FOCUS ON SECURITY

AUSGABE 05, MAI 2018

SECURITAS

Inhaltsverzeichnis

Arbeitsschutz

Sicherheitsschuhe für Mitarbeiter mit Fußerkrankungen thematisiert GIT-SICHERHEIT in der Ausgabe 4-2018, S. 96/97. Fußschutz sollte auf die individuellen Bedürfnisse der Träger eingehen – etwa, wenn sie unter Einschränkungen leiden. Das Fußschutzmodell „Dialution" von Elten verbinde zwei wesentliche Eigenschaften: Zum einen wirke der Spezialschuh präventiv und kurativ bei individuellen Fußproblemen. Zum anderen sei der Schuh aufgrund seiner vielfältigen Einsatzmöglichkeiten ein Allrounder, der auch an Arbeitsplätzen mit erhöhter Verletzungsgefahr zuverlässig schütze.

Automatensicherheit

Security insight weist in der Ausgabe 2-2018, S. 36, darauf hin, dass über 700 Fahrkartenautomaten der Berliner Verkehrsgesellschaft (BVG) mit dem **Geminy-System** nachgerüstet worden seien. Geminy-Produkte würden die Schließzylinder hinter einem gehärteten Stahlschieber schützen. Potenzielle Täter versuchten erst gar nicht, so geschützte Automaten aufzubrechen. Die Vorrichtung halte Manipulation, Schlagtechnik, Ziehen, Bohren, Verkleben, Verstopfen, Abbrechen und Vandalismus stand. Die Härtung und die galvanische Veredelung mit einem korrosionsbeständigen Dreischicht-System aus Kupfer, Nickel und Chrom gewährleisteten enorme Stabilität und Widerstandskraft.

Betrug

Wie das BKA am 27. April mitteilt, melde sich ein angeblicher **„Daniel Fischer" vom Auswärtigen Amt** per E-Mail oder am Telefon bei deutschen Unternehmen und bitte um ein vertrauliches Gespräch mit der Geschäftsleitung. In dem Gespräch wolle er erläutern, dass die Bundesregierung für den Freikauf deutscher Geiseln in Mali finanzielle Unterstützung der Privatwirtschaft benötige. Das BKA rät, das Gespräch zu beenden und bei der örtlichen Polizeidienststelle Anzeige zu erstatten. Es könne nützlich sein, sich die Telefonnummer des Anrufers zu notieren und den Vorfall bei der Bundesnetzagentur zu melden.

Biometrie

HDI Global stellt in sicherheit.info die Zwei-Faktor-Authentifizierungs- und Verifizierungsplattform **HID Approve** vor. Das neue iPhone X von Apple biete mit der Gesichtserkennung Face ID einen sicheren Zugang zu Online- oder Mobile-Banking und digitalen Signaturen, die bei Finanztransaktionen zum Einsatz kommen. Auch der Remote Zugriff auf Unternehmensapplikationen und -daten könne so gesichert werden. HID Global biete Unternehmen nun die Möglichkeit, die Vorteile von Apples Face ID in Verbindung mit der Authentifizierungslösung HID Approve zu nutzen. Dies sei eine App, die aus einem mobilen Gerät einen „Authentifikator" macht. Damit könnten Online-Zugriffe und Transaktionen wie der VPN-Zugang zum Unternehmensnetz oder Überweisungen zusätzlich abgesichert werden. HID Global kombiniere die Gesichtserkennungstechnologie mit Threat Detection und Intelligence, sodass Unternehmen potenzielle Betrugsversuche oder missbräuchliche Nutzungen schneller erkennen können.

Brandschutz

Ansaugmelder in der Elbphilharmonie thematisiert PROTECTOR in der Ausgabe 4-2018, S. 48/49. Für die Branddetektion im Großen Saal seien nur Ansaugrauchmelder in Frage gekommen, da der Saal eine Höhe von 25 Metern aufweist. Zusammen mit Wärmesensorkabeln im Boden der Besucherränge steuerten die Geräte eine Hochdrucknebellöschanlage an. Wird ein Brand detektiert, dann würden die Sprinklerköpfe der Löschanlage vorgeflutet, bis dahin seien sie trocken. Detektieren die Wärmekabel zusätzlich einen Anstieg der Temperatur im Raum, löse die Löschanlage erst aus. Durch die Täuschungsalarmsicherheit komme es nur bei einem echten Brand zu diesem Szenario.

Eine Komplettlösung für sichere **Fluchtwege in Tiefgaragen** stellt GfS – Gesellschaft für Sicherheitstechnik mbH in der Ausgabe 4-2018 der Zeitschrift PROTECTOR, S. 50/51, vor. Als Kernkomponente komme ein Einhand-Türwächter zum Einsatz. Dieser werde mit einem selbstverriegelnden Antipanikschloss in der Ausführung Wechselfunktion E und einem Klinke-/Knaufbeschlag kombiniert. Das Schloss habe den Vorteil, dass es immer, wenn die Tür geschlossen ist, über die Schlossfalle und den Schließriegel verriegelt sei.

So sei eine Sabotage mittels Scheckkarte oder ähnlichen Hilfsmitteln unmöglich. Eine Begehung im Notfall sei Dank des GfS Einhand-Türwächters über die Türklinke jederzeit möglich. Wird die Klinke gedrückt, löse dies einen Alarm aus, der optional per Funk oder Kabel auf weitere Alarmgeber oder Telefonzentralen aufgeschaltet werden könne.

Dipl.-Ing. (FH) Heidi Burow-Strafhoff, G+H ISOLIERUNG GmbH, befasst sich in PROTECTOR, Ausgabe 4-2018, S. 52/53, mit der **Eindämmung von Kabelbränden.** G+H habe mit dem „PYROMENT IK90" einen Installationskanal entwickelt und geprüft, der aus einem Blechkanal mit im Inneren aufgebrachtem Dämmschichtbildner besteht. Mit Dämmdicken von 1,6 bis drei Millimeter reagiere er auf Hitze, schäume auf, schmiege sich wie eine innenliegende Isolierung an die Kabel und Rohre und stoppe damit aktiv eine Brandweiterleitung auch im Inneren des Kanals. Das System gebe es auch in runder Ausführung. Damit könnten Rohre mit Synthesekautschukisolierungen in Rettungswegen schnell ummantelt werden.

Compliance

In der Beilage „Zukunft Mittelstand" weist die FAZ am 26. April auf eine Anfang 2018 herausgegebene Studie des F.A.Z.-Instituts und der Prüfungs- und Beratungsgesellschaft Ebner Stolz hin, mit der die **Compliance-Brennpunkte in mittelständischen Unternehmen** untersucht wurden. Beteiligt haben sich 447 Entscheider aus großen und mittleren Unternehmen. Und es habe sich ein ernüchterndes Bild gezeigt: Jedes fünfte Unternehmen war in den letzten zwei Jahren in Compliance-Verstöße involviert – mit beträchtlichen Schadenssummen. Sie hätten sich bei 42 Prozent auf mehr als 100.000 Euro belaufen. Bei knapp mehr als der Hälfte der Unternehmen seien Schäden durch Compliance-Verstöße von mehr als 50.000 Euro entstanden. 99 Prozent der Großunternehmen und 80 Prozent der Mittelständler hätten Compliance-Risiken für sich als wesentlich eingestuft. Die größten Risiken würden in den Themen IT-Sicherheit und Datenschutz gesehen (94 und 95 Prozent). Auch dem Steuerrecht werde erhebliches Risikopotenzial zugeschrieben: 85 Prozent der Unternehmen hätten Steuerrecht als wichtiges Compliance-Handlungsfeld ausgemacht. Am risikoträchtigsten seien die Verrechnungspreise und die Umsatzsteuer. Befeuert worden seien die Compliance-Sorgen durch eine Verschärfung der Rechtsprechung zu strafbefreienden Selbstanzeigen und der Reaktion der Finanzverwaltung hierauf. Diese stehe auf dem Standpunkt, dass ein steuerliches internes Kontrollsystem die Unternehmen im Einzelfall vom Vorwurf einer leichtfertigen Steuerverkürzung entbinden könne. Mehr als die Hälfte der Großunternehmen verfüge über ein „Tax Compliance Management System" (CMS). In mittelständischen Unternehmen bestehe hingegen Nachholbedarf. Nur sechs Prozent verfügten über ein solches System. Die Implementierung entsprechender Prozesse für ein Tax CMS sei im Steuerbereich extrem komplex, weil zahlreiche Schnittstellen der Steuerabteilung zu anderen Abteilungen bestünden. Während 91 Prozent der Großunternehmen bereits Compliance-Richtlinien eingeführt hätten, hielten nur 66 Prozent der mittelständischen Unternehmen ein entsprechendes Regelwerk vor. 73 Prozent der Großunternehmen hätten ein unternehmensweites Compliance-Managementsystem eingeführt. Im Mittelstand seien es hingegen nur 27 Prozent.

Datenschutz

Henning Bulka beantwortet auf RP.ONLINE am 5. April **die wichtigsten Fragen zur DSGVO,** die am 25. Mai in Kraft tritt. Sie betreffen den Geltungsbereich der VO, die Änderungen für die Bürger und für Unternehmen, die zweijährige Übergangsfrist, Sanktionen bei Verstößen, die Möglichkeit einer neuen Abmahnwelle und die Notwendigkeit eines unternehmenseigenen Datenschutzbeauftragten. Für Unternehmen seien die verschärften Dokumentations- und Rechenschaftspflichten wichtig: ob der Nutzer oder Kunde seine ausdrückliche Zustimmung dazu gegeben hat, dass seine Daten gespeichert und verwendet werden dürfen. Die Zustimmung müsse das Unternehmen nachweisen. Wie personenbezogene Daten verarbeitet werden, wer darauf Zugriff hat und wie die Daten geschützt werden, müssten Unternehmen mit der DSGVO in einem „Verzeichnis von Verarbeitungstätigkeiten" festhalten. Nötig sei dies zum Beispiel, wenn ein Betrieb Personalakten elektronisch verwaltet oder eine Kundendatei führt. Über die Anforderungen, etwa an die technische Umsetzung, herrsche noch an vielen Stellen Unklarheit. Künftig sei es zudem noch wichtiger, Daten nur zweckgebunden zu verwenden.

Die DSGVO ist in 11 Kapitel gegliedert:

Kap. 1: Art. 1–4 (Gegenstand und Ziele, Anwendungsbereich, Begriffsbestimmungen)

Kap. 2: Art. 5–11 Grundsätze (Grundsätze für die Datenverarbeitung, Rechtmäßigkeit der Verarbeitung, Bedingungen für die Einwilligung)

Kap. 3: Art. 12–23 Rechte der betroffenen Person (Transparenz und Modalitäten, Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten, Berichtigung und Löschung, Widerspruchsrecht und automatisierte Entscheidungsfindung, Beschränkungen)

Kap. 4: Art. 24–43 Verantwortlicher und Auftragsverarbeiter (Allgemeine Pflichten, Sicherheit personenbezogener Daten, Datenschutzbeauftragter, Verhaltensregeln und Zertifizierung)

Kap. 5: Art. 44–50 Übermittlung personenbezogener Daten an Drittländer (Allgemeine Grundsätze, Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses und vorbehaltlich geeigneter Garantien, verbindliche interne Datenschutzvorschriften, nach Unionsrecht nicht zulässige Übermittlung oder Offenlegung, Ausnahmen, internationale Zusammenarbeit)

Kap. 6: Art. 51–59 Unabhängige Aufsichtsbehörden (Unabhängigkeit, Zuständigkeit, Aufgaben und Befugnisse)

Kap. 7: Art. 60–76 Zusammenarbeit und Kohärenz (Zusammenarbeit der Aufsichtsbehörden, Kohärenz, Europäischer Datenschutzausschuss)

Kap. 8: Art. 77–84 Rechtsbehelfe, Haftung und Sanktionen (Beschwerde bei einer Aufsichtsbehörde, gerichtlicher Rechtsbehelf gegen eine Aufsichtsbehörde, gegen Verantwortliche oder Auftragsverarbeiter, Aussetzung des Verfahrens, Haftung und Schadenersatz, Verhängung von Geldbußen, Sanktionen)

Kap. 9: Art. 85–91 Vorschriften für besondere Verarbeitungssituationen (Meinungsäußerung und Informationsfreiheit, Zugang der Öffentlichkeit zu amtlichen Dokumenten, Verarbeitung der nationalen Kennziffer, Datenverarbeitung im Beschäftigungskontext, Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken, Geheimhaltungspflichten, Datenschutzvorschriften von Kirchen und religiösen Gemeinschaften)

Kap. 10: Art. 92–93 delegierte Rechtsakte und Durchführungsrechtsakte (Ausübung der Befugnisübertragung, Ausschussverfahren)

Kap. 11: Art. 94–99 Schlussbestimmungen (Aufhebung der Richtlinie 95/46/EG, Verhältnis zur Richtlinie 2002/58/EG, Berichte der Kommission, Überprüfung anderer Rechtsakte der Union zum Datenschutz, Inkrafttreten und Anwendung)

heise.de berichtet am 10. April über einen Beitrag von Justin Hendrix, NYC Media Lab, und David Carroll, Parsons School of Design, in Technology Review online. Auch wenn **Facebook** den Zugriff auf seine Nutzerdaten nach dem Datenmissbrauch durch Cambridge Analytica inzwischen eingeschränkt habe, gebe es heute mehr Informationen über Bürger auf dem Markt als je zuvor. Zusammen würden die Methoden Data-Mining, künstliche Intelligenz, Psychologie, Marketing, Ökonomie und experimentelle Design-Theorie einen exponentiellen Anstieg bei der Zahl der Überwachungssensoren bringen – von Sprachassistenten bis zu Technik im Internet der Dinge, die ihre Nutzer den ganzen Tag über begleiten. Unsere Geräte würden immer besser darin werden, Gesichtsausdrücke zu erkennen, Sprache zu verstehen und physiologische Signale zu analysieren. Es sei an der Zeit, solche Technologien als mögliche Bedrohung zu betrachten.

Datensicherheit

Der US-Kongress habe Ende März den Ermittlern weltweiten Zugriff auf Server verschafft, die US-Firmen gehören, berichtet Friedhelm Greis auf ZEIT ONLINE am 21. April. Die EU-Kommission habe noch weiterreichende Pläne vorgestellt. Das Besondere dabei: Die von der Gesetzgebung betroffenen Staaten könnten in gegenseitigen Abkommen künftig weltweit ihren Ermittlern Zugriff auf Server erlauben, ganz unabhängig von deren Standort. Der **Cloud Act** sehe daneben ausdrücklich vor, dass die USA mit ausländischen Staaten Regierungsvereinbarungen treffen. Sie sollten ausländischen Ermittlungsbehörden den Zugriff auf Daten erlauben, die von US-Firmen gespeichert werden. Im Gegenzug sollten die US-Ermittler ebenfalls Zugriff auf Daten von US-Bürgern haben, die in dem entsprechenden Land gespeichert sind. Dabei sollten die Datenschutzbestimmungen des anderen Landes nicht beachtet werden müssen. Das bisherige System der Rechtshilfeabkommen wäre in diesen Fällen obsolet. Auch der Vorschlag der EU-Kommission sehe vor, dass Strafverfolgungsbehörden weltweit auf Daten zugreifen können, die von Internetfirmen gespeichert werden, die ihre Dienste in der EU anbieten. Die betroffenen Firmen sollten nur dann die Heraus-

gabe elektronischer Beweismittel verweigern dürfen, wenn Gesetze in ihrem Heimatland das untersagen oder Daten von Personen aus anderen Ländern betroffen sind. Aus diesem Grunde liege es nahe, dass die europäischen Staaten mit den USA ein entsprechendes Regierungsabkommen abschließen, das den gegenseitigen Zugriff auf Daten ermöglicht. Bürgerrechtsorganisationen warnen, es gebe keine Vorgaben, was den Straftatenkatalog für den Datenzugriff betrifft. Die Ermittler seien weder dazu verpflichtet, die betroffene Person zu informieren, noch das Land, in dem die Person sich aufhält oder in dem die Daten gespeichert werden.

Ein **„Siegel für sichere Daten"** titelt die FAZ am 3. Mai. Mit zwei neuen Prüfsiegeln – eines für Produkte und eines für Dienstleistungen – könnten sich Unternehmen vom TÜV bestätigen lassen, dass sie dessen Standards erfüllen. In einem globalen „Center of Excellence IoT Privacy" begleiteten TÜV-Fachleute die Entwicklung speziell unter dem Aspekt der Sicherheit und des Schutzes privater Daten. Die Entwicklungen zur künstlichen Intelligenz seien eine der Herausforderungen. Schadsoftware werde „intelligenter" und passe sich Abwehrprogrammen an, sodass die Verteidiger ebenfalls aufrüsten müssten.

Datenübertragung

GIT-SICHERHEIT.de befasst sich am 28. Februar mit der **kabellosen Übertragungstechnik** („Wireless Safety"). Eine neue Generation der Kabellos-Übertragungstechnik müsse bezüglich Echtzeitfähigkeit und Zuverlässigkeit signifikante Verbesserungen mit sich bringen. Das EchoRing System sei eine solche neuartige Übertragungstechnik, die auf massiver Kooperation basiere. Im Kontext des Zukunftskonzeptes Industrie 4.0 werde sich der Grad der Vernetzung von Produktionsmitteln, -gütern, Maschinen und Mitarbeitern so erhöhen, dass sich eine rein kabelbasierte Vernetzung von Safety Anwendungen nicht mehr darstellen lassen werde. Das EchoRing System von R3 Communications sei ein hochzuverlässiges und gleichzeitig echtzeitfähiges Kabellossystem. Es basiere auf einem Token-Passing Verfahren, einer logischen Token Ring Architektur. EchoRing erfülle Echtzeitanforderungen im Bereich weniger Millisekunden. Daten, die über den EchoRing übertragen werden, gelangten spätestens nach einer garantierten Signallaufzeit vom Sender zum Empfänger. Und es erfülle hohe Ansprüche an die Übertragungsqualität. Bei der Übertragung von hunderttausend Telegrammen gebe es im Schnitt maximal ein Bit, das fehlerhaft ist.

Einbruch

Wie nnz-online.de am 5. Mai berichtet, hat das Securitas Operation Center **(SOC) im ersten Quartal 2018 19** Prozent **weniger Einbrüche** registriert als in den ersten drei Monaten des Vorjahres. Besonders stark sei gegenüber dem 1. Quartal 2017 der Rückgang der im SOC erfassten Echteinbrüche bei Drogeriegeschäften (minus 80 Prozent), im Lebensmittelhandel (minus 36 Prozent) und im sonstigen Einzelhandel (minus 47 Prozent) gewesen. Allerdings seien in diesen drei Branchen die Einbruchzahlen immer noch auf relativ hohem Niveau. Der höchste Anstieg im 1. Quartal 2018 sei bei Einbrüchen in Baumärkte (125 Prozent) und in Banken (67 Prozent) registriert worden. Die Versuchsquote sei sehr unterschiedlich auf verschiedene Branchen verteilt. Die relativ hohen Versuchsquoten – im Bankensektor 50 Prozent – , die nur den Anteil der Versuche umfassen, bei denen Alarm ausgelöst wurde, sprächen für die Wirksamkeit der präventiven Abwehr von Einbrechern durch mechanische und elektronische Sicherungsmaßnahmen, insbesondere im Bereich von Eingangstüren und Fenstern.

Geldautomatensicherheit

Am 19. April hat das BKA das Bundeslagebild **„Angriffe auf Geldautomaten 2017"** vorgestellt. 2017 ist die Zahl der Sprengungen von Geldautomaten (GA) um 16 Prozent auf 268 zurückgegangen. In Deutschland würden insbesondere reisende Täter solche Taten verüben. Hier dominierten Tätergruppierungen aus den Niederlanden. Intensive Bekämpfungsmaßnahmen in Nordrhein-Westfalen und Niedersachsen hätten zu einem Verdrängungseffekt geführt. Niederländische Tätergruppierungen hätten ihren Aktionsradius insbesondere auf Hessen, Rheinland-Pfalz und Baden-Württemberg ausgeweitet. 2017 sei ein erneuter Anstieg der Skimming-Fälle auf 499 zu verzeichnen gewesen, mit dem Brennpunkt Berlin. Überwiegend kämen Tatverdächtige aus Bulgarien und Rumänien. Der Schaden sei um 15 Prozent auf 2,2 Mio. Euro gestiegen. Trotzdem zeige sich, dass die in den letzten

Jahren mit der Umstellung auf Chiptechnologie eingeführten, überwiegend technischen Sicherheitsmaßnahmen greifen. Es werde deutlich, dass die Täter durch andersartig gestaltete Angriffe auf GA auf die Veränderung im Skimmingbereich reagieren und sich neu aufstellen. Beispiel hierfür seien vermehrte Hackingangriffe auf GA-Netzwerke, die im Gegensatz zum Skimming eine wesentlich höhere Gewinnerwartung versprächen. Grundsätzlich eröffneten die fortschreitenden technischen Entwicklungen, wie z. B. die auch in Deutschland immer weiter verbreitete NFC (Near Field Communication)-Funktion bei Zahlungskarten, neue Tatgelegenheiten.

Hotelsicherheit

IT-Sicherheitsforscher hätten eine **Schwachstelle in elektronischen Schließsystemen** von Hotels entdeckt, berichtet Süddeutsche.de am 25. April. Die Schwachstelle betreffe mehr als eine Million Hotelzimmer in 166 Ländern. Die Türen könnten geöffnet werden, ohne Spuren zu hinterlassen. Die Angreifer könnten eine Hotelkarte mit Hilfe eines technischen Geräts klonen, um anschließend alle Gästezimmer des jeweiligen Hotels zu betreten. Dafür werde ein eigener Generalschlüssel errechnet. Hotelgäste könnten sich aber weiterhin sicher in ihren Zimmern fühlen, denn die Forscher hätten Jahre gebraucht, um die Schwachstelle aufzuspüren. Das Risiko sei also gering.

Internet der Dinge

Die Lichttechnik-Konzerne Osram und Philips verbinden Licht mit dem Internet der Dinge, berichtet die FAZ am 2. Mai. Die von Osram entwickelten **Funkleuchten** könnten als Sensordatenquellen dienen, die auf der von Osram entwickelten Plattform für das Internet der Dinge aufgesetzt würden. Über smarte Komponenten, Anwendungen und Programme seien zum Beispiel sensorbasierte Logistiklösungen in Lagergebäuden möglich. Konkurrent Philips Lighting setze auf Datenübertragung durch Licht, arbeite also nach einem anderen Prinzip als das Funkwellen-Modell von Osram/Nokia. Das sichtbare Lichtspektrum sei eine ungenutzte Ressource mit großer Bandbreite für eine stabile Verbindung von mehreren IoT-Geräten. Die Technik biete sich in Umgebungen mit hohen Sicherheitsanforderungen an, zum Beispiel in einem Finanzinstitut oder in staatlichen Institutionen. Das System mit dem Namen **„Light Fidelity"** biete eine zusätzliche Sicherheitsebene, weil Licht keine festen Wände durchdringen kann und ein direkter Sichtkontakt zum Licht benötigt wird, um auf das Netzwerk zuzugreifen. Somit ergäben sich andere Anwendungsprofile als für die Deckenleuchte von Osram.

Die **Verknüpfung von physischen Sicherheitskomponenten mit dem IoT** habe zweierlei Vorteile: Zum einen maximiere das harmonische Zusammenspiel aller Komponenten im System die Effektivität, zum anderen übermittelten die individuellen Hardwareeinheiten Daten, die bei richtiger Handhabung eine Business Intelligence ermöglichen (GIT-SICHERHEIT.de vom 24. April). Die Vorteile von IoT und vernetzten Sicherheitssystemen zeige das Beispiel eines Parkplatzes, auf dem verschiedene Technologien über ein Netzwerk zusammenarbeiten und so die Zutrittskontrolle sichern. Die Komponenten des Systems kommunizierten über offene Protokolle miteinander. Die standardisierte, sichere Kommunikation ermögliche die Einbindung verschiedener Komponenten von verschiedenen Herstellern. Dadurch könnten Unternehmen die für ihre Bedürfnisse am besten geeigneten Geräte nutzen.

IT-Sicherheit

Benjamin Stiebel befasst sich in der April-Ausgabe des Behörden Spiegel mit **IT-Sicherheit und Datenschutz in Druckumgebungen**. Die Druckumgebung sei ein „blinder Fleck" in den Sicherheitskonzepten. Eine der wichtigsten Baustellen sei die Datenhaltung. Drucker speicherten standardmäßig Nutzerdaten inklusive Inhalten der verarbeiteten Dokumente auf internen Festplatten. Eine Verschlüsselung dieser Daten sei notwendig. Metadaten sollten im Idealfall abgeschaltet oder nur anonymisiert übertragen werden. Auch Übertragungswege im Netzwerk vor Ort müssten abgesichert werden. Der Zugriff auf die Druckerfestplatte von außen sollte gesperrt sein. Mindestens dann, wenn hohe Anforderungen an die Geheimhaltung gelten, sollten Druckdaten auch verschlüsselt übertragen werden. Noch bevor technische und organisatorische Maßnahmen im Detail ausgearbeitet werden, müsse auf allen Ebenen Bewusstsein geschaffen werden. Im zweiten Schritt seien klare Verantwortlichkeiten festzulegen. Unverzichtbar sei die Rückendeckung durch die Unternehmensleitung.

Krzysztof Paschke, GRC Partner GmbH, behandelt in der April-Ausgabe des Behörden Spiegel die Compliance Management Software **DocSetMinder**. Sie setze mit dem Modul „IT-Grundschutz" konsequent alle Anforderungen und die Methodik des modernisierten IT-Grundschutzes um. Durchdachte Softwarefunktionen unterstützten die Anwender aktiv in jeder Phase des Sicherheitsprozesses von der Planung über die Umsetzung bis hin zum Audit. Für den Übergang von den BSI-Standards 100-2/-3 zu 200-2/-3 werde der parallele Betrieb gewährleistet. In Kombination mit den Modulen „EU-DSGVO" und „Notfallmanagement" sei DocSetMinder eine Komplettlösung für die Informationssicherheit und den Datenschutz.

Prof. Reiner Creutzburg, TU Brandenburg, weist in der April-Ausgabe des Behörden Spiegel auf einen Aktionsplan hin, mit dem die Europäische Kommission die Chancen nutzen wolle, die sich aus technologiegestützten **Innovationen bei Finanzdienstleistungen** ergeben. Sie werde ein U-FinTech-Labor einrichten und habe bereits das „EU Blockchain Observatory and Forum" aus der Taufe gehoben, das 2018 über Chancen und Risiken von Krypto-Anlagen berichten werde. Die Kommission werde auch Workshops veranstalten, um den Informationsaustausch im Bereich der Cybersicherheit zu verbessern. Noch stehe Blockchain vor einigen Herausforderungen und keinesfalls seien alle Fragen zur Sicherheit von konkreten Anwendungen der Technologie geklärt.

Nach Berichten amerikanischer Sicherheitsbehörden und des britischen NCSC sollen **russische Hacker** seit über zwei Jahren systematisch die Netzwerke von Unternehmen und Regierungsorganisationen infiltriert haben (FAZ vom 18. April). Dabei hätten sie vor allem Router genutzt, um ihre Ziele auszuspionieren, geistiges Eigentum zu stehlen und sich einen dauerhaften Zugang zu Netzwerken zu verschaffen. Unternehmen, Internetprovider und alliierte Staaten sollten daher mehr für die Sicherheit ihrer Router tun. Gerade in kleineren Unternehmen seien sie nur selten mit Schutzprogrammen ausgestattet. Häufig lieferten Firmen die Geräte mit Software aus, die leicht zu bedienen ist, aber auch ebenso leicht zu knacken. In Fällen, in denen der Router eine Abfrage von außen nicht erlaube, täuschten die Hacker dem Gerät vor, innerhalb des Netzwerks zu sitzen.

Um Unternehmen Tipps zum Schutz gegen Cyberangriffe zu geben und aufzuzeigen, wie diese bei Betroffenheit einer Cybercrime-Straftat vorgehen können, stellen die Zentralen Ansprechstellen Cybercrime (ZAC) der LKÄ und des BKA mit der Neuauflage der Broschüre „**Cybercrime – Handlungsempfehlungen für die Wirtschaft** (PDF 473KB)" nützliche Informationen für Wirtschaftsunternehmen zur Verfügung. Darauf weist das BKA auf seiner Website hin. Zudem solle die Broschüre dazu ermutigen, strafrechtlich relevante Vorfälle bei der Polizei anzuzeigen, und darüber informieren, was in solchen Fällen von der Polizei erwartet werden könne. Denn nur durch einen engen Schulterschluss von Polizei und Wirtschaft könnten Täter ermittelt, von weiteren Taten abgehalten und so Cybercrime nachhaltig bekämpft werden. Davon profitierten Unternehmen und deren Geschäftspartner.

Wie die FAZ am 3. Mai berichtet, wird die für die Finanzstabilität zuständige EZB mit den wichtigsten Finanzinstituten des Euroraums **Cybermanöver** durchführen, um die Widerstandsfähigkeit der jeweiligen Computersysteme zu prüfen. Die Tests sollten wirklichkeitsnah die Taktiken und Vorgehensweisen von Kriminellen nachzeichnen. Ein größerer Schaden könne das Vertrauen in das gesamte Finanzsystem untergraben.

In den **Chips von Intel** klaffen laut einem Bericht des Computermagazins „c't" acht neue gravierende Sicherheitslücken, meldet faz.net am 3. Mai. Besonders betroffen seien Anbieter von Cloud-Diensten wie Amazon. Die niemals endende Patch-Flut sei keine akzeptable Lösung.

Wegen einer internen Sicherheitslücke hat der Online-kurzmitteilungsdienst **Twitter** seine etwa 330 Mio. Nutzer aufgefordert, vorsichtshalber ihre Passwörter zu ändern, meldet zeit.de am 4. Mai. Ein jetzt in der Software entdeckter Fehler habe dazu geführt, dass Passwörter unverschlüsselt in einem internen Verzeichnis gespeichert worden seien. Die Vorsichtsmaßnahme sei sinnvoll, obwohl der Fehler inzwischen behoben sei.

Cybersicherheit sei ein zentrales Zukunftsthema für **Handwerksbetriebe**, betont das BSI am 23. April. Das BSI und der Zentralverband des Deutschen Handwerks (ZDH) weiten ihre gemeinsamen Anstrengungen für mehr Cybersicherheit im Handwerk aus. Der ZDH sei seit Oktober 2017 aktives Mitglied der Allianz für Cybersicherheit. Zu den Maßnahmen, die zum Cybersicherheitstag am 11. Juli in Münster vorgestellt würden und die den Handwerksbetrieben in Sachen Cybersicherheit unmittelbar weiterhelfen könnten, zählten eine Online-Präsenz mit zielgruppenspezifischen Informationen zur IT-Sicherheit für Handwerksbetriebe und das Konzept für die Multiplikatoren-Schulungen „Cybersicherheit im Handwerk".

Das BSI hat am 24. April Empfehlungen an KMU zum **sicheren Einsatz von Breitband-Routern** gegeben. Im Allgemeinen würden Internetzugänge mithilfe von DSL-, Kabel- oder Glasfaser-Anschlüssen realisiert. Eine Netzanbindung an diese Anschlüsse erfolge bei KMU überwiegend durch Breitband-Router. Häufig bilde ein solcher Router die einzige zentrale und wesentliche Sicherheitskomponente zum Schutz des internen Netzes. Gelinge einem Angreifer der Zugriff auf den Router, könne er auf verschiedene Weise Schaden verursachen. Die BSI-Veröffentlichung fasst wesentliche Aspekte zusammen, die beim Kauf bzw. bei der Miete eines Breitband-Routers beachtet werden sollten. Des Weiteren werden Empfehlungen für einen sicheren Betrieb von Routern ausgesprochen. Die Empfehlungen beziehen sich auf den Zugriffsschutz (Benutzeroberfläche und WLAN), auf die Aktualisierung der Firmware, auf Dienste und Portweiterleitungen, auf Telefonie, Virtual Private Network, auf das Management-Informationssystem, die Konfiguration, die Multifaktor-Authentifizierung und die Kundenbetreuung.

Dr. Michael Spehr, Redaktion der FAZ, befasst sich in der Ausgabe vom 8. Mai mit dem **Schutz von Cloud-Daten gegen Verschlüsselungs-Trojaner**. Mit der nahtlosen Anbindung des Cloud-Speichers an den eigenen PC sei man im Unterschied zu einer Datensicherung auf externen Laufwerken nicht gegen Verschlüsselungs-Trojaner geschützt. Einige Cloud-Anbieter böten Schutz gegen solche Schädlinge und würden auch helfen, wenn Excel-Tabellen zerstört oder Word-Dokumente gelöscht wurden. Nun bringe Microsoft einen ähnlichen Schutz für seinen Cloud-Speicher Onedrive auf den Markt. Microsoft wolle sogar Ransomware erkennen, um anschließend die Wiederherstellung der betroffenen Dateien vorzuschlagen. Bislang ließen sich Dateien oder Ordner in der Form eines Links freigeben. Der Link gewähre den Zugriff. Künftig lasse sich zusätzlich ein Kennwort setzen, sodass Dritte über den Link allein nicht mehr an die Inhalte gelangen. Microsoft prüfe, ob der Link eventuell zu einer verdächtigen Seite führt, und warne dann den Nutzer.

IuK-Kriminalität

Trend Micro weist auf eine **neue Schadsoftware für Apples macOS** hin, die sich derzeit über speziell gestaltete Word-Dokumente verbreite (so silicon.de am 6. April). Sie richte sich speziell gegen Macs, auf denen die Programmiersprache Perl installiert ist. Ihre Aufgabe sei es, Macs dauerhaft zu kompromittieren, zu überwachen und Daten zu sammeln. Der als OSX_OCEANLOTUS.D bezeichnete Schädling werde den Forschern zufolge wahrscheinlich per E-Mail verbreitet – bisher offenbar nur im Rahmen einer Spear-Phishing-Kampagne. Das infizierte Word-Dokument gebe vor, von einer vietnamesischen Organisation namens HDMC zu stammen, die sich für Demokratie und nationale Unabhängigkeit einsetzt. Öffnet ein Opfer die Word-Datei, werde er aufgefordert, die Ausführung von Makros zu aktivieren, was die Hintertür ausführt und einen Dropper sowie eine schädliche XML-Datei in den Systemordner einschleuse. Der Dropper wiederum führe seine Aufgaben auch dann aus, wenn der aktive Nutzer nicht als Root angemeldet ist.

Hacker könnten öffentliche Notfallalarmsysteme des Herstellers ATI Systems zum Teil übernehmen und beispielsweise **Fehlalarme auslösen**, berichtet heise.de am 12. April. Das hätten Sicherheitsforscher von Bastille entdeckt. Ihre Ergebnisse stellten sie auf der Website zur SirenJack getauften Schwachstelle vor. Dort könne man auch prüfen, welche Systeme betroffen sind. Der Missbrauch sei möglich, da die Systeme mit einem unverschlüsselten Funkprotokoll arbeiten. So könne ein Hacker mit einem vergleichsweise günstigen Funksender für rund 30 Dollar und einem Computer in die Kommunikation einsteigen und Aktivierungsbefehle absetzen. Mittlerweile habe sich ATI Systems um die Problematik gekümmert und wolle nach Tests zeitnah Sicherheitspatches zur Verfügung stellen.

Nach Erhebungen von IT-Sicherheitsanbietern bleiben **Angriffe auf Daten lange unentdeckt**, berichtet die FAZ am 18. April. Die Schätzungen, wann ein Abfluss von Daten bemerkt wurde, reichten von 175 Tagen bis zu anderthalb Jahren. Der deutsche Mittelstand sehe das locker. Das sei das Ergebnis einer Umfrage der Commerzbank unter 2.000 mittelständischen Unternehmen. Zwar hielten 73 Prozent der Unternehmen Angriffe mit Trojanern oder Viren für eine reale Bedrohung, doch griffen selbst Mittelständler, die von Cybercrime betroffen waren, nicht häufiger auf technische IT-Sicherheitsmaßnahmen zurück.

Spiegel.online berichtet am 16. April, Wissenschaftler der Ben-Gurion-Universität in Israel hätten eine Möglichkeit gefunden, wie man Daten über das Stromnetz von einem Rechner schmuggeln kann – selbst dann, wenn der Rechner praktisch unter Quarantäne steht und keinerlei Online-Verbindung hat. **„Powerhammer"** würden die Forscher

ihre Software nennen. Voraussetzung sei allerdings, dass der Computer bereits vor dem Angriff mit einer Schadsoftware infiziert worden ist. Über das Stromnetz könnten dann unter anderem Sicherheitsschlüssel und Passwörter ausgelesen werden. Die sensiblen Daten würden komprimiert und mit einer bestimmten Frequenz über das Stromkabel übertragen. Die Anwendungen auf dem PC laufen nach Angaben der Wissenschaftler währenddessen wie gewohnt weiter, ohne dass die Opfer der Attacke etwas davon merken. Die Übertragungsrate sei allerdings sehr „mickrig".

Forscher des chinesischen Sicherheitsanbieters Qihoo 360 haben eine Zero-Day-Lücke im **Microsoft-Browser Internet Explorer** entdeckt, meldet silicon.de am 24. April. Sie werde derzeit „weltweit" von einer Hackergruppe eingesetzt, um Windows-PCs mit Malware zu infizieren. Die Angriffe erfolgten bisher aber nur zielgerichtet gegen einzelne Opfer. Die Lücke betreffe offenbar alle aktuellen Versionen des Microsoft-Browsers.

Iranische Hacker haben laut einem Bericht des Spiegel Zugriff auf Daten von 23 deutschen Universitäten erhalten, berichtet golem.de am 20. April, Demnach seien mehrere Dokumente von ihnen kopiert worden. Darunter befänden sich auch nicht veröffentlichte Forschungsarbeiten. Die Angriffe seien bereits seit 2014 erfolgt. Es könne sein, dass die Angreifer durch Methoden wie Social Engineering an sicherheitsrelevante Informationen oder Passwörter gelangt sind.

Cyberkriminelle verschaffen sich Zugang zu **Onlineshops von Magento**. Darauf weist Peter Niggl in Security insight, Ausgabe 2-2018, S. 14, hin. Kriminelle sollen sich Zugriff auf über 1.000 Onlineshops verschafft haben, wie das New Yorker IT-Sicherheitsunternehmen Flashpoint bekannt gegeben habe. Der Cyberangriff sei zum einen durch Versuche mit Standard-Passwörtern in das System einzudringen, erfolgt, zum anderen sei er über ein so genanntes Brute-Forcing erfolgt. Flashpoint habe die IP-Adressen eines Großteils der gehackten Shops in den USA und Europa lokalisiert.

Kommunale Sicherheit

In der April-Ausgabe des Behörden Spiegel erläutert Reinhard Rupprecht, Securitas Deutschland, warum das Potenzial der privaten Sicherheitsdienstleister mit ihren über 260.000 Beschäftigten zur **Unterstützung der kommunalen Sicherheit** längst nicht ausgeschöpft ist und beschreibt folgende Möglichkeiten: Bestreifung und Kontrolle auch großflächiger Wohnquartiere im Auftrag von Wohnungsgesellschaften; Unterstützung des kommunalen Ordnungsdienstes insbesondere durch Bestreifung von Angsträumen während der Dunkelheit und an Wochenenden; Beteiligung an der Entwicklung einer Gesamtkonzeption kommunaler Sicherheit; Teilnahme an nicht-kommerziellen Ordnungspartnerschaften.

Luftverkehrssicherheit

PD Markus Bierschenk, Bundespolizeipräsidium, äußert sich in der April-Ausgabe des Behörden Spiegel zu **notwendigen Veränderungen** im Funktionsbereich der Luftverkehrssicherheit. Der Bedarf an Kontrolltechnik, an Polizeibeamten und Luftsicherheitsassistenten steige bei gleichzeitig wachsenden Anforderungen an Kompetenz und Zuverlässigkeit. Die Entwicklung der Sprengstoffdetektion habe diverse Szenarien zu berücksichtigen, wie sie umfangreicher noch nie waren. BMI und Bundespolizei beabsichtigten, an den Röntgengeräten für das Handgepäck die automatische Erkennung von Festsprengstoffen zu aktivieren. Die Nachrüstung der Geräte sei bereits erfolgt. Eine weitere zukunftsweisende Entwicklung könne die Einbeziehung von Computertomografen in die Handgepäckkontrolle darstellen. Eine gute und strukturierte Passagiervorbereitung, -information und -steuerung durch Flughafenbetreiber und Airlines übten maßgeblich Einfluss auf die Kontrollsituation aus. Die Bundespolizei und die Sicherheitsdienstleister seien mit immer höheren Peaks und immer beengteren Platzverhältnissen konfrontiert. Hier bestehe dringender Handlungsbedarf. Technische Systeme seien ein Beispiel, wie gegengesteuert werden kann. So würden zum Beispiel Sensoriksysteme heute bei der Berechnung der Passagierströme einschließlich deren Eintreffverhaltens an den einzelnen Prozessstellen helfen. Die Verantwortung für die Steuerung von Fluggast- und Gepäckkontrollen könne künftig an die Flughafenbetreiber übertragen werden.

Maschinensicherheit

Armin Hornberger, Pepperl+Fuchs, stellt in der Ausgabe 4-2018 der Zeitschrift GIT, S. 84/85, die **Positioniersysteme** „safePXV" und „safePGV" vor. Basis der neuen Sicherheitstechnologie sei die seit Jahren bewährte und besonders zuverlässige Kombination aus einem 2-D-Lesekopf und dem DataMatrix-Code. Allerdings komme bei den genannten Systemen ein spezielles Band mit zwei sich überlagernden DataMatrix-Codes in Rot und Blau zum Einsatz. Das eigentliche Gehirn dieser Positioniersysteme sei die innovative, neue Firmware. Durch sie würden die unterschiedlichen LED-Farben mit einem als sicher zu bewertenden Algorithmus angesteuert. Jeder Code werde dann unabhängig im Sicherheitsteil des Sensors direkt auf Plausibilität überprüft. Dabei müsse die mathematisch zufällige Blitzfolge mit der tatsächlichen Position übereinstimmen. Es werde stetig geprüft, ob die Software in der Kamera noch korrekt funktioniert. Eine einzigartige und absolut zuverlässige Sensor-Technologie kontrolliere permanent sich selbst. Entstanden sei so ein System, das erstmals die hohen Sicherheitsanforderungen nach SIL 3/PLe erfüllt – und das hoch effizient mit nur einem Sensor. Optimal geeignet sei der neue safePXV für lineare sichere Absolut-Positionierung von Elektrohängebahnen, für Regalbediengeräte in der Lager- und Fördertechnik, Drehtische im Maschinenbau sowie für den Aufzugsbau und für Windräder. Der neue safePGV sei für die Navigation von fahrerlosen Transportsystemen in der Lager- und Fördertechnik, der Zuführung und der Produktion optimiert worden. Beispielsweise könne in der Automobilfertigung jederzeit ein Mindestabstand zwischen den Fahrzeugen sichergestellt und der Schutz aller daran beschäftigten Personen gewährleistet werden. Im Bereich von Krananlagen sei es mit der neuen Safety-Technologie sehr effizient und ohne großen Aufwand möglich, die Arbeitssicherheit deutlich zu erhöhen. Auch beim Ent- und Umladen von Containern in Hafenanlagen könne die neue Technologie die Sicherheit deutlich erhöhen.

Dipl.-Ing. (BA) Johanna Schüßler, Bihl+Wiedemann, erläutert in der Ausgabe 4-2018 der Zeitschrift GIT, S. 86–88, wie Sicherheitstechnik mit AS-i Safety Gateways effizient **in Feldbusse integriert** werden. Die Gateways sammeln die Daten sicherheitstechnischer Komponenten in der Peripherie einer Anlage ein und transportieren sie in der Funktion eines „Bus-Bahnhofs" in Netzwerke und Steuerungswelten unterschiedlicher Hersteller. Komplexe Automatisierungslösungen könnten so dezentral – und damit transparenter, flexibler, performanter, beherrschbarer und deutlich kostengünstiger – organisiert und realisiert werden. Besonders performant würden die Safety Gateways, wenn sie über die sichere Kopplung Safe Link um fast 2.000 sichere Ein- und Ausgänge erweitert werden. Für das übergeordnete Netzwerk stelle das Gateway unabhängig von der Teilnehmerzahl im Feld jedoch nur einen einzigen „Slave" dar, der die kommunikative Stabilität des Feldbusses nicht beeinträchtigt. Die sichere Feldbuskommunikation sei in die Gateways integriert – sie verschafften sicherheitsgerichteten Sensoren und Aktoren einen „direkten Draht" zu allen gängigen Automatisierungssystemen. Es gebe eine Reihe von Kostenaspekten, mit der sich die wirtschaftliche Effizienz der AS-i Safety Gateways und der mit ihnen realisierten Konzepte belegen lasse. Erfahrungsgemäß stelle sich mit As-i Safety Gateways bei Aufbau, Verkabelung und Inbetriebnahme eine unmittelbare Kostenersparnis von über 50 Prozent ein. Die nachträgliche Erweiterbarkeit sei über den Kostenaspekt hinaus auch ein Beweis für die Flexibilität, die die steuerungsunabhängige Integration von Sicherheitstechnik bietet. Das Konzept biete in vielerlei Hinsicht einzigartige Effizienzvorteile.

Für die Sicherheit von Maschinen gibt es **drei Gruppen von Normen**, nämlich die Gruppen A, B und C. In einer mehrteiligen Artikelserie für GIT-SICHERHEIT befasst sich Jens Rothenburg von der Firma Euchner vor allem mit den übergeordneten A- und B-Normen – und der Frage, wie sie im praktischen Umgang zu nutzen sind. In Teil 3 dieser Beitragsreihe (GIT 3-2018) sei die Methodik zur Risikobeurteilung mit Hilfe des Anhangs A der EN ISO 13849-1 vorgestellt worden. In diesem Beitrag (Ausgabe 4-2018, S. 90/91) wird die Methodik aus der EN 62061 betrachtet. Beide Verfahren erfüllten grundsätzlich die Vorgaben der EN ISO 12100 Sicherheit von Maschinen (A-Norm).

Museumssicherheit

Schutzkonzepte für Kulturgüter behandelt Hendrick Lehmann in PROTECTOR, Ausgabe 4-2018, S. 26–28. Die Reiss-Engelhorn-Museen in Mannheim hätten einen Notfallplan für Kunst- und Kulturobjekte in Dauerausstellungen ausgearbeitet, der verschiedenen Szenarien Rechnung trage. Ein solches Konzept gliedere sich in zwei Teile, in eine Notfall- und eine Katastrophenplanung. Für jedes Gebäude sei ein „Notfall-Kit" zu erstellen, das im Ernstfall eine schnelle Sicherung und Bewahrung des Objektes ermögliche. In vielen deutschen Städten existiere bereits ein Notfallbund.

In solchen Verbänden schlössen sich lokale oder regionale Museen, Bibliotheken und Archive zusammen, um vorhandene Fachkompetenzen und Ressourcen ihrer Mitglieder zu bündeln und sich im Ernstfall gegenseitig zu unterstützen.

Notfallmelder

Schneider Intercom GmbH stellt in der Ausgabe 4-2018 der Zeitschrift PROTECTOR, S. 15, den **Notfallmelder „SaveME"** vor. Durch die Verbindung dieser App mit einem Intercom-Server könne eine ständige Verfügbarkeit sichergestellt werden. Der Clou: Die Alarmierung per „SaveME" finde nicht zwingend über das Display des Smartphones statt. Mittels tragbarer Bluetooth-Taster könne ein Notruf völlig unbemerkt aus der Hosen- oder Jackentasche getätigt werden. Die App liefere der Leitstelle nicht nur die exakte Inhouse-Position und außerhalb von Gebäuden die GPS-Position des Hilfsbedürftigen, sondern ermögliche auch eine direkte Sprachverbindung. „SaveME" unterstütze auch das Krisenmanagement mit weiterführenden Informationen, beispielsweise mit der Bereitstellung von Gebäude- oder Geländeplänen.

Mit der Optimierung der Krisenkommunikation befasst sich Guido Frohn, TAS Sicherheits- und Kommunikationstechnik, in PROTECTOR, Ausgabe 4-2018, S. 45. Eine wichtige Komponente sei ein Alarmierungsserver, wie ihn die Firma TAS mit dem **„ARUTEL"** anbiete. Die genaue Position des Notrufenden im Gebäude werde parallel zur Mobilfunkverbindung über ortsfeste Einrichtungen im Rahmen der VDE0827-Installation oder über Dienstpläne ermittelt.

Piraterie

Nach der Piraterie-Statistik des Schifffahrtsbüros der Internationalen Handelskammer (ICC) fanden **im 1. Quartal 2018 66 Piratenangriffe** auf Schiffe statt. Elf Schiffe seien beschossen, 39 geentert und vier entführt worden. 100 Seeleute seien als Geiseln genommen worden (FAZ vom 3. Mai). Ein paar Entführungen seien verhindert worden, weil die herannahenden Piratenboote von den Schiffsbesatzungen rechtzeitig entdeckt wurden. In einigen Fällen hätten sich die Besatzungen rechtzeitig in ihre „Zitadellen" zurückziehen können. Besonders schlimm hätten es die Piraten am Golf von Guinea an der Westküste Afrikas getrieben. Mehr als 40 Prozent der Angriffe hätten sich dort ereignet, wo die großen Tanker mit nigerianischem Öl ihre Fahrt aufnehmen. Das Ziel der Angreifer seien meist komplette Tankschiffe mit ihrer Ladung. Am schlimmsten sei es zur Zeit vor der Küste Nigerias. Allein 22 Zwischenfälle seien hier registriert worden. Nur neun kleinere Überfälle seien im 1. Quartal aus indonesischen Gewässern gemeldet worden. Elfmal seien Schiffe in Amerika geentert worden, davon vier in Venezuela und vier vor Haiti.

Polizeiliche Kriminalstatistik 2017

Am 8. Mai haben Bundesinnenminister Horst Seehofer und der Vorsitzende der IMK, Innenminister Holger Stahlknecht, die PKS 2017 vorgestellt. Ohne Berücksichtigung ausländerrechtlicher Verstöße wurden **5.582.130 Straftatenverdachtsfälle** polizeilich registriert. Das waren **5,1** Prozent **weniger als 2016**. Die Häufigkeitszahl (Straftaten pro 100.000 Einwohner – HZ) sank um 5,5 Prozent auf 6.764. Das ist die niedrigste HZ im 30-jährigen Vergleich. Die Aufklärungsquote erreichte (ohne ausländerrechtliche Verstöße) mit 55,7 Prozent den höchsten Stand seit 2005 (2016: 54 Prozent). Wie in den Vorjahren dominierte auch 2017 die Diebstahlskriminalität, und zwar mit einem Anteil an der Gesamtkriminalität ohne ausländerrechtliche Verstöße von 37,5 Prozent. Gegenüber 2016 sank sie um 11,8 Prozent auf 2.093.000 Fälle. **Signifikant zugenommen** haben gegenüber 2016 die Wirtschaftskriminalität (um 28,7 Prozent auf 74.070 Delikte, im Wesentlichen verursacht durch ein komplexes Ermittlungsverfahren mit zahlreichen Einzeldelikten), Straftaten gegen das Waffengesetz (um 10,3 Prozent auf 38.000), der Leistungskreditbetrug (um 24,9 Prozent auf 7.428), die Rauschgiftkriminalität (um 9,2 Prozent auf 330.580) und die Verbreitung pornografischer Schriften (um 12,9 Prozent auf 10.000 Fälle). **Besonders stark abgenommen** haben im Vergleich zu 2016 die ermittelten Fälle von Raubkriminalität (um 9,7 Prozent auf 38.849), von Straßenkriminalität (um 8,6 Prozent auf 1,2 Mio.), der Diebstahl von unbaren Zahlungsmitteln (um 14,6 Prozent auf 120.351), der Diebstahl aus Büros, Fabrik- und Lagerräumen (um 12,4 Prozent auf 107.824), der Wohnungseinbruchdiebstahl (um 23 Prozent auf 127.540), der Diebstahl an und aus Kfz (11,8 Prozent auf 277.000), der Taschendiebstahl (um 22,7 Prozent auf 127.376), der Betrug mittels rechtswidrig erlangter unbarer Zahlungsmittel (um 14,1 Prozent auf

63.900), die Wettbewerbs-, Korruptions- und Amtskriminalität (um 10,3 Prozent auf 3.850), die Fälle der Beleidigung auf sexueller Grundlage (um 29 Prozent auf 26.256) und Straftaten nach dem Arzneimittelgesetz (um 16,8 Prozent auf 2.721). Die Kriminalitätsbelastung war am höchsten in den Stadtstaaten Bremen (HZ 467,6), Berlin (HZ 453,4) und Hamburg (HZ 433,1), am niedrigsten in Bayern (HZ 159,1) und Baden-Württemberg (HZ 173,7). Unter den Großstädten ab 200.000 Einwohner waren Dortmund (HZ 484,5) und Frankfurt am Main (HZ 476,5) am stärksten, Rostock (HZ 240), München (HZ 250,4), Münster (HZ 265,9) und Dresden (HZ 262,1) am geringsten belastet. Eine ausführlichere Zusammenfassung – insbesondere zu den die Wirtschaft besonders belastenden Kriminalitätsphänomenen – findet sich auf der Website von Securitas Deutschland (Presse/Sicherheitslage).

Predictive Maintenance

Die Angst des Mittelstands vor dem Internet der Dinge thematisiert die FAZ am 16. April. In Fachkreisen sei „Predictive Maintenance" ein Zauberwort. Unter dieser „**vorausschauenden Wartung**" verstehe man die Tatsache, dass eine Produktionsanlage heute nicht mehr ausfallen müsse, bevor sie repariert wird. Ein intelligentes System kümmere sich vorher darum. Maschinen reparieren, bevor sie kaputtgehen und der Stillstand droht, heiße die Devise. Das Einsparpotenzial sei riesig. In den Großkonzernen sei das Thema schon präsent. Defizite gebe es dagegen in kleineren Unternehmen. In Deutschland reagierten noch viel zu wenige Unternehmenseigentümer und -manager auf diese fundamentalen Umbrüche in der Wirtschaft.

Produktpiraterie

Die FAZ berichtet am 25. April über die **Studie „Produktpiraterie 2018",** die der VDMA zusammen mit dem Fraunhofer Institut für Angewandte und Integrierte Sicherheit erstellt hat. Sie weise auf einen geschätzten Schaden durch Fälscher von 7,3 Mrd. Euro hin, was umgerechnet knapp 30.000 Arbeitsplätzen entspreche. Rückschläge und die fehlenden Fortschritte bei der Bekämpfung der Produktpiraten treibe die Branche um. Das Hauptproblem bleibe China. Das Land sei der mit Abstand größte Gefahrenherd. 82 Prozent der 140 befragten Unternehmen aus der Maschinenbaubranche habe China als häufigsten Herkunftsort von Plagiaten genannt. Auch als Absatzmarkt für derlei Produkte sei China am häufigsten genannt worden. Platz zwei unter den hartnäckigsten Ideendieben belege zwar nach wie vor Deutschland, aber der Abstand zu China sei gewaltig, und 19 Prozent Nennungen gegenüber 24 Prozent noch vor zwei Jahren sei ein gewisser Fortschritt. Auf Platz drei folge Italien mit 18 Prozent. Insgesamt hätten 71 Prozent der Unternehmen angegeben, von Produktpiraterie betroffen zu sein. Bisher seien vor allem technische Nachbauten das Problem gewesen, aber in diesem Jahr rückten zum ersten Mal Imitationen des äußeren Erscheinungsbildes oder ganzer Marken in den Fokus. 36 Prozent der Unternehmen hätten berichtet, dass solche Fälschungen eine Gefahr für Bediener, Anwender oder für die Umwelt darstellten. Bedenklich sei außerdem, dass der Vertrieb von Plagiaten über entsprechende Plattformen im Internet stark zugenommen habe. Frust werde auch deutlich, wenn mehr als 80 Prozent der Betroffenen beklagen, dass sie sich von Behörden oder lokalen Messegesellschaften im Ausland im Stich gelassen fühlten. Die Maßnahmen in den typischen Plagiatsländern würden nicht annähernd ausreichen, um die Unternehmen im Kampf gegen Plagiate zu schützen.

Rechenzentrumssicherheit

Franziska Leitermann, CLOUD & HEAT Technologies GmbH, stellt in der Ausgabe 4-2018 der Zeitschrift PROTECTOR, S. 72/73, **moderne Konzepte für Rechenzentren** vor. Die rasanten Entwicklungen in einer Welt mit immer mehr vernetzten Geräten bedeuteten immer mehr Gefahrenquellen für den Verlust wichtiger Daten. Viele Gründe sprächen dafür, Cloud-Dienste zu nutzen. Einer der Hintergründe für den zu erwartenden steigenden Cloud-Traffic bis 2021 sei die rasante Entwicklung in den Bereichen IoT, Künstliche Intelligenz und Industrie 4.0. Bei der Datenverarbeitung in der Cloud seien oft durch die Entfernungen Verzögerungen im Millisekundenbereich hinzunehmen. Eine Möglichkeit, Latenzzeiten zwischen Ereignis und Reaktion möglichst gering zu halten, sei, die Datenlagerung und -verarbeitung nicht in großen, zentralen Rechenzentren, z. B. in den USA, vorzunehmen, sondern in dezentralen und verteilten Rechenzentren, am besten in unmittelbarer lokaler Nähe zum Nutzer. So ließen sich auch Problemstellungen in Bezug auf die Ausfallsicherheit lösen. Die Ausfallsicherheit werde erhöht, wenn die Daten in kleinste Einheiten-Blöcke unterteilt würden. Der Transfer geschehe

dann besonders schnell und die Daten seien besonders schnell verfügbar, da der zweite, redundante Standort schnell einspringen könne, falls ein System ausfällt. Ein „Geolokalisator" erkenne, welches der verteilten Rechenzentren gerade das mit der schnellsten Verfügbarkeit ist und überträgt automatisch die Daten von diesem aus. Das Forschungsprojekt „fast realtime", eingebettet in das Förderprogramm „fast" des BMBF „Zwanzig20 – Partnerschaft für Innovation", habe sich dieser Perspektive gewidmet. Für verschiedenste Anwendungsgebiete wie Industrie oder Logistik sollten innovative Echtzeitsysteme entwickelt werden, die den jeweiligen Nutzern hohe Sicherheitsstandards und gleichzeitig schnellste Datenverarbeitung garantieren.

Schließsysteme

PROTECTOR enthält in der Ausgabe 4-2018, S. 42/43, eine **Marktübersicht** über 113 mechatronische Schließsysteme von 47 Anbietern. Die Online-Tabelle bietet je Firma 53 abgefragte Kriterien, unter anderem aus den Bereichen System, Schließmedium, Schließzylinder und Software.

Unter der Überschrift „Fluchtweg steht vor Einbruchschutz" stellt die Gretsch-Unitas GmbH in der Ausgabe 4-2018 der Zeitschrift PROTECTOR, S. 44, die Mehrfachverriegelung **„Audomatic3 TEOR"** vor. Die Haustür sei von außen verschlossen, könne aber von innen jederzeit ohne Schlüssel geöffnet werden. Soll die Tür tagsüber von außen ohne Schlüssel zu öffnen sein, könne der Schlüsseleigner die Automatik-Funktion der Sicherheitsschlösser kontrolliert in eine Komfortstellung setzen.

Sicherheitsforschung

Das BMBF hat eine Richtlinie zur Fördermaßnahme „Anwender – Innovativ: Forschung für die zivile Sicherheit II" im Bundesanzeiger vom 27. April 2018 veröffentlicht. Die Förderung der Sicherheitsforschung durch die Bundesregierung verfolge das Ziel, den Schutz der Gesellschaft vor Bedrohungen zu verbessern, die zum Beispiel durch Naturkatastrophen, Terrorismus, organisierte Kriminalität und Großschadenslagen ausgelöst würden. Dabei solle die **Forschungsförderung für Anwender** intensiviert werden. Zu ihnen gehörten Betreiber Kritischer Infrastrukturen, Sicherheitsdienstleister und vergleichbare Unternehmen der privaten Sicherheitswirtschaft. Gegenstand der Förderung seien direkt durch den Anwender initiierte und koordinierte Forschungs- und vorwettbewerbliche Entwicklungsvorhaben, die technologieübergreifend und anwendungsbezogen sind. Ergebnisse sollten den dringlichen, direkten, aktuellen Bedarfen der Anwender entsprechen und zielgerichtet deren Handlungsfähigkeiten verbessern. Um dies zu erreichen, sei im Rahmen dieser Förderrichtlinien ein weites Spektrum von Aktivitäten förderfähig – von der anwendungsbezogenen Erforschung neuer Technologien und Konzepte bis hin zur Weiterentwicklung und Qualifizierung vorhandener Lösungen für spezifische Anwendungsbereiche.

Sicherheitswirtschaft

Christian Ringler, Milestone Systems GmbH, untersucht in der Ausgabe 4-2018 der Zeitschrift PROTECTOR, S. 6–8, Chancen und Möglichkeiten der **Plattformökonomie** für die Sicherheitswirtschaft. Plattformen seien ein Geschäftsmodell, das exponentiell skaliert, wächst und weiteren Firmen zum Erfolg verhilft. Erfolgreich seien künftig nicht mehr Unternehmen, sondern Cluster diverser Unternehmen, die gemeinsam eine Plattform bilden. Dies setze voraus, dass die Lösung von Partnern in einem Netzwerk einzigartig ist, jeder in dem Cluster seinen eigenen Beitrag zur Wertschöpfungskette beiträgt und das Cluster ständig ausgebaut wird. Die meisten Integrationsplattformen böten vorkonfigurierte Schnittstellen. Der Plattform-Owner stelle die technische Plattform zur Verfügung. Diese verfüge über eine hohe Performance, Skalierbarkeit, Zuverlässigkeit und eine offene Schnittstelle. Um die Plattform-Owner herum entwickele sich ein Cluster mit Technologiepartnern, die entscheidenden Einfluss darauf haben, dass das Geschäftsmodell überhaupt funktioniert. „Solution Partner" seien diejenigen, die Lösungsansätze und Integrationen liefern. „Developer Partner" seien dafür zuständig, Integrationsprojekte schneller und flexibler zu unterstützen. Systemintegratoren und „Service Provider" seien diejenigen, die die geforderten Lösungen zusammenstellen, installieren und im Betrieb unterstützen. Die wichtigste Komponente im Plattformmodell sei aber der Anwender. Er müsse die Mehrwerte dieser Plattform und seiner speziellen Lösung möglichst schnell und einfach verstehen. Es müsse ein positiver Mehrwert erkennbar sein.

Chancen und Risiken von Plattformökonomien in der Sicherheitstechnik behandelt auch Dr. Peter Fey, Dr. Wieselhuber & Partner GmbH, in der Ausgabe 4-2018 von PROTECTOR, S. 10/11. Für klassische Anbieter der Sicherheitstechnik bestehe die Gefahr, dass sich völlig neue Wertschöpfungsstrukturen und Marktmodelle etablieren – mit dramatischen Folgen: Verlust des Kundenzugangs, der bisherigen marktsichernden Stellung und der generierten Daten an den Intermediär; Reduktion auf die Rolle des reinen Zulieferers oder des reisenden Handwerksbetriebs; Hinzunahme weiterer Partner durch den Intermediär. Zur richtigen Gefahr aus der Perspektive der Anbieter würden Plattformökonomien jedoch erst dann, wenn sie über eine ausreichend große Nutzer-Community verfügen. Eine entscheidende Frage sei, wie die etablierten Unternehmen der Sicherheitstechnik ihr vorhandenes Domänenwissen mit Hilfe digitaler, datengetriebener Services für den Kunden nutzbar machen können. Gelinge dies bei gleichzeitiger Absicherung des Wissensvorsprungs gegenüber Dritten, könnten auch zukünftig Differenzierungspotenziale realisiert werden.

Sicherheit.info berichtet am 19. April über Ergebnisse einer Online-Befragung von Unternehmen, die Revier- und Alarminterventionen in Auftrag geben. 60 Unternehmen hätten sich an der Befragung beteiligt. Sie erwarteten weitreichende Veränderungen bei der Mobilität. **Elektromobilität** sei für die Befragten die Lösung der Wahl. E-Fahrzeuge erfüllen ihrer Meinung nach sowohl die technischen als auch die ökologischen Anforderungen an künftige Konzepte. Auch würden die befragten Unternehmen mit Elektrofahrzeugen eine ökonomische Aufwertung ihrer Fuhrparks verbinden. Demgegenüber stünden noch vorhandene Defizite in der Infrastruktur für Ladevorrichtungen und in den Reichweiten zu erschwinglichen Preisen.

Social Media

Marcus Nebel, SIMEDIA Akademie GmbH, befasst sich in der Ausgabe 4-2018 der Zeitschrift PROTECTOR, S. 66/67, mit **Social Media in der Unternehmenssicherheit**. Unterschieden werde das Horizontmonitoring, das dazu diene, definierte Risikothemen beziehungsweise Ereignisarten zu betrachten, und das Incident Monitoring, das im Krisenfall ein konkretes Ereignis durch kontinuierliche Datenanalyse begleitet. Möglichkeiten der Personenanalyse böten Potenziale, um Personenschutzmaßnahmen zu ergänzen und zu optimieren oder im Sinne eines Penetrationstests die Gefährdung für Social-Engineering-Angriffe auf sicherheitskritische Mitarbeiter abzuschätzen. In jedem Fall sei eine tiefgehende Beschäftigung mit den rechtlichen Fragestellungen notwendig.

Spionage

Dr. Michael Spehr, Redaktion der FAZ, zeigt in der Ausgabe vom 8. Mai, wie Geheimdienste und Codeknacker arbeiten, um trotzdem an Daten zu gelangen, die kryptologisch nicht angreifbar sind. Mit **„Seitenkanalattacke"** bezeichne man die Methode, ein kryptografisches Gerät während der Ausführung seiner Algorithmen zu beobachten und nicht etwa zu hacken. So basiere der Seitenkanalangriff darin, eine Korrelation zwischen den beobachteten Daten und dem verwendeten Schlüssel zu finden. Passive Seitenkanalangriffe analysierten die Laufzeit des Algorithmus, den Energieverbrauch des Prozessors oder seine elektromagnetische Abstrahlung. Wenn zum Beispiel Sicherheitschips für Zugangssysteme mit kryptografischen Verfahren nicht knackbar sind, könne man die Chips als solche in den Blick nehmen. Dazu werde dann beispielsweise ein Mikroskop mit der Abkürzung Triphemos verwendet, das mit höchster Präzision die äußerst schwache Infrarotstrahlung erkenne, die entsteht, wenn Transistoren schalten. Das bislang größtmögliche Einfallstor für einen Seitenkanalangriff habe sich in den Angriffsszenarien Meltdown und Spectre gezeigt, die auf das Herz aller Rechner, die Prozessoren, gezielt hätten. Auch die Messung der elektromagnetischen Abstrahlung eines Rechners und die Analyse seines Energieverbrauchs würden gern für Seitenkanalangriffe genutzt. Jenseits geballter Geheimdiensttechnik könne ein Seitenkanalangriff schon mit einfachsten Mitteln erfolgreich sein: Der Spion schaut zu, wenn die geheimen Dokumente benutzt werden. Dazu reiche schon ein leistungsfähiges Teleskop, mit dessen Hilfe die Pupille des Verdächtigen in den Blick genommen wird, die das Bild des Computermonitors reflektiert.

Steuerhinterziehung

Wie hasepost.de am 5. Mai meldet, stoßen hessische Steuerfahnder auf eine **Betrugsmasche bei einzelnen Sicherheitsdienstleistern**, die an die berüchtigten

Umsatzsteuerkarusselle erinnere. Aufträge würden danach von Sicherheitsfirmen häufig an eine unüberschaubare Kette von hintereinander geschalteten Subunternehmen weitergeleitet, schreibe der „Spiegel". Am Ende der Kette stelle ein Unternehmer eine fingierte Rechnung mit dem Steuerbetrag für die erbrachte Dienstleistung aus, führe die Steuer jedoch nicht an den Fiskus ab. Für das Finanzamt seien die letzten Glieder der verschachtelten Kette oft nicht mehr greifbar. Der hessische Finanzminister fordere Maßnahmen gegen das Betrugsmodell. Denkbar seien Verfahren, die bei Umsatzsteuerkartellen oder auch in der Baubranche Erfolg zeigten. Durch eine Rechtsänderung könne grundsätzlich der Leistungsempfänger oder der erste Auftragnehmer für die Steuerschuld verantwortlich gemacht werden.

Transparenzregister

Rechtsanwalt Roman G. Weber weist in der Ausgabe 4-2018 von PROTECTOR, S. 68/69, darauf hin, dass es seit Jahresbeginn 2018 das Transparenzregister zur **Bekämpfung von Geldwäsche und Terrorfinanzierung** gibt. Viele Unternehmen seien nicht informiert, ob die damit zusammenhängenden Pflichten für sie relevant sind. Der Autor gibt Antworten auf folgende Fragen: Wie ist das Register aufgebaut? Wer ist verpflichtet? Wer ist ein „wirtschaftlich Berechtigter"? (Für die wohl in Deutschland häufigste Konstellation der juristischen Person gelte: Wirtschaftlich Berechtigter ist jede natürliche Person, die unmittelbar oder mittelbar mehr als 25 Prozent der Kapitalanteile hält, mehr als 25 Prozent der Stimmrechte kontrolliert oder auf vergleichbare Weise Kontrolle ausübt.) Was ist zu melden? Wer darf Einsicht nehmen?

Videoüberwachung

Mit dem Software-Release 9.0 stelle IPS Intelligent Video Analytics ihren Kunden und Partnern zahlreiche **neue und optimierte Features** zur Verfügung, berichtet sicherheit.info am 9. April. Aufgrund wachsender Bedrohungen und einer mehr und mehr vernetzten Infrastruktur lege IPS ein noch größeres Augenmerk auf Themen wie Verschlüsselungen und die Verwendung von Zertifikaten. Video-Streams werden über das sichere Übertragungsprotokoll HTTPS zwischen Kamera und Device Server übertragen. Für zusätzliche Sicherheit sorge IPS durch die Unterstützung des Protokolls TLS1.2. Neben der vollumfänglichen SOAP Schnittstelle stelle IPS mit der Software-Version 9.0 drei neue TCP-Schnittstellen zur Verfügung, die die Anbindung an Fremdsysteme erheblich vereinfachen und die der Anwender je nach Umfang und Komplexität seines Systems wählen könne. Somit sei der IPS „Videomanager" mit einem Höchstmaß an Flexibilität ausgestattet. Mit der Version 9.0 würden auch einige der server- und kamerabasierten Videoanalysen einen Ausbau der Funktionen sowie eine Verbesserung der Anzeige erfahren. Das Modul Public Transport sei um eine weitere Überwachungszone ergänzt: Neben Gleisbettüberwachung detektiere das Modul auch, ob sich Personen auf dem Sicherheitsstreifen an Bahngleisen aufhalten. Das Modul Outdoor Detection verfüge nun auch über eine optionale richtungsunabhängige Detektionsmöglichkeit.

GIT-SICHERHEIT.de stellt am 27. April den **IP-Decodermonitor FDF2304W-IP** von EIZO vor, der zum Betrieb keinen Computer, keine Software und keine andere Hardware benötige. Mit der „Low Light Correction" ließen sich dunkle Bereiche besser darstellen. Sie ermittle automatisch dunkle und schwer zu erkennende Bildbereiche und passe die Helligkeit aller Pixel an. Auf diese Weise würden solche Bildbereiche aufgehellt und zudem mit einer realistischen Tiefenwirkung wiedergegeben. Die Funktionseinstellung Outline Enhancer analysiere angezeigte Inhalte und sorge dafür, dass das Rauschen nicht verstärkt wird. Gleichzeitig würden unscharfe Bereiche korrigiert und das Bild werde weiter geschärft. Zur Helligkeitsregelung und Vorbeugung von Flimmereffekten sei der Monitor mit einer LED-Hintergrundbeleuchtung ausgestattet. Bilder würden pixelgenau in bildschirmfüllender Full HD-Auflösung dargestellt.

In der Ausgabe 5-2018 – Videoüberwachung Special – der Zeitschrift PROTECTOR werden die Ergebnisse des **14. PROTECTOR & WiK Forum Videosicherheit** vorgestellt (S. 6–35). Die Wertschöpfungskette in der Videobranche stehe anhaltend unter Druck. Das werfe die Frage auf, wie lange sich mit den Produkten noch ausreichend Gewinn erzielen lässt. An welchen Stellschrauben Hersteller, Errichter und Distributoren drehen müssten, um zukunftsfähig zu bleiben, sei Thema beim Forum Videosicherheit 2018 gewesen. Es zeige sich, dass die Preisdiskussion von den Produkten auf die Dienstleistung ausstrahle und der Sparzwang auch in der Planung angekommen sei. Dennoch lasse sich mit einer fachkundigen Planung oft mehr einsparen als mit einem Rabatt auf einzelne Kameras. Eine sinnvolle Integration könne sich auszahlen, wenn sie Prozesse optimiert, die allgemeine Sicherheit erhöhe oder

einfach Strukturen verschlanke. Integratoren und Errichter müssten die Produkte der Hersteller und vor allem deren Grenzen kennen, weil sonst aus Integration schnell Frustration werden könne. Die Videotechnik erfahre seit Jahren eine stetige Erweiterung ihrer Anwendungsfelder: Beispiele bildeten Drohnen, präventive Bodycams und Brandfrüherkennung. Eine Triebfeder für neue Anwendungen bilde die Cloud-Architektur.

Mit der **Haftung für Datenschutzverstöße** bei der Videoüberwachung befasst sich in der Ausgabe 5-2018 – Videoüberwachung Special – der Zeitschrift PROTECTOR, S. 36–38, Walter C. Dieterich, Deutsche Datenschutzhilfe e. V. Legen zwei oder mehrere Verantwortliche Art und Umfang der Videoüberwachung gleichberechtigt und gemeinsam fest, könne der Betroffene seine Rechte gegenüber jedem für die Verarbeitung Verantwortlichen geltend machen. Sowohl der Errichter wie auch der Endkunde hafteten im Außenverhältnis auf den gesamten Schaden. Beiden stehe aber die Möglichkeit der „Schuldbefreiung" zur Verfügung. Darum müssten sie nachweisen, dass sie nicht für den Umstand verantwortlich sind, durch den ein Schaden aufgetreten ist.

Rudolf Rohr, barox Kommunikation AG, beschreibt in PROTECTOR, Ausgabe 5-2018 – Videoüberwachung Special, S. 39, **Sicherheitsvorkehrungen für Videonetzwerke**. Für einen wirkungsvollen Schutz gegen Phishing und „Man-in-the-middle-Angriffe" sei gerade bei professionellen Anwendungen über die Transportverschlüsselung hinaus zusätzliche Sicherheit erforderlich. Mit der personalisierten Verschlüsselung komme eine zusätzliche Sicherungsmaßnahme für Videoswitche zum Einsatz, die doppelte Sicherheit bietet. Ein Fernzugriff über das Internet sei ausgeschlossen. Erst durch die Kombination von Passwort – geschützt durch HTTPS – und dem personalisierten Authentifizierungsschlüssel erhielten Mitarbeiter Zugang zum Videonetzwerk.

Wenn IP-Kameras über das Netzwerk erreichbar sind, bedeute dies auch, dass die Videoüberwachung jetzt denselben Bedrohungen durch Hacker und Malware ausgesetzt sei wie andere IT-Systeme. Wie sich der **Risikofaktor senken** lässt, zeigt Genetec Deutschland GmbH in PROTECTOR, Ausgabe 5-2018 – Videoüberwachung Special, S. 40/41. Bei der Auswahl einer Verpixelungstechnologie müssten Unternehmen sehr sorgfältig vorgehen, weil nicht alle Algorithmen eine vollständige Verpixelung leisten könnten, auch wenn Personen kurz stehen bleiben oder sich die Beleuchtungssituation ändert. Bewährt habe sich die direkte Integration der Verpixelung in die übergeordnete Management-Plattform, wie es zum Beispiel der „Privacy PROTECTOR" im Genetec Security Center ermögliche. Die Verpixelung werde dann durch dieselben Autorisierungsverfahren geschützt wie die Management-Plattform. Unerlässlich sei die Verschlüsselung der Kommunikationskanäle über das TLS-Protokoll. Bei der Geräteauswahl sei darauf zu achten, dass nicht benötigte Dienste/Ports deaktiviert werden können.

Cloudbasierte Videoüberwachungssysteme für Hochsicherheitsanwendungen ist das Thema von Hendrik Schulte im Walde, Schille Informationssysteme GmbH, und Florian Benne, Microsoft Deutschland GmbH, in der Ausgabe 5-2018 von PROTECTOR – Videoüberwachung Special, S. 42–44. Der Einsatz von Cloud-Technologie biete Skalierbarkeit von Ressourcen und Workloads, Kostenersparnis bei der Hardware, geringen Installations- und Wartungsaufwand, nutzungsabhängige Abrechnungsmodelle, integrierte Backup-, Failover- und Wiederherstellungsoptionen oder automatisiertes Ressourcenmanagement. Jeder externe Zugriff werde durch einen einmaligen zufällig generierten Schlüssel abgesichert, der durch Dritte nicht nachvollzogen werden könne. Für die Sicherheitstechnik sei der Weg in die Cloud ein logischer Schritt.

Mit **neuronalen Prozessoren in der Videoanalyse** befasst sich der Journalist Bernd Schöne im Heft 5-2018 der Zeitschrift PROTECTOR – Videoüberwachung Special, S. 48–51. Bei jedem Vorgang verändere sich das neuronale Netz. Es entstünden neue Verknüpfungen oder bestehende würden verstärkt. IBM habe mit „True North" bereits die zweite Generation dieser neuronalen Prozessoren vorgestellt. True North verfüge über 5,4 Mrd. Transistoren und 4.096 Rechenkerne. Jeder Kern stelle 256 Silizium-Neuronen zur Verfügung. Ein einziger Chip könne die Bilder von 100 Überwachungskameras simultan und in Echtzeit auswerten. Der Energiebedarf bleibe mit einigen Hundert Milliwatt bescheiden. Das sei der Vorteil gegenüber Grafikkarten, seit 2006 Technologieführer der künstlichen Intelligenz. Ihre hoch spezialisierten Prozessoren seien vorzüglich geeignet, neuronale Netze zu simulieren.

Hochkomplexe Videosicherheitssysteme sind das Thema für Petra Keller, Geutebrück GmbH, im Videoüberwachung Special, Ausgabe 5-2018 der Zeitschrift PROTECTOR, S. 54/55. Professionelle Videosicherheitssysteme zeichneten sich dadurch aus, dass sie weder dem User trauen noch der Technik, die sie umgibt. Ihre Stärke sei es, dass sie einem potenziellen Ausfall stets einen Schritt voraus sind: durch „Spiegelung" der Hardwarebauteile und des Betriebssystems, durch redundante Anordnung unabhängiger Festplatten (RAID-System). Failover-Konzepte sicherten dank intelligenter

Steuerung durch die Software die Verfügbarkeit. Das Konzept der Ausfallsicherheit schließe nicht nur die Recorderseite mit ein, sondern auch die Seite der Kameras. Edge Recording bedeute: Die Bilddaten werden zusätzlich in der Kamera auf einer SD-Karte gespeichert. Sollte das Netzwerk ausfallen, seien die Bilddaten gesichert.

Das Videoüberwachung Special von PROTECTOR, Ausgabe 5-2018, enthält **Marktübersichten**:

- über 160 hochauflösende Netzwerkkameras von 54 Anbietern mit 63 abgefragten Kriterien, unter anderen Videospezifikationen, Bildübertragung, Audiospezifikationen, Schnittstellen, Aufbau und Betrieb sowie Sicherheit (S. 56/57)
- über 119 Videomanagementsysteme von 66 Anbietern mit 53 abgefragten Kriterien (S. 58/59)
- über 56 Systeme der Kennzeichenerkennung von 28 Anbietern mit 28 abgefragten Kriterien (S. 60/61).

Whistleblower

Die EU-Kommission will **Informanten besser schützen**, berichtet die FAZ am 24. April. Die Mitgliedstaaten sollten sicherstellen, dass solche Informanten nicht mehr bestraft werden, wenn sie auf Missstände in Unternehmen aufmerksam machen. Dazu gehöre, dass der Arbeitgeber etwa in anschließenden Arbeitsrechtsstreitigkeiten nachweisen müsse, dass er den Hinweisgeber nicht wegen seines Handelns entlassen hat. Privatunternehmen mit mehr als 50 Mitarbeitern oder einem Jahresumsatz von mindestens 10 Mio. Euro sollten sichere Kanäle schaffen, um die Meldung von Missständen zu erleichtern. Sie müssten zudem innerhalb von drei Monaten auf die Beschwerde reagieren. Auf diesen internen Beschwerdeweg solle nach dem Vorschlag eine Beschwerde bei einer zuständigen öffentlichen Behörde folgen können. Auch die Medien sollten Hinweisgeber ohne negative Konsequenzen direkt informieren können, wenn die internen Kanäle für die Meldung von Missständen nicht funktionierten oder wenn ansonsten ein nicht wieder gut zu machender Schaden drohe.

Wirtschaftsschutz

Jan Wolter, ASW-Geschäftsführer, weist in der Ausgabe 4-2018 der Zeitschrift PROTECTOR, S. 58, darauf hin, dass der Begriff Wirtschaftsschutz im **Koalitionsvertrag 2018** kein einziges Mal auftaucht. Von einer engeren Zusammenarbeit zwischen Staat und Wirtschaft bei der Abwehr von Gefahren werde, außer mit Bezug auf Cyber, nicht gesprochen. Es stehe zu befürchten, dass die Bundesregierung sich „Cyberscheuklappen" aufsetze und links und rechts von IT-Sicherheit nichts mehr sieht.

Zutrittskontrolle

Dr. Jörg Wissdorf, Interflex Datensysteme GmbH, behandelt in der Ausgabe 4-2018 der Zeitschrift PROTECTOR, S. 32/33, die **technische Entwicklung der Zutrittskontrolle**. Unter dem Stichwort „Zutritt 5.0" bringe Interflex neue Lösungen für die Zutrittskontrolle auf den Markt. Eine Option für alle, die häufig in verschiedene Niederlassungen ihres Unternehmens Zutritt benötigen, sei das Smartphone als Türöffner. Durch die Integration der Funktionen auf einem einzigen Medium bräuchten Mitarbeiter nicht mehr eine Vielzahl von unterschiedlichen ID-Karten, PIN-Codes, Passwörtern und Schlüsseln zu verwalten. Das Smartphone fungiere als Zutrittsausweis. Zutrittssysteme 5.0 erlaubten bei Alarm automatisch die Einleitung von Sicherheitsmaßnahmen und sendeten eine Nachricht an den zuständigen Administrator. Bei Systemen mit Alarmfunktionen werde ereignisabhängig ein Alarm ausgelöst – bei unzulässigem Zutrittsversuch, überschrittener Türöffnungszeit oder Sabotage. Die jeweiligen Reaktionen ließen sich über entsprechende Konfigurationstools individuell definieren.

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