# *Focus on Security*

Ausgabe 05, Mai 2016

SECURITAS

***Inhalt***

## *Brandschutz*

Brandschutz von Siemens für den **Gotthard-Basistunnel** stellt GIT in der Ausgabe 4-2016, S. 70/71 vor. Die Röhren des Basistunnels seien alle 300 Meter durch Querschläge verbunden, sodass die Zugpassagiere im Brandfall in die andere Röhre flüchten können. Die Anlage sei mit unzähligen Sensoren, Überwachungseinrichtungen und Steuerungen bestückt, die über Tausende von Kilometern Glasfaserkabel mit den beiden Control-Centern am Nord- und am Südportal verbunden sind. Das gelte auch für die Brandorterkennung in den vier Nothaltestellen. Sie erfolge mit drei unterschiedlichen Detektionssystemen und steuere bei einer bevorstehenden Evakuierung direkt die Lüftungsklappen an. Eine Besonderheit sei die Installation der Fibrolaser-Branderkennungstechnik von Siemens. Auch am Boden wache Fibrolaser über erste Gefahrenanzeichen. Ergänzt werde Fibrolaser durch Wärmebildkameras und durch Rauchmelder, die ständig Temperatur und Luft auf Rauchpartikel prüfen.

Frank Liebelt und Dipl.-Phys. Bertrand Völkers, Flir Commercial Vision Systems, befassen sich in Ausgabe 4-2016 der Fachzeitschrift PROTECTOR, S. 32/33 mit **Brandfrüherkennung in Abfallanlagen.** Die Kameras der Flir FC Serie R, die die gesamte Oberfläche eines Müllbunkers (25 x 25 Meter) überwachen, seien fest installierte radiometrische Kameras, die präzise, berührungslose Temperaturmessungen liefern. Das mache sie zu einer idealen Lösung für Hot-Spot- und Brandfrüherkennung. Die beiden Kameras würden die tatsächlichen Temperaturen der Abfallhaufen messen und immer, wenn eine bestimmte Temperaturschwelle erreicht wird, gäben sie einen Alarm aus. Neben radiometrischer Temperaturmessung könne die Kamera auch Einbruchserkennung und visuelle Alarmverifikationen liefern.

**Forschung zu alternativen Regalsprinklersystemen** thematisiert Frank Drolsbach, FM Global, in der Ausgabe 4-2016 von PROTECTOR, S. 36/37. In einem Unternehmen sollten sämtliche Bereiche mit Sprinklern ausgestattet werden, in denen sich Materialien befinden oder Prozesse ablaufen, die zur Entstehung oder Ausbreitung eines Brandes beitragen können. Besonders im Lager gebe es zahlreiche, oft unterschätzte, Gefahrenquellen sowie den Risikofaktor Mensch, der Computer und Lagerroboter bedient. Aufgrund der rasanten Feuerausbreitung in Hochregallagern sei zu empfehlen, bei Deckenhöhen über 13,5 Meter Sprinkler nicht nur an der Decke, sondern zusätzlich auch in einzelnen Ebenen der Regale zu installieren. Effektiv sei die Installation von Regalsprinkleranordnungen, die eine Brandbekämpfung in den Vertikalschächten (Längs- und Querschächten) in einem Regal erlauben. Hierzu würden Sprinkler entweder in jedem oder in jedem zweiten Querschacht positioniert. Um die Ausbreitung eines Brandes über die Gangseiten des Regals zu unterbinden, würden bei einigen Anordnungen auch Gangsprinkler (zusätzliche Sprinklerreihen an den Gangseiten der Regale) zum Einsatz gebracht. FM Global habe zu diesen bestehenden Regalsprinklersystemen alternative Systeme für Nasssprinkleranlagen entwickelt. Bei den alternativen Systemen kämen im Regal Sprinklerköpfe mit großen Auslassöffnungen und entsprechend hohen Wassermengen pro Sprinklerkopf zum Einsatz. Sie seien in der Lage, größere Feuersäulen zu unterdrücken.

Warum **Brandschutz und Ästhetik** sich nicht ausschließen müssen, erläutert Dr. Wolfgang Krause, bvfa, in der Ausgabe 2-2016 von Security insight, S. 16/17. Störten sich manche designaffine Architekten früher daran, dass Sprinklerköpfe aus der Decke ragen , ließen sich diese inzwischen fast unsichtbar integrieren, dezent zurücksetzen oder deckenbündig anbringen. Ob Neubau oder Bestand, wichtig seien vor allem drei Punkte in der Architektur: das Verständnis dafür, dass Brandschutz nicht störend, sondern elemen-

tar wichtig für Leben, Sachwerte und Umwelt ist; die frühzeitige Zusammenarbeit aller Beteiligten und das Wissen um die technischen Möglichkeiten.

Bernhard Tschoepe, AG Betrieblicher Brandschutz Berlin e. V., schaltet sich in der Ausgabe 2-2016 von Security insight, S. 18/19, in die Debatte um eine **neue Generation von Feuerlöschern** ein, deren Wartungsintervall zehn Jahre beträgt. Statt der Blechbehälter würde Hochdruck-Polyethylen verwendet, ein extrem belastbarer Kunststoff, der nicht roste. Fülle man diesen Behälter mit einem qualitativ belastbaren Löschpulver oder zuverlässigen Premix-Lösungen, könne ein solcher Löscher zehn Jahre – jedenfalls nach Aussagen des Herstellers – auskommen, ohne das Gerät zu öffnen. Schon seit vielen Jahren nutzten die Feuerwehren Atemluftflaschen aus Kunststoff, ähnlich umwickelt mit Kohlenstofffasern und mit 300 bar Betriebsdruck. Da wirkten die maximal in den Feuerlöschern auftretenden 14,5 bar bescheiden.

## *Cloud Computing*

Box hat nach einem Bericht von silicon.de am 13. April im Rahmen der Box World Tour in Europa „**Box Zones**" angekündigt, womit Unternehmen die Auswahlmöglichkeit zur regionalen Datenspeicherung in Europa und Asien bereitgestellt werden solle. Box Zones werde Unternehmen bei der Zentralisierung ihrer wichtigen Inhalte unterstützen und ihre Produktivität erhöhen sowie gleichzeitig den Erfordernissen lokaler Datenspeicherung gerecht werden. Durch Einsatz von Amazon Web Services (AWS) und IBM Cloud werde es Box Zones möglich machen, Inhalte in Box in Deutschland, Irland, Singapur und Japan gemäß den Erfordernissen der Kunden zu speichern.

Deutsche IT-Entscheider seien immer noch misstrauisch, wenn es darum geht, ihre sensiblen Daten Public-Cloud-Anbietern anzuvertrauen, wie der **Cloud Security Report** von Intel Security zeige, berichtet silicon.de am 19. April. Immerhin nutzten 71 Prozent der Unternehmen in Deutschland bereits seit über einem Jahr Cloud Computing und trauten der Verwendung auch. Dabei käme allerdings mit 54 Prozent am häufigsten die Private Cloud zum Einsatz. Gerade einmal 8 Prozent würden ihre vertraulichen Daten vollständig in die Hände von Public-Cloud-Anbietern geben. Weltweit seien 1.200 IT-Entscheider zu ihren Plänen und Investitionen, Bedenken und Sicherheitsvorfällen befragt worden. Ein Großteil der befragten deutschen Organisationen plane in alle Cloud-Dienstleistungsmodelle zu investieren: 89 Prozent in Security as a Service, 86 Prozent in Infrastructure as a Service, 75 Prozent in Software as a Service und 65 Prozent in Platform as a Service. 22 Prozent der weltweit Befragten hätten mitgeteilt, dass ihre Bedenken bei der Nutzung von Security as a Service von vergangenen Vorfällen bezüglich Datensicherheit geprägt würden. Sicherheitstechnisch glaubten 61 Prozent der deutschen Befragten, dass die Schatten-IT die Gewährleistung der Sicherheit in der Cloud negativ beeinflusst. Für 50 Prozent der deutschen Befragten stehe beim Ranking der Technologie der E-Mail-Schutz ganz oben, gefolgt von Web-Sicherheit (43 Prozent), Anti-Malware (37 Prozent), Firewall (34 Prozent), Verschlüsselung und Zugangsverwaltung (34 Prozent) sowie die Vorbeugung von Datenverlusten (28 Prozent).

## *Datenschutz*

Die FAZ berichtet am 2. April über eine Studie des Centrums für Europäische Politik (Cep). Nach ihr basiere die nach dem vom EuGH beanstandeten „Safe-Harbor-Abkommen" erzielte neue Regelung „**Privacy Shield**" auf einseitigen Zusicherungen der Amerikaner und Forderungen der Brüsseler

Kommission. Einen völkerrechtlichen Vertrag gebe es nicht. Zudem fehlten „abschreckende Sanktionen" für Verstöße. Auch das von der US-Regierung versprochene Ombudsmann-System sei nicht mit einer gerichtlichen Überprüfung vereinbar und daher unzureichend. Wie rechtsverbindlich der Beschwerdemechanismus beim US-Außenministerium ist, sei fraglich. Rechtsbehelfe gegen dessen Entscheidungen fehlten ebenfalls.

Der Softwarekonzern Microsoft habe ein neues Kapitel in den **Auseinandersetzungen der Technologiebranche mit der US-Regierung** aufgeschlagen und eine Klage gegen das Justizministerium eingereicht, berichtet die FAZ am 16. April. Ähnlich wie Apple positioniere sich Microsoft hier als Kämpfer für die Privatsphäre seiner Kunden. Mit seiner Klage wolle sich das Unternehmen dagegen wehren, dass immer mehr Anfragen der US-Regierung nach Daten von Kunden mit einer Geheimhaltungspflicht verbunden seien. Die juristische Grundlage für solche Maulkörbe sei eine Klausel in einem Gesetz aus dem Jahr 1986, die Microsoft nicht nur für veraltet, sondern für verfassungswidrig hält und deren Aufhebung das Unternehmen in der Klage fordere. Das Justizministerium habe zunächst nur mitgeteilt, die Klage überprüfen zu wollen. Microsoft bestreite nicht, dass Geheimhaltungspflichten bisweilen angebracht sind, zum Beispiel, wenn mit einer Enthüllung die Gefahr verbunden wäre, dass eine Person Schaden erleidet oder dass Beweismaterial vernichtet wird. Aber nach Auffassung des Unternehmens nehmen solche Fälle überhand. Microsoft sei in den vergangenen eineinhalb Jahren von der Regierung 5.624 Mal aufgefordert worden, Kundendaten herauszugeben, und in 2.576 Fällen sei das Unternehmen dabei zu Stillschweigen verdonnert worden. Davon wiederum hätten 1.752 Maulkörbe keinerlei Zeitbeschränkung gehabt.

## *Drohnen*

Die Securitas Werkfeuerwehr des Chemieparks Bitterfeld hat nach einem Bericht der Mitteldeutschen Zeitung vom 6. April eine **Super-Drohne entwickelt**. Dieses fliegende Auge könne nicht nur fotografieren oder filmen. Es sei auch in der Lage, mit ausgefeilter Technik in Havariesituationen wichtige Entscheidungshilfen zu geben. Sie könne entweichende Gase analysieren, Fotos oder Videos von Orten oder Gefahrensituationen aufnehmen und per Funk in die Leitstelle oder über das Internet zu anderen Entscheidungsträgern senden. Mit den vier Zweipropeller-Motoren von je 400 Watt Leistung könne man die eingebaute Video- und Wärmebildkamera, die Gasanalysetechnik und die Batterien rund 20 Minuten in der Luft halten. In dieser Zeit könne die Drohne zum Beispiel von einer brennenden Lagerhalle eine Gesamtübersicht liefern und per Wärmebildtechnik lokalisieren, wo sich der Brandherd befindet. Die Drohne sei explosionsgeschützt. Dadurch könne sie an Stellen fliegen, die für die Feuerwehrleute zu gefährlich sind. Regen mache ihr nichts aus.

„Drohne soll mit Flugzeug kollidiert sein", meldet tagesspiegel.de am 18. April. Der **Zwischenfall in London Heathrow**, bei dem ein unbemanntes Fluggerät mit einem Passagierflugzeug zusammengestoßen sein soll, habe eine Debatte über die Sicherheit an Flughäfen ausgelöst. Der Pilot eines British Airways-Flug habe berichtet, seine Maschine sei beim Landeanflug auf London mit einer Drohne kollidiert. Experten hätten nach dem Zwischenfall gefordert, die Piloten von Hobbydrohnen sollten besser über die Risiken und die Regeln aufgeklärt werden. Gesetze müssten verschärft werden. Der britische Verkehrsminister habe mitgeteilt, die Regierung erwäge eine verpflichtende Registrierung von unbemannten Flugobjekten einzuführen.

Die Gefahr droht nicht von kommerziellen Anwendern, heißt es in der FAZ am 22. April. Sorgen bereite stattdessen die stark wachsende Zahl an Hobbypiloten in Deutschland. Generell seien Drohnenflüge in Sichtweite des Piloten erlaubt, wobei die Flughöhe auf 300 Meter beschränkt ist und die Flugverbotszonen rund um einen Flughafen zu beachten sind. Die Kollisionsgefahr am Rande von Flughäfen ist laut Jörg Lamprecht von der Firma Dedrone riesengroß. Es bestehe die Gefahr, dass Drohnen von den Triebwerken angesaugt werden, was bei Starts und Landengen verheerende Folgen hätte. Dedrone sei auf die Entdeckung unbemannter Flugobjekte spezialisiert und biete Firmenkunden eine Technologie zum Schutz vor zivilen Drohnen an.

## *Einbruchschutz*

Die Fachzeitschrift GIT befasst sich in der Ausgabe 4-2016, S. 26, mit der **Türsicherung** zum Schutz vor Einbrüchen. Ob Quer- oder Vertikalriegel, Kastenzusatzschlösser oder Bandsicherungen: neun von 15 Türsicherungen seien „mangelhaft". Die Sicherungen kosteten zwischen 20 und 695 Euro. Zu diesem Ergebnis sei die Stiftung Warentest in der Februar-Ausgabe ihrer Zeitschrift test gekommen. Ein Querriegel reiche meist, um eine solide Tür nachträglich zu sichern. Funktioniert ein Querriegel nicht, etwa bei Altbautüren, empfehle sich ein „gutes" Stangenschloss für 595 Euro. Dann sei zusätzlich eine „sehr gute" Bandsicherung zu Preisen von 78 bzw. 40 Euro sinnvoll.

## *Endgerätesicherheit*

Seit der Einführung des Fingerabdrucksensors Touch ID im iPhone 5S habe der Anteil der Nutzer, die ihr iPhone durch einen **Gerätecode** schützen, erheblich zugenommen, meldet heise.de am 18. April. Inzwischen setzten neun von zehn iPhone-Besitzern auf die Code-Sperre, wie Apple gegenüber US-Journalisten mitgeteilt habe. An den Gerätecode des Nutzers sei auch die seit iOS 8 umfassende Verschlüsselung der Daten geknüpft – ohne Kenntnis der PIN oder des Passwortes sollte der Zugriff auf die Daten für Dritte unmöglich sein.

## *Gefahrstoffe*

Die Anforderungen an umweltschützende und gesetzeskonforme Lagertechnik seien hoch, schreibt die Denios AG in der Ausgabe 4-2016 der Zeitschrift GIT, S. 104/105. Dies wirke sich unmittelbar auf die Ausstattungsmerkmale der Lagertechnik aus, zum Beispiel auf die Auffangwanne. Sie müsse bei einer Leckage den Inhalt des größten Behälters. bzw. mindestens zehn Prozent der eingelagerten Gesamtmenge, aufnehmen können. Denios-Ingenieure hätten Gefahrstoffdepots zur vorschriftmäßigen **Lagerung von wassergefährdenden Stoffen** (Wassergefährdungsklasse 1–3) und aggressiven Chemikalien neu entwickelt, die vollständig aus Polyethylen (PE) gefertigt sind. Kleingebinde und Fässer fänden darin ebenso Platz wie IBC. Die Depots könnten sowohl im Innen- als auch im Außenbereich aufgestellt werden. Korrosionsfrei, witterungsbeständig und stabil böten sie effizienten Schutz. Die neuesten Depots verfügten erstmalig über praktische und platzsparende Schiebetüren. Gehe es um die Lagerung von aggressiven Flüssigkeiten, seien Auffangsysteme aus Stahl nicht immer erste Wahl. Die Gefahrstoffdepots beständen aus rotationsgeformten Kunststoff-Komponenten. Pulverförmiges Thermoplast werde in Hohlkörperformen bis zum Schmelzpunkt erhitzt.

## *Geldwäsche*

Robert Kilian, Vorsitzender des deutschen Chapter der Association of Certified Fraud Manager, argumentiert in Security insight, Ausgabe 2-2016, S. 38–41, gegen die **Abschaffung des Bargeldes** zur Eindämmung der Geldwäsche. Der Bericht der Financial Intelligence Unit des BKA für das Jahr 2014 zeige, dass lediglich ein Prozent der Geldwäscheverdachtsanzeigen aus dem Nicht-Finanzsektor gekommen sei. Der Großteil der Geldwäsche werde über Banken versucht. Der Einsatz von zum Teil ahnungslosen Finanzagenten, die leichtgläubig ihr Konto für Transaktionen zur Verfügung stellten und der jüngst aufgedeckte Umsatzsteuerbetrug durch terroristische Täter seien nur zwei Beispiele für diese Entwicklung. Schon heute werde der Großteil der Geldwäsche unentdeckt elektronisch abgewickelt. Die Absenkung der Bartransaktionsgrenze führe sicherlich nicht zu einem veränderten Verhalten bei den verpflichteten Unternehmen, sondern nur zu Verärgerung und zur Suche nach Umgehungsmöglichkeiten. Deutschland stelle einen Schwerpunkt der Geldwäsche dar. Ein Ansatz zur Verbesserung liege in der Sensibilisierung. Unternehmen, die mit hochwertigen, teuren Gütern handeln, aber auch Händler mit hohem Absatz von Massenwaren sowie alle Beteiligten bei Immobiliengeschäften, müssten für die Problematik der Geldwäsche sensibilisiert werden.

## *Industrie 4.0*

Für die Industrie 4.0 seien **neue Sicherheitsstandards gefragt**, schreibt Prof. Dr. Jörn Müller-Quade, Karlsruhe Institute of Technology, in der FAZ am 21. April. In die Produktionsnetzwerke seien heute in der Regel eine Vielzahl von Partnern eng eingebunden. Es brauche mehrstufige Schutzmaßnahmen, weil in einer derart komplexen Situation nicht vollständig verhindert werden könne, dass einige Komponenten erfolgreich angegriffen werden. IT-Sicherheit müsse so konzipiert sein, dass die strikten Echtzeitbedingungen der Produktion nicht nur eingehalten werden, sondern die Echtzeitfähigkeit selbst bei intelligenten Angriffen noch sichergestellt ist. Safety und Security müssten für die sichere Produktion gemeinsam betrachtet werden. Dies stelle die IT-Sicherheit auch vor neue methodische Herausforderungen. Nötig sei eine Abkehr von der Betrachtung einzelner Sicherheitskomponenten wie Firewalls, Verschlüsselung oder Angriffserkennungssystemen, hin zu einer integrierten Betrachtung des Gesamtsystems. Statt die Systeme nur gegen bekannte Angriffe zu schützen, sei eine Methodik vonnöten, bei der mögliche Auswirkungen auch bisher nie gesehener Angriffe in mathematischen Modellen antizipiert werden.

## *IT-Sicherheit*

Mit der **Verletzlichkeit von Bussystemen** durch Hacker befasst sich PROTECTOR in der Ausgabe 4-2016, S. 42/43. Alle modernen Automobile würden durch ein Netzwerk von Computerbussen durchzogen, die eine Vielzahl von elektronisch kontrollierten Einheiten verbinden. Alle Busse seien mit dem wichtigsten Bus verbunden, der auch Motorbremse und ABS steuert, dem CAN-Bus (Controller Area Network). Er sei weit verbreitet und werde auch in Produktionsumgebungen und in Robotern verwendet. Die zahlreichen Angriffsmöglichkeiten auf diesen Bus beunruhigten deshalb auch Sicherheitsbeauftragte von Industrieanlagen. Wenn Hacker auf den CAN-Bus vordringen, könnten sie problemlos einen DoS-Angriff starten. In deutschen Fahrzeugen seien aber die einzelnen Gerätegruppen durch Segmentierung besser voneinander abgeschirmt, sodass der Angreifer hier zusätzliche Hürden überwinden müsse. Segmentierung sei auch

bei Industriesteuerungen das Mittel der Wahl, um Angriffe zu erschweren.

Helmut Brückmann weist in der April-Ausgabe von veko-online.de darauf hin, dass führende Security Analysten vom TÜV Rheinland sowie aus Großbritannien und den USA **neun Trends** für die Entwicklung der Cyberbedrohung und der IT-Sicherheit in den nächsten zwölf Monaten erkannt und erarbeitet hätten:

1. Cyberkriminalität wird einfacher und lukrativer.
2. Das Internet der Dinge eröffnet zusätzliche Angriffsmöglichkeiten.
3. Die Cloud sorgt für neue Betriebsmodelle.
4. Informationssicherheit geht über klassische Compliance hinaus.
5. Datenschutz und Datensicherheit bestimmen weiterhin die öffentliche Diskussion.
6. Incident Response wird zum „Daily Business".
7. Organisationen setzen verstärkt auf Managed Security Services.
8. Industrial Control System Security gewinnt eine neue Relevanz.
9. Der Bedarf an externer Cyber Threat Intelligence steigt.

Ein Angreifer mit **Kontrolle über einen WLAN-Hotspot** könne iPads zurück in das Jahr 1970 schicken und das Gerät dadurch außer Gefecht setzen, meldet heise.de am 13. April. Erst iOS 9.3.1 sorge angeblich für Abhilfe. Jüngst sei bekannt geworden, dass ein manueller Datumswechsel neuere iOS-Geräte lahmlegt. Drehe man das Datum zurück auf Anfang 1970, starteten iPhones oder iPads mit 64 Bit-Prozessoren nicht mehr richtig. Sicherheitsforscher hätten nun eine Methode beschrieben, mit der sich dieser Angriff automatisieren lasse. Die erzwungene Datumsrückstellung führe dazu, dass zuerst kein Aufruf von Webseiten mehr möglich sei. Starte der Nutzer das Gerät dann neu, zeige dieses sich verwirrt. Das Entsperren sei nicht länger möglich, zudem überhitze der Akku des iPad. Das Gerät schalte sich letztendlich ab und starte nicht mehr.

Die britische Communications Electronics Security Group, eine Abteilung des Nachrichtendienstes GCHQ, rate IT-Abteilungen davon ab, regelmäßige Änderungen von Passwörtern zu erzwingen, berichtet heise.de am 17. April. Das führe in der Praxis nicht zu höherer Sicherheit, unter anderem, weil sich daraus neue Risiken ergäben. Sichere Passwörter dürften nicht leicht zu knacken sein, seien deshalb recht lang und ließen sich nicht leicht merken. Wenn die IT-Administratoren die Wahl sicherer Passwörter erzwingen und auch noch deren häufigen Wechsel, dann reagierten mehr Nutzer darauf, indem sie Passwörter notieren, sie auch für andere Dienste verwenden oder beim erzwungenen Wechsel nur minimale Änderungen vornehmen.

Volker Kraiss, Kraiss & Wilke Security Consult GmbH, befasst sich in Ausgabe 5-2016 der Zeitschrift PROTECTOR, S. 44/45, mit der Abwehr von Cybercrime. Auf dem Markt befindliche Geräte und Software der Zeiterfassung und Zutrittskontrolle entsprächen mit ganz wenigen Ausnahmen nicht den Anforderungen an die Informationssicherheit. Die Angriffsmöglichkeiten der Cyberkriminellen seien vielfältig. Der Autor skizziert: Replay-Angriff oder Identitätsdiebstahl; Man in the Middle-Angriff oder Erbeuten von Keys; Spoofing oder das Vortäuschen; Firmware-Angriff oder Back-Door; Command-Injection oder Manipulation; Boot-Angriff oder Vollzugriff; Chip-Hacking oder Aufbohren/Freiätzen. Als einzusetzende Sicherheitsstandards benennt Kraiss: Trusted Platform Modules; Trusted Computing Concept, Root of Trust, X.509 Zertifikate, OAuth2 + SSL-Authentication, role-based User-Management, Advanced Event-Machine, Schlüssel im TPM, Secure Boot und verschlüsselte DB-Filesysteme. Updates sollten nur in Kombination mit geprüften Signaturen erfolgen.

## *IuK-Kriminalität*

Der TÜV sorgt sich um die Datensicherheit in Unternehmen, meldet die FAZ am 13. April. In Zeiten der digitalen Transformation könne die Wirtschaft leicht zum Ziel von Hackerangriffen werden. Um das zu beweisen, habe der TÜV Süd unter Verwendung realer Hardware und Software den **Betrieb eines Wasserwerks simuliert** und so potenzielle Angreifer angelockt. Während der achtmonatigen Laufzeit des Projekts habe es mehr als 60.000 ungebetene Zugriffe aus aller Welt gegeben, allen voran aus China, den USA und Südkorea. Zwei Dutzend Angreifer hätten sich bei der Sicherheit und Systemsteuerung von Kraftwerken so gut ausgekannt, „dass sie den Schalter hätten umlegen können". Großenteils würden die Risiken für die IT-Infrastruktur von Unternehmen nach wie vor unterschätzt.

Das BfV habe im November 2015 auf einen Cyberangriff auf einen deutschen Großkonzern hingewiesen, der sich in eine weltweit zu beobachtende Serie gleichartiger Angriffe einreihe und praktisch jedes Unternehmen treffen könne. Die dafür verantwortliche Gruppierung sei spätestens seit Juni 2015 aktiv. Sie nutze ein hochprofessionelles Schadprogramm, das von kommerziellen Antivirenprogrammen nur selten erkannt werde. Die Abteilung für Öffentlichkeitsarbeit des angegriffenen Konzerns habe eine englischsprachige Mail eines vorgeblichen Journalisten erhalten, der behauptete, in einem Hotelzimmer in Hongkong sei eine Minderjährige sexuell missbraucht worden. Der Täter sei auf einem Video erkennbar, das er innerhalb der nächsten drei Tage veröffentlichen werde. Er wolle dem Unternehmen zuvor Gelegenheit geben, den Täter anhand des kompromittierenden Videos als potenziellen Mitarbeiter zu identifizieren. Durch das Aufrufen der Videoseite über einen Link sei auf den verwendeten Rechnern der Opfer die Schadsoftware PlugX installiert worden, durch die der Angreifer die Möglichkeit erhalte, tief in das Firmennetzwerk einzugreifen. Das BfV werde die Kampagne weiterhin beobachten und Hintergrundinformationen sowie Handlungsempfehlungen für (potenziell) betroffene Unternehmen zur Verfügung stellen (Sonderbericht Wirtschaftsschutz vom 14. April).

Der Sonderbericht Wirtschaftsschutz der deutschen Bundessicherheitsbehörden vom 14. April weist darauf hin, dass nach dem aktuellen Bericht eines IT-Unternehmens Piratenangriffe auf See und in Häfen mittels Cyberspionage unterstützt würden. Eine offenbar kriminelle Gruppierung habe ein schwach geschütztes IT-System des Logistikbereichs einer Reederei kompromittiert und dabei Zugang zu wichtigen schiffsspezifischen Informationen erhalten, die sie für ihre Zwecke ausgenutzt hätte. Beim Schmuggel von Drogen sowie in Zusammenhang mit Entführungsfällen oder Schutzgelderpressungen habe in mehreren Fällen Ähnliches beobachtet werden können. Der Markt cyberkrimineller Dienstleistungen steige rasant an. Hier habe sich bereits der Begriff „**Hacking as a service**" etabliert. Noch schöpfe die Organisierte Kriminalität die Potenziale der Mittel im Cyberraum nicht aus. Aber es zeichne sich ab, dass diese zunehmend genutzt würden. Eine Cyberbedrohung von Reedereien als Beispiel für die weltweit verzahnte Logistik stelle mittelbar auch eine Gefahr für von dieser abhängige deutsche Unternehmen dar.

Nach einem Bericht von silicon.de vom 13. April hat Symantec im Jahr 2015 **430 Mio. neue Varianten an Schadsoftware** identifiziert. Das sei das Ergebnis des aktuellen Internet Threat Security Report des Sicherheitsanbieters. Diese Zahl liege 36 Prozent über der von 2014. Die Zahl der Zero-Day-Schwachstellen habe sich sogar um 125 Prozent auf 54 erhöht. Zugleich sei die Anzahl der Unternehmen, die nicht über ihre Datenverluste berichteten, um 85 Prozent gestiegen. Ungepatchte Sicherheits-

lücken hätten dabei nicht nur in Betriebssystemen und Anwendungen, sondern auch in 75 Prozent aller legitimen Websites gesteckt. 16 Prozent davon beinhalteten sogar als schwerwiegend eingestufte Anfälligkeiten. Die Annahme, der Besuch legitimer Websites schütze vor Cyberkriminellen, sei nicht mehr gültig. Die Mehrzahl der Schadsoftware habe Symantec 2015 in China gefunden. Der Anteil der Volksrepublik habe sich auf 23,7 Prozent gesteigert. Deutschland finde sich mit 2,2 Prozent auf dem achten Rang. Bei den zielgerichteten Angriffen liege Deutschland im weltweiten Vergleich auf Platz zehn mit einem Anteil von 2,2 Prozent und 2,1 Angriffen pro Organisation.

Die Frankfurter Allgemeine Sonntagszeitung befasst sich am 17. April mit der „**Underground Economy**". Das sei der kriminelle Markt im Netz. Auf den Foren und in den Online-Shops würden nicht nur Drogen gehandelt, sondern auch Falschgeld, gefälschte Ausweise, ausgespähte Kreditkarten- und Online-Banking-Daten sowie kriminelle Dienstleistungen, zum Beispiel die Infektion von Computern mit Schadsoftware. Zudem gebe es Anleitungen für alle möglichen Straftaten auf dem Gebiet der Internetkriminalität. Allein die deutschsprachigen Underground-Economy-Foren hätten derzeit annähernd 100.000 registrierte Nutzer. Nach Erkenntnissen von Ermittlern seien die meisten Nutzer sehr jung und wollten häufig nur ausprobieren, was möglich ist. Dann würden sie in der Szene aufsteigen: erst zu einfachen Mitgliedern in den Foren, dann zu Vollmitgliedern, schließlich zu Moderatoren und Administratoren. Die hielten die Foren technisch am Leben und stellten so Kriminellen wie etwa Drogen- und Waffenhändlern eine gut funktionierende Infrastruktur zur Verfügung. Beim BKA heiße es, relevante Motive der Internetkriminellen seien „der Spaß am Hacken, Neugier und Unterhaltungsaspekte. Aber auch die Gruppenzugehörigkeit, das Streben nach Status und Macht sowie das Streben nach Zerstörung oder Rache könnten eine Rolle spielen". Den Anwendern der Technik gehe es oft nicht um Anerkennung, sondern vor allem ums schnelle Geld. Anfang des Jahres hätten unbekannte Täter mehrere Krankenhausrechner in Nordrhein-Westfalen mit einer Schadsoftware infiziert. Die Schadsoftware habe Daten auf den Rechnern der Kliniken verschlüsselt. Die Kriminellen forderten für die Entschlüsselung Geld. Nach Aussagen von Ermittlern passierten solche Erpressungen ständig.

Die FAZ warnt am 20. April vor Online-Läden. **Gefälschte Markengeschäfte** täuschten Kunden. Die Betrüger profitierten von der wachsenden Selbstverständlichkeit des Online-Einkaufs. Das Abschalten der Internetseiten sei nicht so einfach, wie man sich das wünschen würde. Schließlich stünden die Server oft im Ausland. Die „Watchlist Internet" des österreichischen Internet-Ombudsmanns liste inzwischen über 200 betrügerische Online-Läden auf. Häufig gehe es um Elektroartikel. Doch es gebe auch „Fake-Shops" für Kaffemaschinen oder für Muskelaufbaupräparate und sogar für falsche Internetapotheken. Die Ermittlungen in der Anonymität des Internets stellten oft unlösbare Herausforderungen dar, teile die Göttinger Schwerpunktstaatsanwaltschaft zur Bekämpfung der Internetkriminalität mit.

Am 26. April berichtet die FAZ, dass nach Informationen der Nachrichtenagentur Reuters es Cyberkriminellen gelungen sei, möglicherweise in eine Software des internationalen **Zahlungsverkehrssystems SWIFT** einzudringen. Mit einem Schadprogramm hätten sie die SWIFT-Kundensoftware Alliance Access manipuliert. Damit hätten sie ihre Spuren verwischen wollen. Eine SWIFT-Sprecherin habe die Existenz eines Schadprogramms, das auf die Kundensoftware abziele, bestätigt. Ein Software-Update solle das Schadprogramm ausschalten. Außerdem solle eine Sicherheitswarnung an Finanzinstitute herausgegeben werden.

**Cyberangriffe auf die Gesundheitsbranche** haben nach einem Bericht von silicon.de vom 25. April ein nie dagewesenes Ausmaß erreicht. Fünf der acht schwersten IT-Sicherheitsvorfälle auf die Gesundheitsbranche der letzten fünf Jahre hätten sich im ersten Halbjahr 2015 ereignet. Jedes Mal seien über eine Million Datensätze gefährdet gewesen, 100 Mio. im gesamten Jahr. Damit sei der Gesundheitssektor laut IBM Cyber Security Intelligence Index 2016 das attraktivste Angriffsziel für Cyberkriminelle gewesen. Mittlerweile hätten sich beispielsweise Patientenakten zur absolut heißen Ware auf dem Internetschwarzmarkt entwickelt. Auf Basis dieser Beute ließen sich weitere Straftaten wie Identitätsdiebstahl oder Erpressung verüben. Bei oft unzureichender Absicherung sorgten Social Media, die Cloud, Big Data sowie der verstärkte Einsatz von Smartphone und Tablets im Unternehmen laut IBM für immer mehr Angriffsfläche. So stammten dem Unternehmen zufolge 2015 ca. 60 Prozent der Cyberattacken aus den eigenen Reihen der betroffenen Organisationen. Angreifer seien beispielsweise unzufriedene Ex-Angestellte, die noch über Passwörter verfügen oder gar Zugänge einrichten, bevor sie das Unternehmen verlassen.

Nach einem Bericht von heise.de vom 26. April sei der **Verizon Data Breach Investigations Report** (DBIR) die wohl umfassendste Untersuchung von weltweiten Datenlecks. Das Fazit der Autoren des aktuellen Reports: Es habe sich wenig getan in den letzten Jahren. Weiterhin stünden sämtliche Industriesektoren im Visier von Angreifern – wenngleich der Löwenanteil der Attacken Organisationen im Finanzsektor aufs Korn nimmt. Gut 90 Prozent aller untersuchten Datenpannen hätten eine finanzielle Motivation. Zudem räume der DBIR mit dem Mythos auf, dass ein respektabler Teil der Attacken von Innentätern ausgehe. Den Daten zufolge seien es in über 80 Prozent der Fälle externe Angreifer. Auch hinsichtlich der Wahl der Waffen zeige sich ein unverändertes Bild: Social Engineering sei ein sehr beliebter Einstieg für gezielte Angriffe. Gut 30 Prozent aller Phishing-E-Mails würden geöffnet, in 12 Prozent der Fälle klicke das Opfer auf den vergifteten Anhang oder den in der Nachricht platzierten Link. Aber auch klassisches Hacking gehöre noch immer zum Repertoire von Datendieben. Massenhaftes Verteilen von Malware gebe es nach wie vor im Finanzsektor, um beispielsweise Online-Banking-Nutzer zu berauben. Lorenz Kuhlee, Verizon Business, zeige wenig Verständnis für die nach wie vor große Zahl von Angriffen, deren Grundlage zuvor abgefischte Log-in-Daten seien. Denn mit der Zweifaktor-Authentifizierung gebe es seit langem eine bewährte Methode, dieser Angriffsart das Wasser abzugraben. Jedes Unternehmen sei im Visier von Angreifern, vom Kleinstunternehmen bis zum Dax-Konzern, vom kleinen Webshop bis zur Online-Präsenz eines Großunternehmens. Der Report erfasse auch Angriffe auf Industrieanlagen. Verizon erkenne eine Zunahme der Angriffe auf kritische Infrastrukturen weltweit. So gebe es einen stetigen Anstieg von Zwischenfällen und Verstößen in der Energieversorgung, der Produktion, im öffentlichen Sektor und in hohem Maße im Transportsektor in den vergangenen drei Jahren.

## *Kernkraftwerkssicherheit*

Nach einem Bericht der FAZ am 15. April hat das Umweltministerium Baden-Württemberg dem Energiekonzern EnBW bis auf weiteres den Betrieb seines **Kernkraftwerkes Philippsburg II** untersagt. Nach Angaben des Betreibers EnBW sei im Dezember 2015 eine sogenannte wiederkehrende Prüfung an einem Störfallmonitor von einem Mitarbeiter eines externen Dienstleisters offenbar nur vorgetäuscht worden. Bei der weiteren Untersuchung sei festgestellt worden, dass derselbe Mitarbeiter vermutlich sieben weitere Prüfungen an vergleichbaren Einrichtungen ebenfalls nur vorgetäuscht habe. Das Kraftwerk dürfe erst wieder hochgefahren

werden, wenn EnBW nachgewiesen habe, dass die Anlage „vorschriftsmäßig und sicher betrieben wird."

Nach einer Meldung von silicon.de vom 25. April ist bei routinemäßigen Prüfarbeiten im **Kernkraftwerk Gundremmingen** auf einem Rechner Schadsoftware gefunden worden. Laut dem Kernkraftwerk nahm der Virus aus zwei Gründen keinen Einfluss auf die Steuerung der Lademaschine. Erstens sei der befallene Rechner aufgrund der Systemarchitektur von den Steuerungsanlagen getrennt gewesen, zweitens habe es sich nicht um eine gezielt für diese Steuerungsanlagen konzipierte Malware gehandelt, sondern um eine Schadsoftware für Bürocomputer.

## *Kfz-Unfallsicherheit*

Nach einer Meldung in der FAZ am 5. April machen sicherheitsrelevante Systeme im Kfz nur etwa ein Prozent aller festgestellten Fahrzeugmängel aus, aber davon entfielen immerhin 48 Prozent auf Funktionsstörungen an Airbags und 32 Prozent auf ABS-Fehler. Eine zentrale Rolle bei der Aufspürung solcher Schwachstellen werde der am 1. Juli an den Start gehende **Hauptuntersuchungs-Adapter** spielen Mit ihm könne der Prüfer über die Onboard-Schnittstelle des Fahrzeugs die Ausführung der verbauten Sicherheitssysteme abfragen, aktuelle Sensordaten überwachen sowie Funktionswirkung und Zustand der sicherheitsrelevanten Fahrzeugsysteme kontrollieren. Zudem solle ein bordeigener Notbremsassistent (Advanced Emergency Braking System – AEBS) Kollisionsunfälle durch automatische Vollbremsung verhindern.

## *Korruption*

Wie viel Geld im Gesundheitssystem jedes Jahr durch Untreue, Abrechnungsbetrug und Korruption versickert, könne nur geschätzt werden, schreibt die Wochenzeitung DAS PARLAMENT am 18. April. Von bis zu 20 Mrd. Euro sei die Rede. Der GKV-Spitzenverband spreche wie das BKA von einem „großen Dunkelfeld". Regelmäßig würden mutmaßliche Betrügereien gemeldet. Die Krankenkassen hätten laut einer Aufstellung des GKV-Spitzenverbandes in den Jahren 2012/2013 rund 27.000 Fälle von Fehlverhalten gemeldet. Zusammen mit Altfällen würden rund 41.500 Fälle verfolgt. Nach dem jetzt vom Bundestag beschlossenen Gesetz, das **Korruption im Gesundheitswesen** erstmals ausdrücklich als Straftatbestand ausweist (§§ 299 a, 299 b, 300 StGB), werden künftig neben den niedergelassenen Vertragsärzten auch alle anderen Angehörigen von Heilberufen, für deren Ausübung oder Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erforderlich ist, von den Straftatbeständen der Bestechlichkeit und der Bestechung erfasst. Korruptionsfälle in den Gesundheitsberufen werden künftig als Offizialdelikte verfolgt.

## *Krisenregionen*

Matthias Wagner, Gesellschaft für Internationale Zusammenarbeit, gibt in Security insight, Ausgabe 2-2016, S. 46/47, Unternehmen **Tipps zum Schutz von Geschäftsreisenden** in Krisen- und Risikoregionen: Stellen Sie vor der Reise den Reisenden Informationen über das Land, die Sicherheitslage und wichtige Kontakte zur Verfügung. Bereiten Sie ein Willkommenspaket mit Informationen und einem Mobiltelefon mit lokaler SIM-Karte vor. Lassen Sie die Reisenden vom Flughafen abholen. Führen Sie vor Ort ein Sicherheitsbriefing durch und informieren Sie über die Risiken und Notfallmaßnahmen. Empfehlen Sie den Reisenden, die deutsche Auslandsvertretung zu kontaktieren und sich in die Krisenvorsorgeliste, das ELEFANT-System, einzutragen. Informieren Sie regelmäßig

über sicherheitsrelevante Entwicklungen. Der Reisende sollte die Ankunft im Land sowie An- und Abwesenheiten stets melden. Notfallkontaktdaten sollten beim Arbeitgeber hinterlegt sein.

In der Ausgabe 5-2016 von PROTECTOR, S. 71–73, befasst sich Dr. Nicolas Schwank mit der Bedeutung internationaler politischer Konflikte für die global vernetzte Wirtschaft. 2015 habe das mit **CONIAS** eng verbundene Heidelberger Institut für Internationale Konfliktforschung 409 Konflikte gezählt, von denen 43 aufgrund des massiven Einsatzes organisierter Gewalt als „hochgewaltsam" eingestuft worden seien. CONIAS (Conflict Information and Analysis System) sei ein über mehrere Jahrzehnte an der Universität Heidelberg in Zusammenarbeit mit der EU fortentwickelter Forschungsansatz zur Analyse von Konfliktdynamiken inklusive umfassender Datenbank zur Risikoeinschätzung politischer Konflikte. Die Datenbasis reiche zurück bis 1945. Gundlegende Idee des Ansatzes sei es, durch den Vergleich der Verlaufsmuster möglichst vieler politischer Konflikte bereits in Frühphasen das Eskalationspotenzial aktueller politischer Konflikte zu erkennen. Jährlich würden dazu rund drei Mrd. Artikel aus 40.000 Quellen gesichtet. Die Bestimmung des spezifischen Risikos erfolge mittels klar konzipierter Indikatoren, die auf dem Handeln und Kommunizieren der jeweiligen Konfliktakteure basierten. Die Qualität des Ansatzes zeige sich darin, dass die Methodik jeden der knapp 300 Kriege seit 1945 bereits in einer frühen Konfliktphase erfasse. Je nach Konflikttyp habe eine spätere kriegerische Eskalation in bis zu 90 Prozent der Fälle frühzeitig erkannt werden können. Wesentlich dramatischer als die Krisen des internationalen Systems sei die Entwicklung bei den innerstaatlichen gewaltsamen Konflikten zu sehen. Viele Konfliktgruppen seien ständig auf der Suche nach neuen Finanzquellen. Dadurch verwischten zunehmend die Unterschiede zu großen kriminellen Vereinigungen. Die langfristigen Auswertungen aus CONIAS zeigten einen eindeutigen Trend: Die politisch motivierte Gewalt nehme seit dem Ende des Kalten Krieges dramatisch zu.

## *Marktmanipulation*

Die FAZ weist am 15. April darauf hin, dass zahlreiche Bestimmungen über Insiderhandel, Kursmanipulation und Publizitätspflichten sich zum 3. Juli dramatisch ändern. Grund dafür seien zwei EU-Direktiven. Eine davon sei eine Verordnung, die von diesem Stichtag an europaweit unmittelbar gilt. Die andere sei eine Richtlinie, die Deutschland umsetzen müsse. Die wichtigste Neuerung sei eine ganz drastische **Verschärfung der Sanktionen** für Verstöße. Auf Unternehmen komme zudem ein erheblich höherer Bürokratieaufwand für Meldepflichten zu. Schon der Versuch einer Marktmanipulation könne künftig bestraft werden. Schwere Fälle würden erstmals als Verbrechen eingestuft. Unternehmen drohe eine Buße von bis zu 15 Prozent des Umsatzes des gesamten Konzerns, also ohne jede Obergrenze. Verstöße müsse die Bundesanstalt für Finanzdienstleistungsaufsicht (Bafin) nach dem Prinzip des „Naming and Shaming" im Internet veröffentlichen, und zwar schon, bevor der Verdacht rechtskräftig bewiesen ist. Ausgeweitet werde überdies die Definition von Insiderinformationen. Das dehne den Bereich strafbarer Geschäfte und der gesetzlichen Ad hoc-Meldepflichten unter anderem auf den Freiverkehr aus. Geschäfte von Vorständen und Aufsichtsräten mit Aktien des eigenen Unternehmens müssten häufiger als bisher aufgedeckt werden. Auch gelte für Führungskräfte ein längeres Handelsverbot.

## *Maschinensicherheit*

**Sichere Betriebsartenwahl**, in Maschinenvisualisierung integriert, thematisiert GIT in der Ausgabe 4-2016, S. 82–84. Betriebsarten wie Einrichten, Reinigen und Fehlerbeheben

erforderten sicherheitstechnisch gesehen besondere Aufmerksamkeit, denn manuelle Eingriffe und geöffnete Schutzeinrichtungen änderten die sicherheitstechnischen Rahmenbedingungen. Dass die Sonderbetriebsart auch wirklich nur vom dafür autorisierten und besonders unterwiesenen Personenkreis benutzt wird, sollten Betriebsartenwahlschalter mit Schlüsselfunktion sicherstellen. Immer öfter seien aber mehrere Sonderbetriebsarten notwendig, und so käme es oft zu einer komplexen Matrix an Sonderbetriebsarten und dem zugehörigen Personenkreis. Mit dem „openSAFETY-Interface" böte B&R Industrie Elektronik GmbH Bediengeräte mit integrierten Bedienelementen wie den erwähnten Betriebsartenwahlschalter mit Schlüsselfunktion, aber auch allen anderen typischen Funktionen wie Starttaster oder Not-Aus-Taster. Die Bedienelemente seien in die Bildschirmfront integriert. Diese Bediengeräte seien für Anwender gedacht, die nach wie vor einen **Schlüsselschalter für die Auswahl der Betriebsart** bevorzugen. Möchte man den Betriebsartenwahlschalter vollständig in die Maschinenvisualisierung integrieren, so werde das mit dem Technologiepaket Safe Option aus der „B&R mapp Technology" ermöglicht.

Dipl.-Phys. Andreas Jüttner verspricht in der Ausgabe 4-2016 der Zeitschrift GIT (S. 86/87), mit dem Sicherheits-Lichtschrankenset MLDSET werde die **Errichtung von Zugangssicherungen mit Muting** so einfach wie noch nie. Die Kernkomponente von MLDSET sei die Mehrstrahl-Sicherheitslichtschranke MLD 500 in Transceiver-Ausführung. Solche Systeme bestünden aus einem aktiven Transceiver – Sender und Empfänger befänden sich in einem gemeinsamen Gehäuse – und einem passiven Umlenkspiegel ohne elektrischen Anschluss. Ein weiterer Vorteil der MLD-Geräte sei, dass sie generell für Niedertemperatur-Umgebungen geeignet und bis -30 Grad voll funktionsfähig sind.

Jonas Urlaub, Kübler Group, behandelt in der Ausgabe 4-2016 der Fachzeitschrift GIT (S. 88/89) **Sicherheits-Module bei Fahrgeschäften**. Damit die Sicherheitstechnik bei Karussels und Bahnen stets stabil und zuverlässig arbeiten kann, kämen zertifizierte Drehzahlwächter nach den Standards SIL3 und PLe zum Einsatz. Diese Safety-M-Sicherheitsmodule benötigten wenig Bauraum und passten universell zu den Einsätzen an Fahrgeschäften. Nicht nur die automatische Geschwindigkeitsregelung übernähmen die Safety-Drehzahlwächter. Die Geräte besäßen umfassende geschwindigkeits- und positionsbezogene Sicherheitsfunktionen zur Antriebsüberwachung, zertifiziert nach DIN EN 61800-5-2 und in der Firmware integriert.

**Geräteschutz vor Überspannung** thematisiert Thomas Bings, Phoenix Contact GmbH & Co. KG, in der Ausgabe 4-2016 der Fachzeitschrift GIT (S. 90/91, 93). Mittels Typ-3-Überspannungssschutzbaustein schütze man Endgeräte. Dazu müsse er mit einem geeigneten Überstromschutz abgesichert werden. Weil bei den Typ-3-Ableitern aus der Produktfamilie SEC von Phoenix Contact dieser Schutz bereits integriert sei, könne auf eine separate Vorsicherung verzichtet werden. So werde 50 Prozent Platz auf der Tragschiene eingespart.

GIT weist in der Ausgabe 4-2016, S. 92, auf neue **standardisierte Kennwert-Bibliotheken für den Maschinenbau** (VDMA 66413) hin. Bislang habe man bei der Berechnung der Ausfallwahrscheinlichkeit vor dem Problem gestanden, dass sich die Gerätekennwerte von Hersteller zu Hersteller im Format unterschieden. Nun hätten Anbieter und Anwender zur Lösung dieser Aufgabe gemeinsam ein standardisiertes Format erarbeitet. Das VDMA Einheitsblatt 66413 beschreibe die erforderlichen sicherheitsrelevanten Kennwerte von Automatisierungsgeräten und lege ein einheitliches elektronisches Datenformat für die Bereitstellung der Sicherheitskennwerte fest.

## *Notausgang*

Security insight stellt in der Ausgabe 2-2016, S. 53, ein von GfS, Gesellschaft für Sicherheitstechnik GmbH, entwickeltes, multifunktionales Überwachungsgerät für Notausgangstüren und Fluchtfenster vor. Werden Tür oder Fenster missbräuchlich geöffnet, ertöne ein lauter Alarm von 95 dB/1m. Das Gerät werde in der Standardversion mit einer 9-Volt-Blockbatterie betrieben, könne aber auch an ein Stromnetz angeschlossen werden. Da es völlig unabhängig von vorhandenem Türbeschlag oder Fenstergriff funktioniere, eigne es sich hervorragend zur Nachrüstung.

## *Öffentlicher Personenverkehr*

Rainer Cohrs, Münchner U-Bahn-Bewachungsgesellschaft, äußert sich in Security insight, Ausgabe 2-2016, S. 10/11, zur **Münchner U-Bahnwache**, einem Joint Venture zwischen den Stadtwerken München (51 Prozent) und Securitas (49 Prozent). Die Mitarbeiter würden von Polizeibeamten ausgebildet. Jeder absolviere eine Ausbildung von über 750 Stunden. Die offen getragene Bewaffnung sei eine Voraussetzung für die gemischten Streifen von Polizeibeamten und U-Bahnwache. Gewaltdelikte gebe es im Münchner U-Bahnverkehr einmal pro drei Millionen Fahrten, also sehr selten. Auch Raub- und Diebstahlsdelikte kämen kaum vor. In den Fahrzeugen und Bahnhöfen seien über 4.000 Videokameras installiert. Die Fahrgäste hätten kein Problem mit der Videoüberwachung.

Einen leichten Rückgang der Zahl der registrierten Straftaten auf **Bahnhöfen und in Zügen** 2015 von ca. 60.000 auf 58.200 meldet die FAZ am 26. April. 2015 habe die Deutsche Bahn mehr als 1,5 Mio. Euro für die Reparatur von Vandalismus-Schäden durch Hooligans ausgegeben und mehr als 700.000 Euro für zusätzliche Sicherheitskräfte. Künftig wolle die Deutsche Bahn noch schärfer gegen gewaltbereite Fußballfans vorgehen. Hausverbote würden an Ort und Stelle ausgesprochen, randalierende Hooligans sofort aus dem Zug verwiesen. Die Eisenbahn- und Verkehrsgewerkschaft konstatiere zunehmende Gewalt gegen Beschäftigte in den Verkehrsbetrieben. Habe die Bahn 2013 noch 1.200 Übergriffe gegen Mitarbeiter registriert, seien es 2015 schon 1.800 gewesen. Es handle sich weniger um Kriminelle, als vielmehr um Menschen „aus der Mitte der Gesellschaft".

Hendrick Lehmann, Redaktion PROTECTOR, befasst sich in Ausgabe 5-2016, S. 28–31, mit der strategischen **Planung in kritischen Verkehrsnetzen**. Unternehmen und Verkehrsbetreiber zusammen hätten unter Führung des Lehrstuhls für Operation Research an der Universität der Bundeswehr München nach einem ganzheitlichen Ansatz eines Risikomanagements für den schienengebundenen öffentlichen Personenverkehr geforscht. Zunächst seien die möglichen Bedrohungen des öffentlichen Personenverkehrs analysiert worden. Gleichzeitig seien die Kosten möglicher Sicherheitsmaßnahmen erfasst worden. Geklärt werden sollte auch, inwieweit Sicherheitssysteme potenzielle Angriffe entdecken können und wie ein effektives Krisenmanagement aussehen könnte. Die Bewegungsmuster von Personen in Notsituationen seien erfasst und in einer Simulation reproduziert worden. Neben Personenströmen ließen sich in Simulationen auch komplexe Szenarien abbilden, die bereits mit dem Verhalten des Attentäters beginnen würden. In einer agentenbasierten Simulation würden Anschlagsszenarien simuliert und die Effektivität diverser Sicherheitsmaßnahmen sowie deren Interdependenzen getestet. Die Darstellung werde in einem 3-D-Umfeld realisiert. Mit einer ausreichend großen Zahl an Simulationen ließen sich valide Aussagen treffen, unter welchen Bedingungen Sicherheitssysteme besser oder schlechter funktionieren, und Schwachstellen aufdecken.

Fragen der **Terrorismusabwehr im ÖPNV** behandelt LUCIUS Consulting GbR in Heft 5-2016 der Zeitschrift PROTECTOR, Ausgabe 5-2016, S. 66–70. Die wesentliche Basis einer effektiven Terrorismusabwehr seien fundierte Grundkenntnisse und aktuelle Informationen über Theorie und Praxis des islamischen Terrorismus. Bei der Optimierung sollte mit der kritischen Überprüfung bisheriger Einsatz- und Streifenpläne begonnen werden. Die Präsenz von Sicherheitskräften sollte sich nicht im operativen Einsatz widerspiegeln, sondern insbesondere im sicheren und selbstbewussten Auftreten. In vielen Verkehrsbetrieben müsste aber auch an der allgemeinen Kommunikationsstrategie gearbeitet werden. Verkehrsbetriebe sollten klare Botschaften senden, sodass dem Fahrgast deutlich werde, welches Verhalten von ihm erwartet wird.

Es müsse auch über eine grundsätzliche Erweiterung und Innovation der Sicherheitssysteme im ÖPNV nachgedacht werden. Die Implementierung von Zugangsschleusen, Körper- oder Gepäckscannern, Stichprobenkontrollen von Gepäckstücken, personalisierten Fahrscheinen sowie frühzeitiger Erkennungssysteme für Sprengstoff sollten konzeptionell erarbeitet werden. Entscheidend für den Nutzen der technischen Observation sei eine effektive und gründliche Bildauswertung durch den Bediener. Der wichtigste Sensor sei der Mitarbeiter im operativen Sicherheitsdienst, der mit seinen Sinnen und Verstand die Umwelt aus verschiedenen Blickwinkeln wahrnimmt und so Gefahren oder Auffälligkeiten erkenne. Geachtet werden sollte beispielsweise auf Wunden, Verletzungen und Verbrennungen, einschlägige Tätowierungen oder blasse Hautpartien, die auf eine frische Bartrasur schließen ließen. Das optische Erscheinungsbild werde darüber hinaus hinsichtlich besonderer Kleidungsmerkmale analysiert, etwa ungewöhnliche, vor allem lange oder weite Kleidung wie zum Beispiel Regenmäntel, auch wenn es nicht regnet. Wirksam beeinträchtigt würden Vorbereitungshandlungen von Terroristen auch durch sogenannte RAMs (Random Antiterror Measures). RAMs sollten signifikant vom Routinedienst abweichen und dürften nicht berechenbar sein. Und sogenannte Reaktionsmuster seien ein effektives, weil trainierbares, Mittel der reaktiven Terrorismusabwehrverfahren. Sie sollten für bestimmte, regelmäßig wiederkehrende sowie zukünftig mögliche Situationen und Szenarien entwickelt werden. Im Rahmen der behördlichen Terrorismusabwehrmaßnahmen müssten die ÖPNV-Betriebe nicht nur unterstützend tätig sein, sondern könnten mit einem eigenen Terrorabwehrkonzept einen wesentlichen Beitrag zur Terrorismusabwehr leisten.

## *Perimeterschutz*

Die Zeitschrift PROTECTOR enthält in der Ausgabe 5-2016, S. 37, eine Marktübersicht über 124 Freilandsicherungssysteme von 53 Anbietern. Zu den 63 abgefragten Kriterien gehören Zonenlänge sowie Tür- und Torüberwachung.

## *Piraterie*

Die Bundeswehr soll den Atalanta-Einsatz am Horn von Afrika fortsetzen, berichtet die Wochenzeitung Das Parlament am 18. April. Die personelle Obergrenze für den bewaffneten Einsatz soll allerdings von derzeit 950 auf 600 Soldaten verringert werden, wie aus einer Antwort der Bundesregierung (18/8091) hervorgehe. Der Parlamentarische Staatssekretär des Verteidigungsministeriums, Ralf Brauksiepe, habe die Mission als eine „Erfolgsgeschichte" bezeichnet. Seit 2012 habe es **keine Schiffsentführungen mehr** gegeben, auch die Zahl der versuchten Raubüberfälle auf Handelsschiffe sei auf null gesunken.

## Polizeiliche Kriminalstatistik

Das Wochenmagazin FOCUS analysiert am 30. April – im Vorgriff auf die Bundeskriminalstatistik, die am 23. Mai veröffentlicht werden soll – die Kriminalstatistiken der Bundesländer. Die Zahl der registrierten Straftaten (Verdachtsfälle) sei gegenüber dem Vorjahr um vier Prozent gestiegen, auf nunmehr 6,33 Mio. Fälle. Die Zahl der Tatverdächtigen sei um 13 Prozent auf mehr auf 2,43 Mio. in die Höhe geschnellt. Einen deutlichen Sprung habe es auch bei der Häufigkeitszahl (Zahl der Straftaten pro 100.000 Einwohner) gegeben: von 7.530 auf 8.667 (15 Prozent). Die höchste Zahl wurde in Berlin mit 16.414 registriert (die niedrigste in Baden-Württemberg mit 5.761). Bei Kfz-Diebstählen sei die Häufigkeitszahl ebenfalls in Berlin am höchsten (192), am niedrigsten in Baden-Württemberg (14) und Bayern (15). Nach FOCUS-Recherchen stieg der bundesweite Anteil nichtdeutscher Tatverdächtiger 2015 gegenüber 2014 um fast 51 Prozent auf 932.000. Damit machten Ausländer 38,3 Prozent der Verdächtigen aus. Erneut zugenommen habe die Gewalt gegen Polizisten.

## Produktpiraterie

Am Institut für Technische Optik der Universität Stuttgart sei ein System mit einer Mikrolinse entwickelt worden, die es dem Käufer einfach machen solle, festzustellen, ob der Kaufgegenstand ein Original oder eine Kopie ist. Er könne das Produkt im Laden in Sekundenschnelle überprüfen und Fälschungen erkennen. Der brauche dafür lediglich ein gewöhnliches handelsübliches Smartphone mit Kamera ohne weitere Zusatzeinrichtung. Die Mikrolinse diene nicht selbst als Sicherheitsmerkmal, sondern ermögliche im Zusammenwirken mit dem Smartphone eine Erfassung von Zufallsmerkmalen der Produktoberfläche. Kopiert ein Fälscher das Produkt, zeige das Bild eine komplett andere Struktur als die vom Hersteller als Referenz hinterlegte Struktur. Die Erfindung umzusetzen lohne sich allerdings nur für eine große Produktionsmenge.

Die deutschen **Maschinenbauer** bleiben im Visier von Produktpiraten – und sie verlieren dadurch nicht nur viel Umsatz, sondern auch die Möglichkeit, mehrere Zehntausend weitere Stellen zu schaffen, berichtet die FAZ am 30. April. Das sei das Ergebnis einer Studie, die der VDMA auf der Hannover Messe vorgestellt habe. Demnach seien 70 Prozent der deutschen Unternehmen betroffen, der geschätzte Umsatzschaden betrage 7,3 Mrd. Euro. Als häufigste Plagiateure hätten die befragten Unternehmen Konkurrenten (76 Prozent) vor sogenannten Underground Factories (27 Prozent) und Kunden (16 Prozent) genannt. China gelte weiterhin als Fälscher-Herstellungsland Nummer eins. Die diesmal ermittelten 83 Prozent markierten einen neuen Rekord.

## Reisesicherheit

Der Bundesverband ASW hat in einem Leitblatt Empfehlungen bei Angriffen und Anschlägen in Hotels und anderen Gebäuden gegeben, und zwar mit folgenden Grundregeln: – Machen Sie sich grundsätzlich immer mit Alarmierungsmodalitäten und Fluchtwegen vertraut. – Vermeiden Sie Panik und bringen Sie Ihre Angst so unter Kontrolle, dass Sie schnell und situationsgerecht handlungsfähig werden. – Schalten Sie alle Töne von Mobiltelefonen und Smartphones aus. – Versenden Sie keine Kurznachrichten über Twitter, Facebook & Co. – Grundsätzlich sollten Sie versuchen zu flüchten. Erscheint Ihnen eine risikolose Flucht nicht möglich, verstecken Sie sich. – Versuchen Sie in keinem Fall, verbal oder physisch auf die Täter einzuwirken. Für das Verhalten im Hotelzimmer rät der ASW: – Ziehen Sie die Schlüssel-

karte, schalten Sie Licht, Radio und andere Verbraucher ab. Öffnen Sie auch nicht mehr die Minibar, weil deren Nutzung eventuell an der Rezeption sichtbar ist. – Verriegeln Sie nicht die Tür. Wenn der Angreifer nicht mit Sicherheit weiß, dass Sie sich im Zimmer befinden, versuchen Sie den Eindruck zu erwecken, es sei leer. – Verbarrikadieren Sie die Tür, wenn Sie annehmen müssen, der Angreifer weiß, dass Sie sich im Zimmer befinden. – Verstecken Sie sich. – Versuchen Sie, wenn möglich, Informationen nach draußen zu geben.

## *Schließsysteme*

Für mehr **Flexibilität mit batteriebetriebenen Schlössern** plädiert PROTECTOR in der Ausgabe 4-2016, S. 24/25. Mechatronische Schließzylinder ohne Netzwerkanbindung hätten einen großen Nachteil: Beim Verlust einer Schlüsselkarte blieben die darauf übertragenen Berechtigungen 24 Stunden oder länger gültig. Dadurch steige das Sicherheitsrisiko. Bei batteriebetriebenen Schließzylindern, die per Wireless-Signal und Netzwerkschnittstelle (Gateway) eingebunden werden, ließen sich dagegen Zugangsrechte sofort anpassen. Batteriebetriebene mechatronische Systeme öffneten sich durch RFID-basierte Karten, sofern der Inhaber berechtigt ist. Die Integration von batteriebetriebenen Schließzylindern in die zentrale Zutrittssteuerung erfolge zum Beispiel offline über ein „Network on Card-System". Bei diesen Systemen würden die Berechtigungen für 24 Stunden oder länger auf die jeweiligen Karten programmiert. Mit wireless-fähigen, batteriebetriebenen Schließzylindern (E-Zylindern) oder Türdrückern bestehe nun die Möglichkeit, die Türen über Funk an das Host-System anzubinden. Ein Anwendungsbeispiel für Wireless-Gateway seien Meeting- und Konferenzräume, deren Berechtigungen sich fortwährend ändern, je nachdem, welche Mitarbeiter oder sonstige Personen sie gerade nutzen. Hier sei eine schnelle und einfache Rechtevergabe sinnvoll.

**Elektronische Zutrittslösung für Schulen** thematisiert PROTECTOR in der Ausgabe 4-2016, S. 26/27. Das Sicherheitskonzept für Schulen beruhe auf den drei Säulen: Alarmierung in Gefahrensituationen, Schließung von Räumen auch ohne die Anwesenheit von Lehrern und Außensicherung. Ein elektronisches Zutrittssystem löse gleich mehrere Probleme. Es sei einfacher zu handhaben und schütze gleichzeitig die Außenhaut der Gebäude, vor allem, wenn kein Schulbetrieb herrscht, denn die Türen würden außerhalb der Schulzeiten automatisch geschlossen. Beim Salto Virtual Network sei die Schreib-/Lese-Funktion patentiert und erfolge die Datenübertragung verschlüsselt. Information über gesperrte Identmedien oder beispielsweise Batteriestände würden von den Beschlägen und Zylindern auf die Identmedien geschrieben und somit weitergegeben. Online-Wandleser übertragen die ausgelesenen Daten an den zentralen Server und übermitteln gleichzeitig die aktuellen Schließberechtigungen auf das Identmedium.

Die Zeitschrift PROTECTOR gibt in Ausgabe 4-2016, S. 28/29, eine **Marktübersicht zu 116 mechatronischen Schließsystemen** von 48 Anbietern. Die Online-Tabelle bietet je Firma 22 abgefragte Kriterien, unter anderem aus den Bereichen Datenübertragung, Schließzylinder, lieferbare Typen und Baulängen, Eignung für einzelne Schlossarten und Außenmontage, IP-Klasse, Temperaturbereich und relative Luftfeuchtigkeit, Zylinder, Software, Hardwarevoraussetzungen, unterstützte Betriebssysteme, Netzwerkfähigkeit integrierter Software, Mandantenfähigkeit, Zugriffsschutz auf personifizierte Daten, integrierte Zutrittskontrollfunktionen.

## *Sicherheitskleidung*

Moderne **Dämpfungstechnologie für Sicherheitsschuhe** thematisiert GIT in der Ausgabe 4-2016, S. 100/101. Wenn sich Mitarbeiter in ihren Sicherheitsschuhen viel auf harten Böden bewegen, lange stehen oder häufig in der Hocke arbeiten, belaste das Sehnen, Muskeln und Gelenke, insbesondere wenn der Fußschutz schlecht gedämpft ist. Deshalb hätten Fußschutz-Hersteller gemeinsam mit Wissenschaftlern nach Lösungen gesucht. So seien Sicherheitsschuhe entstanden, die dämpfen und federn wie nie zuvor.

## *Sicherheitstechnik*

Dr. Peter Fey, Unternehmensberatung Dr. Wieselhuber & Partner, stellt in der Ausgabe 4-2016 der Zeitschrift PROTECTOR, S. 8/9, **Ergebnisse des dritten Branchenbarometers** von PROTECTOR & WiK vor. Die höchsten Wachstumsraten würden branchentypisch im Bereich Video erwartet (74 Prozent erwarteten ein Wachstum von über acht Prozent). Die zweithöchsten Wachstumswerte weist das Segment Zutrittskontrolle (über 90 Prozent rechneten mit einem Wachstum zwischen drei und acht Prozent). Die niedrigsten Wachstumsraten würden mit ein bis vier Prozent in den Bereichen Einbruchmeldesysteme, sonstige Gefahrenmeldetechnik und mechanische Sicherheitslösungen erwartet. In Summe lägen die Ergebnisse mit einer durchschnittlichen Wachstumserwartung von 5,2 Prozent geringfügig oberhalb des vor einem halben Jahr abgefragten Werts (fünf Prozent). Die Umsatzerwartung hinke der Entwicklung der Märkte geringfügig hinterher. Das lasse vermuten, dass die Wettbewerbssituation Druck ausübt. 55 Prozent der Unternehmen gingen von fallenden Preisen zwischen ein bis mehr als acht Prozent aus. 35 Prozent erwarteten hingegen leicht steigende Preise in Höhe von ein bis zwei Prozent. Für die Strategie der Kostenführerschaft ergebe sich lediglich eine unterdurchschnittliche Ausprägung in Höhe von 2,3 (Maximalwert 5,0). Die wesentlichen Differenzierungshebel würden in einem sehr guten After-Sales-Service (4,5), einem ausgezeichneten Lieferservice und einer einfachen Usability beziehungsweise Nutzeroberfläche, einer guten Pre-Sales-Beratung sowie in branchenspezifischen Sonderlösungen und in einer exzellenten Hardware gesehen. Mit hohen Ausprägungen werde mit der Ausweitung des Wettbewerbsumfeldes durch neue Branchenplayer gerechnet. Dabei erhielten die meisten Nennungen Unternehmen aus dem Bereich Smart Home und Smart Building/Gebäudeautomatisierung (beide 3,6).

## *Spionage*

Die geopolitische Lage Deutschlands im Zentrum Europas, der Einfluss in der EU, die Mitgliedschaft in der NATO, die große Wirtschaftskraft mit vielen innovativen Unternehmen und die weltweite Anerkennung deutscher Wissenschafts- und Forschungsleistungen öffentlicher und privater Stellen rückten die Bundesrepublik ins Zentrum nachrichtendienstlicher Aufklärungsbestrebungen, argumentiert das BfV im Newsletter Ausgabe 1-2016. **Russische nachrichtendienstliche elektronische Angriffe** gegen deutsche Ziele seien meist Teil mehrjähriger, international ausgerichteter Cyberspionage-Operationen im Rahmen einer umfassenden strategischen Informationsgewinnung. Deren Angriffskampagnen zeichneten sich durch eine hohe technische Qualifikation aus, verdeutlichten starke finanzielle Ressourcen und ließen in Art und globalem Umfang der Operationen außergewöhnliche Operativ- und Auswertefähigkeiten erkennen. Einige dieser Operationen ließen sich über eine Zeitspanne von sieben bis zehn Jahren zurückverfolgen. Viele dieser Angriffskampagnen wiesen untereinander technische Gemeinsamkeiten auf.

Auch bei der Informationsgewinnung mittels elektronischer Angriffe liege der Fokus der russischen Dienste auf allen Politikfeldern, die russische Interessen berühren können. Die russischen Angreifer demonstrierten ihr technisches Know-how unter anderem anhand einer großen Bandbreite schwer zu detektierender Angriffsvektoren. Sie umfasse E-Mails mit Schadanhang oder Links zu Webseiten mit Schadcode, USB-Sticks, Phishing-Seiten, Watering Holes und infizierte legitime Webseiten. Spear-Phishing-Angriffe zeichneten sich durch gutes Social Engineering der auf das Opfer zugeschnittenen E-Mails aus. Bei der Analyse staatlich gesteuerter elektronischer Angriffe aus Russland zeige sich deutlich die hohe informationstechnische Qualität dieser Angriffsoperationen. Die festgestellten Angriffe erfolgten meist sehr zielgerichtet und passgenau. Die jeweiligen Opfer würden gezielt ausgewählt.

Die deutsche Wirtschaft besser vor Angriffen auf ihre Unternehmenswerte schützen – das ist nach einer Erklärung der Bundesregierung vom 26. April das Ziel der „**Initiative Wirtschaftsschutz**". Dahinter stünden das Bundesinnenministerium sowie Verbände und Sicherheitsbehörden. Sie haben heute die Nationale Wirtschaftsschutzstrategie vorgestellt und die neue Internetplattform der Initiative (www.wirtschaftsschutz.info) offiziell freigeschaltet. Das Herzstück der Initiative sei die Informationsplattform. Auf dem Internetangebot stellten Sicherheitsbehörden und Verbände Informationen für sämtliche deutsche Unternehmen zur Verfügung. Ein Leitfaden für Unternehmen sowie Seminare und Veranstaltungen rundeten das Angebot der „Initiative Wirtschaftsschutz" ab. An der Initiative beteiligen sich der BDI, die DIHK, die ASW und der BDSW. Bei der Vorstellung sagte der Präsident des BDI, „ein Unternehmer, der glaubt, sein Unternehmen ist zu unwichtig, um angegriffen zu werden, begehe einen großen Fehler". Der Präsident der DIHK wies darauf hin, dass die deutsche Wirtschaft ca. 1.300 Weltmarktführer habe. Er riet von gesetzlichen Regelungen zum Wirtschaftsschutz ab und präferierte partnerschaftliche Zusammenarbeit. Der Bundesinnenminister betonte, die Initiative wolle das Bewusstsein dafür schaffen, dass Sicherheit kein Selbstzweck ist, Chefsache ist, und dass in Sicherheit investiert werden muss. Innovation und Sicherheit seien zwei Seiten einer Medaille. Das Schutzniveau gleiche in Deutschland einem Flickenteppich. Der digitalen Innovation müsse eine digitale Sicherheitskette entsprechen. Das Bundeskabinett habe vor zwei Wochen die Verordnung zur Umsetzung des IT-Sicherheitsgesetzes beschlossen. Eine Verordnung für andere kritische Infrastrukturbereiche werde bald folgen. Auch Unternehmen, die von dieser Verordnung nicht erfasst werden, würden gut daran tun, die Standards zu übernehmen.

## *Steuerhinterziehung*

Wuppertaler Steuerfahnder bereiteten eine **Fahndungswelle wegen dubioser Aktiengeschäfte** („Cum Ex-Deals") vor, berichtet die FAZ am 15. April. Hintergrund sei eine Datensammlung über ungedeckte Leerverkäufe, die die Behörde gekauft habe. Viele Fälle habe man an andere Finanzämter im ganzen Bundesgebiet weitergegeben. Solche Fälle seien strafbar, weil sie auf heimlichen Absprachen beruhten, um den Fiskus zu betrügen. Der einzige Zweck solcher Transaktionen bestehe darin, sich eine nur einmal gezahlte Kapitalertragsteuer mehrfach erstatten zu lassen. Das könne nur funktionieren, wenn die Beteiligten sich kennen. Eine Gesetzeslücke, auf die sich die Beteiligten berufen, habe es nie gegeben.

## *Terrorismus*

Florian Peil, Security Analyst & Consultant, beleuchtet in der Ausgabe 4-2016 von PROTECTOR (S. 66-69) **Strategie und Taktiken**

**der Dschihadisten**. Die Terrorstrategie sei 2005 von Abu Musab Al-Suri formuliert worden („Aufruf zum globalen islamischen Widerstand", 1.600 Seiten). Die Schrift sei für Dschihadisten aller Couleur die vermutlich einflussreichste strategische Schrift. Auch Al Qaida-Chef Aiman al-Zawahiri habe sie in seinen Videobotschaften mehrfach empfohlen. Al-Suri propagiere zweierlei: Erstens eine Strategie des dezentralen oder führerlosen Dschihad, zweitens enthalte die Schrift konkrete Anweisungen für die Durchführung von Terroranschlägen. Dabei spreche sich Al-Suri in aller Deutlichkeit für Massenmorde aus. Der IS setze auch darauf, mit derartigen Anschlägen aggressive Reaktionen gegen Muslime zu provozieren. Diesen solle keine andere Option mehr bleiben, als sich dem IS anzuschließen. Die Anschläge von Paris und Brüssel stellten nicht nur in strategischer Hinsicht einen Meilenstein dar. Neu sei zum einen der Einsatz unabhängig operierender Hit-Teams, das Vorgehen gegen mehrere weiche Ziele unterschiedlicher Natur sowie der kombinierte Einsatz von Schusswaffen, Bomben und Sprengstoffgürteln. Der Modus Operandi von Paris könne die Blaupause für weitere Anschläge sein, gewissermaßen als „best practices" des Terrorismus. Die Attentäter von Mali, wo zwei mit Sturmgewehren bewaffnete Terroristen das Radisson Blu Hotel in Bamako stürmten, gehörten nicht dem IS an, sondern seien Mitglieder von Al Qaida im Islamischen Maghreb (AQIM) gewesen. Große Hotels zählten gegenwärtig zu den bevorzugten Angriffszielen von Dschihadisten, insbesondere in der Sahelzone. Dies sei darauf zurückzuführen, dass Botschaften und andere diplomatische Einrichtungen ihre Sicherheitsmaßnahmen seit den 1980er-Jahren verstärkt hätten.

In der Ausgabe 2-2016 der Fachzeitschrift Security insight, S. 44/45, nehmen Pascal Michel und Michael Pülmanns, SmartRiskSolutions GmbH, Stellung zum Abschlussbericht des britischen Untersuchungsrichters über einen **Terroranschlag auf eine Gasanlage in Algerien** am 16. Januar 2013 mit 39 Todesopfern. Im Wesentlichen kritisiere der Untersuchungsrichter drei Kernbereiche des Sicherheitsmanagements: Risikoanalyse, Sicherheitsmaßnahmen des Konsortiums sowie die starke Abstützung auf die algerischen Sicherheitskräfte für den Schutz des Gasfeldes. Und sie ziehen **Konsequenzen für Unternehmen**: Das Lagemonitoring müsse lokale Medienberichte beachten und in die Beurteilung einfließen lassen. Empfehlungen der Sicherheitsmanager seien schnell umzusetzen, und dies sei auch zu überprüfen. Sicherheitsmaßnahmen sollten auch einem regionalen Benchmark unterzogen werden.

## *VdS*

Sicherheitsberater Adolf Kraheck befasst sich in Security insight, Ausgabe 2-2016, S. 12–15, kritisch mit dem **VdS-Prüfsiegel**. Dass Versicherungen so großen Wert auf VdS-Zertifikate legen, lasse sich leicht erklären. Der GDV sei Alleingesellschafter dieses privatwirtschaftlichen Unternehmens. Die Prüfungen nähmen viel Zeit in Anspruch und kosteten Hersteller und Planer-/Errichterbetriebe viel Geld. Der Druck zur Zertifizierung sei ständig gewachsen. Der Aufwand, den – wenn es nach VdS ginge – jeder Errichterbetrieb zu betreiben hätte, um nachzuweisen, dass er in seiner beruflichen Aus- und Weiterbildung nichts gelernt habe und jetzt bei VdS alles nachhole, schlägt sich selbstverständlich in den Kosten der angebotenen Leistungen nieder. Vergleicht man eine DIN-Norm und die entsprechenden VdS-Richtlinien miteinander, so sei festzustellen, dass bei den VdS-Richtlinien lediglich an einigen Stellen langjährig in der Branche bekannte Begriffe geändert, unwesentliche Sätze hinzugefügt beziehungsweise in der DIN-Norm definierte Werte mehr oder weniger geringfügig abgeändert wurden. Fazit: Die Anforderungen, die Sicherheitsentscheider an Errichter und Hersteller der Sicherheitsbranche stellen,

sollten einem realen Hintergrund entspringen. Hier gehe es um gegenseitiges Vertrauen. Könne ein Errichter Hunderte Zertifizierungen vorweisen, bedeute das nicht, dass er damit automatisch und uneingeschränkt vertrauenswürdig ist. Umgekehrt seien fehlende Zertifizierungen kein Ausdruck mangelnder Kompetenz und Verschwiegenheit. Es sei erstaunlich, dass ein privates Unternehmen, das eigenwirtschaftlichen Interessen nachgeht, als neutral gelte. Jeder Errichterbetrieb, deren Mitarbeiter eine gute Ausbildung genossen haben, sich regelmäßig weiterbilden und im Laufe der Zeit Berufserfahrung sammeln, sei in der Lage, Arbeiten auf höchstem Qualitätsniveau zu verrichten. Im Gegenzug könne er bei Verzicht auf überflüssige Zertifizierungen und bei minimalem internen Verwaltungsaufwand günstige Preise anbieten.

## *Videoüberwachung*

Axis Communications habe die wichtigsten **sechs Trends in der Videotechnik im Jahr 2016** ermittelt, berichtet GIT in der Ausgabe 4-2016, S. 20: Das Internet der Dinge ermögliche eine Integration von Videoüberwachungskameras, Rauchmeldern, Gassensoren, Bedienfeldern von Zutrittskontrollsystemen und Lautsprechern in eine gemeinsame Verwaltungskonsole. Die Cloud werde sich als „Security as a Service" entwickeln. Unternehmen würden 2016 mehr Investitionen in Lösungen stecken, die aus den von den Sicherheitssystemen produzierten Big Data verwertbare Informationen ableiten und effektiv verfügbar machen könnten. Der Zugriff aus der Ferne werde dieses Jahr noch stärker zunehmen. Die Megapixel-Technologie werde auch 2016 weiter verbessert werden. Und zunehmend kämen ausgereifte Video- und Audio-Analyseformen auf den Markt. Damit könnten sich Sicherheitssysteme von passiver Überwachung zu intelligenten und anpassungsfähigen Analysesystemen entwickeln.

Die Unterstützung der **Sicherheit auf öffentlichen Plätzen** thematisiert Jens Aperdannier in der Ausgabe 4-2016 der Zeitschrift GIT, S. 22/23. Die Enhanced-Video-Technologie filtere potenzielle Sicherheitsbedrohungen aus der großen Datenmenge eines oder mehrerer Video-Streams. Enhanced Video Solutions würden erkennen, wenn gesperrte Bereiche betreten werden, sie überwachten Bewegungen, sie identifizierten Objekte und Menschenansammlungen, die oft auf bestehende oder sich anbahnende Probleme hindeuten. Verschiedene Plattformen würden auf einem Bildschirm zusammengefasst.

Verschiedene **Ausprägungen von Videomanagementsystemen** (VMS) behandelt die Zeitschrift PROTECTOR in der Ausgabe 4-2016, S. 30. Dahua Technology biete mit DSS eine ganze Reihe von VMS Produkten auf eigener Hardware-Basis an. Zusätzlich seien auch reine Software-Varianten zur Installation auf Kundenhardware verfügbar. Die Modelle DSS7016 sowie DSS4004 seien moderne integrierte VMS-Pakete. Sie dienten als Steuerzentrale und Nutzerinterface für die Videoanlage. Die integrierten Funktionen umfassten Benutzerrechtemanagement, Geräteverwaltung und -statusabfrage, Speicherstatus, Lichtbild-Anzeige, Aufzeichnung, Wiedergabe und Bildexport. Zum Funktionsumfang der DSS-Geräte gehörten darüber hinaus auch Speichermanagement, Anzeigeverwaltung für Videowände, Matrix-Controller und Monitore sowie Zwei-Wege-Audios. Unterstützt würden zudem eine POS-Integration für Kassensysteme und diverse intelligente Videoanalyse-Funktionen. Das Linux-basierte Betriebssystem der VMS-Lösungen biete ein solides Fundament mit verlässlichem Schutz gegen Angriffe durch Schadsoftware. Das Gesamtpaket aus Hard- und Software sorge für maximale Leistung.

„**Prozessvisualisierung**" helfe bei Dokumentation, Aufklärung und Kostensenkung, argumentiert Geutebrück in der Ausgabe 2-2016 der Zeitschrift Security insight, S. 36.

Das gelte für Waren- und Gepäckflüsse am Flughafen, für die Warehouse-Logistik wie für den Parkplatzservice. Mit wenig Aufwand könne die Videoüberwachung in Flughäfen erweitert werden: An relevanten Schnittstellen wie beim Check-in oder vor dem Verladen ins Flugzeug würden die zuvor gescannten Waren und Gepäckstücke auf Bildern erfasst. Auf Knopfdruck könne so nachvollzogen werden, wo vermisste Sendungen sind beziehungsweise an welcher Stelle in der Lieferkette sie das letzte Mal gesichtet wurden. Im Lager würden Scan-Daten der Waren mit Videobildern verknüpft. So sei der Zustand der Ware zu jedem Zeitpunkt bis ins Detail erfasst. Warenbestände würden dokumentiert. Wenn Dokumentation und Realität nicht übereinstimmen, würden Videonachweise helfen. Die Ein- und Ausfahrt von Fahrzeugen werde durch eine Nummernschilderkennung dokumentiert. Parallel werde der Zustand jedes Gästefahrzeugs auf hochauflösenden Bildern festgehalten. Bei Bedarf gebe der Parkwächter das Nummernschild ein und sehe sofort, ob der Kratzer bei Ankunft im Hotel bereits vorhanden war.

Die Zeitschrift PROTECTOR enthält in der Ausgabe 5-2016, S. 37/38, eine **Marktübersicht über 151 hochauflösende Netzwerkkameras** von 52 Anbietern. Abgefragt wurden 63 Kriterien aus den Bereichen Videospezifikationen, Bildübertragung, Audiospezifikationen, Schnittstellen, Aufbau und Betrieb sowie Sicherheit.

Vorgestellt werden in der Ausgabe 5-2016 der Zeitschrift PROTECTOR, S. 38, **Wärmebildkameras** für Perimetersicherung, Verkehr und Industrie. Hybrid arbeitende Thermalkameras vereinten die Vorteile des Wärmebildes mit herkömmlicher optischer Überwachung. Sie würden Objekttemperaturen präzise messen und die Temperaturverteilung sogar auf kleineren oder sich schnell bewegenden Objekten erfassen. Die Wärmebildeinheit der Hybridmodelle eigne sich besonders für den Einsatz bei Nacht oder zur präzisen thermografischen Analyse.

## *Wirtschaftskriminalität*

Überbewertete Unternehmen sind ein Anreiz für Wirtschaftskriminalität, titelt die FAZ am 20. April. Wer bis zum Jahresende seine Umsatzziele nicht erreicht und daher einen geringeren Bonus befürchten müsse, werde geneigt sein, auch auf nicht ganz geraden Wegen noch schnell Umsätze zu generieren. Fast jeder zweite Manager halte es zur Erfüllung finanzieller Zielvorgaben für gerechtfertigt, Vorschriften zu umgehen. Das sei das Ergebnis einer Umfrage unter fast 3.000 Unternehmen in 62 Ländern. Besser sehe die Bilanz bezüglich der Korruption aus. Dass es dennoch einige Länder mit sehr hoher Korruption gebe – allen voran Brasilien, gefolgt von der Ukraine, Thailand und Nigeria – liege daran, dass die Umsetzung der Gesetze im Argen liege. Die Befragung – wenn auch nur mit 50 deutschen Teilnehmern auf kleiner Basis – habe für Deutschland ein hohes Niveau der Korruptionsbekämpfung ergeben. Eine Gefährdung des Wettbewerbs durch zu scharfe Regeln sehen nur 16 Prozent.

## *Wirtschaftsschutz*

Der Sonderbericht Wirtschaftsschutz der deutschen Bundessicherheitsbehörden vom 14. April weist darauf hin, dass die Präsidenten des BfV und von Bitkom am 17. März das Memorandum of Understanding „Gemeinsames Handeln für digitale Sorgfalt – Know-how-Schutz in Deutschland stärken" unterzeichnet haben. Kernzielgruppe der **Zusammenarbeit von Bitkom und BfV** seien die „Hidden Champions", hochinnovative deutsche Weltmarktführer, die verstärkt im Fokus von Wirtschaftsspionage oder ausländischer Konkurrenzausspähung stünden. 1.000 der 2.300 vertretenen Unternehmen des Bitkom seien Mittelständler, hinzu kämen 300 Start-ups. Diese sollten durch gemeinsame Angebote zum Wirtschaftsschutz sensibili-

siert werden. Über die Verbandskontakte des BfV würden mehr Firmen sensibilisiert. Die Zusammenarbeit des BfV mit Partnerverbänden lasse deutsche Unternehmen Sicherheit als Unternehmensziel kennenlernen, das für ihren nachhaltigen wirtschaftlichen Erfolg unabdingbar sei.

Timo Kolb, HiSolutions AG, befasst sich am 25. April in der FAZ mit der von Bundesinnenminister de Maizière vorgestellten „**Initiative Wirtschaftsschutz**". Die deutsche Wirtschaft sei wegen des geringen Abstands zu Mitbewerbern noch attraktiver als Opfer von Wirtschafts- und Industriespionage geworden. Eine aktuelle Studie der FH Campus Wien zeige, dass insbesondere mittelständische Unternehmen von Spionagevorfällen betroffen sind. Nach der Wiener Studie seien in mehr als 70 Prozent der Fälle unmittelbares Agieren von Menschen erforderlich. Rein technische Abwehrmethoden griffen also zu kurz. Eine entsprechende Bewusstseinsschärfung sei die Hauptaufgabe der „Initiative Wirtschaftsschutz". Bei der Wiener Studie seien mehr als 10 Prozent Mitarbeiter als direkte Täter identifiziert worden. Die Sicherheitsverantwortlichen müssten in die unternehmerische Strategiefindung einbezogen werden. Ziel einer Attacke könne auch die Senkung der Produktqualität oder eine Reputationsminderung sein. Der Aufwand zu einem angemessenen Schutz sei oft weniger hoch als vermutet, aber es bleibe eine Sisyphusaufgabe.

## *Zufahrtskontrolle*

Die Zeitschrift GIT weist in Ausgabe 4-2016 (S. 65) darauf hin, dass bei der Fachmesse IT-Trans 2016 ein **RFID-Produktprogramm** für die Zufahrtskontrolle und den Perimeterschutz von Bus- und Bahndepots vorgestellt wurde. Mit Lesereichweiten von bis zu 16 Metern würden die leistungsfähigen UHF-Reader die Berechtigung von Fahrzeugen zur Einfahrt erkennen und den Impuls zum Öffnen und Schließen von Schranken und Toren praktisch im Vorbeifahren geben. Interesssant für Verkehrsbetriebe seien die leistungsfähigen Torsteuerungen mit integriertem Frequenzumrichter (FU). Der Vorteil der FU-Steuerungen liege im schnellen und materialschonenden Öffnungs- und Schließvorgang.

## *Zutrittskontrolle*

**Zutrittssteuerung mittels Smartphone** thematisiert die Fachzeitschrift GIT in der Ausgabe 4-2016, S. 48/49. Mit Wireless-Technologien wie Bluetooth Smart oder NFC, die heute von den meisten Geräten unterstützt werden, ließen sich Smartphones, unabhängig von speziellen Eingangssystemen, als universale digitale Ausweise nutzen, die für einen sicheren Zugang auch zu IT-Systemen und Applikationen sorgen. Mit einer derartigen universellen Access-Lösung könnten Unternehmen eine einheitliche Identity-Management-Plattform aufbauen, mit einer zentralen Steuerung von physischem Zutritt und logischem Zugang über ein einziges System. In der Mobile Access-Lösung würden PINs und Passwörter überflüssig. Die nahezu unbegrenzten technischen Möglichkeiten der Smartphones bereiteten den Weg für fortgeschrittene Sicherheitslösungen. Biometrische Authentifizierung oder gestengesteuerte Zutrittskontrolle sei mit diesen Geräten ohne weiteres realisierbar.

GIT stellt in der Ausgabe 4-2016, S. 46/47 die **Produktlinie Mobile Key** von Simons Voss vor, die sich für Anlagen mit bis zu 20 Türen und 100 Nutzern eigne. Das webbasierte System sei geradezu spielerisch leicht zu bedienen. Es eigne sich auch in kleinen Anlagen mit wenigen Türen und Büros. Wie bei einer großen Anlage bestehe das Mobile-Key-Schließsystem aus digitalen Zylindern für die Türen einerseits und Trans-

pondern (wahlweise PIN-Code-Tastatur) zum Öffnen und Schließen andererseits. Berechtigungsvergabe, Zeitpläne, Protokolle oder auch eine Fernöffnung ließen sich per Web-Applikation auf einem beliebigen Endgerät verwalten. Mit der einfach gestalteten App lege man beispielsweise Konten an und erstelle Schließpläne. Diese Daten würden auf den Simon-Voss-Server übertragen, dort als Schließplan angelegt und zurück in die Web-App geschickt – und von dort auf ein kleines, kompaktes Programmiergerät geladen.

**Ausweismanagement** behandelt Ingo Kauffmann, Nexus, in Ausgabe 4-2016 der Zeitschrift GIT, S. 62/63. Die Zusammenführung von Ausweis- und Berechtigungsmanagement in einem System habe für die anwendenden Unternehmen unter anderem folgende Vorteile: Zentrale Richtlinien und übergeordnete Prozesse schafften Klarheit und schlössen Sicherheitslücken. Effiziente und einfache Abläufe reduzierten den administrativen Aufwand. Zutritts- und Nutzungsrechte ließen sich global und automatisch zuteilen und entziehen. Manuelle Prozesse würden weitgehend eliminiert, das reduziere Risiken. Die Zusammenführung ermögliche die Bündelung verschiedener Funktionen und Prozesse von Abrechnung bis Zeiterfassung, und der Handling-Aufwand für die Nutzer werde gering gehalten. Von reibungslosen und auf maximale Sicherheit ausgerichteten internen Prozessen profitiere dann auch der externe Besucher. Bei seinem Eintreffen liege der gedruckte RFID-gestützte Besucherausweis schon bereit.

# *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