Focus on Security

Ausgabe 03, März 2016

SECURITAS

Inhalt

Anschläge

Nach einer Meldung des BKA vom 5. Februar versuchten Unbekannte am 1. Februar, mittels mehrerer mit Flüssigkeit gefüllter PET-Flaschen und Zündvorrichtungen Feuer an einem Kabelschacht an der **Bahnstrecke Berlin-Hannover** zu legen. Da der Brandsatz nicht zündete, veröffentlichten unbekannte Verfasser ein Selbstbezichtigungsschreiben auf der Internetseite „linksunten.indymedia.org" und informierten auch die Deutsche Bahn. Die Gleise wurden zeitweise gesperrt, wodurch der Bahnverkehr erheblich beeinträchtigt war. Wie im Selbstbezichtigungsschreiben formuliert, zielten die Täter mit der Aktion „auf die Festung Europa in ihrer wirtschaftlichen Funktionsfähigkeit." In derselben Wochenlage informiert das BKA über eine Aktionswoche der Umweltaktivisten im Rheinischen Braunkohlerevier. Unbekannte errichteten Blockaden durch Baumstämme und bewarfen Baustellen- und Einsatzfahrzeuge mit Steinen und Pyrotechnik. Am 25. Januar setzten Unbekannte eine Kompaktstation zur Stromversorgung in Brand und verursachten damit Sachschaden in Höhe von ca. 50.000 Euro. Bereits am 21. Januar hatten vermummte Personen RWE-Mitarbeiter und Sicherheitskräfte angegriffen und einen Stromverteiler der **Hambachbahn** beschädigt (Sachschaden ca. 100.000 Euro). Nach der Bewertung des BKA bleiben die Themen „Umweltschutz" und „Klima" für die linke Szene relevante Aktionsbereiche, in deren Zusammenhang regelmäßig Straftaten zum Nachteil von Firmen begangen werden, die für den Klimawandel verantwortlich gemacht werden.

Nach einer Meldung von migazin.de vom 16. Februar gab es im Jahr 2015 1.027 Übergriffe auf **Flüchtlingsunterkünfte**. Das habe die Bundesregierung mitgeteilt. Die meisten Anschläge und Übergriffe, insgesamt 219, habe Nordrhein-Westfallen gemeldet. Es folge Sachsen mit 109 Delikten, Niedersachsen mit 98 Attacken, Bayern mit 74 und Baden-Württemberg mit 70. Die mit Abstand am stärksten belastete Kommune sei Berlin mit 58 Attacken. Die Sicherheitsbehörden hätten 2015 nach vorläufigen Zahlen des BMI fast 14.000 rechtsextrem motivierte Straftaten registriert, darunter 921 Gewalttaten.

Arbeitsschutz

Mit den Herausforderungen der **Industrie 4.0** für den Arbeitsschutz befasst sich GIT-Sicherheit in der Ausgabe 1/2-2016, S. 100/101. Die vierte industrielle Revolution werde durch eine zunehmende Interaktion von virtuellen und realen Produktions- und Logistikprozessen auf der Basis sogenannter cyberphysischer Systeme charakterisiert sein. Die ganzheitliche Gestaltung der Schnittstellen Mensch/Maschine unter den Gesichtspunkten des Arbeitsschutzes sei die Hauptaufgabe einer wirksamen Prävention. Cyberphysische Systeme eröffneten eine Vielzahl von neuen Chancen für Sicherheit und Gesundheit der Beschäftigten in menschengerechten Arbeitssystemen, würden aber auch die Gefahr unkalkulierbarer Risiken bergen, wenn arbeitsschutzrelevante Aspekte zu spät berücksichtigt werden. Eine präventive und prospektive Arbeitssystemgestaltung erfordere daher auch eine stärkere Vernetzung der Fachleute aus Arbeitsschutz, Produktentwicklung, Produktions- und Arbeitsplanung und der IT.

GIT-Sicherheit skizziert in der Ausgabe 1/2-2016, S. 102/103, modernen **Arbeitsschutz für Schweißer**. Die TRGS 528 regele die konkreten Anforderungen an den Schweißarbeitsplatz. Immer mehr Schweißer setzten heute auf Masken mit Automatikschweißfilter. Die neueste Generation biete zuverlässigen Schutz vor UV- und IR-Strahlen. Es sei ratsam, vorhandene technische Lösungen mit einer persönlichen Atemschutzausrüstung wie zum Beispiel einer Schweißerschutzmaske mit passender Atemschutzmaske zu ergänzen.

Die meisten modernen Automatikschweißmasken böten integrierte Atemschutzsysteme.

Betrug

Das LKA Baden-Württemberg warnt am 20. Januar vor einer neuen Masche des sogenannten **Geschäftsführerbetrugs**, nachdem das Amt schon im September 2015 eine entsprechende Warnung vor Tätern veröffentlicht hatte, die Aufträge der Geschäftsführung vortäuschen, um mit gefälschten E-Mail-Absenderangaben und Vortäuschen eines bevorstehenden Firmenkaufs an Unternehmensgelder zu gelangen. Nach neueren Erkenntnissen geben sich die Kriminellen verstärkt als angebliche Kunden und Geschäftspartner aus und suchen den telefonischen Kontakt zu Unternehmen, um Informationen über interne Zuständigkeiten, Telefondurchwahlen und die persönliche E-Mail-Adresse der Zahlungsberechtigten zu erfahren. Besonders gefährdet seien die Geschäftsführung und die Buchhaltung. Gezielt würden Informationen aus sozialen Netzwerken und Karriereportalen genutzt. Ergänzend zur Warnmeldung vom September 2015 rät das LKA dazu, Mitarbeiter entsprechend zu sensibilisieren, Plausibilitätsprüfungen vor der Übermittlung sensibler Daten an Dritte durchzuführen, in sozialen Netzwerken und Karriereportalen restriktiv mit persönlichen Daten umzugehen und Standards zu entwickeln, welche die Verfahrensweise bei atypischen Zahlungsaufforderungen beschreiben.

Biometrie

Dr. Hubert Halbritter und Bianka Schnabel, Osram Opto Semiconductors GmbH, befassen sich in der Ausgabe 1/2-2016 der Zeitschrift PROTECTOR (S. 40/41) mit biometrischen Identifizierungsverfahren. Für geringe Fehlerraten sei eine gute Ausleuchtung der zu erfassenden Körperregion mit der passenden Wellenlänge essenziell. Aus diesem Grund müssten insbesondere für kleinformatige mobile Geräte entsprechend kompakte Emitter eingesetzt werden, die trotzdem genügend Helligkeit an die gewünschte Stelle übertragen. Dies verlange nach hohen optischen Leistungen, neuen Wellenlängen und innovativen Gehäusen, die die benötigte Abstrahlcharakteristik gewährleisten. Im Vergleich zur Gesichtserkennung würden **Irisscanner** als sehr zuverlässig gelten. Hier erfolge die Identifizierung über das Irismuster, das weder vom Alterungsprozess noch durch äußere Einflüsse wie Verletzungen verändert werde. Die Falschabweisungsrate liege mit weniger als einem Prozent weit unter der der Fingerabdruckscanner, und auch das Risiko der Falschakzeptanz sei mit einer Rate von 1:1.000.000 extrem gering. Um das Irismuster sicher identifizieren zu können, müsse der Kontrast der aufgenommenen Bilder stimmen. Dieser hänge stark von Augenfarbe und verwendetem Licht ab. Anstelle der Iris könne auch die Retina zur Identifizierung dienen. Bei einem **Retinascan** müsse die Person durch ein Okular des Scanners schauen, wobei das Auge mit infrarotem Licht durchleuchtet wird. Auf der Aufnahme erschienen dann die Blutgefäße aufgrund der stärkeren Absorptionsfähigkeit des Blute, dunkler. Mit derselben Methode arbeiteten auch **Venenscanner**, die ebenfalls Merkmale aus dem Körperinneren nutzen, die nicht aus einem Foto extrahiert werden können. Der Einsatz von Irisscannern bei Smartphones und Tablets zeichne sich als Trend für die nächste biometrische Lösung ab. Ihre Zuverlässigkeit und kompakte Form, die keine Mindestfläche für die Finger oder die Hand benötigt, erscheine für die Hersteller vielversprechend. Ein weiterer Vorteil sei der niedrige Energieverbrauch des Sensors.

Brandmeldesysteme

PROTECTOR gibt in der Ausgabe 1 / 2-2016 (S. 24/25) eine Marktübersicht über 66

Brandmeldesysteme von 30 Anbietern. Je Firma wurden 35 Kriterien abgefragt.

Brandschutz

Ein Merkblatt des bvfa informiert über den Einsatz von Sprinkleranlagen und ihre sichere Stromversorgung in **Alten- und Pflegeeinrichtungen**, meldet GIT-SICHERHEIT.de am 28. Januar. 15 Menschen seien 2015 in diesen Einrichtungen durch Brände zu Tode gekommen. Ein wichtiger Faktor sei die zuverlässige Stromversorgung der Sprinklerpumpen. Durch die sogenannte „Sprinklerschaltung" werde gewährleistet, dass die Stromzuführung der Sprinkleranlage auch dann aktiv bleibt, wenn der Strom im restlichen Gebäude ausgeschaltet wird oder eine Störung auftritt. Die ausschließliche Energieversorgung über die „Sprinklerschaltung" sei ausreichend, da das öffentliche Netz nachweislich eine sehr hohe Verfügbarkeit aufweise. Das Merkblatt, steht auf www.bvfa.de zum kostenlosen Download zur Verfügung.

PROTECTOR befasst sich in der Ausgabe 1/2-2016 (S. 16-18)mit dem Brandschutz in **Kraftwerken**. Er richtet sich grundsätzlich nach den Brandrisiken, die in einem Kraftwerk sehr unterschiedlich ausfallen könnten, je nachdem, ob es sich um eines zur Erzeugung von Strom aus Kohle, Solar, Wind- oder Kernenergie handelt. Häufig würden Wasserstoff und Öle im Bereich der Transformatoren als Betriebsstoffe genutzt. Hier bestehe aufgrund des Einsatzes von Ölen als Kühlmittel ein besonderes Brandpotenzial. Die meisten Ereignisse träten nicht im laufenden Betrieb, sondern während der Revision von Anlagen auf. In einer langzeitigen Vorplanung müssten alle baulichen, anlagentechnischen und organisatorischen Aspekte einbezogen werden. Während der Gesetzgeber bislang keine spezifischen Bauvorschriften für Kraftwerke herausgegeben habe, gebe es dafür diverse Richtlinien vom VdS oder dem VGB, dem europäischen technischen Fachverband für die Strom- und Wärmeerzeugung. Abhängig vom Kraftwerkstyp und -bereich kämen unterschiedliche Brandschutzlösungen zum Einsatz. Hierbei sei vor allem dem vorbeugenden Brandschutz besondere Bedeutung zuzumessen. Zu den aufeinander abzustimmenden Gewerken zählten etwa CO_2-Niederdruckanlagen für Schaltanlagen, Schaumlöschanlagen für Kohlesilos, Wassernebellöschanlagen für Generatoren und Kabelkanäle sowie Sprühwasserlöschanlagen für Kohlebandanlagen und Transformatoren. Sprühwasserlöschanlagen hätten gegenüber Sprinkleranlagen den Vorteil, dass sie sich im Brandfall selektiv zuschalten lassen.

Markus Meer, Securiton, gibt in Ausgabe 1/2-2016 der Zeitschrift PROTECTOR, S. 19, einen Ausblick auf **Neuerungen im anlagentechnischen Brandschutz**. Früher sei eine Störung eines Brandmelders oder ein Alarm via Relaiskontakt weitergegeben worden. Mit der neuen Funktion „Config over Line" könnten nun über eine bestehende Ringleitung durch sogenanntes Tunneling wesentlich mehr Informationen an die Brandmeldezentrale übertragen werden, auch Daten wie Rauchdichte und Temperaturprofile. Kunden erhielten volle Anzeige, Auswertung und Konfiguration direkt über die Brandmeldezentrale oder per Fernzugriff praktisch überall auf der Welt. Mit der intelligenten Systemintegration sei jetzt auch die Einmannrevision möglich. Der vollumfängliche Zugriff aus der Ferne sei vom Computer, Laptop, Tablet oder Smartphone aus möglich und auch ein großer Vorteil bei weitläufigen Industrieanlagen.

Sven Hackbarth und André Hugendick, Dorma Deutschland GmbH, skizzieren in der Ausgabe 1/2-2016 von PROTECTOR, S. 20/21, Lösungen, mit denen sich die Anforderungen an **Barrierefreiheit** und Brandschutz problemlos realisieren lassen. Die DIN 18040, Teil 1 für öffentliche Gebäude, Teil 2 für private Gebäude, beschreibe die Anforderungen insbesondere für Türen. Bei Türschließern der Serie TS 93

von Dorma würde seit jeher eine spezielle Easy-Open-Technologie eingesetzt. Sie ermögliche ein stark abfallendes Öffnungsmoment für eine leichte Türbegehung nach DIN 18040 und DIN SPEC 1104. Feststellanlagen und Freilauftürschließer sorgten für leichte Begehbarkeit. Drehflügeltürantriebe würden üblicherweise als zugelassene Feststellanlage an Feuer- und Rauchschutztüren eingesetzt. Die Drehflügeltürantriebe ED 100 und ED 250 würden die vom Nutzer aufgewendete Kraft erkennen und die Unterstützung entsprechend anpassen. Drehflügelantriebe ließen sich auch problemlos vernetzen, etwa in das digitale Türmanagement größerer Gebäude. Durch die Visualisierung von Türzuständen in Echtzeit ließen sich die Antriebe einfach und sicher überwachen und per Mausklick bedienen. Die Überwachung per PC erlaube die Ferndiagnose .

Norbert Schäfer, Siemens, befasst sich in Ausgabe 1/2-2016 der Zeitschrift PROTECTOR, S.22/23, mit dem Brandschutz im **Chemielabor**. Rund ein Drittel aller Brände in Deutschland sei auf Elektrizität als Brandursache zurückzuführen. Unter diesen Bränden würden wiederum knapp 30 Prozent durch Mängel in der Elektroinstallation verursacht. Fehlerstrom-Schutzeinrichtungen erfassten Fehlerströme und Fehlerlichtbögen gegen Erde. Serielle Fehlerlichtbögen könnten diese Schutzgeräte also nicht erkennen. Dagegen erkenne der von Siemens entwickelte Brandschutzschalter 5SM6 gefährliche Fehlerlichtbögen automatisch und zuverlässig. Im Detektionsfall schalte er den betroffenen Stromkreis sofort sicher ab. Er erfasse nicht nur Strom und Fehlerspannung, sondern messe auch kontinuierlich das Hochfrequenzrauschen hinsichtlich Intensität, Dauer und den dazwischen liegenden Lücken.

Der Sicherheits-Berater befasst sich in der Ausgabe 4-2016, S. 47/48, mit dem Brandschutz in **Rechenzentren**. Die Abschaltung der Stromspannung von IT-Hardware im Rechenzentrum werde bei einer Löschung durch eine Löschgasanlage in vielen Richtlinien, Normen und Merkblättern verlangt (VdS 2304, VdS 2380, DIN 50600). Der Grund dafür liege darin, dass der Gefahr einer Rückzündung oder der Weiterentwicklung eines Brandes vorgebeugt werden solle. Als Alternativlösung biete sich an, intelligente Power-Managementkonzepte einzusetzen. Denn diese ermöglichten, nur die Komponente, an der das Schadenereignis erkannt wurde, gezielt abzuschalten. Dabei könnten entweder einzelne Racks oder ganze Rackreihen gezielt abgeschaltet werden.

Securiton gab am 16. Februar bekannt, dass neben dem Ansaugrauchmelder SecuriRAS ASD 535 für das Überwachen größerer Flächen jetzt eine Version SecuriRAS ASD 532 für kleinere Flächen (Ansauglänge bis zu 120 Meter) zur Verfügung stehe.

Cloud Computing

In der Februar-Ausgabe des Behörden Spiegel nimmt Hans-Georg Göhring, Direktor des neuen **Informationstechnikzentrums Bund** (ITZBund) im Interview Stellung zu den Aufgaben der neuen Behörde mit rund 2.400 Beschäftigten. In der Behörde sind das bisherige ZIVIT sowie die IT-Dienstleister BIT und DLZ-IT integriert. Der größte Standort ist derzeit Bonn mit 500 Mitarbeitern. Ziel seien drei Produktionsrechenzentren in Berlin, Frankfurt/Wiesbaden und Köln/Bonn. Sowohl für „Infrastructure as a service" wie „Software as a service" und „Platform as a service" werde ITZBund entsprechend den Anforderungen der Nutzer Cloud-Dienste zur Verfügung stellen. Der Aufbau einer Trusted Private Cloud stehe derzeit im Vordergrund.

90 Prozent aller CIOs und IT-Entscheider könnten sich Cloud-Services für ihre IT-Landschaften vorstellen, schreibt Martin Schindler auf silicon.de am 15. Februar. Doch es gebe erhebliche Hemmnisse bei der Einführung

dieser neuen Technologie. In einer Umfrage des Partners Fritz & Macziol unter 2.200 CIOs zeige sich, dass 90 Prozent der Entscheider gerne Infrastructur as a Service (IaaS), Patform as a Service (PaaS) oder Software as a Service (SaaS) einsetzen würden. 75 Prozent der Unternehmen mieden derzeit noch Public Cloud-Services, wie eine Studie von KPMG zeige. Bestehende Anwender bauten vor allem auf Saas und IaaS aus dem Netz. Hybride Architekturen, die Services aus der Public Cloud mit der Private Cloud oder InPremise-Infrastrukturen verbinden, würden noch als Zukunftsmodell gelten. Die mangelnde interne, auch emotionale Unterstützung von IT-Projekten sei der wichtigste Grund, warum nach Angaben von Cloud-Projektmanagern 50 bis 60 Prozent der IT-Projekte ihr Ziel verfehlten. Um Anwendern die noch verhältnismäßig neue Disziplin nahezubringen, versuche die AG EuroCloud des eco-Verbandes mit dem Ende 2015 erschienenen **„Leitfaden Cloud-Projektmanagement"** gegenzusteuern. Die Praxiserfahrung von Fritz & Macziol zeige, dass extern betriebene Cloud-Angebote IT-Infrastruktur- und Plattformfragen in der Regel günstiger lösen, wogegen Applikationen bei den Unternehmen selbst besser aufgehoben seien. Für CIOs entstehe bei der Einführung von Cloud-Diensten auch das Dilemma, dass gegen die Einführung zwar hohe Ressentiments bestehen, dass aber bei Bedarf die Fachabteilungen schnell selbst Public-Cloud-Dienste nutzen, ohne die Kontrolle der IT-Abteilung.

Datenschutz

Unternehmen kritisierten eine breite **Streuung von Steuerdaten**, berichtet die FAZ am 16. Februar. Sie fürchteten sich vor dem wachsenden Datenaustausch zwischen Steuerbehörden verschiedener Länder. So habe Wolfgang Salzberger, „Steuerchef" des Technologiekonzerns Linde betont, sein Unternehmen habe schon erlebt, dass Geschäftspartner in Verhandlungen plötzlich solche Kenntnisse gehabt hätten. Das BFM betone, eine bei der OECD eingerichtete Institution überprüfe vor Ort regelmäßig, dass Steuerbehörden Vertraulichkeit wahren. Zudem müsse kein Unternehmen Geschäftsgeheimnisse preisgeben.

Die FAZ berichtet am 1. März, dass die EU-Kommission die Details des neuen **„EU US Privacy Shield"** vorgelegt hat, auf dessen Grundlage Konzerne und auch kleine Unternehmen künftig wieder persönliche Daten von Europäern in den USA speichern können sollten – inklusive konkreter Datenschutzzusagen der US-Regierung. Die sichere zu, dass ihre Geheimdienste die Daten von EU-Bürgern nicht mehr massenhaft ausspähen. Und sie habe inzwischen gesetzlich sichergestellt, dass EU-Bürger vor amerikanischen Gerichten gegen bestimmte Datenschutzverstöße vorgehen können. Abschließend werde die EU-Kommission entscheiden, wenn die EU-Datenschutzbehörden die Texte geprüft und die EU-Staaten zugestimmt haben.

Drohnen

Der SicherheitsBerater direkt befasst sich in der Ausgabe 2-2016 mit der **Zulässigkeit des Einsatzes** von Drohnen. In welchen Bereichen sie nicht fliegen dürfen, sei von Bundesland zu Bundesland unterschiedlich geregelt. Zu Flughäfen müsse ein Mindestabstand von 1,5 km eingehalten werden. Der Überflug von Privatgrundstücken könne einen Eingriff in die Privatsphäre darstellen (Urteil AG Potsdam vom 16. April 2015). Die Flughöhe könne je nach Bundesland auf 30 bis 100 Meter beschränkt sein. Bei Aufnahmen von Bauwerken seien eventuelle Urheberrechte zu beachten. Die Aufnahme militärischer Einrichtungen sei nach § 109 g StGB strafbar. Fotos, mit denen eine Person identifiziert werden kann, dürften nur mit Zustimmung des Betroffenen veröffentlicht

werden, soweit es sich nicht um Aufnahmen von größeren Veranstaltungen handele.

GIT-SICHERHEIT.de berichtet am 10. Februar, Forscher der Uni Zürich, der Uni der italienischen Schweiz sowie der Fachhochschule Südschweiz hätten für Drohnen eine Software entwickelt, die **Waldwege erkennen** und ihnen selbstständig folgen könne. Mit den neuen Drohnen könnten in Wäldern und Berggebieten vermisste Personen schnell gefunden und gerettet werden. Die Drohne nehme ihre Umgebung mit Hilfe von zwei kleinen Kamera wahr, ähnlich jener in Smartphones. Anstelle von komplizierten und teuren Sensoren mache die Drohne von künstlicher Intelligenz Gebrauch, um vom Menschen gemachte Wege in den Kamerabildern zu erkennen. Die Forscher lösten das Problem mit Hilfe eines sogenannten tiefen neuronalen Netzwerks. Dieser Computer-Algorithmus lerne anhand von vielen Übungsbeispielen komplexe Aufgaben zu lösen, ähnlich wie das menschliche Gehirn aus Erfahrung lernt. Das neuronale Netzwerk habe in 85 Prozent aller Fälle die korrekte Richtung des Weges gefunden. Menschen hätten bei der identischen Fragestellung in 82 Prozent aller Fälle richtig gelegen. Nachdem die Drohne gelernt habe, Waldwegen zu folgen, müsste ihr beigebracht werden, Menschen zu erkennen.

Endgerätesicherheit

Empfehlenswerte Security-Apps für Android-Smartphones benennt TECCHANNEL.de.de am 2. Februar. Malware, Diebstahl und unbefugter Zugriff seien ernsthafte Bedrohungen. Der Google-Playmarket biete jedoch eine Vielzahl an Sicherheits-Apps für Smartphones. Von so gut wie jedem Antivirensoftware-Hersteller gebe es mittlerweile eine Android-Lösung. Regelmäßige Tests gebe es unter anderem bei AV-Test und der Stiftung Warentest. Besonders empfehlenswert seien die kostenlosen Security-Suiten **Avira Mobile Security und Norton Mobile Security**. Beide versprächen den Schutz vor Malware auf dem Smartphone. Beide Programme besäßen jedoch Funktionen, die über die eines bloßen Malware-Scanners hinausgehen. So könnten sie eingehende Telefonanrufe sowie SMS von unliebsamen Kontakten filtern. Mit einigen Programmen aus dem Google-Playmarket ließen sich bestimmte Smartphone-Bereiche durch einen PIN-Code schützen. Eine empfehlenswerte App sei hier Perfect App Lock. Sie versehe einzelne Programme mit einem PIN-Schutz oder einem Gesten-Schutz. Für die Smartphone-Sicherung in regelmäßigen Abständen, um einen vollständigen Verlust der Daten zu verhindern, halte der Markt viele Anwendungen bereit. Eine Firewall gehöre auf dem Desktop-PC quasi zur Grundausstattung. DroidWall biete eine vergleichbare Funktionalität für Android-Smartphones. Es erfordere allerdings einen Root-Zugriff auf das Smartphone. Das sei bei vielen Geräten ein Garantieproblem.

Geheimnisschutz

Rechtsanwältin Sandra Sophia Redeker, Noerr LLP, nimmt im SicherheitsBerater direkt, Ausgabe 2-2016, Stellung zur EU-Richtlinie zum Geheimnisschutz. Sie weist darauf hin, dass die Richtlinie den Begriff des Geschäftsgeheimnisses so definiert, dass als Geschäftsgeheimnis von Gerichten künftig nur noch das Know-how betrachtet wird, zu dessen Schutz sogenannte „angemessene Geheimhaltungsmaßnahmen" getroffen wurden. Dies bringe eine Umkehrung der Beweislast. Bei Beurteilung der Angemessenheit müssten nicht nur tatsächliche Zugangssicherungen, sondern auch IT-Sicherungsmaßnahmen und rechtlich wirksame Verträge zum Schutz der Vertraulichkeit bewertet werden.

Geldwäsche

EU geht gegen Finanzierung des Terrors vor, titelt die FAZ am 3. Februar. Bisher könnten Kriminelle wie Terroristen weitgehend unkontrolliert reale Währungen gegen digitale Währungen wie Bitcoins eintauschen. Das mache sie attraktiv für Geldwäsche und Terrorfinanzierung. Die EU-Kommission wolle die Anbieter von Bitcoins und anderen Internet-Währungen deshalb verpflichten, die Quelle des Geldes zu überprüfen. Anfällig für Missbrauch durch Kriminelle und Terroristen sind nach Ansicht der EU weiterhin anonyme Prepaid-Karten, bei denen der Nutzer eine bestimmte Summe einzahlt, über die er dann ohne Angabe von Namen verfügen kann. Die Kommission wolle die anonyme Nutzung von Prepaid-Karten daher einschränkten. Ausweiten wolle die Kommission die Kontrollen für die Einfuhr von Bargeld in die EU. Schon heute müssten Einreisende Bargeldbeträge ab 10.000 Euro beim Zoll angeben. Künftig sollen die Zollbehörden auch Zugriff auf geringere Summen haben, wenn es einen klaren Verdacht auf Terrorfinanzierung gibt. Außerdem solle auch die Einfuhr wertvoller Metalle unter die Regelung fallen.

IT-Sicherheit

Die Deutsche Telekom wolle ihre Geschäfte rund um die Cybersicherheit in einer neuen Unternehmenseinheit bündeln, in der sie mehr als 1.000 Sicherheitsfachleute aus allen Konzernbereichen zusammenzieht, meldet die FAZ am 3. Februar. In der Entwicklung seien unter anderem spezielle Lösungen für Mittelständler, eine App für den Schutz des Smartphones und bessere Verschlüsselungstechnik für E-Mails.

In der Fachzeitschrift PROTECTOR, Ausgabe 1/2-2016, S. 44, zeigt der Buchautor Joachim Jakobs, dass sich KMU mit der **VdS-IT-Sicherheitsrichtlinie 3473** angemessen vor Cybergefahren schützen können. Der „Quick-Check für Cybersecurity" enthalte 39 sicherheitsrelevante Aussagen. Beim „Quick Audit" prüfe ein VdS-Vertreter vor Ort, ob die Selbsteinschätzung den Tatsachen entspricht. Die Richtlinie verlange zunächst vom „Topmanagement", einen Informationssicherheitsbeauftragten (ISB) zu bestimmen. Zudem verlange die Richtlinie, ein Informationssicherheitsteam (IST) zu bestimmen, das unter anderem aus dem ISB, dem Topmanagement, dem IT-Verantwortlichen, einem Mitarbeiter der Personalabteilung und dem Datenschutzbeauftragten bestehen soll. Zusammen mit dem IST erstelle der ISB eine Informationssicherheitsleitlinie, in der Ziele und der Stellenwert der Informationssicherheit für das Unternehmen definiert würden. Besonders wichtig sei das Identifizieren kritischer IT-Ressourcen. Diese Ressourcen müsse der ISB ermitteln, jährlich prüfen und bei Bedarf anpassen. Zur systematischen Strukturierung und Absicherung der IT-Systeme müsse eine Inventarisierung vorhanden sein, in der alle IT-Systeme des Unternehmens verzeichnet sind.

Mit intelligenten Informationsnetzen können Energieerzeugung und -verbrauch effizient verknüpft und ausbalanciert werden. Wichtige Elemente eines solchen Netzes sind intelligente Messsysteme (**„Smart Metering Systems").** Wie das BSI am 11. Februar mitteilt, entwickelt es im Auftrag des BMWi Anforderungen an vertrauenswürdige Produktkomponenten (Smart Meter Gateway mit integriertem Sicherheitsmodul), deren sicheren IT-Betrieb (Administration) und an die vertrauenswürdige Kommunikationsinfrastruktur (Smart Metering Public Key Infrastructure). Die Einhaltung der Vorgaben wird im Rahmen eines Zertifizierungsverfahrens durch das BSI überprüft. Das BSI informiert in einer Broschüre über Smart Meter Gateway, das Schutzprofil für das Sicherheitsmodul, kryptographische Vorgaben, über Smart Metering PKI, Administration und Betrieb, Schutzprofile sowie technische Richtlinien

nach § 22 Abs. 2 Satz 1 Messstellenbetriebsgesetz.

Mit Microsofts neuem **Betriebssystem Windows 10** hole man sich die Schnüffler auf den Rechner, schreibt die FAZ am 16. Februar. Professor Pohl habe untersucht, welche Nutzerdaten an Microsoft-Server geschickt werden. Die Sammlung reiche vom Namen und den Kontaktdaten über demographische Daten zu den Inhalten von Dokumenten, Fotos, Musik oder Videos. Ganz unverblümt spreche Microsoft in seinen Datenweitergaberichtlinien davon, dass Daten mit Geschäftspartnern, mit Tochterunternehmen und mit „Verkäufern, die für uns arbeiten", geteilt würden. Man könne das Ausspähen abschalten, lasse Microsoft wissen. Nutzer, die Privatsphäre wünschen, müssten jedoch selbst aktiv werden. Weil sich Windows 10 fortwährend aktualisiere, könne man sich nicht darauf verlassen, dass einmal getätigte Einstellungen dauerhaft Bestand haben. Es könne klug sein, die Synchronisierung mit verschiedenen eigenen Geräten ebenso zu unterbinden wie den permanenten Zugriff des Betriebssystems auf das betreffende Microsoft-Konto. Man mache genau das, was Microsoft nicht will, und melde sich bei Windows 10 nicht mit seinem Microsoft-Konto an, sondern wähle während der Einrichtung ein lokales Konto. Was weitere Datenschutz-Einstellungen betrifft, komme man nicht umhin, über das Startmenü und die Einstellungen einen Eintrag nach dem anderen zu prüfen. Einige Optionen seien in Windows 10 Home und Pro gar nicht abwählbar, etwa die automatisierte Übertragung von Diagnose- und Nutzerdaten. Hier solle man „Einfach" wählen, um die Schnüffelei zu minimieren.

Cybersecurity bezeichnet der Behörden Spiegel in der Februar-Ausgabe als den „Brandschutz des 21. Jahrhunderts". Obwohl das Bewusstsein für die Gefahren durch Cyberkriminalität in Deutschland wachse, schützten besonders Firmen ihre IT-Systeme häufig nur unzureichend. Die Anwendung der bestehenden ISO 27000er-Reihe und der BSI-Grundschutzkataloge seien in der Umsetzung besonders für KMU zu mächtig und komplex. Auf die Sicherheitslücke habe VdS Schadenverhütung mit der Richtlinie „VdS-zertifizierte Cybersecurity" (VdS 3473) reagiert. Die Richtlinie basiere auf den anerkannten Standards ISO 27001/2 und BSI-Grundschutz. Hinter der branchenneutralen Richtlinie, die für KMU direkt anwendbar sei, verberge sich ein Verfahren, mit dem der Informationssicherheitsstatus eines Unternehmens auditiert und zertifiziert werden kann. Mit ca. 20 Prozent des Aufwandes im Vergleich zu ISO 27001 könnten Unternehmen aus der Richtlinie Maßnahmen und Prozesse ableiten, wie sie im IT-Bereich ein angemessenes Schutzniveau erreichen. Mit dem VdS Schick-Check – einem kostenlosen Webtool, das im Internet unter www.vds-quick-check.de zur Verfügung steht – könnten Einrichtungen sich ein erstes Bild über den Status ihrer Cybersecurity verschaffen. Die Ergebnisse könnten anschließend von VdS in einem sogenannten Quick-Audit vor Ort verifiziert werden.

Viele Unternehmen hätten das Problem, dass sie Security-Komponenten von mehreren Anbietern verwenden und diese jeweils manuell ausgewertet werden müssten. Darauf weist der Behörden Spiegel in seiner Februar-Ausgabe hin. Hier könne ein **SIEM-System** Abhilfe schaffen, das sich aus zwei Faktoren zusammensetze: „Security Event Management" (SEM) und „Security Information Management" (SIM). Es könne Bedrohungen in Echtzeit erfassen und analysieren. Maßnahmen, die unter SIM zusammengefasst werden, bezögen sich auf die zentrale Sammlung, Übertragung, Speicherung, Analyse und Weiterleitung von Log-Daten aus Netzwerk-Komponenten. Nur wenige Unternehmen leisteten sich ein SIEM-System, da es mit einem hohen Kostenaufwand verbunden sei. Das BMBF unterstütze seit 2012 ein Projekt der Universität Hannover und der DECOIT GmbH, das sich zum Ziel gesetzt habe, ein System zu entwickeln, mit dem auch KMUs ihre IT-Systeme umfassend überwachen

können. Das Projekt nenne sich **SIMU** und stehe für „SIEM für Klein- und Mittelständische Unternehmen". Mit dem abgeschlossenen Projekt sei eine leichte Integrierbarkeit in IT-Infrastrukturen von KMUs geschaffen worden. Die Nachweisbarkeit von sicherheitsrelevanten Ereignissen im Netz sei leichter, der nötige Aufwand für Konfiguration, Betrieb und Wartung sei verringert worden. Es sei eine Skalierbarkeit für unterschiedlichste Szenarien hergestellt worden.

Die wachsenden Listen von Schwachstellen in Industrial Control Systems (ICS) werde in wenigen Jahren das wichtigste Problem der Sicherheitspolitiker, prognostiziert nach einer Meldung von heise.de vom 15. Februar der Sicherheitsexperte und IZ Harvest Berater Richard Stiennon.

Als Sicherheit für **mobile Arbeitsplätze** empfiehlt der Sicherheits-Berater in Ausgabe 4-2016: Verinnerlichung der Sicherheitsrichtlinien, Minimierung der Risiken von Datenpannen, Aktualität von Zugriffsrechten, Multifaktorauthentifizierung, Verschlüsselung der Geräte und Vorbereitung für notwendige Sperrung und Löschung (S. 50/51).

Im Streit mit dem FBI um eine **iPhone-Entsperrung** habe Apple die US-Regierung aufgefordert, die Entsperrungsanordnung zurückzuziehen, meldet heise.de am 22. Februar. Apple poche stattdessen auf eine politische Diskussion. Eine Expertenkommission solle sich mit der Verschlüsselungsproblematik für Strafverfolgungsbehörden im Kontext nationaler Sicherheit und Datenschutz auseinandersetzen. Ein Gericht hatte angeordnet, dass Apple dem FBI beim Entsperren eines iPhones des toten Attentäters helfen muss, der zusammen mit seiner Frau 14 Menschen im kalifornischen San Bernardino tötete.

Viele **kabellose „Mäuse"** und Tastaturen, die nicht mit Bluetooth operieren, lassen sich nach einem Bericht von heise.de vom 24. Februar aus bis zu hundert Meter Entfernung kapern – mit Hardware, die weniger als 13 Euro koste. Ein Hacker könne so die Kontrolle über die Eingabegeräte übernehmen und agieren, als wenn er selbst vor dem Rechner säße. Viele der betroffenen Geräte könnten nicht mit Updates versorgt werden, da die Sicherheitslücke fest in der Hardware verdrahtet sei. Betroffen von dem als „MouseJack" bezeichneten Angriff seien Geräte von Dell, HP, Lenovo. Logitech und Microsoft. Schutz gegen solche Angriffe böten Geräte, die sich mit Bluetooth verbinden.

IuK-Kriminalität

In einem Arbeitspapier (Version 3.0 vom 22. Januar) informiert das BSI (certbund) über Möglichkeiten der Ersten Hilfe bei einem **Advanced Persistant Threat (APT)-Angriff**, also einem zielgerichteten Cyberangriff auf sehr stark eingegrenzte Systeme und Netzwerke. In einem ersten Teil werden generelle Verhaltensregeln für das Incident Management vorgestellt: Ruhig bleiben und geplant handeln/Auffassung der Vorfallsbewältigung als Projekt/Verständnis des APT-Angriffs als Teil einer Kampagne/Krisenkommunikation über getrennte Netze/externe Unterstützung durch BSI, LfV, Polizei und Unternehmen mit Schwerpunkt Computerforensik. In einem zweiten Teil werden technische Maßnahmen vorgestellt, mit denen man das Ausmaß des Angriffs eingrenzen kann: Forensische Beweissicherung/Antivirus Programme/Umgang mit Logdaten/Netzwerkverkehr-Analyse/ Erfassung von Verkehrs- und Inhaltsdaten/ Art des Loggens/Beginn der Analyse/Bereinigung. Das Arbeitspapier solle helfen, keine Fehler in der Anfangsphase zu begehen, die später dazu führen, dass der Angriff nicht aufgeklärt oder bereinigt werden kann.

heise.de meldet am 1. Februar, dass Kriminelle derzeit gehäuft E-Mails mit Schadcode im Anhang über **gefälschte Absenderadressen von Netzwerk-Kopierern** versenden. Mitarbeiter

von Firmen sollten aktuell den Absender von E-Mails mit Dateianhang besonders intensiv prüfen weil Trojaner-Mails mit der Absenderadresse kopierer@domain.de im Umlauf seien. Domain.de werde dabei von der Adresse der Webseite des jeweiligen Unternehmens ersetzt. Wer eine derartige E-Mail empfängt, sollte sie umgehend löschen.

Zum Safer Internet Day am 9. Februar informierte das BSI am 5. Februar über Risiken durch **Ransomware**. Auf Rechner eingeschleust wird solche Ransomware üblicherweise durch schädliche Dateianhänge von E-Mails, welche zum Beispiel als vermeintliche Rechnung getarnt verwendet werden, oder mittels Drive by Exploits. Bei Firmen können wichtige Geschäfts- oder Personaldaten sowie ganze Netzlaufwerke von ungewollter Verschlüsselung betroffen sein und hohe materielle Verluste zur Folge haben. Das BSI rät davon ab, auf Lösegeldforderungen einzugehen, da die Dateien oder Programme auch nach Bezahlen der geforderten Geldsumme in vielen Fällen nicht entschlüsselt werden. Stattdessen sollten Betroffene den Bildschirm mitsamt der Erpressungsnachricht fotografieren und Anzeige erstatten. Vor dem Angriff manuell oder mithilfe einer Backup-Software erstellte Sicherungskopien sind meist die einzige Möglichkeit, die Dateien wiederherzustellen.

Ein **Remote-Trojaner** attackiert mehr als 400.000 Nutzer unter Unternehmern, meldet silicon.de am 9. Februar. **Adwind** greife über eine Malware as a Service-Plattform auf Rechner zu. Der Schädling soll noch immer aktiv sein. Die Sicherheitsforscher von Kapersky Lab würden jedoch darauf hinweisen, dass Adwind hauptsächlich bei nicht zielgerichteten Angriffen zum Einsatz kommt und eher im Rahmen von Massen-Spamkampagnen genutzt werde. Fast die Hälfte der festgestellten Angriffe seit August 2015 konzentrierten sich auf zehn konkrete Länder, darunter auch Deutschland. Öffnet ein potenzielles Opfer die an die Phishing-Mail angehängte JAR-Datei, installiere sich Adwind selbstständig und versuche eine Verbindung zu einem Command-and-Control-Server herzustellen. Die Malware könne nicht nur heimlich zusätzliche Schadsoftware über ihre Backdoor-Funktion nachladen und ausführen, sondern umfasse auch selbst ein großes Funktionsspektrum. Das beinhalte neben dem Sammeln allgemeiner System- und Nutzerinformationen unter anderem das Mitlesen von Tastaturanschlägen, den Diebstahl von im Browser-Cache gespeicherten Passwörtern sowie das Abgreifen von Daten aus Webformularen.

Ecrm.logrhythm.com informiert am 16. Februar über ein Whitepaper „**Der APT-Lebenszyklus und sein Log Trail**". Advanced Persistent Threats (APTs) stellten ein zunehmendes Problem in der IT-Sicherheitsbranche dar. Sie unterschieden sich von anderen Hackerangriffen, da sie ein bestimmtes Ziel einer Organisation hätten – und das seien meist wertvolle Geschäftsdaten. Wenn Unternehmen eine tief gehende Sicherheitsstrategie mit umfassender, automatisierter und kontinuierlicher Überwachung sowie fortschrittlichen Sicherheitsanalysen kombinierten, könnten Anzeichen eines APTs früher und mit höherer Genauigkeit erkannt und der Schaden eines erfolgreichen Angriffs erheblich vermindert werden.

Hacker erbeuten Patientenakten, titelt die FAZ am 25. Februar. Nicht Kreditkarten, sondern digital erfasste Patientenakten seien derzeit das begehrteste Ziel von Computerhackern. 2015 seien rund 100 Mio. solcher Datenpakete auf den internationalen Schwarzmarkt gekommen. Für den Datensatz eines Patienten würden bis zu 200 Dollar gezahlt. Mit dem Weiterverkauf der Daten einer Geld- oder Kreditkarte lasse sich nicht mehr halb so viel verdienen. Eine Patientenkarte speicherte einzigartige vertrauliche und persönliche Informationen. Mit ihnen könnten Cyberkriminelle dann weitere Straftaten wie Identitätsdiebstahl, Erpressung oder digitales Räubertum verüben.

Mehrere **Krankenhäuser in NRW** seien Opfer einer Schadsoftware geworden, die über E-Mails in die Kliniken gelangt sei, meldet die WirtschaftsWoche am 19. Februar. Der folgende Notstopp der Rechner, der tagelange Ausfall elektronischer Patientenakten mache die Verletzlichkeit digitaler Infrastrukturen im Medizinsektor schlagartig klar. Leider finde sich im Entwurf der Ausführungsverordnung zum IT-Sicherheitsgesetz zum Gesundheitswesen kein Wort.

Kaspersky warnt nach einer Meldung von heise.de vom 23. Februar vor einem **Banking-Trojaner** für Android, der aktuell eine große Gefahr für deutsche Anwender darstelle. Der Trojaner namens Acecard sei seit 2014 in mehr als zehn Varianten des Schadcodes aufgetreten. Diese tarnten sich als legitime Apps und gelangten so unter anderem in den Google Play Store. Auf dem Handy des Opfers angekommen, überlagere der Trojaner dann Online-Banking- und Messaging-Apps wie WhatsApp und greife Passwörter und TANs ab. Von Mai bis Dezember 2015 seien über 6.000 Kunden über den Trojaner angegriffen worden. Da der Schadcode viele legitime Apps überlagere und sich als diese ausgeben könne, bedeute er „eine der größten Gefahren", die Kaspersky derzeit kenne. Das Unternehmen empfiehlt Android-Nutzern, keine verdächtig aussehenden Apps aus dem Play Store oder anderen Quellen herunterzuladen. Oft tarne sich der Trojaner als Spiel, Porno-App oder als Flash Player.

heise.de warnt am 24. Februar vor dem **Krypto-Trojaner Locky**, der sich als Fax tarne. Online-Ganoven würden E-Mails verschicken, die vorgeben dass der Empfänger ein Fax erhalten hat. Eine Mail stamme vermeintlich von dem VoIP-Provider Sipgate. Die Erpresser haben als Vorlage offenbar eine legitime Benachrichtigungs-Mail des Anbieters im HTML-Format missbraucht. Ihr Betreff laute „Neues Fax von 034205-99***". Ein weiterer E-Mail-Betreff laute „Scanned image". Im Text heiße es „Image data in PDF format has been attached to this E-Mail". Die Mail sei simpel, aber vermutlich effektiv: Einige Multifunktionsgeräte und Kopierer mit Mail-Funktion verschickten durchaus ähnlich formulierte Nachrichten. Bei der Absenderadresse werde in diesem Fall die Domain der Mail-Adresse genutzt, an welche die Mail geschickt wurde. Als Absendername sei „admin" angegeben. Im Anhang der Mail befinde sich ein ZIP-Archiv, das eine Skript-Datei mit der Endung .js enthalte.

Nach einer Meldung von heise.de vom 25. Februar liegt Heise Security der Quellcode einer noch nicht sonderlich weit verbreiteten **Ransomware** vor, die das Open-Source-Verschlüsselungsprogramm Gnu Privacy Guard missbrauche. GPG gelte als hochsicheres Verschlüsselungs-Tool, an dem sich selbst die NSA die Zähne ausbeißen würde. Der Erpressungs-Trojaner werde derzeit vor allem via Mail verbreitet und befalle Windows-Systeme. Die Erpresser würden nicht gleich Lösegeld-Forderungen stellen, sondern Hilfe durch „Experten" anbieten. Letztlich wollten sie dann aber doch für die Entschlüsselung der gekaperten Daten Geld in Form von nicht zu ihnen verfolgbaren Bitcoins.

Kritische Infrastrukturen

GIT-SICHERHEIT.de weist am 24. Februar darauf hin, dass das BMI den Referenten-Entwurf einer „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz" veröffentlicht hat. Mit der **„KRITIS"-Verordnung** werde § 10 des BSI-Gesetzes in einem ersten Schritt umgesetzt. Für die Bestimmung Kritischer Infrastrukturen in den Sektoren Energie, Wasser, Informationstechnik und Telekommunikation sowie Ernährung würden relevante Anlagekategorien definiert und mit Schwellenwerten, korrespondierend mit dem jeweiligen Versorgungsgrad, versehen. TeleTrusT habe dazu angemerkt: Die Zugrundelegung der 500.000-Regel für

die Schwellenwerte werde als kritisch betrachtet. Die Regel basiere auf der Annahme, dass Ausfälle, bei denen weniger Haushalte betroffen sind, technisch und organisatorisch aufgefangen werden können. Es werde angeregt, die Schwellenwerte um einen geeigneten Sicherheitspuffer zu ergänzen. Der Benennung absoluter Zahlen für Schwellenwerte lasse eine qualitative Berücksichtigung möglicher „Domino-Effekte" außer Acht. Wie ein europaweiter Stromausfall von 2006 gezeigt habe, könne durch Abschalten einer einzigen, eher weniger wichtigen Leitung das Gesamtsystem massiv beeinträchtigt sein. Das für die Anlagenkategorie „Standortkopplung" zugrunde gelegte Datenvolumen auf Basis des wichtigsten, und – gemessen am Datendurchsatz – weltweit größten Internetknotenpunkts (DE-CIX) erscheine für die Betrachtung für ITK-Unternehmen zu hoch. Da über den Internetknotenpunkt nicht nur der inländische, sondern auch der internationale Datenverkehr prozessiert wird , sei das Anwenden des Datenvolumens des DE-CIX auf industrielle und/oder unternehmensinterne Datenverbindungen nicht plausibel. Unklar bleibe im Referentenentwurf, inwieweit moderne Telekommunikationsanwendungen wie IP-Telefonie eingeschlossen sind.

Lagersicherheit

Zutrittskontrolle beim sogenannten Bekannten Versender thematisiert GIT-Sicherheit in der Ausgabe 1/2-2016, S. 74/75. Das Luftfrachtbundesamt gebe für die Zertifizierung als „Bekannter Versender" keine exakten Vorschriften aus, sondern überlasse es den Firmen, den eigenen Exportbereich als sogenannten „gekapselten Bereich" zu sichern. Das im Beitrag vorgestellte Unternehmen Ziehm Imaging habe sich dafür entschieden, das Exportlager komplett mit Zutrittskontrolle auszustatten. An allen Eingängen seien Zutrittskontrollleser installiert, die bei zu langer Türöffnung einen Alarm auslösen. Das Rolltor sei zur Schleuse umgebaut worden. An jedem Eingang dokumentiere zusätzlich eine Videokamera alle Zutrittsereignisse. Das Videosystem sei mit der Zutrittskontrollsoftware verbunden, die Videobilder würden mit Hilfe der Videomanagementsoftare ausgewertet. Außerhalb der normalen Arbeitszeiten löse eine gefilmte Bewegung im Exportfrachtbereich eine Alarmierung aus. Der Alarm werde per E-Mail an das Handy des Luftfrachtbeauftragten weitergeleitet. Um Spediteuren auch außerhalb der Arbeitszeiten Abholmöglichkeiten zu geben, werde fertige Luftfracht in Export-Container gepackt, die im Sicherheitsbereich hinter verschlossenen Gitterboxen auf Abholung warteten. Der Speditionsfahrer besitze einen RFID-Tag, für den er am Haupteingang tagesaktuell eine Berechtigung für einen kurzen Zeitraum erhalte.

Maschinensicherheit

Vorgestellt wird in Ausgabe 1/2-2016 der Zeitschrift GIT-Sicherheit, S. 88/89, eine neue Variante des **Laserscanners der Baureihe RSL 440** von Leuze electronic. Er habe die größte funktionale Bandbreite, 100 umschaltbare Feld- bzw. 50 umschaltbare Quadpaare und bis zu 10 unabhängige Sensor-Konfigurationen. Die gesamte Baureihe umfasse 16 Gerätevarianten mit Reichweiten bis 8,25 m. Die Sicherheits-Laserscanner ließen sich via Bluetooth und Ehternet-TCP/IP einfach konfigutieren. Der große Abtastwinkel der Geräte von 270 Grad spiele zum Beispiel bei der Montage an Ecken zur Absicherung nach vorne und seitlich seine Vorteile voll aus und könne hier je nach Anwendung einen zweiten Laserscanner ersetzen.

Das **Sicherheits-Lichtgitter mit Bluetooth-Schnittstelle** präsentiert GIT-Sicherheit in der Ausgabe 1/2-2016, S. 90/91. Das F3SG von Omron verfüge über eine optionale Bluetooth-Schnittstelle. Die komplexe Version könne mit bis zu drei weiteren Modellen

kaskadiert werden und überzeuge durch eine Vielzahl an Zusatzfunktionen. Eine völlig neuartige Funktion für Lichtgitter stelle das „dynamische Muting" dar. Wenn Werkstücke mit unterschiedlichen Höhen auf der gleichen Förderstrecke in einen Gefahrenbereich hinein oder heraus transportiert werden müssen, stelle sich die Höhe der Mutingzone des Lichtgitters automatisch auf die Höhe des Werkstücks ein.

Mechanische Sicherheit

Mit der **Nachrüstung von Türen** befasst sich GIT-Sicherheit in der Ausgabe 1/2-2016, S. 72. Eine vergleichsweise einfache Form der Nachrüstung an Türen sei der Austausch des Schlosses inklusive Schließzylinder und des Schließblechs. Hierbei sollten jedoch die Vorgaben der DIN 18251 für Einsteckschlösser berücksichtigt werden. Das Schließblech sollte durch ein Sicherheitsschließblech ersetzt und fachgerecht befestigt werden. Bei Verwendung von Stahlzargen seien zusätzlich geeignete Verstärkungsplatten zu befestigen. Für die Nachrüstung mit aufschraubbaren und in die Falz eingelassenen Nachrüstprodukten seien die Normen DIN 18104-1 und -2 zu berücksichtigen.

Notfallvorsorge

Der Sicherheitsberater direkt weist in der Ausgabe 2-2016 auf eine vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe veröffentlichten 66-seitigen Ratgeber für Notfallvorsorge und richtiges Handeln in Notsituationen hin.

Öffentliche Sicherheit

Was kostet unsere Sicherheit? – titelt der Behörden Spiegel in der Februar-Ausgabe. Gut 50 Mrd. Euro würden jährlich Bund, Länder und Kommunen für die öffentliche Ordnung und Sicherheit ausgeben. Relativ zur Wirtschaftsleistung sei das weniger als die Mehrheit der anderen europäischen Länder hierfür im Durchschnitt ausgeben. 2013 waren dies in Deutschland 1,6 Prozent des BIP, im EU-Durchschnitt 1,8 Prozent. 2016 würden die Ausgaben des Bundes deutlich ansteigen. Für die öffentliche Sicherheit seien 5,12 Mrd. Euro veranschlagt. Die Kommunen meldeten auch schon die ersten Bedarfe zur Mitfinanzierung ihrer Sicherheit an. Köln habe sich Ende Januar mit sieben anderen NRW-Kommunen zusammengetan und die „Kölner Erklärung zur kommunalen Sicherheit" verfasst. Darin forderten die Städte entschieden die Unterstützung des Bundes und des Landes NRW, um sich den gestiegenen Herausforderungen in Sachen Sicherheit und Integration stellen zu können.

Perimeterschutz

Martin Vogler, Senstar GmbH, beschäftigt sich in der Ausgabe 1/2-2016 von PROTECTOR, S. 42, mit dem Objektschutz im Außenbereich. Eine Zaunanlage sei zunächst einmal ein Bauwerk ohne jeglichen Erkenntnisgewinn für Alarmierung und Organisation von Abwehrmaßnahmen. Sei Unsichtbarkeit der bestimmende Faktor, führe kaum ein Weg an einem Bodenmeldekabelsystem vorbei. Modernste Auswertealgorithmen und anlagenindividuelle Parametrierungsmöglichkeiten sorgten für eine zuverlässige Unterscheidung zwischen Alarm- und Störungsmeldungen und externen Umwelteinflüssen.

Piraterie

Wie der BDSW am 15. Februar berichtet, hat das Internationale Schifffahrtsbüro vor wenigen Tagen darauf hingewiesen, dass aus dem Seegebiet rund um das Horn von Afrika 2015 keine Aktivitäten somalischer Seeräuber gemeldet worden seien. Als Grund nenne das IMB den Einsatz der internationalen Marinestreitkräfte und den verbesserten Schutz von Handelsschiffen auch in Zusammenarbeit mit privaten Sicherheitsdiensten.

Produktpiraterie

In der Ausgabe 1/2-2016 befasst sich PROTECTOR mit Plagiaten aus **China**. Die durch Plagiate verursachten Schäden zögen sich durch sämtliche Industriezweige. Es gäbe Unternehmen, die mehr als 50 Prozent Einbußen durch Fälschung ihrer Produkte erleiden. Besonders hart getroffen sei nach wie vor der deutsche Maschinen- und Anlagenbau. Ein relativ neuer Trend sei das Fälschen kompletter Verkaufseinrichtungen und kompletter Filialen. Schon vor Jahren sei mitten in Peking die Niederlassung eines deutschen Automobilkonzerns eröffnet worden, von der die deutsche Konzernspitze nicht das Geringste wusste. Und Ende August 2015 sei in Shenzhen ein Finanzinstitut aufgefallen, das sich „Goldman Sachs Financial Leasing Co." genannt habe, aber mit der US-Investmentbank nicht das Geringste zu tun habe.

Salafismus

Über die Gefährlichkeit der Salafisten in Deutschland informiert gmx.net am 17. Februar. In Deutschland solle es nach Angaben des Verfassungsschutzes insgesamt rund 44.000 Islamisten geben. Die größte Gefahr gehe von den Salafisten aus. 2011 habe der Verfassungsschutz noch mit 3.800 Personen in dieser Szene gerechnet. Im Dezember 2015 habe der BfV-Präsident bereits von 8.350 Salafisten gesprochen, Tendenz steigend. Sie wollten Staat und Gesellschaft nach ihren Vorstellungen umgestalten. Ihre Propaganda verbreiteten sie vor allem im Internet und bei PR-Aktionen wie der „Scharia-Polizei" in Wuppertal oder dem „Lies"-Projekt, mit dem sie Interessierte mit einer kostenlosen Koran-Ausgabe anlocken und in ihren Bann ziehen wollten. Der Aufruf zur Gewalt oder die tatsächliche Ausübung von Gewalt werde in Deutschland „aus taktischen Gründen" eher vermieden. Insgesamt gehe der Verfassungsschutz derzeit von 1.100 gewaltbereiten Islamisten aus. 430 Personen würden als gefährlich eingeschätzt. Sie könnten jederzeit eine Straftat begehen. Besonders großen Zulauf fänden die Salafisten dort, wo die Perspektivlosigkeit insbesondere junger Migranten groß ist. Netzwerke in den Städten spielten eine wichtige Rolle. 690 Salafisten sollten in Berlin leben, etwa die Hälfte von ihnen gewaltorientiert. Etwa 2.500 Salafisten lebten in Nordrhein-Westfalen. Davon seien 500 gewaltbereit. Salafisten betonten ihre eigene moralische Überlegenheit. Damit gelinge es, vor allem Konvertiten und nicht praktizierende Muslime zu beeindrucken. Besonders minderjährige unbegleitete Flüchtlinge seien ein potenzielles Ziel. Der Verfassungsschutz empfehle Flüchtlingsheimen daher gezielte Gegen- und Sicherheitsmaßnahmen.

Schlüsselmanagement

Eine optimierte Verwaltung von Fahrzeugschlüssen im Autohaus thematisiert GIT-Sicherheit in der Ausgabe 1/2-2016, S. 60/61. Viele unterschiedliche Autoschlüssel sicher verwahren, sie aber trotzdem schnell herausgeben zu können – das sei ein Alltagsproblem vieler größerer Autohäuser. Im Gebrauchtwagen-Markt „Carena Autopark" im brandenburgischen Hoppegarten würden die

Schlüsselschränke über die Commander Connect Software (Deister electronic) angesteuert. Die Identifikation der Mitarbeiter erfolge mit den vorhandenen Transponderkarten über ein Bedienterminal direkt an den Schlüsselschränken. Sie Software gebe die Fahrzeugschlüssel erst nach erfolgreicher Identifikation des Benutzers frei. Die maximale Anzahl der Schlüssel, die ein Mitarbeiter entnehmen darf, könne in der Software festgelegt werden. Der RFID-Chip im Keytag habe eine feste Identifikationsnummer, die mit der internen Fahrzeugnummer in der Software gekoppelt werde. Durch das Herausziehen bzw. Einstecken des Keytags in die Steckplätze im Schlüsselschrank werde jede Entnahme bzw. Rückgabe elektronisch protokolliert.

Sicherheitsgefühl

In der FAZ vom 17. Februar berichtet Prof. Dr. Renate Köcher über eine Befragung und Analyse des Instituts für Demoskopie Allensbach zum **Sicherheitsgefühl der Deutschen**. Danach hatten vor zehn Jahren 47 Prozent der Bürger den Eindruck, dass die Kriminalität in Deutschland zunimmt. 2014 seien es bereits 60 Prozent gewesen, jetzt 69 Prozent. Der Zustrom an Flüchtlingen sei damit nicht für die wachsende Besorgnis entscheidend vergrößere sie jedoch. 79 Prozent seien überzeugt, dass mit der Zahl der Flüchtlinge auch die Kriminalität zunehmen wird. Vor fünf Jahren hätten sich noch zwei Drittel persönlich sicher gefühlt, und nur 26 Prozent machten sich Sorgen, sie könnten Opfer eines Verbrechens werden. 2014 habe dieser Anteil bereits bei 45 Prozent gelegen, jetzt bei 51 Prozent. Der Anteil derer, die sich akut bedroht fühlten, habe sich in den vergangenen Jahren von drei auf neun Prozent verdreifacht. Der Anteil derer, die in der Nähe ein Gebiet benennen können, in dem sie nachts nicht allein unterwegs sein möchten, habe in den vergangenen zehn Jahren von 33 auf 44 Prozent zugenommen. Es habe sich gezeigt, dass 92 Prozent der Befragten mehr Personal für die Polizei wollen und 90 Prozent eine bessere Ausrüstung der Sicherheitskräfte. 90 Prozent hielten es auch für richtig, Flughäfen oder Bahnhöfe kontinuierlich mit Kameras zu überwachen. Und 84 Prozent unterstützten die Erfassung von Fingerabdrücken von jeder Person, die einreist. Die Hälfte befürworte auch die flächendeckende Erfassung und Speicherung von Fingerabdrücken aller Bürger, um die Verbrechensbekämpfung zu erleichtern. Die Mehrheit könne sich für den verstärkten Einsatz der Bundeswehr im Innern erwärmen, zum Beispiel zum Schutz von Gebäuden und Personen. Kritisch würden vor allem Maßnahmen gesehen, die die Innere Sicherheit aus der Verantwortung des Staates verstärkt in die der Bürger überführen. Weder die Gründung von Bürgerwehren noch die Erleichterung des Waffenbesitzes fänden nennenswerte Unterstützung.

Steuerbetrug

Mit der doppelten Steuererstattung durch „CUM-EX-GESCHÄFTE" befasst sich die Wochenzeitung DAS PARLAMENT am 22. Februar. Bei den „Cum-Ex-Geschäften" mittels Leerverkäufen sei eine Situation herbeigeführt worden, in der eine Aktie rechtlich gesehen für eine kurze Zeit scheinbar mehrere Eigentümer hatte. Der Zeitraum sei dabei so gewählt worden, dass in ihn die Auszahlung der Dividende fiel. Das habe dazu geführt, dass für eine nur einmal an die Finanzbehörden abgeführte Kapitalertragsteuer mehrere Steuerbescheinigungen ausgestellt worden seien. Die Kapitalertragssteuer sei dadurch mehrfach auf die Steuern der verschiedenen Eigentümer angerechnet worden, was zu mehrfachen Entlastungen an anderer Stelle geführt habe, obwohl es die entsprechende Belastung nur einmal gegeben habe. Dem Fiskus seien durch solche Geschäfte im Zeitraum von zehn Jahren etwa zwölf Mrd. Euro verloren gegangen. An der Plünderung

der deutschen Staatskasse hätten sich über 100 Banken und Fonds aus vielen Ländern beteiligt.

Tresorsicherheit

Einige grundsätzliche Regeln, die man bei der Auswahl seines Tresors beachten sollte, skizziert Andreas Roß, Gunnebo Deutschland, in GIT-Sicherheit, Ausgabe 1/2-2016, S. 62/63. Tresore würden in acht Sicherheitsklassen von 0 bis VII eingeteilt. Je nach Land seien die Versicherungswerte für die verschiedenen Widerstandsklassen unterschiedlich hoch. Es sei unbedingt darauf zu achten, dass Anbieter bzw. deren Produkte ECB-S zertifiziert sind. Nur dann sei garantiert, dass europäische Branchenstandards eingehalten werden. Da es bei einem Einbruch um Minuten gehe, sollte der Safe mit einem Alarmsystem oder anderen Formen von Überwachung einhergehen.

Vernetzte Autos

Die FAZ berichtet am 1. März über die wichtigsten Erkenntnisse einer Studie zur Sicherheit von Anwendungen in vernetzten Autos von Veracode: Anwendungen aus dem Internet stellten eine erhebliche Herausforderung für die Sicherheit dar. Alle interviewten Hersteller hätten Sicherheitsbedenken, vor allem gegenüber Anwendungen, die sie nicht selbst entwickelt haben. Darüber hinaus fänden die Befragten, dass Hersteller für die Sicherheit eines vernetzten Autos haftbar sein sollten. Dazu zähle auch die Fähigkeit von Apps, Cyberangriffen zu widerstehen. Die Hersteller gingen derzeit im Prinzip davon aus, sich nicht um den Datenschutz der Fahrer sorgen zu müssen. 46 Prozent der Autofahrer hätten jedoch Bedenken rund um das Thema Datenschutz, insbesondere vor dem Hintergrund immer stärker integrierter Anwendungen. Das Risiko eines Verlusts von Kreditkaten- oder anderen persönlich Daten steige.

Videoüberwachung

GIT-SICHERHEIT.de weist am 22. Januar auf eine **neue Wärmebildkamera-Serie** von Dahua Technology hin. Die intelligenten Wärmebildkameras verfügten über einen Sensor, der in der Lage ist, auch geringste Temperaturunterschiede zu erkennen. Die Kameras dieser Serie erreichten eine höhere Erkennungsgenauigkeit und arbeiteten selbst in vollständiger Dunkelheit und unter ungünstigen Wetterverhältnissen. Sie könnten Temperatur und Temperaturverteilung selbst auf kleinen und sich schnell bewegenden Objekten präzise erfassen. Die Dahua Hybrid-Wärmebild-PTZ-Netzwerkkamera sei eine leistungsfähige Kombination aus einer optischen Kamera mit integriertem 40-fach optischem Zoomobjektiv und einer Wärmebildkamera, die in ihren Schwenk- und Neigebewegungen präzise synchronisiert ist. Sie könne das Gesamtbild erfassen, ohne dass die Entfernung vergrößert oder ein Ausschnitt gewählt werden muss. Das Spezialobjektiv fokussiere auch Infrarotlicht, das von Objekten im Aufnahmebereich abgegeben wird. Sie könne gleichzeitig mehrere unabhängige H.264-Streams für unterschiedliche Qualitätsanforderungen und Bandbreitenbeschränkungen liefern.

Im Interview mit der Zeitschrift PROTECTOR (Ausgabe 1/2-2016, S. 14/15) nimmt Prof. Dr.-Ing. habil. Jürgen Beyerer, Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung, Stellung zum **Forschungsprojekt Nest**. Das Nest-System sei primär für die Überwachung weiträumiger Bereiche mit verteilten Kameras oder verteilter Sensorik konzipiert worden. Entsprechend seien die Softwareplattform und die Komponenten zur Videoanalyse hinsichtlich Skalierbarkeit des Gesamtsystems ausgelegt. Durch die

notwendige große Anzahl an Kameras sei sehr früh erkannt worden, dass eine „Videowand"-Darstellung der Videoströme als Visualisierungs- und Interaktionsschnittstelle nicht geeignet ist. Das System sei deshalb mit einer synchronen Karten-/Videodarstellung konzipiert worden. Dabei könne der Benutzer mit einem Zwei-Monitor-System sowohl anhand der Videoströme als auch mit der Kartendarstellung der zu überwachenden Liegenschaft Kameras selektieren und steuern, aber auch Objekte auswählen und Positionen anfahren. Soll ein bestimmter Bereich einer Liegenschaft überprüft werden, so reiche ein Klick auf diese Karte, und eine Kamera schwenke auf die entsprechende Position. Gleichzeitig würden detektierte Bewegungen von Objekten nicht nur in dem entsprechenden Videostrom auf einer Monitorwand visualisiert, sondern prominent auch auf der Kartenoberfläche. Dadurch entstehe eine zentrale „Lagedarstellung", die für das Sicherheitspersonal eine intuitive Informationsschnittstelle darstellt.

PROTECTOR behandelt in der Ausgabe 1/2-2016 (S. 28/29) die **thermische Radiometrie** zur Gefahrenerkennung. Es gebe mittlerweile Videosysteme, bei denen die Thermaltechnologie und die optische Sensortechnologie mit einem intelligenten On-board-Videosensor kombiniert sind, wodurch sich Objekte und Personen in kompletter Dunkelheit über hunderte Meter oder bei Sichteinschränkungen durch Rauch oder Smog automatisch detektieren und durch die optischen Bildsensoren identifizieren lassen. Thermalkameras eigneten sich zur Alarmierung von Temperaturgrenzen oder -bereichen, was entscheidend bei der Erkennung von Feuer oder Hitzequellen ist. Sie würden daher beim Werkschutz und zur Sicherheit in Produktionshallen sowie zur Maschinen- und Geräteüberwachung eingesetzt. Außerdem nutzten Nahrungsmittelindustrie und Logistik-Systeme die TR-Technologie sowohl bei Produktion und Lagerung als auch beim Transport von Gefahrengütern. Im Gegensatz zu Kameras mit optischen Bildsensoren sei eines der entscheidenden Qualitätskriterien für eine Thermalkamera die Fähigkeit, so geringe Temperaturunterschiede wie möglich zu erfassen und im Bild durch Farbunterschiede darzustellen. Diese Empfindlichkeit werde durch den Rausch-Signalabstand NETD in Millikelvin (mk) angegeben. So ließen sich mit einem NETD von 50 mk bereits minimale Temperaturunterschiede von 0,05 Grad visualisieren. Die Systeme seien in der Lage, die Wärmestrahlung im gesamten Bildbereich zu messen und pro Pixel einen Temperaturwert zuzuordnen. Die Genauigkeit der Temperaturmessung hänge vom Emissionsgrad des gemessenen Objekts ab, der vom Material und der Oberfläche des Messobjekts bestimmt wird. Der große Vorteil der Wärmebildtechnik liege darin, dass die Detektion und Messung auch aus Entfernungen von bis zu mehreren hundert Metern und damit auch in großen und schwer zugänglichen Bereichen erfolgen könne.

Videomanagementsoftware für **Handelsketten mit Filialnetz** behandelt PROTECTOR in der Ausgabe 1/2-2016 (S. 30/31) am Beispiel der belgischen Einzelhandelskette Colruyt mit 470 Filialen. In der Wachzentrale am Hauptsitz des Konzerns würden die Meldungen aller Filialen, aber auch die der Bürogebäude und Logistiklager zusammenlaufen. Während der Perimeterschutz aus dem Leitstand erfolgt, liege die Diebstahlprävention in der Verantwortung der einzelnen Filialen. Jede Filiale verfüge über ein Videoüberwachungssystem, das aus einem abgesetzten Server, Kameras und einem oder mehreren Aufzeichnungsgeräten bestehe. Sind die (Seetec Cayuga)-Server mit dem Internet verbunden, lade der Seetec Auto Updater automatisch Patches, Updates und Upgrades für die Software herunter und übernehme anschließend die Aktualisierung des Systems.

Es gebe inzwischen eine Reihe speziell für den kleineren Handel entwickelter, einfach zu

bedienender, Systeme wie das F34 Überwachungssystem von Axis Communications, berichtet PROTECTOR in der Ausgabe 1/2-2016 (S. 32). Dieses einfach installierbare, unauffällige Überwachungssystem aus vier Kameras sei insbesondere für **kleine Geschäfte und Büros** geeignet. Die Kamera sei in eine Sensoreinheit und eine Haupteinheit aufgeteilt. Die Haupteinheit Axis F34 könne mit vier Sensoreinheiten gleichzeitig verbunden werden. Managed-Services oder auch „Video Surveillance as a Service" seien vor allem für Endkunden interessant, die einen zuverlässigen und kostengünstigen Videoschutz rund um die Uhr benötigen, der sie jedoch keinerlei technische Investitionen oder Wartungsaufwand koste.

Den **Nutzen hoher Bildauflösung** erläutert Katharina Geutebrück in der Ausgabe 1/2-2016 der Zeitschrift GIT-Sicherheit, S. 46-48. Eine hochauflösende Kamera könne mehrere Kameras mit niedrigerer Auflösung ersetzen. Das spare Kosten nicht nur für die Kamera, sondern auch für Montage und Verkabelung. Hochauflösende Kameras seien weniger lichtempfindlich, das heißt sie benötigten mehr Licht für ein rauschfreies, klares Bild. Versuche man, fehlende Lichtempfindlichkeit durch eine längere Belichtungsdauer zu kompensieren, führe dies zu Bewegungsunschärfen. Höher auflösende Kameras benötigten mehr Bandbreite im Netzwerk, mehr Kapazität im Speichersystem und auch mehr Rechenleistung auf den Wiedergabestationen. Eine mittelmäßige Kamera mit einem qualitativ hochwertigen Objektiv liefere in der Regel eine bessere Bildqualität als eine Top-Kamera mit einem billigen Objektiv.

Video-Trends im Einzelhandel behandelt GIT-Sicherheit in der Ausgabe 1/2-2016, S. 53. IP-Kameras könnten die Gesamtanzahl der Kameras durch die wesentlich bessere Bildqualität gegenüber analogen Systemen deutlich reduzieren. Zudem könnten Speicherlösungen realisiert werden, die um ein Vielfaches günstiger seien als ein Onsite-Server oder Digital-Videorecorder. Insgesamt reduziere die Umstellung auf digitale Systeme die Investitionskosten im Unternehmen deutlich. Zur Zeit seien zwei ineinander greifende Trends im Einzelhandel sichtbar: Erstens die Integration der einzelnen Sicherheitssysteme und zweitens der vermehrte Einsatz von intelligenten Analysen zur Optimierung der Ladengeschäfte. Der Kreis der Lieferanten und Logistikdienstleister, die Abholungen oder Anlieferungen durchführen, vergrößere sich. Damit der Retailer einen hundertprozentigen Überblick behalte, erhalte jeder Lieferant für einen Auftrag einen einmaligen QR- oder Barcode. Diesen zeige er in die Kamera, die den Code dann mit einer Whitelist abgleiche. Ist er korrekt und der Lieferant autorisiert, öffne sich die Tür.

Wächterkontrollsysteme

Mit neuesten Technologien für Wächterkontrollsysteme befasst sich Winfrid Stotz, CSS Computer Security Service Gmb in der Ausgabe 2-2016 der Zeitschrift Protector, S. 52. Angesichts der stetig steigenden Anforderungen an die Sicherheits- und Werkschutzmitarbeiter kämen insbesondere der Datenübertragung in Echtzeit, der Einzelplatzabsicherung und den umfassenden Dokumentationsmöglichkeiten zentrale Bedeutung zu. Neu seien Lösungen wie zum Beispiel Tourtrax.net, eine „Software as a Service", die eine einfache Zeiterfassung und Protokollierung von Kontrollgängen jetzt auch per Smartphone ermögliche. Der Einsatz von RFID- oder Barcode-Technologie gewährleiste eine genaue und mobile Zeiterfassung sowie Online-Übertragung in Echtzeit. Dabei sei eine Ortung der Geräte über Kontrollpunkte oder GPS ebenfalls möglich. Die Lösung unterstütze neben Android-Systemen mit NFC-Technologie auch alle bisherigen CSS-Online-Wächterkontrollsysteme.

Zutrittskontrolle

Neue Weitbereichsleser mit passender Smartcard von HID Global stellt GIT-Sicherheit in der Ausgabe 1/2-2016, S. 54/55, vor. Die neueste Technik elektronischer Zutrittskontrolle könne Schranken, Türen und Tore öffnen, Zugangsberechtigte wahrnehmen und das, ohne sich den Arm vor dem Sensor auszurenken. Lesereichweiten von bis zu fünf Metern ermöglichen es, direkt aus dem Auto erkannt zu werden. HID Global bringe jetzt solch ein Produkt auf den Markt. Die Serie werde um ein Weitbereichslesegerät erweitert, den iClass SE U90 Long Range Reader. Dazu passend komme auch eine UHF-Smartcard, die sowohl Schranken und Tor öffnet, als auch die Zutrittskontrolle ermögliche. Der Leser anonymisiere Identitätsdaten durch AES 128-Verschlüsselung und schütze diese mit End-to-End-Kommunikationstechnologie. Die UHF-Smartcard biete eine sichere Kontrolle an Parkplätzen. Sie identifiziere mit einer Reichweite von bis zu neun Metern. Außerdem habe sie mit 100.000 Schreibzyklen eine hohe Lese-/Schreibzuverlässigkeit und eine lange Lebensdauer. Durch SIO (Secure Identity Object) würden die Identitätsdaten auf der Karte mit Multilayer-Sicherheit geschützt. Das Lesegerät sende ein Passwort, um Zugang zum geschützten Speicher der Karte zu erhalten, in dem vertrauliche oder geschäftssensible Daten gespeichert werden. Zusätzlich füge das SIO-Datenmodell eine weitere Verschlüsselungs- und Authentifizierungsebene hinzu.

Impressum

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

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

Herausgeber:
Manfred Buhl, Vorsitzender der Geschäftsführung, Düsseldorf

Verantwortlicher Redakteur:
Bernd Weiler, Leiter Kommunikation und Marketing

Beratender Redakteur:
Reinhard Rupprecht, Bonn

focus.securitas.de

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

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

E-Mail: info@securitas.de