Focus on Security

Ausgabe 04, April 2015

SECURITAS

Inhalt

Anschläge

Wie das BKA in der Wochenlage am 27. Februar mitteilte, haben unbekannte Täter am 19. Februar in Frankfurt am Main sieben Fensterscheiben der Firma **„Deutsche Annington Immobilien SE“** eingeworfen und auf dem Parkplatz der Firma drei Firmenfahrzeuge mit Brandbeschleuniger in Brand gesetzt. In der Nacht zum 23. Februar verübten Unbekannte in Berlin Brandstiftungen an zwei Fahrzeugen der Firma **„Sicherheit Nord“**. Unter der Überschrift „Aktion gegen Deutsche Annington in Frankfurt“ veröffentlichten unbekannte Verfasser unter dem Pseudonym „destroika“ auf der Internetseite „linksunten.indymedia.org“ ein Selbstbezichtigungsschreiben, in dem die Taten u. a. in den Kontext zur Eröffnung der neuen EZB-Zentrale am 18. März gestellt werden. Weitere unbekannte Verfasser veröffentlichten unter der Überschrift „Für ein Höllenfeuer auf Erden…“ ein Selbstbezichtigungsschreiben zu den Brandstiftungen zum Nachteil der „Sicherheit Nord“. Sie stellten die Tat in den Begründungszusammenhang „Repression“, „für eine Gesellschaft ohne Zwang und Knäste“ und „für die Anarchie“.

In der Wochenlage am 20. März teilt das BKA mit, dass am 13. März Unbekannte einen **Pkw der DB** in Dresden in Brand gesteckt haben. Unbekannte Verfasser veröffentlichten ein Selbstbezichtigungsschreiben, in dem sie die Tat mit dem „menschenunwürdigen Verhalten“ der DB und deren Personal begründen.

Bahnsicherheit

Mitarbeiter der Deutschen Bahn haben es teilweise mit **immer aggressiveren Kunden** zu tun, berichtet das Magazin Focus am 28. Februar. 2014 habe das Unternehmen mehrere hundert Hausverbote erteilt und angekündigt, häufiger und härter mit Haus- und Reiseverboten gegen Gewalttäter vorzugehen. Die Zahl tätlicher Angriffe habe 2014 gegenüber dem Vorjahr um 25 Prozent auf 1.500 zugenommen. Die Bundespolizei habe 2014 bei der Bahn 13.650 Körperverletzungsdelikte gezählt, 7 Prozent weniger als 2013, heißt es dagegen in der FAZ am 11. März. Der Vandalismus sei ebenfalls um 7 Prozent auf 11.500 Fälle zurückgegangen. Einen Anstieg habe es nur bei den Graffiti gegeben (um 25 Prozent auf 19.350 Taten mit einem Schaden von 8,1 Mio. Euro). Die bedeutend geringere Kriminalitätsbelastung als der sonstige öffentliche Raum sei vor allem auf eine verstärkte Präsenz der nunmehr 3.700 Bahn-Sicherheitskräfte zurückzuführen, habe der Sicherheitschef der Bahn, Gerd Neubeck, ausgeführt. Jährlich investiere die Bahn rund 160 Mio. Euro in die Sicherheit. Die Bahn werde die Videotechnik an mehr als 100 Bahnhöfen weiter ausbauen. Auch bei der Bekämpfung der Buntmetalldiebstähle verzeichne die Bahn Erfolge. Die Fallzahlen seien 2014 um weitere 15 Prozent auf etwa 1.500 Taten zurückgegangen. Den materiellen Schaden beziffere die Bahn auf 17,1 Mio. Euro. Der Schaden durch Vandalismus habe bei 27 Mio. Euro gelegen. Die Anzahl aufgebrochener Fahrkartenautomaten sei um knapp ein Drittel auf 380 gesunken. Dadurch sei ein Schaden von 6,7 Mio. Euro entstanden. Die Zahl der registrierten Aggressionen und Übergriffe gegen ihre Mitarbeiter sei um ein Viertel auf 1.500 gestiegen.

Betrug

Der ASW Bundesverband hat **Leitfäden zum Thema „Anti-Fraud-Management“** veröffentlicht, wie er im Newsletter Sicherheitspolitik vom 13. März bekannt gibt. Die „Leitplanken zur Durchführung interner Ermittlungen“ führten den Leser an verschiedenen kritischen Aspekten vorbei und zeigten unterschiedliche Blickwinkel und Positionen zu einzelnen Themenfeldern auf. Auch der

Leitfaden „Investigation Tools" diene als Entscheidungshilfe für Ermittlungen. Beide Leitfäden könnten beim ASW Bundesverband über die Homepage bestellt werden. Erstellt worden seien beide Publikationen im Kompetenz-Center „Anti-Fraud-Management".

Biometrie

Der Sparkassenverband Bayern steuert nach einer Meldung von s+s report (Ausgabe 1-2015, S. 6) mit Hilfe einer Biometrie-Lösung Zutritt und Zeiterfassung. Mitarbeiter müssten sich künftig nicht mehr um verlorene oder defekte Unternehmensausweise kümmern. Das Buchen der Arbeitszeiten sowie der Zugang zum Arbeitsplatz erfolge mittels berührungsloser **3-D-Fingererkennung**.

Brandschutz

Euralarm schlägt **EU-Richtlinien zu Brandschutz und Sicherheit für Touristenunterkünfte** vor, titelt GIT-SICHERHEIT.de am 23. Februar. Euralarm sei der Überzeugung, dass die europäische Tourismusbranche Sicherheitsstandards auf Weltklasseniveau einführen muss, die auf europäischer Ebene durchgesetzt und reguliert werden müssten. Zum Beispiel sei in einigen Ländern die Installation von Brandmeldern in Schlafzimmern und Fluren vorgeschrieben, wohingegen in anderen Ländern nur die Installation in Hotelfluren vorgeschrieben sei. Der Schwerpunkt der vorgeschlagenen EU-Richtlinie sollte auf folgenden Aspekten liegen: Konformität der Brandschutzprodukte/-systeme mit EN-Standards, die mit EU-weiter Genehmigung extern nachgewiesen wird; Notwendigkeit qualifizierter Unternehmen für Planung/Design, Installation, Inbetriebnahme und Wartung, die gemäß den europäischen Standards arbeiten; obligatorische Standinspektionen durch unabhängige externe Parteien in festgelegten Abständen nach Art, Größe und Höhe der Einrichtung.

Ausgabe 1-2015 der Fachzeitschrift s+s report enthält mehrere Beiträge zu Brandschutzthemen:
Dr. Michael Buser, Risk Experts – Risiko Engineering GmbH, befasst sich mit geschäumten Kunststoffen zur **Dämmung von Gebäuden** (S. 8/9). Sie böten aufgrund ihrer anwendungstechnischen Vorteile optimale Voraussetzungen für den Einsatz als Dämmstoff. Brandschutztechnisch hätten diese Dämmmaterialien allerdings einen wesentlichen Nachteil. Hinter dem Begriff „schwer entflammbar" (B1) verberge sich ein kritisches Brandverhalten. Im Sinne eines nachhaltigen Personen-, Umwelt- und Sachwertschutzes sei die Verwendung von konventionellen, nicht-brennbaren Dämmstoffen (z. B. Mineralwolle) vorzuziehen. Sofern an der Verwendung von geschäumten Dämmstoffen festgehalten wird, sei ungeachtet entschärfter baurechtlicher Anforderungen aus brandschutztechnischer Sicht der generelle Einbau von Brandschutzriegeln zu fordern.

Dipl.-Biol. Tim Pelzl, DGUV München, Gerhard Sprenger, DGUV BG Nahrungsmittel und Gastgewerbe, und Bernd Manning, VdS Schadenverhütung, behandeln Aufgaben, Qualifikation, Ausbildung und Bestellung von **Brandschutzbeauftragten** (S. 15–18). Ihr Fazit: Im Rahmen der zu erstellenden Gefährdungsbeurteilung sollte die Bestellung eines Brandschutzbeauftragten bei identifiziertem Bedarf die Regel sein. Sowohl die jetzt erschienene DGUV Information 205-003, die VdS 3111 und die vfdb-Richtlinie 12-09/01 stellten in der Gesamtschau mit der Arbeitsstättenregel „Maßnahmen bei Bränden" (ASR A2.2) und weiteren Publikationen von DGUV, vfdb und VdS ein schlüssiges Konzept zum Thema betrieblicher Brandschutz aus Sicht der gesetzlichen Unfallversicherung dar.

Ivar Fjeldheim, Jakob Hatteland Computer AS, stellt ein VdS-anerkanntes Schutzkonzept

für ein **automatisches Lager von Kleinladungsträgern** (KLT-Lager) aus Kunststoff vor. Die KLT werden in einer Gerüstkonstruktion aus Aluminiumstranggussprofilen gestapelt, automatisch von Robotern aufgenommen und zu Kommissionierplätzen transportiert (AutoStore-System). Durchschnittlich würden ca. 30.000 bis 40.000 KLT in einer Einheit gelagert, wobei die derzeit größte Einheit bis zu 168.000 KLT umfassen könne. Um in großen AutoStore-Anlagen die Brandausbreitung verhindern zu können, seien Trennwände aus Stahlblech eingebaut, die die Brandausbreitung bis zur Auslösung der Sprinkleranlage verhindern. VdS habe das Schutzkonzept gemäß VdS CEA 4001 für AutoStore auf der Basis einer Sprinkleranlage anerkannt (S. 19–21).

M.Sc. Bettina Bormann und Dipl.-Ing. Martin Hesels, VdS Schadenverhütung, befassen sich mit der **gemeinsamen Nutzung von Geräten und Übertragungswegen** einer bestehenden IT-Infrastruktur in Brandmeldesystemen (S. 37–41). Sie erscheine vernünftig und vorteilhaft. Jedoch seien einige wichtige Fragen nach wie vor ungeklärt. Die Autoren gehen diesen Fragen nach und stellen zusammenfassend fest, dass neue Technologien und ihr Einsatz in Verbindung mit Brandmeldeanlagen zurzeit noch mit größter Vorsicht zu behandeln sind. Die entstehenden Vor- und Nachteile müssten umfassend beurteilt und ihre Konsequenzen erörtert werden, bevor Veränderungen vorbehaltlos akzeptiert werden. Einerseits müssten neue Komponenten und Geräte in die Welt der Normen eingefügt werden. Andererseits entstünden neue Probleme, die durch die Erarbeitung geeigneter Regeln für eine sichere Anwendung geklärt werden müssten. Das Hauptproblem liege in der fehlenden Konformität der Komponenten und Geräte mit der EN54-Normenreihe sowie den in diesen Normen verankerten Anforderungen an Leistung und Zuverlässigkeit. Der Einsatz von IP-Technologie und Cloud-Lösungen bringe Unsicherheiten bezüglich der Verantwortlichkeiten und der zuverlässigen Leistungsfähigkeit der Brandmeldeanlagen mit sich. Des Weiteren entstünden Konkurrenzsituationen, sobald ein Netzwerk nicht ausschließlich von der BMA genutzt werde.

Wie die Fachzeitschrift s+s report berichtet (S. 53), haben der GDV und VdS Schadenverhütung gemeinsam eine DVD produziert, die professionelles Videomaterial zur **Illustration von typischen Brandgefahren** bietet. Themen seien brennbare Anlagerungen an Gebäuden, Brandlasten in Produktions- und Lagerbereichen, Brandgefahren an Maschinen sowie elektrische Anlagen. Die DVD könne beim VdS-Verlag unter der Bestellnummer VdS 3401 bezogen werden.

Cloud Computing

Oliver Tuszik, Cisco, fordert in einem Verlagsspezial „ITK 2015" der FAZ am 12. März **Europäische Standards für das Cloud Computing**. Rechtliche Rahmenbedingungen, die die Sicherheit von Cloud Services international regeln, suche man vergebens. Um Vorschriften für den Datenschutz, den Persönlichkeitsschutz und den Schutz kritischer Infrastrukturen einzuhalten, müssten sich Unternehmen genau überlegen, welche Daten sie in der Cloud ablegen – und welches Cloud-Modell sie dafür wählen: die eigene, private Cloud, die Public Cloud, die hybride Cloud oder die Intercloud, die verschiedene Clouds miteinander vernetzt. Auch im eigenen Rechenzentrum müssten Unternehmen ein sehr hohes Sicherheitsniveau gewährleisten – ob mit oder ohne Cloud-Technologien. Lange Zeit habe die Public Cloud als unsicher gegolten, aber inzwischen hätten die meisten Cloud-Anbieter Sicherheitsmaßnahmen eingeführt. Unternehmen sollten aber keine sensiblen, geschäftskritischen oder personenbezogenen Daten in der Public Cloud ablegen. Der Autor ist überzeugt, dass nicht deutsche Regeln, sondern europäische Standards erforderlich seien. Nur bei

einem möglichst großen, frei zugänglichen Wirtschaftsraum seien schnelle Innovationen möglich, könnten neue Dienste rasch zur Verfügung gestellt werden.

Die **Digitalisierung der Geschäftsprozesse** sorge dafür, dass IT-Infrastrukturen sowie die darauf befindlichen Daten eine immer stärkere Bedeutung im Unternehmen einnehmen. IT-Infrastrukturen seien heutzutage weniger ein geschlossenes System, sondern ein hybrides Netzwerk. Die engere Vernetzung mit externen Partnern und Unternehmen sowie den Kunden sei ein strategischer Imperativ. Neue Wege fänden Cyberkriminelle oftmals in der Public Cloud. Der Betrieb von Geschäftsanwendungen auf einer solchen Infrastruktur werde oftmals fachbereichsintern entschieden. Der Nachteil an einem solchen Public Cloud-Deployment sei außerdem, dass die unternehmensinternen Sicherheitsexperten keine Kontrollmöglichkeit der Systeme haben. Analog zum Applikationsbetrieb in der Cloud gebe es mittlerweile auch „Security as a Service". Die Sicherheitslösungen der Provider würden auch hier aus dem Rechenzentrum des Anbieters in die Infrastruktur der Anwenderunternehmen integriert. Der Vorteil einer Security Lösung aus der Cloud liege darin, dass Unternehmen auf den gleichen Umfang einzelner Sicherheitsmodule zugreifen können und dabei immer auf dem neuesten Stand der Technik seien. Einen Cloud-Anbieter ohne sichere Verschlüsselung solle man unbedingt meiden. Um den Applikationsbetrieb und die Sicherheit aus der Public Cloud zu verbinden, eigneten sich Managed Cloud-Infrastrukturen besonders gut. Hierbei würden die Systeme auf einer einheitlichen Sicherheitsinfrastruktur zusammengeführt und betrieben (TecChannel.de vom 6. März).

Unison – anspruchsvoller Chatdienst für Unternehmen – titelt TecChannel.de am 7. März. Bei Unison handele es sich um einen Cloud-Dienst aus New York, der 2011 gestartet wurde und das Ziel verfolgt, die Kommunikation und Zusammenarbeit von Business-Teams zu optimieren. Mit einem umfangreichen Featureset, das Gruppenchats, einfaches File-Sharing, automatische Benachrichtigungen sowie Audio- und Videoanrufe enthält, stehe der Dienst in direkter Konkurrenz zu Schwergewichten auf dem Productivity-Markt. Den Unterschied zu fest etablierten Lösungen wolle Unison mit weiterführenden Features wie Datenverschlüsselung, professionellen User-Management-Funktionen sowie mit speziellen Compliance-Features erbringen.

Zur CeBIT zeige eine Arbeitsgruppe aus Politik, Wirtschaft und Wissenschaft eine **Erweiterung der ISO/IEC-Norm 27018 (Datenschutz in der Cloud),** die sich speziell an die Bedürfnisse deutscher Nutzer richte. Ziel sei die Schaffung einer Grundlage einer datenschutzkonformen Zertifizierung. Diese solle Cloud-Anbieter hinsichtlich des Datenschutzniveaus vergleichbar machen und außerdem Rechtssicherheit im Hinblick auf Verpflichtungen nach den geltenden Datenschutzgesetzen sicherstellen. Ein Anforderungskatalog Cloud-Angebote sieht drei Schutzklassen vor:

I. Der Dienstanbieter muss durch technische und organisatorische Maßnahmen, die dem Risiko angemessen sind, gewährleisten, dass die Daten nicht unbefugt verändert oder gelöscht werden. Die Maßnahmen müssen so gestaltet sein, dass sie dies auch ausschließen, falls technische oder organisatorische Fehler geschehen, einschließlich von Bedienfehlern oder fahrlässiger Handlungen Dritter. Vorsätzliche Eingriffe müssen durch einen Mindestschutz erschwert werden.

II. Die Maßnahmen müssen auch technische oder organisatorische Fehler durch den Cloud-Anbieter und seine Mitarbeiter ausschließen. Außerdem sind die Daten so zu schützen, dass zu erwartende Eingriffe „hinreichend sicher" verhindert werden. Dazu gehört vor allem der Schutz gegen bekannte Angriffsszenarien.

III. Die zuvor genannten Maßnahmen müssen dem Stand der Technik entsprechen. Außerdem muss der Dienst in der Lage sein, Eingriffe oder auch Missbräuche festzustellen. Höhere Anforderungen als die der Schutzklasse III beziehen sich auf eine vollständige Nachweisbarkeit der Vertrauenswürdigkeit aller verwendeten Komponenten und führen zur Schutzklasse „III+".

Zusätzlich habe das Zertifikat auch Rechtsfolgen. Denn dadurch, dass ein Unternehmen einen Anbieter auswählt, der mit der für die Unternehmensdaten notwendigen Schutzklasse ausgezeichnet ist, erfülle das Unternehmen die vom Gesetz vorgeschriebenen Kontrollpflichten.

Datenschutz

Die „European Union Agency for Network and Information Security" (ENISA) habe im Januar ihre Empfehlungen zur festen Einbindung von Datenschutz in Anwendungen und Prozessen vorgelegt, berichtet der Behörden Spiegel in seiner Februar-Ausgabe. Der Bericht „**Privacy and Data Protection by Design – form Policy to Engineering** " schließe sich einer Jahrzehnte währenden Diskussion darüber an, wie rechtliche Anforderungen in Systeme eingebettet werden können. Dabei spielten die technischen Mechanismen eine Rolle, die sogenannten „Privacy-Enhancing Technologies" (PETs) wie Verschlüsselung, Protokolle für anonyme Kommunikation, sogenannte attributbasierte Nachweise, die „Attribute-Based Credentials", die es ermöglichen, einzelne Attribute zu bescheinigen, ohne die eigene Identität zu offenbaren. Auch wenn der Nutzen der PETs wissenschaftlich belegt ist, fänden sie wenig Anwendung in der Praxis. Es werde auch festgehalten, dass „Privacy by Design" ein technischer Ansatz für ein soziales Problem sei und man bei der Nutzung von Technik nicht gänzlich ohne Daten kommunizieren könne.

Ein hohes und **europaweit einheitliches Datenschutzniveau** könne auch für den Mittelstand sowie für Start-up-Unternehmen ein Vorteil im internationalen Wettbewerb sein. Diese Ansicht habe die Mehrheit der zu einem öffentlichen Fachgespräch des Ausschusses Digitale Agenda geladenen Experten im Bundestag geäußert, berichtet der Behörden Spiegel in seiner März-Ausgabe. Entscheidend für die Wirtschaft sei nicht so sehr, ob es einen strengen oder einen nicht so strengen Datenschutz gebe, habe Hermann Weiß von Natgurtrip.org gesagt. „Die Wirtschaft kann mit jeder Regelung umgehen, sie braucht aber Planungssicherheit." In derselben Ausgabe wird über den 18. Europäischen Polizeikongress in Berlin berichtet, auf dem der nordrhein-westfälische Landeskriminaldirektor, Dieter Schürmann, Möglichkeiten und Grenzen von „Predictive Policing" skizzierte. Da hierfür nur Daten ohne konkreten Personenbezug genutzt würden und für die Nutzung keine zusätzliche Datenerhebung notwendig sei, bleibe der Datenschutz vollständig gewahrt. Gleichwohl spiele er eine äußerst wichtige Rolle. In Deutschland werde „Predictive Policing", mit dem sich die Wahrscheinlichkeit bevorstehender Straftaten vorhersagen lasse, in Bayern und Nordrhein-Westfalen getestet.

Evakuierung

Markus Niederberger und Jürgen Rumeney, Siemens Building Technologies, stellen in s+s report (Ausgabe 1-2015, S. 54–56) eine von Siemens Corporate Technology entwickelte **Simulationssoftware „Crowd Control"** zur Evakuierungsplanung vor. Es handele sich um eine innovative Berechnungsmethode, bei der die Forscher auf ein aggregierendes Verfahren gesetzt hätten: Räume werden in einzelne Zellen unterteilt, die dem Platzbedarf eines Menschen entsprechen. Das Verhalten leerer und besetzter Zellen werde mittels Kraftfelder definiert. Ausgangspunkte

und Zielorte der Personen könnten eingefügt werden, ebenso Hindernisse wie geparkte Fahrzeuge oder Feuer. Das Modell könne so simulieren, wie sich Mengen von Hunderten, Tausenden oder Zehntausenden von Menschen verhalten – und zwar zehnmal schneller als sie sich in Echtzeit bewegen. Werde die Software mit realen Informationen aus Überwachungskameras gekoppelt, lasse sich die Bewegung von Menschenmassen bis zu fünf Minuten im Voraus prognostizieren. Die Software unterstütze auch Architekten dabei, Gebäude mit hohem Publikumsverkehr sicherer zu konzipieren. Basierend auf CAD-Daten des Baukörpers generiere die Software automatisiert ein 3-D-Modell. Die Autoren behandeln die Optimierung von Bestandsgebäuden und -systemen, ein virtuelles Training für Ersthelfer und die dynamische Evakuierung bei Bränden. In Zukunft könnte das Gebäudemanagementsystem sogar direkt an das Computersystem der Feuerwehr gekoppelt werden.

Gefahrenmeldeanlagen

Dipl.-Ing. (FH) Dieter Fischer, Telefonbau Arthur Schwabe GmbH & Co. KG, thematisiert in s+s report (Ausgabe 1-2015, S. 42/43) die **Neuaufschaltung von Gefahrenmeldeanlagen** in Zeiten von NGN und EN 50518. Der Monteur müsse in der Lage sein, bei zwangsweise als Netzabschluss beigestellten Routern für die Alarmübertragung gefährliche Funktionen zu erkennen und sicher abzuschalten. Er müsse auch prüfen, ob die Stromversorgung auch aus dem Übertragungsgerät erfolgen kann. Und er müsse in der Lage sein, selber die Funktion der Übertragungsstrecke mittels anerkannter Messgeräte zu bewerten und dadurch gegenüber dem Provider-Personal ein kompetenter Gesprächspartner zu sein.

Gefahrenmelderzentrale

In der Ausgabe März 2015 der Zeitschrift GIT stellt das Unternehmen ABB die KNX-Gefahrenmelderzentrale GM/A 8.1 vor, die die **Integration von Alarmtechnik und Gebäudesystemtechnik** ermögliche. Sie lasse sich vollständig in den weltweiten KNX-Standard integrieren und erfülle gleichzeitig alle internationalen Normanforderungen der Alarmtechnik. Durch ihren breiten Einsatzbereich eigne sie sich für Projekte mit einfachen bis hohen Sicherheitsanforderungen. Durch das Scharfschalten der Alarmanlage würden auch Automatikfunktionen der Gebäudesystemtechnik ausgelöst, Stromkreise abgeschaltet, Rollläden tageszeitabhängig geschlossen, die Beleuchtung ausgeschaltet oder die Anwesenheitssimulation gestartet. Die GMZ verfüge über alle notwendigen Systemschnittstellen. Über einen Ethernet-Anschluss könne der Handwerker und der Nutzer mit einem Standard-Webbrowser auf den integrierten Webserver zugreifen. Die hier hinterlegte Softwareapplikation diene zur Parametrierung, Diagnose und Bedienung der Alarmfunktionen. Die GM/A 8.1 verwalte maximal fünf logische Sicherheitsbereiche. In Projekten, in denen sie als Gefahrenwarnanlage eingesetzt wird, könnten auch über KNX weitere Meldergruppen angeschlossen werden. Für die Notstromversorgung könnten zwei 18 Ah-Akkus an die Zentrale angeschlossen werden. Vom Einbruchschutz über die Überfallalarmierung bis zur Überwachung von technischen Gefahren, alles könnte ohne Spezialsoftware durchgeführt werden (S. 52/53).

Geschäftsrisiken

Alle Jahre befragt die Allianz Versicherung Risiko-Manager aus mehr als 40 Ländern nach den größten Geschäftsrisiken, meldet COMPUTERWOCHE.de am 6. März. 2015 hätten 17 Prozent der 516 Befragten Cyber-

kriminalität, Spionage und Datenmissbrauch als das größte Risiko bezeichnet. Unter den zehn größten Risiken liege die IT-Sicherheit auf Platz 5. Die größte Bedrohung sähen die Manager in der Betriebs- und Lieferkettenunterbrechung (46 Prozent), gefolgt von Naturkatastrophen (30 Prozent), Feuer und Explosion (27 Prozent) sowie rechtlichen Veränderungen (18 Prozent).

ID-Sicherheit

HID Global hat nach einer Meldung in Ausgabe 1-2015 der Fachzeitschrift WiK sechs zentrale **Technologietrends für den Markt der ID-Sicherheit** im Jahr 2015 formuliert: Innovationen auf Basis interoperabler Technologien, die neue vernetzte Lösungen ermöglichen; Einführung neuer „Credentials-" Formfaktoren; neue Möglichkeiten zur Öffnung von Türen; Verbesserungen bei der Verwaltung von Identitäten; verstärkte Nutzung biometrischer Verfahren; wachsende Popularität von vernetzten Geräten und Applikationen im Bereich „Internet der Dinge". Bei einzelnen Branchen würden u. a. folgende Trends gesehen:

- Einzelhandel: Abwehr von Datendiebstahlversuchen, mobile Identifizierung, integrierte biometrische Authentifizierung; Drucker zur Sofort-Ausgabe von Kundenkarten

- Finanzwesen: zunehmendes Verschmelzen physischer Zutritts- und logischer Zugangskontrolle zu einheitlichen Lösungen; zunehmende Bedeutung biometrischer ID-Verfahren

- Transportwesen: IP-basierte Zugangskontrolle gewinnt weiter an Bedeutung.

IT-Sicherheit

Ausspähungsrisiken durch das „Internet der Dinge" beschreibt das Magazin Focus am 28. Februar. Die IT-Branche sei sich einig: 2015 werde das Jahr des Internet of Things. Die in den USA für Telekommunikation zuständige Behörde FTC warne vor massiven Risiken für Sicherheit und Privatsphäre, die sich durch das Internet der Dinge ergeben. Websites wie Opentopia oder NSA Simulator sammelten Hunderte von zugänglichen Kameras. Das Ausspionieren fremder Webcams sei in gewissen Foren mittlerweile beinahe zum Volkssport geworden. Die Suchmaschine Shodan liste die IP-Adressen von zahllosen vernetzten Druckern, Kühlschränken, Webcams und Klimaanlagen auf. Wenn man die Adressen hat, könne man die Geräte mit dem nötigen Know-how auch manipulieren. Forscher der Columbia University hätten eine Schwachstelle im Smart-TV-Protokoll HbbTV entdeckt, durch die Angreifer die komplette Kontrolle über das heimische WLAN erobern können.

Im Zusammenhang mit der Übernahme der Secusmart GmbH durch Blackberry habe Blackberry dem BSI gestattet, den Quellcode des Blackberry-Betriebssystems einzusehen, meldet der Behörden Spiegel in seiner Februar-Ausgabe. Damit könne das BSI nachvollziehen, ob Hintertüren im System eingebaut sind. Solche Prüfrechte des BSI, die es auch nach dem Entwurf für das IT-Sicherheitsgesetz in speziellen Fällen geben soll, stießen nicht uneingeschränkt auf Begeisterung bei IT-Unternehmen. Unternehmen wie IBM, Oracle oder Apple sähen das Ganze kritisch. Blackberry solle sich zudem verpflichtet haben, Sicherheitslücken im Betriebssystem der Regierung zu melden.

Auf der CeBIT im April werde ein neuer **Standard zur Zertifizierung und Testierung von Cybersecurity** vorgestellt, berichtet der Behörden Spiegel in seiner Februar-Ausgabe.

Ein Konsortium aus IT- und Cyberexperten unter Federführung der VdS Schadenverhütung, deren Alleingesellschafter der GDV ist, habe ein auf KMU zugeschnittenes Verfahren entwickelt, mit der der „Informationssicherheitsstatus" eines Unternehmens auditiert und zertifiziert werden könne (Richtlinie 3473). Ein VdS-Zertifikat solle unter anderem auch Versicherern zur Risikoeinschätzung beim Angebot für Deckungen von Cyberschäden dienen. Für KMU biete der Spezialversicherer Hisox zum Beispiel seit 2011 eine „Cyberpolice" an.

COMPUTERWOCHE.de befasst sich am 4. März mit dem geplanten **IT-Sicherheitsgesetz** und seinen Folgen. Es solle die notwendige IT-Security für kritische Infrastrukturen gesetzlich verordnen. Vor allem die Anbieter von Informationstechnik seien nun ausdrücklich vom Anwendungsbereich erfasst. Sie würden deshalb in zweifacher Hinsicht berührt: Als Dienstleister für Unternehmen aus den relevanten Sektoren müssten sie – aufgrund vertraglicher Übereinkunft mit ihren Kunden – die sektorspezifischen Anforderungen erfüllen. Gleichzeitig würden sie als Betreiber kritischer Infrastrukturen (KI-Betreiber) eingestuft, sodass sie aus diesem Grund die sektorspezifischen Vorgaben für IT-Dienstleister umsetzen müssen. Einzelheiten zum Anwendungsbereich und zum Adressatenkreis würden in einer Rechtsverordnung festgelegt. Die Gesetzesbegründung führe dazu aus, dass die Rechtsverordnung qualitativ bestimmte Leistungen als kritisch einstuft, und zudem verpflichte das Gesetz Unternehmen dazu, einen Mindeststandard an IT-Sicherheitsmaßnahmen einzuführen. Wie genau dieser Mindeststandard aussehen soll, sei derzeit noch nicht klar. Es solle im Nachgang durch ein Expertengremium ermittelt werden. Aktuell spreche vieles dafür, dass sich der Mindeststandard an den Vorgaben der ISO-Normen und des BSI-Grundschutzes orientieren wird. Ferner sehe das Gesetz eine Pflicht zur Meldung von Cyber-Security-Incidents vor. Bereits bei einer potenziellen Bedrohung für die kritische Infrastruktur müsse eine Meldung an das BSI erfolgen, wobei hier der Name des KI-Betreibers nicht genannt werden müsse. Kommt es aber zu einer tatsächlichen Beeinträchtigung, sei der KI-Betreiber namentlich zu nennen. Der aktuelle Vorschlag des Gesetzes führe über eine Änderung des Telemediengesetzes die Vorratsdatenspeicherung wieder „durch die Hintertür" ein.

Eine neu entdeckte Sicherheitslücke mit dem Namen **„Freak Attack"** mache Millionen von Internetnutzern anfällig für Hacker-Angriffe, heißt es in der FAZ am 5. März. Betroffen seien Nutzer von Apple-Geräten und Produkten mit dem zu Google gehörenden Betriebssystem Android. Sie könnten zum Ziel von Hackern werden, wenn sie bestimmte Internetseiten aufrufen. Nutzer dieser Seiten seien der Gefahr ausgesetzt, dass vertrauliche Informationen wie Passwörter gestohlen werden.

Markus Pfister, In&Out AG, befasst sich in Ausgabe 1-2015 der Zeitschrift Sicherheitsforum mit Frameworks, unabdingbaren **Navigationssystemen für die IT-Sicherheit** (S. 33–35). Der Einsatz empfehle sich aus folgenden Gründen: prozessorientiert, dauerhafte Verbesserung, vom Gesetzgeber anerkannt, Templates und Tools vorhanden, erleichtert die Zusammenarbeit mit Geschäftspartnern. Der Autor behandelt den IT-Grundschutz als Vorleistung für ISO-Zertifizierung, die ISO Normen 27001 und 27002, die Zertifizierung, COBIT (Control Objectives for Information and Related Technology, ein IT-Governance-Framework) und ITIL (eine Sammlung von Best Practices zur Implementierung eines IT Service Managements).

Wegen der wachsenden Zahl von Straftaten im Internet habe das Bundeskabinett ein ressortübergreifendes **Forschungsprogramm für mehr Sicherheit im Internet** beschlossen, meldet die FAZ am 12. März. Das Programm „Sicher und selbstbestimmt in der digitalen Welt" werde das BMBW bis zum Jahr

2020 mit etwa 180 Mio. Euro fördern. Das Programm bündle alle einschlägigen Aktivitäten und fördere die Entwicklung von Lösungen für Bürger, Wirtschaft und den Staat. Es werde sich auf vier Schwerpunkte konzentrieren: neue Technologien, sichere und vertrauenswürdige Informations- und Kommunikationssysteme, Anwendungsfelder der Sicherheit sowie Privatheit und Schutz von Daten. Derzeit würden das Bezahlen im Internet, das Verschicken von privaten Nachrichten, das Einloggen bei Facebook durch Verschlüsselungsverfahren gesichert, die dem Leistungsniveau derzeit existierender Computer entsprechen. Neue Computergenerationen würden jedoch noch unerreichte Rechenleistungen realisieren können. Deshalb seien neue Sicherheitsvorkehrungen nötig geworden. Bei der sogenannten „Quantenkommunikation" könne jedes „Mithören" vom Empfänger bemerkt werden. Diese Technologie werde das Rahmenprogramm in besonderer Weise fördern. Zu den sensibelsten Angriffszielen gehörten Industrieanlagen sowie kritische Infrastrukturen wie Strom- und Wasserversorgung, die ausspioniert werden könnten. Das Risiko für die Unternehmen werde immer größer. In einer Großstadt wie Berlin würde ein einstündiger Stromausfall zur Mittagszeit infolge eines Hackerangriffs zu einem Schaden von bis zu 23 Mio. Euro führen. Die Folgen für kritische Infrastrukturen – etwa in der Medizin, vor allem für Krankenhäuser – würden weit schwerer wiegen. Zu den sensiblen Bereichen gehörten auch Angriffe auf Computer der Nahrungsmittelindustrie, bei denen die Zusammensetzung von Speisen unbemerkt verändert werden könnte. Ziel der Forscher sei, eine Methode zu entwickeln, die eine Auswertung von Daten in verschlüsselter Form erlaube.

Christophe Birkeland und Michael Hartmann, beide Blue Coat Norway AS, gehen in dem Verlagsspezial „ITK 2015" der FAZ am 12. März der Frage nach, welche **Mindeststandards** IT-Systeme von Unternehmen einhalten müssten, um die Sicherheit ihrer Infrastruktur zu gewährleisten. Folgende fünf Mindeststandards seien unerlässlich: 1. Unternehmen müssten einen größeren Einblick in den Traffic des ganzen Netzwerks sicherstellen, um Auffälligkeiten zu erkennen und direkt Inhalte einsehen zu können. Nur so würden die zugrunde liegenden Auslöser und das Ausmaß des Angriffs erkannt. 2. Unternehmen müssten prüfen, welche Maßnahmen sie zur Identifizierung unbekannter oder neuartiger Bedrohungen einsetzen, die ihre signaturbasierten Schutzvorkehrungen umgehen können. 3. Eine Balance zwischen der Minderung des Bedrohungsrisikos in verschlüsseltem Traffic, der Gewährleistung der Netzwerk-Performance und der Einhaltung von Datenschutzbestimmungen sei heutzutage für jedes Unternehmen unabdingbar. 4. Noch wichtiger als für herkömmliche Unternehmen sei die Implementation strenger Sicherheitsvorkehrungen für die Betreiber kritischer Infrastrukturen. 5. Allgemein müssten sich Unternehmen nachhaltiger in kollektive Threat Intelligence einbringen und einbinden: ob durch ein informelles Teilen von Informationen oder dadurch, dass die eigene Netzwerksicherheitsinfrastruktur zu einem großen Threat-Intelligence-Netzwerk beiträgt – jeder Netzwerkeffekt vermittle schneller, mehr und qualitativ bessere Informationen zu Bedrohungen und Sicherheitslösungen. Die Wochenzeitung Das Parlament lässt in ihrem Bericht zur Bundestagsberatung über den Entwurf eines IT-Sicherheitsgesetzes vom 23. März (S. 1) Konstantin von Notz zu Wort kommen: „Im Bereich der IT-Sicherheit brennt in Deutschland die Hütte lichterloh." Ein Risiko für Betriebs- und Geschäftsgeheimnisse stelle aber nicht nur die OK dar, „sondern auch die sich verselbstständigenden Geheimdienste und ihnen gefällig zuarbeitende Unternehmen". Wie sehr die Sicherheit bedroht werde, belegten nach den Worten von Stephan Mayer (CSU) die Zahlen des BSI. So gebe es weltweit derzeit mehr als 250 Mio. verschiedene Varianten von Schadstoffprogrammen. Tagtäglich kämen etwa 300.000 neue hinzu. Dennoch hätten viele Firmen den Ernst der Lage offenbar noch nicht erkannt.

Noch nie waren Netze, die damit verbundenen Geräte und die Nutzer so angreifbar wie heute, schreibt die FAZ am 18. März. Das Sicherheitsunternehmen Sophos simuliere auf der CeBIT mit seinem Eisenbahnsystem **Honeytrain** das ungeschützte Steuerungssystem eines öffentlichen Nahverkehrsbetriebs. Die Security-Tochtergesellschaft des Halbleiterherstellers Intel präsentiere eine Sicherheitslösung, um sogenannte kritische Infrastrukturen zu schützen. Die Energiewirtschaft sei auf Cyberangriffe nicht ausreichend vorbereitet. Nach einer Studie hätte von 200 befragten Entscheidern fast ein Drittel keine besonderen Sicherheitsvorkehrungen für die Kontrolle intelligenter Netze getroffen, obwohl wiederum ein Drittel der Befragten mit einem großen Sicherheitsvorfall innerhalb der nächsten zwölf Monate rechne.

Nach einem Bericht in der FAZ vom 17. März entstehen Deutschland durch Hackerangriffe Jahr für Jahr Schäden in Milliardenhöhe. Der Cybersicherheitsrat schätze sie auf bis zu 50 Mrd. Euro. Nach den Worten von Minister Gabriel bremsten gerade in Kleinbetrieben Bedenken in Fragen der Datensicherheit die Digitalisierung. Der Mittelstand scheue noch zu oft davor zurück, Produktion und Dienstleistung stärker zu vernetzen und die dabei anfallenden Datenberge wo nötig auch in fremde Hände zu geben. Nach den Worten von Jadran Mesic, für die Analyse von Cyberangriffen zuständiger Abteilungsleiter im Verfassungsschutz, hätten Spione in Deutschland vor allem Automobil- und Rüstungskonzerne sowie Forschungseinrichtungen im Visier. Ende 2014 seien rund 6.500 Software-Schwachstellen bekannt gewesen, heiße es in einer Untersuchung des Potsdamer Hasso Plattner-Instituts für Softwaresystemtechnik. Viele kritische Schwachstellen beträfen Internet-Browser, die gern für Angriffe genutzt werden. Für den Internet Explorer von Microsoft seien 700 solcher Schwachstellen gezählt worden. Bei Chrome von Google 600 und beim Firefox von Mozilla 570.

In einer Sonder-Ausgabe Cybersicherheit mit Stand vom 13. März informiert das BSI:

Das BSI wurde über eine **Steuerungskomponente** eines Schwimmbades informiert, die unmittelbar mit dem Internet verbunden war. In diesem Zusammenhang rät das BSI:

- Eine Steuerungskomponente gehört nicht direkt mit dem Internet verbunden.
- Zugänge dürfen gerade bei Steuerungsanlagen nicht einfach gesperrt werden.
- Externe Zugänge sollten nur dann eingerichtet werden, wenn eine echte Erfordernis vorliegt.
- Ein externer Zugang sollte mittels VPN-Technologien abgesichert werden, um eine Zugangsbeschränkung und die Vertraulichkeit und Integrität der kommunizierten Daten zu gewährleisten. Jedem Nutzer sollte ein individuelles und hinreichend sicheres Passwort zugewiesen werden.
- Eine Aushebelung des Zugriffsschutzes, insbesondere wenn dieser in der Steuerung schon vorhanden ist, verbietet sich in jedem Fall. Darüber hinaus werden solche Umgehungen häufig nicht wieder entfernt, wenn sie erst einmal implementiert sind.

Distributed Denial of Service (DDoS)-Attacken gehören, wie das BSI in dem Sonderbericht ausführt, zu den am häufigsten beobachteten Angriffsmustern im Cyberraum. Mit gezielten Maßnahmen können die Auswirkungen für Opfer jedoch signifikant reduziert werden. Dazu stellt das BSI eine Checkliste auf:

- Bilden Sie ein Krisenreaktionsteam aus erfahrenen Mitarbeitern des IT-Betriebs, den IT-Sicherheitsteams, dem IT-Sicherheitsbeauftragten sowie der Presse- und Öffentlichkeitsarbeit.
- Berichten Sie den Vorfall entsprechend Ihrer internen Richtlinie zur Eskalation an das Management.
- Binden Sie den eigenen Internet-Serviceprovider bzw. Hostingprovider frühzeitig ein.
- Sie sollten ihr Justiziariat oder ihren Anwalt einschalten und Strafanzeige erstatten.

- Für die Presse- und Öffentlichkeitsarbeit müssen Informationen zum Vorfall aufbereitet werden.
- Vertragspartner und/oder Kunden sollten über die möglichen Einschränkungen der Verfügbarkeit informiert werden.
- Berichten Sie den Vorfall an das BSI.

In demselben Sonderbericht Wirtschaftsschutz wird dargelegt, einer Arbeitsgruppe der israelischen Firma ALUMNI sei es unter Laborbedingungen offensichtlich gelungen, ein von Mobilfunkanbietern angebotenes nachrüstbares Funk- und Sicherheitsmodul für Fahrzeuge zu kompromittieren. Die dabei erkannte Sicherheitslücke eröffnet demzufolge den Zugriff auf die OBD-2-Schnittstelle von Fahrzeugen. Über diese Schnittstelle bestünde dann auch die Möglichkeit der Manipulation von Sicherheitskomponenten des Fahrzeugs. Das Produkt soll auch älteren Fahrzeugen die Funktionalität des „vernetzten Autos" geben und dazu beitragen, das Fahren sicherer, einfacher und sparsamer zu machen. Durch die erkannte Sicherheitslücke könnte das Produkt jedoch von Cyberkriminellen für deren Zwecke missbraucht werden.

Sicheren Daten- und Informationsaustausch über öffentliche Netze thematisiert Thomas Buch, Rohde & Schwarz SIT, in s+s report (Ausgabe 1-2015, S. 44–49). Er gibt eine Übersicht über die Vorgehensweisen krimineller Akteure, über Gesetzesanforderungen und -vorhaben und liefert konkrete Ansätze für den sicheren Datenaustausch zwischen den Schutzobjekten und den Serviceprovidern. Top-Bedrohungen in Industrie- oder Produktionssteuerungsanlagen seien: Infektion mit Schadsoftware über Internet und Intranet, Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware, Social Engineering, menschliches Fehlverhalten und Sabotage, Einbruch über Fernwartungszugänge, mit dem Internet verbundene Steuerungskomponenten, technisches Fehlverhalten, Kompromittierung von Smartphones im Produktionsumfeld, Kompromittierung von Extranet und Cloud-Komponenten sowie DDoS-Angriffe. Er zeigt, gegen welche Cyberrisiken sich Kunden versichern können und empfiehlt folgende Schutzmaßnahmen: Einsatz vertrauenswürdiger IT-Sicherheitssysteme , Vorlage von Zertifizierungs- und Zulassungsstandards der Hersteller und die Einbindung von Herstellern und Systemintegratoren in die Erarbeitung von IT-Sicherheitskonzepten.

IuK-Kriminalität

In einer Pressemitteilung des BKA vom 25. Februar heißt es: „Das Bundeskriminalamt hat den in Deutschland gehosteten Teil der Netzinfrastruktur eines weltweiten Botnetzes von Cyberkriminellen deaktiviert. Diese Maßnahme war Teil von internationalen Ermittlungen in Großbritannien, Italien und den Niederlanden, die auch von mehreren IT-Firmen unterstützt wurden. Die Arbeitsgruppe „Joint Cybercrime Action Task Force (J-CAT)" des European Cybercrime Centre (EC3) von Europol hatte das gemeinsame Vorgehen koordiniert. Nach bisherigen Erkenntnissen waren weltweit 3,2 Mio. Computersysteme Teil des sogenannten Ramnit-Botnetzes."

Ein Drittel der Unternehmen in Deutschland habe 2014 einen digitalen Angriff entdeckt, meldet COMPUTERWOCHE.de am 25. Februar. Das habe eine repräsentative Umfrage des IT-Verbandes BitKOM unter gut 450 Firmen ergeben. Fast zwei Drittel der attackierten Firmen hätten angegeben, dass die Angriffe vor Ort geschehen seien. 40 Prozent der betroffenen Unternehmen hätten Angriffe auf ihre IT-Systeme über das Internet verzeichnet. KMU würden häufiger Opfer von Angreifern. BitKOM rate Unternehmen, spezielle Software zum Aufspüren von Angriffen einzusetzen und ihre Systeme regelmäßig zu überprüfen. Hackerangriffe fielen bei den betroffenen Unternehmen mitunter lange Zeit nicht auf. Wichtig seien technische Vorkeh-

rungen wie der Grundschutz mit aktuellen Virenscannern und Firewalls.

Laut einer Umfrage von KPMG habe der **Gesamtschaden in Deutschland allein 2014 durch Cyberkriminalität 54 Mrd. Euro** betragen (FAZ vom 11. März). Als häufigstes hätten sich die Täter bargeldlose Zahlungssysteme ausgesucht: 30 Prozent aller Delikte seien auf diesen Bereich entfallen. 55 Prozent aller Finanzdienstleister seien 2014 virtuell attackiert worden. Quer durch alle Branchen seien 2014 rund 40 Prozent aller Unternehmen betroffen, nach 27 Prozent 2013. Neun von zehn Unternehmen sähen generell ein hohes Risiko für deutsche Unternehmen, Opfer von Cyberverbrechen zu werden. Dagegen schätze weniger als die Hälfte die eigene Gefährdungslage als hoch ein. Viele Unternehmen treibe nicht nur die Sorge um, dass eigene Mitarbeiter als Computerkriminelle auftreten könnten. Vielmehr würden die Beschäftigten auch als diejenigen gelten, die aus Leichtsinn oder Unkenntnis Attacken erst ermöglichen. Als besonders risikobehaftet werde die Handynutzung und die dienstliche E-Mail-Kommunikation eingeschätzt. Für Mittelständler könne eine Computerattacke möglicherweise existenzgefährdend sein. Die Verletzung von Geschäfts- und Betriebsgeheimnissen sowie von Urheberrechten führten im Durchschnitt jeweils zu rund 600.000 Euro Schaden. Rund 90 Prozent der Befragten beobachteten, dass die Vorfälle immer komplexer werden.

Melissa Hathaway, ehemalige Beraterin von Präsident Obama, äußert sich zu möglichen **Hackerangriffen auf die Strom- und Wasserversorgung** (FAZ vom 7. März). Nicht nur die Industrie sei gefährdet. Wenn das Stromnetz oder die Wasserversorgung sabotiert würde, könne noch viel mehr passieren. Hacker könnten von jedem beliebigen Punkt der Welt aus Staatsfinanzen korrumpieren. Sie könnten Flugzeuge und Schiffe manövrieren. Sie seien sogar dazu in der Lage, Geschütze, Panzer, Raketen oder Drohnen zu kontrollieren. Cyberangriffe seien zur alltäglichen Bedrohung vor allem der Hochtechnologie-Nationen geworden. Kein Land sei auf die Angriffe vorbereitet. Es müsse Kontrollen dafür geben, ob neue Technik mit einem ausreichenden Blick auf Sicherheit entwickelt worden ist. Hathaway spricht von einem Technik-TÜV.

Auf die gleichermaßen kuriose wie gefährliche Schwachstelle **FREAK** weist zeit.de am 6. März hin. Sie bewirke, dass Angreifer vermeintlich sichere Verbindungen im Internet abhören und schlimmstenfalls Passwörter und ähnlich sensible Daten abfangen können. Der Name stehe für Factoring attack on RSA-EXPORT Keys. Die Schwachstelle gehe auf die Jahre zurück, als es US-Firmen noch verboten gewesen sei, effiziente Verschlüsselungstechnik ins Ausland zu verkaufen. Infolgedessen sei auch die Export-Version der RSA-Verschlüsselung abgeschwächt worden. Die Exportbeschränkungen seien Ende der neunziger Jahre zwar aufgehoben worden, die unsichere Verschlüsselung sei allerdings nie komplett verschwunden. Sie werde nach wie vor von aktueller Server- und Anwender-Software unterstützt. Unsicher seien der Internet Explorer, Safari, der Standard-Android-Browser, der Blackberry Browser, Chrome, iCab, Mercury sowie Opera und der UC Browser.

Ende Februar habe eine Sondereinheit, die von Europol geleitet und von Symantec, Microsoft und anderen Branchenpartnern unterstützt worden sei, Server und die IT-Infrastruktur der Gruppe von Cyberkriminellen hinter dem **„Ramnit-Botnetz"** beschlagnahmt, berichtet der Behörden Spiegel in seiner März-Ausgabe. Während einer fünfjährigen Aktivität habe sich das Ramnit-Botnetz zu einem hochkriminellen Unternehmen entwickelt, das mehr als 3,2 Mio. Computer infiziert und Bankdaten, Passwörter, Cookies und persönliche Daten der Opfer abgegriffen habe. Die Kooperation der Polizeien mit IT-Sicherheitsspezialisten habe dazu geführt, dass die „Command and Control"-Server vom

Netz genommen und 300 Internet-Domänen der Täter umgeleitet wurden. In derselben Ausgabe wird darüber berichtet, dass seit dem Jahr 2001 die von Kaspersky Labs „Equation-Group" getauften Hacker Computer und IT-Systeme mehrerer Tausend Opfer in über 30 Ländern weltweit aus Regierungsinstitutionen und Unternehmen verschiedener Branchen infiltriert hätten. Die Kriminellen seien in annähernd all ihren Aktivitäten einzigartig, da sie Werkzeuge nutzen würden, die sehr kompliziert und kostenintensiv zu entwickeln sind. Darüber hinaus habe die „Equation-Group" auch klassische Spionage-Taktiken genutzt, um böswilligen Code bei ihren Opfern zu platzieren. Zur Infektion seien eine Reihe von Implantaten (Trojanern) eingesetzt worden. Zwei Module seien entdeckt worden, mit denen die Neuprogrammierung der Festplatten-Firmware bei einem Dutzend beliebter Festplattenhersteller möglich sei. Der sogenannte „Fanny-Wurm" habe den Zweck, die Topologie eines Netzwerkes, das nicht über eine Leitung erreichbar ist, zu erfassen.

Die **Malware PoSeidon gefährdet Kassensysteme**, meldet silicon.de am 25. März. Cisco habe die Malware entdeckt. PoSeidon könne via „Memory Scraping" PINs von Kunden abgreifen. Dabei werden diese eigentlich nicht im Kassensystem gespeichert. Allerdings sammele PoSeidon nicht nur PINs, sondern sämtliche Kreditkartendaten. Sie verfüge außerdem über einen Keylogger und könne somit Tastatureingaben aufzeichnen. Anschließend sende die Malware die Informationen an fremde Server. Viele davon stehen Cisco zufolge in Russland. Mit den Daten erstellten die Kriminellen dann falsche Kredit- und Kontodaten. Kassensysteme würden zwar Kreditkartendaten für die Übertragung an einen Bezahldienst verschlüsseln. Allerdings müssten sie zu einem Zeitpunkt einmal als Klartext vorliegen – sicherheitshalber nicht auf der Festplatte, sondern im flüchtigen Speicher. Kriminelle, die diesen Speicher im richtigen Moment auslesen, könnten die nötigen Daten unverschlüsselt abfangen. Dieses Verfahren heiße „Memory Scraping".

Kartenbetrug

Das BKA habe in Hanau zwei mutmaßliche Anführer einer rumänischen Fälscherbande festgenommen, meldet die FAZ am 28. Februar. Die Gruppe soll 2014 in ganz Deutschland an Tankstellen **Zapfautomaten manipuliert** haben, um durch ein kleines Zusatzgerät die Daten auf den Magnetstreifen der Kunden abzugreifen. Zugleich sollen sie deren Geheimnummern ausgespäht haben. Mit diesen Daten hätten sie dann gefälschte Kartendubletten hergestellt, um damit in Deutschland sowie sechs weiteren europäischen Ländern zu tanken. Der dadurch verursachte Schaden habe den Ermittlungen zufolge 3,5 Mio. Euro betragen. Bereits Ende 2014 hätte die Polizei fünf Mitglieder des mutmaßlichen Fälscherrings in Deutschland verhaftet.

Betrug mit Prepaid-Karten thematisiert die FAZ am 21. März. Prepaid-Karten hätten nur ein Sicherheitsmerkmal: den Strichcode. Der stehe auf der Karte und auf der Verpackung. Eine Masche von Betrügern könne also sein: Sie nehmen die Karte vom Pappträger ab und kleben eine andere darauf. Sie hoffen dann darauf, dass jemand anders den Strichcode auf dem Pappträger aktiviert und der Verkäuferin der unterschiedliche Barcode nicht auffällt. Dann hätte der Betrüger eine aufgeladene Karte griffbereit zum eigenen Einkauf in der Tasche. Der sich reich beschenkt fühlende Kunde habe nur den Kartenträger aufgeladen, aber ihm fehle die passende Karte. Die habe der Betrüger. Von Banken ausgegebene Giro- und Kreditkarten seien seit 2010 zusätzlich zum Strichcode oder Magnetstreifen noch durch einen EMV-Chip gesichert. Der Magnetstreifen diene damit nur noch als „Türöffner" in Filialen und bei Zahlungen in bestimmten außereuropäischen Ländern. Die Daten im EMV-Chip seien so

aufwendig verschlüsselt, dass er momentan nicht zu knacken sei. Und der Chip werde weiterentwickelt. Die nächste Generation habe nicht mehr statische Kryptogramme, sondern elliptische. Der Code von Online-Gutscheinen sei insofern sicherer als Prepaid-Karten, als es keine Karte, damit keinen Strichcode und keinen Kartenträger gibt. Der Code, meist eine Nummer, müsse freigelegt werden. Noch wichtiger: Guthabenkarte und Gutschein könnten anders als Guthabenkarte und Pappkartenträger nicht voneinander getrennt werden.

Korruption

Der Behörden Spiegel meldet in der Februar-Ausgabe, dass die Bundesregierung den Entwurf eines Gesetzes zur Bekämpfung der Korruption beschlossen habe, der das deutsche Strafrecht an die Vorgaben aus dem EU-Rahmenbeschluss zur Bekämpfung der Bestechung im privaten Sektor anpasse. Bisher scheide die Strafbarkeit nach § 299 StGB aus, wenn es an einer Wettbewerbsverzerrung fehlt. Nach den Vorgaben der EU müssten aber auch die Fälle strafbar sein, in denen es nicht zu einer Wettbewerbsverzerrung, sondern nur zu einer Verletzung der Pflichten gegenüber dem Geschäftsherrn kommt.

Krisenregionen

Pascal Michel, Result Group GmbH, befasst sich in Ausgabe 1-2015 der Fachzeitschrift WiK (S.18–21) mit Fragen der **Gebäudesicherheit in Krisengebieten**. Nach Aussagen der US-Behörden habe es 2013 weltweit 950 registrierte Terroranschläge gegen Firmen gegeben (2003: 170), davon 112 gegen Firmengebäude. Der Schutz eines Gebäudes in einem (möglichen) Krisengebiet setze sich aus mehreren virtuellen und physischen Schutzkreisen zusammen. Lageinformationen und Lagemonitoring bildeten den ersten Schutzring. Einen weiteren Schutzkreis bildeten die „Community Relations", Maßnahmen, die darauf abzielten, die Akzeptanz bei der lokalen Bevölkerung zu erhöhen und diese in die Firmenaktivitäten vor Ort einzubinden. Glasflächen erhöhten das Risiko bei einer Explosion. Experten schätzten, dass 80 Prozent der Verletzungen und Todesopfer durch Sekundärsplitter entstehen. Bei der Detonation einer Autobombe mit 220 kg TNT reiche die tödliche Druckwelle unter Laborbedingungen 30 Meter, Splitterverletzungen seien sogar bis zu einer Entfernung von fast 400 Metern möglich. Notwendig sei auch eine Notfallplanung auf der Mitarbeiterebene. Diese umfasse unter anderem das Vorhalten einer erweiterten Erste-Hilfe-Ausstattung, die Bereitstellung von Schutzwesten und ein entsprechendes Training.

Eine BKA-Lageanalyse für die Wirtschaft vom 20. März befasst sich mit der **Terrorismuslage in Tunesien**. Am 18. März haben mindestens zwei in Militäruniformen gekleidete und mit Schnellfeuergewehren bewaffnete Personen das Parlamentsgebäude in Tunis angegriffen, um einen Anschlag auf das zeitgleich zum Thema Antiterror-Gesetzgebung tagende Parlament zu verüben. Die Täter konnten von den Sicherheitskräften des Parlaments am Eindringen in das Gebäude gehindert werden und flüchteten anschließend ins direkt neben dem Parlament gelegene Nationalmuseum von Bardo. Bei ihrer Flucht töteten sie bereits auf dem Vorplatz des Museums mehrere Personen und nahmen im Museum Geiseln. Das Gelände wurde am selben Nachmittag durch tunesische Sicherheitskräfte gestürmt, wobei die beiden Attentäter erschossen wurden. Bei dem Angriff sind laut Presseberichten mindestens 25 Menschen ums Leben gekommen, darunter auch westeuropäische Touristen. Am 19. März konnte eine Bekennung des IS im Internet gesichert werden. Gegenwärtig müsse – wie auch in anderen Staaten Nordafrikas – nicht nur ein zufälliges Mitbetroffensein

westlicher Staatsangehöriger bei entsprechenden Anschlagsgeschehen einkalkuliert werden. Vielmehr sei zu befürchten, dass dieser Personenkreis in den direkten Fokus der vor Ort aktiven Gruppierungen gerückt ist. Der aktuelle Anschlag in Tunis bestätige die vorgenannte Einschätzung und belege zudem, dass terroristische Elemente in Tunesien trotz des repressiven Drucks in der Lage sind, entsprechende Anschlagsvorhaben vorzubereiten und durchzuführen. Im Ergebnis sei festzustellen, dass sich die Sicherheitslage für westliche Ausländer in Tunesien seit Mai 2013 verschärft hat. Deutsche Interessen und Einrichtungen nähmen nach derzeitiger Erkenntnislage im Vergleich zu anderen westlichen Staaten keine herausragende Stellung ein.

Kritische Infrastrukturen

In der Februar-Ausgabe des Behörden Spiegel beschreibt der Präsident des Bundesamtes für Bevölkerungsschutz (BBK) **KritisKAT**, ein Verfahren zur Auswahl von kritischen Infrastrukturen und insbesondere von wichtigen Bestandteilen davon. Hier seien Auswahlkriterien und Schwellenwerte entwickelt worden. Davor habe es lediglich eine Liste von Sektoren und Branchen gegeben. Eine konkrete Bestimmung wichtiger Prozesse und Anlagen habe nicht vorgenommen werden können. Das Bauchgefühl habe entschieden, wer oder was eine konkrete kritische Infrastruktur ist und mit welchen Betreibern im Rahmen eines kooperativen Ansatzes gesprochen werden sollte. Aktuell arbeite das BBK in enger Kooperation mit dem BSI an einem Leitfaden, der die Anwendung des Verfahrens darlegt.

Almut Eger, 4m2s, und Jörg Kretzschmar, Contechnet Ltd., gehen in der Ausgabe 1-2015 der Zeitschrift Sicherheitsforum (S. 61–63) der Frage nach, welche Vorbereitungen und Maßnahmen aus unternehmerischer Sicht für den Schutz kritischer Infrastrukturen nötig und sinnvoll sind. Die Maßnahme müsse ökonomisch sinnvoll sein, einen hohen Nutzen im Ereignis und im Alltag zeigen, den gesetzlichen Anforderungen genügen und in ihrer Wirkung überprüfbar sein. Schutzmaßnahmen machten aus ökonomischer Sicht nur dann Sinn, wenn das Zusammenspiel von Ressourcen und Prozessen gegeben ist.

Logistiksicherheit

Mitte Januar habe das BMVI das mit der Wirtschaft erarbeitete Konzept „**Sicherheitsstrategie für die Güterverkehrs- und Logistikwirtschaft“** vorgelegt, berichtet WiK in der Ausgabe 1-2015, S. 28. Die Strategie richte sich zunächst an die Behörden im Geschäftsbereich des BMVI, für die sie als Handlungsrahmen für die Aktivitäten in der Gefahrenabwehr bei Verkehrsträgern dienen solle. Als konkrete Ziele würden im Konzept u. a. genannt:

- eine verkehrsträgerübergreifende Notfallplanung für ausgewählte Szenarien (u. a. terroristische Anschläge, Extremwetter, langanhaltende Strom- oder IT-Ausfälle)
- Optimierung der Krisenmanagementstrukturen und Einrichtung einer Kommunikationsplattform für Krisenfälle
- Prüfung des Bedarfs zusätzlicher Schutzmaßnahmen bei kritischen Infrastrukturen des Sektors „Transport und Verkehr“, u. a. der betrieblichen Notfallpläne, der Notstromkonzepte, der Standards in der IT-Sicherheit und der Objektschutzmaßnahmen. Bei der Behebung von Sicherheitslücken werde keine pauschale Regulierung, sondern Freiwilligkeit oder eine branchenspezifische Selbstregulierung angestrebt
- verbesserter Transfer von einschlägigen Forschungsergebnissen
- Förderung des Erfahrungsaustausches über bewährte Verfahrensweisen, auch international.

Maschinensicherheit

Andreas Schenk, steute Schaltgeräte, zeigt in der März-Ausgabe der Fachzeitschrift GIT (S. 112/113) die **Vorteile eines kabellosen Bedienschalters**. Wireless-Schaltgeräte würden sich in der gesamten Automatisierungstechnik durchsetzen, seit Neuestem auch in Sicherheitsanwendungen. Für diesen Zweck sei eine eigene sicherheitsgerichtete Funktechnologie entwickelt worden. Sie biete Vorteile wie höhere Flexibilität und verringerten Installationsaufwand. Das Funksystem nutze die physikalische Schicht des Standards IEEE 802.15.1. Aufgrund der hohen Zuverlässigkeit, die u. a. durch das Frequency Hopping Spread Spectrum auf 79 Kanälen und durch das adaptive Frequenzsprungverfahren gewährleistet sei, sowie aufgrund der sehr guten Koexistenz zu anderen Funksystemen eigne es sich insbesondere für den Einsatz in rauen industriellen Umgebungen. Dabei sei das Sender-/Empfänger-Gesamtsystem grundsätzlich zweikanalig ausgelegt. Die Energieversorgung erfolge batteriegestützt. Das schaffe die Voraussetzung für eine hochverfügbare bidirektionale Funkverbindung. Das aus dem Funkfußschalter und der Empfangseinheit bestehende System sei EG-baumustergeprüft und gemäß ISO EN 13849-1 in Performance Level d sowie in das Safety Integrated Level 2 nach IEC 62061 eingestuft. Der Bediener könne den Schalter stets in optimale Position bringen, ohne darauf zu achten, dass er nicht über das Kabel stolpert. Zudem seien die Fußschalter ausgesprochen standfest, Voraussetzung für ergonomischen und intuitiven Betrieb.

Vorgestellt wird in derselben Ausgabe ein **elektronisches Schlüsselsystem** (Electronic Key System). Der besondere Vorteil bestehe darin, dass der Schlüssel in der Schlüsselaufnahme gehalten wird, während Bedien- oder Instandhaltungspersonal an der Maschine arbeitet. Die kontaktlose Übertragung der Daten erlaube den Einsatz der Schlüsselaufnahme im industriellen Umfeld. Der EK habe die Form eines robusten Anhängers. In ihm seien ein Speicherchip und ein Transponder eingebaut. Bei der Schlüsselaufnahme handele es sich um ein Schreib-/Lesesystem mit integrierter Schnittstellenelektronik (S. 114/115).

Ölunfälle

Mit Ölunfällen befasst sich Dipl.-Ing. Gerhard Wochner, Swiss TS Technical Services AG, in Ausgabe 1-2015 der Zeitschrift Sicherheitsforum (S. 40/41). Ölunfälle durch unvollständig ausgerüstete Notstromsysteme oder Bauheizungen kämen leider noch immer häufig vor, obwohl sie leicht zu vermeiden wären. Die Kontrolle durch einen Fachmann zeige Mängel und Gegenmaßnahmen auf und schaffe die notwendige Sicherheit zugunsten von Anlagebetreibern und Umwelt. Die visuellen Kontrollen, Ultraschallmessungen sowie Funktionstests mit Protokoll seien im Ablauf integriert und müssten individuell auf die Einzelkomponenten abgestimmt eingesetzt werden.

Organisierte Kriminalität (OK)

Nach Ermittlungen des Zolls seien immer mehr international vernetzte Kriminelle in Deutschland aktiv, berichtet die FAZ am 13. März. Die illegalen Geschäfte reichten von der Schwarzarbeit auf Baustellen über den abgabefreien Zigarettenhandel bis zum Schmuggel von Rauschgift und Waffen. Auf fast jeder Großbaustelle stoße der Zoll bei seinen Kontrollen auf die Auswüchse von OK. Nahezu alle Bereiche des Wirtschaftslebens seien davon mit steigender Tendenz betroffen. Durch bandenmäßige und flächendeckende Hinterziehung von Sozialversicherungsbeiträgen und Steuern entstünden

dem Staat Schäden in Milliardenhöhe. Der durch den Zoll 2014 aufgedeckte Schaden werde auf mehr als 795 Mio. Euro beziffert. Die international vernetzten Gruppierungen bestünden aus bis zu hundert Kriminellen, die hochgradig konspirativ und abgeschottet vorgehen. Solche Täter seien nur durch komplexe Ermittlungen, intensive grenzüberschreitende Zusammenarbeit und hoch spezialisierte Ermittlungseinheiten zu bekämpfen. 2014 seien 14.657 Ermittlungsverfahren eingeleitet worden, 13.900 wegen mittlerer, schwerer und organisierter Kriminalität. Fast 103.000 Ermittlungsverfahren seien wegen illegaler Beschäftigung eingeleitet worden (2013: 95.020). Der Zoll stelle im Bereich der Schwarzarbeit zunehmend einen hohen Grad organisierter Wirtschaftskriminalität fest. Der Zoll habe 2014 den Schmuggel von 140 Mio. Zigaretten verhindert. Er habe zudem 13,5 Tonnen Rauschgift aus dem Verkehr gezogen, darunter 1,6 Tonnen Marihuana, 1,2 Tonnen Kokain, 674 kg Haschisch und 383 kg Amphetamine. Er habe weiterhin in mehr als 45.000 Fällen verhindert, dass gefälschte Waren in den Verkehr gebracht wurden.

Predictive Maintenance

Wenn ein Fließband, eine Windkraftanlage oder ein Lkw still steht, koste das Geld. Um diese Zeiten zu minimieren, setzten Unternehmen auf Predictive Maintenance, auf Systeme, mit denen sich Ausfälle vorhersagen lassen (Verlagsspezial „ITK 2015" der FAZ am 12. März). Laut einer Studie des amerikanischen Department of Energy könnten mit Hilfe von Instandhaltungsmanagement-Software (Predictive Maintenance) die Wartungszeiten um 25 bis 30 Prozent und die Ausfallzeiten durch Reparatur um 70 bis 75 Prozent reduziert werden. Das amerikanische Lkw-Mietunternehmen Truck Leasing beispielsweise habe seine komplette Flotte mit Sensoren versehen, die Daten über den Reifendruck, den Turbolader und die Fahrweise übermitteln. Schlägt das High-Performance-Analyticsystem Alarm, dass in 1.000 km ein Reifen platzen oder die Handbremse versagen könnte, könne die Disposition den Fahrer etwa zu einer Raststätte mit angeschlossener Werkstatt umleiten und die notwendigen Ersatzteile dort anliefern lassen. Ein Unfall, größere Schäden und lange Stillstandszeiten würden durch dieses „Frühwarnsystem" vermieden. Doch die „Big Data-Wahrheit" beginne bereits früher: bei der Herstellung von Produkten. Durch die Erhebung und Auswertung von durch Maschinen, Anlagen und im Herstellungsprozess befindlichen Gütern generierte Daten lasse sich schon während der Fertigungsprozesse die Qualität der gerade produzierten Teile kontrollieren. Mit der „Maschine/Maschine-Kommunikation", mit dem „Internet der Dinge" erwarteten Fachleute einen wahren Run auf Analysetools, mit denen demnächst auftretende Mängel an Produkten, die gerade hergestellt werden, vorhergesagt werden könnten. Mittlerweile setzten nicht nur Großunternehmen Systeme ein, mit denen ein Stillstand verhindert wird, sondern auch mittelständische Betriebe, etwa Zulieferfirmen der Automobil- und der Flugzeugindustrie.

Predictive Policing

Claus Schaffner, Redaktion WiK, stellt in der Ausgabe 1-2015, S. 9/10, Tools für ein Predictive Policing vor. In der Funktionsweise ähnelten sich die Tools, unterschiedlich nach Hersteller seien allerdings die Algorithmen, mit denen die Datensätze ausgewertet werden. Personenbezogene Daten würden dabei normalerweise nicht verwendet. Die Tools stellten digitale Karten zur Verfügung, auf denen grafisch beispielsweise dargestellt wird, wo und zu welchem Zeitpunkt mit einer erhöhten Wahrscheinlichkeit mit Einbrüchen gerechnet werden kann. Alle Analyse-Tools seien allerdings nur so gut wie der zugrunde liegende Datensatz dahinter. Bei der Stadtpo-

lizei Zürich, die die Prognosesoftware dauerhaft einsetzen wolle, hätten sich bei fünf von sechs Prognosen Folgedelikte ereignet, und beinahe die Hälfte der prognostizierten Folgedelikte sei kleinräumig erfolgt, sodass sich Einsatzkräfte auf spezifische Gebiete konzentrieren konnten. Prinzipiell ließen sich die Datensätze für verschiedene Einsatzzwecke auch maßschneidern. In Zusammenarbeit mit der Deutschen Hochschule der Polizei in Münster werde anhand eines Praxisszenarios geprüft, inwiefern moderne Prognosesysteme den Polizeiführer bei der Lagebeurteilung am Beispiel von Fußballspielen unterstützen können – beispielsweise anhand mannschaftsbezogener Daten, wie Tabellenplatz und dem Verhältnis der Fangemeinden zueinander oder anhand geografischer Daten wie etwa der Entfernung des Spielortes zum Sitz der Gastmannschaft.

Produktpiraterie

Das Geschäft mit der Schönheit locke immer mehr Produktpiraten, meldet die FAZ am 24. März. 2014 seien **gefälschte Körperpflegeprodukte** im Wert von annähernd 23 Mio. Euro sichergestellt worden. Die Zahl beschlagnahmter Waren sei um 54 Prozent auf fast 1,58 Mio. Stück gestiegen. Damit stünden Kosmetika noch vor Kleidung „auf einem traurigen ersten Platz" in der Konsumgüterindustrie. Gefälschte Kosmetikprodukte würden besonders gern über das Internet direkt an die Kunden verkauft und verschickt. Die Verkaufsplattformen und Marktplätze verdienten zwar daran, entzögen sich bisher aber weitgehend ihrer Verantwortung.

Rechenzentrumssicherheit

In der Fachzeitschrift PROTECTOR (Ausgabe 3-2015, S. 16–18) wird ein mehrstufiges Konzept für die **physische Datensicherheit** vorgestellt. In dem beschriebenen Anwendungsbeispiel (Hagebau-RZ in Hamburg) müssen berechtigte Personen stets unterschiedliche beziehungsweise mehrstufige Zutrittskontrollen durchlaufen. Es kommen sowohl Schließsysteme mit PIN-Code, Kartenlesegeräte und Systeme mit biometrischer Erkennung zum Einsatz. Je nach Zugangstür sei die Kontrolle dabei mindestens zweistufig ausgelegt. Grundsätzlich müsse sich jeder, der ins Gebäude will, zuerst beim Pförtner anmelden und legitimieren. Durch die Vereinzelungsschleuse gelangen berechtigte Personen nur, wenn sie über eine entsprechende Key-Card und einen personenzugewiesenen PIN beziehungsweise eine Key-Card mit gespeichertem Fingerabdruck verfügen. Als zusätzliche Maßnahme seien die Server in den separaten Rechnerräumen nochmals durch verzinkte Gitterboxen gesichert. Bis jemand dahin gelangt, hätte das elektronische Einbruchmeldesystem bereits mehrmals Alarm ausgelöst. Von außen seien die Gebäude zusätzlich mit einem videoüberwachten Zaun gesichert. Das Zufahrtstor zum Gebände und zur Tiefgarage öffne sich nur für autorisierte Besucher und schließe wieder nach einem sehr eng gefassten Zeitfenster.

In derselben Ausgabe wird die **Sicherheit von Serverräumen** thematisiert (S. 19). Im Serverraum würden Multifunktionssensoren einen zuverlässigen Rundumschutz vor vielen Bedrohungen bieten. Mit acht integrierten Sensoren überwache das Sensorgerät bis zu 18 Gefahren. Durch die ständige Kontrolle der Raumtemperator könnten Ausfälle von Kühlaggregaten erkannt und daraus resultierende Systemausfälle verhindert werden. Im Bereich Brandschutz komme eine hochempfindliche Kohlenmonoxiderkennung zum Einsatz. Im Bereich Rack-Monitoring werde der Multisensor-Rack direkt in den Serverracks installiert, wo er alle kritischen Gefahren überwacht und zusätzlich Strom und Spannung über die integrierte Power Distribution Unit (Stromverteilereinheit) kontrolliert. Durch LAN-Fähigkeit und Internetanbindung ließen

sich die Systeme zentral steuern und böten umfassende Analyse- und Monitoring-Auswertungen. Der Zugriff über eine Handy-App sowie Alarmbenachrichtigungen per E-Mail und SMS ermöglichten zu jeder Zeit eine schnelle Reaktion auf kritische Veränderungen der Messwerte.

Risiko-Management

Prof. Dr. Kerstin Windhövel, Fachhochschule für Wirtschaft in Zürich, und Dipl. Entrepreneur FH Uwe Müller-Gauss, Müller-Gauss Consulting, plädieren in der Ausgabe 1-2015 der Zeitschrift Sicherheitsforum (S. 22–25) für ein **innovatives und integrales Risiko-Managementsystem**. Das Risikomanagement sei keine einmalige Aufgabe, sondern stelle einen Kreislauf aus fünf Schritten dar: „Risikobewusstsein schaffen", „Risiken identifizieren", „Risiken bewerten", „Risiken bewältigen" und „Risiken kontrollieren". Diese Abfolge müsse regelmäßig, jedoch mindestens einmal jährlich, von den Verantwortlichen durchgeführt werden, da sich das Umfeld jeder Vorsorgeeinrichtung oder die Organisation selbst ändere. Somit müsse auch ein Risiko-Managementsystem kontinuierlich den neuen Gegebenheiten angepasst werden.

Schleusensicherheit

Ralph Münkel, Siemens AG, plädiert in der März-Ausgabe der Fachzeitschrift GIT (S. 116–118) für die fehlersichere Automatisierung einer Schleuse. Schleusen seien nach der Maschinenrichtlinie 2006/42/EG als Maschinen eingestuft. Die Richtlinie fordere eine Risikoanalyse und die Einstufung der einzelnen Funktionen in Gefährdungsklassen. Die Steuerungen seien über einen Ring in Lichtwellenleitertechnik miteinander verbunden. Die zentrale Steuerung koordiniere den Betrieb der beiden Tore und steuere die Signalanlagen ebenfalls fehlersicher an. Der Schleusenvorgang werde vom Schleusenturm aus eingeleitet und überwacht. Für den Gefahrenfall seien am Visualisierungsbedienstand Nothalt-Taster nach VDE 0113 Teil 1 installiert. Die Automatisierung erhöhe nicht nur die Schleusensicherheit, sondern sei auch die Voraussetzung für die Fernbedienung von einer Fernbedienzentrale aus. Erhöhte Sicherheitsanforderungen bestünden für die eindeutige Zuordnung der Taster für Wasserstopp und Nothalt beim Betrieb der Leitzentrale. Ein Funktionsbaustein stelle trotz der Anwahl der Schleuse über ein „nicht sicheres" HMI-System eine verifizierte, sichere Verbindung zwischen der Nothalt-Funktion der angewählten Schleuse und den auf dem Bedienplatz der Leitzentrale befindlichen Tastern her.

Sicherheitsmarkt

Dr. Peter Fey, Dr. Wieselhuber & Partner, sieht am Sicherheitsmarkt „bewegte Zeiten" (PROTECTOR, Ausgabe 3-2015, S. 10/11). Die Nachfrage nach Sicherheitslösungen werde auch in Zukunft ungebremst steigen. Internationale Marktstudien prophezeiten der Sicherheitsbranche von 2014 bis 2019 weltweit ein Wachstum von durchschnittlich 9 Prozent im Jahr. Aktuelle globale Entwicklungen zeigten positive Auswirkungen, z. B. steigende Bandenkriminalität, Terrorrisiken, Migration sowie anhaltende Urbanisierung und zunehmendes Verkehrs- und Transportaufkommen. Hinzu kämen technisch induzierte Trends, z. B. mobile Anwendungen, Cloud-Lösungen, IP-Standards. In den letzten Jahren habe sich für die sicherheitstechnischen Unternehmen eine zielgerichtete Orientierung an den vertikalen Marktsegmenten als unumgänglich herausgestellt. In Zukunft gehe der Trend noch stärker als bisher weg von Insellösungen hin zu integrierten Gesamtsystemen und Dienstleistungen.

Sicherheitstechnik

Die Fachzeitschrift s+s report (Ausgabe 1-2015, S. 6) berichtet, dass im Prevention Forum der europäischen Vereinigung der Versicherungswirtschaft eine neue Expertengruppe gebildet worden sei, die aktuelle Themen der Sicherungstechnik bearbeiten soll: die „Expert Group 5". Vorsitzender sei Thomas Urban, Bereichsleiter Security bei VdS. Erste Themen auf der Agenda der EG5 seien Aspekte der Videodetektion und der geplanten europäischen Service-Norm sowie das Gebiet Cyber Security.

Spionage

Wenn eine Behörde eine „No Spy-Klausel" bei der IT-Beschaffung einführt, läuft sie Gefahr, den Wettbewerb zu beschränken. Wenn ein bietendes Unternehmen nicht mehr bieten kann, weil es einem ausländischen Nachrichtendienst verpflichtet ist und ehrlich bleibt, sei es vom Markt, glaubt der Behörden Spiegel in seiner Februar-Ausgabe. Dr. Johann Bizer, Dataport, meint: „Wenn der Generalverdacht lautet, dass No Spy-Klauseln zu Wettbewerbsbeschränkungen führen, wäre die richtige Antwort von Anbieterseite darauf, seine Strukturen so zu verändern, dass wir zusammenarbeiten und die geforderte Vertraulichkeit gewährleisten können."

In den Informationen deutscher Sicherheitsbehörden vom 6. März wird auf den Verdacht der Wirtschaftsspionage gegen eine hessische Firma aus der Branche **Umwelttechnik** hingewiesen. Chinesische Delegationen zeigten bei Videopräsentationen immer für ein bestimmtes durch die Firma entwickeltes Produkt sehr starkes Interesse. Die hessische Sicherheitsbehörde habe daher mit dem IT-Sicherheitsbeauftragten vereinbart, zunächst die Geschäftsführung zum Thema Wirtschaftsspionage zu sensibilisieren. In einem weiteren Schritt sollten die Mitarbeiter mit den Schwerpunkten „Sicherheit auf Reisen/China" und „IT-gestützte Spionage" sensibilisiert werden.

Steuerhinterziehung

Die verpflichtende Einführung betrugssicherer Registrierkassen und Taxameter zum Schutz vor Steuerhinterziehung lasse weiter auf sich warten, meldet das Magazin Focus am 28. Februar. Das BMF habe noch zehn offene „rechtliche, organisatorische und technische Fragen" aufgelistet, an deren Klärung zurzeit intensiv gearbeitet würde. Ursprünglich sollte der kryptografische Manipulationsschutz unter dem Kürzel Insika 2009 eingeführt werden. Bereits 2003 habe der Bundesrechnungshof Steuerausfälle in Milliardenhöhe durch systematischen Betrug an elektronischen Kassen sowie an Taxametern festgestellt. Eine Bund/Länder-Arbeitsgruppe habe den Einsatz manipulationssicherer Systeme mit einer Smartcard vorgeschlagen. Diese Karten sollten über das Bundeszentralamt für Steuern ausgegeben und verwaltet werden. Nun aber werde beabsichtigt, eine Zentralstelle außerhalb der Finanzverwaltung damit zu beauftragen.

Terrorismusbekämpfung

Der Kampf gegen den Terrorismus macht vor Unternehmen nicht halt, schreibt die FAZ am 28. März. Verordnungen der EU schreiben vor, dass die Konten der Personen und Organisationen, die terrorismusverdächtig sind und daher auf Listen erfasst werden, eingefroren werden müssen. Außerdem dürfen ihnen weder direkt noch indirekt Gelder bereitgestellt werden. Darunter fällt auch der Arbeitslohn. Zahlt der Arbeitgeber das Gehalt trotzdem weiter aus, komme er selbst in Schwierigkeiten. Ihm drohen bis zu fünf Jahre

Haft, so steht es im Außenwirtschaftsgesetz. Wenn der Arbeitgeber von dem Terrorverdacht nichts wusste, könne er mit einem Bußgeld davonkommen. Nichts zu befürchten habe er nur dann, wenn er nachweisen kann, dass er seine Belegschaft einer sorgfältigen Kontrolle unterzogen hat. Wichtig sei der Nachweis von Kontrollen auch noch aus einem anderen Grund: Der Zoll verleihe den Status als „zugelassener Wirtschaftsbeteiligter" (AEO-S und AEO-F-Zertifikat) nur Unternehmen, die alle Beschäftigten in den sicherheitsrelevanten Bereichen mit europäischen Terrorlisten abgleichen. Das AEO-Zertifikat sei ein Vertrauenssiegel: Die Abfertigung am Zoll ist beschleunigt, ein wichtiges Privileg für Unternehmen im Export- und Importgeschäft. In welchen Zeitabständen die Kontrolle erfolgt, sei in den EU-Verordnungen nicht geregelt. Für das AEO-Zertifikat gebe es eine Dienstvorschrift des BFM: Der Zoll verlangt von den Unternehmen mindestens eine jährliche Prüfung. Angesichts der häufigen Erweiterungen der Listen erfülle der Arbeitgeber seine Pflicht nicht, wenn er nur alle paar Jahre eine Prüfung vornehme. Es spreche nichts dagegen, die Kontrollen an eine andere Firma zu übertragen. Sie müsse nur sorgfältig ausgewählt und instruiert werden.

Transportdiebstahl

Folgende Tatorte aktueller Sachbeschädigungen an Lkw und Ladungs-Diebstähle wurden am 7. und am 14. März vom ASW gemeldet:

- 11./12.2. Plauen, A 72, Parkplatz Vogtland-Nord
- 11./12.2. Auetal, A 2, Rastplatz Auetal Nord, Fahrtrichtung Dortmund
- 16./17.2. Ziesar, A 2, Rast- und Tankkomplex Buckautal-Süd, Fahrtrichtung Potsdam
- 17.2. Hausen, A 7, Rastanlage Riedener Wald West, Fahrtrichtung Nürnberg
- 18./19.2. A 4, Tank- und Rastanlage Eichelborn
- 20./21.2. Herzlake, Dieselstraße
- 21.2 Herzlake, Osterstraße, Firmengelände
- 24./25.2. Beelitz, A 9, Parkplatz „Zauche" zw. Anschlussstelle Brück und Beelitz, Richtung Potsdam
- 24./25.2. A 4, Parkplätze Rödertal und Am Eichelberg, Fahrtrichtung Dresden
- 25./26.2. Rees-Empel, Firmengelände an der Hurler Straße
- 26./27.2. Lippetal-Lippborg, A 2, Rastplatz Strängenbach
- 26.2. Erfurt-Dresden, A 4, Parkplatz Willroder Forst
- 28.2. Recklinghausen, Alte Grenzstraße und A 2, Raststätte Lehrter See-Süd
- 5.3. Mühlau, A 72, Parkplatz Mühlbachtal
- 6./9.3. Plauen, J.-C.-Dietrich-Straße, Hof einer Spedition
- 10.3. Marienheide-Gimborn, Schlossstraße, Hotel in Dänikhorst

Unternehmens-Intelligence

Unternehmens-Intelligence ist das Thema eines Beitrags von Jörn Weber, corma GmbH, in der Ausgabe 1-2015 der Zeitschrift WiK, S.22–24. Ergebe sich ein Betrugs- oder Diebstahlsverdacht, dann stelle sich für die Ermittlungen auch die Frage, ob es sich um einen Einzeltäter handelt oder ob er mit anderen Tätern vernetzt sei. Um ein mögliches Täternetzwerk zu entdecken, sollten alle unternehmensweit relevanten Informationen zentral erfasst und gespeichert werden. In einer Datenbank könnten alle fragwürdigen Vorfälle, Personen und Unternehmen sowie deren Beziehungen untereinander gesammelt werden. Die veränderte Intelligenz der Täter mache es erforderlich, dass auch der Ermittler sein Wissen und sein Vorgehen auf Marktplätze im Internet, anonyme Internetseiten, digitale Beweissicherung, strukturierte Internetrecherche und das gezielte Überwachen auf neue Fundstellen anpasst. Um unstrukturierte Daten möglichst zielorientiert nutzen und auch Abgleiche mit vorherigen Analysen oder vorhandenen Fallinformationen

erstellen zu können, sollten sie in eine zentrale Intelligence-Plattform einfließen. Ihr großer Vorteil bestehe darin, dass große Datenmengen aus vielfältigen Quellen schnell analysiert werden können.

Unternehmensstrafrecht

Rechtsanwalt Konstantin von Busekist thematisiert in der FAZ am 30. März die Erwägung von Justizminister Maas, einen Vorschlag für ein Unternehmensstrafrecht einzubringen. Das deutsche Straf- und Strafprozessrecht kenne ein Unternehmensstrafrecht nicht. Eine Verschiebung des Compliance-Vorwurfs gegenüber dem Unternehmen ins Strafrecht werde keinerlei Präventionswirkung schaffen. Werde aber der Vorwurf „mangelhafter Organisation" erhoben, scheine es angebracht, Grundsätze einer „guten Organisation" zu definieren und diese auch gesetzlich festzulegen. Aktuell existiere zwar ein Wirtschaftsprüfungsstandard für Compliance-Managementsysteme, der entsprechende Anforderungen an Unternehmen definiere; eine gesetzliche Regelung, die diese klar verankert, gebe es jedoch nicht. Wünschenswert wären beispielsweise konkrete Vorgaben für eine Selbstanzeige von Gesetzesverletzungen durch Unternehmen.

Verschlüsselung

In der Wirtschaft, insbesondere von mittelständischen Unternehmen, werde die Diskussion über ein Verschlüsselungsverbot mit Sorge betrachtet, berichtet der Behörden Spiegel in seiner Februar-Ausgabe. Der Präsident des Bundesverbands IT-Mittelstand, Dr. Oliver Grün, warne: „Die Aushebelung der Verschlüsselung beschädigt den Datenschutzstandort Deutschland. Wenn jede Kommunikation – egal wie gut sie gesichert ist – theoretisch mit einem Knopfdruck von Sicherheitsbehörden umgangen werden kann, entsteht eine enorme Gefahr des Missbrauchs." Es sei davon auszugehen, dass kriminelle oder terroristische Organisationen auf andere Möglichkeiten der Kommunikation ausweichen, befürchte Dr. Holger Mühlbauer, GF des TeleTrust. Insbesondere sei völlig unklar, wie eine Schlüsselhinterlegung technisch und rechtlich im Rahmen des grenzüberschreitenden Datenverkehrs greifen solle. Eine grenzüberschreitende einheitliche Verschlüsselung, bei der Bündnispartner Zugang zu Schlüsseln haben, komme für Sicherheitsbehörden nicht in Betracht. Bisher habe sich kein Staat durchringen können, seine Souveränität in dieser Frage aufzugeben und mit anderen Schlüssel zu teilen. Dessen sei sich auch de Maizière bewusst. Das BSI solle jedenfalls und müsse sich weiter mit Ver- und Entschlüsselung beschäftigen und zur Sicherheit beitragen.

Videoüberwachung

Mehr Effizienz und neue Anwendungen mit IP thematisiert Bosch Sicherheitssysteme in der Ausgabe 3-2015 der Zeitschrift PROTECTOR (S. 34/35). Ethernet und das IP-Protokoll würden in der gesamten Sicherheitstechnik immer mehr an Bedeutung gewinnen. Sie ermöglichten die einfache Vernetzung und die Integration unterschiedlicher Gewerke wie Video und Zutrittskontrolle und einen kosteneffizienten Betrieb der gesamten Sicherheitstechnik. Die Verwendung weltweit standardisierter Übertragungsmedien und Protokolle vereinfache ganz erheblich die Kommunikation zwischen mehreren Systemen. Die Integration unterschiedlicher Gewerke erhöhe das gesamte Sicherheitsniveau, da Ereignisse und Alarme unterschiedlicher Systeme automatisch korreliert werden könnten. Die Flexibilität und die Skalierbarkeit seien weitere große Pluspunkte vernetzter Systeme. IP ermögliche auch völlig neue Anwendungen wie etwa Cloud-basierte Dienste sowie deutlich verbesserte Remote Services. Wie GIT in der März-Ausgabe 2015 (S. 11)

meldet, hat IHS ein White Paper vorgelegt, nach dem der Videoüberwachungsmarkt im Verlauf des Jahres 2015 um 10 Prozent wachsen kann. Weltweit habe das Marktvolumen Ende 2014 etwa 15 Mrd. betragen. Bis 2018 erwarte man, 23,6 Mrd. zu erreichen, was einer jährlichen Steigerungsrate von 12 Prozent entspräche.

Wie GIT in dieser Ausgabe weiter berichtet, klärt ein Urteil des EuGH die Rechte und Pflichten der Hausbesitzer mit Videokameras. Der Einsatz sei zum Schutz von Leib und Leben grundsätzlich zulässig. Dies gelte auch dann, wenn private Kameras Teile öffentlicher Bereiche aufnehmen. Hierbei greife zwar grundsätzlich der europäische Datenschutz, der die Einwilligung der Gefilmten verlangt. Allerdings gebe es Ausnahmen: wenn die Videoüberwachung zur Verwirklichung des berechtigten Interesses des für die Verarbeitung Verantwortlichen erforderlich ist. Als „berechtigtes Interesse" werteten die Richter den Schutz des Eigentums, der Gesundheit und des Lebens. Weiterhin könne auf eine Einwilligung verzichtet werden, wenn dies unmöglich ist oder unverhältnismäßigen Aufwand erfordert (S. 39).

Mit dem **Schutz kritischer Infrastrukturanlagen mit IP-Überwachung** befasst sich Edwin Beerentemfel, Axis Communications, in der März-Ausgabe von GIT (S. 68–70). Es gebe für den Schutz des Außengeländes eine Vielzahl verschiedener traditioneller Technologien, mit deren Hilfe Eindringlinge erkannt werden können. In Kombination mit Netzwerk-Kameras erhöhten sie den Schutz für risikoreiche Infrastrukturen. Die Kombination aus Wärmebild- und PTZ-Domkamera eigne sich auch bestens zum Schutz von Leitungssystemen. Sicherheitsanlagen auf der Basis einer IP-Infrastruktur seien skalierbar, zuverlässig und zukunftsfähig. Das Netzwerk-Videosystem sei gegenwärtig die umfassendste Lösung für Sicherheit und Produktivität.

Cagatay Kilic, Western Digital, befürwortet in der März-Ausgabe von GIT (S. 86/87) **optimierte Datenspeicher für Überwachungssysteme**. Bei den Kameras sollten sich Käufer für Kits entscheiden, die mindestens eine HD-Kamera mit einer Bildauflösung von 1.280 x 720 Pixel oder sogar eine Full HD-Kamera mit einer Auflösung von 1.920 x 1.080 Pixel beinhalten. Eine Schlüsselkomponente eines Überwachungssystems sei der verwendete Datenspeicher. Er könne in der Tat die Wirksamkeit eines ganzen Systems sichern oder in Frage stellen. Wenn ein System ohne Datenspeicher gekauft wird, solle sich der Käufer idealerweise nach Festplatten umsehen, die eine Optimierung für Überwachungsanwendungen, wie zum Beispiel die AllFrame-Technologie, beinhalten. Diese verbessere die Wiedergabeleistung und vermeide durch den Einsatz von ATA-Streaming Fehler und Bildverluste. Die Laufwerke sollten ebenfalls für einen Rund-um-die-Uhr-Einsatz ausgelegt sein und Funktionen wie zum Beispiel IntelliPower beinhalten, die den Stromverbrauch des Laufwerks und somit die Wärmeerzeugung reduzieren.

Erwin Oertle, Siemens Schweiz AG, legt in der Ausgabe 1-2015 der Zeitschrift Sicherheitsforum (S. 12/13) dar, dass **Innovationen in der Videotechnik** immer leistungsfähigere Hard- und Softwarekomponenten ermöglichen und so bessere Überwachungsmöglichkeiten bieten. Einer der größten Trends sei bei der Auflösung zu finden: Sie werde immer besser und setze sich als Standard durch. High Definition (HD) und Full-HD gehörten heute schon zur Regel. Dass hier enormes Potenzial liegt, zeigten die Trends: 4K und 8K, also 8 MP bzw. 32 MP. Die ersten 4K-Kameras seien bereits auf dem Markt erhältlich. 4K-Kameras mit hoher Auflösung eigneten sich insbesondere für die Personenerkennung, Stadien- und Parkplatzüberwachung. Die Objektivhersteller der Kameras arbeiteten mit Hochdruck an der Entwicklung von kostengünstigen 4K-Zoomobjektiven, die eine vollflächige 8 MP-Auflösung haben. Höhere Bandbreiten erforderten eine performante

Hardware zur Bildverarbeitung und Visualisierung. Ein weiterer Trend zeige sich beim Kompressionsstandard. Gekoppelt mit den 4K-Entwicklungen sei der Kompressionsstandard H.265 in Sichtweite. Dass er zusätzlich die Bildqualität verbessert und den Bandbreiten- und Speicherbedarf um 25–50 Prozent reduziert, seien wichtige Kernmerkmale des neuen Standards. Um das komprimierte Format wieder visualisieren zu können, brauche es eine drei- bis fünfmal höhere Rechnerleistung als bisher. Ein weiterer Trend liege in der Leistungsstärke der Kameras. Die CPUs würden immer stärker und besser, was wiederum eine höhere Intelligenz der Kamera ermögliche. Im Zusammenhang mit der Intelligenz von Kameras zeige sich ein weiterer Trend: das Georeferencing mit 3-D-Videosensorik. Eine ebenfalls sehr interessante Entwicklung, die sehr gut auf die Videotechnik überschwappen könnte, sei der 3-D-Druck. In derselben Ausgabe weist Jochen Sauer, Axis Communications, auf die neu überarbeitete Norm DIN EN 50132-7 „Alarmanlagen – CCTV-Überwachungsanlagen für Sicherungsanwendungen – Teil 7: Anwendungsregeln" hin, die Empfehlungen zur Auswahl, Planung, Installation sowie Inbetriebnahme und Wartung enthielten (S. 19–21). Mit der **WDR-Technologie** (Wide Dynamic Range) könnten Kameras deutlich homogenere Bilder erzeugen. Damit würden Personen, Fahrzeuge und Gegenstände identifizierbar, unabhängig davon, ob sie sich in einem sehr dunklen oder sehr hellen Bereich befinden. Herkömmliche Kameras mit Tag- und Nachtfunktionalität schalteten in der Dunkelheit in den schwarz/weiß-Modus. Es existierten jedoch Technologien, die auch bei extrem schwacher Beleuchtung Farbbilder aufnehmen können.

Mit den **notwendigen Fachkenntnissen des Errichters** befasst sich s+s report in der Ausgabe 1-2015, S. 50–52. Grundlegende IT-Kenntnisse gehörten ebenso zum Handwerkszeug wie die Fähigkeit, ein Sicherheitskonzept für den Auftraggeber zu erstellen, das sowohl dessen Anforderungen genügt als auch den rechtlichen Grundlagen entspricht. Die Fachzeitschrift listet „Fallstricke" auf, die der professionelle Video-Errichter vermeiden sollte: 1. Vernachlässigung von Datenschutzgesetzen, 2. Nichtbeachtung einschlägiger Normen und Richtlinien, 3. Schutzziele einer Videoüberwachungsanlage sind zwischen Errichter und Auftraggeber nicht exakt genug definiert, 4. keine Risikoanalyse erstellt, 5. mangelnde Dokumentation, die für Probleme bei der späteren Wartung und Erweiterung der Videoüberwachungsanlage sorgt, 6. Planungsfehler im allgemeinen, 7. Fehler bei der Übergabe an den Auftraggeber, 8. mangelnder After Sales Support, 9. einmal gelernt reicht aus, 10. Eigentor Billigqualität.

Zutrittskontrolle

Fernando Pires, Morse Watchmans Inc., behandelt in der Fachzeitschrift PROTECTOR (Ausgabe 3-2015, S. 24/25) die **Integration der Schlüsselkontrolle in vernetzte Sicherheitssysteme**. Offene Protokolle ermöglichten die Konnektivität mit der Zugangskontrolle und anderen Systemen, die von einer Reise von Integrationspartnern für mehrere Sicherheits- und Kontrollebenen bereitgestellt werden: Integration mehrerer Standorte mit gemeinsamer Nutzung von Datenbanken und Programmierung, Informationen in Echtzeit, lokaler und Fernzugriff computergestütztes Reporting, spezifische Warnmeldungen und benutzerfreundliches Schlüsselentnahme-Management sowie Zugangskontrolle zur nächsten Ebene.

Dieselbe Ausgabe enthält eine **Marktübersicht zu Vereinzelungsanlagen**. Vorgestellt werden 94 Systeme von 24 Anbietern. Abgefragt wurden: Sicherheitsniveau, Durchgangsfrequenz in Verbindung mit ZK-Anlage (Personen/Minute), Maße, Schnittstellen, Steuerung, mechanische oder elektronische Vereinzelung, Durchwurf- bzw. Durchschusshemmung, Fluchtwegintegration, Stromausfallverhalten, Ausführungsvarianten, Montage und Erweiterungsmöglichkeiten (S. 26/27).

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, René Helbig, Elke Hollenberg, Gabriele Biesing
Vorsitzender des Aufsichtsrates: Dr. Carl A. Schade

E-Mail: info@securitas.de