Focus on Security

Ausgabe 12, Dezember 2016

SECURITAS

Inhalt

Autonome Autos

Automatische Schließmechanismen, Reifendruckmesser und vergleichbare Systeme nutzen Funkfrequenzen. Das Infotainment-System sei über WLAN mit dem Internet verbunden. All diese Dinge seien potenzielle Einfallstore. Für autonome Autos brauche man nun zusätzlich Sensoren: Radar, Lidar (Light detection and ranging) und Kameras, die miteinander kommunizieren müssen. Diese Technologien würden zu Schwachstellen, wenn sie nicht richtig geschützt sind (ASW-Newsletter vom 4. November).

Betrug

Nach einem Bericht in der FAZ am 11. November sollen **Krankenkassen** Ärzten Geld dafür geben, „ihre Patienten auf dem Papier kränker zu machen, als sie sind". Sie zahlten dafür eine Milliarde Euro. Manipulationen am Risikostrukturausgleich zwischen den Kassen beschäftigten den Gesundheitsausschuss. Der habe einen Ministeriumsbericht beraten, in dem drei Betrugsformen beschrieben werden. Demnach rufen Kassen Patienten an, etwa um sie nach einem leichten Herzinfarkt über ein abermaliges Risiko „aufzuklären" und zu einem neuen Arztbesuch zu veranlassen, womit die Diagnose ein weiteres Mal notiert und im Finanzausgleich relevant werde. Auch schickten Kassen „Kodierberater" mit Patientenlisten zu Ärzten, um für den Finanzausgleich bedeutsame Krankheiten festzustellen und zuweilen nachträglich zu korrigieren.

Brandschutz

Brandschutz per Brennstoffzelle und deren sauerstoffarmer Abluft behandelt GIT in der Ausgabe 11-2016, S. 68/69. In Rechenzentren, IT- oder Telekommunikationsanlagen bestehe durch die Vielzahl dort installierter elektrischer Anlagen ein besonders hohes Brandrisiko. Der Grund für Brände seien meist technische Defekte oder Kurzschlüsse an elektrischen Geräten, die als Schwelbrand häufig erst entdeckt würden, wenn es bereits zu spät ist. Mit dem System „Quattro Generation" verspreche Fuji N2telligence den „ersten Brandschutz mit Return on Invest". Kern des Systems sei eine Brennstoffzelle. Brennstoffzellen erzeugten gleichzeitig Strom und Wärme nach dem Prinzip der Kraft-Wärme-Kopplung, dies aber im Vergleich nahezu lautlos und durch die direkte Umsetzung der chemischen Energie in nutzbare, elektrische Energie weitaus effizienter. Schadstoffemissionen gebe es keine. Brennstoffzellen erreichten bei der Umwandlung von Erdgas zu Strom und Wärme bereits mehr als 90 Prozent Effizienz und sparten somit jährlich hunderte Tonnen an CO_2. Während der Energiebereitstellung entstehe in der Brennstoffzelle prozessbedingt eine Abluft, welche sauber ist und einen geringeren Sauerstoffgehalt als unsere 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. Brandschutz stelle keinen Kostenblock mehr dar, sondern das System erwirtschafte sogar seinen eigenen Return on invest.

Für die **Sicherstellung des einwandfreien Betriebs von Brandschutzanlagen** gebe es klare Vorgaben, wird in der Ausgabe 11-2016 der Zeitschrift GIT, S. 76/77, betont. Der Beitrag geht auf normgerechte Instandhaltung, rechtliche Grundlagen und fünf Gründe für die Instandhaltung durch die jeweilige Errichterfirma ein: Sie sei für den jeweiligen Anlagetyp gemäß DIN 14675 zertifiziert und vom VdS anerkannt, verfüge über geschultes Personal, halte Ersatzteile vor und könne sie zeitnah beschaffen, gewährleiste Notdienstbereitschaft und unterstütze Betreiber bei Fragen rund um das Thema Brandschutz.

Datenschutz für Unternehmen

Ein Artikel in der FAZ am 18. November befasst sich mit der möglichen **Lockerung des Datenschutzes.** Bislang setze er enge Grenzen. Auswerten dürften die Unternehmen nur, was sie für den eigens festgelegten Geschäftszweck benötigen. In einem Papier aus dem für die digitale Infrastruktur zuständigen Bundesverkehrsministerium heiße es, man müsse weg vom Grundsatz der Datensparsamkeit, hin zu einem kreativen und sicheren Datenreichtum. Das Prinzip der Datensparsamkeit entstamme der deutschen Rechtsprechung, finde sich aber auch in der EU-Datenschutzgrundverordnung. Das Ministerium spreche sich für einen klaren Rechtsrahmen aus, der die Verfügungsrechte über die Daten regelt, und betone zugleich, diese Daten gehörten den Menschen. Eine Verwendung der Informationen dürfe ausschließlich anonymisiert und pseudonymisiert erfolgen. Das Ministerium wolle gemeinsam mit der Wirtschaft bis 2023 rund 100 Mrd. Euro in den Ausbau der Netze investieren und damit neben dem Glasfaserausbau auch die Entwicklung des neuen Mobilfunkstandards 5G vorantreiben. „Open Data", etwa frei zugängliche Verkehrs-, Wetter- oder Geodaten könnten innovative Geschäftsideen fördern, etwa Apps, die bei der Suche nach einem Parkplatz helfen. Nach einem Gesetzentwurf des BMI sollten alle Regierungsdaten künftig zeitnah zur Verfügung stehen. Ausnahmen seien zu begründen. Die Regierungsdaten sollten im schon vorhandenen Portal GovData kostenlos freigegeben werden.

Die große Koalition wolle das Bundeskartellamt zu einer Art Verbraucherschutzbehörde für das Internet ausbauen, heißt es in der FAZ am 21. November. Wenn Verstöße zu einem Massenphänomen werden, das eine Vielzahl von Verbrauchern schädigt, solle die Bonner Wettbewerbsbehörde mit erweiterten Befugnissen gegen Internetunternehmen vorgehen und unlautere Geschäftsmethoden beenden. Unternehmen, die sich nicht an die Anordnungen des Kartellamtes halten, müssten mit Geldbußen rechnen. Außerdem sollten die Wettbewerbshüter zur „Abschöpfung" finanzieller Vorteile ermächtigt werden, die ein Unternehmen durch unlauteren Wettbewerb erzielt hat. Zusätzlich sehe die geplante Regelung vor, dass das Kartellamt für den Verbraucherschutz spezielle „Sektoruntersuchungen" durchführen kann, um „neuartige Gefährdungslagen" aufzuklären. So stehe es in ersten Entwürfen, mit denen die Union und die SPD dieses Vorhaben in die Reform des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) aufnehmen wollten. Sehen einzelne Verbraucher ihre Rechte verletzt, bleibe der Gang vors Gericht aber der übliche Weg. Einen individuellen Anspruch auf ein Eingreifen des Kartellamtes werde es nicht geben.

Drohnen

Normen Wollmann, Ela-Soft GmbH, beschreibt in der Ausgabe 11-2016 der Zeitschrift PROTECTOR, S. 40/41, die **Kombination autonom fliegender Drohnen mit Sicherheitssystemen**. Die Kombination mit einem Ereignis aus einem Sicherheitssystem sei neu. Ela-Soft mit dem Funktionsmodul GEMOS Drone sei ein herstellerneutrales Gefahrenmanagementsystem, das eine besonders offene und neutrale Plattform darstelle. Der Autor behandelt drei Szenarien: den Einbruchsfall, den Brandfall und geplante Kontrollflüge.

Die **Deutsche Telekom** wolle einer Meldung der FAZ vom 7. November demnächst ein Drohnen-Abwehrsystem anbieten. Die Technologie solle noch in diesem Jahr an den Start gehen. Die Telekom setze auf Partner, die entsprechende Technologien entwickeln. Die Deutsche Flugsicherung gehe davon aus, dass es in Deutschland mehr als 400.000 Drohnen gebe. Die Bandbreite

reiche von Spielzeug-Quadcoptern bis hin zu Fluggeräten, die in der Lage seien, mehrere Kilogramm Last zu tragen. Neuere Modelle würden sogar automatisch Hindernisse umfliegen, die von Sensoren erfasst werden.

Nach Angaben der Deutschen Flugsicherung wurden, wie die FAZ am 16. November meldet, in den ersten zehn Monaten 61 Zwischenfälle mit ferngesteuerten Flugobjekten gezählt, im selben Zeitraum 2015 seien es bloß zwölf gewesen. Die meisten **Behinderungen durch Drohnen** registriere die DFS rund um den Frankfurter Flughafen mit 16 Vorfällen. Wegen des Anstiegs schlägt die DFS nun eine härtere Gangart gegen Hobby-Drohnenpiloten vor. Sie fordere einen allgemeinen „Drohnenführerschein". Ab einem Startgewicht von 250 Gramm sollten die Fernlenker ihre Sachkunde nachweisen müssen. Außerdem sollten alle Drohnen – auch von Hobbysteuerern – in ein zentrales Register eingetragen werden. Um Drohnen, die zur Gefahr für Flugzeuge werden, künftig aufzuspüren, beteilige sich die DFS an einem Forschungsprojekt, bei dem Handy-Chips in die Fluggeräte eingebaut werden sollen. Drohnen seien dann wie Mobiltelefone zu orten.

Endgerätesicherheit

Mit einem manipulierten Video, das derzeit über Messenger und soziale Netzwerke verbreitet werde, ließen sich iPhone und iPad zum Einfrieren bringen, heisst es am 20. November bei heise.de. iOS beginne kurze Zeit nach der Wiedergabe ins Stocken zu geraten und die Bedienoberfläche verweigere anschließend jegliche Eingabe. Auf manchen Geräten tauche das Drehrädchen-Icon auf, das sonst beim Herunterfahren kurz erscheine. Besonders problematisch scheine das Abspielen im integrierten Browser Safari. Hier helfe nur noch ein erzwungener Neustart. Das „Fünf-Sekunden-Video" stamme offenbar aus der chinesischen Video-Sharing-App Miaopai.

Entführung

Peter Bensmann habe **Lösegeldpolicen in Deutschland etabliert**, berichtet die FAZ am 17. November. Der Markt für solche Deckungen werde relevanter. Im vergangenen Jahr habe der spezialisierte Dienstleister Toribos 58.000 Entführungen gemeldet. Unbekannte Fälle gingen in die Hunderttausende. Die Länder mit dem höchsten Risiko lägen in Afrika, im Nahen Osten sowie in Zentralasien. Das Unternehmen von Bensmann trage den seltenen Titel „Assekuradeur". Es sei kein Makler oder Vermittler, aber auch kein Versicherer, sondern zeichne Spezialrisiken auf die Bilanz eines Versicherers. Zehn Mitarbeiter kümmern sich im Hansekuranz Kontor darum, Risiken zu zeichnen. Dazu greife Bensmann auf 142 Partner auf der ganzen Welt zurück, die durch „Standby"-Honorare vergütet würden und im akuten Fall als Krisenmanager eingriffen. In Kolumbien etwa komme es vor, dass die Hotel-Rezeption melde, ein Geschäftspartner habe eine Sightseeing-Tour gebucht. Das virtuelle Opfer lasse sich fünf Stunden durch die Stadt führen, während sein Unternehmen in der Zwischenzeit eine Entführung gemeldet bekomme. Unternehmen, die Mitarbeiter in Krisenregionen schicken, sollten im Vorfeld Krisenstäbe einrichten. Selbst Unwägbarkeiten müsse man vorab erörtern: Krankheiten der Mitarbeiter, die sie dem Arbeitgeber verschweigen wollten, gehörten genauso dazu wie die Konsequenzen eines Doppellebens. Wenn sich eine Entführung trotz aller Vorkehrungen nicht verhindern lässt, zahle der Versicherer unter anderem Lösegeld, Vermögensschäden und die Kosten für die Krisenberatung. Bensmann: „Nehmen Sie immer ein Zimmer zwischen dem zweiten und dem sechsten Stock." Denn genau bis zu dieser Höhe gingen üblicherweise die Feuerleitern in Hotels. Policen schützten auch Reeder gegen Piratenangriffe oder entstehende Kosten, wenn ein Schiff umgeleitet werden müsse, weil bewaffnete Guards überraschend nicht zur Verfügung stehen.

Pascal Michel, SmartRiskSolutions GmbH, befasst sich im ASW-Newsletter vom 18. November mit der **virtuellen Entführung**. Dies sei ein Betrugsdelikt, bei dem die Täter den Anschein erwecken, einen Familienangehörigen entführt zu haben. Vier Voraussetzungen benötige der Täter, um erfolgreich zu sein: Er müsse Informationen zum angeblichen Opfer und die Telefonnummer der Familienangehörigen beschaffen. Ferner müsse er verhindern, dass die Opferfamilie das vermeintliche Opfer oder die Polizei kontaktiert sowie glaubwürdig den Eindruck erwecken, dass er tatsächlich ein Entführungsopfer in seiner Gewalt hat. In den einfachen Fällen riefen die Täter listenweise Personen auf gut Glück an. Die Anrufe erfolgten teilweise aus mexikanischen Gefängnissen mittels Mobiltelefonen. Bei 20–30 Telefonaten am Tag genüge bereits ein erfolgreicher Anruf, bei dem der Angerufene das Geld an einen Komplizen übergibt. Die geforderten Summen lägen in der Regel bei mehreren tausend Dollar, also einer leicht zu beschaffenden Geldmenge. Die Täter setzten ein sehr kurzes Ultimatum von 1–2 Stunden. Ein Komplize hole am vereinbarten Übergabeort das Geld ab oder lasse es auf ein Auslandskonto transferieren. Eine andere Variante bestehe darin, einen Hotelgast zu kontaktieren. Der Täter gebe sich als Polizist aus und erkläre, man habe Informationen, dass ein Drogenkartell seine Entführung plane. Der Hotelgast werde aufgefordert, sich in ein anderes Hotel zu begeben und gebeten, sein Handy abzugeben, da das Kartell das Handy auch im ausgeschalteten Zustand überwachen und orten könne. Wie immer ist das Wissen um die Existenz solcher Delikte und die Tätertaktiken ein wichtiger Schritt zur Prävention. Man solle vermeiden, Informationen wie Telefonnummern in sozialen Netzwerken preiszugeben. Grundsätzlich sei zunächst von einer realen Entführung auszugehen. Es wird empfohlen, „das Tempo aus dem Fall herauszunehmen" und ein Gespräch mit dem Opfer oder einen anderen Lebensbeweis zu fordern.

Geldwäsche

Bundesfinanzminister Schäuble wolle die Möglichkeit eröffnen, sich via Internet in einem elektronischen Transparenzregister über die Hintermänner von Unternehmen, Trusts und Vereinigungen zu informieren, meldet die FAZ am 25. November. Ziel sei ein effektiverer Kampf gegen Geldwäsche und Terrorfinanzierung. Das geplante Register solle dem Ministerium zufolge als Portal fungieren, über das Dokumente aus anderen öffentlich zugänglichen Registern wie dem Handelsregister abgerufen werden können.

Internet der Dinge

Hacker-Attacken auf das Internet der Dinge verschrecken Nutzer, titelt die FAZ am 7. November. Das Problem sei, dass viele Geräte nicht nachgerüstet werden können. Das Startup-Unternehmen Smartfog verkaufe seine Überwachungskameras in einem Abonnement-Modell. Wer knapp sechs Euro im Monat zahlt, bekomme die Kamera und könne 24 Stunden Videomaterial speichern und damit etwa nachschauen, ob sich Einbrecher an den Rollläden zu schaffen machen. Wer mehr bezahlt, könne länger aufzeichnen, bis zu 30 Tage. Spätestens dann würden die Videodaten gelöscht, die ohnehin verschlüsselt übertragen werden. Die Anzahl der Geräte im Internet der Dinge steige rasant. Eine Studie von McKinsey prognostiziere allein für Deutschland ein Umsatzpotenzial von rund 23 Mrd. Euro für 2020. Den größten Teil mache mit fast neun Mrd. Euro die Industrie 4.0 aus. Für den gesamten Bereich der Smart Homes rechne McKinsey mit etwas weniger als einer Milliarde Euro. Die Marktforscher von Deloitte hätten ermittelt, das besonders im Bereich der vernetzten Häuser noch Zurückhaltung herrsche. Gründe seien hohe Preise und Vorbehalte wegen des Datenschutzes.

IT-Sicherheit

Die FAZ befasst sich am 3. November mit **Browser-Erweiterungen**. Im Internet würden laufend und überall Nutzerdaten gesammelt, aufbereitet und gehandelt. Deshalb rüstete, wer ein wenig Sicherheitsbewusstsein entwickelt hatte, seinen Internet-Browser mit kleinen Zusatzprogrammen und Erweiterungen (Add-ons) auf. Einige dieser Add-ons würden damit werben, zuverlässig gegen Tracker, nervige Werbung, sogenannte Zählpixel und andere Instrumente der Verhaltensdatensammler zu schützen. Nun stehen genau jene Zusatzprogramme, die den Nutzer schützen sollen, im Verdacht, ihn komplett zu durchleuchten. Recherchen des NDR hätten gezeigt, dass die so gewonnenen, vermeintlich anonymen Daten sich sehr wohl konkreten Personen zuordnen lassen. Über einen Lockvogel habe der NDR von den Zwischenhändlern einen Monat lang Zugriff auf die Daten Millionen deutscher Internetnutzer. Einsehbar sei dort für den kompletten August zunächst gewesen, wann und von wo der Nutzer X welche Internetseiten aufgerufen habe. Über die Adressen der E-Mail-Konten oder Social Media-Accounts, die oft den Namen des Kontoinhabers in der Adresszeile des Browsers führen, werde schnell klar, wem sich die Daten zuordnen lassen. Empfohlen werde nun, nur Add-ons zu benutzen, denen der Nutzer vertraut.

Hacker nutzen eine **Sicherheitslücke in Windows-Software** aus, berichtet die FAZ am 3. November. Für die Attacke mache das Unternehmen eine Gruppe verantwortlich, der Verbindungen zur russischen Regierung nachgesagt würden und die auch hinter einem Hacking-Angriff auf die Bundesgeschäftsstelle der Demokratischen Partei (DNC) in diesem Jahr stecken soll. Microsoft nenne diese Gruppe „Strontium". Sie ziele üblicherweise auf Regierungsbehörden und mit ihnen verbundene Unternehmen wie Rüstungskonzerne ab. Die Hacker seien in der Branche auch unter dem Namen „Fancy Bear" bekennt. Dass Google die Öffentlichkeit über die Sicherheitslücke informiert hat, bevor eine Lösung dafür gefunden wurde, erhöhe das Risiko für alle Kunden. Google habe darauf hingewiesen, dass es seiner Richtlinie gefolgt sei, sieben Tage nach dem Melden einer Schwachstelle an die Öffentlichkeit zu gehen. Nach Microsoft-Angaben handele es sich um einen sogenannten „Phishing"-Angriff, mit dem die Hacker versucht hätten, sich die Kontrolle über die Computer ihrer Opfer zu verschaffen.

Die Geschäftsprozesse verließen sich immer mehr auf die IT-Services, ist Martin Beims überzeugt (silicon.de am 1. November). Hieraus erwachse eine paradoxe Situation: IT-Services sollten leistungsfähiger werden, und das bei immer geringeren Kosten. Gleichzeitig steige durch die **Bedeutungszunahme von IT-Services** der mögliche Schaden bei auftretendem Systemausfall enorm an. Was zeichne gutes IT-Service-Management aus? Lösen Werkzeuge wie ITIL (IT Infrastructure Library) die Herausforderungen in der IT? In der aktuellen Version der ITIL würden die Prozesse, Rollen und Aktivitäten in einem durchgängigen Lebenszyklus beschrieben. Dieser spanne sich von der Ausrichtung der Service-Organisation über die Erfassung der Anforderungen, die Gestaltung, Implementierung und den Betrieb bis hin zur kontinuierlichen Anpassung der Servicequalität. Der Service Lifecycle gliedere sich in fünf Phasen: Service Strategie, Service Design, Service Transition, Service Operation und Continual Service Improvement. Um die Qualität und Quantität von IT-Services zu planen, zu überwachen und zu steuern, sei ein gut organisiertes IT-Service-Management unabdingbar. Effektives Service-Management orientiere sich immer an definierten und messbaren Zielen. IT-Services seien nur sinnvoll, wenn sie die Geschäftsprozesse des jeweiligen Kunden bestmöglich unterstützen und gleichzeitig den wirtschaftlichen Rahmenbedingungen und Vorgaben im Unternehmen gerecht werden.

Gut 2,1 Mrd. Euro wolle die britische Regierung über die kommenden fünf Jahre hinweg ausgeben, um IT- und Netzinfrastrukturen besser zu schützen, schreibt heise.de am 2. November. Die bis 2021 reichende Cybersicherheitsstrategie habe das Kabinett am 1. November auf den Weg gebracht. Die Ausgaben sollten damit fast verdoppelt werden. Die Fähigkeiten der Strafverfolger würden gestärkt und internationale Partnerschaften ausgebaut. Einen weiteren Schwerpunkt lege die Politik mit dem Plan darauf, mehr Experten für IT-Sicherheit auszubilden.

In der Ausgabe 11-2016 der Zeitschrift PROTECTOR behandelt Susanne Keck, RÜHL-CONSULTING GRUPPE, den „**Faktor Mensch in der Informationssicherheit**", konkret die „Einsatzmöglichkeiten von E-Portfolios (digitale Portfolios) zur Erfüllung der Anforderungen der ISO/IEC 27001" (S. 70/71). Die meisten Teilnehmer einer Befragung hätten die Akzeptanz (39 Prozent) und die technische Umsetzung (37 Prozent) als größte Herausforderungen beim Einsatz von E-Portfolios genannt. Wichtige Erfolgsfaktoren seien unter anderem die Festlegung des Portfoliotyps, Inhalte genau zu planen, eine klare Aufgabenfestlegung sowie die Portfolioarbeit in die Schulungen zu integrieren. Zudem müssten Evaluierungskriterien klar festgelegt und in die Praxis implementiert werden.

Wie die FAZ am 10. November berichtet, hat das Bundeskabinett eine **neue Cybersicherheitsstrategie beschlossen**. Diese soll „Risiken der digitalisierten Welt" begegnen. In der mehr als 40 Seiten starken Darstellung der Sicherheitsstrategie heiße es, das bestehende Abwehrzentrum solle unter Federführung des BMI zur „zentralen Kooperations- und Koordinationsplattform" weiterentwickelt werden. Es sei vorgesehen, dass das Abwehrzentrum bei Cybervorfällen, die zahlreiche Institutionen betreffen, zu einem Krisenreaktionszentrum wächst. Das BSI wolle „Mobile Incident Response Teams" aufstellen, die Cybervorfälle in den für das Gemeinwesen „besonders bedeutenden" Einrichtungen analysieren und bereinigen sollen.

In der Sonderausgabe der FAZ „Innovationstreiber IKT" am 17. November betont Prof. Dr. Andreas Blum, DHPG, dass IT-Sicherheit weit über die IT-Infrastruktur hinausgeht. Dies belege vor allem die gefährlichste, aber oftmals wenig beachtete Schwachstelle bei deutschen Mittelständlern, die eigenen Mitarbeiter. Fehlende IT-Kenntnisse oder eine mangelnde Sensibilität für Risiken einer fahrlässigen Nutzung der IT sorgten dafür, dass Betrüger die „Schwachstelle Mensch" leichter ausnutzen können. Mittelständler sollten ihre Angestellten für den richtigen Umgang mit solchen Gefahren im Arbeitsalltag regelmäßig schulen und ihr Bewusstsein für Risikopotenziale schärfen. Um Manipulationen, aber auch unbewusste Fehler, weitestgehend zu vermeiden oder aufzudecken, seien prozessintegrierte Kontrollmaßnahmen erforderlich. Eine weitere IT-Schwachstelle bei deutschen Mittelständlern ergebe sich durch die zunehmend verschwimmende Grenze zwischen der privaten und geschäftlichen Nutzung von mobilen Endgeräten wie Smartphones oder Notebooks. Mittelständler sollten die Vor- und Nachteile von BYOD- oder COPE-Strategien genau abwägen. Entscheiden sich mittelständische Unternehmen trotz der Risiken für einen privaten und geschäftlichen Gebrauch von mobilen Endgeräten, gelte es, den Datenschutz und die -sicherheit zu gewährleisten.

Wie sich der **Mittelstand** gegen Hacker schützt, zeigt Bernd Hanstein, Rittal, in der Ausgabe 11-2016 der Zeitschrift GIT, S. 63–65. Laut Kaspersky Lab habe Deutschland im weltweiten Vergleich zwischen April 2015 und März 2016 am stärksten unter Beschuss durch die besonders gefährliche **Ransomware** gestanden. Eine wahre Fundgrube für Gefahrenquellen aller Art sei der Grundschutzkatalog des BSI. Aufgeteilt in fünf Kategorien, von elementaren Gefährdungen bis zu vorsätzlichen Handlungen, seien hier knapp

630 verschiedene Varianten beschrieben, die zum IT-Ausfall oder Datenverlust führen. Die IT-Sicherheit müsse im Rechenzentrum bereits auf Ebene der Infrastruktur beginnen. Komponenten für die Energieversorgung wie USC und PDU (intelligente Stromverteiler) sowie Geräte für die Kälteversorgung wie Chiller, Klimasysteme und Pumpen verfügten über Netzwerkschnittstellen und seien IP-basiert. Daher müssten Hersteller und Betreiber dafür sorgen, dass diese Systeme gegen Angriffe gesichert sind. Unterstützung böten hier spezielle Software-Werkzeuge, die eine Infrastruktur zum Beispiel nach offenen Ports oder nach Standard-Passwörtern analysieren.

Für **proaktive IT-Sicherheitslösungen** plädiert Rohde & Schwarz in der Ausgabe 11-2016 der Zeitschrift GIT, S. 66/67. Herkömmliche Sicherheitsmechanismen und Antivirensoftware böten Unternehmen heute keinen adäquaten Schutz mehr gegen Hackerangriffe. „Zero Day Exploits" etwa nutzten eine Sicherheitslücke aus, noch bevor diese bekannt ist. Die neuen Lösungen für Endprodukte beruhten auf dem technologischen Ansatz „Security by design". Die Datensicherheit sei hier eine Kernsäule des Produkts und werde bereits bei der Entwicklung in das Betriebssystem integriert.

Keine Haftung für WLAN-Schlüssel, titelt die FAZ am 25. November. Muss eine Privatperson ihren WLAN-Router über die Voreinstellung hinaus zusätzlich absichern, um damit das illegale Herunterladen von Dateien durch andere Nutzer zu verhindern? Diese Frage der Störerhaftung in einem passwortgeschützten Netzwerk musste der BHG in einer Klage zur Erstattung von Abmahnkosten klären. Verbraucher sind nicht verpflichtet, ein eigenes sicheres Passwort einzugeben, entschieden die Richter: Komme es innerhalb der marktüblichen Sicherheitsverschlüsselung zu einem Missbrauch in Form des sogenannten Filesharings durch einen Hacker, hafte der Verbraucher weder für den Schaden noch für die entstandenen Abmahnkosten.

IuK-Kriminalität

Der Sicherheitsanbieter Avast habe noch einmal eindrücklich vor dem **Banking-Trojaner GM Bot** gewarnt, berichtet silicon.de am 2. November. Die Malware, die auch als Acecard, SiemBunk oder Bankosy bezeichnet werde, basiere auf Open Source-Code. Der sei im Darknet kostenfrei erhältlich, sodass Kriminelle auf dieser Grundlage schnell und vergleichsweise unkompliziert Schadprogramme erstellen und in Umlauf bringen können. Laut Avast seien derzeit schon Kunden von Sparkasse, Postbank, Commerzbank, Volksbank Raiffeisenbank und Deutscher Bank ins Visier der Kriminellen geraten. Ihren Opfern präsentiere die Android-Malware auf dem Smartphone täuschend echt nachgebaute Log-in-Seiten. Allein in den vergangenen drei Monaten habe Software von Avast derartige Angriffe von GM Bot über 200.000 Mal abwehren können. Die Malware tarne sich wie bei Android Schadsoftware üblich, als App für einen anderen Zweck.

Abo-Fallen und Trojaner kommen mit Multimedia-Anzeigen aufs Smartphone, titelt die FAZ am 16. November. Betrüger nutzten vor allem zwei Schwachstellen aus: Die Abo-Falle, in welche man mit dem Handy tappt, stehe an erster Stelle. Dabei schließe man angeblich ein rechtskräftiges Abonnement ab, nachdem schnell hintereinander verschiedene Anzeigen auf dem Display aufgeploppt sind. Die Betrüger hätten meist eine Adresse im fernen Ausland. Sich bei ihnen zu beschweren, sei sinnlos. Um dem Missbrauch einen Riegel vorzuschieben, müsse man bei seinem Anbieter eine kostenlose Drittanbietersperre einrichten lassen. Rund 40 Prozent aller Anfragen bei den Verbraucherzentralen entfielen auf den Anbieter Mobilcom-Debitel. Ein zweites Problem mit Werbeanzeigen betreffe nur das Google-Betriebssystem Android. Ein neuer Banking-Trojaner namens Svpeng solle bereits mehrere hunderttausend Geräte befallen haben. Er schleiche sich über

Anzeigen im Google-Browser Chrome auf das Smartphone. Zuvor nutze er als Versteck das Werbenetz Adsense, das ebenfalls von Google betrieben wird. Nach einem Klick auf eine infizierte Werbeanzeige erscheine die Meldung, dass ein wichtiges Update des Browsers erforderlich sei. Bestätigt der Nutzer, lade er keineswegs die aktualisierte Version, sondern die Schadsoftware.

Datendiebstahl koste den Kabel- und Drahtkonzern **Leoni** 40 Mio. Euro, berichtet die FAZ am 17. November. Das Unternehmen sei Opfer einer Betrugsmethode mit falschen E-Mail-Adressen und manipulierten Unterschriften geworden, die Fachleute „Chefbetrug" oder „Fake-President-Masche" nennen würden. Unter Verwendung gefälschter Dokumente und Identitäten sowie unter Nutzung elektronischer Kommunikationswege hätten Unbekannte Gelder des Unternehmens auf Zielkonten im asiatischen Ausland transferiert. Zum Schutz vor Cyberkriminalität habe Leoni eine Versicherung abgeschlossen.

Capgemini sollen mehrere Gigabyte an persönlichen Daten von Jobbewerbern abhanden gekommen sein, schreibt Martin Schindler am 11. November in silicon.de. Nach einem Bericht von Sicherheitsforscher Troy Hunt, dem ein Teil der Daten vorliegen soll, seien darin mehr als 780.000 unterschiedliche E-Mail-Adressen sowie zahlreiche weitere persönliche Daten über die Bewerber enthalten. Die durchgesickerte MySQL-Datenbank sei mehr als 30 Gigabyte groß. Daten sollen neben den E-Mail-Adressen und Namen von Bewerbern auch Telefonnummern, Anschriften, Anschreiben und vollständige Lebensläufe gespeichert worden sein. Unklar sei, ob die Daten tatsächlich von kriminellen, externen Hackern oder von einem Insider gestohlen wurden.

Peter Marwan schreibt am 24. November in silicon.de, Forscher des Sicherheitsanbieters Zscaler hätten um gefährliche Funktionen ergänzte Varianten der **Ransomware Stampado** entdeckt. Die könnten sich nun ähnlich wie ein Computer-Wurm selbst weiterverbreiten. Außerdem seien sie in der Lage, Dateien nicht nur auf der lokalen Festplatte, sondern auch auf Netzlaufwerken und externen Speichermedien zu verschlüsseln, um dann Lösegeld zu erpressen. Das sollte man allerdings auf keinen Fall bezahlen. Inzwischen liege nämlich ein Entschlüsselungstool für Stampado vor. Die Erstinfektion mit Stampado erfolge in der Regel über E-Mails oder Drive-by-Downloads. Stampado installiere sich dann im Ordner „AppData" unter dem Namen des legitimen Windows-Prozesses „svchost.exe" und versuche so seine Entdeckung und Entfernung zu erschweren.

Kindergartensicherheit

PROTECTOR stellt in der Ausgabe 11-2016, S. 38/39, ein **Türenmanagement für Kindergärten** vor. Die Eingangstüren seien durch eine Fluchttürverriegelung gesichert. Von innen könne die Tür über zwei Taster geöffnet werden. Ein Taster befinde sich in 1,80 Meter Höhe. Ein zweiter Taster sei auf etwa einem Meter Höhe angebracht. So könnten auch Kinder die Tür im Notfall selbst öffnen. Dieser Taster sei in ein Fluchtwegterminal integriert. Wird er gedrückt, öffne sich die Tür und ein Alarm ertöne. So könnten sich die Schützlinge nicht unbemerkt hinaus schleichen. Das Zutrittskontrollsystem Scala.net erlaube eine in ein Netzwerk integrierte Anlagenstruktur. Einen zusätzlichen Schutz vor Langfingern biete das Mediator-System an den Außentüren der Kita. Der Mediator ist ein selbstverriegelndes Panikschloss. Durch die integrierte Panik-Funktion könne die Tür von innen jederzeit ohne Schlüssel oder Transponder geöffnet werden.

Kommunikationssicherheit

Johann Deutinger, Ferrari Electronic AG, befasst sich in der Ausgabe 11-2016 des PROTECTOR, S. 37, mit **Unified Communications-Lösungen** (UC). Sie bündelten die gesamte Kommunikation wie E-Mail, Telefonie, Fax, Videokonferenzen oder Präsenzanzeige in einer Oberfläche. Immer häufiger hätten Unternehmen aber auch weitere Anforderungen an eine UC-Lösung – sie wollten die Gebäudeautomation darüber steuern. Wenn Unternehmen ihre Telefonanlage auf Microsoft Lync oder Skype for Business migrierten, könnten sie auch die Zutrittskontrolle via Video-Türsprechanlage integrieren. Dazu benötigten sie herstellerspezifische Gegenstellen zur Rufannahme und Videoanzeige. In die Oberfläche von Lync oder Skype for Business ließen sich Systeme wie die Türgegensprechanlage, Türöffner, Schranken, aber auch Alarmanlagen oder Überwachungskameras integrieren.

Korruption

Jeder dritte Teilnehmer einer Umfrage von Transparency International sei der Ansicht, dass alle oder die meisten Führungskräfte in der Wirtschaft in Korruption verstrickt sind, meldet die FAZ am 17. November. Das Image der Manager sei damit deutlich schlechter als das von Politikern oder der Polizei. So schätzten von den 1.500 Befragten lediglich sechs Prozent alle oder die meisten Parlamentsmitglieder als korrupt ein. Bei der Polizei hielten vier Prozent alle oder die meisten Bediensteten für korrupt. In Unternehmen versagten selbst die besten Vorkehrungen gegen Korruption, wenn Integrität nicht von der Unternehmensleitung vorgelebt wird. Im internationalen Vergleich schneide Deutschland am besten ab – vor Schweden und der Schweiz. Korruption nannten nur zwei Prozent als eines der drei wichtigsten Probleme, denen sich ihr Land gegenübersehe. In der Republik Moldau seien es mit 67 Prozent die meisten, gefolgt von Spanien mit 66 Prozent.

Krisenregionen

Am 18. November hat das BKA eine Information über die Gefährdungslage in der **Türkei** veröffentlicht. Derzeit sei in allen Teilen des Landes von einer erhöhten terroristischen Gefährdung auszugehen. Hierbei könnten sich die Aktivitäten auch gegen touristische Ziele richten, um so den türkischen Staat und seine bedeutenden Einnahmequellen empfindlich zu treffen. Es sei weiterhin mit der gesamten Bandbreite terroristischer Aktionen der PKK und ihr nahestehenden Gruppierungen zu rechnen. In Bezug auf den sogenannten IS bleibe festzuhalten, dass dieser die Türkei nunmehr als legitimes Angriffsziel benenne und zur Durchführung von Anschlägen aufrufe. Deutsche Einrichtungen und Interessen in der Türkei stünden nicht im unmittelbaren Zielspektrum der genannten Akteure. Das Risiko des zufälligen Mitbetroffenseins sei für westliche und somit auch deutsche Staatsbürger jedoch jederzeit gegeben und müsse nach der Vielzahl der schweren Anschläge der letzten Monate und der negativen Gesamtentwicklung als erhöht bezeichnet werden.

Luftverkehrssicherheit

Schattenblick.de berichtet am 7. November, dass der von der Bundesregierung vorgelegte Gesetzentwurf zur Änderung des **Luftsicherheitsgesetzes** (18/9752) bei Experten auf unterschiedliche Einschätzungen stoße. Dies sei bei einer Sachverständigen-Anhörung des Innenausschusses zu der Vorlage deutlich geworden. Mit der Neuregelung solle das nationale Recht an die EU-Luftsicherheitsverordnung angepasst werden. Zugleich solle der Vorlage zufolge das Sicherheitsniveau

im Bereich der Luftfracht erhöht werden. So solle das BMI unter bestimmten Voraussetzungen ein „Einflug-, Überflug-, Start- oder Frachtbeförderungsverbot für einzelne Luftfahrzeuge oder eine näher bestimmte Gruppe von Luftfahrzeugen" verhängen können. Laut Ministerium sollen zudem zum Schutz des zivilen Luftverkehrs vor Anschlägen durch mögliche Innentäter die Vorschriften für die Zuverlässigkeitsüberprüfung verschärft werden: Danach bedürften künftig auch die Arbeitnehmer, für die bislang eine sogenannte beschäftigungsbezogene Überprüfung durch den Arbeitgeber ausreichend war, einer behördlichen Zuverlässigkeitsüberprüfung. Dies betreffe insbesondere das im Frachtbereich tätige Personal. Darüber hinaus werde erstmals die Zulassung und Überwachung der an der sicheren Lieferkette für Luftfracht beteiligten Unternehmen im nationalen Recht geregelt. Gleichzeitig würden die Verfahren konkretisiert, mit denen die europäischen Bestimmungen zur Kontrolle der Luftfahrtunternehmen, die Luftfracht oder Luftpost von einem Drittstaaten-Flughafen in die EU befördern, in Deutschland umgesetzt werden. Mit der Einführung einer bundeseinheitlichen Zertifizierungs- und Zulassungspflicht für Luftsicherheitskontrolltechnik sollten schließlich einheitliche Qualitätsstandards in allen Bereichen sichergestellt werden, in denen diese besondere Technik zum Einsatz kommt.

kn-online.de meldet am 16. November, dass eine neue Technik am Flughafen Köln/Bonn in den Testbetrieb gegangen sei. Angeschoben worden sei sie vom Bundesinnenministerium und vom Bundesverband der Deutschen Luftverkehrswirtschaft. Das Ziel: Die **Sicherheitschecks am Flughafen** sollten **weniger nervenzehrend** sein. Dafür sei nicht nur die Technik überarbeitet worden, sondern auch die Abläufe. Erfahrene Vielflieger mit reichlich Kontrollerfahrung könnten flugs Passagiere überholen, die etwas länger brauchen, weil sie erst mal alle Münzen aus den Hosentaschen nesteln müssen. Es gebe nun fünf nebeneinander angeordnete Stationen. Dort würden automatisch Wannen bereitgestellt. Auch beim Scanner gehe es nun flotter zu. Der Scanner brauche weniger als eine Sekunde, die Arme müssten nicht mehr über den Kopf gehalten werden. Wer die Schuhe ausziehen muss, finde dafür eine „eigene Sitzinsel" vor. Flughafenchef Michael Garvens spreche von einem Quantensprung.

Maschinensicherheit

Die optimale Sicherheit für Nutzer und Prüfer von **Industriearmaturen** wird von Tilo Schmidt, Pilz GmbH & Co. KG, in der Zeitschrift GIT in der Ausgabe 11-2016, S. 92/93, thematisiert. Anlagen in der industriellen Steuerungs- und Regelungstechnik stünden häufig unter Druck. Damit die eingesetzten Komponenten den extremen Anforderungen in der Praxis Stand halten, habe ATG Automatisierungstechnik Gröditz GmbH gemeinsam mit Pilz GmbH & Co. KG Prüfstände beim Armaturenhersteller Gestra optimiert. Mit dem Automatisierungssystem PSS 4000 von Pilz könnten sich Kunden auf zuverlässige Produkte, Prüfer auf einen sicheren Arbeitsplatz bei bis zu 1.250 bar Wasserdruck verlassen.

Elektronische Schlüsselsysteme für die sichere Betriebsartenwahl behandelt GIT in der Ausgabe 11-2016, S. 94–97. Die Forderung nach einer sicherheitstechnischen Bewertung der Betriebsartenwahl sei dadurch begründet, dass bei der Umschaltung von einer Betriebsart in eine andere verschiedene sicherheitstechnische Einrichtungen an der Maschine zu- und abgeschaltet werden. Das Umschalten zwischen unterschiedlichen Sicherheitseinrichtungen müsse einen Performance Level nach EN ISO 13849-1 erfüllen. Um einen Betriebsartenwahlschalter normativ beurteilen zu können, müssten dessen Bestandteile betrachtet werden. Die gegenüber einem Schlüssel sicherere Alternative sei eine elektronische Zugangsbeschränkung.

Euchner biete hierfür beispielsweise das Electronic-Key-System EKS an, ein auf der Transpondertechnologie basierendes System. Es bestehe aus einer Schreib-Lese-Station sowie einem oder mehreren Schlüsseln mit programmierbarem Speicher und diene der elektronischen Zugriffsverwaltung. Das EKS erfülle alle normativen und gesetzlichen Anforderungen für ein Zugangssystem zur Betriebsartenwahl. Der Beitrag behandelt die Betriebsartenwahl mit EKS und Touchpanel, die sichere Zugangsbeschränkung durch EKS, die Betriebsartenwahl mit EKS und Tasten sowie EKS Light und EKS Light FSA.

Mit **mechanischen Schutzeinrichtungen** befasst sich Dipl.-Ing. Rainer Semmler, TÜV SÜD, in der Ausgabe 11-2016 der Zeitschrift GIT, S. 98–100. Kann in Produktionsanlagen ein gefährlicher Überdruck entstehen, dann werden Berstscheiben und Sicherheitsventile eingebaut. Sie müssten bei einem definierten Druck ansprechen. Angaben zur Zuverlässigkeit seien für diese Bauteile bisher Mangelware. Für die Risikobewertung fehlten definierte Kriterien und Methoden. Benötigt würden Lösungsansätze, die sowohl die Risiken quantifizieren als auch auf Qualitätssicherung und Produktprüfungen setzen. Berstscheiben und Sicherheitsventile seien als Bestandteil des Gesamtkonzepts von prozesstechnischen Schutzeinrichtungen unverzichtbar. Anders als die sicherheitsrelevanten Einrichtungen der Prozessleittechnik (PLT) unterlägen die **mechanischen Schutzeinrichtungen** nicht den Anforderungen der internationalen Standards DIN EN 61508 und 61511 zur funktionalen Sicherheit. Es fehlten Schnittstellen und definierte Vorgehensweisen, um auch mechanische Schutzeinrichtungen adäquat zu berücksichtigen. Sensoren, Prozessoren und Aktoren müssten äußerst zuverlässig arbeiten. Dieses Ziel könne gut erreicht werden. Durch die Normen zur funktionalen Sicherheit seien die Hersteller dazu verpflichtet, fundierte Angaben zu den Produkteigenschaften zu machen. Schutzeinrichtungen und betriebliche Maßnahmen wirkten den Gefährdungen eines Produktionsprozesses auf verschiedenen Ebenen entgegen. Würden die definierten Grenzwerte der normalen Prozesssteuerung überschritten, greifen die Schutzeinrichtungen ein. Sie sollen das Ereignis verhindern bzw. seine Auswirkungen begrenzen. Wenn die Schutzeinrichtungen, Systeme und Maßnahmen nicht greifen, trete der betriebliche Notfallplan in Kraft. Maßnahmen, die der Qualitätssicherung dienen (z. B. Produktprüfungen, Typenzertifikate) würden vielfach noch zu wenig beachtet.

Die **Bewertung der Sicherheit von Maschinensteuerungen** thematisiert GIT in der Ausgabe 11-2016, S. 101–103. Die lizenzfreie Software Sistema (Sicherheit von Steuerungen an Maschinen) diene 60.000 registrierten Nutzern der Bewertung der Sicherheit von Maschinensteuerungen im Rahmen der DIN EN 13849-1. Das Windows-Tool bilde die Struktur der sicherheitsbezogenen Steuerungsteile auf der Basis der sogenannten vorgesehenen Architekturen nach und berechne Zuverlässigkeitswerte auf verschiedenen Detailebenen einschließlich des erreichten Performance Level (PL). 2016 sei eine völlig überarbeitete und erweiterte Version 2 der Software veröffentlicht worden. Sie sei an die durch die 3. Ausgabe der DIN EN ISO 13849-1 entstandenen neuen Möglichkeiten angepasst. Zusätzlich seien eine neue Importschnittstelle und eine zusätzliche Bedienoberfläche zum Einlesen von Kennwert-Bibliotheken im Format des VDMA-Einheitsblattes 66413 realisiert. Die Software werde weiterhin das eigene Format der Sistema-Bibliotheken unterstützen und deren Funktionen ausbauen. Für den Maschinen- und Steuerungsbau böten die Sistema-Bibliotheken nach wie vor die einzige Möglichkeit, selber auch Bauteile und komplexere Steuerungsteile für die Wiederverwendung zu speichern.

Für **regelmäßige Inspektionen** zur Sicherheit von Mensch und Maschine plädiert GIT in der Ausgabe 11-2016, S. 104/105. Durch

die Betriebsmittelsicherheitsverordnung werde in Deutschland die Prüfung einer Maschine oder Anlage vor der ersten Inbetriebnahme, nach längeren Stillstandzeiten, nach Veränderungen und in regelmäßigen Abständen gefordert. Der Leistungsumfang der Sicherheitsinspektionen umfasse: die Erfassung und Kennzeichnung der Maschine und Schutzeinrichtung, die Prüfung des sachgerechten Anbaus der Schutzeinrichtung, optionale Nachlaufzeitmessung und Prüfung des Sicherheitsabstandes der Schutzeinrichtung zur Gefahrstelle, die Prüfung der Schaltpläne auf schaltungstechnische Einbindung der Schutzeinrichtung in die Maschinensteuerung, die Prüfung aller Funktionen der Schutzeinrichtung und des sicheren Zusammenwirkens mit der Maschinensteuerung, die praxisgerechte Hilfe bei der Problemanalyse und dem Aufzeigen von Lösungen sowie die Dokumentation aller Prüfergebnisse.

Dipl.-Ing. Rolf Hausmann, Phoenix Contact, stellt in der Ausgabe 11-2016 der Zeitschrift GIT, S. 106/107, die **intelligente Statusanzeige des Überspannungsschutzes** mit Überwachungsfunktion in der Prozesstechnik vor. Blitzschutznormen würden eine regelmäßige Überprüfung der Schutzgeräte empfehlen. Dies lasse sich auch über eine Sichtprüfung durchführen, wenn das Überspannungsschutzgerät (ÜSG) eine Statusanzeige besitzt. Mit dem intelligenten Überspannungsschutz Plugtrab PT-IQ von Phoenix Contact werde der Zustand der Schutzgeräte über eine elektrische Messung kontinuierlich überwacht. Gemessen würden sowohl Leckströme als auch Überspannungsimpulse an jedem spannungsbegrenzenden Bauelement. Die Messergebnisse würden an einen internen Mikrocontroller weitergegeben und ausgewertet. Der Beitrag behandelt den Einsatz in explosionsgeschützten Bereichen und die Auswahl des geeigneten Schutzes. Ein Monitoring-System signalisiere bereits einen Verschleiß der Schutzgeräte, bevor sie durch eine Überlastung ausfallen.

Fanny Platbrood, Sick AG, zeigt in der Ausgabe 11-2016 der Zeitschrift GIT, S. 108–110, Sicherheitslösungen für die **intelligente Mensch-Roboter-Kollaboration**. Dominierend seien zwei Interaktionsszenarien: die Koexistenz und die Kooperation. Raum und Zeit seien hierbei die maßgebenden Interaktionsparameter. Im Rahmen von Industrie 4.0 rücke eine dritte Interaktionsform zunehmend in den Mittelpunkt: die Kollaboration von Menschen und Robotern (MRK). Hierbei teilten sich beide zum gleichen Zeitpunkt denselben Arbeitsraum. Der Beitrag behandelt insbesondere sicherheitsgerichtete Betriebsarten kollaborierender Robotersysteme und die funktionale Sicherheit für MRK: Expertise, Portfolio und Umsetzung aus einer Hand. Die Geschwindigkeits- und Abstandsüberwachung in MRK-Anwendungen biete das größte Zukunftspotenzial der verschiedenen Kollaborationsarten der ISO/TS 15066.

Öffentlicher Personennahverkehr

In der Ausgabe 11-2016 weist PROTECTOR darauf hin, dass die BVG in Berlin zum Schutz und der Betreuung von über einer Milliarde Fahrgäste pro Jahr neben dem eigenen Sicherheitsdienst auch rund 115 Mitarbeiter des Sicherheitsdienstleisters WISAG einsetzen. Die durchliefen vor ihrem ersten Einsatz eine 15-tägige Schulung. Lerninhalte seien unter anderem die Dienstvorschriften der U-Bahn, Verkehrsgeografie und Kundenorientierung. Darüber hinaus müsse eine Ausbildung als Ersthelfer, im Gebrauch der Feuerlöscher und eine erfolgreiche arbeitsmedizinische Vorsorgeuntersuchung G 25 für Fahr-, Steuer- und Überwachungstätigkeiten vorliegen.

Öffentliche Sicherheit

Bundesinnenminister de Maizière hat im Rahmen einer BKA-Tagung am 16. November

über fünf **Elemente einer „Polizei des Jahres 2020**" gesprochen. Sie seien Teil einer Vision und zugleich Hausaufgaben. Im Wesentlichen handelt es sich um folgende Elemente:

1. Im „BKA 2020"

- Verbesserung der IT-Infrastruktur zu einer hochmodernen und einheitlichen IT-Architektur
- Volle Umsetzung der Anforderungen des Bundesverfassungsgerichts (hypothetische Datenneuerhebung)
- Schaffung eines neuen BKA-Gesetzes
- Aufbau eines Fluggastdaten-Informationssystems
- Entwicklung technischer Hilfsmittel und Wahrung des neuesten Stands
- Konzentration des technischen Know-how in einer „Zentralen Stelle für Informationstechnik im Sicherheitsbereich" (ZITIS)

2. Bund-Länder-Kooperation

- Einheitliches Fallbearbeitungssystem
- Kerndatensystem, dessen Rückgrat Fingerabdruckdaten bilden als Vorbild eines neuen Informationssystems der Polizei
- Statt Datenablage in verschiedenen „Töpfen" einheitliche analysefähige Plattform

3. Europa

- Statt unterschiedlicher „Datentöpfe" (z. B. Eurodac, Fingerabdruckdatei ohne Namensbezug) allgemeine Vernetzung der Informationssysteme (Eurodac, Schengener Informationssystem, VISA-Informationssystem, Europäisches Einreise-/Ausreisesystem und Europäisches Reiseinformations- und Genehmigungssystem) mit genau geregelten Zweckbindungen

4. Recht

- Modernes Recht, das die Chancen der neuen Technik nutzbar macht
- Datenschutz mit geordnetem Zugriffsmanagement, Vollprotokollierungen mit Analysefunktionen für die Datenschutzaufsicht und Datenmanagement, das sich an der Qualität der Eingriffe bei der Datenerhebung orientiert

5. Polizei und Gesellschaft

- Schaffung der erforderlichen und gebotenen Mittel und Instrumente für die Polizei
- Verbesserte Videoüberwachung an öffentlich zugänglichen Plätzen
- Bodycams für die Bundespolizei
- Lesesysteme für die Kennzeichen von Kfz, um Fahndungen schneller und einfacher durchzuführen
- Schärfere Bestrafung von gewalttätigen Angriffen auf Polizisten, Justizbedienstete und Rettungskräfte
- Schärfere Bestrafung von Wohnungseinbrüchen

Raubkopien

Nach einer Meldung der FAZ hat die Polizei bei einem Mann aus Esslingen nach 3.000 Kisten im Januar jetzt nochmals tonnenweise illegal gepresste CDs, DVDs und Vinyl-Schallplatten bei Durchsuchungen in Lagerhallen und Presswerken in Deutschland und Polen sichergestellt. Nach Meinung einer auf Urheberrecht spezialisierten Rechtsanwaltskanzlei sei klar, dass hier kriminelle Netzwerke tätig waren. Von Einzeltätern ließen sich Fälschungen und Kopien in dieser Größenordnung, in verschiedenen Presswerken produziert und mit professionellen Covern versehen, nicht bewältigen.

Risikomanagement

Dr. Michael Buser, Risk Experts Risiko Engineering GmbH, befasst sich in der Ausgabe 11-2016 von PROTECTOR, S. 72/73, mit dem

Thema Risikomanagement. Es sei Zeit, dass „konventionelle Maßnahmen" durch „risikoadäquate Strategien" abgelöst werden. Im Gegensatz zur konventionellen Herangehensweise (baulicher, technischer und organisatorischer Schutz in Ergänzung zu abwehrenden Maßnahmen) würden die Elemente „Hardware", „Software" und „Lifeware" als integrale Bestandteile der Sicherheitskultur eines Unternehmens verstanden. Es komme auf das interaktive Zusammenspiel und damit auf die komplexen Wechselwirkungen zwischen einzelnen Faktoren an, die das Risiko bestimmen. Am Ende werde der Faktor Mensch noch wichtiger.

Sicherheitsgewerbe

In der Ausgabe 11-2016 der Zeitschrift GIT, S.16–19, nimmt Dr. Harald Olschok, BDSW, im Interview zur erfolgreichen **Neuausrichtung der Sicherheitswirtschaft** Stellung. Nach vorläufigen Schätzungen betrage der Umsatz des Bereichs der Sicherheitsdienstleistungen im Jahr 2015 ca. 6,9 Mrd. Euro. Das seien 47 Prozent des Gesamtumsatzes der Sicherheitswirtschaft. 5.500 Unternehmen beschäftigen 247.000 Sicherheitsmitarbeiter und damit 72 Prozent der Beschäftigten in der Sicherheitswirtschaft. Die erfolgreiche Einführung der beiden Ausbildungsberufe und der Modernisierung der Geprüften Schutz- und Sicherheitskraft dürfe nicht darüber hinwegtäuschen, dass die meisten Beschäftigten lediglich über eine modulare, aufgabenbezogene Qualifizierung verfügen. Im August 2016 seien bundesweit 12.180 Stellen nicht besetzt gewesen. Die demografische Entwicklung werde dazu führen, dass die Löhne in den nächsten Jahren überproportional steigen müssten. Der Staat sei ohne private Sicherheitskräfte nicht in der Lage, das hohe Sicherheitsniveau zu halten. Bis zu 12.000 private Sicherheitskräfte seien pro Spieltag in den drei Bundesligen im Einsatz. Notwendig seien gesetzliche Vorgaben für den Einsatz von Sicherheits- und Ordnungskräften in Fußballstadien. Das Sicherheitsgewerbe wolle keine Überregulierung, wolle aber ganz sensible Aufgaben nicht allein den Marktkräften überlassen. Der BDSW fordere ein sektorspezifisches Gesetz für die Aufgabenfelder, in denen eine enge Zusammenarbeit mit der Polizei zwingend notwendig sei. Dazu gehöre neben dem Schutz von Flüchtlingsunterkünften auch der Schutz der Einrichtungen der kritischen Infrastruktur und der Veranstaltungsschutz.

Eigentlich sollte man davon ausgehen können, dass nach den Personal-**Skandalen mit Security-Personal** in den Landesunterkünften für Flüchtlinge mittlerweile überall untadelige Sicherheitsfirmen im Einsatz sind, heisst es in rp-online.de am 18. November. Doch offenbar hätten einige Entscheidungsträger in den Behörden aus früheren Fehlern nicht viel gelernt. Anders sei es kaum zu erklären, dass eine Bezirksregierung ernsthaft einem Unternehmen den Zuschlag für Schutz und Überwachung einer Unterkunft erteilen wollte, dem in einem anderen Bundesland wegen fragwürdiger Methoden gekündigt worden sei. Offenbar scheine für einige Spitzenbeamte der Preis und nicht die Qualität ausschlaggebend bei der Vergabe zu sein.

Sicherheitstechnik

PROTECTOR weist in der Ausgabe 11-2016, S. 8, auf die Trendstudie „**Das sichere Gebäude der Zukunft**" hin, die Hekatron mit 2b AHEAD ThinkTank und dem Unternehmen Schentzek & Kühn erstellt habe. Danach werde künftig die Digitalisierung alle Lebensbereiche mit Informations- und Kommunikationstechnologien durchdringen. Das „Internet der Dinge" umfasse in Zukunft nicht nur einzelne Häuser, sondern ganze Städte, letztlich die ganze Welt. Die notwendige Sensorik werde in den nächsten Jahren noch deutlich kostengünstiger sein und praktisch in jedes

Bauteil integriert. Alle Gewerke würden über interoperable Netzwerke verbunden sein. Intelligente Algorithmen und die notwendigen Rechnerleistungen würden zur Verfügung stehen.

Gerhard Gumprecht, Honeywell Building Solutions, beschreibt in der Ausgabe 11-2016 der Zeitschrift GIT, S. 22/23, Technologie-Innovationen, die Sicherheitskonzepte verändern. Er bezeichnet als die **sechs interessantesten Entwicklungen der Security Trends**: Biometrie werde zum Mainstream. Dank biometrischer Authentifizierungsmethoden stiegen gleichzeitig die Sicherheit und der Komfort für die Betreiber. Intelligenz bewege sich „an den Rand". Speicher und Intelligenz befänden sich heute in den Geräten selbst oder am „Rand" der Cloud. Die sogenannte „Edge Intelligence" beeinflusse auch Innovationen wie elektronische Schlösser oder E-Locks, die eine drahtlose Zugangskontrolle für Türen bieten. IT und Sicherheit konvergieren. Dies bringe einige Vorteile mit sich, etwa dass die Identifizierung von Nutzern und ihre Anmeldeinformationen bzw. Berechtigungen vereinheitlicht werden für eine einfache und präzisere Verwaltung. Mehr Daten mit weniger Ressourcen verwalten: Der alleinige Betrieb von Einzelsystemen sei kaum mehr üblich. Komplexe Technologien, Geschäftsanwendungen und Sicherheitssysteme in Gebäuden sollten nicht nur effektiv und möglichst ressourcenschonend miteinander verknüpft werden, sie erzeugten immer größere Datenvolumina. Mobilität stehe an erster Stelle. Und Nutzererfahrung gehe vor komplexen Handbüchern und Anleitungen.

Steuerhinterziehung

„Muss sich bald jeder Händler in Deutschland eine elektronische Kasse anschaffen und für jeden Kauf einen Beleg ausstellen?", fragt die FAZ am 21. November. Gehe es nach der SPD, soll jeder Kunde einen Beleg für seinen Kauf erhalten. Nur eine Bagatellgrenze wäre wahrscheinlich. Die Union wolle zwar ebenfalls die Steuerhinterziehung mit Hilfe manipulierter Kassensysteme bekämpfen, aber das österreichische Vorgehen hält sie für wenig tauglich. „Wir wollen weder eine generelle Pflicht zur Anschaffung einer Registrierkasse noch eine allgemeine Belegausgabepflicht", habe Ralph Brinkhaus, stellvertretender Vorsitzender der Unionsfraktion, gesagt.

Tunnelsicherheit

Hendrick Lehmann, Redaktion PROTECTOR, erklärt in der Ausgabe 11-2016, S. 20–22, das **Brandschutzkonzept im neuen Gotthard-Tunnel**. Hauptproblem für die Feuerwehren sei die effektive Brandbekämpfung bei hohen Temperaturen am Brandherd, die bis zu 1.300 Grad Celsius betragen und Schäden an den Tunnelgewerken verursachen können. Gleichzeitig müsse sichergestellt sein, dass trotz der widrigen Bedingungen im Brandfall eine Personenrettung möglich ist. Die beiden Tunnelröhren seien durch zwei sogenannte Multifunktionsstellen in drei etwa gleich lange Abschnitte unterteilt. Hier befinden sich jeweils eine Haltestelle pro Fahrrichtung mit je zwei Spurwechseln. Zwischen beiden Tunnelröhren befinden sich alle 325 Meter Stollen, in denen Zugreisende auf Hilfe warten könnten. Die Türen müssten während 90 Minuten eine Brandtemperatur von 1.000 Grad aushalten. Alle den Tunnel nutzenden Züge müssten über das Zugsicherungssystem ETCS Level 2 verfügen. Eine Evakuierung finde über die je 600 Meter langen Plattformen statt. Eine Evakuierung von bis zu eintausend Personen sei in kurzer Zeit möglich. Die Frischluftzufuhr könne bei einem Brand auf bis zu 450 Kubikmeter gesteigert werden, damit freie Sicht bis auf zwei Meter Höhe garantiert werde. Das Gesamtsystem, das alle Gewerke und Anlagen steuert, kontrolliert und überwacht, müsse permanent verfügbar sein. Neben dem Tunnelleitsystem seien auch

die weiteren Systeme wie Datennetz, Servernetz oder elektrische Versorgung redundant aufgebaut. Die Tunnelleittechnik übernehme die Überwachung der korrekten Abwicklung der Notfallprozeduren mittels Zeitkontrolle, die die einzelnen Schritte verfolgt.

Verkehrsmanagement

Benjamin Schiereck, FLIR Systems, erläutert in PROTECTOR, Ausgabe 11-2016, S. 24/25, das **Verkehrsmanagement in Darmstadt**. Videosensoren eigneten sich ideal, um den Verkehrsfluss in Abhängigkeit vom Verkehrsaufkommen zu steuern. Außerdem biete die Videoerkennung gegenüber den Induktionsschleifen den großen Vorteil, dass keine umfangreichen Bauvorhaben mehr geplant und umgesetzt werden müssen. In bestimmten Stadtteilen könnten die Verkehrsbehörden mit den Videosensoren beispielsweise einen beginnenden Stau erkennen und den Verkehrsfluss durch längere Grünphasen dahingehend verbessern, dass sich der Stau schnell wieder auflöst. Um die Sicherheit der Schulkinder und anderen Verkehrsteilnehmer zu gewährleisten, habe die Stadt FLIR C-Walk-Sensoren installiert, die größere Personengruppen erkennen und die Grünphasen der Ampel entsprechend anpassen können.

Verschlüsselung

Patrick Beuth berichtet am 31. Oktober in zeit.de, zwei künstliche neuronale Netzwerke von Google hätten selbstständig gelernt, ihre Kommunikation kryptografisch abzusichern. Die Forscher hätten ihren Alice und Bob genannten **künstlichen neuronalen Netzwerken** eine Aufgabe gestellt: Alice sollte Bob eine Nachricht zukommen lassen, die nur Bob entziffern kann – nicht jedoch ein drittes Netzwerk namens Eve, das die Nachricht abfängt. Nach rund 10.000 Versuchen hätten Alice und Bob angefangen, Eves Entschlüsselungsversuchen entgegenzuarbeiten, und sie seien dabei schneller besser geworden als Eve. Nach rund 15.000 Versuchen hätten sie das Ziel erreicht. Sie hätten einen Verschlüsselungsalgorithmus erfunden, der es ihnen erlaubte, Botschaften auszutauschen, die Eve als passiver Mithörer entweder gar nicht oder nur noch durch Zufall entschlüsseln konnte. Wie diese Methode genau funktioniert, würden die Forscher nicht wissen.

Anlässlich des 10. Nationalen IT-Gipfels sei seit 17. November die Webseite Krypto-Charta (www.krypto-charta.de) online verfügbar. Diese biete für Bürgerinnen und Bürger, Unternehmen und Verwaltung nutzerfreundliche Tools zur Verschlüsselung der E-Mail-Kommunikation. In der **Charta zur Ende-zu-Ende-Verschlüsselung** seien die Rahmenbedingungen formuliert, die die bereits zahlreich vorhandenen Aktivitäten bündeln und fokussieren. So bekennen sich die Unterzeichner unter anderem dazu, nutzerfreundliche Angebote zu entwickeln und aktiv für Verschlüsselung von Kommunikation zu werben. Die Charta setze damit ein Ziel der Digitalen Agenda 2014–2017 der Bundesregierung um.

Videoüberwachung

Simon Pannarale, Wilkon Systems GmbH & Co. KG, stellt in Ausgabe 11-2016 der Zeitschrift PROTECTOR, S. 26/27, **mobilfunkgestützte Videoanlagen** im Praxiseinsatz vor. Sollen kleinere Filialen, abseits gelegene Lagerhallen oder Agrarbetriebe vollständig aus der Ferne videoüberwacht werden, scheitere dies oft an einem zu geringen Upstream des dortigen Internetanschlusses. Man helfe sich in der Praxis dadurch, dass für den Fernzugriff auf Livebilder ein zweiter, extrem komprimierter, Videostream genutzt wird. Der Grundgedanke einer intelligenten Lösung sei simpel. Die Aufzeichnung in bester Qualität erfolge in der

Filiale. Ergänzend erfolge im Headquarter eine zweite Aufzeichnung in extrem niedriger Qualität. Für eine „Rund-um-die-Uhr-Übertragung" von der Filiale ins Headquarter seien bei einer Bildauflösung von 320 mal 240 Pixeln und bei einem Bild pro Sekunde monatlich je Kamera nur circa 15 Gigabyte einzuplanen. Steht der Zeitpunkt eines Ereignisses fest, müssten in der Regel nur noch wenige Minuten hochauflösendes Videomaterial an das Headquarter übertragen werden, um es genauer zu analysieren und zu archivieren. Benötigt werde für die Anlage ein Outdoor LTE-Router. Im Headquarter werde darüber hinaus eine VPN-Firewall benötigt. Für die Auswahl der Kamera seien bei einer Mobilfunklösung neben der Überwachungsaufgabe weitere Kriterien zu berücksichtigen. Geeignet seien zum Beispiel Kameras mit sogenannter Zipstream-Technologie, die deutlich weniger Datenvolumen benötigen.

Dipl.-Ing. Christian Gieseler, eks Engel GmbH & Co. KG, befasst sich in Ausgabe 11-2016 der Zeitschrift PROTECTOR, S. 32/33, mit der **Ferndiagnose via Livestream**. Mittels Video-Kollaboration ließen sich Unternehmensprozesse noch effizienter gestalten, da das Know-how von Mitarbeitern an jedem Ort der Welt zusammengeführt werden könne. Das portable und plattformunabhängige S-Live-System ermögliche es, Expertenwissen in Echtzeit zusammenzuführen. Durch die Kombination aus Soft- und Hardware sowie dem reibungslosen Zusammenspiel aller Komponenten ließen sich Videos in HD-Qualität weltweit bereitstellen. Die Daten würden über die bestehende IT- und Mobilfunkinfrastruktur übertragen, und die parallele Nutzung verschiedener Übertragungswege sorge zusammen mit Datensplitting für größtmögliche Abhörsicherheit.

PROTECTOR enthält in der Ausgabe 11-2016, S. 34/35, eine **Marktübersicht** über 52 Systeme von 28 Anbietern zur **Kennzeichenerkennung**. Abgefragt wurden unter anderem Einsatzgebiete, Referenzanlagen, Systemumfang, Zulassungen, Systempreis, Fahrzeugtypen, Kennzeichentypen, Kennzeichenposition, Auswertungsmöglichkeiten, Einsatzbedingungen, Auswertesicherheit, unterstützte Betriebssysteme und Schnittstellen.

Jens Aperdannier, Tyco Integrated Fire & Security, stellt in Ausgabe 11-2016 der Zeitschrift PROTECTOR, S. 37, **intelligente Technik an öffentlichen Plätzen** vor. Laut dem ARD-Deutschlandtrend seien 82 Prozent für eine Ausweitung der Videoüberwachung öffentlicher Plätze. Für die Auswertung der anfallenden großen Datenmengen böten Technologieanbieter wie Tyco längst intelligente Videolösungen, zum Beispiel ein intuitives Exacq-Videomanagementsystem in Verbindung mit Videoanalysetools. Die Enhanced Video Technologie filtere potenzielle Sicherheitsbedrohungen aus einem oder mehreren Video-Streams und schlage bei verdächtigen Situationen automatisch Alarm. Auch geparkte Fahrzeuge, die Rettungswege blockieren, oder Falschfahrer detektiere das Videosystem.

Ganz neue Perspektiven bei Kameras von Tamron werden in der Ausgabe 11-2016 der Zeitschrift GIT, S. 46/47, dargestellt. Tamron zeige mit seinem neuen Advanced Small Size Camera Module Block MP1010M-VC, welches Potenzial der wachsende Markt „kleiner" Kameras biete. Die steigende Nachfrage nach kleinen Hochleistungs-Videokameras beweise, dass sich dieser Trend auch im Bereich mobiler Einheiten zur Verkehrsüberwachung fortsetze. Dank des Bildstabilisators, der intelligenten Defog-Funktion und der Rauschreduktion zeichne das MP1010M-VC Modul selbst unter schwierigen Bedingungen scharfe und detailreiche Bilder auf. Das Modul eigne sich auch für Einsätze an Drohnen, zur Baustellenkontrolle sowie zur Verbesserung der Sicherheit in öffentlichen Verkehrsmitteln. Kernelement des VC-Systems sei eine elektronisch gesteuerte Linsengruppe, die sich parallel zur Bildebene bewegt. Horizontale

und vertikale Bewegungen würden dabei von zwei Gyrosensoren erfasst und an einen Mikroprozessor weitergeleitet. Dieser berechne den Rotationswinkel und gebe entsprechende Steuerbefehle an die Antriebseinheit weiter, die wiederum das VC-Element entgegen der Vibrationsrichtung verschiebe. Dieser Vorgang wiederhole sich mit einer Frequenz von 4 kHz, also 4.000mal pro Sekunde. Eingegangen wird auch auf die Full-HD-Auflösung und 60p-Bildrate, auf den 58,2 Grad Weitwinkel mit 10x optischem Zoom, die Defog-Funktion und Privacy Zone Masking.

Sichere Speicherlösungen für Überwachungsdaten thematisiert GIT in der Ausgabe 11-2016, S. 50/51. Fast die Hälfte der weltweit generierten Daten stamme inzwischen aus Videoüberwachungssystemen. Ein Unternehmen, das sein bestehendes Videosystem erweitern, aufrüsten oder erneuern will, müsse die Datenspeicherung in den Vordergrund stellen und im ersten Schritt den richtigen Datenspeicher auswählen. Spezialisierte Surveillance-Festplatten böten hier leistungsstarke und zukunftsfähige Anwendungsmöglichkeiten. Für eine tiefergehende Analyse von Videoaufnahmen eigne sich insbesondere eine Kombination aus Surveillance-Festplatten und speziellen Festplatten für Geschäftsanwendungen, da letztere eine höhere Lesegeschwindigkeit böten. Dieser kombinierte Ansatz könne die Rentabilität des gesamten Systems deutlich verbessern, indem Aufnahme und Wiedergabe optimiert und Daten schneller verarbeitet werden.

Penta-Brid Videorekorder löst Kompatibilitätsprobleme bei der Videoaufzeichnung, berichtet GIT in der Ausgabe 11-2016, S. 53. Die gleichzeitige Aufzeichnung von IP-Videosignalen und Videoströmen aus den unterschiedlichen „Video über Koax-Technologien" erleichtere Dahua mit der Einführung des XVR-Videorekorders. Das Gerät sei mit den intelligenten Funktionen von IVS sowie Gesichtserkennung ausgestattet und erfasse und analysiere Tripwire-Ereignisse, das Eindringen und Verschwinden aus dem Bildmaterial. Außerdem erfüllten diese intelligenten Funktionen den hohen Effizienz- und Intelligenzbedarf von Applikationen.

Vorratsdatenspeicherung

Der Umsetzung der Vorratsdatenspeicherung in Deutschland stehe vorerst nichts mehr im Wege, zitiert der ASW-Newsletter vom 4. November golem.de. Der Anforderungskatalog der Bundesnetzagentur für die Provider sei auf europäischer Ebene gebilligt worden. Sowohl die EU-Kommission als auch die übrigen 27 Mitgliedsstaaten hätten innerhalb der dreimonatigen Stillhaltefrist keine Einwände erhoben oder Änderungen gefordert.

Wächterkontrollsystem

Online-Wächterkontrollsystem ist das Thema von Michael Kulig, Coredinate GmbH, in der Ausgabe 11-2016 von PROTECTOR, S. 68. Das seien Assistenzsysteme für eine Sicherheitsdienstleistung auf höchstem Niveau. Neben dem doch recht banalen Kontrollpunktscan zeigten diese Systeme den Arbeitsfortschritt beim Rundgang, alle Ansprechpartner für Notfälle, eine komplette Dienstanweisung, die Feststellungen der Kollegen aus den Schichten zuvor, eine Aufgabenüberwachung und die Möglichkeit, festgestellte Ereignisse zusammen mit einem Beweisbild direkt zu dokumentieren – alles in Echtzeit, ohne einen Datensammler dafür auslesen oder gar zu diesem Zweck anfahren zu müssen. Beide Seiten – der Mitarbeiter vor Ort wie der Vorgesetzte in der Einsatzzentrale – sähen den Arbeitsfortschritt in Echtzeit.

Wohnungseinbruch

GIT zeigt in der Ausgabe 11-2016, S. 38–40, wie Alarmanlagen die eigenen vier Wände vor Einbrüchen schützen. Funk-Alarmanlagen seien zudem flexibel und könnten jederzeit um zusätzliche Melder erweitert werden, was ideal für Bestandsbauten und bei Modernisierung sei. Gefahrenmeldeanlagen meldeten nicht nur Einbrüche, sondern informierten darüber hinaus über den kompletten Sicherheitszustand der Wohnung. Sie brauchten somit keine Angst mehr zu haben, dass der Gashahn offen steht, das Bügeleisen brennt oder der Waschmaschinen-Schlauch platzt. Das vernetzte Haus sei die Zukunft auch des Einbruchschutzes. Spezielle Apps erlaubten eine Fernsteuerung und -überwachung der Einbruchmelde- und Gefahrenwarnanlage und anderer Bestandteile der Haustechnik. Die vollständige Bedienung und Darstellung aller Betriebszustände der Alarmanlagenzentrale sei auch unterwegs möglich.

Impressum

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

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

Herausgeber:
Manfred Buhl, Vorsitzender der Geschäftsführung, Düsseldorf

Verantwortlicher Redakteur:
Bernd Weiler, Leiter Kommunikation und Marketing

Beratender Redakteur:
Reinhard Rupprecht, Bonn

focus.securitas.de

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

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

E-Mail: info@securitas.de