte Vermögensgegenstände „verwertet" und der Erlös an die Geschädigten „ausgekehrt". Reicht das Geld nicht, um alle Schadensersatzansprüche zu bedienen, beantrage die Staatsanwaltschaft ein Insolvenzverfahren, in dessen Rahmen jeder Anleger einen bestimmten Prozentsatz seines Geldes zurückbekommt.

Brandschutz

Feuerbeständiger Beton ist das Thema von Reto Zanettin, Empa, in der Zeitschrift Sicherheitsforum, Ausgabe 1-2016, S. 27. Polypropylen (PP)-Fasern optimierten die Widerstandsfähigkeit gegen Feuer. Mehr als zwei Kilogramm PP-Fasern pro Kubikmeter selbstverdichtender Hochleistungsbeton (SHB) beeinträchtige aber die Selbstverdichtung. Forscher von Empa hätten nun eine Serie dünnwandiger, mit Drähten aus kohlefaserverstärktem Kunststoff vorgespannter Betonplatten hergestellt. Jede enthalte zwei Kilogramm PP-Fasern pro Kubikmeter Beton. In einige Platten hätten die Forscher zudem eine geringe Menge superabsorbierende Polymere (SAP) gemischt. Nach 90 Minuten der Einwirkung von Feuer mit Temperaturen von bis zu 1.000 Grad habe sich gezeigt: Die mit SAP angereicherten Betonplatten hatten zwar einige Risse, zu Abplatzungen kam es aber nur bei den SAP-freien Betonplatten.

Rauch- und Wärmeabzugsanlagen werden nach den Worten von Alwine Hartwig, VdS, zu einem immer öfter bauaufsichtlich geforderten Teil von Sicherheitskonzepten (GIT, Ausgabe 3-2016, S. 33). Das Berechnungsprogramm für RWA, VdS 2897, mit dem Errichter diese Technik ganz einfach planen und auslegen könnten, sei jetzt überarbeitet worden. Nach Eingabe der geplanten Art der Nutzung, geometrischer Abmessungen und der Art der Brandmeldung erstelle das Programm direkt präzise Vorgaben zur Auslegung der Technik nach den verschiedensten Normen und Richtlinien. Das optimierte Programm beinhalte die neue VdS 2098, die DIN 18232/2 und den neuen Teil 5 sowie zur optimalen Unterstützung bei Änderungen an Altanlagen auch noch die VdS CEA 4020.

Am 31. März meldete die Mitteldeutsche Zeitung, dass bei einem Brand auf dem Areal der Firma Miltitz Aromatics im Chemiepark Bitterfeld-Wolfen am 30. März ein Feuer ausgebrochen sei. Zu der Entzündung an der Isolierung sei es nach dem Auslösen eines Sicherheitsventils bei der Erprobung einer Versuchsanlage gekommen. Durch die Havarie sei Isopren ausgetreten. Dabei handle es sich um eine hochentzündliche Flüssigkeit, deren Dämpfe mit der Luft durchaus explosive Gemische bilden könnten. Starker Wind habe den Grundstoff sehr fein und weiträumig verteilt. Die Flammen selbst seien durch die

Securitas-Werkfeuerwehr schnell gelöscht worden.

Cloud Computing

Je kleiner die mittelständischen Unternehmen, desto größer seien ihre Vorbehalte gegen Cloud Computing wegen Sicherheitsrisiken, mangelnder Kenntnis über Angebote und wegen Unsicherheit über die Standorte der Rechenzentren, schreibt die FAZ am 8. März. Das BMWi wolle die Vorbehalte zerstreuen und habe deshalb ein Technologieprogramm gestartet, das unter dem Projektnamen **„Trusted Cloud Kompetenznetzwerk"** eine unabhängige, gemeinsame Plattform geschaffen habe. 100 Mio. Euro seien für das seit vier Jahren geplante Projekt veranschlagt. Von der eigenen Plattform verspreche sich das BMWi, die vermuteten Sorgen der Unternehmen ausräumen zu können. Angezeigt würden nämlich nur Anbieter, die den Qualitätsrichtlinien des Bundes entsprechen, also deutsche Datenschutzvorschriften einhalten und transparent über ihre Leistungen und Kosten informieren. Bryn Kelly, Rackspace, weist auf den Cloud-Monitor 2015 von Bitkom und KPMG hin, nach dem 60 Prozent der Firmen, die den Private-Cloud-Einsatz planen, Angst hätten vor einem unberechtigten Zugriff auf sensible Daten. Die Studie zeige jedoch auch, dass 85 Prozent der von deutschen Unternehmen registrierten IT-Angriffe nicht im Zusammenhang mit den eingesetzten Cloud-Lösungen stehen. Gerade das Thema Sicherheit sei heute sogar ein Grund, um in die Cloud zu gehen. Vor der Entscheidung für ein Cloud-Angebot sollten Unternehmen aber einiges beachten. Den wohl wichtigsten Punkt bildeten die eingesetzten Sicherheitsmaßnahmen sowie deren Verwaltung und Aktualisierung. Kontrollen sollten von Anfang an in die Produkte und Lösungen integriert werden. Der Aufwand für Compliance und Auditierung könne durch sinnvolle Verknüpfung und Vereinheitlichung von Richtlinien, Standards und Technologien gesenkt werden. Die Unternehmen müssten stabile, sichere und gleichzeitig flexible, erweiterbare IT-Architekturen und Service-Modelle für Cloud Computing einführen. Unternehmen sollten regelmäßig einen frischen Blick auf ihre Sicherheitsprozesse werfen. Denn durch die ständige Weiterentwicklung seien selbst bewährte Ansätze nach einer gewissen Zeit veraltet.

Datenschutz

Rechtsanwalt Dr. Tobias Fuchs, KPMG, hält in einem Verlagsspezial der FAZ am 10. März **Big Data** und Datenschutz für miteinander vereinbar. Allerdings sei nicht alles, was heute in puncto Big Data bereits technisch machbar ist, auch rechtskonform. Das Datenschutzrecht verbiete grundsätzlich alles, was nicht ausdrücklich erlaubt ist. Würden aber personenbezogene Daten anonymisiert und würde ihr Personenbezug ausgeschlossen, sei der unternehmerischen Phantasie keine datenschutzrechtlichen Grenzen gesetzt. Gelockerte Vorgabe würden auch für pseudonymisierte Daten gelten. Wo für Big-Data-Anwendungen noch gesetzliche Erlaubnistatbestände fehlen, bleibe als rechtliche Grundlage die explizite Einwilligung des Betroffenen. Unternehmen müssten Big Data erschließen können und dürfen. Sie sollten jedoch deren Vorteile, aber auch gegebenenfalls drohende Risiken für die Betroffenen klar kommunizieren.

In demselben Verlagsspezial werden Ergebnisse von **Befragungen durch Symantec und BITKOM** wiedergegeben. Danach vertrauen 59 Prozent der befragten Personen im Umgang mit persönlichen Daten den Krankenhäusern, 58 Prozent den Banken, 30 Prozent der Regierung, 24 Prozent dem Einzelhandel und nur 18 Prozent Technikunternehmen sowie neun Prozent Social Media (Datenquelle Symantec). In den letzten zwei

Jahren waren 51 Prozent der Unternehmen von Datendiebstahl, Wirtschaftsspionage oder Sabotage betroffen (weitere 21 Prozent vermutlich betroffen). In einzelnen Branchen waren betroffen: Automobilbau 68 Prozent, Chemie und Pharma 66 Prozent, Finanz- und Versicherungen 60 Prozent, Gesundheit 58 Prozent, Medien und Kultur 58 Prozent, Handel 52 Prozent, IT und Maschinen- und Anlagenbau 44 Prozent, Ernährung 44 Prozent (Datenquelle BITKOM).

Objektüberwachung in Firmen sei sehr stark an Datenschutz gebunden. Diesem Umstand komme nun die neue Software von Panasonic entgegen: Panasonic's Privacy Protection Solution. Das neue System hülle Kunden und Mitarbeiter vollständig in eine Silhouette. Das bedeute, man könne die Bewegungen maskierter Objekte weiterhin sehen und damit gleichzeitig überwachungsbedürftige Areale beobachten. Das Moving Object Removal (MOR) funktioniere wie eine Maske über sich bewegenden Objekten und blockiere die Areale, die man verdecken möchte. Im Kontrast dazu könne man die MOR-Funktion für Areale, die mit hoher Präzision überwacht werden sollen, ausschalten. Auch unmaskiertes Bildmaterial könne im Nachhinein auf Serverseite maskiert werden (GIT, Ausgabe 3-2016, S. 52/53).

Für vollen Objektschutz alles im Blick haben, ohne Rechte zu verletzen, das sei ein wenig die Quadratur des Kreises, argumentiert die Geutebrück GmbH in GIT, Ausgabe 3-2016, S. 54/55. Geutebrück löse dies über eine „Feinjustierung" der Rechte auf Kameraebene, arbeitsplatzabhängig, getrennt für Live- und Speicherbilder, für Speicherbilder mit einstellbarem Zeithorizont, für die Steuerung beweglicher Kameras mit Prioritäten entsprechend Alarm- oder Nutzerlevel, mit Vier-Augen-Passwort. Ein Audit-Trail diene als Revisor-Logbuch. Es protokolliere manipulationssicher alle Aktionen im System und erstelle entsprechende Berichte. Man erhalte also umfassend Antwort auf die Fragen: Wer hat wann, wo, sich an welchem Arbeitsplatz angemeldet? Welche Aktion versucht, wofür er keine Berechtigung hat? Welche Live-Kamera wie lange genutzt? Welche Speicherbilder angesehen? Welche bewegliche Kamera gesteuert? Welche Bilder wohin exportiert? Welche Einstellungen geändert?

Detektion

Um rechtzeitig herauszufinden, ob es sich bei einem stehen gelassenen Gepäckstück möglicherweise um eine Bombe handelt, setzt die Polizei nun auf ferngesteuerte **Roboter mit Hightechsensoren**, die den Inhalt eines verdächtigen Gepäckstücks dreidimensional erfassen können, berichtet die WirtschaftsWoche am 18. März. Entwickelt habe diesen intelligenten Einsatzhelfer das Fraunhofer-Institut für Hochfrequenzphysik und Radartechnik (FHR) in Wachtberg bei Bonn – zusammen mit Wissenschaftlern der Universität Hannover und dem LKA NRW. Das Spannende am fahrenden ferngesteuerten Roboter sei das Gehäuse an seinem Arm. Darin befinde sich neben einer Kamera ein Radarsensor, der erstmals Objekte hochauflösend dreidimensional vermessen könne. Elektromagnetische Wellen würden die Objekte von allen Seiten durchdringen und würden dann zurückgeworfen. Dieses Echo der Strahlen werde ausgewertet. 2019 solle der Roboter auf den Markt kommen.

Drohnen

Security insight befasst sich in Ausgabe 1-2016, S. 38, mit der Geländesicherung durch einen **„Werkschutzkopter".** Wer beispielsweise per Kamera Menschenmassen aus der Vogelperspektive beobachtet, könne viel schneller auf mögliche Gefahren reagieren, als wenn man sich ausschließlich auf die Ordnungsdienste zwischen Zuschauern oder

Demonstrationsteilnehmern verlässt. Das Erkunden von Dachflächen, Behältermanagement, Sichtung von Glutnestern im Brandfall, Ortung von Leckagen und Kontrolle von Sonnenkollektoren oder Schornsteinen gehe mit dem Multicopter schneller und preiswerter. VW ziehe beispielsweise auch in Erwägung, die großen konzerneigenen Parkflächen für Neufahrzeuge aus der Luft zu überwachen.

Einbruchschutz

Für mehr **Sicherheit für Fenster und Türen** plädiert Ulrike Krüger, Schüco International KG, in der FAZ am 9. März. Alle vier Minuten werde irgendwo in Deutschland in ein Haus oder in eine Wohnung eingebrochen. Mit einbruchhemmenden Fenstern, Schiebesystemen und Haustüren lasse sich dem gezielt vorbeugen. Guten Schutz über eine Dauer von mindestens drei Minuten leiste die Widerstandsklasse RC 2 gegenüber Gelegenheitstätern, die mit erhöhtem Werkzeugeinsatz wie zum Beispiel Schraubendreher plus Zange oder einem Keil zur Sache gehen. Mit RC 3 geprüfte Fenster und Türen böten einen verlässlichen Schutz über eine Dauer von mindestens fünf Minuten gegen geübte Gelegenheits- und Gewohnheitstäter, die bei ihren Aufbruchversuchen schweres Werkzeug, etwa einen Kuhfuß plus Zusatzwerkzeuge wie Schraubendreher, Zange oder Keil, einsetzen. Experten der Polizei würden mindestens die Widerstandsklasse RC 2 empfehlen. Moderne Fenster, Schiebesysteme und Haustüren von Qualitätsherstellern seien in RC 2 und höher ausführbar. Die Öffnungs- und Verschlussüberwachung von Fenstern, Türen und Schiebesystemen per profilintegrierter Sensoren sei integraler Bestandteil eines intelligenten Sicherheitsmanagements mit automatisierten Systemlösungen. Zu den vielseitigsten Sensoren zählten hier Magnetschalter für unterschiedlichste Sicherheitsanwendungen von der Anbindung an eine Einbruchmeldeanlage über die Alarmmeldung bei unberechtigter Entriegelung, Öffnung oder Sabotageversuchen.

Die Zahl der **Wohnungseinbrüche** in Deutschland ist nach einem Bericht der Zeitung DIE WELT auf den höchsten Stand seit mehr als 20 Jahren gestiegen. Für 2015 weise die Kriminalstatistik 167.136 erfasste Fälle aus und damit 9,9 Prozent mehr als 2015.

Explosionsschutz

Frühzeitige Branderkennung innerhalb von ATEX-Zonen thematisiert Security insight in der Ausgabe 1-2016, S. 34. Industrietaugliche Brandmelder für den Einsatz unter rauen Umgebungsbedingungen mit Zulassung für den Einsatz in staubexplosionsgefährdeten Bereichen biete die GTE Industrieelektronik GmbH mit der Produktlinie „Adicos". Durch eine frühzeitige Detektion schwelbrandcharakteristischer Brandgase erkenne der staubunempfindliche Brandgasmelder GSME Brände von Kohle, Ersatzbrennstoffen, Biomasse sowie einer Vielzahl weiterer Materialien bereits in ihrer Entstehungsphase. Einsatzbereiche für diese Geräte fänden sich entlang der Förderwege in Kraft- und Hüttenwerken sowie in der chemischen Industrie und in kleinen Silos. In Bereichen, in denen sich Brandgasmelder nicht einsetzen lassen, seien häufig Thermokameras ein probates Mittel zur frühzeitigen Branderkennung. Seit 2016 sei Hotspot als eine der ersten Thermokameras mit Zulassung für den Einsatz in staubexplosionsgefährdeten Bereichen nach ATEX-Zone 20 verfügbar.

„Ex-Bereiche" (also Betriebs- oder Lagerzonen mit prozessbedingter Explosionsgefahr) gelten als besondere Herausforderung für den Brandschutz, heißt es in einem weiteren Beitrag in Security insight, Ausgabe 1-2016, S. 36/37. Mit **BUS-fähigen Ex-Barrieren** würden Hersteller zu einem einfacheren und vor allem effizienteren Brandschutz in

besonders gefährdeten Bereichen beitragen. Ziel sollte sein, auch Brandmelder in explosionsgefährdeten Bereichen der Zone 1 als voll adressierbare Melder einsetzen zu können. So könne über die Brandmeldezentrale jeder Ex-Melder lokalisiert und sein jeweiliger Zustand ermittelt werden. Der Einsatz der BUS-fähigen Ex-Sicherheitsbarriere vereinfache den Betrieb sowie die Wartung eigensicherer Ex-Melder.

Fälschungskriminalität

Der **Handel mit gefälschten Bankkonten** blüht, titelt die FAZ am 11. März. Wer online ein Konto eröffnen will, der muss sich auf einer Postfiliale für das Postident-Verfahren oder im Video-Identverfahren ausweisen. Doch beide Methoden seien wertlos, wenn Kriminelle dabei gut genug gefälschte Ausweise verwenden. Von solchen Fälschungen seien fast alle Geldinstitute betroffen, bei denen Kunden Konten im Internet eröffnen können. Auf mehr oder weniger versteckten Internetforen würden Betrüger Zugangsdaten zu erschlichenen Onlinekonten anbieten, für einen Aufpreis gebe es auch gleich die dazu passende Geld- und Kreditkarte sowie den gefälschten Personalausweis dazu. Das Paket koste zwischen 1.000 und 2.000 Euro. Banken könnten sich dagegen nur begrenzt schützen.

Flottenmanagement

Fernando Pires, Morse Watchmans Ltd., erklärt in Protect, Ausgabe 3-2016, S. 34, wie moderne **Schlüsselverwaltung** zu einem effizienteren Flottenmanagement führt. Für nahezu jeden Aspekt des Flottenmanagements – von der Erfassung und Ausgabe über die Inspektion und Trackingfunktionen bis hin zu Sicherheitsmechanismen und Fernsteuerung gebe es heute Lösungen, die Effizienz zu erhöhen. Eine besonders wirksame Maßnahme sei die automatische Verfolgung, Verwaltung und Verwahrung von Schlüsseln. Dies geschehe idealerweise mit Schlüsseldepots, die jeden Vorgang mit Datum, Uhrzeit und Identität des Benutzers protokollieren. Automatisierte Schlüsselmanagementsysteme erfreuten sich steigender Beliebtheit, nicht nur, weil sie weit akkurater arbeiten als ein manuelles Fahrtenbuch, sondern auch, weil sie wesentlich komfortabler in der Nutzung sind. Funktionen wie beleuchtete Schlüsselschächte und biometrische Zugriffskontrolle machten die Bedienung nutzerfreundlicher.

Gebäudesicherheit

Fünf Schritte zur Gebäudeplanung mit Sicherheitstechnik werden in GIT (Ausgabe 3-2016, S. 60/61) beschrieben: 1. Individuelle Gebäude-Risikoanalyse; 2. Beachtung vorhandener Normen, insbesondere der 2015 überarbeiteten DIN-Norm 50132-7 (Sie decke alle Bereiche von Videoüberwachungsanlagen ab.); 3. Überprüfung von Integrationsmöglichkeiten; 4. grafische Visualisierung, 3-D-Zeichenprogramme würden bereits so früh wie möglich bei der Planung eines Bauprojekts mit einbezogen; 5. Implementierung.

Geldautomatensicherheit

Nach einem Bericht in der FAZ am 10. März erreichte die Zahl gesprengter Geldautomaten im Dezember 2015 mit 43 einen Höhepunkt. Die Banken befassten sich seit längerem intensiv mit Möglichkeiten, solche Sprengungen zu erschweren. Ein Schritt könne sein, dass Hohlräume in Automaten stärker ausgefüllt werden oder eine Automatik die Geldscheine bei Erschütterungen einfärbt. Allerdings sei das mit Kosten verbunden, zudem solle sich bereits ein Markt

für eingefärbte Geldscheine entwickelt haben. Andere Möglichkeiten seien eine stärkere Videoüberwachung oder die Verringerung der Geldbeträge in den Automaten. Für rund 2.000 bis 3.000 Euro würden auch spezielle Gas-Neutralisierungssysteme für Geldautomaten angeboten. Nach einer Antwort der Bundesregierung auf eine parlamentarische Anfrage seien seit dem Jahr 2010 die Täter in 179 Fällen tatsächlich an Bargeld gelangt. Das entspreche etwa einer Erfolgsquote von 37 Prozent. Bei diesen Straftaten seien jeweils zwischen 500 und etwa 380.000 Euro erbeutet worden. Dabei sei im Einzelfall ein Sachschaden zwischen mehreren hundert Euro und etwa einer Million Euro entstanden. Nach Einschätzung der Bundesregierung sei der Einsatz von **Einfärbetechnik** ein geeignetes Mittel. Die Kosten für ein solches System lägen zwischen 2.000 und 3.000 Euro.

Mit neuen Formen des Angriffs auf Geldausgabeautomaten befasst sich auch PROTECTOR in der Ausgabe 3-2016, S. 22–24. Am größten sei das Risiko für Automaten, die in Containern oder Pavillons aufgestellt sind und frei stehen. Der Vorteil der **Verfärbung oder Verklebung von Banknoten** bestehe vor allem in der Nachrüstbarkeit für bestehende Automaten. Allerdings gebe es ein paar Nachteile, so etwa die Unterhaltskosten für die Tintenpatronen oder im Fall einer Auslösung der aufwändige Erstattungsprozess markierter Geldscheine bei der Bundesbank. Es gebe Lösungen, die auf eine Detektierung des einströmenden Gases abzielen und dieses dann neutralisieren. Beim System von TSG würden **Hochspannungsmodule** in den Geldautomaten verbaut, die nach Detektierung von Gas durch eine Fast Response Detection Unit gezündet werden. Hierdurch verpuffe lange vor dem Erreichen einer kritischen Konzentration das Gas. Gleichzeitig werde die Alarmkette in Gang gesetzt. Das System verfüge über eine eigene Stromversorgung im Falle eines Stromausfalls und sei vollständig funktionsüberwacht, sodass bei einer Störung eine Meldung abgesetzt wird.

Geldwäsche

Geldwäscher entkommen fast immer, titelt die FAZ am 29. März. Wenn die Justiz doch mal jemanden erwischt, seien es meist „kleine Fische". „Der Finanzagent als Geldkurier des Betrügers ist das große Massenphänomen bei den eingegangenen Verdachtsmeldungen", stellt das BKA nüchtern fest. „Der Tatbestand der Geldwäsche ist in seiner jetzigen Fassung verfehlt", sagt der Justizminister von NRW Thomas Kutschaty. Er kämpfe daher für eine praktikablere Regelung und für die Einführung eines eigenen Strafrechts für Unternehmen. Nur ein Prozent der Anzeigen kämen von außerhalb des Finanzsektors. Bundesrichter Fischer argumentiere, dass nach schier zahllosen Ausweitungen der Vorschriften fast alles als Geldwäsche gelten könne. Schon eine „leichtfertige" Entgegennahme könne geahndet werden. Selbst Strafverteidiger müssten damit rechnen, dass sie wegen Geldwäsche verknackt werden, wenn sie sich von einem Angeklagten ihr Honorar in bar aus einem Geldkoffer bezahlen lassen. Nach der Rechtsprechung des BGH sei Ziel der Vorschriften die Bekämpfung organisierter Kriminalität. Für das Bestreben, Kriminelle nicht in den Genuss der Tatbeute kommen zu lassen, seien die Vorschriften prinzipiell geeignet, erforderlich und verhältnismäßig (Az: 2 BvR 1520/01). Trotzdem gebe es noch diverse Methoden, Schwarzgeld unauffällig ins legale Wirtschaftsleben zu schleusen.

Gesundheitsdaten

Ralf Zlamal, beratender Datenschutzbeauftragter des Instituts für IT-Recht, befasst sich in einem Beitrag für silicon.de vom 2. März mit dem **Datenschutz** bei Gesundheitsdaten von Beschäftigten. Dienstleister von Gesundheitsportalen und Gesundheits-Apps analysierten das Bewegungsverhalten, das Konsumverhalten und das subjektive Wohl-

befinden ihrer Nutzer. Bereits dieses Angebot werde von Datenschutzbehörden kritisch gesehen, weil es die Preisgabe sehr sensibler personenbezogener Daten darstelle. Die Nutzung eines webbasierten Gesundheitsportals durch den Arbeitgeber sei datenschutzrechtlich unzulässig. Bei einem Hinweis auf ein solches Portal seien folgende Rahmenbedingungen zu beachten: Das Portal müsse rechtlich und technisch vollständig vom Arbeitgeber getrennt sein. Der Arbeitgeber müsse die Beschäftigten darüber informieren, dass es sich bei dem Angebot um eine freiwillige Leistung handelt, die vollständig der Privatsphäre der Beschäftigten zuzuordnen ist. Die Beschäftigten melden sich ausschließlich mit ihren privaten Daten an dem Gesundheitsportal an. Bei der Nutzung von Apps des Gesundheitsportals auf betrieblichen Endgeräten müsse sichergestellt sein, dass der Arbeitgeber keine Informationen erhält. Die generierten Daten dürften nicht für Zwecke des Arbeitgebers verwendet und auch nicht an ihn weitergegeben werden.

Industrie 4.0

Industrie 4.0, d.h. die „Informatisierung" von Fertigungstechnik und Logistik bei der digitalen Kommunikation zwischen den Maschinen, berge enorme Risiken für das produzierende Gewerbe, heißt es in einem Beitrag in Security insight, Ausgabe 1-2016, S. 30/31. Der am stärksten durch digitale Angriffe gefährdete Wirtschaftszweig sei die Automobilindustrie mit 68 Prozent, so der Digitalverband Bitkom. Nur 20 Prozent der von Bitkom befragten Unternehmen meldeten Fälle von Datendiebstahl, Industriespionage oder Sabotage an staatliche Stellen. Die Unternehmen würden dafür als Gründe ihre Angst vor negativen Auswirkungen, einen zu hohen Aufwand sowie geringe Chancen der Aufklärung und Inkompetenz der Sicherheitsbehörden nennen.

Internet der Dinge

In einem Verlagsspezial der FAZ vom 10. März behandelt Prof. Rainer Böhme, Universität Innsbruck, wirksame **Sicherheitsstrategien** für das Internet der Dinge. Es müssten neue und an das Internet der Dinge angepasste Sicherheitstechniken erforscht und standardisiert werden. Die wirtschaftlichen Rahmenbedingungen müssten diejenigen Hersteller belohnen, die sichere Produkte anbieten. Und die Endnutzer könnten die Verantwortung für sicherheitsbewusstes Verhalten nicht an die Hersteller delegieren, denn sie allein würden entscheiden, wann wer welche „Dinge" wie nutzen darf. Dabei zeige sich die Bedeutung einer sicheren Authentifikation. Als technische Lösungsansätze würden selbstlernende Systeme gelten. Diese verhielten sich jedoch weniger berechenbar als Systeme mit festen Regeln. Hinsichtlich der Rahmenbedingungen wäre es ein erster Schritt, die Haftung für fehlerhafte und unsichere Softwareprodukte eindeutig zu regeln und bei digital vernetzten „Dingen" konsequent durchzusetzen. Dies schließe sichere Voreinstellungen und eine kostenlose Bereitstellung von Sicherheits-Updates ein. Diese dürften nicht mit Änderungen der Funktionalität kombiniert werden und müssten die gesamte Lebenszeit der betroffenen Geräte abdecken. Nur eine Kombination aus Technik und Regulierung sowie langfristig die Sozialisation der Nutzer mit der Logik digitaler Sicherheitsmechanismen könne ein kostspieliges Déjà-vu beim Internet der Dinge vermeiden.

IT-Sicherheit

IT-Sicherheit gehört zu den zentralen Themen auf der **Cebit**. Die FAZ weist am 15. März darauf hin, dass dort mehr als 500 Aussteller IT-Sicherheitsprodukte anbieten. Größte Aufmerksamkeit gelte dem autonomen Auto. Mit der dafür nötigen Kommunikationstech-

nik würden die Fahrzeuge zur Außenwelt hin geöffnet und damit einem möglichen Missbrauch durch potenzielle Angreifer ausgesetzt, argumentiert Arne Schönbohm, Präsident des BSI. Die Authentizität der ausgetauschten Nachrichten müsse sichergestellt werden. Um etwa die Kommunikation zwischen Fahrzeugen und Verkehrsleitzentralen abzusichern, treibe das BSI die Entwicklung eines Sicherheitskonzepts mit Verve voran. Zu den ersten Angeboten des neuen Geschäftsbereichs Telekom Security der Deutschen Telekom gehöre eine Produktfamilie namens „Magenta Security". Für Privat-, Geschäfts- und Großkunden solle es jeweils eigene Lösungen geben, die spätestens im Sommer 2016 zur Verfügung stünden. Eine Art Burgmauer um das Unternehmensnetzwerk in Form von Firewalls und Virenscannern reiche nicht mehr. Vielmehr gehe es darum, berechtigte Benutzer von Angreifern zu unterscheiden. Am besten funktioniere dies durch verhaltensbasierte Analysesysteme. Angreifer seien durch ein anomales Verhalten zu erkennen, die bewegten sich im Gegensatz zum normalen Nutzer „seitwärts": Danach suchten sie überall im Unternehmensnetzwerk nach Dateien, in denen sie Passwörter und Nutzerkennungen abgreifen können. Kaspersky Lab wolle verdächtige Vorgänge in einer sicheren Sandbox, also einer isolierten virtuellen Umgebung, analysieren. Und Secusmart wolle mit einer App Spionageaktivitäten über das Handy ein Ende bereiten.

Ab sofort können Admins die **Makro-Funktion von Office 2016** in einem Unternehmen allumfassend blockieren, um so ein beliebtes Einfallstor für Schädlinge zu verbarrikadieren, meldet heise.de am 23. März. Für die Einrichtung stelle Microsoft eine Gruppenrichtlinien-Vorlage zum Download bereit. Eine Warnung nach dem Schließen der „geschützten Ansicht" weise darauf hin, dass ausschließlich ein Admin die Makro-Funktion aktivieren kann.

IuK-Kriminalität

Spear-Phishing sei eine spezielle Angriffsvariante, die gezielt per E-Mail durchgeführt wird. Im Fokus der Angreifer stehen vertrauliche Daten von Unternehmen. Laut einer Befragung des E-Mail-Sicherheitsdienstleisters CLOUDMARK vom Januar 2016 kosteten Spear-Phishingattacken auf ausgewählte Mitarbeiter die Unternehmen in den USA bereits Millionen Dollar, bei größeren Firmen sollen die Angriffe im Schnitt Schäden in Höhe von 1,6 Mio. Dollar anrichten. Vor allem IT-Mitarbeiter (44 Prozent) und Mitarbeiter der Finanzabteilung (43 Prozent) gerieten in das Visier der Phisher. In einem Beitrag im Sonderbericht Wirtschaftsschutz vom 4. März empfiehlt das BSI, auf Spear-Phishing-E-Mails nicht zu antworten und beim vermeintlichen Absender zum Beispiel telefonisch nachzufragen, ob die E-Mail tatsächlich von ihm stammt. Dateianhänge und Links in E-Mails sollten im Zweifelsfall nicht bzw. erst nach Rücksprache mit dem vermeintlichen Absender geöffnet werden.

Im Februar 2016 haben mehrere Varianten ausgereifter **Ransomware** wie „TeslaCrypt", „Locky" oder „CTB-Locker" durch weitreichende Verbreitung öffentlichkeitswirksam auf sich aufmerksam gemacht, berichtet das BSI im Sonderbericht Wirtschaftsschutz am 4. März. Hunderte Webseiten sowie Tausende weitere Systeme von Unternehmen und Privatanwendern gehörten zu den Opfern. Die neue Form von Ransomware ziele darauf ab, den Nutzer durch das Verschlüsseln von Dokumenten, Bildern und anderen Daten zu erpressen. Neuere Varianten verschlüsselten auch Daten auf über das lokale System zugänglichen externen Datenspeichern, Netzlaufwerken und Cloud-Speichern. Häufig handele es sich um sehr professionell gestaltete E-Mails mit vorgeblichen Rechnungsdokumenten im Anhang. Besonders perfide sei, dass Angreifer, wenn das System kompromittiert ist, lokale Adressbücher auswerteten und

Kopien der Ransomware an Kontakte des Anwenders versendeten. Diese erhielten somit E-Mails von einem vertrauenswürdigen bekannten Absender. Welche Auswirkungen ein Befall mit Ransomware haben könne, hänge neben der wirtschaftlichen Belastbarkeit und IT-Abhängigkeit der Geschäftsprozesse der Opfer nicht zuletzt vom Stand der Umsetzung üblicher Maßnahmen der IT-Sicherheit ab. Die regelmäßige Anfertigung von Backups aller wichtigen Daten stelle die wichtigste und letzten Endes einzige zuverlässige Maßnahme dar. Das Wissen aller Mitarbeiter über den korrekten Umgang mit suspekten E-Mails könne in den aktuellen Fällen ein wertvoller Beitrag zum Schutz der Unternehmens-IT darstellen. Netzsegmentierung und eine wohlüberlegte Unterteilung von Netzlaufwerken, Zugriffsrechten und anderen gemeinsam genutzten Ressourcen könne die Schadenswirkung einer lokalen Infektion eindämmen oder begrenzen.

Mit systematischen Cyberangriffen mit dem Ziel der **Spionage** gegen westliche **Hochtechnologiefirmen** befasst sich der BND im Sonderbericht Wirtschaftsschutz am 4. März. Eine aktuell andauernde Cyberspionagekampagne werde von verschiedenen IT-Sicherheitsunternehmen als APT3, Clandestine Fox oder Gothic Panda bezeichnet. Die dahinter stehenden Akteure griffen Hochwertziele an, die über Informationen zu technologischen Innovationen verfügen. Zu den betroffenen Wirtschaftszweigen gehörten die Luft- und Raumfahrtindustrie, der Energie-, Telekommunikations- und Finanzsektor, die Halbleiter- und Computerindustrie, insbesondere für Spitzentechnologie am Weltmarkt bekannte westliche Firmen. Sie nutzten Social Engineering, hätten jedoch auch die Möglichkeit, Datenbestände zu manipulieren und auch die Verfügbarkeit, z. B. von Industriesteuerungssystemen, zu stören.

Auf mögliche bevorstehende Angriffe der **Angriffskampagne Sofacy/APT28** auf Unternehmen der Energiebranche weist das BfV im Cyberbrief Nr. 1-2016 hin. Sie sei seit spätestens 2007 aktiv und stelle derzeit wohl eine der aktivsten und aggressivsten Kampagnen im virtuellen Raum dar. Führende IT-Sicherheitsunternehmen gingen bei Sofacy/APT28 von einer Steuerung durch staatliche Stellen in Russland aus. Aktuell gebe es Hinweise auf Vorbereitungshandlungen der Kampagne für Angriffe auf Ziele in der Energiebranche. Es lasse sich jedoch nicht eingrenzen, welche Unternehmen konkret im Fokus stehen könnten. Dem BfV sei bislang noch kein Fall eines Angriffs auf deutsche Unternehmen der Energiebranche bekannt. Aus eigenen Quellen sei bekannt, dass einige deutsche Forschungsinstitutionen und Unternehmen, vor allem aus dem Bereich Lasertechnologie und Optik, von Sofacy/APT28 betroffen waren. Hintergrundinformationen seien über sensea@bfv.bund.de zugänglich.

Über die **„erste sprechende Erpresser-Malware"** berichtet silicon.de am 7. März. Die Erpressersoftware Cerber „Ransom_Cerber.A" soll die erste Ransomware sein, die bei den Opfern über eine Sprachdatei Lösegeldforderungen stellt. Derzeit spreche Cerber nur Englisch. Cerber weise die Opfer in einer Textdatei aber auch an, den Tor-Browser herunterzuladen und über das gleichnamige Anonymisierungsnetzwerk eine bestimmte Website zu besuchen. Hier böten die Kriminellen den Opfern weitere Sprachen an, darunter auch Deutsch. Die Hintermänner würden ein Lösegeld von 1,24 Bitcoin verlangen, was derzeit rund 523 Dollar entspreche. Als Schutz vor Erpressersoftware empfehle Trend Micro eine als 3-2-1 bezeichnete Backupstrategie. Dabei würden insgesamt drei verschiedene Kopien aller Daten erzeugt, und zwar auf mindestens zwei unterschiedlichen Medien, wobei eine Kopie extern an einem sicheren Ort hinterlegt werde.

Jedes zweite deutsche Unternehmen sei mindestens schon einmal Opfer einer **DDoS**-Attacke gewesen, heißt es bei TECCHANNEL.de am 6. März. Regelmäßig zeigten Studien

die Anfälligkeit gegen diese vergleichsweise einfachen, gleichwohl immer ausgefeilteren Angriffsvektoren auf. Wessen Geschäft hauptsächlich im Betrieb eines Online-Shops und/oder -Services besteht, sei unmittelbar betroffen. Unternehmen, die teilweise auf Cloud-Infrastruktur zurückgreifen, stünden ebenfalls in der DDoS-Schusslinie. Es könne jeden erwischen – jederzeit, unvorbereitet und mit kaum abschätzbaren Konsequenzen.

Das BSI hat einen **Leitfaden zur Thematik Ransomware** veröffentlicht. Seit Dezember 2015 beobachte das Amt große Spam-Wellen, über die massenhaft Ransomware verteilt wird. Dazu werde unter anderem die Infrastruktur des Dridex-Botnetzes verwendet, mittels der vorher Banking-Trojaner verteilt wurden. Daneben gebe es auch vermehrt Meldungen über die Infektion mit Drive by Exploits auf infizierten Webseiten und Werbebannern. Gegenüber Oktober 2015 seien im Februar 2016 mehr als zehnmal so häufig Ransomware durch Virenschutzprogramme in Deutschland detektiert worden. Aus der Sicht der Kriminellen hätten Cyberangriffe mittels Ransomware den Vorteil, dass es zu einem direkten Geldtransfer zwischen Opfer und Täter über anonyme Zahlungsmittel wie Bitcoins oder anonymen Guthaben- und Bezahlkarten kommt. Im Vergleich zu Cyberangriffen über Banking-Trojaner seien weder Mittelsmänner für Überweisungen noch Waren-Agenten notwendig, um einen erfolgreichen Angriff zu monetarisieren. Für das Opfer habe der Angriff ganz konkrete Konsequenzen. Hier verhindere oder erstatte keine Bank den Schaden. Das BSI stellt in dem Leitfaden konkrete Hilfen für die Prävention und die Reaktion im Schadensfall bereit. Das Amt beschreibt verschiedene Präventionsmaßnahmen: die Verhinderung einer Infektion, Backups und Datensicherungskonzepte, Awareness, Maßnahmen zur Verhinderung der Ausführung unerwünschter Software, Erkennung von Ransomwaredateien auf Fileservern, einen zentralen Logserver, Schwachstellenscan und Penetrationstests. Das BSI behandelt Reaktionsmaßnahmen: Lösegeldforderung, Anzeigenerstattung, Incident Response und externe Expertise.

Antiviren-Experten von F-Secure haben sich, wie heise.de am 30. März meldet, die von **Exploit-Kits** ausgenutzten Sicherheitslücken angesehen. Nach dem Ergebnis hätten sich unter den Top 15 der Schwachstellen-Hitparade allein 13 Lücken in **Adobes Flash** gefunden. Die hauptsächlich für das Abspielen von Videos genutzte Browser-Erweiterung dürfte damit für mehr Infektionen von Computern mit Schadprogrammen verantwortlich sein als alle andere Software zusammen. Exploit-Kits seien das Mittel der Wahl, um Besucher einer Web-Site bereits beim Öffnen der Seite im Browser zu infizieren. Sie testeten mit passenden Skripten im Hintergrund, welche Browser-Version mit welchen Erweiterungen sie gerade vor sich haben. Findet sich im Repertoire ein dazu passender Exploit, werde damit die von den Kriminellen vorgegebene Schadsoftware installiert. Oft handele es sich dabei um Online Banking-Trojaner oder Ransomware. Das alles geschehe unbemerkt im Hintergrund.

Kfz-Aufbruch

Heise.de meldet am 17. März, der ADAC habe überprüft, wie leicht sich aktuelle Pkw-Modelle durch einen **Mißbrauch des „Keyless Entry"-Systems** aufschließen und starten lassen. Das erschreckende Ergebnis: Alle 24 untersuchten Fahrzeuge seien anfällig. Die erforderliche Hardware habe sich der ADAC für wenige hundert Euro selbst gebaut. Betroffen seien Fahrzeuge zahlreicher namhafter Hersteller wie Audi, BMW, Ford, Renault, Opel und VW.

Das Magazin Focus befasst sich am 19. März mit dem **Diebstahl von Navis**. Der boome bundesweit. Experten schätzten den Schaden auf einen dreistelligen Millionenbereich.

In Berlin seien 2015 knapp 6.000 Wagen aufgebrochen worden, in Köln habe die Polizei 1.354 Fälle registriert. Mit einfacher Hacker-Software aus dem Internet gelinge es Banden offenbar, die PIN-Codes der Navis zu überlisten. Besonders viele Kfz-Aufbrüche begingen litauische Banden. In der Heimat würden die Verbrechersyndikate meist junge Leute anwerben, sie bei hiesigen Residenten in Wohnungen unterbringen und sie auf Diebestour schicken. Den besten Schutz vor Autoknackern, so verrate der Kölner Chef des Bundes Deutscher Kriminalbeamter, böten mobile Alarmanlagen oder das gute alte Babyphone.

Kommunikationssicherheit

Ziel von Angriffen auf Telefonanlagen sei es, die telefonische Verfügbarkeit ausgewählter Teilnehmer über die Dauer einer solchen Attacke stark einzuschränken oder gänzlich zu blockieren, berichtet der BND im Sonderbericht Wirtschaftsschutz am 4. März. Als ein Angriffswerkzeug habe **SKYPE** identifiziert werden können. SKYPE biete den Angreifern durch Verschleierung ihrer Identität guten Schutz vor Entdeckung und lasse sie nun auch nicht mehr vor Angriffen gegen Telefonsysteme von Betreibern kritischer Infrastrukturen zurückschrecken. Auch der Aufbau von Telefonkonferenzen als Angriffsvariante sei mit SKYPE denkbar einfach. **TDoS**-Angriffe über SKYPE zu generieren, stelle für potenzielle Täter eine relativ einfache Möglichkeit dar, um großen Schaden zielgenau in einem gewollten Zeitfenster zu realisieren.

Krankenhaussicherheit

Seit Anfang 2016 sei es zu einer signifikant hohen Anzahl an erfolgreichen Cybersabotageangriffen gegen Krankenhäuser in der westlichen Welt gekommen, berichtet der BND im Sonderbericht Wirtschaftsschutz am 4. März. Die Angriffe auf deutsche Krankenhäuser ließen auf einen Zusammenhang mit der Erpressersoftware GPCODE schließen. Die Angriffe fänden in der Regel über die für Schadsoftware bekannten Infektionswege statt. Den Tätern komme entgegen, dass die Verantwortlichen in Krankenhäusern durch die öffentliche Wahrnehmung und den steigenden Kosten beim zögerlichen Agieren relativ leicht zum Nachgeben bereit seien.

Kreditkartenbetrug

Apple und Banken unternähmen nicht genug, um das Hinzufügen von gestohlenen Karten zum Apple Pay-Account zu unterbinden, moniert nach einer Meldung von heise.de vom 3. März ein Sicherheitsforscher. Im Unterschied zu Android Pay und Samsung Pay sei bei Apple Pay das ungehinderte Durchprobieren der Kartenprüfnummer möglich.

Krisenmanagement

Martina Teixeira und Duarte Gouveia, ANA-Aeroporto de Lisboa, beschreiben in GIT, Ausgabe 3-2016, S. 28–30, das von einem Team der ANA-Aeroporto de Lisboa Portela und anderen Unternehmen entwickelte **Managementtrainingstool CRISIS**, das auf Basis einer virtuellen Simulation alle erdenklichen Krisen- und Ausnahmesituationen darstellen könne. Es ermögliche, komplexere Krisensituationen auch in kurzen Abständen zu simulieren. Die virtuelle Umgebung von CRISIS basiere auf dem Grafik- und Animationsprogramm 3ds Max. Es sei in der Lage, Gebäude, Fahrzeuge und Personen naturgetreu nachzuempfinden. Aufgrund der flexiblen Programmierung lasse sich jede gewünschte Umgebung detailliert am Rechner nachbauen. Im Verlauf der Simulation veränderten sich durch die Handlungen der Teil-

nehmer immer wieder die Programmparameter und somit die Situation. Das umfangreiche Datenmaterial und der schnelle Zugriff darauf ermöglichten es den Teams, ihren Fokus auf das Sammeln von Wissen und Erfahrung zu legen, wodurch u. a. die Fähigkeiten zur Problemdiagnose, Planung und Teamkoordination gestärkt würden, anstatt vorgegebene Abläufe lediglich einzuüben.

Krisenregionen

Das Institut für Wirtschaftsschutz und Sicherheitsforschung (IWiS) hat ein Positionspapier veröffentlicht, das die Risiken für deutsche Unternehmen in ausgewählten **afrikanischen Ländern** analysiert, um als Grundlage für eine eventuelle Investitionsentscheidung zu dienen, berichtet Security insight in der Ausgabe 1-2016, S. 46. Die Studie „Marktchancen in Afrika 2015 – Potenziale für den deutschen Mittelstand" des Afrika-Vereins der deutschen Wirtschaft sei dabei Referenzrahmen für die Auswahl der Länder gewesen, deren Sicherheitslage das Positionspapier beleuchtet (Südafrika, Nigeria, Ghana, Marokko, Algerien, Angola, Tunesien, Ägypten, Mosambik, Tansania, Äthiopien, die Elfenbeinküste, Kenia und Namibia). Das Positionspapier ist kostenfrei herunterzuladen auf www.iwis-institut.de.

Kritische Infrastrukturen

Almut Eger, 4m2s, und Jörg Kretzschmar, Contechnet Ltd., beleuchten in der Ausgabe 1-2016 der Zeitschrift Sicherheitsforum, S. 28–32, IT-Sicherheit bei kritischen Infrastrukturen unter der Kosten- und Effizienz-Lupe. Sie sehen die Investition in IT als Teil einer integrierten Sicherheit, untersuchen unternehmenskritische Faktoren, bewerten hohe Awareness und intelligente Software als Schritte zu mehr Informationssicherheit. In Deutschland sei seit 2015 ein Tool auf dem Markt, das explizit die Forderungen des ISO/TEC 27001 und des BSI IT-Grundschutzes mit den Katalogen 100-1 bis 100-4 abdeckt. Die ersten Praxistests seien vielversprechend. Es existiere auch ein Tool, das nicht nur im Aufbau, sondern auch im Betrieb eines ISMS fortlaufend Auskunft über den aktuellen Stand und die weitere Entwicklung der Informationssicherheit gibt.

Lebensmittelfälschung

Polizeidienste haben nach einer Mitteilung von EUROPOL von November bis Februar in 56 Ländern mehr als 100.000 Tonnen und eine Million Liter gefälschter Lebensmittel sichergestellt, meldet die FAZ am 31. März. Kriminelle Banden hätten gewaltige Profite erzielt.

Leitstellenvernetzung

Monika Rech-Heider, Fachverband Leitstellen e. V., plädiert in PROTECTOR, Ausgabe 3-2016, S. 42/43, für vernetzte und integrierte Industrieleitstellen. Der Fachverband Leitstellen e. V. kritisiere nicht nur die Diversität in den Leitstellen, sondern auch die nicht einheitlich geregelten Ausbildungswege der Disponenten. Heute sei es „state of art", die Gewerke der Werksfeuerwehr und des Werkschutzes in einer integrierten Leitstelle zusammenzufassen und automatisierte Prozesse zu definieren. Alle physikalischen Sicherheitssysteme wie Brand- und Gaswarnmelder, Zutritts- und Wächtersysteme, Anlagen der Gebäudetechnik, Kameras und Kommunikations-, Alarmierungs- und Benachrichtigungssysteme müssten auf einer einheitlichen Plattform zusammengeführt werden.

Logistiksicherheit

Supply Chain Security gilt als eine der wesentlichen Säulen im Risikomanagement eines Unternehmens, ist das Institut für Wirtschaftsschutz und Sicherheitsforschung (IWiS) überzeugt (Security insight, Ausgabe 1-2016, S. 54/55). Unternehmenssicherheit sei unter anderem auf sichere, störungsfreie und störungsarme Produktionsverhältnisse, auf Soll-Bestände der Rohstoffe und Halbfertigerzeugnisse, auf Soll-Bestände der Fertigprodukte, auf den Schutz des Transports und der Lagerung durch zertifizierte oder anderweitig geprüfte Unternehmen sowie auf zeitgerechte und vollständige Lieferung fokussiert. Der Ladungsdiebstahl habe nach Auswertung von Statistiken von TAPA EMEA (Transportes Asset Protection Association Europe, Middle East, Africa) erheblich zugenommen, 2014 allein in Deutschland um 42,5 Prozent. TAPA schätze den jährlichen Schaden durch Ladungsdiebstahl auf etwa 8,3 Mrd. Euro.

Luftverkehrssicherheit

Der Transport von **Lithium/Ionen-Akkus** im kommerziellen Frachtgut auf Passagierflügen soll ab April verboten werden, meldet spiegel.de am 26. Februar. Das habe die ICAO beschlossen. Lithium/Ionen-Batterien sind unter anderem in Laptops und Smartphones verbaut. Passagiere dürfen die Akkus weiterhin im Handgepäck in die Kabine mitnehmen und es im großen Gepäck verstauen, das im Frachtraum transportiert wird. Hintergrund der Entscheidung der UNO-Sonderorganisation seien Sorgen um eine Feuergefahr durch die Batterien. Der Beschluss der ICAO sei nicht bindend. Die meisten UN-Mitglieder folgten jedoch den Vorgaben der Behörde.

Marktmissbrauch

Wie die WirtschaftsWoche am 24. März berichtet, regelt vom 3. Juli an eine EU-Verordnung gegen Marktmissbrauch, was börsennotierte Unternehmen melden müssen. Melden müssen sie auch Zwischenschritte (etwa beim bevorstehenden Rückzug des Firmenchefs) bis zu einer kursrelevanten Entscheidung innerhalb von drei Tagen. Manager dürfen innerhalb von 30 Tagen vor der Veröffentlichung eines Jahres- oder Quartalsberichts nicht mit Aktien ihres Unternehmens handeln. Auch Unternehmen, die im Freiverkehr gehandelt werden, müssen künftig Aktiengeschäfte ihrer Manager melden und ein Insiderverzeichnis führen. Zu den Insidern zählen auch Wirtschaftsprüfer, Rechtsanwälte und Steuerberater, die im Auftrag des Unternehmens arbeiten. Ein unzulässiges Insidergeschäft besteht schon darin, dass ein Insider eine Order wegen einer unveröffentlichten Information storniert oder ändert. Künftig ist auch der Versuch der Marktmanipulation strafbar. Die Sanktionen bei Verstößen gegen das Marktmissbrauchsrecht werden verschärft. So gelte beispielsweise bei Verstößen gegen die Pflicht von ad hoc-Meldungen eine Mindeststrafe von einer Million Euro für einzelne Personen. Bei Unternehmen könne die Strafe bis zu 15 Prozent des Umsatzes betragen.

Maschinensicherheit

Andreas Schenk, steute Schaltgeräte GmbH & Co. KG, und Walter Steinemann, Carl Geisser AG, zeigen in der Ausgabe 3-2016 der Zeitschrift GIT (S. 94/95), dass mit einem **Sicherheits-Funkfußschalter** die Ergonomie verbessert und die Verfügbarkeit der Anlage erhöht wird, weil keine Leitungen beschädigt werden. Wegen der hohen Zuverlässigkeit, die u. a. durch das „Frequency Hopping Spread Spectrum" auf 79 Kanälen und durch

das adaptive Frequenzsprungverfahren gewährleistet sei, sowie aufgrund der sehr guten Koexistenz zu anderen Funksystemen eigne es sich insbesondere für den Einsatz in rauen industriellen Umgebungen. Fußschalter und Auswerteeinheit ließen sich eindeutig zuordnen, sodass mehrere sichere Fußschalter parallel in einem Funkbereich arbeiten könnten. Die Energieversorgung der Fußschalter erfolge batteriegestützt. Das schaffe die Voraussetzung für eine hochverfügbare direktionale Funkverbindung.

Intelligente Lichtgitter für sichere Maschinen werden in Ausgabe 3-2016 der Zeitschrift GIT (S. 96/97) vorgestellt. Mit neuartigen Lichtgittern auf der Basis von openSAFETY ermögliche die Ethernet Powerlink Standardization Group (EPSG) völlig neue Sicherheitskonzepte für die moderne Fertigung. Als erster Hersteller werde Datalogic 2016 ein netzwerkbasiertes Lichtgitter auf Basis des neuen Profils auf den Markt bringen. Das intelligente Lichtgitter werde direkt an das Echtzeitnetzwerk Powerlink angeschlossen. Das darauf aufsetzende Sicherheitsprotokoll openSAFETY ersetze die bisher notwendige Hartverdrahtung des Lichtgitters. Einen einfacheren Weg böten Lichtgitter mit Einzelstrahlauswertung. Aus der Information, welcher Lichtstrahl zuerst durchbrochen wird, lasse sich die Richtung bestimmen, aus der das Produkt kommt. Die Sicherheitssteuerung stelle fest, ob exakt das erwartete Produkt durch das Lichtgitter fährt. Bei einer Automatisierungs-Lösung mit openSAFETY-Lichtgitter werde das „Muting" einfach in der Automatisierungs-Software programmiert. Besonders bei Seriengeräten werde mit dem openSAFETY-Lichtgitter der Arbeitsaufwand bei der Inbetriebnahme erheblich verringert. Mussten Fehlermeldungen bisher mühsam von blinkenden LEDs abgelesen und interpretiert werden, könne der Bediener nun alle Diagnoseinformationen im Klartext abrufen.

Mitarbeiterkriminalität

Amazon habe sich in den USA eine besondere Strategie ausgedacht, um Diebstähle durch Mitarbeiter zu bekämpfen, berichtet die FAZ am 10. März. Während die Arbeiter morgens anstehen, um sich zum Dienst einzustempeln, müssten sie sich an manchen Standorten neuerdings auf Videoscreens ansehen, wie ehemalige Kollegen entlassen wurden, weil sie auf frischer Tat beim Stehlen ertappt wurden. Die Beschuldigten würden zwar nicht mit Namen genannt und nur von einer schwarzen Silhouette repräsentiert. Doch die Nachricht sei eindeutig: Über jeder der Silhouetten prange das Wort „terminated" – gekündigt. Gestohlen worden seien DVDs, ein iPad, Schmuck, ein Feuerzeug, Make-up, eine Mikrowelle, Handyhüllen oder Videospiele.

Notrufsystem

Die deutsche Versicherungswirtschaft habe mit „Unfallmeldedienst" ein automatisches Notruf-System entwickelt, das in nahezu allen Autos eingesetzt werden könne, berichtet silicon.de am 17. März. Der Stecker für den Zigarettenanzünder erkenne Zusammenstöße und Aufprallstärke durch Beschleunigungssensoren. Per Smartphone-App informiere er eine Notrufzentrale, zugleich werde eine Sprechverbindung hergestellt. Ab 4. April würden viele Autoversicherer ihren Kunden diesen Stecker anbieten. Ein nachrüstbarer eCall-Adapter funktioniere im Zusammenwirken mit einer Smartphone-App. Die Versicherer würden versprechen, dass das Smartphone nur wenige Daten übermittelt – und dies ausschließlich nach einem Unfall oder einem manuell veranlassten Hilferuf. Es sei mit dem Unfallmeldedienst unmöglich, Rückschlüsse auf die Fahrweise zu ziehen oder Bewegungsprofile zu erstellen.

Perimeterschutz

Andreas Wolf, Dallmeier electronic GmbH & Co. KG, plädiert in GIT, Ausgabe 3-2016, S. 46–48, für die **Kombination von Multifocal-Sensortechnologie und Wärmebildkameras**. Es gehe beim Perimeterschutz meist um sehr lange Distanzen. Panomera sei eine von Dallmeier entwickelte Kameratechnologie, die insbesondere für die Überwachung und Absicherung größerer Areale und langer Strecken geeignet sei. Die ausgeklügelte und bereits patentierte Anordnung von optischen Sensoren sorge dafür, dass der zu überwachende Bereich von nur einem Standort aus mit gleichbleibender Bildauflösung, hoher Dynamik und durchgehender Tiefenschärfe überwacht werden kann. Bei der Multifocal-Sensortechnologie erfolge die Konfiguration automatisch, weil 3-D schon in der Panomera verbaut ist, damit werde das Sicherheitsproblem der manuellen Konfiguration eliminiert. Die Kopplung von Panomera und Wärmebild böte für die aktive Perimeter-Überwachung eine ideale Kombination. Die Verknüpfung beider Technologien habe das Ziel, die Schwachpunkte durch die jeweils andere Technologie aufzufangen. Thermal-Sensoren erreichten im Sinne der Videoanalytik dann ihre Grenzen, wenn die unmittelbare Umgebungstemperatur nahezu identisch zum Objekt ist und die Absolut-Temperaturdifferenz sehr hoch ist, sodass wenige Grauwerte pro Grad Differenztemperatur zur Verfügung stehen. Das Quality of Video Modul erfasse verschiedene Messwerte im Video und ermittele daraus u. a. Schärfemaße, Kontrastverhältnisse und Sichtbarkeitsmerkmale sowie im Fall von Thermal-Sensoren auch die gemessenen Temperaturbereiche.

Rechenzentrumssicherheit

Ines Pettigrew, Tyco Integrated Fiore & Security Deutschland, behandelt in der Ausgabe 3-2016 der Zeitschrift PROTECTOR, S. 46/47, **Sicherheits- und Brandschutzsysteme** in Rechenzentren. Für die Branddetektion sei in Serverräumen ein Ansaugrauchmelder die ideale Lösung. Er sorge auch bei einer hohen klimatisch bedingten Luftwechselrate für eine genaue Detektion. Das sei umso wichtiger, weil die moderne Technik auch Falsch- und Täuschungsalarme und damit teure Betriebsunterbrechungen vermeide. Neben den reinen IT-Serverräumen mit den Server Racks sollte der Brandmelder als drei-Kriterienmelder für Rauch, Wärme und Kohlenmonoxid sowie der CO-Brandmelder für die weitere Gebäudeperipherie eingesetzt werden. Gaslöschanlagen seien immer dann das Mittel der Wahl, wenn absolut rückstandsfrei gelöscht werden muss. Aber auch Wassernebel-Anlagen kämen in Rechenzentren zum Einsatz, zum Beispiel in den Zwischenböden und direkt an den IT-Serverracks. Ein Physical Security Information Management System (PSIM) könne die Zusammenführung und Auswertung der Alarmdaten unterstützen.

Rittal sorge für sichere und **intelligent gekühlte IT** bei Prosegur, argumentiert Christian Ludwig, Rittal, in der Zeitschrift GIT, Ausgabe 3-2016, S. 70–72. Zu dem innovativen Klimakonzept gehörten die Rittal LCP Rack Kühlgeräte. Diese seien seitlich am Rack montiert und bildeten einen eigenen Luftkreislauf zur Kühlung der IT-Komponenten. Das LCP kühle die Luft über den Luft/Wasser-Wärmetauscher und blase die kalte Luft an der Vorderseite der Server wieder aus. Die Kühlung erfolge unabhängig von der Umgebungsluft im Rechenzentrum. Damit es gar nicht erst zu einem größeren Feuer kommt, nutze Prosegur das Brandmelde- und Löschsystem DET-AC von Rittal. Die Produktfamilie bestehe aus einer Brandfrüherkennungsanlage sowie einem Aktivlöschsystem. Sobald eine Rauchentwicklung entdeckt wird, starte ein mehrstufiger Alarmierungsprozess, der im Brandfall zu einer Flutung des Serverschranks mit dem Löschmittel NOVEC 1230 führen würde.

Schließsysteme

Mechanische und elektronische Zutrittskontrolle thematisiert PROTECTOR in der Ausgabe 3-2016, S. 26/27. **Elektronische Zutrittssysteme** bestünden zum einen aus bewährten mechanischen Elementen, und zum anderen erleichterten hochentwickelte Technologien wie Funk und RFID das Programmieren und die tägliche Benutzung. Der Zugang könne durch einen Chip, einen Schlüsselanhänger oder eine Karte gewährt werden. Für die Türverriegelung werde ein selbstverriegelnder Mehrfachverschluss mit Notausgangsfunktion „Panik E" benötigt, damit der automatische Riegelausstoß nach dem Ein- oder Austritt eines Bewohners erfolgt. Die Freischaltung des Drückers und dem somit verbundenen Riegeleinzug übernehme ein auf Einbruchschutz geprüfter Funkbeschlag. Komplettiert werde das System von einem an die Türsprechanlage angebundenen Input-/Output-Modul.

Sichere **Funktechnik zur Türsteuerung** thematisiert PROTECTOR in der Ausgabe 3-2016, S. 30/31. Sichere Funksignale würden vor der Übertragung verschlüsselt. Nur der berechtigte Empfänger könne das chiffrierte Signal wieder entschlüsseln. Die Gretsch-Unitas-Gruppe setze dabei auf eine sehr sichere AES 128-Bit-Verschlüsselung. Bei den Funklösungen des Unternehmens würden Sender und Empfänger gegenseitig miteinander „reden". Schickt also der Nutzer mit dem Handsender ein Signal an das Türmodul, öffne dieses nicht direkt das Schloss, sondern antworte dem Sender. Erst nach einer Bestätigung werde der Befehl ausgeführt.

Schnelllauftore

GIT thematisiert in der Ausgabe 3-2016, S. 98/99, **Torsicherheit per Lasertechnologie**. Innerhalb der dynamischen Erfassungszone reagiere der Laserscanner wie ein schneller Impulsgeber: Wird ein bewegtes Objekt erfasst, löse der Scanner im Bruchteil einer Sekunde aus und das Tor öffne sich. Die Geometrie und Logik dieser Erfassungszone könne vor Ort mit einer Fernbedienung bis maximal 10 x 10 Metern individuell programmiert werden. Der Scanner detektiere jede Bewegung und werte dabei unter anderem auch Entfernung, Richtung und Geschwindigkeit aus, um für einen „punktgenauen" Öffnungsimpuls zu sorgen. Dieser erfolge jedoch nicht, wenn Fahrzeuge oder Menschen lediglich entlang der Fassade passieren. Komplexe Softwarelogarithmen verhinderten, dass der Scanner durch Regen, Schnee oder Fremdlicht fehlausgelöst werden kann. Durch 16.000 Messungen in der Sekunde entgehe dem Laserscanner nichts.

Sicherheitsgewerbe

Fünf wesentliche Herausforderungen sieht Manfred Buhl, Securitas Deutschland, im Jahr 2016: den leergefegten Arbeitsmarkt, den Schutz von Flüchtlingen und ihren Unterkünften, die Luftverkehrssicherheit, die Integration von Sicherheitstechnik in ganzheitliche Sicherheitslösungen und die Durchsetzung von besseren politischen und rechtlichen Rahmenbedingungen (Security insight, Ausgabe 1-2016, S. 28/29).

Social Engineering

Mit der Problematik befasst sich die FAZ am 3. März. Es sei schwierig zu erkennen, wenn Kriminelle falsche Identitäten einschließlich zugehöriger Profile in sozialen Netzwerken anlegen, um gezielt das Vertrauen von Personen zu gewinnen und sich so beispielsweise Zugangsdaten zu IT-Systemen verschaffen. Bereits beim Abschluss des Arbeitsvertrages sollte sich ein Unternehmen gegen solche

Angriffe schützen, etwa durch Aufnahme weitreichender Vertraulichkeitsverpflichtungen in die Formulararbeitsverträge. Besonders gefährdete Arbeitnehmer könnten zudem verpflichtet werden, auch allgemeine Informationen nicht öffentlich preiszugeben. Ein entscheidender Baustein bei der Abwehr sei die Sensibilisierung der Beschäftigten. In der Praxis etabliert hätten sich auch **„Social Engineering Audits",** mit denen gezielt Sicherheitsrisiken aufgedeckt werden sollen. Die Durchführung eines solchen Praxistests bedürfe an sich zwar nicht der vorherigen Zustimmung des Betriebsrates. Sofern hierbei jedoch Daten durch technische Einrichtungen erhoben werden, müsste der Betriebsrat dies absegnen. Inwieweit Mitarbeiterdaten im Rahmen solcher präventiver Audits verarbeitet werden dürfen, sei umstritten. Erklärtes Ziel müsse die Aufdeckung systemischer Schwachstellen sein, nicht die Ermittlung unzulässiger Verhaltensweisen einzelner Mitarbeiter. Heimliche Tonaufnahmen seien sogar strafbar.

Spionage

Russische nachrichtendienstliche elektronische Angriffe gegen deutsche Ziele zeichnen sich durch eine hohe technische Qualifikation aus, berichtet das BfV im Sonderbericht Wirtschaftsschutz am 4. März. Schwerpunkte der Know-how-Abschöpfung lägen in den Bereichen Energie-, Militär-, Röntgen- und Nukleartechnik sowie Luft- und Raumfahrt. Das technische Know-how zeige sich in einer großen Bandbreite schwer zu detektierender Angriffsvektoren. Sie umfasse E-Mails mit Schadanhang oder Links zu Webseiten mit Schadcode, USB-Sticks, Phishing-Seiten, Watering Holes oder infizierte legitime Webseiten. Spear-Phishingangriffe zeichneten sich durch gutes Social Engineering der auf das Opfer zugeschnittenen E-Mails aus.

Claudia Körmer Mag., Fachhochschule Campus Wien, und Astrid Hofer, Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (Österreich), analysieren im Sicherheitsforum (Ausgabe 1-2016, S. 14–18) die Ergebnisse einer **Befragung von 1.100 Firmen** zur Wirtschafts- und Industriespionage. Rund fünf Prozent der Befragten hätten angegeben, in den letzten fünf Jahren mindestens einmal Opfer von Wirtschafts- und Industriespionage gewesen zu sein. Rund drei Viertel der Betroffenen haben weniger als 250 Mitarbeiter. In fast der Hälfte der Fälle würden die Täter von den Befragten unter den Mitbewerbern vermutet. Nachrichtendienste oder Kunden würden mit jeweils knapp neun Prozent wesentlich seltener als Täter genannt. Als Gründe, warum nach einem Spionageverdacht keine Behörde verständigt wurde, hätten 58 Prozent die mangelnde Beweislage gegenüber dem Täter, 45 Prozent eine geringe Erwartungshaltung gegenüber einer Verurteilung, 28 Prozent fehlendes Vertrauen zu Strafverfolgungsbehörden und 24 Prozent Unkenntnis, ob Spionagefälle strafrechtlich verfolgt werden, angegeben. In nur rund der Hälfte der befragten Unternehmen seien sensible Informationen identifiziert worden, deren Verlust einen großen materiellen oder immateriellen Schaden nach sich ziehen könnte, und in nur einem Drittel seien schützenswerte Güter als solche deklariert und schriftlich festgehalten worden. Neun von zehn Unternehmen gäben an, keine Behörden zu kennen, die proaktive Unterstützung anbieten.

Stadionsicherheit

In der Ausgabe 1-2016 des DSD, S. 28/29, plädiert Hendrik Große Lefert für eine spezifische Qualifizierung von Personen, die als Ordner in Fußballstadien eingesetzt werden. Über 8.700 Ordner sorgten spieltäglich mit dafür, dass die Stadien der bundesweiten Spielklassen zu den sichersten der Welt zählten. Die von gewerblichen Ordnern auch für Fußballeinsätze verlangte vierzig-

stündige Unterrichtung ohne Fußballbezug, ohne Praxisanteile und ohne Prüfung sei nicht zielführend. Der DFB habe deshalb die Projektgruppe „**Qualifizierung von Sicherheits- und Ordnungsdiensten**" ins Leben gerufen, deren Ziel es gewesen sei, ein fußballspezifisches Qualifizierungskonzept für alle beim Profifußball eingesetzten „Veranstaltungsordner" zu entwickeln, unabhängig, ob sie gewerblich oder als vereinseigene Ordner tätig sind. Das von der Projektgruppe entwickelte Schulungskonzept sehe unterschiedliche Qualifizierungen für Ordner, Führungskräfte, Sonderkräfte (Ermittlungen) und Sonderkräfte VIP in insgesamt elf Modulen. Die Dauer betrage bei Ordnern 21, bei Führungskräften 31, bei Ordnern VIP 6–8 Stunden. Berücksichtigt worden seien die hohe Ordner-Fluktuation, die vielfach geringe, nicht kontinuierliche Einsatzhäufigkeit, die immer gleichen Versammlungsstätten und das gewohnte Publikum sowie die gewohnten Veranstaltungsabläufe.

Terrorismus

In der Wochenlage vom 24. März nimmt das BKA Stellung zu Auswirkungen der Terroranschläge in Brüssel vom 22. März. Im Ergebnis müsse für Belgien derzeit eine hohe Gefährdungssituation konstatiert werden. Bislang lägen den Bundessicherheitsbehörden weder Erkenntnisse noch Hinweise vor, die darauf hindeuteten, dass sich das Anschlagsgeschehen mittel- oder unmittelbar gegen deutsche Interessen vor Ort richtete. Hinweise auf gleichgelagerte Anschlagsplanungen in der Bundesrepublik lägen nicht vor. In Bezug auf die Gefährdungslage aus dem Phänomenbereich des islamistischen Terrorismus sei für die Bundesrepublik weiterhin eine anhaltend hohe abstrakte Gefahr zu konstatieren, die sich jederzeit in Form sicherheitsrelevanter Ereignisse bis hin zu terroristischen Anschlägen konkretisieren könne.

Underground Economy

Das BKA definiert in der Wochenlage vom 4. März die Underground Economy als Szene, die sich über illegal betriebene, kommerziell ausgerichtete Kommunikations- und Verkaufsplattformen im Internet austauscht, dort Dienstleistungen zur Begehung von Straftaten anbietet sowie Straftaten, insbesondere im Bereich Cybercrime, begeht. Ende Februar hätten bundesweit sowie im Ausland Exekutivmaßnahmen gegen eine international agierende Tätergruppierung der Underground Economy stattgefunden. Es seien bei der Durchsuchung von 69 Objekten über 40 kg Rauschgift, Waffen, gefälschte Ausweisdokumente und Kreditkarten sowie Falschgeld aufgefunden worden. Bargeld und Vermögenswerte in Höhe von über 160.000 Euro seien sichergestellt worden. Die von der Tätergruppierung genutzten Foren seien als wesentliche Elemente der Underground Economy einzustufen. Ausgehend von den Betreibern von Online-Marktplätzen sei der Nachweis der Existenz einer Cyber-OK-Struktur gelungen. Dabei sei beachtenswert, dass sich die im Cyberraum aktiven Kriminellen zumeist im realen Leben gar nicht kennen, dass also die Strukturen nicht den tradierten OK-Begriffen entsprechen. Die Ermittlungsergebnisse belegten die Bedeutung des neu geschaffenen Tatbestands der Datenhehlerei (§ 202 d StGB), da der Handel mit rechtswidrig erlangten Daten auf kriminellen Online-Marktplätzen bisher durch eine Strafbarkeitslücke geschützt gewesen sei.

Unternehmenssicherheit

Dr. Ingo Hensing und Christian Plate, RWE AG, skizzieren in PROTECTOR, Ausgabe 3-2016, S. 78–82, den **„Security Change Management Prozess"** des zentral organisierten Teams von 20 Mitarbeitern in der RWE Zentrale ab April 2013. Eine ganzheit-

liche SWOT-Analyse sei die Grundlage für den Veränderungsprozess gewesen. Nach Herauslösung der Security Ressourcen aus den operativen Geschäftsfeldern habe die Bündelung im neu gegründeten „Center of Expertise Operational Security Management" stattfinden können. Das zentral aufgestellte Security Team stelle sein Know-how den operativen Geschäftsfeldern bereit und sei dort geschäftsnah eingebunden. In dieser Form der Matrixorganisation und funktionalen Steuerung seien die Sicherheitsleiter der einzelnen Geschäftssegmente die Garanten für den Erfolg. Die zentral gebündelte Security-Kompetenzplattform bestehe aus circa 100 Mitarbeitern, europaweit verteilt. Sie setze die zentrale Security Governance Funktion ohne Reibungsverluste um und arbeite service- und lösungsorientiert. Wesentlicher Hebel bei den Einsparungen sei der sozialverträgliche Abbau bislang intern erbrachter Bewachungsleistungen durch Leistungsverzicht sowie durch Fremdvergabe nach Neubewertung und die Substitution von personellen Bewachungsleistungen durch den Einsatz moderner Sicherheitstechnik. Für die Erarbeitung von Ideen, Strategien, Modellen und Konsequenzen sei der Bottom-up-Ansatz etabliert worden. Die Vorstände und Geschäftsführungen erhielten Informationen im Rahmen eines vierteljährlichen Sicherheitsberichts. Dazu komme ein Security Newsflash für die breite Unternehmensöffentlichkeit. Implementiert wurde ein in Eigenleistung entwickeltes, konzernweit einheitliches und web-basiertes Incident Reporting & Information System, an das ein web-basiertes Geospatial Crime Mapping Analytics Tool angebunden sei, das Unternehmensassets und Sicherheitsvorfälle beleuchte. Die IT-Security Governance werde vom CIO auf die Konzernsicherheit übertragen.

Vernetzung der betrieblichen Sicherheit thematisiert GIT in der Ausgabe 3-2016, S. 34. Unternehmer seien heutzutage vielfältigen betrieblichen Haftungsrisiken ausgesetzt. Um diese zu beherrschen, eigne sich das Betriebssicherheitsmanagement (BSM). Es sei ein Instrument, mit dem Risiken identifiziert und Maßnahmen interdisziplinär abgeleitet und somit Haftungsrisiken vermindert werden könnten. Die neue Richtlinie VDI 4055 wende sich an Unternehmer, die ein BSM in ihren Unternehmen etablieren wollten. Qualitätsmanagementsysteme, Arbeitsschutzmanagementsysteme oder Umweltschutzmanagementsysteme seien in der Praxis häufig parallele und nicht optimal verzahnte Systeme, die teilweise auch durch unterschiedliche Beauftragte gepflegt werden. Das BSM möchte genau diese interdisziplinäre Verzahnung zur Nutzung von Synergien und zum Lösen von möglichen Konflikten mit Blick auf einzelne Risikogruppen im Unternehmen erreichen. Die Richtlinie VDI 4055 sei ab sofort als Entwurf beim Beuth Verlag erhältlich.

Urheberrechtsverletzung

Wie silicon.de am 16. März berichtet, können nach Sicht des Generalanwalts Szpunar des Europäischen Gerichtshofs Betreiber eines kostenlosen öffentlichen WLAN-Netzes nicht für Urheberrechtsverletzungen eines Nutzers verantwortlich gemacht werden. Sie seien lediglich als Anbieter sogenannter Dienste der reinen Durchleitung anzusehen und somit nicht haftbar. Deutsche Gerichte hätten die Frage der Haftung von Anschlussbetreibern für Urheberrechtsverletzungen, die Dritte bei der Nutzung von offenen WLAN-Netzen begehen würden, bislang nicht ausreichend geklärt. Der Generalanwalt vertrete die Auffassung, dass die Auflegung eines Passworts dem Erfordernis zuwiderlaufen würde, ein angemessenes Gleichgewicht herzustellen zwischen dem Recht des geistigen Eigentums, das die Inhaber von Urheberrechten genießen, und der unternehmerischen Freiheit der betroffenen Diensteanbieter. Außerdem würde diese Maßnahme durch die Beschränkung des Zugangs auf rechtmäßige Kommunikation das Recht auf Freiheit der Meinungsäußerung und Informationsfreiheit einschränken.

Vergabeanforderungen

Rechtsanwalt Alexander Nette, LL.M, befasst sich in der Ausgabe 1-2016 des DSD, S. 50/51, mit „aktuellen" vergaberechtlichen Problemen bei **Aufträgen zum Schutz von Flüchtlingsunterkünften**. Ein sehr verbreiteter Fehler sei die Einordnung der Beschaffung von Sicherheitsleistungen mit der Bewirtschaftung der Unterkunft an „einen" Dienstleister. Die Vergabe von Sicherheitsdienstleistungen sei in die Kategorie 23 des Anhangs 1 B der VOL/A einzuordnen. Das sei gesicherte Rechtsprechung. Die Trennung der Sicherheitsleistungen von der Bewirtschaftung werde jedoch regelmäßig missachtet und alles an einen „Generalunternehmer" vergeben. Ebenso würden in derartigen Vergabeverfahren häufig freiwillige Verbandsmitgliedschaften als Eignungsnachweise gefordert. Die freiwillige Verbandsmitgliedschaft sei jedoch kein zulässiger Eignungsnachweis für Leistungsfähigkeit und Zuverlässigkeit. Häufig würden „irrwitzige" Öffnungsklauseln verlangt, um möglichst „flexibel" auf sich ändernde Verhältnisse reagieren zu können. Solche Öffnungsklauseln seien lediglich dann zulässig, wenn aus der Klausel selbst die Anpassungsmöglichkeiten des Auftraggebers hinreichend klar hervorgehen. Gleiches gelte für die Frage des Eignungsnachweises hinsichtlich der Mitarbeiter, in denen die öffentlichen Auftraggeber regelmäßig vermeintliche Fachkunde in den Eignungskriterien abfragen und dadurch häufig über das Ziel hinaus schießen oder auf dem Markt nicht umsetzbare Vorgaben für den Bieterkreis aufstellen.

Verschlüsselung

EncroChat nutze gehärtete Android-Smartphones als Ersatz für Blackberry-PGP-Smartphones, berichtet silicon.de am 3. März. Der niederländische Anbieter halte diese für weniger sicher. Das Unternehmen verweise dazu darauf, dass das Netherlands Forensics Institute (NFI), die Forensikabteilung der niederländischen Polizei, nach eigenen Angaben Nachrichten lesen kann, die per PGP verschlüsselt auf einem Blackberry-Smartphone gespeichert sind. Es solle sich dabei um die Geräte handeln, die mit Verschlüsselungstools von Blackberry und PGP erweitert wurden und von Drittanbietern verkauft werden. In einem Fall habe das NFI angeblich 279 von 325 verschlüsselten Nachrichten auf einem Blackberry-PGP-Gerät wiederherstellen können.

Die WirtschaftsWoche geht am 11. März auf den **Streit zwischen FBI und Apple** ein, nachdem das FBI von Apple gefordert hatte, eine „Hintertür" in ein verschlüsseltes iPhone 5C „aufzustoßen". Es gehörte dem islamistischen Terroristen Syed Farook, der im Dezember in den USA 14 Menschen erschossen hatte. Besonders die US-Behörden nutzten solche Fälle nur zu gern. Sie wollten so die Sicherheitsbarrieren durchlöchern, die praktisch alle IT-Unternehmen zum Schutz ihrer Nutzer errichtet hätten. Die Taktik habe auch für Deutschland Folgen. Denn bei Konzernen wie Mittelständlern gleichermaßen wachse die Sorge, verschlüsselte Geschäftsgeheimnisse auf Firmenhandys und Cloud-Servern könnten nicht mehr sicher sein, sollten sich ausländische Ermittler durch Hintertüren beliebig Zugang verschaffen können. Es spreche vieles dafür, dass sich Konzerne wie Apple, Google, Microsoft und Facebook nicht auf Dauer gegen den politischen und öffentlichen Druck stemmen können. Terroranschläge würden die Meinung der Bevölkerung verschieben. Microsoft übertrage daher den Betrieb zweier Rechenzentren an die Deutsche Telekom. Das solle sie vor Zugriffen der US-Behörden schützen. Deutsche Konzernvorstände und Mittelständler interessierten sich verstärkt für heimische Verschlüsselungssysteme. Das bisher ambitionierteste Projekt starteten die vier Dax-Konzerne Allianz, Bayer, BASF und VW. In Berlin bauten sie die Deutsche Cybersicherheitsorganisation auf.

Das Ziel: Sie solle besonders hochwertige Schutzverfahren entwickeln. Die Bundesregierung ermuntere die übrige Wirtschaft, dem Beispiel zu folgen.

Heise.de meldet am 30. März, dass auch Udo Helmbrecht, Direktor der EU-Agentur für Netz- und Informationssicherheit, fordert, eine starke Verschlüsselung zu unterstützen. Europol-Direktor Rob Wainwright hätte zunächst vor Verschlüsselung gewarnt, bevor er sich gegen ein Verbot von Verschlüsselung ausgesprochen habe. Und Andrus Ansip, Vizepräsident der EU-Kommission, habe sich gegen jegliche Hintertüren in Verschlüsselungssystemen ausgesprochen.

Versorgungssicherheit

Stefan Vogt, Honeywell Security Group, erklärt in der Ausgabe 3-2016 der Zeitschrift GIT, S. 42–44, warum Sicherheitssysteme für Versorgungsunternehmen auch wirtschaftlich sinnvoll sind. Eine Zutrittskontrolle in Kombination mit einem Videoüberwachungs- und Managementsystem erlaube es Sicherheitsverantwortlichen, ein unternehmensweites Sicherheitssystem von einem zentralen Standpunkt aus zu kontrollieren. Daten, die durch Videoanalyse gewonnen werden, würden Sicherheitsverantwortlichen bei der schnellen und fundierten Entscheidungsfindung helfen. Cloud-Video und Zutrittskontrollsysteme ließen sich einfach über IP implementieren und bildeten eine hervorragende Komponente wirtschaftlicher und einfach zu wartender, fernüberwachter Sicherheitssysteme. Durch die Investition in integrierte Videoanalysen und Cloud-basierte Sicherheitssysteme könnten Versorgungsunternehmen die Verwaltung eines verzweigten Netzwerks aus Anlagen, Vertriebssystemen, Umspannwerken und Arbeitsplätzen vereinfachen.

Videoüberwachung

Für die **Integration von Videotechnik und Zutrittskontrolle** plädiert in PROTECTOR, Ausgabe 3-2016, S. 28/29, Dipl.-Ing. Hans-Ulrich Heß, Primion Technology GmbH. Dieses Zusammenspiel sei heute „state of the art". Sinnvolle Applikation im Zusammenspiel von Zutrittskontrolle und Videotechnik seien Personen-Verifikation, Alarmbehandlung-Verifikation, Aufbruch-Verifikation, Durchsetzung von Präventionsmaßnahmen und Investigations-Historie. Klassische Einsatzgebiete im Zusammenspiel von Zutrittskontrolle und Videoüberwachung seien alle Umgebungen, wo ein hoher Sicherheitsstandard erforderlich sei, wie etwa Flughäfen, Bahnhöfe oder Energiekraftwerke und Rechenzentren.

Veko-online.de berichtet in der März-Ausgabe über die **Ausrüstung des Shanghai Towers**, des zweithöchsten Gebäudes der Welt, mit einem Videoüberwachungssystem, einer Beschallungs- und Evakuierungsanlage sowie Einbruchmeldesystem durch BOSCH Sicherheitssysteme. Kernstück der Sicherheitslösung seien die 2.100 hochauflösenden feststehenden Bosch DINION und FLEXIDOME-Kameras sowie die beweglichen AUTODOME-Kameras. Sie lieferten hochauflösende Aufnahmen, unabhängig von den aktuellen Lichtverhältnissen oder den Bewegungen der aufgenommenen Personen. Die AUTODOME IP-Kameras ermöglichten dem Sicherheitspersonal das Verfolgen von Personen und Objekten mittels Intelligent Tracking. Die Intelligent Dynamic Noise Reduction sorge dafür, dass die Bitraten bei der Bildübertragung um bis zu 50 Prozent reduziert werden und damit die Netzwerklast deutlich senke. 150 integrierte Bosch VIDEOJET 7000-Decoder erlaubten dem Sicherheitspersonal sowohl die kontinuierliche Live-Überwachung als auch die Wiedergabe von gespeicherten Aufnahmen selbst bei Leitungsunterbrechung oder Stromausfall. Mit mehr als 100 Verstärkern und 6.000 im Gebäude verteilten Laut-

sprechern könnten auf die unterschiedlichen Gebäudeteile zugeschnittene Evakuierungsinstruktionen erteilt werden. Die Audio- und Steuersignale aus sechs Kontrollzentren seien über ein Local Area Network vernetzt. Die Kontrollzentren bildeten eine Ring-Redundanz.

Wirtschaftsschutz

Der ASW hat ein Positionspapier „Wirtschaftsschutz in Deutschland" vorgelegt, mit Gefährdungsprognosen und Empfehlungen für Unternehmen und Politik, meldet PROTECTOR in der Ausgabe 3-2016, S. 67. Es gehe von vier Megatrends mit konkreten Auswirkungen auf die Wirtschaft aus: Staatszerfall, klimatische und ökologische Verwerfungen, Digitalisierung und Vernetzung sowie asymmetrische Bedrohung und hybride Kriegsführung. Die Unternehmen sollten verstärkt in ihre Sicherheit investieren, denn ein wirksamer Basisschutz sei nicht nur vergleichsweise kostengünstig zu haben, sondern auch wirtschaftlich sinnvoll. Der Schlüssel zum Erfolg werde vor allem in einer engeren Zusammenarbeit mit anderen Unternehmen und in einer engeren Kooperation mit den Sicherheitsbehörden gesehen. Download unter http://asw-bundesverband.de/positionspapiere.

Zutrittskontrolle

Mit dem **Smartphone als neuem digitalen Ausweis** befasst sich Security insight in der Ausgabe 1-2016, S. 19. Möglich machten dies neue Technologien und Kommunikationsverfahren wie NFC und Bluetooth Smart. Es sei offensichtlich, dass ein integrierter Mobile Access-Ansatz die Kosten nachhaltig senkt, denn so würden Investitionen in separate Infrastrukturen für die physische und logische Authentifizierung überflüssig. Kostensenkungen ergäben sich auch durch die vollständige Digitalisierung der Prozesse, die bei Verlust oder Mitarbeiterwechsel die Bestellung und den Druck neuer Ausweiskarten überflüssig mache. Voraussetzung für die Umsetzung einer mobilen Zugangslösung sei der Aufbau einer Infrastruktur mit einem sicheren und durchgängigen Identity- und Access-Management.

PROTECTOR enthält in der Ausgabe 3-2016, S. 36/37, eine Marktübersicht zu 94 Systemen von **Vereinzelungsanlagen** von 24 Anbietern. Abgefragt wurden die Kriterien Sicherheitsniveau, Durchgangsfrequenz, Schnittstellen, Steuerung, Mechanik oder Elektronik, Durchwurf-, Einbruch-, Feuer-, Durchschusshemmung, Fluchtwegintegration, Stromausfallverhalten.

Impressum

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

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

Herausgeber:
Manfred Buhl, Vorsitzender der Geschäftsführung, Düsseldorf

Verantwortlicher Redakteur:
Bernd Weiler, Leiter Kommunikation und Marketing

Beratender Redakteur:
Reinhard Rupprecht, Bonn

focus.securitas.de

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

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

E-Mail: info@securitas.de