# *Focus on Security*

Ausgabe 03, März 2017

SECURITAS

***Inhalt***

## *Arzneimittelsicherheit*

Security insight weist in der Ausgabe 1/2017, S. 37, darauf hin, dass Cyberkriminelle ein kommerzielles Interesse an **Patientendaten** haben könnten, wenn es zum Beispiel um mögliche Versicherungen geht. Sogenannte Keylogger zum Ausspähen von Arztpraxen seien dazu in der Lage, alles aufzuzeichnen, was auf der Tastatur geschrieben wird. Die nur etwa einen Zentimeter großen Geräte ermöglichten es Kriminellen zum Beispiel auch, Passwörter und verschlüsselte E-Mails mitzulesen. Der Keylogger sende ihnen die Daten per E-Mail zu.

Security insight weist in der Ausgabe 1/2017, S. 8, auf die UmsetzungsVO zur EU-**Fälschungsschutzrichtlinie** hin. Sie lege fest, dass ab 9. Februar 2019 pharmazeutische Unternehmen verschreibungspflichtige Arzneimittel nur noch mit zwei Sicherheitsmerkmalen in den Verkehr bringen dürfen. Das Datenbanksystem der pharmazeutischen Industrie – wesentlicher Baustein für das securPharm-System zur Sicherheitsprüfung – sei soweit ausgebaut, dass sich alle Unternehmen anschließen könnten.

## *Automatische Kennzeichenerfassung (AKE)*

In der Ausgabe 1/2017 von VEKO Online erklärt und verteidigt PD Stefan Pfeiffer die polizeiliche Anwendung der AKE. Sie helfe, Straftäter zu fassen, etwa in den Bereichen Kfz-Verschiebung, Schleusung, Menschenhandel, internationaler Waffen- und Sprengstoffhandel, illegale Ein- und Durchfuhr von Drogen, Verschieben von Diebesgut durch international organisierte Banden und im internationalen Terrorismus. Die Digitalkamera der AKE erfasse das Kennzeichen der vorbeifahrenden Fahrzeuge von hinten, sodass die Fahrzeuginsassen nicht erkannt werden könnten. Dann werde das Kennzeichen ausgelesen und an entsprechender Stelle mit den Fahndungsbeständen abgeglichen. Dies dauere im Regelfall ca. 0,5 Sekunden. Liege eine Übereinstimmung vor, werde von der Stelle, wo der Treffer aufläuft, nochmals eine manuelle Nachkontrolle durchgeführt. Erst nach erneuter Bestätigung des Treffers würden die entsprechenden polizeilichen Maßnahmen eingeleitet. Da bei fehlendem Treffer die Daten unverzüglich gelöscht werden, sei das Erstellen eines Bewegungsbildes unmöglich.

## *Brandschutz*

Dr. Jörg Keller, GTE Industrieelektronik GmbH, befasst sich in der Ausgabe 1/2-2017 der Zeitschrift PROTECTOR, S. 19, mit der Branddetektion in der Industrie. Als technische Alternative zu Rauchmeldern für den Einsatz in Industrieanlagen böten sich vor allem Brandgasmelder sowie Infrarot-Wärmemelder an. **Multisensor-Brandgasmelder** detektierten charakteristische Brandgase wie Kohlenwasserstoffe, Kohlenmonoxid sowie Wasserstoff. Gerade während der Entstehungsphase eines Brandes, in der wenig Rauch freigesetzt wird, ermöglichten sie eine zuverlässige Früherkennung. Weiterhin ließen sich Brandgasmelder sehr gut gegen Umgebungseinflüsse wie Stäube, Nebel oder mechanische Beeinträchtigungen schützen. Infrarot-Wärmemelder eigneten sich für die Brandfrüherkennung in Bereichen der Lagerhaltung, beim Transport und bei der Aufbereitung brennbarer Stoffe. Insbesondere könnten sie sehr effizient eingesetzt werden, um überhitzte Maschinenteile oder Glutnester auf Förderanlagen zu entdecken. Durch Infrarot-Wärmemelder werde unabhängig von Luftströmungen in Räumlichkeiten mit schwierigen Strömungsverhältnissen eine eindeutig zu beschreibende Detektionsleistung erreicht, weiterhin sei dieses Verfahren schnell. Inzwischen seien kompakte Kame-

rasysteme wie der Adicos Hotspot verfügbar, die eine Alarmauswertung des Überwachungsbereichs direkt im Gerät vornehmen.

Joachim Meisehen, Novar GmbH, behandelt in der Ausgabe 1/2-2017 der Zeitschrift PROTECTOR, S. 20/21, **Ansaugrauchmelder** (ARM) und deren Anwendung. Die besonderen Vorteile der ARM bestünden vor allem in der abgesetzten Positionierung des ARM vom eigentlichen Überwachungsbereich und dem somit vereinfachten Zugang für Wartungszwecke sowie in der Fähigkeit, die angesaugten Luftproben vor dem Eintritt in den Melder von Staub und Kondensat zu reinigen. Server- oder Telekommunikationsräume, Hochregallager, Produktionsbereiche, Zwischendecken, große offene Hallen oder Transformatorräume zählten zu den umfangreichen Einsatzbereichen von ARM. Auch überall dort, wo die räumliche Ästhetik nicht gestört werden soll, beispielsweise in Museen, Kirchen, Theatern oder Schlössern, würden ARM verwendet. Der Hersteller Honeywell verfüge mit der neuen Produktfamilie Faast über ARM der neuesten Generation. Interne Filter, Algorithmen und eine geräteabhängige Dual-Wellenlängen-Detektionskammer verhinderten Täuschungsalarme.

**Gestuftes Brandschutzkonzept für Rechenzentren** ist das Thema der Zeitschrift PROTECTOR in der Ausgabe 1/2-2017, S. 22/23. Ein solches neues Brandschutzkonzept speziell für Rechenzentren von Wagner basiere auf dem Ansatz, bei geringster Rauchdetektion den Schutzbereich frühzeitig in eine brandhemmende, aber begehbare, Schutzatmosphäre zu versetzen. Die Brandursache könne dann analysiert und behoben werden, ohne dabei den Betrieb zu stören. Die Stickstofflöschanlage könne gestuft in zwei unterschiedliche Sicherheitslagen fahren: in eine brandhemmende Sauerstoffkonzentration und in eine löschfähige Restsauerstoffkonzentration unterhalb der Entzündungsgrenze. Durch die Kombination mit einer Sauerstoffreduzierungsanlage werde die jeweilige Sicherheitslage gehalten. Auf weitere Löschmittelbehälter könne dadurch verzichtet werden, und gleichzeitig bestehe nahezu maximaler Schutz durch die unbegrenzt mögliche Haltezeit. Auf eine personengefährdende Löschgaskonzentration könne verzichtet werden. Die Bevorratung des Löschmittels falle im Vergleich zu herkömmlichen Anlagen bis zu 37 Prozent geringer aus. Druckentlastungsflächen könnten um bis zu 80 Prozent verkleinert werden. In der Gesamtbetrachtung des Energieverbrauchs eines Rechenzentrums entfielen auf die zweistufige Brandschutzlösung weniger als 0,003 Prozent.

PROTECTOR enthält in der Ausgabe 1/2-2017, S. 24/25, eine **Marktübersicht über 67 Brandmeldesysteme** von 29 Anbietern. Eine Online-Tabelle biete 35 abgefragte Kriterien, unter anderem aus den Bereichen Zertifizierungen, Systemaufbau, Vernetzung, Fernbedienung, Löschanlagensteuerung, Art der Melder, Melderadressierung, Steuerung von Fremdgeräten, Überwachung der Ausgänge, Datenschnittstellen, Lageplantableau, Programmierung, Zugriffsschutz und Ereignisspeicher.

Moderne Brandschutztechnik in einem Hallenbau stellt Security insight in der Ausgabe 1/2017, S. 36/37, vor. Im Eingangsbereich des „Showrooms Kran-Halle" habe GEZE mit automatischen Schiebetüranlagen in Fluchtwegausführung barrierefreien und sicheren Begehkomfort geschaffen. Vorbeugenden Brandschutz gewährleisten die vernetzten RWA-Abluftöffnungen auf dem großflächigen Dach des gesamten Gebäudekomplexes. Das Fenstertechnik-Portfolio habe den optimalen RWA-Spindelantrieb geliefert. Die Vernetzung der RWA-Abluftöffnungen habe den weiteren Vorteil, dass mit Hilfe eines BUS-Kopplers auch die Branderkennung und individuelle Steuerung der RWA-Systeme über die Brandmeldezentrale erfolgen kann.

## Gefahrenmelder

Die hochflexible M2M-SIM-Karte mache die Alarmübertragung einer SPC-Anlage ein großes Stück unabhängiger von der im Ernstfall notwendigen Internetverbindung beim Auftraggeber, berichtet Security insight in der Ausgabe 1/2017, S. 8. In Kooperation mit dem Telekommunikationsanbieter Vodafone könne Protection One seinen Kunden einen ebenso flexiblen wie sicheren Ersatzweg für die Übertragung von Alarmen und den damit verbundenen Daten anbieten. Sobald der Hauptübertragungsweg im Alarmfall durch DSL-Ausfall oder -Störung nicht nutzbar ist, erfolge die Meldung an die eigene NSL automatisch über den Ersatzweg. Diese M2M-Übertragung werde über die SPC-Alarmanlage mit Notstrom gespeist.

## Geldautomatensicherheit

Nach Angaben des BKA hat sich die Zahl der gemeldeten **Geldautomaten-Sprengungen 2016** gegenüber dem Rekordjahr 2015 noch einmal ungefähr verdoppelt, meldet die FAZ am 21. Februar. Damals hatte es 157 Fälle gegeben. Darauf hätten die Banken mit unterschiedlichen Schritten reagiert. In manchen Orten seien die Selbstbedienungszonen mit Geldautomaten (GA) und Kontoauszugsdruckern zunächst nachts geschlossen und die GA entleert worden. Als ein Weg, um die Täter abzuschrecken, gelte der Einsatz von Mechanismen, die das Geld bei starken Erschütterungen mit einer Spezialtinte einfärben. In den Niederlanden setze man diese Technik flächendeckend ein. Diese Technik sei aber „kein Allheilmittel". Das Einfärben verhindere nicht die Sprengungen. Zum anderen solle es so etwas wie einen „Markt für eingefärbtes Geld" geben. Andere Techniken versuchten, die Sprengung ganz zu vereiteln. Dazu gehörten Verfahren, den GA so zu präparieren, dass man weniger Gas einleiten kann. Andere Verfahren beruhten darauf, dass das Gas gleich wieder entweichen soll oder neutralisiert werde. Wieder andere Verfahren versuchten, das Gas mit sogenannten Piezozündern in vielen kleinen Zündungen verpuffen zu lassen. Es gebe auch Ansätze, den Tresor des GA so stabil zu machen, dass er Sprengungen von außen wie von innen aushält. Auch eine stärkere Videoüberwachung werde von manchen Banken als Schritt gesehen, um GA besser zu schützen. Wie die Deutsche Kreditwirtschaft (DK) mitteile, entscheide jede Bank oder Sparkasse je nach Gefährdungslage und Situation selbst, welche Schritte sie gehe.

## Geldwäsche

Das Bundeskabinett wolle schärfere Melde- und Registerpflichten zum Kampf gegen Geldwäsche beschließen, meldet die FAZ am 22. Februar. Herzstück sei ein neues **Transparenzregister**. An dieses Register solle der „wirtschaftlich Berechtigte" gemeldet werden, also derjenige, der wirklich über Vermögen verfügen kann. Anlass sei die 4. Anti-Geldwäscherichtlinie der EU. Zur Einsicht berechtigt sei „insbesondere" ein Interesse, das sich auf Geldwäschetaten bezieht, weil das Vermögen aus Korruption oder Terrorfinanzierung stammt. Das Gesetz treffe deutlich mehr Akteure als zuvor, nicht nur Banken und Versicherungen, sondern auch Anwälte, Wirtschaftsprüfer, Treuhänder, Immobilienmakler, Veranstalter von Glücksspielen und auch „Güterhändler", das heißt Unternehmer, die mit Gütern handeln und dabei in bar 10.000 Euro oder mehr annehmen, also etwa Antiquitäten- oder Schmuckhändler.

## Hehlerei

**Hehlerei via Internet** behandelt Sven Laukat, r.o.l.a. Business Solutions GmbH, in

Security insight, Ausgabe 1/2017, S. 19/20. Kleinanzeigen-Plattformen seien insgesamt ein großer Absatzmarkt im Internet. Bei der dortigen Suche nach Hehlerware müsse als erstes eingeschätzt werden, in welchen Ländern das Diebesgut auftauchen könnte. Das hänge oft davon ab, um welche Größenordnung es sich handle und wer die Täter seien oder sein könnten. Deshalb gebe es nicht wenige Unternehmen, die Informationen anfordern. Dabei gehe es nicht um einen mitgenommenen Kugelschreiber, sondern um Mengen, die sich durchaus aufspüren ließen und somit schon eine kritische Masse bildeten. Bei anderen Anbietern als Ebay gestalte sich die Recherche im Internet deutlich aufwändiger. So habe er ein Tool entwickeln müssen, mit dem die französische Plattform laboncoin.fr ausgelesen werden könne. Über dieses Tool hätte r.o.l.a. seit März 2016 1,5 Mio. Angebote mit etwa 3 Mio. zugehörigen Bildern ausgelesen.

## *Industrie 4.0*

Hendrick Lehmann beleuchtet in der Ausgabe 1/2-2017 der Zeitschrift PROTECTOR, S. 16–18, **Chancen und Risiken** von Industrie 4.0. Das IT-Sicherheitsgesetz von 2015 habe durchaus Relevanz für alle Unternehmen, die Webseiten unterhalten. Hier würden durch eine Änderung des § 13 Telemediengesetz erhöhte Anforderungen an die technischen und organisatorischen Maßnahmen zum Schutz ihrer Kundendaten und der von ihnen genutzten IT-Systeme gelten. Diese Unternehmen müssten Sorge dafür tragen, dass Angriffe von außen nicht in die innere Prozess-Struktur eindringen können. So seien etwa entsprechende Authentifizierungsverfahren umzusetzen, und durch entsprechende Sicherungen, wie regelmäßige Patches und Updates, sei das Risiko von Drive by Downloads zu minimieren. Ein weiterer zentraler Punkt sei die Standardisierung von Technologien und Schnittstellen. Internationale Standards seien Voraussetzung für eine global orientierte Wertschöpfungskette, mit ihren funktionalen, datenorientierten und nichtfunktionalen Komponenten unter besonderer Einbeziehung von IT-Sicherheitsaspekten. Die digital vernetzte Form der Produktion eröffne neben Chancen auch neue Risiken, denn virtuelle Angriffe könnten sich nicht auf eine Anlage beschränken, sondern könnten sich durch die Vernetzung womöglich kaskadierend fortsetzen. Der Staat sei gefordert, durch entsprechende klare Gesetze Verantwortlichkeiten zu benennen und behördliche Hilfestellung zu leisten.

## *IT-Sicherheit*

Immer häufiger würden Regierungen, Unternehmen und Privatleute von Hackern attackiert, schreibt die FAZ am 28. Februar und verweist auf das vom BSI im November 2016 veröffentlichte **Lagebild der IT-Sicherheit in Deutschland 2016**. Es verdeutlicht eine neue Qualität der Gefährdung: Die zunehmende Digitalisierung und Vernetzung durch Entwicklungen wie dem Internet der Dinge, Industrie 4.0 oder Smart Everything böten Cyberangreifern fast täglich neue Angriffsflächen und weitreichende Möglichkeiten, Informationen auszuspähen, Geschäfts- und Verwaltungsprozesse zu sabotieren oder sich anderweitig auf Kosten Dritter kriminell zu bereichern. Der Lagebericht umfasst zur Gefährdungslage Ursachen und Rahmenbedingungen, Angriffsmethoden und -mittel. Er enthält einen Überblick zur Gefährdungslage KRITIS und Erkenntnisse aus dem UP KRITIS sowie die Gestaltung der IT-Sicherheit für die Wirtschaft. Aus der Gesamtbewertung ergeben sich für die Wirtschaft insbesondere folgende Ergebnisse: „Aus dem vorliegenden Lagebericht des BSI wird unumwunden deutlich, dass die Komplexität der Bedrohungslage ebenso wie die damit einhergehenden Gefahren für die fortschreitende Digitalisierung zunimmt." „Die Gefährdungs-

lage ist weiterhin angespannt. Zusätzlich zu bereits bekannten Phänomenen kann das BSI aber auch eine neue Qualität in der Bedrohung feststellen. Die bekannten Einfallstore für Cyberangriffe bleiben im Wesentlichen unverändert. In den am häufigsten eingesetzten Soft- und teilweise auch Hardwareprodukten finden sich Schwachstellen, welche es Angreifern erlauben, Informationen abfließen zu lassen oder die Kontrolle über die Systeme zu erlangen. Organisiert aufgebaute und betriebene Botnetze stehen für die Angreifer zur Verfügung, um Schadsoftware oder Spam-E-Mails massenhaft zu verteilen. Ebenso können diese Botnetze für Angriffe auf die Verfügbarkeit von Diensten erfolgreich eingesetzt werden. Anwender setzen auch gängige und einfache Sicherheitsmaßnahmen häufig nicht oder nicht hinreichend ein. Durch anonyme Zahlungsmethoden wie beispielsweise Bitcoin ergeben sich neue Möglichkeiten für Cyberkriminelle in der Vermarktung von Angriffswerkzeugen, aber auch in der Erpressung. Die sprunghaft angestiegenen Fälle von Ransomware verdeutlichen eindrucksvoll, wie verwundbar mittlerweile das alltägliche Leben für Cyberangriffe geworden ist." „Die Wertschöpfung der deutschen Wirtschaft durch Vorsprung in Know-how und Technik darf nicht durch Industriespionage gefährdet werden." „Für die Sicherheit der Kritischen Infrastrukturen in Deutschland hat das BSI durch das IT-Sicherheitsgesetz eine neue Aufgabe übertragen bekommen. In enger Kooperation mit den jetzt im Fokus stehenden Branchen und Unternehmen werden sinnvolle und umsetzbare Maßnahmen entwickelt, um die Versorgung der Bevölkerung sicherzustellen." Das BSI hat „seine Zusammenarbeit mit Staat und Wirtschaft intensiviert. Hierzu wurden nicht nur bereits bestehende Kooperationsplattformen wie UP KRITIS und die Allianz für Cybersicherheit erweitert und gestärkt. Darüber hinaus prägt das BSI die entscheidenden Standards der Informationssicherheit mit besonderer Beachtung der Umsetzbarkeit in der Wirtschaft – von der Neuausrichtung des IT-Grundschutzes bis hin zu besonderen Standards der Industrie 4.0. Weiterhin bietet das BSI die Sicherheitszertifizierung an, mit der die Wirtschaft im Markt den Nachweis der umgesetzten Sicherheitsstandards führen kann." Das BSI leistet „seinen Beitrag zum Gelingen der Energiewende durch die Erarbeitung von Sicherheitskriterien für die Infrastruktur der intelligenten Stromzähler, und es unterstützt bei der Erarbeitung der Sicherheitsaspekte einer Verkehrsinfrastruktur, in der autonome oder hochautomatisierte Fahrzeuge Realität werden. Darüber hinaus hat das BSI die wesentlichen Sicherheitsanker der elektronischen Gesundheitskarte und der dazu notwendigen Systeme mitgestaltet und zertifiziert. Gleichzeitig konnte das BSI auch Standards und Empfehlungen für die Wirtschaft herausgeben, wie etwa Empfehlungen für eine sichere E-Mail-Infrastruktur, die bereits aufgegriffen werden." „Dies entlässt jedoch die Wirtschaft nicht aus ihrer Verantwortung, auch die eigenen Maßnahmen zur Prävention und Sensibilisierung auszubauen. Das BSI steht bereit, um bei der Gestaltung der einzelnen Maßnahmen zu unterstützen. Ebenso besteht ein großer Bedarf an erweiterten Detektions- und Reaktionsfähigkeiten in der Wirtschaft. Das BSI wird Initiativen hierzu begleiten und so sinnvoll selbst tätig werden. Im Bereich der Kritischen Infrastrukturen kann ein vordringlicher Bedarf hieran festgestellt werden, aber in der Fläche bei den kleinen und mittleren Unternehmen (KMU) muss sich ebenfalls etwas bewegen." „Erste Schritte zu mehr unmittelbarer Kooperation mit der Wirtschaft sind bereits erfolgt. So wurde kürzlich eine individuelle Kooperationsvereinbarung mit der Volkswagen AG abgeschlossen. Ähnliches ist auch mit der Continental AG geplant. Ebenso geht das BSI gesammelt auf alle DAX- und MDAX-Unternehmen zu, um die Zusammenarbeit zu intensivieren. Erste Ergebnisse dieser Kooperationen sind sehr vielversprechend." „Zur Verbesserung der Reaktionsfähigkeit des BSI bei besonderen Cyberlagen werden Mobile-Incident-Response-Teams (MIRT)

zur Unterstützung akut betroffener Stellen eingerichtet." „Die Digitalisierung mit ihren Chancen und Risiken ist in vollem Gange." „Eine erfolgreiche Digitalisierung von Staat, Wirtschaft und Gesellschaft wird es ohne Cybersicherheit nicht geben."

Cyberkriminalität habe die globale Wirtschaft im Jahr 2016 416 Mrd. Euro gekostet, berichtet die FAZ am 17. Februar. Innerhalb der nächsten zwei Jahre sollen die Kosten in Unternehmen auf 2,4 Billionen Euro wachsen. Das gehe aus einem Bericht von Samsung hervor. Zwei von drei Unternehmen in Deutschland würden die IT-Sicherheit für den wichtigsten Faktor für die Technologiesparte in diesem Jahr halten. Das ergebe die jährliche Trendumfrage des Digitalverbandes Bitkom. Guten Schutz könne man nur mit fähigen Mitarbeitern erreichen. Laut Samsung-Bericht würden fast 70 Prozent der Millenials offen zugeben, IT-Richtlinien zu umgehen und Apps zu verwenden, die von ihren Arbeitgebern nicht genehmigt wurden. Eine Befragung unter 19.000 Fachleuten zur Cybersicherheit habe nun ergeben, dass der **Fachkräftemangel** in dem Berufsfeld in den nächsten fünf Jahren mehr als 1,8 Mio. betragen wird. Nur jeder vierte Befragte arbeite für deutsche Mittelständler, fast zwei Drittel bei großen Organisationen.

Um auf die zunehmenden Gefahren für vernetzte Industriesysteme hinzuweisen, hätten Sicherheitsforscher des Georgia Institute of Technology eine Studie vorgelegt, in der geschildert werde, wie sich dafür spezielle **Erpressersoftware** erstellen und über Lücken in speicherprogrammierbare Steuerungen (SPS) einschleusen lasse, berichtet Peter Marwan am 15. Februar in silicon.de. Der auf der Sicherheitskonferenz RSA in San Francisco vorgestellte Forschungsbericht beschreibe stellvertretend für andere für die tägliche Versorgung benötigte Einrichtungen einen Angriff auf eine simulierte Wasseraufbereitungsanlage. Mit ihrem Ransomware-Angriff sei es den Forschern gelungen, das gesamte Kontrollsystem der Aufbereitungsanlage lahmzulegen. Sie legten dar, dass Erpresser etwa mit der unkontrollierten Zugabe von Chlor zum Trinkwasser drohen könnten, die sich über die Anlage steuern lässt. Durch den Zugriff auf die SPS hätten sie aber nicht nur Ventile steuern, sondern auch die Displayanzeigen manipulieren können. Bei ihren Arbeiten hätten die Forscher auch 1.400 Exemplare eines bestimmten SPS-Typs gefunden, die leicht über das Internet angreifbar waren. Viele der Geräte hätten sich zwar hinter einer Unternehmens-Firewall befunden, aber die biete nur Schutz, solange das Netzwerk nicht kompromittiert ist.

Die EU-Richtlinie 2016/1148 zur Netz- und Informationssicherheit, kurz **NIS-Richtlinie**, sei bis zum 10. Mai 2018 in den Mitgliedstaaten umzusetzen. Darauf weist der Behörden Spiegel in der Februar-Ausgabe hin. In Deutschland seien die meisten Vorgaben der NIS-Richtlinie durch die Tätigkeit des BSI mit eigenem Computer Emergency Response Team (CERT-Bund) und dem IT-Sicherheitsgesetz bereits erfüllt. Den Entwurf eines weiteren Gesetzes zur Umsetzung der Richtlinie habe das Bundeskabinett bereits beschlossen. Arne Schönbohm, BSI-Präsident habe zu dem Gesetzentwurf erklärt: „Konkret bedeutet dies unter anderem, dass das BSI die Betreiber Kritischer Infrastrukturen und andere wichtige Akteure außerhalb der Bundesverwaltung künftig noch besser und intensiver unterstützen kann."

Das BMI habe den Startschuss für den Aufbau einer Zentralen Stelle für Informationstechnik im Sicherheitsbereich (**ZITIS**) gegeben, meldet der Behörden Spiegel in der Februar-Ausgabe. Es solle Beratungs- sowie Unterstützungsaufgaben übernehmen und sich mit der Erforschung und Entwicklung von Methoden, Produkten und übergreifenden Strategien für die Sicherheitsbehörden beschäftigen. Die Aufgaben von ZITIS sollten insbesondere in den Bereichen der digitalen Forensik, der Telekommunikations-

überwachung, der Kryptoanalyse (Dekryptierung), der Massendatenauswertung/Big Data sowie der technischen Fragen von Kriminalitätsbekämpfung, Gefahrenabwehr und Spionageabwehr liegen.

**Cyberversicherungen für den Mittelstand** thematisiert Ole Sieverding, Hiscox, in der Ausgabe 1/2-2017 der Zeitschrift PROTECTOR, S. 72. Cyberversicherung mache für Unternehmen jeder Größe Sinn. Bei der Risikoanalyse sollten folgende Fragen geklärt werden: Wie abhängig ist das eigene Unternehmen von der IT und wie lange könnte ein Ausfall maximal dauern? Über wie viele Kundendaten verfügt das Unternehmen, die für Cyberkriminelle interessant sein könnten? Könnte aus einer Attacke auch Dritten ein Schaden entstehen, etwa, wenn eine E-Mail mit Schadsoftware an einen Lieferanten weitergeleitet wird? Mit der doppelten Verteidigungsstrategie aus regelmäßigen IT-Checks und Updates sowie einer Cyberversicherung für den Ernstfall bereiteten die Gefahren aus dem Netz keine schlaflosen Nächte mehr.

## *IuK-Kriminalität*

Nach einer Meldung von heise.de vom 8. Februar versuchen Angreifer mit einem simplen Trick, Menschenrechtler und Personen aus der Rüstungsindustrie zur Installation einer Malware zu bringen, die nun auch für Macs ausgelegt sei. Die MacDownloader genannte Schadsoftware tarne sich als vermeintlicher Adobe Flash-Installer sowie zugleich als ein Entfernungs-Tool für Adware von Bitdefender, die sich seit längerem mit Cyberangriffen aus dem Iran befassen. Einmal installiert versuche die Malware anschließend, den Schlüsselbund (Keychain) an den Angreifer zu übermitteln. Ein gefälschter Systemdialog solle den Nutzer zudem dazu bringen, Benutzernamen und Passwort einzugeben – um den Angreifern dann den Zugang zu den verschlüsselten Daten der Keychain-App zu ermöglichen.

Nach einem Bericht von Peter Marwan in silicon.de am 8. Februar habe Kaspersky Lab eine Reihe ausgeklügelter **Cyberangriffe auf Firmen aus der Finanz- und Telekommunikationsbranche** sowie Behörden in 40 Ländern untersucht. Die Angreifer machten sich dabei in Unternehmen weitverbreitete Tools für Penetrationstests und Administratoren sowie das PowerShell-Framework zur Aufgabenautomatisierung unter Windows zunutze. Besonderheit sei den Experten zufolge, dass dabei Malware zum Einsatz komme, die lediglich im Speicher aktiv ist. Die Angreifer seien nur solange im System zu fassen, wie sie Informationen sammeln. Kaspersky vermute hinter den Angriffen die Gruppen GCMAN und Carbanak. Letztere sei 2015 bekannt geworden, als sie durch ebenfalls sehr gezielte und technisch komplexe Angriffe, die von viel Insiderwissen zeugten, von Banken mehrere hundert Millionen Euro erbeutet hätten. Einmal aufmerksam geworden habe Kaspersky Lab seitdem bereits ähnliche Attacken auf über 140 Netzwerke vor allem von Banken, Telekommunikationsunternehmen und Behörden identifizieren können. Speicherforensik werde für die Analyse von Malware und deren Funktionen besonders wichtig. Bei den bislang untersuchten Attacken hätten die Angreifer jede denkbare antiforensische Technik genutzt und demonstriert, dass keine Malware-Dateien benötigt würden, um Daten erfolgreich aus einem Netzwerk herauszuschleusen. Um solche Angriffe abzuwehren, seien Memory-Introspection-Technologien erforderlich, mit denen sich Methoden zur Memory-Manipulation aufspüren ließen. Ansätze, die nur auf die Erkennung von Schadcode angewiesen sind, seien dabei überfordert. Es dauere normalerweise Monate, bis eine Organisation einen solchen Einbruch festgestellt habe. Je mehr Sicherheitsmechanismen greifen – wie etwa Erkennung von Anomalien und Honeypots – umso höher seien die Chancen, Angriffe zu erkennen und vorzubeugen.

Deutschland hat 625 Mrd. Nachrichten im Posteingang, titelt die FAZ am 13. Februar. Fast zwei Drittel aller versendeten E-Mails an Unternehmen seien Spam, wobei acht bis zehn Prozent als bösartig gelten würden. Das gehe aus dem jährlichen **Cybersicherheits-Bericht des Netzwerkausrüsters Cisco** hervor, für den das Unternehmen fast 3.000 sogenannte Chief Security Officers und Leiter von IT-Sicherheitsabteilungen aus 13 Ländern befragt habe. Deutschland sei seit langer Zeit ein attraktives Ziel für Cyberkriminelle. In Statistiken nehme die Bundesrepublik regelmäßig die Spitzenposition ein. Grundsätzlich gelte: Mit steigender Zahl der Spam-Nachrichten steige auch der Schutz, die Filterprogramme der großen Sicherheitsunternehmen und E-Mail-Anbieter basierten heutzutage auch auf maschinellem Lernen, griffen Informationen aus den wachsenden Daten ab und verbessern somit ihre Filter. Auch die Betrüger würden besser: Früher hätten noch Texte in schlechtem Deutsch dazu aufgefordert, einen Link in einer E-Mail anzuklicken. Heute sähen Spam-Mails einem echten Newsletter oder einer Rechnung täuschend ähnlich.

Peter Marwan weist in silicon.de am 14. Februar darauf hin, dass ein neu entdeckter **Loader für Microsoft Office** gefährliche Makros verwende, um mit deren Hilfe mehrere Malware-Familien zu verbreiten. Der Loader sei von Experten des IT-Sicherheitsanbieters Palo Alto Networks in über 650 unterschiedlichen Samples identifiziert worden. Mit ihnen seien in unterschiedlichen Branchen bereits über 12.000 Angriffe auf Firmen durchgeführt worden. Am häufigsten seien High-Tech-Unternehmen, Dienstleister, Rechtsanwälte und Behörden betroffen. Bei den E-Mails handele es sich meist um vermeintliche Aufträge, Rechnungsnummern, Produktlisten, Vertragsunterlagen oder andere Dokumente, denen der Empfänger eine Geschäftsrelevanz unterstelle. Angesichts der großen Menge einfach verfügbarer Malware-Familien sowie deren Verbreitung im großen Stil nehme Palo Alto Networks an, dass die Hintermänner nicht ausgewählte Firmen oder Organisationen angreifen, sondern in erster Linie großflächige Kampagnen fahren. Laut Palo Alto Networks seien alle Makros mit einer großen Menge an Datenmüll-Code und höchstwahrscheinlich mit einem sogenannten Builder zufällig ausgewählten und generierten Variablen verschleiert. Eine Besonderheit sei es, dass die Angreifer einen sogenannten UAC-Bypass anlegen, also die Benutzerkontensteuerung umgehen.

Ebenfalls in silicon.de berichtet Peter Marwan am 14. Februar, seit Oktober 2016 seien von bislang Unbekannten mit einem individuell angepassten und in präparierte Websites integrierten Exploit Kit gezielt ausgewählte Besucher dieser Websites angegriffen worden. Die Schadsoftware sei nur aktiv, wenn der Besucher von einer von rund 150 unterschiedlichen IP-Adressen aus auf die Website gekommen sei. Diese IP-Adressen würden 104 Organisationen aus 31 Ländern, größtenteils Banken, aber auch Telekommunikationsfirmen und Internetfirmen gehören. Das gehe aus einer jetzt von Symantec vorgelegten Analyse hervor. Das Vorgehen der Angreifer erinnere die Symantec-Forscher an die **Hackergruppe Lazarus**, vor allem wegen eines Hacking-Tools. Die Lazarus-Gruppe habe schon früher Geldinstitute ins Visier genommen.

Autoren von Ransomware stürzen sich zunehmend auf **Android-Nutzer**, berichtet Martin Schindler bei silicon.de am 22. Februar. Erpressungsversuche auf diesem Betriebssystem hätten 2016 um 50 Prozent zugenommen, wie der Sicherheitsanbieter Eset mitteile. Denn immer häufiger würden mobile Geräte wie Smartphones oder Tablets genutzt, um für die Anwender wertvolle Daten zu speichern. Während Lock-Screen Ransomware einen eigenen Sperrbildschirm einrichte und somit ein Gerät unbrauchbar mache, verschlüssele Crypto-Ransomware die Dateien eines Nutzers. Die Verbreitung

erfolge immer häufiger über E-Mails mit speziell präparierten Links. Per Social Engineering sollten Nutzer dazu verleitet werden, die Links anzuklicken, die zu mit Malware infizierten Android-Installationspaketen führen. In den meisten Fällen tarne sich Ransomware als legitime App – meistens sei die Schadsoftware in Spielen oder Apps versteckt, die für den Zugriff auf pornografische Inhalte benötigt werden. Besonders aggressiv sei die Ransomware Lockerpin, die erstmals im August 2015 entdeckt worden sei. Sie ändere die PIN des Sperrbildschirms und werfe dem Opfer im Namen des FBI vor, es habe illegale Inhalte gespeichert. Die Lösegeldforderung belaufe sich auf 500 Dollar.

Bernd Schöne, freier Journalist, wirft in der Ausgabe 1/2-2017 der Zeitschrift PROTECTOR, S. 44/45, einen Blick zurück auf das Jahr **2016**. Es werde wohl als **Jahr der Ransomware** in die Geschichte eingehen. Verschlüsselungstrojaner machten überall reiche Beute und scheinen einen neuen Geschäftsbereich von Cyberkriminellen zu eröffnen. Typisch für 2016 seien große Zahlen gewesen. Im November sei es bei der Telekom zu einer Großstörung gekommen. 900.000 DSL-Endpunkte seien nach einem Denial-of-Service-Angriff für Tage offline gewesen. Eine völlig neue Dimension habe sich beim IT-gestützten Betrug ergeben. Unter der Bezeichnung „Chefmasche" habe sich ein neuer Angriffsvek-tor entwickelt. Die Kriminellen suggerierten bei dieser Methode einem zeichnungsberechtigten Mitarbeiter, sie seien sein Vorgesetzter und benötigten dringend Geld, etwa um ein wichtiges Geschäft anzukurbeln. Erstmals seien 2016 Kühlschränke, Web-Cams, Festplatten-Receiver und Router als Angreifer für Bot-Netzwerke aufgetreten. Kriminelle böten für diese Angriffe aktuell Botnetze aus 400.000 und mehr IoT-Geräten zur Miete an. Webcams seien 2016 das Sorgenkind schlechthin gewesen. Miserabel abgesichert hätten sie zu günstigen Preisen beim Discounter gelegen. An der falschen Stelle angebracht hätten sie sich als Augen und Ohren für Hacker erwiesen.

**Darknet-Monitoring für Unternehmen** thematisiert Security insight in der Ausgabe 1/2017, S. 52. Zur automatischen Suche im Darknet könnten sogenannte Onion-Scanner innerhalb des TOR-Netzwerks genutzt werden, um versteckte Dienste mit potenziellen Schwachstellen zu ermitteln. Gefundene Knoten ließen sich visualisieren, um mögliche Zusammenhänge zwischen einzelnen Seiten erkennen zu können. Zusätzlich ließen sich Informationen über die Zeit, wie lange Seiten im Darknet bereits online sind, welche Seite neu dazugekommen ist und ob eine Seite noch verfügbar ist, auslesen. Aufgedeckt werden könnten Sicherheitsvorfälle, durch die möglicherweise sensible Unternehmensdaten ins Darknet geraten sind und dort bereits zum Verkauf stehen. Ebenso sei es möglich, geplante DDoS-Attacken gegebenenfalls bereits im Vorfeld zu erkennen, denn die würden als Dienstleistungen zum Verkauf angeboten.

## *Korruption*

Wiederholt seien Manager der **Rüstungsindustrie** wegen Bestechung belangt worden, berichtet die FAZ am 23. Februar. So habe das LG München 2011 zwei ehemalige Mitarbeiter von Ferrostaal zu jeweils zwei Jahren auf Bewährung verurteilt, und das Unternehmen habe eine Geldbuße von 149 Mio. Euro zahlen müssen.

## *Krisenmanagement*

Krisenmanagement ist das Thema, das Ronald Hauber, ISCM GmbH, in der Ausgabe 1/2-2017 der Zeitschrift PROTECTOR, S. 74, behandelt. Krise sei ein Ereignis mit erheblichen Auswirkungen auf das gesamte Unternehmen. Wegen seiner Komplexität, Dynamik und Ungewissheiten erfordere eine Krise eine Sonderform des Managements. Die Verantwortung und Zuständigkeit für das

Krisenmanagement müsse geklärt, die Strukturen für den Krisenstab und das Assistenzteam müssten vorhanden und die Prozesse und Arbeitsmittel darauf abgestimmt sein. Die Prozessabläufe für den Krisenfall müssten implementiert werden. Weil meist die Informationslage dürftig und die Zeit knapp sei, sollte man im Krisenstab auf langatmige Diskussionen verzichten, sondern einem stringenten Führungsmodell folgen.

Krisenmanagement nach dem britischen **Standard BS 11200** thematisiert Dipl.-Math. Ralf Marczoch, mata solutions GmbH, in Security insight, Ausgabe 1/2017, S. 44/45. Der Standard bilde eine moderne Sichtweise des Krisenmanagements mit hilfreichen „Good Practices" ab. Zum einen habe es sich vor allem für international agierende Unternehmen bewährt, sich an internationalen Standards zu orientieren. Zum anderen unterstützten die Inhalte ein Szenario-unabhängiges Krisenmanagement für „das Unvorhersehbare". Eine weitere Auseinandersetzung mit dem BS 11200 sei sehr empfehlenswert. Ein erster Schritt wäre, zum Beispiel die Inhalte der eigenen Richtlinien oder Handbücher mit den Inhalten dieses Standards abzugleichen.

## *Künstliche Intelligenz*

Der Super-Computer von IBM stehe für den Siegeszug künstlicher Intelligenz, schreibt die FAZ am 19. Februar. Das **Watson-System** könne dank seiner ausgefeilten Technik binnen eines Wimpernschlags Milliarden von Daten ordnen und analysieren. Die Maschine könne lesen, sprechen und schreiben. Sie könne Texte analysieren, Zusammenfassungen von Diskussionen und Debatten erstellen, die Arbeit ganzer Fabriken organisieren. Die französische Staatsbahn wolle mit Watson Hunderttausende Sensoren entlang ihres 300.000 km langen Streckennetzes überwachen. KI-Systeme arbeiteten zwar immer noch wie herkömmliche Computer im binären Code. Doch seien sie so eingerichtet, dass sie Millionen Berechnungen gleichzeitig ausführen, ihre Arbeit ständig evaluieren und in die anstehende Lösung neuer Aufgaben einbeziehen: Computer mit eingebauten Optimierungsprogrammen. Wie die Neuronen in einem Gehirn reagierten die Chips aufeinander, gäben sich Signale, würden wie von Geisterhand aktiv oder passiv.

## *Luftfrachtsicherheit*

Herbert Hoeck, Sicherheitsdienstleister, behandelt in der Ausgabe 1/2017 von VEKO Online das Thema Luftfrachtsicherung. Nur als sicher eingestufte Luftfracht dürfe ohne eigentliche Sicherheitskontrollen an Fluggesellschaften übergeben werden. Die lückenlose Schließung der Sicherheitskette durch den „Bekannten Versender" und den „Reglementierten Beauftragten" hält er für ein „Papierkonzept", auf dessen Sinnhaftigkeit und Wirksamkeit nicht weiter eingegangen werden soll. Anders als bei der Handgepäckkontrolle könnten die Sicherheitsmitarbeiter am Flughafen keine nutzvollen Hinweise über den Inhalt der Luftfracht einholen. Hinzu komme, dass die Röntgengeräte aufgrund der Sendungsinhalte häufig an die physikalischen Grenzen stoßen. Sei eine Durchdringung der Fracht mit Röntgenstrahlung nicht möglich, müsse eine alternative Kontrollmethode angewendet werden. In Betracht kämen **Sprengstoffdetektoren und der Einsatz von Sprengstoffspürhunden**. Deren Einsatz beschreibt in dieser Ausgabe Yvonne Post, Securitas Deutschland. Die Sprengstoffdetektionstechnik sei kein unfehlbares Hilfsmittel. Ein hundertprozentiges Erkennen von Sprengstoff sei nicht möglich. Dagegen erzielten der Spieltrieb und die Genetik bestimmter Hundearten (Schäferhund, Riesenschnauzer und Airedale Terrier) hohe Erfolgsquoten. Die Riechschleimhaut sei beim Hund 150 $cm^2$, beim Menschen nur 5 $cm^2$ groß. Hunde nähmen Gerüche etwa

ein bis zehn Millionen Mal besser wahr als der geruchsempfindlichste Mensch. Sprengstoffspürhunde suchten neben militärischen und gewerblichen bekannten Stoffen auch nach sogenannten Selbstlaboraten und Waffen. Die Ausbildung dauere viele Wochen. Neben einem hohen Spieltrieb und einem einwandfreien Gesundheitszustand müssten die Vierbeiner ein ausgeprägt positives Sozialverhalten zeigen. Um im Arbeitsalltag zu bestehen, seien vor allem Konzentrationsfähigkeit und Umweltsicherheit gefragt. Die Kontrolle von Flugpassagieren sei zwar in Deutschland – anders als in den USA und in Israel – noch undenkbar, die Kontrolle von Flugkabinen, Fracht- und Gepäck sowie Fahrzeugen, die auf das Flughafengelände fahren, sei jedoch mittlerweile fester Bestandteil der Sicherheitskonzepte. Die schnelle und zuverlässige Arbeit der Hundeteams sei besonders von Vorteil, wenn man in engen Flugzeugkabinen suchen muss.

## *Luftverkehrssicherheit*

Airliners.de berichtet am 17. Februar, der Präsident der Bundespolizei, Dieter Romann, habe mehr Sicherheit auf den deutschen Airports angemahnt. Diesem Ziel dienten auch drei Pilotprojekte an den Flughäfen in Hamburg, Berlin-Schönefeld und Köln/Bonn, bei denen unter anderem Passagierkontrollen und Einsatz des Sicherheitspersonals optimiert werden sollen. Nach den Worten des Präsidenten der Bundespolizeidirektion Berlin, Thomas Striethörster, hätten die Anschläge auf die Airports in Istanbul und Brüssel auch zu Konsequenzen für die Sicherheit in Berlin geführt. Der Präsident des BDSW, Gregor Lehnert, habe Forderungen der beiden großen Polizeigewerkschaften zurückgewiesen, die eine Bündelung der Sicherheitsaufgaben an den Airports in der Zuständigkeit des Bundes verlangten. Lehnerts Angaben zufolge haben private Luftsicherheitsassistenten 2016 deutschlandweit an Flughäfen rund 41.000 verbotene Gegenstände bei den Passagierkontrollen festgestellt, darunter 891 Schusswaffen, fast 7.000 Schusswaffen-Nachbildungen und 2.400 Gegenstände aus Sprengstoff- und Munitionsteilen.

Security insight weist in der Ausgabe 1/2017, S. 53, auf den neuen § 9 a LuftSiG **(Sicherheitsmaßnahmen der Beteiligten an der sicheren Lieferkette)** hin, mit dem das Sicherheitsniveau im Bereich der Luftfracht verbessert werden solle. Zudem beinhalte der neue § 9 a eine Rechtsgrundlage für die Zulassung der Akteure in der sicheren Lieferkette für Fracht, Post und Bordvorräte. Probleme könnte die in § 9 a enthaltene Verpflichtung von reglementierten Beauftragten oder Luftfahrtunternehmen zur Feststellung der Identität einer Person bereiten, die eine Sendung übergibt. Der neue § 7 LuftSiG enthalte nun eine nicht abschließende Aufzählung von Regelbeispielen, anhand derer die Feststellung einer fehlenden Zuverlässigkeit erleichtert wird. Zur Passagierkontrolle seien zusätzlich Beleihungstatbestände eingeführt worden, die zum Beispiel die Zulassung von Luftsicherheitsplänen, die Zulassung von reglementierten Beauftragten und die Zertifizierung, Zulassung und Überwachung von Sicherheitsausrüstung betreffen.

## *Mitarbeiterkriminalität*

„Tatort Arbeitsplatz" titelt die FAZ am 19. Februar. Destruktives Verhalten zum Nachteil des Unternehmens könne ganz verschiedene Formen annehmen: körperliche Übergriffe, Einschüchterung, Bedrohung. Aus Rache entschlössen sich manche Mitarbeiter auch, sensible Unternehmensdaten zu entwenden, Geschäftsgeheimnisse an den Erzrivalen weiterzugeben oder die Unternehmenssoftware mit Computerviren zu infizieren. Jens Hoffmann, Leiter des Instituts für Psychologie und Bedrohungs-Management, berate große Unternehmen in Deutschland,

der Schweiz und Österreich dabei, **Präventionsstrategien** zu entwickeln. In einer Studie habe er ermittelt, dass die Hälfte der befragten knapp 500 Arbeitnehmer direkte oder indirekte Erfahrungen mit Gewalt am Arbeitsplatz und Suizidgefährdung gemacht hat. Jeder fünfte befragte Mitarbeiter habe in seinem Arbeitsumfeld Gewaltandrohung erlebt, 19 Prozent Stalking, zehn Prozent körperliche Gewalt. Die Studie von 2014 habe auch die Auswirkungen solcher Missstände auf das Unternehmen erhoben: Von einem Unsicherheitsgefühl in der Belegschaft hätten 54 Prozent gesprochen, von Angst immerhin 35 Prozent, von geringerer Leistungsfähigkeit 26 Prozent, von Arbeitsausfall sogar 15 Prozent. Wenn ein Arbeitnehmer seinem Arbeitgeber schweren Schaden zufügen wolle, kämen meist drei Faktoren zusammen: dauerhafte Überforderung im Büro, Konflikte in privaten Beziehungen und fehlende Identifikation mit der Arbeit. Das Gefühl, im Büro ungerecht behandelt worden zu sein, sei ein typischer Auslöser. Es könne sich auch um ganz banale Dinge handeln, die einem Menschen das Gefühl geben, alle hätten sich gegen ihn verschworen. Gefährlicher als der Umstand „heißer Aggressivität" sei für das Umfeld die „kalte Aggressivität". Denn sie ist von außen nicht oder kaum zu erkennen. Die meisten Fälle von schwerer Gewalt am Arbeitsplatz, etwa Amokläufe, würden nach Erfahrung der Psychologen im Zustand „kalter Aggressivität" begangen. Inzwischen habe sich die Erkenntnis durchgesetzt, dass das Risiko eines Amoklaufs oder anderer gewalttätiger Übergriffe sinkt, wenn es Frühwarnsysteme gebe. Nach einer Studie von Hoffmann und einer Kollegin habe die Hälfte der späteren Täter ihre Drohungen gegenüber einem Kollegen oder Vorgesetzten konkret ausgesprochen, ein Viertel den Gewaltakt im beruflichen Umfeld angekündigt. Mit der Überwachung von Mitarbeitern habe die Einrichtung eines Bedrohungsmanagements nicht zu tun.

## *Notruf- und Serviceleitstellen (NSL)*

Bei NSL könne noch vieles verbessert werden, meint Peter Niggl in Security insight, Ausgabe 1/2017, S. 14–18. Stichwort: Missbrauch. Die Berliner Polizei klage schon länger darüber, dass viele Anrufer aus Spaß oder Unwissenheit die Notruf-Nummer wählen. Sie blockierten so kurzzeitig eine der Telefonleitungen und sorgten für Wartezeiten bei echten Notfällen. Von rund 1,3 Mio. Notrufen im Jahr gebe es laut Polizei bei 300.000 keinen Grund für einen Polizeieinsatz. Zwei gegenläufige Tendenzen müssten konstatiert werden. Zum einen die Versuche, die Anzahl der öffentlichen NSL vor allem für Notrufe auf der 112 zu reduzieren, zum anderen, eine ständig wachsende Zahl von NSL privater Anbieter, die unter einem enormen Kostendruck arbeiten. Es scheine an der Zeit, das Thema NSL umfassender zu regulieren, um einem Wildwuchs Grenzen zu setzen.

Die **Aufschaltung von GMA auf private Leitstellen** sorgt für wirksamen Objektschutz, ist Dipl.-Kaufmann Michael Hobeling, HWS Wachdienst Hobeling GmbH, überzeugt (Security insight, Ausgabe 1/2017, S. 46–48). Der zertifizierte NSL-Anbieter trage die Verantwortung für die komplette Sicherungskette und müsse die drei Bereiche, Alarmempfangsstelle (AES), Alarmdienst (AD) und Interventionsdienst (ID) anbieten. Jedoch müsse hinter einer zertifizierten NSL nicht mehr nur ein Unternehmen stehen. Es könne auch eine Kooperation aus mehreren, vielleicht nur auf Teilbereiche spezialisierten Unternehmen sein. Zulässig sei die externe Ausgliederung der AES oder des ID. Zum Nachweis der Einhaltung der Anforderungen der DIN EN 50518 bei der AES müsse jährlich ein Audit durch eine akkreditierte Zertifizierungsstelle durchgeführt werden. Die AES müsse durchgehend erreichbar sein, mindestens durch Verbindung mit einer anderen AES. Der Qualität abträglich sei das

Vorgehen vieler Alarmdienste: Eine einzige, oft sogar die eigene, Einbruchmeldeanlage, werde richtlinienkonform als Muster für die Prüfung nach VdS 3138 aufgeschaltet. Alle anderen von Kunden aufgeschalteten EMA blieben weiterhin ohne Routen über eine AES auf die eigene Empfangstechnik aufgeschaltet. Für sie gebe es dann keine externen Überprüfungen der Empfangskapazitäten, der Auslastung der Kommunikationsnetze oder von Redundanzen und Notstromversorgungen.

## *Öffentlicher Raum – Sicherheit*

Bei der Sicherung öffentlicher Räume vor terroristischen Angriffen gehe der Trend hin zur Kombination verschiedener Komponenten, heißt es in Security insight, Ausgabe 1/2017, S. 32–34. Hochsicherheitsprodukte mit Anpralllast seien eine ideale und präventive Ergänzung zur Absicherung von Fußgängerzonen oder anderen Öffentlichen Bereichen, die von Fahrzeugen auf Zufahrtswegen erreicht werden können. Umfassender Perimeterschutz auf öffentlichen Plätzen könne nur durch eine **Kombination von mechanischen und elektronischen Komponenten** geschaffen werden. Dazu gehörten, je nach Art des Perimeters, eine Außensicherung mit Crash-Pollern oder anderen zertifizierten, anprallast-getesteten Barrieren, gegebenenfalls Fahrzeugschleusen mit Schnellfalttoren oder einer Schranken-Schiebetorkombination, Anlagen zur Personenvereinzelung und Zutrittskontrollsysteme sowie eine ergänzende Videoüberwachung.

## *Personenschutz*

**Anforderungsprofile** für Leitung und Mitarbeiter im Personenschutz thematisiert Steffen Kunze, Trumpf GmbH + Co. KG, in der Ausgabe 1/2017 von Security insight, S. 48/49. Gefragt seien im Anforderungsprofil des Personenschützers im privatwirtschaftlichen Umfeld vorrangig Soft Skills wie ein smartes Erscheinungsbild, psychologisches Einfühlungsvermögen, Dienstleisterdenken, Rhetorik mit entsprechenden Umgangsformen und ein gewisses Understatement. Neben Diplomatie und Konfliktfähigkeit seien hohe Toleranzfähigkeit sowie Frustrations- und Aggressionsgrenzen gefordert. In seinem Umfeld müsse der Personenschützer verschiedenste Spannungsverhältnisse verarbeiten und in diversen Rollen leben wie arbeiten können. Personenschützer lebten in einem ständigen Wechsel zwischen innerer Anspannung und demotivierender Routine.

## *Polizeiliche Kriminalstatistik 2016*

Einige Bundesländer haben bereits die Polizeiliche Kriminalstatistik für das Jahr 2016 veröffentlicht. In **Hamburg** ging die Gesamtzahl der erfassten Delikte gegenüber 2015 um 1,9 Prozent auf 239.230 Taten zurück – der höchste Rückgang seit 2010. Gleichzeitig stieg die Aufklärungsquote (AQ) um ein Prozent von 43,8 auf 44,8 Prozent. 7.510 Wohnungseinbruchsdiebstähle einschließlich Versuche wurden registriert, 16,6 Prozent weniger als 2015. Die AQ stieg hier von 8,9 auf 11,9 Prozent. 43,3 Prozent der Taten blieben im Versuchsstadium stecken. Deutliche Rückgänge gab es auch bei den Raubdelikten, und zwar um 11,2 Prozent auf 2.447.

In **Hessen** registrierte die Polizei 412.104 Straftaten. Das waren 2,2 Prozent mehr als im Vorjahr. Die AQ erreichte mit 62,7 Prozent den höchsten je gemessenen Wert. Während 1996 140.420 Fälle der Straßenkriminalität gemeldet wurden, waren es 2016 nur noch 72.712 Fälle, also 48,2 Prozent weniger. Die Zahl der registrierten Diebstähle ging um

sieben Prozent auf 141.410 Fälle zurück. Der Wohnungseinbruchsdiebstahl sank um 10,3 Prozent auf 10.405 Fälle. Die AQ blieb hier unverändert. Die Versuchsquote stieg auf 46,5 Prozent.

## *Schließsystem*

VEKO online befasst sich in der Ausgabe 1/2017 mit dem **Schließsystem pylocx.** Für den Fall, dass Beschäftigte von Geldtransporteuren streiken und Geldautomaten nicht geöffnet werden könnten, weil die streikenden Mitarbeiter den Schlüssel besitzen, habe die Firma Lock Your World ein völlig neues Schließsystem entwickelt. pylocx bestehe aus vier Komponenten: erstens der mobilen PIN-Tastatur pyKey, die zum Öffnen an – zweitens – eine Kontaktstelle gehalten wird, drittens ein Steuermodul und schließlich ein Schloss. Der Clou liege in der Organisation: Jeder pyKey sei nicht nur der jeweiligen Geldtransportfirma zugeordnet, sondern auch dem einzelnen Mitarbeiter und dem jeweiligen Schloss. So lasse sich nachvollziehen, wer wann die Geldautomaten geöffnet hat. Falle der Dienstleister aus, genüge ein Mausklick, um die Berechtigungen auf die pyKeys eines anderen zu übertragen. Mit der mobilen Tastatur lasse sich das System auch bestromen und schaffe damit dank eines integrierten Akkus Unabhängigkeit von externer Stromversorgung. Das System sei auch vandalismusresistent. Die Kontaktstelle – eine magnetische Fläche, die an eine Blende erinnert und an die der pyKey andockt – sei nämlich aus Stahl gefertigt und im Geldautomaten „versenkt", sodass es keine Angriffsmöglichkeit gebe.

## *Sicherheitsdienstleistung*

Dipl.-Staatswiss. Stephan Leukert befasst sich in der Ausgabe 1/2-2017 der Zeitschrift PROTECTOR, S. 66/67, mit der Beauftragung eines Sicherheitsdienstleisters. Bei der Überprüfung der vertragsgemäßen Dienstausführung sollte sich der Auftraggeber auf klar messbare Kriterien beschränken wie zum Beispiel: Erfüllen die eingesetzten Mitarbeiter die für die jeweilige Position vorgesehenen Qualifikationen? Finden die vereinbarten Weiterbildungen statt? Erhält der Auftraggeber zeitgerecht bestimmte Meldungen, zum Beispiel Berichte aus dem Wächterkontrollsystem? Finden die vereinbarten Kontrollen durch Führungspersonal des Dienstleisters statt? Wird das Qualitätsmanagement wie im Angebot beschrieben umgesetzt? Der Auftraggeber müsse ein System entwickeln, das ihm ermöglicht, bei festgestellten Verstößen tatsächlich wirksame Maßnahmen zu ergreifen. Hierzu biete sich ein **„Service-Level-Agreement"** (SLA) an. Auftraggeber und Auftragnehmer vereinbaren wechselseitige Rechte und Pflichten, die sie zu erfüllen haben sowie Maßnahmen, die bei Nichterfüllung ergriffen werden können. Üblicherweise werden für Vertragsverstöße finanzielle Strafgebühren vereinbart. Der Autor hält es für deutlich sinnvoller, lösungsorientierte Strafgebühren zu entwickeln, die beim Dienstleister Aufwand und damit Kosten verursachen, gleichzeitig aber das dem Verstoß zugrundeliegende Problem untersuchen bzw. beseitigen.

## *Spionage*

„Wenn die Puppe spioniert", titelt die FAZ am 19. Februar. Die Bundesnetzagentur habe in Deutschland die Herstellung, die Einfuhr, den Vertrieb und auch den Besitz des Produktes „My Friend Cayla" untersagt. Wer die Puppe gekauft hat, müsse sie zerstören und einen Nachweis an die Bundesnetzagentur senden. Die Puppe gelte als „verbotene Sendeanlage" nach § 90 des TKG, weil sie ein Spionagegerät sei. Angreifer könnten theoretisch über die ungesicherte Bluetooth-Verbindung

zum Smartphone Gespräche mithören. Laut Bundesnetzagentur sei die Spielzeugpuppe kein Einzelfall. Im April 2016 sei die Behörde gegen 70 Organisationen vorgegangen, die ähnliche Geräte verkauft oder vertrieben haben.

## *Tierdiebstahl*

Die Landwirte **nahe der polnischen Grenze** sehen sich mit einer Welle von Tierdiebstählen in einem ungekannten Ausmaß konfrontiert, meldet die FAZ am 27. Februar. Seit Januar seien in mehreren Fällen schon insgesamt 120 Tiere von den Weiden gestohlen worden. Neu sei vor allem die Professionalität der Diebe. Ein Großteil der Tiere sei aus dünn besiedelten Regionen der Uckermark verschwunden. Die Bauern könnten die großen Weiden dort kaum mit Zäunen sichern. Die Bereitschaft der Versicherer, die Tiere gegen Diebstahl zu versichern, lasse nach. Die professionellen Täter würden ganze Herden stehlen. Fachleute gingen davon aus, dass sie in Osteuropa im Ganzen zur Zucht weiterverwendet werden. Es dauere Monate und Jahre, bis sich die Tiere einer Zuchtherde aneinander gewöhnen. Dementsprechend hoch sei auch der ideelle Schaden. Die Polizei in Brandenburg spreche von einer Aufklärungsquote, die gegen null geht. Sie habe angekündigt, die Vorfälle in einem zentralen Register zu dokumentieren. Auch Traktoren und andere Landmaschinen würden vermehrt gestohlen.

## *Videoüberwachung*

Mit der Möglichkeit der **Videoüberwachung öffentlicher Räume durch Kommunen** befasst sich der Behörden Spiegel in der Februar-Ausgabe. „Gerade die Kommunen verfügen aufgrund der Erfahrungen verschiedener Fachdienststellen über Fachwissen über Gegenden, in denen es häufig zu Ruhestörungen, Vandalismus oder Verschmutzungen kommt. Außerdem wissen sie, in welchen öffentlichen Bereichen sich Bürgerinnen und Bürger unsicher fühlen", habe Ashok Sridharan, Oberbürgermeister von Bonn erklärt. Beim Deutschen Städte- und Gemeindebund dürfte er offene Türen einrennen. Nach der Überzeugung des HGF Gerd Landsberg müsse die Videoüberwachung an öffentlichen Plätzen und Bahnhöfen sowie im ÖPV ausgebaut werden. Nach Einschätzung der CDU-Fraktion im Bonner Stadtrat sei kein neues Gesetz erforderlich, um Videoüberwachung durch Kommunen zu ermöglichen. Bei Polizeigewerkschaften treffe der Vorschlag des Bonner OB nicht auf ungeteilte Zustimmung. In München fordere die CSU den Stadtrat auf, „Angsträume" im Stadtgebiet zu beseitigen. Dabei sollen eine stärkere Beleuchtung, bauliche Anpassungen und die sichtbare Präsenz des geplanten Kommunalen Ordnungsdienstes zum Tragen kommen. An Orten, an denen polizeiliche Überwachung nicht erforderlich sei, werde die Stadt mit eigenen optischen Überwachungsmaßnahmen tätig, soweit dies aus ihrem Blickwinkel der Prävention und Ordnung sinnvoll erscheine. Auswertung und Beobachtung der kommunalen Videoüberwachung könne zusammen mit weiteren städtischen Sicherheits- und Ordnungsaufgaben in einer Sicherheitszentrale des Ordnungsdienstes gebündelt werden.

Eine Studie des Meinungsforschungsinstituts Yougov zur **Akzeptanz von Videoüberwachung** stellt PROTECTOR in der Ausgabe 1/2-2017, S. 30/31, vor. 68 Prozent der Deutschen seien der Meinung, die Sicherheitslage im öffentlichen Raum habe sich in den letzten zwei bis drei Jahren verschlechtert. 60 Prozent sagten, die Anzahl der Situationen, in denen sie sich gefährdet fühlen, habe sich in den letzten 2–3 Jahren erhöht. Lediglich 53 Prozent fühlten sich an öffentlichen Plätzen sicherer, wenn dort Überwachungskameras zu sehen seien. 74 Prozent hätten angegeben, dass sie mehr

Videosysteme zur Sicherung des öffentlichen Raumes befürworten.

Die Implementierung des H.265-Standards behandelt Jörg Majerhofer, Hanwha Techwin Europe, in der Ausgabe 1/2-2017 der Zeitschrift PROTECTOR, S. 32/33. Kompressionstechnologien steuerten Codierung, Qualitätsabgleich und Kompression entsprechend den Bewegungen in einem Bild dynamisch und seien, gekoppelt mit H.265-Kompression, in der Lage, die Bandbreitennutzung im Vergleich zu aktueller H.264-Technologie um bis zu 75 Prozent zu reduzieren. Dadurch könnten Anwender die Kapitalinvestition und laufende Betriebskosten für Aufnahme- und Speichergeräte minimieren. Der **H.265-Standard**, der auch als High Efficiency Video Coding (HEVC) bekannt sei, unterstütze Auflösungen bis zu 8.192 mal 4.320 Pixeln. Die Hauptvorteile von H.265 gegenüber H.264 seien die Erweiterung des Mustervergleichs und der Differenz-Kodierbereiche von 16 mal 64 Pixeln. Es gebe auch eine verbesserte Segmentierung variabler Blockgrößen und Intra-Prädiktion innerhalb desselben Bildes, sowie eine verbesserte Prädiktion von Bewegungsvektoren. Die dynamische GOV (Group of Video)-Technologie, die die GOV-Länge steuert, berechne Bewegungen oder die Komplexität in Videobildern und steuere dann die Intervalle zwischen den I-Frames. Weniger Bewegung und niedrige Komplexität bedeute, den Bandbreitenverbrauch durch Erhöhung des I-Frame-Intervalls zu reduzieren. Die ROI (Region of Interest)-Technologie analysiere statische und dynamische Bereiche in Videos basierend auf einer fortschrittlichen Videoanalyse. Die Predictive-Bitrate-Control-Technologie enthalte eine Vorberechnungslogik, welche die Komplexität vor der Kompression durch den H.264-/H.265-Codec prognostiziert. Sie steuere die Bitrate durch Prädiktion der Szene und verhindere dadurch eine unnötige Erhöhung der Bitrate und optimiere die Streaming-Daten. Durch die massive Rechenleistung der in die neueste Generation von HD-Kameras integrierten DSP (Digital Signal Processor)-Chipsets eröffneten sich Gelegenheiten, den Mehrwert von Videoüberwachungssystemen für Anwender erheblich zu steigern.

## *Vorratsdatenspeicherung*

Die FAZ erinnert am 22. Februar daran, dass das EU-Parlament nach jahrelangen Diskussionen und mehreren höchstrichterlichen Urteilen gegen Vorratsdatensammlungen im April 2016 mehrheitlich dafür gestimmt habe, **Fluggastdaten des EU-Reiseverkehrs** langfristig und verdachtsunabhängig zu speichern und zu analysieren. So sei die sogenannte PNR-Richtlinie (Passenger Name Record) doch noch in Kraft getreten, um neue Datenberge aufzuhäufen und Reisebewegungen systematisch zu rastern. Die Flugbuchungs- und Eincheck-Informationen über Passagiere sollten künftig auch hierzulande von den Fluggesellschaften gemeldet und für sechs Monate festgehalten werden. Danach würden die Informationen nicht etwa gelöscht, sondern weitere viereinhalb Jahre aufgehoben. Zwar sei dafür eine „Depersonalisierung" vorgesehen, die aber ihr Versprechen nicht halte und aufgehoben werden könne. Von 2018 an würden in sechzig Datenkategorien neben Namen und Adressen der Reisenden auch gleich deren Kreditkartennummern, E-Mail- und Kontakt-Adressen, Telefonnummern, alle Daten zu mitreisenden Kindern und andere Buchungsdaten festgehalten.

## *Vorstrafenregister für Vergabeverfahren*

In ein Register sollen Strafverfolgungsbehörden künftig Unternehmen eintragen, deren Leitungspersonal Korruptionstaten zu verantworten hat, berichtet die FAZ am 24. Februar. Damit solle ausgeschlossen werden, dass

öffentliche Aufträge an belastete Unternehmen gehen. Jeder öffentliche Auftraggeber müsse von 30.000 Euro Auftragswert an eine Abfrage starten. Eingetragen würden etwa Korruptionsdelikte, Menschenhandel, Kartellverstöße und Steuerhinterziehung. Geschäftsbelebend für die ohnehin brummende Compliance-Branche dürfte die „Selbstreinigung" sein. Durch sie könnten Unternehmen die vorzeitige Löschung erwirken. Dazu müssten sie den Schaden ausgleichen, aktiv mit den Ermittlern zusammenarbeiten und organisatorische und personelle Maßnahmen ergreifen, um künftige Verstöße zu vermeiden. Ohne weiteres Zutun würden die Einträge nach drei bis fünf Jahren gelöscht. Vorbild seien die in sechs Bundesländern schon bestehenden Korruptionsregister.

## *Wächterkontrollsystem*

Constantin Buda, Reslink Solutions Ltd., geht in der Ausgabe 1/2-2017 der Zeitschrift PROTECTOR, S. 68, auf Wächterkontrollsysteme ein. Ein Mobilfunkgerät sei im Hinblick auf die zur Verfügung stehenden Möglichkeiten anderen Berichtsformen deutlich überlegen: Meldung von Vorfällen in Echtzeit, einschließlich Foto und Video; standortbezogene Datenerfassung und Zugriff auf Kundendaten überall und jederzeit; Alarme – egal welcher Art – am Einsatzort; Warnmeldungen – wegen etwas, das geschehen sollte, jedoch nicht geschehen ist; erweiterte Rundgänge, einschließlich der Überwachung der Aktivitäten in Echtzeit; vollständiger Überwachungspfad der gesamten Tätigkeiten im Außendienst; Offlinemodus und automatisierte Berichterstattung; digitale Formulare und Umfragen, die die Mitarbeiter direkt vor Ort beim Kunden ausfüllen können.

## *Wertpapierhandelsgesetz-Verstoß*

Wie die FAZ am 23. Februar berichtet, drohen künftig deutlich höhere Strafen, wenn Unternehmen ihren Pflichten in der Finanzberichterstattung nicht nachkommen. Die deutsche Finanzaufsicht BaFin habe ihre **Bußgeldleitlinien nach dem Wertpapierhandelsgesetz** (WpHG) konkretisiert. Vor allem für größere Unternehmen könne ein Verstoß gegen die Pflichten zur sofortigen Veröffentlichung kursbeeinflussender Entwicklungen zu Stimmrechtsänderungen oder zu Angaben in den Finanzberichten teuer werden. Bei einem Jahresumsatz von 50 Mrd. Euro und einem Börsenwert des Unternehmens von mehr als 20 Mrd. Euro könne die BaFin gegen den Emittenten ein Bußgeld von bis zu 2,5 Mrd. Euro verhängen, wenn Finanzberichte nicht zur Verfügung gestellt werden. Bislang habe die maximale Strafe 200.000 Euro betragen. Verstoße dieses Unternehmen gegen die Adhoc-Pflichten, könne die Strafe bis zu einer Mrd. Euro ausmachen. Grundsätzlich könne die Finanzaufsicht die Verstöße mit bis zu zehn Mio. Euro, fünf Prozent des konzernweiten Jahresumsatzes oder das Zweifache des aus dem Verstoß gezogenen wirtschaftlichen Vorteils verhängen. Es gelte dann immer die höhere Strafe, bei großen Unternehmen in der Regel das umsatzbezogene Bußgeld.

## *Wohnungseinbruch*

Der Wohnungseinbruch sei 2016 nach einem mehrjährigen Anstieg zurückgegangen, meldet die FAZ am 24. Februar. In NRW sei die Zahl der gemeldeten Einbrüche um 15,7 Prozent gesunken, in Hessen um 10,3 Prozent, im Saarland um 20,1 Prozent und in Hamburg um 16,6 Prozent.

## *Zutrittskontrolle*

PROTECTOR stellt in der Ausgabe 1/2-2017, S. 28/29, ein **System digitaler Zutrittskontrolle** von PCS Systemtechnik GmbH vor. Für den erhöhten Sicherheitsbedarf sensibler Unternehmensbereiche biete PCS die hochsichere Handvenenerkennung Intus PS an. Sie sei fälschungssicher. Das Handvenenmuster werde in ein Template umgewandelt und könne so auf einem Mitarbeiterausweis gespeichert werden. Die Zutrittskontrolle zu sensiblen Bereichen wie dem Rechenzentrum könne mit zwei Faktoren erfolgen: Nur der berechtigte Personenkreis wird am Handvenenscanner eingelernt und erhalte eine Mitarbeiterkarte mit seinen biometrischen Merkmalen. Nach dem Einlernen könne der Mitarbeiter den Ausweis vor den RFID-Teil des Systems halten und anschließend mit der Hand bzw. den Handvenen seine Person verifizieren. Die Handvenenerkennung könne mit EMA verknüpft werden. Bei Unternehmensbereichen wie Warehouse und Lager könnten Ein- und Austrittsleser genutzt werden, um zu dokumentieren, welche Mitarbeiter wann und wie lange anwesend waren und ob alle Mitarbeiter am Feierabend das Werk verlassen haben. Bei der Zutrittskontrolle gehe der **Trend zum Mobile Access**, heißt es in der Aus-gabe 1/2017 der Zeitschrift Security insight, S. 31/32. Dank neuer Mobile-Access-Technologien und Kommunikationsverfahren wie NFC und Bluetooth Smart könnten Smartphones heute problemlos als universale digitale Ausweise für den Zutritt zu Gebäuden genutzt werden. Unerheblich sei deshalb, ob in Gebäuden die Netzabdeckung etwa zu gering für den Empfang eines Signals ist. Für die Nutzung einer Mobile-Access-Lösung sei lediglich erforderlich, auf dem Endgerät die für die App-Nutzung erforderliche Betriebssystemversion sowie eine Push-ID zu installieren. Sollte das Smartphone einmal in fremde Hände gelangen, schütze ein optionaler PIN die App vor unautorisiertem Zugriff auf die mobile ID.

# *Impressum*

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

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

**Herausgeber:**
Manfred Buhl, Vorsitzender der Geschäftsführung, Düsseldorf

**Verantwortlicher Redakteur:**
Bernd Weiler, Leiter Kommunikation und Marketing

**Beratender Redakteur:**
Reinhard Rupprecht, Bonn

**focus.securitas.de**

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

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

E-Mail: info@securitas.de