FOCUS ON SECURITY

AUSGABE 02, FEBRUAR 2018

SECURITAS

Bankensicherheit

Die Bankenaufseher widmeten sich nun verstärkt den **Cyberrisiken der Finanzinstitute** und der Widerstandsfähigkeit ihrer Systeme in der Informationstechnologie, hat nach einer Meldung in der FAZ am 30. Januar der schwedische Notenbankgouverneur angekündigt. Hacker hätten über die japanische Handelsplattform Coincheck 523 Mio. Einheiten der Kunstwährung XEM im Wert von umgerechnet 430 Mio. Euro erbeutet. Die Banken seien inzwischen täglich Angriffen ausgesetzt, die fast alle von den IT-Systemen abgewehrt werden konnten. Im vergangenen Jahr habe die deutsche Finanzaufsicht Bafin Alarm geschlagen, weil die IT-Sicherheitsvorkehrungen deutscher Banken ihrer Ansicht nach zum Teil große Lücken aufweisen.

Betrug

Neben Umsatzsteuerbetrug durch Chinesen tat sich nach einem Bericht in der FAZ am 30. Januar im Onlinehandel eine weitere **illegale Geschäftspraktik** auf. Es gehe um den Verkauf elektronischer Geräte, für die sich Anbieter aus Fernost weder an den gesetzlich festgelegten Entsorgungskosten beteiligen noch die fällige Registriergebühr bezahlen. Die Prellerei betreffe Produkte für den Haushalt, Telekommunikation, medizinische Anwendungen und Sicherheitstechnik.

Im Verfahren gegen Mitglieder einer **„Pflegemafia"** habe das LG Düsseldorf Haftstrafen zwischen zwei und sieben Jahren verhängt, berichtet die FAZ am 6. Februar. Die Staatsanwaltschaft habe ein komplexes Geflecht aus Unternehmen, Pflegekräften sowie kooperierenden Ärzten aufgedeckt. Über dieses System sollen die Angeklagten den Kranken- und Pflegekassen über acht Jahre hinweg Zehntausende nie erbrachte Leistungen der häuslichen Pflege in Rechnung gestellt haben. Die Kooperation der Patienten sei mit Taschengeldern von bis zu 100 Euro monatlich oder mit Dienstleistungen wie Wohnungsreinigungen, Fahrten zu Behörden oder Dolmetschen erkauft worden. Die Angeklagten hätten einen Schaden von mindestens 8,5 Mio. Euro verursacht. Einem Bericht des LKA NRW zufolge ist dies symptomatisch für ein bundesweites Phänomen. Demnach bestehe gegen fast ein Vierteil der 1.000 in Deutschland betriebenen russischen Pflegedienste der Verdacht des Abrechnungsbetrugs.

Biometrie

PC-Hersteller Lenovo meldet ein schweres Sicherheitsleck im verbreiteten Fingerabdruck-Scanner **Fingerprint Manager Pro**, heißt es am 30. Januar bei silicon.de. Damit könnten sich Anwender am System oder bei Webseiten anmelden, die für die Erkennung von Fingerabdrücken konfiguriert sind. Betroffen seien laut Lenovo lediglich Rechner mit den Betriebssystemen Windows 7, 8 und 8.1. In Windows 10 werde diese Utility nicht benötigt. Lenovo rät Nutzern von älteren Betriebssystemen, schnell die Version 8.01.87 des Fingerprint Managers Pro zu installieren oder auch Windows 10 zu aktualisieren.

Eine IBM-Studie untersuche Vorlieben von Nutzern aller Altersgruppen für **Passwörter und biometrische Anmeldungen**, meldet golem.de. Teilnehmer ab 55 Jahren merkten sich viele verschiedene Passwörter auf einmal – auch ohne Passwort-Manager. Junge Leute nutzten Passwörter doppelt und auch gerne biometrische Passwörter. Befragt worden seien 4.000 Erwachsene in den USA, dem asiatisch-pazifischen Raum und Europa. 67 Prozent der befragten Teilnehmer würden ohne Bedenken biometrische Anmeldeoptionen wie etwa Fingerabdrucksensoren nutzen. Fast die Hälfte der Teilnehmer halte Fingerabdrücke für sicherer als Passwörter und PINs (44 Prozent). Für IBM sei ein Fakt für Arbeitgeber in der Zukunft wichtig: Junge Leute unter 24 schätzten einfache und schnellere Anmeldeoptionen wie Fingerabdrucksensoren fast so sehr wie eine sichere Methode (47 Prozent).

GIT befasst sich in der Ausgabe 1/2-2018, S. 50/51, mit der **Handvenenerkennung zur Zutrittskontrolle** an einer Vereinzelungsanlage für den Zutritt von Mitarbeitern zum nichtöffentlichen Flughafenbereich. Bei dem System Intus PS von PCS arbeiten die biometrischen Zutrittsleser mit einer Infrarot-Kamera, die das persönliche Venenmuster in der Handinnenfläche erkennt. Dieses Muster sei bei jedem Menschen individuell und unveränderlich. Es eigne sich hervorragend zur Identifizierung eines Menschen. Das Handvenenmuster sei nicht zu manipulieren und könne nicht kopiert werden. Mit einer False Acceptance Rate von 0,00008 Prozent sei es als hochsicher einzustufen. Das System arbeite mit den RFID-Lesertechnologien Legic, Mifare oder HID: Über das OSDP-Standard-Protokoll oder Wiegend-Takt-Datenprotokoll könne die Handvenenerkennung an die meisten Fremdsysteme für Zutrittskontrolle angeschlossen werden.

Brandschutz

Planungs- und Installationsfehler bei Brandmeldeanlagen (BMA) thematisiert Sascha Puppel, Sachverständigen- und Planungsbüro Sascha Puppel GmbH, in der Ausgabe 1/2-2018 der Zeitschrift PROTECTOR, S. 18–21. Einige typische Fehler: nicht eingehaltene Trennungsabstände zwischen Leitungen und Geräten wie Schlüsseldepots, Freischaltelemente oder Signalgeber zu Blitzableitungen und blitzstromführenden Bauelementen. Auch bei BMA ohne klare Vorgaben seien die entsprechenden „Allgemein anerkannten Regeln der Technik" sowie die Montageanleitungen der Gerätehersteller zu beachten. Bei der Planung und Projektierung von BMA bestünden erhebliche Fehlerpotenziale bei der Auswahl und Anordnung von automatischen und nicht automatischen Brandmeldern. Immer häufiger würden Geräte wie Handfeuer- oder Rauchmelder im ungeschützten Außenbereich vorgefunden, die dort ungeeignet sind. Oftmals sei es Errichtern nicht klar, dass neben dem Funktionserhalt weitere Anforderungen an das Leitungsnetz einer BMA bestehen. Oftmals fände man unzulässige Brandlasten in Flucht- und Rettungswegen. Ursächlich für Störungen und Falschalarme seien oftmals zu geringe Verlege- beziehungsweise Trennungsabstände zwischen Fernmelde- und Stromversorgungsleitungen. Bei größeren Installationen mit längeren Leitungswegen sei die Art und Qualität der Leitungsschirmung von besonderer Bedeutung.

Georg Luber, Siemens AG, befasst sich in Ausgabe 1/2-2018 von PROTECTOR, S. 22–24, mit dem **Brandschutzschalter nach DIN VDE 0100-420**. Allein in Deutschland sei rund ein Drittel aller Brände auf Elektrizität zurückzuführen. Ob beschädigte Kabelisolierungen, gequetschte Leitungen, abgeknickte Stecker, lose Kontaktstellen oder fehlerhafte Endgeräte – an den schadhaften Stellen bestünde die Gefahr unerwünschter Fehlerlichtbögen. Leitungsschutzschalter böten Schutz bei Kurzschluss sowie vor Überlast. Fehlerstrom-Schutzeinrichtungen erfassten Fehlerströme und damit gegebenenfalls Fehlerlichtbögen gegen Erde. Serielle Fehlerlichtbögen könnten diese Schutzeinrichtungen jedoch nicht erkennen. Diese Lücke habe erst durch den Brandschutzschalter geschlossen werden können. Basis sei die von Siemens patentierte Erkennungstechnologie „SIARC". Der Brandschutzschalter analysiere das Hochfrequenz-Rauschen. Der integrierte Microcontroller erkenne unerwünschte Fehlerlichtbögen sofort. Harmlose Störquellen könne der Brandschutzschalter von gefährlichen Lichtbögen unterscheiden. In den Errichtungsbestimmungen IEC 60364-4-42/A1 und HD 60364-4-42/A1 werde die Installation von Brandschutzschaltern als anerkannter „Stand der Technik" empfohlen. Die DIN VDE-Norm schreibe für bestimmte Bereiche den Einsatz des Brandschutzschalters auch für bestehende Gebäude, an denen wesentliche Veränderungen der Elektroinstallation durchgeführt werden, verbindlich vor. Auch in öffentlichen Gebäuden sei er jetzt vorgeschrieben, wenn sich darin unersetzbare Güter befinden. Vorgeschrieben sei er auch in Schlaf- und Aufenthaltsräumen von Kindertagesstätten und Seniorenheimen.

Thomas Litterst, Hekatron Vertriebs GmbH, behandelt in der Ausgabe 1/2-2018 der Zeitschrift PROTECTOR, S. 25–27, **Anwendungsnormen im anlagentechnischen Brandschutz**. Die Normen DIN 14675, 14676 und 14677 seien in den letzten zwei Jahren in unterschiedlichen Arbeitsausschüssen im DIN-Normenausschuss Feuerwehrwesen überarbeitet worden. Eine Notwendigkeit für die Überarbeitung lag in der sogenannten Dienstleistungsrichtlinie für Sicherheitsanlagen DIN EN 16763. Sinn und Zweck des Art. 26 dieser Richtlinie sei es, dass die Marktteilnehmer ein Kompetenznachweissystem für Dienstleistungserbringer schaffen. Der Autor beschreibt die wesentlichen Änderungen und Ergänzungen der drei eingangs bezeichneten Normen. Durch die Aufnahme der Technischen Anschlussbedingungen TAB in den Anhang der Norm DIN 14675 ergebe sich die Chance, die bundesweit über 500 TABs zu vereinfachen und auf die DIN 14675-1 zu referieren. Bei der Norm DIN 14676 (Rauchwarnmelder) seien alle Hinweise zum Kompetenznachweis in den Teil 2 überführt und eine Mindestqualifikation für die Ausführung der Dienstleistung definiert worden. Für die Dienstleister der Normen DIN 14676-2 und DIN 14677-2 sei für den Kompetenznachweis ein einfacheres und kostengünstigeres Nachweissystem außerhalb des akkreditierten Systems in der jeweiligen Norm festgelegt worden.

In der Ausgabe 1/2-2018 der Zeitschrift PROTECTOR, S. 30/31, wird die **Permanent-Inertisierung im Tiefkühllager** mittels Brennstoffzelle erläutert. Durch die trockene Luft und die Vielzahl an brennbaren Verpackungs- und Dämmmaterialien bestehe ein hohes Brandrisiko. Infolge der zunehmenden Automatisierung stiegen die Risiken von Kabelbränden oder Überhitzungen an Fördergeräten weiter an. Während der Energiebereitstellung entstünde in der Brennstoffzelle prozessbedingt eine saubere Abluft, die einen geringeren Sauerstoffgehalt als normale Umgebungsluft habe. Diese Luft falle beim Betrieb des Systems permanent und ganz ohne Zusatzkosten an und werde über ein Rohrleitungssystem in die zu schützenden Räume

geleitet. So werde eine dauerhafte Schutzatmosphäre geschaffen, in der Brände gar nicht erst entstehen können.

Auch Dr. Wolfram Krause, bvfa, behandelt die Thematik **Speziallöschanlagen in industriellen und gewerblichen Anlagen** in PROTECTOR, Ausgabe 1/2-2018, S. 34/35. Die Mitgliedsunternehmen des bvfa meldeten seit zehn Jahren durch Speziallöschanlagen nachweislich gelöschte Brände. Bei der Auswertung für das Jahr 2016 würden zwei Risikoschwerpunkte deutlich: 44 Prozent der gemeldeten und durch solche Anlagen gelöschten Brände seien in Maschinen entstanden, insbesondere bei der Metallbearbeitung. Weitere 42 Prozent der Brände seien in EDV-Anlagen und elektrischen Schalträumen aufgetreten. Elektrischer Strom sei auch 2016 mit 31 Prozent nach wie vor Brandursache Nummer eins. 88 Prozent der Speziallöschanlagen hätten 2016 automatisch ausgelöst. 26 Prozent seien außerhalb der Arbeitszeit gelöscht worden. Die Brände an Maschinen würden nach der bvfa-Statistik vor allem mit Kohlendioxid-Löschanlagen bekämpft, in elektrischen Anlagen überwiegend mit Inertgasen. In 63 Prozent der Fälle seien die gemeldeten Anlagen als Einrichtungsschutz betrieben worden, d. h. geschützt würden ganz gezielt bestimmte Anlagen oder Maschinen mit hohem Risikopotenzial. Die verwendete Löschmittelmenge habe in 78 Prozent der Anlagen durchschnittlich nur 115 kg betragen.

Sören Wittmann, Bosch Sicherheitssysteme, befasst sich in der Ausgabe 1/2-2018 der Zeitschrift PROTECTOR, S. 32/33, mit der **Branddetektion per Video**. Ein solches Brandfrüherkennungssystem habe die Anerkennung durch den VdS erhalten. Über eine direkt in die Kamera integrierte Brandfrüherkennung könne mithilfe spezifischer Algorithmen das Videobild auf Rauch und Flammen gescannt werden. Das System „AVIOTEC IP starlight 8000" entdecke einen Brand in einem früheren Stadium als herkömmliche Brandmelder. Es könne zwischen echtem Feuer oder Rauch und Störgrößen wie Reflexionen, Bewegungen oder Gegenlicht unterscheiden. Alarme könnten an eine bestehende Brandmeldezentrale oder über Ethernet an einer Leitstelle übertragen werden. Beim Einsatz von PoE-Kameras würden auch keine individuellen Stromversorgungen und -kabel benötigt und so die Kosten reduziert. Das System könne zusätzlich auch für automatisierte Überwachungsaufgaben eingesetzt werden. Die Lösung erkenne ungewöhnliche Bewegungen ebenso wie blockierte Notausgänge.

Die **Vorteile von Datensicherungsräumen nach EN 1047-2** im Vergleich zu konventionellen Sicherheitsräumen werden in der Ausgabe 1/2-2018, S. 28/29, erläutert. Die EN 1047-2 beschreibe eine umfangreiche Prüfmethode von äußerer Brandeinwirkung. Sie ermittele den Schutz von temperatur- und feuchtigkeitsempfindlichen Datenträgern und Hardwaresystemen in Datensicherungsräumen und -containern. Die sogenannte Stoßprüfung teste Bauteile und Objekte, auch außerhalb des Datensicherungsraumes, auf deren brandbedingtes Versagen. Die EN 1047-2 biete folglich zusätzlichen zertifizierten Schutz vor einstürzenden Bauteilen. Von den geprüften Abmessungen könnten Hersteller in Serie zu vorgegebenen Toleranzen abweichen. Auch die Raumhöhe dürfe um plus 50 Prozent vergrößert werden. Das größere Volumen wirke sich positiv auf die Temperaturwerte aus. Die stetig angepassten Grenzwerte und Hürden einer Zertifizierung nach EN 1047-2 basierten auf professionellem Fachwissen. Die Standards und Grenzwerte, die für eine Zertifizierung der Datensicherungsräume nach EN 1047-2 gelten, seien europaweit die strengsten. Die Räume bestünden häufig aus Sandwichpanelen. In der Wandung seien spezielle Brandschutz- und Gummidichtungen integriert, die den benötigten Brandschutz und Wasserdampfschutz bieten.

PROTECTOR enthält in Ausgabe 1/2-2018, S. 36/37 eine **Marktübersicht über 65 Brandmeldesysteme** von 28 Anbietern. Abgefragt worden seien 35 Kriterien, z. B. Zertifizierungen, Systemaufbau, Vernetzung, Fernbedienung, Löschanlagensteuerung, maximale Anzahl an Stichleitungen, Ringen, Teilnehmern und Meldern, Art und Adressierung der Melder, Ausgangsüberwachung, Datenschnittstellen, Lageplantableau, Programmierung, Zugriffsschutz, Ereignisspeicher, Selbsttest der Funktionsfähigkeit.

Nach dem katastrophalen Brand der Grenfell Towers in London haben Feuerwehrgremien und die Vereinigung zur Förderung des deutschen Brandschutzes e. V. (vfdb) ein Positionspapier vorgelegt, das sich mit der Brandsicherheit von **Wärmedämm-Verbundsystemen an Fassaden mit EPS als Dämmstoff** befasst. Darüber berichtet GIT in der Ausgabe 1/2-2018, S. 60/61. Brände von Wärmedämmverbundsystemen, in denen Polystyrolschaum verarbeitet ist, stellten die deutschen Feuerwehren vor enorme Herausforderungen. Die rasante Brandausbreitungsgeschwindigkeit und die enorme Rauchintensität dieser Systeme unterschieden sich deutlich von anderen Fassadensystemen. Als Schlussfolgerung der Herausforderungen wird empfohlen:

- Neue Systeme: Brandriegel in jedem Geschoss, Erdgeschoss nichtbrennbar bei beweglichen Brandlasten oder nicht brennbares Einhausen von beweglichen Brandlasten

- Baustellen: besondere Sensibilität ist auf Baustellen hinsichtlich der Lagerung von brennbarem Material notwendig – Abstand zu (vor allem bewohnten) Gebäuden oder Einhausen des Materials
- Systeme im Bestand: Bewegliche Brandlasten wie Müllcontainer, Sperrmüll und Fahrzeuge sind zu beachten. Diese sollten entweder ausreichenden Abstand zur Fassade haben oder nicht brennbar eingehaust werden. Ist das nicht möglich, Ertüchtigung der Fassade im Erdgeschossbereich mit nicht brennbaren Dämmmaterialien.

Die Securiton GmbH Alarm- und Sicherheitssysteme stellt in der Ausgabe 1/2-2018 der Zeitschrift GIT, S. 62, **Sonderbrandmeldetechnik für Krankenhäuser** vor. Die Überwachung mit Ansaugrauchmeldern wie dem SecuriRAS ASD sei eine sichere Sache. Über Ansaugleitungen würden permanent Luftproben zur Auswerteeinheit transportiert und dort analysiert. Bei kleinsten Abweichungen vom Grenzwert schlage der Melder Alarm. Er eigne sich auch für Fahrstühle, Bettenaufzüge sowie Versorgungsschächte und überwache Zwischendecken, Doppelböden, aber auch Luft- oder Kabelkanäle. Für komplexe Gebäude seien Sprachalarmierungsanlagen sinnvoll: Sie sendeten gespeicherte oder live eingesprochene Sprachmitteilungen über ein eigenes Lautsprechersystem.

Compliance

Welchen Nutzen bringt Compliance? fragen Sebastian Rick, KPMG AG Wirtschaftsprüfungsgesellschaft, und Prof. Ralf Jasny, Frankfurt University of Applied Sciences, in der FAZ am 12. Februar. Wie lasse sich der Erfolg verschiedener Compliance-Maßnahmen messen? Compliance-Officer hätten das Gefühl, dass bisherige Versuche zur Messung und Demonstration der Wirksamkeit der Maßnahmen in ihrem Wert beschränkt sind. Abhilfe schaffe das **Compliance-Indexmodell**. Es sei das Ergebnis zweier empirischer Studien, die an der Frankfurt University of Applied Sciences mit Unterstützung des Frankfurter Instituts für Risikomanagement und Regulierung (Firm) durchgeführt worden seien. Es gebe Aufschluss darüber, mit welchen Maßnahmen eine höhere Bereitschaft für regelkonformes Verhalten im Unternehmen erreicht wird, und mache kulturellen Wandel messbar. Im Prinzip umfasse das Modell eine Reihe statistischer Verfahren zur Untersuchung komplexer Beziehungsstrukturen zwischen Maßnahmen und Mitarbeiterverhalten und ermögliche die quantitative Abschätzung der Wirkungszusammenhänge. Das Modell fasse die Wirkungszusammenhänge formal so, dass die Wirkungen von Maßnahmen auf das Mitarbeiterverhalten messbar, quantifizierbar und damit vergleichbar gemacht werden können. Das Ergebnis sei ein Compliance-Index (KPI), anhand dessen der Erfolg der Maßnahmen innerhalb der Organisation gemessen, gesteuert und überwacht werden könne. Außerdem erlaube das Modell interne Benchmark-Analysen, um auf diese Weise Unterschiede in der Compliance-Kultur in einzelnen Organisationsbereichen zu ermitteln.

Cum-Ex-Steuertricks

Der Steuerskandal um sogenannte Cum-Ex-Geschäfte habe deutlich größere Dimensionen, als bisher angenommen, berichtet die FAZ am 12. Januar. Zahlen des BMF gingen auf der Grundlage von Verfahren mit den Finanzbehörden und Steuerstrafprozessen von 417 Verdachtsfällen aus. Dabei handele es sich um ein Gesamtvolumen von 5,3 Mrd. Euro. Für den Trick würden Aktien um den Dividendenstichtag mit (Cum) und ohne (Ex) Dividendenzahlung gehandelt und dann mehrfach Erstattung der Kapitalertragsteuer eingefordert, die nur einmal abgeführt wurde. Vor dem LG München habe jetzt ein Schadenersatzprozess der Hypo-Vereinsbank gegen drei ihrer ehemaligen Vorstände begonnen, die auf Schadenersatz über insgesamt 180 Mio. Euro verklagt wurden. Sie werfe ihnen Pflichtverletzung im Amt vor. Die drei Banker sollen in ihrer Zeit als Vorstände nichts gegen den rechtswidrigen Aktienhandel unternommen haben.

Datenschutz

Die ASW weist in ihrem Newsletter vom 26. Januar darauf hin, dass die EU-Kommission am 24. Januar einen umfangreichen Online-Leitfaden für Behörden und Unternehmen veröffentlicht hat, der diesen dabei helfen soll, ihre Verpflichtungen aus der DSGVO zu erfüllen, die am 25. Mai in Kraft tritt.

Drohnen

Drohnen kommen häufiger Flugzeugen in die Quere, titelt die FAZ am 11. Januar. **88 Mal** hätten nach Angaben der Deutschen Flugsicherung (DFS) Piloten 2017 **Zwischenfälle** gemeldet. Die Fluglotsen sorgten sich daher um die Sicherheit im deutschen Luftraum und forderten schärfere Regelungen für Drohnen. Wie viele Drohnen über Deutschland schweben, dazu gebe es nur Schätzungen. Die DFS rechne bis 2020 mit einer Million. Zwar dürften Drohnen nicht höher als 100 Meter aufsteigen, 1,5 Kilometer um Flughäfen sei ihr Einsatz verboten, Verstöße seien Straftaten. Dennoch seien Flughäfen machtlos beim Schutz ihrer Landebahnen, für Eingriffe in das Geschehen in der Luft fehle ihnen die Befugnis. Die DFS und die Deutsche Telekom arbeiteten derweil an einem Drohnen-Prototyp, der mittels SIM-Karte wie ein „fliegendes Handy" Signale sendet und dann auf Radarschirmen sichtbar wird, bevor ein Flugzeug zu nahe kommt.

Endgerätesicherheit

Das BKA späht auch **verschlüsselte Kommunikation mit Smartphones** aus, die über Messenger wie WhatsApp, Signal oder Telegram erfolgt, meldet silicon.de am 30. Januar. Seit Mitte 2017 erlaube eine Gesetzesänderung Ermittlern, neben laufender Kommunikation wie Telefonaten, Chats und E-Mails auch bereits zuvor auf dem Gerät gespeicherte Daten zu erfassen. Damit werde auch auf Mobilgeräten eine Online-Durchsuchung möglich und könnte viel häufiger als bisher durchgeführt werden. Nach einer Entscheidung des BVerfG (2008) dürfen die Ermittler PCs von Verdächtigen nur dann ausspionieren, wenn „eine konkrete Gefahr für ein überragend wichtiges Rechtsgut" wie ein Menschenleben oder für den Bestand des Staates bestehe. Die Polizeibehörden sprächen jetzt nicht von einem Trojaner für Smartphones, sondern von „Quellen-Telekommunikationsüberwachung" (Quellen-TKÜ oder QTKÜ). Die dafür eingesetzte Software nutze Sicherheitslücken. Dafür müssten auch die ausgenutzten Schwachstellen weiterhin geheim gehalten werden, statt sie an die Hersteller zu melden.

Geldautomatensicherheit

Kriminelle haben mit dem **Ausspähen sensibler Daten von Bankkunden 2017** erstmals seit vier Jahren wieder mehr Schaden angerichtet als vor Jahresfrist, meldet die FAZ am 15. Januar. Auf rund 2,2 Mio. Euro beziffere Euro Kartensysteme den Bruttoschaden durch sogenannte Skimming-Angriffe (Rekordtief 2016 mit 1,9 Mio. Euro). 499 Fälle habe Euro Kartensysteme 2017 gezählt (2016: 369). Brennpunkt sei Berlin mit 287 Fällen. Dabei funktionieren Kartendubletten nur noch in Ländern, in denen Bezahlkarten mit leicht kopierbaren Magnetstreifen ausgerüstet werden. Zum Einsatz seien Kartenfälschungen auf Basis von in Deutschland gestohlenen Kundendaten 2017 in Indonesien, den USA und Australien gekommen. Deutschland setze auf moderne EMV-Technik: Der Datensatz werde verschlüsselt, die Karte bei Gebrauch auf Echtheit geprüft, am Geldautomaten wie an der Ladenkasse.

246 Sprengungen von Geldautomaten wurden nach einem Bericht der FAZ vom 23. Januar vom BKA registriert (2016: 318), davon 123 Versuche. Der Rückgang von 20 Prozent gegenüber dem Vorjahr werde auch damit erklärt, dass viele Automaten mit Anlagen ausgestattet wurden, die eingeleitetes Gas neutralisiert oder Geldscheine bei einer Explosion verfärbt. Das Unternehmen Ratiodata habe nach eigenen Angaben in 3000 Automaten mittlerweile ein Gas-Neutralisierungssystem eingebaut. Die Täter seien in vielen Fällen über die Grenze aus den Niederlanden gekommen. Viele gesprengte Automaten hätten auf dem Land oder am Stadtrand gestanden. Die Angriffe seien meistens zwischen zwei und fünf Uhr morgens erfolgt.

Gewaltkriminalität

Der Newsletter des Behörden Spiegel vom 30. Januar berichtet über die Ergebnisse einer vom Lehrstuhl für Kriminologie der Ruhr-Universität Bochum durchgeführten Studie. Danach seien 2017 in Nordrhein-Westfalen **26 Prozent der Rettungskräfte Opfer körperlicher Gewalt** im Einsatz geworden. Dabei hätten etwa 80 Prozent der Einsatzkräfte Attacken erst gar nicht ihrem Dienstherrn gemeldet. Angesichts solcher Resultate sehe der Landesvorsitzende der komba gewerkschaft nrw Handlungsbedarf in Form einer Verbesserung des Meldewesens sowie hinsichtlich der Berück-

sichtigung von Themen der Gewaltprävention in der Aus- und Fortbildung. Die Berliner Morgenpost meldet am 30. Januar, dass in nur drei Tagen sechs Attacken auf Fahrer und Kontrolleure der Berliner Verkehrsgesellschaft BVG registriert worden seien. Nach dem Sicherheitsbericht der BVG habe es 2016 insgesamt 555 Übergriffe auf Mitarbeiter der BVG gegeben. 2012 seien mit 1.004 noch fast doppelt so viele Angriffe gezählt worden. Aber man beobachte eine deutliche Zunahme der Gewaltbereitschaft. Die Hemmschwelle, jemanden ernsthaft zu verletzen, sei spürbar gesunken.

Industrie 4.0

Viele Unternehmen lassen ihre Mitarbeiter Maschinen – und manchmal ganze industrielle Prozesse – mit Hilfe mobiler Apps kontrollieren und steuern, heißt es in heise.de am 15. Januar. Die Apps versprächen Effizienzvorteile, brächten aber auch neue Ziele für Cyberangriffe. Im schlimmsten Fall könnten Hacker die Lücken nutzen, um Maschinen zu zerstören, vielleicht sogar ganze Fabriken. Zwei Sicherheitsforscher von Embedi hätten 2017 34 Apps untersucht. Insgesamt hätten sie 147 Sicherheitslücken in den Apps gefunden. Einige Lücken könnten Hackern die Möglichkeit geben, sich in den Datenfluss zwischen einer App und der dazugehörigen Anlage einzuschalten. So könnte einem Techniker der Eindruck vermittelt werden, eine Maschine laufe bei einer sicheren Temperatur, obwohl sie in Wirklichkeit gerade überhitzt. Eine andere Lücke könnte Angreifern ermöglichen, Schadcode auf ein mobiles Gerät zu schmuggeln, sodass dieses gefährliche Anwendungen an Server schickt, die mehrere Maschinen kontrollieren. Die Risiken bezögen sich nicht nur auf Produktionsanlagen, sondern auch auf mit dem Internet verbundene Kraftwerke und Transportsysteme.

IT-Sicherheit

Kristin Petersen, Panda Security, erläutert in der Januar-Ausgabe des Behörden Spiegel den **„Cybercrime Trend 2018".** Hacker hätten es in zunehmendem Maße auf die Endpoints abgesehen, weil sie von dort aus leicht auf andere Ziele zugreifen, Informationen herausfiltern, Daten stehlen oder andere Angriffe starten könnten. Neue Angriffsvektoren trügen dazu bei, immer komplexere Angriffsszenarien zu kreieren. Da komme es beispielsweise vermehrt zu „malwarelosen" Attacken, die weder Schwachstellen ausnutzen noch schädliche URLs einsetzen, und gegen die konventionelle Abwehrmaßnahmen nicht funktionieren. Wenn Angreifer den Endpoint nicht erreichen, könnten sie nicht auf andere Ziele zugreifen. Während früher die Priorität darin gelegen habe, die Abwehr gegen Angriffe von außen zu verstärken, sei jetzt der Perimeter verschwommen, Mobilität in jedem Unternehmen die Norm und Unternehmensnetzwerke seien viel exponierter. Intelligente Systeme, die mithilfe cloudbasierter Scan-Technologien alle laufenden IT-Prozesse auf den Endpoints kontinuierlich überwachen, analysieren und klassifizieren, seien heute und in Zukunft alternativlos. Roland Schneider, Fortinet, prognostiziert in der Januar-Ausgabe des Behörden Spiegel für die nächsten Jahre eine ständige Ausweitung der Angriffsfläche bei gleichzeitigem Verlust von umfassender Transparenz und Kontrolle über jetzige Infrastrukturen. Obwohl das Ausmaß der Bedrohung durch Ransomware, Ransomworms und anderen Angriffsformen gegenüber 2016 bereits um das 35-Fache gestiegen ist, sei künftig mit noch mehr Attacken dieser Art zu rechnen. Man gehe davon aus, dass Cyberkriminelle KI-Technologien mit Multivektor-Angriffsmethoden kombinieren werden, um nach Schwachstellen zu suchen. Security-Lösungen müssten um integrierte Sicherheitstechnologien, umsetzbare Threat Intelligence und dynamisch konfigurierbare Security-Fabrics herum aufgebaut werden. Und die Security müsse mit digitaler Geschwindigkeit funktionieren. Dafür müssten nicht nur Reaktionen automatisiert werden. Die Security müsse auch selbstlernend sein, um effektive, autonome Entscheidungen treffen zu können.

Sicherheitslücke erschüttere Chiphersteller Intel, titelt die FAZ am 4. Januar. Die Sicherheitslücke erlaube es gewöhnlichen Computerprogrammen, auf Bereiche von Intel-Prozessoren zuzugreifen, die eigentlich geschützt sein sollten und sensible Daten wie Passwörter enthalten könnten. Sicherheitsforscher hätten mit **Meltdown und Spectre** zwei Angriffsszenarien beschrieben, die das Leck ausnutzen. Beseitigt werden könne die Schwachstelle offenbar nicht von Intel selbst, sondern nur durch Veränderungen der Betriebssysteme, also auf der Softwareseite. Microsoft bereite schon ein Software-Update für sein Betriebssystem Windows vor. Auch an notwendigen Veränderungen für das lizenzgebührenfreie Programm Linux werde gearbeitet. Diese Updates brächten aber offenbar den Nebeneffekt von möglicherweise langsameren Computern mit sich. Nach einer Meldung von heise.de am 5. Januar habe Apple mitgeteilt, alle Mac- und IOS-

Systeme seien von den sogenannten „speculative execution vulnerabilities" betroffen, wenn sie mit Intel- oder ARM-Chips ausgerüstet sind. Damit sei es Anwendungen möglich, auf Kernel-Bereiche zuzugreifen, auf die sie eigentlich nicht zugreifen dürften. So ließen sich etwa Passwörter auslesen, die in einem anderen Fenster eingegeben werden. Diese Probleme beträfen alle modernen Prozessoren und wirkten auf nahezu alle aktuellen Computer- und Betriebssysteme. Gefährdet seien, wie der Behörden Spiegel in der Januar-Ausgabe berichtet, alle Geräte, die komplexe Prozessorchips der Hersteller Intel, AMD, ARM und Qualcomm enthalten.

Wie sich Unternehmen nach einem Cyberangriff **vor Haftung schützen** können, erklären die Rechtsanwälte Jan Pohle und Christian Schoop in der FAZ am 10. Januar. Da es einen absoluten Schutz vor Cyberangriffen nicht gebe, gehöre zu einer ordnungsgemäßen Geschäftsführung nicht nur die Vorsorge, sondern auch ein Krisenplan für den Cyberangriff und das richtige Verhalten im Krisenfall. Mit Inkrafttreten der DS-GVO seien die zuständige Datenschutzbehörde und betroffene Kunden und Mitarbeiter von jeder Verletzung personenbezogener Daten unverzüglich, die Behörden binnen 72 Stunden zu unterrichten. Entscheidungsträger müssten ferner berücksichtigen, dass sie Ermittlungsbehörden einbinden müssen, wenn gegenüber Kunden eine ausdrückliche oder nebenvertragliche Pflicht hierzu besteht. Trotz der Pflicht zur Unterrichtung von Betroffenen habe die Staatsanwaltschaft in bestimmten Fällen ein Interesse daran, den Vorgang „geheim" zu halten, um verdeckt zu ermitteln. Das Unternehmen müsse für Abstimmung sorgen. Um Rechts- und Haftungsrisiken zu vermeiden, müssten die Verantwortlichen in internationalen Unternehmen nicht nur die Verpflichtungen in Deutschland, sondern auch die der weiteren betroffenen Jurisdiktion erfüllen.

Risiken einer Betriebsunterbrechung und von Cybervorfällen sind die größten Geschäftsrisiken in Deutschland. Das ist nach einem Bericht der FAZ vom 17. Januar das Ergebnis des sogenannten **Allianz Risk Barometer**. Der Industrieversicherer Allianz Global Corporate & Speciality (AGCS) habe 1.911 Experten aus 80 Ländern befragt. **Betriebsunterbrechungen seien in 55 Prozent der deutschen Antworten als größtes Risiko benannt worden** (2016: 40 Prozent), Cybervorfälle in 51 Prozent (Vorjahr 44 Prozent). Andreas Berger, Vorstand der AGCS: „Das neue Gold der digitalen Wirtschaft sind immaterielle Werte wie Daten, Plattformen, Netzwerke oder die Reputation des Unternehmens". Störungen in der Lieferkette sowie Cyberbedrohungen gehörten heute zu den größten Risiken. Das Programm „WannaCry" habe rund 200.000 Organisationen und Unternehmen weltweit getroffen. Fachleute schätzten den Schaden auf mindestens acht Mrd. Dollar. Laut AGCS steige das Potenzial sogenannter Cyber-Hurrikane, bei denen Hacker viele Unternehmen gleichzeitig lahmlegen.

Nach einem Bericht von silicon.de vom 23. Januar leidet das Lizenz-Managementsystem „**Hardware against Software Piracy (HASP)"** an verschiedenen schwerwiegenden Schachstellen (Kaspersky Lab). Die Gemalto-Lösung SafeNet Sentinel werde weltweit von Hunderttausenden Unternehmen genutzt, um Software zu legitimieren und diese freizuschalten. Kaspersky habe 14 Schwachstellen gefunden. Die Sicherheitsexperten warnen, dass diese Lecks hochgefährlich seien und Unternehmen einem hohen Risiko ausgesetzt seien. Da das System von vielen Unternehmen verwendet wird, dürfte auch die Zahl der verwundbaren Systeme hoch sein. Die Sentinel-Lösung funktioniere über so genannte Token. Mit diesen speziellen USB-Sticks könne ein Administrator auf einem Client-System überprüfen, ob es sich bei einer Software um eine Raubkopie handelt. Auch nachdem ein Administrator den Token wieder vom System entfernt hat, bleibe der Port geöffnet. Angreifer müssten daher in gepatchten und geschützten Unternehmensnetzwerken nur einmal eine Software installieren, die die HASP-Lösung verwendet, oder den USB-Token nur einmal mit einem PC verbinden, um den Port dauerhaft zu öffnen.

Deutschland muss sich auf Hackerangriffe einstellen, titelt die FAZ am 23. Januar. Es gebe heute mehr als 600 Mio. Schadprogramme. Allein mit Schadprogrammen, die Computer blockieren und zu Geiseln machen, werde Schätzungen zufolge **jedes Jahr eine Milliarde Dollar erpresst**. Nach Daten von IBM haben 70 Prozent der Unternehmenslenker, die von solchen Angriffen betroffen waren, das Lösegeld bezahlt, die Hälfte mehr als 10.000 Dollar, ein Fünftel sogar mehr als 40.000 Dollar. Einer Analyse des deutschen Versicherungsverbands zufolge koste es deutsche Unternehmen im Durchschnitt 609.000 Euro, Schäden aus der Verletzung von Betriebsgeheimnissen auszugleichen. Nur vier von zehn Unternehmen hätten einen Notfallplan erarbeitet, der festlegt, welche Schritte im Fall eines Angriffs folgen. Am besten vorbereitet seien in Deutschland noch die streng regulierten Unternehmen, die zur Kritischen Infrastruktur gehören: Telekommunikation, Energieversorger und Banken. Als übergreifendes Kompetenzzentrum für IT-Sicherheit sei von Konzernen in Deutschland 2015 die Deutsche Cybersicherheitsorganisation DCSO gegründet worden. Sie arbeite mit dem BMI und dem BSI zusammen. Teletrust fordere von

der zukünftigen Bundesregierung, dass sie mindestens eine Mrd. Euro im Jahr für Cybersicherheit ausgibt. Angesichts der jährlichen Schäden für die Wirtschaft von 55 Mrd. Euro sei eine solche Förderung nicht übertrieben.

Um sensible Daten auf staatlichen Servern vor Hackern zu schützen, hat das **Bayerische Landesamt für Sicherheit in der Informationstechnik** (LSI) seine Arbeit aufgenommen, heißt es in SZ.de am 29. Januar. Die IT-Spezialisten sollten sich darum kümmern, dass etwa Steuer-, Gesundheits- und Justizdaten nicht in falsche Hände gelangen. In der Behörde werde es eine Antihacker-Einheit geben, ein Lagezentrum, das die staatlichen Netze überwacht, ein „Profiling"-Team, das neue Angriffsmethoden untersucht, und eine Beratungseinheit, die Bürger und Kommunen unterstützt. Eine Art IT-Feuerwehr solle in Notfällen in kleinere Gemeinden geschickt werden können.

Wie die FAZ am 29. Januar berichtet, hat IBM eine **Umfrage zur Passwortsicherheit** bei 4.000 Internetnutzern weltweit durchgeführt. Je jünger die Befragten sind, desto laxer gehen sie mit Sicherheit um. Die Hälfte der Internetnutzer, die älter als 55 Jahre sind, benutzten komplexe Passwörter. Dafür verwendeten jüngere Internetnutzer häufiger Passwortmanager. Das sind Programme, in denen man komplexe Passwörter oblegen kann und sich dann nur ein starkes Master-Passwort merken muss. Das Programm füllt anschließend die verschiedenen Anmeldungen für Internetseiten automatisch aus. Getrieben von den jüngeren Generationen sei zudem die Authentifizierung mittelts biometrischer Daten. Der Fingerabdruck gelte für fast die Hälfte der Befragten als vertrauenswürdige Alternative zum Passwort.

Das BSI berichtet am 5. Februar über eine **repräsentative Umfrage** zusammen mit der „Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK)" **anlässlich des „**Safer Internet Days". Für 97 Prozent aller Internetnutzer in Deutschland sei die Sicherheit bei der Nutzung des Internets von hoher Bedeutung. Diese Ansicht führe jedoch nicht zwangsläufig zu einem sicherheitsbewussten Verhalten der User. Nur rund jeder Dritte informiere sich gezielt zum Thema IT-Sicherheit. Sicheres Surfen interessiere die Bürger vor allem dann, wenn es ums Geld geht. Für 71 Prozent aller Befragten sei speziell beim Online-Banking die Sicherheit besonders wichtig. Aber nur 45 Prozent sind beim Online-Shopping auf eine sichere Abwicklung bedacht. Sicheres Nutzen von sozialen Netzwerken (elf Prozent), Cloud-Diensten (acht Prozent) und vernetzten Heimgeräten zur Haussteuerung (vier Prozent) sei den Befragten dagegen kaum bis gar nicht wichtig. Von den 823 Befragten, die Opfer von Kriminalität im Internet geworden sind, habe sich über die Hälfte selbst geholfen, rund ein Viertel habe Familie, Freunde oder Bekannte um Hilfe gebeten, und nur rund jeder Fünfte (19 Prozent) habe Anzeige bei der Polizei erstattet.

Mehrere **Schwachstellen im Treibstoff-Managementsystem von Orpak Systems** bedrohten Tankstellen in mehreren Ländern, berichtet heise.de am 8. Februar. Davor warnten Sicherheitsforscher von Kaspersky. Neben der Überwachung von Füllständen von Sprittanks wickele die Software beispielsweise auch Bezahlvorgänge an öffentlichen Tankstellen ab. Die Sicherheitsforscher haben eigenen Angaben zufolge mehr als tausend Orpak-Systeme über die Suchmaschine Shodan gefunden, in die sie hätten einsteigen können. Aber es komme noch schlimmer: Bei der Analyse des Codes wären die Sicherheitsforscher auf eine Wartungs-Hintertür mit hartcodierten Zugangsdaten gestoßen. Darüber könnten Angreifer ihren Untersuchungen zufolge auf jede Orpak-Instanz mit Adminrechten zugreifen, selbst wenn ein Bestreiber das Standard-Passwort des Webinterfaces geändert habe. So könnten Angreifer in derartige Systeme einsteigen, Füllstände und Preise manipulieren und sogar Kreditkarten-Transaktionen hijacken und Bezahldaten mitschneiden.

IuK-Kriminalität

Im Oktober 2017 haben Analysten des Antiviren-Unternehmens Kaspersky Lab eine **Spionagesoftware entdeckt**, die auf das Android-Betriebssystem von Smartphones, Tablets und Netbooks ziele: **Skygofree,** berichtet die FAZ am 20. Januar. Ist ein Gerät infiziert, ließen sich Funktionen des Telefons kapern und fernsteuern. Skygofree verschaffe sich Zugriff auf Anruflisten, Kurznachrichten- und Messenger-Apps, den Aufenthaltsort, Kalender und anderweitig gespeicherte Daten. Mit Skygofree hätten potenzielle Angreifer 48 Befehle ausführen können. Mit dem Befehl „Geofence" lasse sich ein Standort festlegen, bei dem die Spionagesoftware automatisch das Mikrofon des Telefons einschaltet, um die Umgebung auszuhorchen. Das Gerät werde vom Nutzer unbemerkt mit von den Angreifern kontrollierten Wi-Fi-Netzen verbunden. Der Befehl „Camera" wiederum nutze die vorderseitige Bildschirmkamera des Geräts, um ein Foto zu machen, wenn ein Nutzer sein Smartphone oder Tablet entsperrt. Platziert worden sei die Software durch mobile Internetseiten, die das

Website-Design von Mobilfunkanbietern wie Vodafone oder Three nachahmten. Die Seiten würden den Nutzern vorschlagen, „ihre Konfiguration zu aktualisieren", damit sie wieder „mit vollen Geschwindigkeit" im Internet surfen könnten. Infizierte Geräte habe Kaspersky vornehmlich in Italien aufgespürt. Dorthin führe nach Angaben von Vincente Diaz auch die Spur der mutmaßlichen Urheber der Viren-Software. In Deutschland seien 2017 laut einer aktuellen Studie des amerikanischen IT-Sicherheitsunternehmens Norton by Symantec **23 Mio. Menschen Opfer von Cyberkriminalität** geworden, berichtet zeit.de am 23. Januar. Dabei sei ein Gesamtschaden von knapp 2,2 Mrd. Euro entstanden. Die größten finanziellen Schäden seien durch Identitätsdiebstahl, Angriffe mit Erpressersoftware und Kreditkartenbetrug entstanden. Von Ransomware seien sieben Prozent der Nutzer in Deutschland betroffen.

Sicherheitsforscher von Bitfender haben ein **neues Botnetz entdeckt**, das mittlerweile mehr als 20.000 IoT-Geräte gekapert haben und sich weiterhin stark ausbreiten soll, meldet heise.de am 25. Januar. Auch Geräte in Deutschland sollen Teil des auf den Namen „Hide'n Seek" getauften Botnetzes sein. Das Botnetz soll Funktionen beinhalten, die auf Spionage und möglicherweise auch auf anschließende Erpressungsversuche hindeuten.

Was tun gegen Cybermobbing? fragt die FAZ am 6. Februar. Der Internetrechtler Dirk Heckmann schlage schärfere Strafen für „Cybermobbing" vor: So solle es einen neuen Tatbestand „schwere Ehrverletzung im Internet" geben. Jedes fünfte Opfer von Cybermobbing habe Suizidgedanken, und 14 Prozent ließen die Attacken aus dem Netz zu Alkohol oder Tabletten greifen. Die Netzwerke der Anbieter sollten technische Maßnahmen zum Melden rechtswidriger Inhalte bereithalten. Die Abgrenzungsfragen seien „meist äußerst komplex" heiße es in Heckmanns Gesetzentwurf. Schon wegen der schieren Masse der Beschwerden sei das Risiko des „Overblocking", also des übermäßigen Löschens, unvermeidbar.

Eine bisher **unbekannte Malware-Familie missbrauche DNS-Pakete**, um darin heimlich kopierte Kreditkartendaten zu verstecken, meldet heise.de am 8. Februar. Da es sich bei dem Datenverkehr um UDP-Pakete handelt und die Malware Kassensysteme (Point of Sale, PoS) befällt, hätten die Entdecker den Schadcode UDPoS getauft. PoS-Installationen seien ein beliebtes Angriffsziel für Kriminelle. Besonders die Kassensysteme in kleineren Gastronomie-Betrieben und ähnlichen Geschäften liefen häufig noch auf Windows XP und seien deswegen besonders anfällig. Der Schadcode tarne sich unter dem Namen update.exe und extrahiere während der Ausführung dieser Datei die eigentliche Malware-Executables. Schaffe es die Malware, Magnetkarten-Daten aus dem Speicher des Kreditkartensystems zu lesen, schicke sie diese an den Kontrollserver. Auf Kassensystemen kopierte Magnetstreifendaten würden in der Regel dazu verwendet, die entsprechenden Kreditkarten zu klonen. Die Malware greife die Informationen aus Track 1 und 2 der Karten ab. Kopien könnten also dafür verwendet werden, mit den geklonten Karten vor Ort einzukaufen. Das funktioniere allerdings nur in Ländern, in denen Bezahlung mit Magnetkarten-Leser noch üblich sind. Die in Deutschland verbreiteten Chip- und PIN-Systeme könne ein so erstellter Klon in der Regel nicht austricksen.

Kommunale Sicherheit

„Es mangelt an vielen Ecken und Enden. **Kommunale Ordnungsdienste** können Aufgaben nicht effektiv wahrnehmen", titelt der Behörden Spiegel in der Januar-Ausgabe. Für sie griffen die meisten Kommunen auf Angestellte ohne Verwaltungsausbildung zurück. Über 70 Prozent der 184 nordrhein-westfälischen Kommunen, die sich an einer Online-Umfrage beteiligten, sähen ihren Ordnungsdienst nicht in der Lage, die entsprechenden Aufgaben ohne Vollzugshilfe der Polizei durchzuführen. Sie könnten keine weiteren Aufgaben übernehmen und die Einsatzzeiten nicht auf 24 Stunden ausweiten, wie es die Polizei fordere. Eine effiziente Aufgabenwahrnehmung wäre möglich, wenn die Ordnungsbehörden über entsprechende Personalkapazitäten sowie eine qualifizierte Ausbildung und Ausrüstung verfügen würden.

Korruption

Die sogenannte **strukturelle Korruption** ist auch in Deutschland fest verwurzelt, schreibt Dipl.-Verwaltungswirt EKHK Ingo Sorgatz in der Januar-Ausgabe des Behörden Spiegel. Auch in der deutschen Verwaltung zeige die Korruption einen zehnjährig linear steigenden Trend. Dass die öffentliche Beschaffung, der Baubereich oder das Förderwesen Aufgabensektoren mit dauerhaft hohen Korruptionsrisiken sind, liege auf der Hand und enge das Ermessen etwa in

Bezug auf die Implementierung von Vorgangs- und Vor-Ort-Kontrollen (Mehraugen-Prinzip, Annehmen von Geschenken, Rotation etc.) erheblich ein. Zunächst einmal müssten sich die Fachbereiche selbst um ein professionelles internes Kontrollsystem bemühen. Anti-Korruptionsbeauftragte und Interne Revisionen seien in erster Linie Berater und Signalgeber.

Krisenmanagement

Pascal Michel, smartrisksolutions, plädiert in der Ausgabe 1/2-2018 der Zeitschrift PROTECTOR, S. 86/87, für eine **strukturierte Vorbereitung im Krisenmanagement**, d. h. insbesondere für eine Richtlinie zum Thema Opfer- und Angehörigenbetreuung; ein Handbuch mit Regelungen von Zuständigkeiten sowie Schnittstellen zum Krisenstab und zur Unternehmenskommunikation; Leitfäden und Schulungen für die einzusetzenden Mitarbeiter; Notfallübungen.

Ladendiebstahl

Hendrick Lehmann beschreibt in der Ausgabe 1/2-2018 der Zeitschrift PROTECTOR, S. 52–54, den **Ladendiebstahl und Gegenmaßnahmen** im Einzelhandel. 2016 habe das durchschnittliche Niveau der Inventurdifferenzen laut der aktuellen Studie des EHI bei 0,57 Prozent des Nettoumsatzes gelegen. In Euro bedeute das einen Verlust durch Diebstahl im Wert von etwa 3,4 Mrd. Euro. Der Schaden durch Mehrwertsteuerausfälle belaufe sich auf rund 460 Mio. Euro jährlich. Das Dunkelfeld schätze Frank Horst, EHI Retail Institute, auf 98 Prozent. Teilweise versuchten die Täter, die Warensicherungen zu manipulieren, indem sie mit Folie ausgestattete Taschen nutzten. Auf gewerbsmäßige Tätergruppen entfalle mittlerweile etwa ein Viertel des Gesamtschadens der Diebstähle. Rund 15.000 Ladendetektive seien in Deutschland im Einsatz. Im Schnitt gebe jeder Händler etwa 0,32 Prozent seines Umsatzes für Diebstahl reduzierende Maßnahmen aus. Je nach Branche könne das Budget auch mal bis zu 0,97 Prozent des Umsatzes erreichen, etwa bei Unterhaltungselektronik. Mitarbeiterschulungen seien sicherlich die kostengünstigste Möglichkeit, Inventurdifferenzen zu reduzieren. Videoüberwachung sei eine der häufigsten Präventionsmaßnahmen. Die Kameras im Innenbereich verfügten über erweiterte Sichtwinkel und HD-Auflösung, womit sich gleichzeitig je zwei Gänge überwachen ließen. Damit sei nur die Hälfte an Kameras für eine vollflächige Überwachung ohne tote Winkel notwendig, als dies bei analogen Kameras der Fall wäre.

Ladungsdiebstahl

Wie die Leipziger Internet Zeitung am 8. Februar meldet, hat die Arbeitsgemeinschaft Diebstahlprävention in Güterverkehr und Logistik **Maßnahmen gegen Ladungsdiebstähle** vorgestellt. Wie groß das Problem tatsächlich ist, zeigten jetzt erstmals erstellte gemeinsame Berechnungen mehrerer Wirtschaftsverbände unter Beteiligung des Bundesverbandes Güterkraftverkehr Logistik und Entsorgung (BGL) e. V. Demnach würden jährlich Ladungen von nahezu 26.000 Lkw gestohlen. Statistisch schlügen Kriminelle in Deutschland also alle 20 Minuten zu. Allein die gestohlenen Güter hätten einen Wert von 1,3 Mrd. Euro. Weitere Schäden von 900 Mio. Euro entstünden durch Konventionalstrafen für Lieferverzögerungen, Reparaturkosten sowie Umsatzeinbußen und Produktionsausfälle bei den eigentlichen Abnehmern. Die Arbeitsgemeinschaft wolle die Sicherheit der Transportlogistik insbesondere durch höhere Sicherheitsstandards und Investitionen in Ortungstechnik, Diebstahlwarnanlagen, Wegfahrsperren und gesicherte Parkplätze erhöhen. Von den Behörden forderten die Verbände dringend mehr Unterstützung durch einen höheren Fahndungsdruck auf die international und professionell agierenden kriminellen Organisationen. Die Polizei müsse zudem auf Autobahn-Rastplätzen häufiger präsent sein.

Logistiksicherheit

Hochaufgelöste Videotechnik sei für die moderne Logistik ohne Alternative, heißt es in der Ausgabe 1/2-2018, S. 52/53, der Fachzeitschrift GIT. Bei Galliker Transport & Logistics mit 18 Niederlassungen in sechs Ländern würden die Zugänge zum Gelände und den Gebäuden von Videokameras überwacht. Der Portier nutze die Videoüberwachung für die Zuteilung der Parkplätze und Rampen. Tore und Schranken öffneten sich bei der Anfahrt bei den Galliker eigenen oder den registrierten Fahrzeugen automatisch. Dies werde mittels Fahrzeugnummernerkennung ausgelöst.

Maschinensicherheit

Das **Sicherheitskonzept für die Gießstrecke einer Gießerei** stellt SSP-Safety System Products GmbH & Co. KG in der Ausgabe 1/2-2018 der Zeitschrift GIT, S. 70/71, vor. Rauhe Umgebungstemperaturen in der Gießerei erforderten besonders robuste Komponenten. Mit Schlüsseltransfersystem und einem ganzheitlichen Sicherheitskonzept aus Schutzzaun und Lichtvorhang entspreche SSP – Safety System Products dieser Anforderung. Eine Besonderheit sei die Extracted-Key-Funktion, die durch das Abziehen persönlicher Sicherheitsschlüssel optimalen Schutz biete. Die Funktionsweise sei dabei denkbar einfach: Bevor das Personal für die Instandhaltung die Anlage betritt, müsse der Sicherheitsschlüssel gezogen und mit in die Anlage genommen werden. Ohne den Schlüssel könne die Anlage nicht gestartet werden.

Der Begriff „**Wireless Safety**" habe in den letzten Jahren an Bedeutung gewonnen, schreiben die Autoren Dr. Mathias Bohge, R3 – Reliable Realtime Radio Communications GmbH, und Peter Brinkmann, Schleicher Electronic Engineering GmbH, in der Ausgabe 1/2-2018, S. 78–80, der Zeitschrift GIT. Notstopp-Signale oder andere sicherheitsrelevante Informationen müssten dabei ohne Wenn und Aber zuverlässig und in Echtzeit übertragen werden. Genau das sei allerdings das Problem beim Thema „Wireless Safety". Verbindungsabbrüche bei der Datenübertragung und bei Safety-Anwendungen seien kritisch und erforderten ein sofortiges Absichern des Systems. Datenübertragung in Sicherheitssystemen erfolge durch Nutzung von Sicherheitsprotokollen. Mit deren Hilfe würden alle Übertragungsfehler erkannt und führten nie zu einer gefährlichen Situation. Bei mehrfachen Fehlern schalte sich das System aber selbst ab, und das System oder die Anlage werde in Stillstand versetzt. Die Hauptherausforderung bestehe also darin, Übertragungsfehler zu verhindern und Daten zuverlässig zu übertragen. Eine neue Generation der Kabellos-Übertragungstechnik müsse darum bezüglich Echtzeitfähigkeit und Zuverlässigkeit signifikante Verbesserungen mit sich bringen. Das EchoRing-System sei eine solche neuartige Übertragungstechnik, die auf massiver Kooperation basiere. Der EchoRing-Ansatz basiere auf einem Token-Passing-Verfahren, genauer auf einer logischen Token-Ring-Architektur. Die Autoren beschreiben Anforderungen an Wireless-Safety-Handbediengeräte und die Nutzung von Standardhardware.

In Deutschland führten arbeitsbedingte Unfälle 2015 zu einem Produktionsverlust von 46 Mrd. Euro. Zudem sei es **2016** zu **877.071 arbeitsbedingten Verletzungen** in Deutschland gekommen, die jeweils mehr als drei Fehltage nach sich zogen. In der Zeitschrift GIT, Ausgabe 1/2-2018, S. 88–90, erklärt Prabhu Soundarrajan, Honeywell Industrial Safety, wie modernste Sicherheitsmanagement- und Monitoring-Software es ermögliche, Sicherheitsprozesse zu optimieren und die Kosten für die Einhaltung der Sicherheitsvorschriften und die Wartung zu reduzieren. Sicherheitsmanagement-Software wie die Connected Worker Platform von Honeywell nehme sich dieser Herausforderungen an. Die Plattform vereinfache mit ihrer intuitiven und benutzerfreundlichen Oberfläche die Konfiguration, Überprüfung und Wartung der Geräte. Noch wichtiger sei, dass die neuesten Softwarelösungen einen Zugriff auf die Daten in Echtzeit und von einem entfernten Standort aus ermöglichen. Die Plattform unterstütze Angebote, die zur Mitarbeitervernetzung beitragen. Die Automatisierung sorge dafür, dass tragbare Gasdetektoren und andere Geräte Daten automatisch direkt und in Echtzeit an den Kontrollraum übermitteln können.

Naturkatastrophen

Für die Versicherungen sei **2017 das teuerste Jahr der Geschichte,** berichtet die FAZ am 5. Januar. Die versicherten Schäden aus Wetterkatastrophen hätten die Branche rund 135 Mrd. Dollar gekostet und damit mehr als je zuvor. Das gehe aus einer Untersuchung hervor, die der Rückversicherer Munich Re in München veröffentlichte. In der Versicherungswirtschaft nähmen die Sorgen zu, dass sich Schadensjahre wie 2017 – mit den Wirbelstürmen Harvey, Inna und Maria – und 2011 – mit dem Tohoku-Erdbeben und der Katastrophe in Fukushima – häufen. Nach einer Meldung der FAZ vom 26. Januar habe der GDV seine Angaben über Sachschäden präzisiert. Danach wird der versicherte **Gesamtschaden auf eine Mrd. Euro geschätzt**. 900 Mio. entfielen auf Sachschäden an Gebäuden, 100 Mio. auf Schäden an Kfz.

Personenschutz

Protective Intelligence für den Personenschutz thematisiert Oliver Schneider, RiskWorkers GmbH, in PROTECTOR, Ausgabe 1/2-2018, S. 84/85. Sie gehe weiter als Vorfeld-

aufklärung und nutze unter anderem den Cyberraum, um Gefahren und Risiken zu erkennen. Protective Intelligence sei also das Identifizieren, Aufbereiten, Bereitstellen und Bewerten von Informationen aus Tätersicht unter Nutzung aller rechtlich zulässigen Verfahren und Quellen. Neben der Limitierung der Suchmaschinen für die Suche nach relevanten Informationen im Internet und auf Social-Media-Plattformen seien vor allem das Know-how und die technischen Fähigkeiten wichtig, auch im Darknet und Deepweb nach Informationen zu suchen. Der ausschließliche Einsatz von „Suchmaschinen" greife zu kurz, da wesentliche Informationen durch Verschleierung von ihnen nicht gefunden werden könnten.

Schließsysteme

Die Fachzeitschrift GIT stellt in der Ausgabe 1/2-2018, S. 42–44, das System ÜLock-B Inductive vor, das eine **neue Generation von Funk-Sicherheitsschlössern** eröffne. Die „Revolution" liege in einer neuen und hochinnovativen Form der Energieversorgung. Durch automatische induktive Energieübertragung zwischen Schloss und Schließblech gehörten Batterietausch und eine Verkabelung des Türblatts tatsächlich der Vergangenheit an. Die Spannungsversorgung erfolge über die Türzarge. Der Strom werde von dort aus induktiv über einen kleinen Spalt vom Schließblech direkt in das Schloss übertragen. Eine Vielzahl an unterschiedlichen Ansteuerungssystemen verschiedenster Anbieter sei kompatibel (Fingerscan, RFID, Tastatur). Das Schloss verriegele automatisch, sobald die Tür geschlossen ist, durch einen 20 Millimeter-Fallenriegel. Die gesamte Technik inklusive Elektronik befinde sich im Schlosskasten, wodurch keinerlei Angriffsfläche für Manipulationen gegeben sei.

Sicherheitsgewerbe

GIT weist in der Ausgabe 1/2-2018, S. 10, auf die **Lünendonk-Studie 2017** „Sicherheitsdienstleister in Deutschland" hin. Nach dieser Studie wird die Verfügung über gut ausgebildete Mitarbeiter von Seiten der Anbieter zunehmend als Wettbewerbsvorteil erkannt. Mit dem Wegfall respektive der Ausschreibung des bisher kurzfristigen Bedarfs des Schutzes von Flüchtlingsunterkünften werde der Preis wieder ein stärkeres Gewicht in der Vergabe erhalten. Dies werde aller Voraussicht nach zu sinkenden Margen und in den kommenden Jahren zur Beschleunigung der Marktkonsolidierung führen.

Smart-Home-Technik

Immer mehr **Versicherer wollen die Smart-Home-Technik nutzen**, meldet die FAZ am 23. Januar. Kunden sollten so das Gefühl von schneller Hilfe erleben. Inzwischen gebe es nahezu ein Dutzend Kooperationen zwischen Versicherern und Anbietern von Smart-Home-Technik in Deutschland. Versicherungskunden bekämen ein Starterpaket an intelligenten Sensoren, die im Haus an Wasserleitungen, Fenstern, Türen und an der Decke anzubringen sind. Sie sollen ihm auf sein mobiles Endgerät Hinweise auf einen Einbruch, Brand oder Wasserschaden senden. Die Einbindung der Versicherer mache es möglich, ein Netzwerk an erprobten Handwerkern einzubinden, die den Schaden frühzeitig beheben. Eine Meldung an die Feuerwehr sei oft ebenfalls integriert.

Überspannungsschutz

Mit ausfallsicheren Signalwegen und Überspannungskonzepten zur prozesstechnischen Sicherheit befasst sich in der GIT, Ausgabe 1/2-2018, S. 74–76, Dipl.-Ing. Ralf Hausmann, Phoenix Contact. In der Prozesstechnik bestehe für ausgedehnte Anlagen ein erhöhtes Ausfallrisiko durch Überspannungen mit oftmals weitreichenden Folgen für Personen und Umwelt. Der Einsatz von Überspannungsschutzgeräten sei nicht nur empfehlenswert, sondern gemäß DIN VDE 0100-443 auch vorgeschrieben. Der Autor geht der Frage nach, wieviel Platz für SPDs (surge protective devices) benötigt wird. Er behandelt den Einsatz in explosionsgeschützten Bereichen, die einfache Überwachung, die Blitzschutznormen empfehlen, und das von der für SPDs relevanten Anwendungsnorm EN 61643-22 beschriebene mehrstufige Überspannungsschutzkonzept. Jedem Blitzschutzzonenübergang sei eine Schutzgeräte-Kategorie zugeordnet. Mit **Termitrab complete** habe Phoenix Contact ein maßgeschneidertes Produktprogramm am Markt, das weit mehr als nur das Grundbedürfnis nach Überspannungsschutz abdecke. Die platzsparende, wartungsunterstützende und robuste Ausführung erlaube einen vielfältigen Einsatz.

Unternehmensstrafrecht

Unternehmen müssten sich aufgrund des Koalitionsvertrages auf **deutlich höhere Geldbußen** von Ermittlungsbehörden einstellen, meldet die FAZ am 9. Februar. Das Ziel der neuen Regelung seien „Unternehmenssanktionen". Statt der Einführung eines Unternehmensstrafrechts solle der Bußgeldkatalog verschärft werden. An die Stelle der heutigen Obergrenze von zehn Mio. Euro sollen Bußgelder sich an der „Wirtschaftskraft" orientieren – bei Unternehmen mit mehr als 100 Mio. Euro Umsatz betrage die Höchstgrenze hiervon zehn Prozent. Künftig müssten Bußgeldverfahren zwingend eingeleitet werden – ohne Ermessensspielraum der Behörden. Sanktionen gegen börsennotierte Unternehmen sollen künftig in einem Register ausgewiesen werden. Dabei handele es sich um eine neue Datenbank neben dem erst kürzlich eingeführten Wettbewerbsregister.

Videoüberwachung

Der Fernbusanbieter Flixbus teste derzeit **Videoüberwachung in Gepäckräumen** als Maßnahme gegen Drogenschmuggel, berichtet heise online am 25. Januar. Flixbus erhoffe sich eine abschreckende Wirkung auf Schmuggler. Die Polizei führe regelmäßig Personenkontrollen an Bord von Fernbussen durch.

GIT stellt in der Ausgabe 1/2-2018, S. 55, einen **intelligenten, sicheren und effizienten Speicher** für kontinuierliche Videoüberwachung (SkyHawk AI) vor. Netzwerk-Videorecorder (NVRs) würden immer häufiger mit Analysesensoren ausgestattet. Die Verwendung von KI-Anwendungen wie Gesichtserkennung und die Analyse von Unregelmäßigkeiten im Verhalten werde immer häufiger. Parallel dazu steige der Bedarf an schneller Videoanalyse, was den Workload des NVR-Speichers in die Höhe treibe. Sky Hawk AI eigne sich ideal für rechenintensive Workloads, die normalerweise mit KI-Workflows einhergingen. Der hohe Durchsatz und das verbesserte Caching sorgten für niedrige Latenzzeiten und eine hervorragende Random-Read-Performance, um Bilder schnell zu lokalisieren und Videomaterial für die Analyse bereitzustellen.

Waffenrecht

Auswirkungen einer Reduzierung von Waffenscheinen von 2013 bis 2017 um 37 Prozent für die Sicherheitswirtschaft untersucht Stefan Kiessling, Bundesvereinigung der Waffenträger in der Sicherheitswirtschaft (BVWSW) in der Ausgabe 1/2-2018 der Zeitschrift PROTECTOR, S. 82/83. Ein wesentlicher Grund für diese Reduzierung sei ein Urteil des BVerwG vom 11.11.2015, wonach Bewachungsunternehmer eine **Erlaubnis zum Führen von Schusswaffen nur noch für konkrete Bewachungsaufträge** erhalten können, für die glaubhaft gemacht ist, dass aus Gründen der Sicherung einer gefährdeten Person oder eines gefährdeten Objekts Schusswaffen erforderlich sind. Im Gegensatz zum Firmenwaffenschein, bei dem der Sicherheitsunternehmer selbst entscheiden könne, ob eine Tätigkeit bewaffnet durchgeführt wird, müsse er dem Urteil des BVerwG zufolge nun eine konkretisierte Einzelgenehmigung für jeden einzelnen Bewachungsauftrag beantragen. Die BVWSW fordere, dass Bedürfnisüberprüfungen und Gefährdungsanalysen zeitnah durchgeführt werden und dabei transparent, fair und frei von jeglicher Willkür sein müssen. Auch müsse dabei den wirtschaftlichen Interessen der Berufswaffenträger in einem angemessenen Maß Rechnung getragen werden. Wie absurd Begründungen sein können, erschließe sich am Beispiel einer Beurteilung eines Polizeipräsidiums, das verdeckte Bargeldtransporte unter 250.000 Euro für nicht ausreichend gefährdet halte, um sie bewaffnet durchzuführen.

Wettbewerbsregister

Den „weiten Weg zum Wettbewerbsregister" skizziert Rechtsanwalt Dr. Oliver Homann in der Januar-Ausgabe des Behörden Spiegel. Während die technischen Voraussetzungen für das Register 2018 geschaffen werden sollen, werde die Rechtsverordnung erst für 2019/2020 erwartet. Erst nachdem das Register installiert und die Rechtsverordnung in Kraft getreten ist, würden die Meldepflichten für die Strafverfolgungsbehörden und die Abfragepflichten für die öffentlichen Auftraggeber gelten.

Zutrittskontrolle

Ein „**Zutrittskontroll-Komplettterminal" mit Video-sprechanlage** von Hikvision Europe stellt GIT in der Ausgabe 1/2-2018, S. 40/41, vor. Mit seinem integrierten Mifare-Leser und Hikvision Fingerabdrucksensor biete das Gerät verschiedene Authentifizierungsmöglichkeiten. Am wichtigsten sei, dass sich das DS-K1T501-Terminal dank seiner integrierten Kamera zum Auslesen moderner virtueller Zugangsdaten wie QR-Codes einsetzen lasse. Das Gerät biete auch die Möglichkeit, eine zusätzliche Verifizierung per Gesichtserkennung auszuführen. Es verfüge über die gängigsten Kommunikationstechnologien. Den Installateuren stünden mehrere Möglichkeiten zum Konfigurieren der jeweiligen Kommunikationsverbindungen zur Verfügung.

GIT weist in der Ausgabe 1/2-2018, S. 48/49, darauf hin, dass das **Zutrittssystem AirKey** von EVVA um einige neue Features erweitert worden sei: „Send a Key", „Geo-Tagging" (das Smartphone wisse, wo sich die Komponenten der Schließanlage befinden) und iPhone-Kompatibilität (durch die Erweiterung der bisherigen NFC-Komponenten (nur für Android) mit Bluetooth Low Energy sei der Nutzerkreis um ein Vielfaches erweitert worden. Der qualitativ hochwertige AirKey-Zylinder habe Sicherheitsfeatures wie Kernzieh- und Aufbohrschutz, Rotationsbremse und ein integriertes Secure-Element für sichere Datenspeicherung.

Impressum

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

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

Herausgeber
Manfred Buhl, Vorsitzender der Geschäftsführung, Düsseldorf

Verantwortlicher Redakteur
Bernd Weiler, Leiter Kommunikation und Marketing

Beratender Redakteur
Reinhard Rupprecht, Bonn

www.securitas.de/focus

Kontakt

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

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

E-Mail: info@securitas.de