Focus on Security

Ausgabe 08, August 2016

SECURITAS

Inhalt

Amok

Bei einem Amoklauf in München tötete der 18-jährige Schüler David S. am 22. Juli im Olympia-Einkaufszentrum im Münchner Stadtteil Moosach neun Menschen. Vier weiteren brachte er Schussverletzungen bei. Das Tatmotiv war offenbar Hass auf Ausländer. Die Polizei war mit einem Großaufgebot im Einsatz. Zweieinhalb Stunden nach Beginn des Amoklaufs traf eine Polizeistreife in der Nähe des Einkaufzentrums auf den Täter. Dieser erschoss sich, als die Polizisten ihn ansprachen. In der Zeit von 17:52 bis 24 Uhr gingen beim Polizeipräsidium München über 4.300 Notrufe ein. Darunter waren zahlreiche Hinweise zu möglichen weiteren Tätern und zu Schießereien in der Stadt. Sie stellten sich alle als Falschmeldungen heraus.

Bahnsicherheit

Nach den jüngsten Gewalttaten wolle die Deutsche Bahn das Sicherheitspersonal auf Bahnhöfen und in Zügen verstärken, berichtet die FAZ am 28. Juli. „Wir wollen in den nächsten Jahren bei der DB Sicherheit rund 500 Mitarbeiter zusätzlich einstellen", habe der Vorstandsvorsitzende gesagt. Die derzeit 3.700 Sicherheitskräfte sollten überdies besser qualifiziert werden. In den kommenden Jahren würden 85 Mio. Euro in die Videoüberwachung investiert. Schon heute seien 27.000 Kameras in Zügen installiert. Den umfassenden Einsatz sogenannter Körperkameras („Bodycams"), die Sicherheitskräfte an ihrer Uniform tragen, plane die Bahn spätestens von Januar 2017 an.

Betrug

Das Bundeskriminalamt hat einen Flyer mit Warnhinweisen zum **„CEO-Fraud"** veröffentlicht. Beim CEO-Fraud gäben sich Täter – nach Sammlung jeglicher Art von Information über das anzugreifende Unternehmen – beispielsweise als Geschäftsführer (CEO) des Unternehmens aus und veranlassten einen Unternehmensmitarbeiter zum Transfer eines größeren Geldbetrages ins Ausland. Für die Täter seien beispielsweise E-Mail-Erreichbarkeiten von Interesse, da sie darauf die Systematik von Erreichbarkeiten herleiten. Soziale Netzwerke, in denen Mitarbeiter ihre Funktion und Tätigkeit oder persönliche Details preisgeben, stellten ebenfalls eine wichtige Informationsquelle dar. Die Täter nähmen mit den „ausgeforschten" Mitarbeitern Kontakt auf und würden sich als Leitende Angestellte, Geschäftsführer oder Handelspartner ausgeben. Dabei forderten sie z. B. unter Hinweis auf eine angebliche Unternehmensübernahme oder angeblich geänderter Kontoverbindungen den Transfer eines größeren Geldbetrages auf Konten in China und Hong Kong, aber auch in osteuropäischen Staaten. Durch „CEO-Fraud" hätten Kriminelle in den letzten Monaten bereits mehrere Mio. Euro mit zum Teil gravierenden Folgen für das betroffene Unternehmen bzw. die getäuschten Mitarbeiter erbeuten. Das BKA rät, bei ungewöhnlichen Zahlungsanweisungen folgende Schritte durchzuführen: Überprüfen der E-Mail auf Absenderadresse und korrekte Schreibweise, Verifizieren der Zahlungsaufforderung über Rückruf oder schriftliche Rückfrage und Kontaktaufnahme mit der Geschäftsleitung bzw. dem Vorgesetzten.

Bitcoins

Die FAZ befasst sich am 28. Juli mit der Kryptowährung Bitcoin. Im Cybercrime-Bericht, den das BKA vorgestellt habe, tauche immer wieder die elektronische Kunstwährung als bevorzugtes Zahlungsmittel von Kriminellen auf. Erpresser, die etwa Online-Händler damit bedrohen, ihre Internetseite vom Netz zu nehmen, wollten als Lösegeld Bitcoins haben,

denn der Geldfluss dort sei schwer nachzuvollziehen. Bitcoin-Anhänger reklamierten, die Kunstwährung sei dezentral organisiert und damit rund um die Welt davor geschützt, dass Zentralbanken in die Währung eingreifen. Außerdem seien Bitcoin-Transaktionen nicht nur vollständig anonym, sondern gleichzeitig vollständig transparent. Denn jeder Handel mit Bitcoins werde in einer Art digitalem Kontobuch, der Blockchain, verzeichnet und sei dort für jedermann einsehbar. Diese Datei sei auf jedem Rechner von Handelsteilnehmern abgespeichert und solle damit vor Betrug schützen, weil jede Manipulation der Datei auffallen würde, da dem Block von Transaktionen mit einer neuen Überwiesung ein weiterer, unveränderlicher und einzigartiger Block hinzugefügt werde. Die Rechner lösten komplizierte Algorithmen und bekämen als Belohnung die Bitcoins. Je mehr Leute nach ihnen schürfen, desto komplizierter werde die Rechnung. Während anfangs Privatpersonen tagelang ihre Heimcomputer laufen ließen, um Bitcoins zu errechnen, gebe es heute nicht nur spezielle Computerchips, die extra für dieses Mining entwickelt wurden und weniger Strom verbrauchen sollten, sondern auch Unternehmen, die sich auf das Schürfen konzentriert haben. Zudem schlössen sich Menschen zu Mining-Gruppen zusammen, um ihre Rechenkraft zu bündeln. Ein Algorithmus kontrolliere dabei, dass nicht beliebig viele Einheiten der Kryptowährung neu entstehen können. An die Digitalwährung komme man aber nicht nur durch Rechenleistung. Sie könne auch getauscht werden. Durch die Anonymität könne eine Person auch mehrere Wallets, also Bitcoin-Portemonnaies, eröffnen und sich damit selbst digitales Geld hin- und her überweisen. Trotzdem habe die Kryptowährung auch bei offiziellen Stellen inzwischen Interesse geweckt, wenngleich sie noch in keinem Land der Welt als offizielles Zahlungsmittel anerkannt sei. Mit steigender Nutzung der Kryptowährung stellten sich auch grundlegende Rechtsfragen. Der EuGH habe entschieden, dass Bitcoins wie jedes andere Zahlungsmittel zu behandeln seien und deshalb der Umtausch nicht mehrwertsteuerpflichtig sei. Eine kalifornische Richterin habe dagegen Bitcoins als Eigentum und nicht als Geld bewertet.

Brandschutz

Bettina Bormann, VdS Schadenverhütung, befasst sich in der Ausgabe 2-2016 der Zeitschrift r+r report, S. 14/15, mit der **versicherungstechnischen Bewertung von Brandmeldeanlagen** (BMA). Sie behandelt VdS-anerkannte Produkte und Systeme, Richtlinien für Planung und Einbau, Fachfirmen und anerkannte Errichter, Abnahme-und Wiederholungsprüfungen. Die VdS 2095 sei die Grundlage für praxisnahe und alltagstaugliche Projektierung wirksamer BMA. VdS-anerkannte Errichter böten qualifiziert das volle Leistungsspektrum an und könnten ein Installationsattest als Basis für eine versicherungstechnische Bewertung erstellen. Ein mängelfreier Prüfbericht einer Prüfung nach baurechtlichen Vorgaben dokumentiere nur, dass die Vorgaben aus dem Sicherungskonzept eingehalten wurden. Nur eine versicherungstechnische Bewertung mit Schutzgrad stelle sicher, dass eine BMA vollständig im gesamten Schutzbereich auf ihre Wirksamkeit und Zuverlässigkeit bewertet wurde.

Die **Ausrüstung von Kühlraumtüren mit Brandschutzschaltern** behandelt Norbert Schaefer, Siemens, in der Ausgabe 2-2016 der Fachzeitschrift r+r report, S. 18–20. Tür- und Torsysteme in Kühlhäusern und Gefrierräumen unterlägen einer hohen mechanischen Belastung. Im Bereich der Heizkabel und weiterer elektrischer Systeme in der Tür würden die Sicherheitsstandards durch den Einsatz eines neuartigen Brandschutzschalters erhöht. Der Brandschutzschalter 5SM6 erkenne gefährliche Fehlerlichtbögen automatisch mit hoher Zuverlässigkeit und werde in Kombination mit einem Leitungsschutz- oder mit Fehlerstrom-/Leitungs-

schutzschaltern (FI/LS-Schaltern) eingesetzt. Im Detektionsfall schalte er den betroffenen Stromkreis sofort sicher ab. Die Komponente erfasse nicht nur Strom und Fehlerspannung, sondern messe auch kontinuierlich das Hochfrequenzrauschen hinsichtlich Intensität, Dauer und der dazwischen liegenden Lücken. Integrierte Filter in Verbindung mit intelligenter Software verarbeiteten, analysierten und bewerteten diese Signale nach einer Vielzahl von Kriterien. Mit dem Brandschutzschalter werde ein Zusatzschutz geboten, der technisch bisher noch nicht möglich gewesen sei und bereits den aktuellsten Normen entspreche.

Joachim Schäfer, Berufsfeuerwehr Aachen, thematisiert in der Ausgabe 2-2016 der Zeitschrift s+s report, S. 21–25, Gefahren und Schutzmaßnahmen im Zusammenhang mit **Selbstentzündung in Betrieben**. Eine Auswertung des Instituts für Schadenverhütung und Schadenforschung der öffentlichen Versicherer von 2013 habe ergeben, dass bisher 228 Brandschäden auf Selbstentzündung verschiedener Materialien zurückzuführen waren. Das entspreche einem Anteil von ungefähr zwei Prozent am Gesamtschadengeschehen. Vor allem Öle und Fette seien mit einem Anteil von 61 Prozent die Hauptverursacher von Selbstentzündungen. Auslöser könnten ebenso mikrobiell anfällige landwirtschaftliche Produkte oder Recyclingmaterial aus Kunststoff sein. Der Autor unterscheidet zwischen Selbstentzündungen von organischem Material, spontanen chemischen Selbstentzündungen und Selbstentzündungen in sauerstoffreicher Atmosphäre. Im Einzelnen geht der Autor ein auf Selbstentzündungen von landwirtschaftlichen Produkten, Selbstentzündungen bei der Lagerung von Biomasse, Selbstentzündungen von Ölen und Fetten, Selbstentzündungen fettverschmutzter Textilien und Recyclingmaterial aus Kunststoff und beschreibt jeweils spezifische Gefahren und Schutzmaßnahmen. Für alle Bereiche gelte, dass eine gute Trocknung der Produkte und die Verhinderung eines Wärmestaus die allerwichtigsten vorbeugenden Schutzmaßnahmen sind. Anzustreben seien eine intensive Ausbildung des Personals sowie die Beachtung der einschlägigen Verhaltensmaßregeln der verschiedenen anerkannten Fachleute bzw. Einrichtungen.

Cloud Computing

Mittelständische Unternehmen und Verwaltungen setzen bereits häufig Cloud-Lösungen aus den Bereichen E-Mail- und Websicherheit, Datensicherheit, Application Security oder Network Security ein, berichtet heise.de am 5. Juli. Das ergebe eine aktuelle Auswertung der Studie Security Bilanz Deutschland, die sich auf den Mittelstand und öffentliche Verwaltung konzentriere. E-Mail und Web Protection als Cloud-Lösung nutzten demnach bereits über die Hälfte der befragten Unternehmen aus Industrie, Dienstleistungen, Banken und Versicherungen sowie öffentlichen Verwaltungen. Einzig der Handel sei hier noch nicht so weit, mehr als ein Viertel der befragten mittelständischen Händler habe jedoch schon konkrete Planungen, in Zukunft cloud-basierte E-Mail- und Web-Sicherheit zu nutzen.

Maria Winkler, IT & Law Consulting, befasst sich im Video Security Special der Zeitschrift Sicherheitsforum, Juni 2016, S. 19–23, mit der Auslagerung von Daten in die Cloud. **Cloud-Services** versprächen den Unternehmen Kosteneinsparungen durch den flexiblen Einsatz der Informatikressourcen sowie Effizienzsteigerungen, da man sich bei einer Auslagerung an externe spezialisierte Partner auf das Kerngeschäft konzentrieren könne. Die Angebote reichten dabei von einer reinen Speicherung der Daten in der Cloud bis hin zum Bezug von gesamten cloudbasierten Services. Wer Daten auslagere, müsse zwingend die rechtlichen Rahmenbedingungen prüfen. Zur Reduktion von rechtlichen Risiken sollten möglichst frühzeitig folgende Punkte

geklärt werden: Ist es zulässig, die Daten an ein externes Unternehmen auszulagern? Ist es zulässig, die Daten ins Ausland auszulagern? Welche datenschutzrechtlichen Vorgaben sind bei einer grundsätzlichen Zulässigkeit der Auslagerung zu beachten? Bestehen weitere spezialgesetzliche Vorgaben, die zu beachten sind? Entspricht die angebotene Standarddienstleistung den gesetzlichen Vorgaben? Wie kann die Einhaltung der gesetzlichen Vorgaben während der gesamten Vertragsdauer angemessen kontrolliert werden? Welche Risiken enthalten die Vertragsbestimmungen des Cloud-Anbieters. Die Autorin behandelt folgende Themen: Der Cloud-Anbieter darf Daten nicht zweckentfremden; Rechenzentren im Ausland; Einfluss von „Safe Harbor" und Vertragsbestimmungen des Cloud-Anbieters.

Peter Marwan bezeichnet in silicon.de am 19. Juli die Angst vor der Cloud als Bremsklotz für weitere Digitalisierung im Bereich KMU. Einer Untersuchung des Instituts für Mittelstandsforschung (IfM) zufolge nutzen KMU die Software für **Enterprise Resource Planning (ERP) und Customer Relationship Management (CRM**) besonders häufig. Allerdings mache die Verbindung der Geschäftsprozesse mit denen von Zuliefern und Kunden, bedingt durch geringes Vertrauen in die Cloud, derzeit wenig Fortschritte. ERP-Softwarepakete seien 2015 in rund 55 Prozent der deutschen KMU zum Einsatz gekommen. Viele Unternehmen überschätzten sich in Bezug auf den eigenen Grad der Digitalisierung. In der siebten Auflage seines „Cloud Vendor Banchmark" liste Experton 150 relevante und meist mittelständisch geprägte Cloud-Anbieter auf. Unklar bleibe in den IfM-Zahlen, was denn nun eigentlich Digitalisierung ist. Auf dem Weg ins digitale Zeitalter sollten auch neu entstehende Möglichkeiten genutzt werden, möglicherweise sogar, um ganze Marktstrukturen zu verändern und neue Angebote zu entwickeln. Zur Cloud-Nutzung griffen Firmen laut Experton vor allem wegen neuer Anforderungen bei Big Data und Mobilität. Und da die Komplexität in solchen Szenarien häufig die Möglichkeiten der Unternehmen überschreite, steige auch die Nachfrage nach entsprechenden Beratungslösungen. Neben Storage in der Public Cloud setze sich Experton zufolge auch Software as a Service durch. Außerdem würden von den Unternehmen derzeit vor allem Enterprise Cloud Filesharing, Unified-Communications as a Service und Big Data as a Service genutzt.

Einbruch

Der Behörden Spiegel berichtet in der Juli-Ausgabe, dass die Länder Bayern, Baden-Württemberg, Hessen und Rheinland-Pfalz ihre Kooperation im Kampf gegen Einbruchskriminalität verstärken. Kern der unterzeichneten Vereinbarung sei ein Acht Punkte-Programm, das insbesondere einen schnelleren und besseren Informationsaustausch, eine stärkere gemeinsame Täterfahndung sowie eine noch intensivere Zusammenarbeit bei konkreten Ermittlungsverfahren sowie in der Prävention vorsehe.

Endgerätesicherheit

Große Teile der Mobilfunkinfrastruktur sind laut Sicherheitsforschern über eine Lücke in einer Software-Bibliothek gefährdet, berichtet golem.de. Ein Fix stehe zwar bereit, doch Updates werde es für die meisten Geräte wohl nicht geben. Eine kürzlich veröffentlichte Sicherheitslücke in einer Software-Bibliothek stelle nicht nur für Mobilfunktürme, sondern auch für Router, Switches und individuelle Smartphones im Mobilfunknetzwerk ein Risiko dar.

Errichter

Die Fachzeitschrift s+s report, Ausgabe 2-2016, S. 61, weist auf den **europäischen Norm-Entwurf „Dienstleistungen für Sicherheitsanlagen**" hin. Es sei ein Versuch einer EU-weiten Festlegung von Mindestanforderungen an die Errichter von Brandmelde-, Lösch- und Alarmanlagen. Mit ihrem Inkrafttreten werde die EN 16763 gravierenden Einfluss auf den Markt für technische Brand- und Einbruchschutzdienstleistungen nehmen. Vor diesem Hintergrund habe auch VdS die bekannte Anerkennung für Errichter dieser Gewerke optimiert: Der **„Errichter 2.0"** biete ein kombiniertes Verfahren für bis zu drei Fachrichtungen (Brandmelde-, Einbruchmelde- und Videoüberwachungsanlagen), umfasse die nötigen Normanforderungen und erleichtere die VdS-Anerkennung gerade für die zahlreichen „Kombi-Errichter". Die entsprechenden Richtlinien zur „Anerkennung von Errichterunternehmen für Gefahrenmeldeanlagen (GMA)", VdS 3403, seien seit 1. Januar 2016 in Kraft.

Flughafensicherheit

„Flughäfen gegen mehr Sperren" titelt die FAZ am 5. Juli. Aus Sicht deutscher Luftfahrtmanager sei der unkontrollierte Zugang zum Flughafengebäude technisch und wirtschaftlich notwendig. Jede zusätzliche Kontrollstelle schaffe einen zusätzlichen Angriffspunkt, wenn sich dort Wartende sammelten. Mehr Sperren seien nicht hilfreich. Im Ausland gebe es schon viele Beispiele für Beschränkungen. In Moskau müssten Besucher Taschen vorzeigen und durch einen Metalldetektor schreiten. In der Türkei sei das Durchleuchten aller Gepäckstücke am Eingang Standard. In Brüssel seien nach dem Anschlag Gepäck- und Ausweiskontrollen eingeführt, nach Beschwerden über lange Wartezeiten aber wieder abgeschwächt worden.

Gasdetektion

Dipl.-Ing. Herbert Schmolke, VdS, befasst sich in der Ausgabe 2-2016 von s+s report, S. 56–58, mit der **Anerkennung von Sachverständigen für Gasdetektion**. Die Anerkennung von Personen, die in technischen Einrichtungen prüfend tätig sind, durch einen unabhängigen Dritten sei nicht zwangsläufig normativ erforderlich, könne aber sehr sinnvoll oder sogar unumgänglich sein, z. B. wenn von Behörden oder Anlagenbetreibern für bestimmte Prüfungen der Nachweis einer ausreichenden fachlichen Kompetenz für die korrekte Ausführung gefordert wird. Mit einem Zertifikat werde öffentlich bestätigt, dass einem unabhängigen Dritten gegenüber die fachliche Kompetenz und die erfolgreiche Teilnahme an eventuell erforderlich Aus- und Fortbildungsveranstaltungen nachgewiesen wurden. Der Autor thematisiert die Bedeutung der Sachverständigenanerkennung bei Gasleckageuntersuchungen, das VdS-Anerkennungsverfahren für eine geeignete Gasdetektion und die Anforderungen an den VdS-anerkannten Sachverständigen für Gasdetektion. Die Anerkennung erlösche nach Ablauf von vier Jahren, könne aber verlängert werden.

Gefahrenmeldeanlagen

Dipl.-Ing. Herbert Schmolke, VdS, erläutert in Ausgabe 2-2016 der Fachzeitschrift s+s report **Schutzmaßnahmen gegen Überspannung** für Gefahrenmeldeanlagen (S. 47–51). Die Richtlinie VdS 2833 „Schutzmaßnahmen gegen Überspannung für Gefahrenmeldeanlagen" sei aktualisiert worden. Der Autor behandelt grundsätzliche Anforderungen, Maßnahmen, die stets zwingend erforderlich sind (Installationsbereiche, Potenzialausgleich, Anlagenteile der GMA, Schlüsseldepots und Feuerwehr-Schlüsseldepots, Leitungsverlegung außerhalb von Gebäuden,

Sicherheitsabstände zu blitzstromführenden Teilen, Schirmanschlüsse bei Geflechtschirmen und Maßnahmen, die nur nach Risikobewertung vorzusehen sind.

Gehäusesicherheit

Gehäuse für Steuerung und Sekundärverkabelung in Umspannwerken, Versorgungssysteme auf den Betriebsgeländen großer Pharma- und Chemiekonzerne oder Bahnverkehrsleitsysteme seien Angriffen durch Mensch und Wetter ausgesetzt, heißt es in der Ausgabe 7/8-2016 der Zeitschrift PROTECTOR. Bis heute seien viele Systeme rein mechanisch gesichert. Damit sei eine lückenlose Dokumentation der Aktivitäten an diesen Gehäusen nicht möglich. Hinzu kämen eine aufwändige Schlüsselverwaltung und hohe Kosten im Falle des Austausches von kompletten Schließanlagen. Um Gehäuse vor solchen Angriffen zu schützen, müsse ein besonderer Fokus auf die Verschlusssysteme gelegt werden. Der Verschluss sei meist der anfälligste Bereich an einem Gehäuse. Die Firma Dirak aus Ennepetal biete unter ihrer Marke für mechatronische Verschlusslösungen „E-Line by Dirak" ein vandalismussicheres Verschlusssystem an, das die Anforderungen im öffentlichen Bereich in Funktion, Material und Design aufgreife. Neben einem neuen Dichtungskonzept, das den Verschluss nach IP65 abdichte und somit vor Wasser- und Staubeintritt schütze, sei der Schwenkhebel aus Zinkdruckguss vandalismussicher konstruiert und entsprechend der Widerstandsklasse „Resistance-Class II (RC2)-09/RC2" nach DIN EN 1630:2011 erfolgreich geprüft worden. Der Griff sei mit einem Antigraffiti-Lack ausgestattet. Das Verschlusssystem sei voll vernetzt einsetzbar.

Geldfälschung

Nach der Einführung der neuen 20-Euro-Scheine im November 2015 sei die Zahl ihrer Fälschungen deutlich zurückgegangen, berichtet die FAZ am 22. Juli. Dies ergebe sich aus den neuen Falschgeldzahlen der EZB. Nur noch 27 Prozent aller gefälschten Scheine in Deutschland seien 20-Euro-Scheine. Zuvor seien es 40 Prozent gewesen. An Bedeutung gewonnen habe dadurch für die Fälscher der **50-Euro-Schein**. Gut 26.000 falsche 50-Euro-Scheine habe die Bundesbank registriert. Damit seien mehr als die Hälfte der 45.700 registrierten Blüten 50-Euro-Scheine. Am 4. April 2017 sollen die neuen 50-Euro-Scheine eingeführt und damit den Fälschern in diesem wichtigsten Bereich ihr Tun erschwert werden. Die Zentralbanken würden auf das Prinzip „Fühlen-Sehen-Kippen" hinweisen, mit dem Fälschungen sich anhand der zahlreichen Sicherheitsmerkmale gut erkennen ließen. Insgesamt sei die Zahl der Fälschungen in Deutschland im ersten Halbjahr 2016 leicht gestiegen, im Euroraum jedoch deutlich zurückgegangen.

Geldwäsche

31 Personen seien wegen Verdachts auf Geldwäsche in Shanghai festgenommen worden, meldet Deutsche Inkerman Froud Weekly in der Ausgabe 170. Das System habe darin bestanden, dass Kunden Yuan auf Inlandskontos von Kriminellen überwiesen worden. Durch einen Zahlungskanal, der außerhalb der normalen Banksysteme lag, seien dann entsprechende Beträge in Fremdwährung auf die ausländischen Konten der Kunden eingezahlt worden. Das System sei als die größte illegale Bankoperation bezeichnet worden, die Shanghai in jüngster Zeit gesehen habe.

Hagelschutz

Dipl.-Ing Hans Starl, Elementarschaden Präventionszentrum Austria, erläutert in der Ausgabe 2-2016 der Zeitschrift s+s report, S. 52/53, den erfolgreichen **Hagelschutz dank Hagelsimulationsmaschine**. Sowohl der Schadensprävention als auch der Prüfung von Baumaterialien auf ihre Hagelresistenz komme eine immer größere Bedeutung zu. Wirkungsvoller Hagelschutz lasse sich durch die Berücksichtigung eines Drei-Schritte-Systems erreichen: Überprüfung der Hagelgefährdung des Standorts anhand der Hagelgefährdungskarte, Überprüfung von Baumaterialien auf deren Hagelresistenz mittels Hagelsimulationsmaschine und Eintragung der Prüfergebnisse in das Hagelschutzregister. Der Autor behandelt die Hagelgefährdung des Standorts und die Überprüfung mittels Hagelsimulationsmaschine. Das österreichische Institut für Brandschutztechnik und Sicherheitsforschung (IBS) habe ein Prüfgerät entwickelt, das es ermögliche, Baumaterialien der Gebäudehülle auf deren Hagelresistenz zu prüfen und zu klassifizieren. Mit der Hagelsimulationsmaschine würden genormte, im Labor produzierte Eiskugeln bis zu einem Durchmesser von 70 mm pneumatisch auf eine Auftreffgeschwindigkeit von bis zu 140 km/h gebracht. Die Prüfungsergebnisse aller Bauteile würden im Hagelschutzregister transparent, vergleichbar und standardisiert publiziert. Aktuell seien bereits mehr als 350 Produkte der Gebäudehülle registriert.

IT-Forensik

Rechtsanwältin Friederike Scholz und Holger Berens, beide Rheinische Fachhochschule Köln, stecken in Ausgabe 2-2016 der Zeitschrift s+s report, S. 38–40, den **rechtlichen Rahmen der IT-Forensik** ab. Nach der Definition des BSI sei IT-Forensik die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems. Man unterscheide zwei verschiedene Arten der forensischen Analyse: das „Live-Response-Verfahren", eine Analyse des laufenden, nicht abgeschalteten Systems, und die „Post-Mortem-Analyse", bei der das ausgeschaltete System analysiert werde, indem ein digitales Duplikat bitweise 1:1 erstellt wird. Ein großer Nachteil bestehe bei dieser Methode darin, dass flüchtige Daten beim Ausschalten gelöscht würden und somit zur Untersuchung nicht mehr zur Verfügung stünden. Hieraus folge, dass eine Kombination beider Methoden sinnvoll ist. Folgende Fragen stünden im Mittelpunkt einer Untersuchung: Was, wo, wann und wie ist etwas geschehen, wer hat es getan und was kann gegen eine Wiederholung unternommen werden? Um diese Fragen beantworten zu können, sei das sogenannte **Secure-Analyse-Present-Modell** die wohl am häufigsten angewandte Methode. Schon allein die Durchführung der IT-Forensik mit entsprechender Software sei mitbestimmungspflichtig. Dies gelte dann auch schon bei der generellen, anonymisierten Sammlung der Datenspuren.

IT-Sicherheit

Dipl. Wirtschaftsjurist Sebastian Brose, VdS Schadenverhütung, stellt in der Ausgabe 2-2016 von s+s report, S. 26–28, einen von VdS entwickelten **Quick Check** für Industrial **Control Systems** (ICS) vor. Längst nicht alle Unternehmen verfügten über ein ausreichendes Sicherheitskonzept gegen Cyberangriffe. Mit einem webbasierten kostenlosen VdS-Quick-Check könnten sich Unternehmen innerhalb von 20 Minuten selbst ein erstes Bild über den Status der Cybersecurity ihres Unternehmens verschaffen. Der Fragenkatalog von VdS umfasse 39 Fragen zum

individuellen Schutzgrad des Unternehmens. Die Auswertung bestehe aus zwei Berichten (Kurz- und Langfassung), die auch konkrete Maßnahmenempfehlungen zur sofortigen Umsetzung enthielten. Neben dem auf Office-Anwendungen ausgerichteten ersten VdS-Quick-Check habe VdS nun einen zweiten VdS-Quick-Check veröffentlicht, dessen Schwerpunkt auf Steuerungs- und Automatisierungssystemen, sogenannten Industrial Control Systems (ICS), liege. Die beiden Quick-Checks bildeten den Auftakt für ein mehrstufiges Verfahren, das zusammen mit dem Quick-Audit und einer Zertifizierung nach VdS 3473 einen wirkungsvollen IT-Sicherheitsschutz für mittelständische Unternehmen böte. Die VdS Richtlinien 3473 gehören nach einer BSI-Studie bereits zu den Top 3-Standards bei der Implementierung eines Managementsystems für Informationssicherheit (ISMS) und hätten sich als richtungsweisender Cybersecurity-Standard für mittelständische Unternehmen fest etabliert. Die Organisation von Informationssicherheit sei ein wesentlicher Schwachpunkt in den Unternehmen. Die Mehrheit der teilnehmenden Unternehmen verfüge über ein Schutzkonzept für ihre IT-Systeme, jedoch würden keine systematischen Risikoanalysen durchgeführt. Golem.de weist auf ein neues Tool hin, das darauf aufmerksam machen soll, dass **häufig benutzte Passwörter** ein Risiko darstellen. Nutzer könnten damit ihre eigene Verwundbarkeit testen. Kopierte Nutzerdaten von Online-Diensten seien vor allem deshalb ein Problem, weil viele Nutzer ihre Passwörter wiederverwenden. Da meist die Mailadresse als Login-Name eingesetzt wird, ließen sich entwendete Nutzerdaten häufig missbrauchen, um auch andere Accounts zu kompromittieren. Vielen Nutzern dürfte gar nicht mehr bewusst sein, bei welchen Diensten sie sich in den vergangenen Jahren mit welchen Passwörtern angemeldet haben. Mit dem Kommandozeilentool Shard ließen sich verschiedene Accounts jetzt einfach durchprobieren. Große Webdienste hätten in der Regel Sicherheitsmechanismen, wenn in kurzer Zeit zahlreiche erfolglose Login-Versuche erfolgen oder von einer IP-Adresse aus in kurzer Zeit viele Kombinationen von Nutzername und Passwort durchprobiert werden. Mit dem Webdienst „Have I been pwned" könnten Nutzer feststellen, ob ihre Accounts von großen Datenpannen oder Einbrüchen betroffen sind.

In der Juli-Ausgabe des Behörden Spiegel fordert BSI-Präsident Arne Schönbohm Dialogbereitschaft von der Wirtschaft. „Alleine können wir es nicht schaffen," sagte Schönbohm. Als Beleg für seine Aussagen habe er die **zunehmenden Cyberangriffe auf Kritische Infrastrukturen 2016** erwähnt. Allein 60 Krankenhäuser seien durch Ransomware angegriffen worden. Schönbohm forderte dazu auf, kein Lösegeld zu zahlen, weil die Zahlungen das Geschäftsfeld anfeuern würden. Awareness sei besonders wichtig, weil drei Viertel aller Attacken über infizierte E-Mail-Anhänge erfolgten. Daneben sei eine effektive Back-up-Strategie der beste Schutz, um sich gegen Erpressertrojaner zu wappnen. Bei einem Cyberangriff auf das Atomkraftwerk in Grundremmingen habe das BSI verhindert, dass der Angriff die Steuerung des AKWs erreichte. Um auf das gestiegene Bedrohungspotenzial zu reagieren, habe das BMI eine schnelle Eingreiftruppe für Cybervorfälle gegründet, die beim BSI angesiedelt werde. Schönbohm hält es für zwingend erforderlich, dass das Thema IT-Sicherheit bei allen Unternehmen auf Vorstandsebene angesiedelt wird.

Hans-Joachim Popp, CIO des Deutschen Zentrums für Luft- und Raumfahrt, fordert in der Juli-Ausgabe des Behörden Spiegel **mehr IT-Sicherheit im Hochtechnologiebereich**. Dieser sei besonders anfällig für Wirtschaftsspionage. Das Internet müsse stärker reguliert werden. Dies könne unter anderem dadurch geschehen, dass man verhindere, dass Cyberkriminelle mit Schadsoftware hinterlegte Webseiten bauen würden. Der wilde Westen im Cyberraum sei völlig ohne Regulierung.

Unternehmen sollten sich fragen, welche Systeme mit dem Internet verbunden sein müssen. Insbesondere Back-ups sollten offline aufbewahrt werden. Dr. Klaus Mittelbach, ZVEI, beklagte, dass bei der Entwicklung der Industrie 4.0 der IT-Sicherheit oftmals eine zu geringe Bedeutung beigemessen werde. Er messe der Elektroindustrie eine Schlüsselrolle beim Gelingen der Modernisierungen im Rahmen der Industrie 4.0 zu. Wichtig sei, das Thema Cybersicherheit in Europa zu organisieren. Die IT-Sicherheit sei ein entscheidender Faktor für die Zukunftsfähigkeit des Standortes Deutschland.

IuK-Kriminalität

Die jüngste Welle an **Sicherheitslücken und Hacker-Angriffen auf Banken** rufen nach einer Meldung der FAZ vom 30. Juni die internationalen Finanzaufseher auf den Plan. Die Bank für internationalen Zahlungsausgleich und die Vereinigung der internationalen Wertpapieraufsichtsbehörden Ioscos veröffentlichten einen Leitfaden, wie sich Banken und andere Finanzinstitute besser gegen Cyberrisiken wappnen können. Cyberabwehr solle Führungsaufgabe werden. Konkrete Abwehrpläne und effektive Sicherheitskontrollen seien weitere zentrale Vorgaben. Für Aufsehen habe der Cyberangriff auf die Zentralbank von Bangladesch gesorgt, bei dem Hacker im Februar 81 Mio. Dollar erbeutet hätten.

Nach einer Meldung von silicon.de vom 7. Juli rechnen 80 Prozent der europäischen IT-Sicherheitsspezialisten damit, dass ihr Unternehmen in den kommenden zwölf Monaten Ziel mindestens einer **DDoS-Attacke** und einer mit einhergehenden Lösegeldforderung werde. Zu diesem Ergebnis komme eine Umfrage des Sicherheitsanbieters Corero Network Security. Corero Network Security zufolge nehmen DDoS-Attacken mit einhergehender Lösegeldforderung seit Ende 2015 zu. Besorgniserregend sei, dass 43 Prozent der Befragten unter Umständen durchaus bereit wären, solch einer Forderung nachzukommen. Wenn eine Webseite nicht erreichbar ist, könne das ein Unternehmen mehr als 6.500 Dollar pro Minute kosten. Einer Warnung der britischen Polizei zufolge drohe die Hackergruppe Lizard Squad derzeit britischen Firmen mit DDoS-Angriffen, falls sie sich weigerten, fünf Bitcoin (umgerechnet 1.750 Euro) zu zahlen. Außerdem testeten die Angreifer die Systeme ihrer Opfer immer häufiger mit kurzen, deren Systeme nicht überlastenden DDoS-Attacken.

Wer dieser Tage eine E-Mail im Namen des Filehosting-Dienstes **WeTransfer** erhält, sollte die Nachricht genauestens unter die Lupe nehmen, berichtet heise.de am 5. Juli. Derzeit seien gezielt gefälschte E-Mails im Umlauf. Wer auf den Download-Link innerhalb der auf den ersten Blick legitim wirkenden Mail klicke, lade ein Zip-Archiv mit JavaScript-Dateien herunter. Öffne man eine davon nach dem Entpacken, fange man sich einen Computer-Schädling ein.

Der Behörden Spiegel berichtet in seiner Juli-Ausgabe über den Münchner Cyber Dialog zwischen Führungskräften und Experten. Thomas Seifert, Symantec, berichtete, sein Unternehmen registriere weltweit 2.000 Cyberangriffe pro Sekunde. Die Datenbank des Unternehmens ermögliche, fünf generelle aktuelle Trends zu erkennen: Erstens seien zielgerichtete Angriffe 2015 um 55 Prozent gestiegen. Ein zweiter Trend sei die Zunahme sogenannter Zero-Day-Attacken. Eine dritte Entwicklung sei die Verlagerung von Ransomware vom Konsumenten auf Unternehmen. Der vierte Trend: verseuchte Web-Seiten, die verstärkt für Angriffe genutzt würden. Weiterhin sei eine erhöhte Zahl an Cyberangriffen zu beobachten, die sehr hohe wirtschaftliche Schäden anrichten. Zum Thema „Bring Your Own Device" (BYOD) hielten es die Diskussionsteilnehmer für unerlässlich, dass die IT der Unternehmen die genutzten Endgeräte verwaltet und Zugriff auf die Geräte haben

müsse. Carsten Scholz, Allianz, betonte, dass Android aufgrund großer Sicherheitslücken im Prinzip nicht nutzbar sei. Für IT-Verantwortliche sei es bisweilen schwierig, gegenüber dem Vorstand Argumente für die Erhöhung des IT-Sicherheitsniveaus zu finden, denn IT-Sicherheit sei nicht messbar.

Dr. Klaus Gheri befasst sich am 19. Juli in silicon.de mit der Bedeutung von **Endpunkt-Sicherheit für IoT** (Internet of things)-Umgebungen. Eine unzureichende Verschlüsselung und schwache Authentifizierungsschemata seien die häufigsten Ursachen, die IoT-Geräte für Datendiebstähle anfällig machten. Ein moderner Geschäftsbetrieb verlange vernetzte Geräte, um den wirtschaftlichen und technologischen Anschluss nicht zu verlieren und auf jegliche Informationen und Veränderungen schnell reagieren zu können. Eine der größten Herausforderungen für Unternehmen sei es, alle Informationen an die zentrale Stelle zurückzumelden, ohne dass sie unbefugt abgeschöpft würden. Welcher Schaden durch den Angriff auf ein IoT-Gerät entstehen könne, zeigt der Autor am Gefahrenpotenzial für Windparks und für vernetzte industrielle Kühlanlagen. Tools für eine sichere und skalierfähige IoT-Verbindung sollten relativ klein und leicht integrierbar sein. Das größte Hindernis, um das IoT sicher zu machen, sei schlichtweg, dass es keine Generallösung gebe. Das Spektrum der IoT-fähigen Geräte reiche von Wearables über intelligente Glühbirnen bis hin zu industriellen Fertigungsmaschinen. Je nachdem, um was für ein IoT-Gerät es sich handelt, gebe es einen anderen wirtschaftlichen Ansatz. Die Aufgabe bestehe nun darin, für jeden einzelnen Anwendungsfall eine adäquate Sicherheitskonfiguration zu finden. Beinhaltet das IoT-Netzwerk Hunderte oder gar Tausende Geräte, sei es ein logistischer Kraftakt, jedes einzelne Gerät mit einer effektiven Security-Lösung auszustatten. Es gebe tatsächlich viele Anwendungsfälle für sichere, skalierfähige Schnittstellentechnologien. Bezüglich der Adaptierung werde die Technologie kleiner und kostengünstiger werden, dabei aber mehr Funktionalitäten bieten. Lösungen bräuchten beispielsweise eine zusätzliche Datenverkehrsüberwachung durch das Gerät selbst und die direkte Verbindung zum Internet. Der Trend der Miniaturisierung werde anhalten.

Deutschland ist nach Einschätzung des BKA-Präsidenten Holger Münch im internationalen Vergleich ein Hauptzielland für Kriminalität, die sich gegen Informationstechnik richtet oder mittels dieser begangen wird, berichtet die FAZ am 28. Juli. Zwar belaufe sich der polizeilich erfasste Gesamtschaden durch Internetkriminalität im Jahr 2015 auf „nur" 40,5 Mio. Euro, die Dunkelziffer sei aber sehr hoch. Der geschätzte tatsächliche Gesamtschaden betrage 1,6 Prozent des BSP. Vor allem die Industrie sei durch die fortschreitende Digitalisierung immer größeren Gefahren ausgesetzt. Er teile die Einschätzung des Chaos Computer Clubs, der davon gewarnt habe, die anonymen Bereiche des Internets zu dämonisieren. Das sogenannte **Darknet** sei wichtig für Personen, deren freie Meinungsäußerung durch staatliche Repressionen bedroht sei. Man dürfe aber das Darknet auch nicht verharmlosen. Derzeit seien Strafverfahren gegen 85 Personen anhängig, die im Verdacht stünden, im Darknet mit Waffen oder Sprengstoff gehandelt zu haben. Digitale Schwarzmärkte spielten eine immer größere Rolle. Sie bestünden nur temporär, um das Risiko, von Strafverfolgern entdeckt zu werden, zu minimieren. Im Darknet würden Waffen, Drogen, gestohlene Kreditkartendaten sowie Fälschungen aller Art angeboten. Zunehmend wichtiger werde auf dem digitalen Schwarzmarkt der Verkauf illegaler Dienstleistungen, die die Begehung jeder Art von Internetkriminalität erst ermöglichten. Beispiel: Erpressung mit der Androhung der Verschlüsselung oder Löschung von Daten. Allein in Deutschland hätten die Ermittlungsbehörden 2015 fünf solcher Schwarzmärkte ausgehoben. In der internationalen Zusammenarbeit seien es 30 gewesen. Das BKA erkenne eine zunehmende Verlagerung von Delikten aus der analogen

in die digitale Welt. Grund dafür sei nicht nur die mögliche Anonymität, sondern auch der Umstand, dass man ohne tiefergehende Computerkenntnisse ins Darknet gelangen könne. Versandt würden die Waren mit der Post, zumeist an Packstationen, bei denen sich die Empfänger mit gefälschten Ausweisen registriert hätten.

Wie Deutsche Inkerman Fraud Weekly in der Ausgabe 171 berichtet, hat das britische Statistikamt (ONS) zum ersten Mal Zahlen für Betrug durch Cyberkriminalität in seine Statistiken aufgenommen. In den zwölf Monaten bis März 2016 seien über zwei Mio. Straftaten durch Computermissbrauch und 3,8 Mio. Online-Betrugsdelikte erfasst worden. Andere Missbrauchsdelikte seien zu 68 Prozent Malware gewesen, während 32 aus Hacken oder unbefugtem Zugriff bestanden hätten. Die Zahlen des ONS ließen erkennen, dass die Methoden der Cyberkriminalität immer populärer würden und dass jedes Jahr einer von zehn Briten zum Opfer eines Cybervergehens werde.

Kartellrecht

„Neue Waffen gegen digitale Kartellsünder" titelt die FAZ am 1. Juli. Damit das Bundeskartellamt mit schärferen Waffen auf digitalen Märkten agieren kann, habe der Bundeswirtschaftsminister nun die 9. Novelle des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) auf den Weg gebracht. In der Novelle werde klargestellt , dass ein Markt im Sinne des Kartellrechts auch dann vorliegen kann, wenn zwischen den unmittelbar Beteiligten kein Geld fließt – wie etwa bei Suchmaschinen, Vergleichsportalen oder Informationsdiensten. Der Entwurf enthalte außerdem einen Katalog neuer, speziell auf digitale Märkte zugeschnittener Kriterien zur Beurteilung der Marktmacht von Unternehmen, die auf mehrseitigen Märkten oder in Netzwerken agieren. Dazu gehörten etwa Netzwerkeffekte, Größenvorteile sowie der Zugang zu Daten und das Innovationspotenzial. Die Fusionskontrolle solle künftig auf Fälle ausgeweitet werden, in denen ein Transaktionswert (Kaufpreis) bei mehr als 350 Mio. Euro liege und gleichzeitig das übernommene Unternehmen nur Umsätze von weniger als fünf Mio. Euro erwirtschaftet. Zweiter Kernpunkt der Novelle sei eine Verschärfung der Haftung für Bußgelder. Im Entwurf sei vorgesehen, dass Bußen nicht nur gegen die handelnde Gesellschaft, sondern auch gegen deren Mutterkonzern oder Rechtsnachfolger verhängt werden können.

Krankenhaussicherheit

Einbrecher drangen am 25. Juli in die Dill-Kliniken ein und entwendeten aus dem Krankenhaus in Dillenburg 18 medizinische Geräte, vor allem Endoskope, im Wert von 370.000 Euro, berichtet die FAZ am 28. Juli. Die Dill-Kliniken seien nicht der einzige Schauplatz groß angelegten Diebstahls von Behandlungs- und Diagnosetechnik. Erst wenige Tage vor diesem Einbruch hätte sich ein ähnlicher Fall in Görlitz ereignet, wo Diebe in das Malteser Krankenhaus St. Carolus eingedrungen seien. Dort sei ein Schaden in Höhe von rund 400.000 Euro entstanden, als die Täter unter anderem ein Ultraschallgeräte, Monitore und Untersuchungstürme gestohlen hätten. Diebstähle von medizinischem Gerät seien in den vergangenen Monaten in ganz Deutschland gehäuft aufgetreten. Ende Mai beispielsweise sei dem Universitätsklinikum Magdeburg ein Schaden von rund einer halben Mio. Euro durch den Diebstahl von neun Bronchoskopen entstanden. Besonders häufig hätten Diebe in Nordrhein-Westfalen zugeschlagen. Zuletzt seien dort unter anderem das Marienhospital Gelsenkirchen und das Marienkrankenhaus Bergisch Gladbach betroffen gewesen. In der Helios-Klinik Bad Berleburg wiederum seien personenbezogene Daten gestohlen worden.

Kritische Infrastrukturen

Wie heise.de am 24. Juli meldet, zieht das BSI ein Jahr nach Inkrafttreten des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme Bilanz. Demnach seien bislang sieben Meldungen wegen Cyberattacken eingegangen. Das Gesetz schreibt vor, dass bestimmte Unternehmen schwerwiegende Cyberattacken dem BSI melden müssen. Dazu gehören etwa Strom- und Wasserversorger, Telekom-Unternehmen oder Krankenhäuser. BITKOM gehe davon aus, dass bislang nicht alle meldepflichtigen Vorfälle an die Behörde weitergegeben worden sind, zumal das Gesetz nicht klar definiert habe, welche Branchen Angriffe melden müssen. Zudem seien die Meldewege noch nicht allen betroffenen Unternehmen und Einrichtungen bekannt.

Luftverkehrssicherheit

Dipl.-Wirtschaftsjurist Sebastian Brose, VdS, stellt in Ausgabe 2-2016 von s+s report, S. 42/43, ein **neues Zertifikat für Flughafen- und Liftsicherheitsdienstleister** vor. Er erläutert den Inhalt der DIN EN-Norm 16082 „Flughafen- und Luftsicherheitsdienstleistungen". Auf Kundenwunsch habe VdS die Richtlinien VdS 3108 erarbeitet. Sie regeln die Zertifizierung von Flughafen- und Luftsicherheitsdienstleistern nach der DIN-Norm und beschreiben das Verfahren.

Dirk Fischlein, Securitas Aviation, greift in Ausgabe 7/8-2016 der Zeitschrift PROTECTOR, S. 48/49, das Thema **Luftverkehrs- und Flughafensicherheit** auf. Am Leistungsangebot von Securitas, das mit rund 3.500 spezialisierten Mitarbeitern auf allen großen deutschen Flughäfen präsent sei und international mit rund 25.000 Einsatzkräften an rund 200 Flughäfen in 25 Ländern Luftsicherheit gewährleiste, werde die Bandbreite der Leistungen deutlich. Für die Luftsicherheit sei es keinesfalls relevant, ob die Kontrollen durch Angestellte des Bundes oder private Sicherheitsunternehmen vollzogen würden. Im Vordergrund stehe vielmehr die Zuverlässigkeit und Leistungsfähigkeit des Sicherheitsdienstleister. Um qualifizierte Passagier- und Gepäckkontrollen auch weiterhin zu gewährleisten, müssten insbesondere folgende Voraussetzungen erfüllt werden: Es sollten nur leistungsstarke Sicherheitsunternehmen beauftragt werden. Durch zügige Zuverlässigkeitsprüfungen müsse ausgeschlossen werden, dass unzuverlässige Personen eingesetzt werden. Es dürften nur Sicherheitsunternehmen beauftragt werden, die sicherstellen können, dass die einzusetzenden Kräfte qualifiziert sind. Bei der Vergabe von Aufträgen dürfe nicht der Preis, sondern müsse die Qualität entsprechend der DIN 77200 ausschlaggebend sein. Das Sicherheitsunternehmen müsste ein nachhaltiges Qualitätsmanagement nachweisen. Anders als die Luftverkehrssicherheit sei die Flughafensicherheit im allgemein zugänglichen Bereich derzeit eher kritisch zu betrachten. Hier sollten unter anderem Videoüberwachung mit intelligenter Analysesoftware und sofortige Interventionsmöglichkeiten, professionelle Verhaltensbeobachtung und nicht vorhersehbare Kontrollen im Außen- und Innenbereich der Terminals in Erwägung gezogen werden.

Museumssicherheit

Hans-Peter Büttner, Berater in Videoüberwachungstechnik, und Hans-Jürgen Harras, Staatliche Museen zu Berlin, behandeln im Video Security Special der Zeitschrift Sicherheitsforum, Juni 2016, S. 9-13, die Überwachung von musealen Objekten im Museum durch Videoüberwachung. Die Kameratechnik biete neben einer höheren Auflösung viele automatisierte Prozesse zu deren Einstellung und Inbetriebnahme. Ein Teil der Intelligenz, die ausschließlich in der analogen Video-

zentrale lokalisiert war, verlagere sich jetzt in die Kamera direkt. Damit ergäben sich neue Möglichkeiten zur Gestaltung von komplexen Videosystemen. Wegen der Bedingungen für die Videobildübertragung sowie zur Sicherheit sollte ein separates Netzwerk, möglichst auf LWL-Basis, genutzt werden. Videosensoren, die intelligente Videoanalyse, die vielfältigen Möglichkeiten zur Speicherung der Bilder sowie komplexe Steuerungs- und Auswertesysteme ermöglichten für die bisher mit Videotechnik in Museen und Ausstellungen gelösten Aufgaben eine beachtliche Qualifizierung. Die Autoren erläutern die schrittweise Umstellung auf IP, unterstützende Funktionen, Videosensoren und -bewegungsmelder, Detektion bei Entfernen von Gegenständen, Sicherung durch virtuelle Vorhänge, Gesichtserkennung und den Datenschutz und ziehen folgendes Fazit: Mit modernen digitalen Videosystemen und -kameras können Museen und Ausstellungen die ausgestellten Gegenstände gut überwachen. Es sind keine zusätzlichen Eingriffe oder Manipulationen an den ausgestellten Werken erforderlich. Durch den Einsatz von Videosensorik und Videoanalyse können unmittelbar auf unerwünschte Ereignisse folgende Alarmierungen ausgelöst werden.

Notfallmanagement

Andreas Deliandreadis, Everbridge Deutschland, thematisiert in der Ausgabe 7/8-2016 der Fachzeitschrift PROTECTOR, S. 24/25, die **Notfallkommunikation nach einem Cyberangriff**. Die Anzahl der Unternehmen, die DDoS-Angriffe melden, verdoppele sich von Jahr zu Jahr. Für Unternehmen sei es dringend erforderlich, über einen ausgearbeiteten Krisenplan zu verfügen, der Antworten auf folge Fragen gibt: Welche Maßnahmen sind im Fall eines DDoS-Angriffs zu ergreifen? Wie lässt sich effektiv mit Mitarbeitern und Kunden kommunizieren, wenn die internen Kommunikationssysteme ausgefallen sind?

In einer jüngeren Erhebung von Business Continuity Institutes (BCI) seien 467 Teilnehmer in 67 Ländern nach ihren Notfallkommunikationsplänen befragt worden. Von den Unternehmen, die über keinen Notfallkommunikationsplan verfügten, hätten erstaunliche 68 Prozent angegeben, sie würden einen Notfallkommunikationsplan erst entwickeln, nachdem ein Ereignis eingetreten sei, das sich auf den Geschäftsbetrieb auswirke. Diese Haltung könne sich als verhängnisvoll erweisen. Nur 55 Prozent der vom BCI befragten Organisationen verfügten über eine eigene Notfallkommunikations-Software. Um zu gewährleisten, dass bei einem partiellen Systemausfall Botschaften an die richtigen Empfänger gelangen, müsse die Notfallkommunikationsplattform des Unternehmens von seinem normalen Netzwerk vollständig getrennt sein. Die Nutzung einer cloudbasierten Software-as-a-Service-Plattform sei die einzig effektive Möglichkeit, die Kontinuität der Kommunikation zu gewährleisten. Wichtig sei, dass die richtige Botschaft zum richtigen Empfänger gelangt und ihre Zustellung bestätigt werden muss. Nur cloudbasierte Tools böten Unternehmen die Möglichkeit, alle relevanten Beteiligten schnell zu informieren.

Perimeterschutz

PROTECTOR erläutert in der Ausgabe 7/8-2016, S. 26/27, die Funktion von **Schnellfalttoren**. Ein Unternehmen habe eine Gleistoranlage gesucht, die im Hinblick auf die Geschwindigkeit der ein- und ausfahrenden Züge eine möglichst hohe Öffnungs- und Schließgeschwindigkeit bietet. Die Wahl sei schließlich auf das gemäß DIN EN 13241-1 TÜV-baumeistergeprüfte Entraquick II Schnellfalttor gefallen. Das freitragende Schnellfalttor komme ohne störende Ober- oder Unterholmführung aus und biete hindernisfreie Sicherheit in jeder Ein- oder Ausfahrsituation.Risikomanagement

Prof. Volker Stein und Prof. Arnd Wiedemann, beide Universität Gießen, befassen sich in einem Bei- trag in der FAZ vom 4. Juli mit **Risikomanagement und** mit **Risk Government**. Größere Unternehmen verfügten in der Regel über eine Risikomanagementfunktion mit klar umrissenen Aufgaben. Besonders die relevanten Risiken, also die mit großem Einfluss auf den Unternehmenswert, würden auf der Basis von Standardisierungsvorschriften (ISO, OECD, Branchenverbände) gemessen, bewertet, mit der Risikotragfähigkeit des Unternehmens abgeglichen und im Hinblick auf das Risiko/Ertragsverhältnis optimiert. Das Risikomanagement verbreitere sich zunehmend von der Abbildung finanzieller Risiken auf allgemeine Managementrisiken und wolle auch strategischen Ansprüchen genügen. Dennoch sei grundsätzliche Kritik angebracht: Bezogen auf das Gesamtunternehmen agiere das Risikomanagement zu mechanistisch, weil es standardisierte Risikomodelle und Risikomanagementprozesse auf vorselektierte Standardrisiken anwende. Im Rahmen ihrer Überwachungsfunktion könne die interne Revision Defizite zwar aufdecken, aber nicht selbst bewältigen. Gesucht sei daher eine Risikosteuerung, die auch eine übergeordnete Regelungsebene einschließe. Die Corporate Governance sei ein solcher Regelungsrahmen, der aus einer anderen Richtung Risiken von und in Unternehmen in den Blick nehme. Als Reaktion auf die Finanzkrise 2008 sei die Forderung nach einem ganzheitlichen Risikomanagement aufgekommen, das sich auf Risiken in der Unternehmensführung spezialisiere. Der Kniff von Enterprise-Risk-Management (ERM) bestehe darin, dem traditionellen Risikomanagement „Governance" hinzuzufügen, also die Risikomanagementfunktion selbst besser zu steuern. „Risikokultur" tauche vermehrt als modisches Schlagwort auf. Mit ihrer Hilfe sollten Normen gesetzt werden, die Einstellung und Verhalten von Unternehmen zu Risikoentscheidungen und Risikomanagement beeinflussen, ergänzt um eine wertbezogene Risikokommunikation und entsprechende Anreizstrukturen. Aber wie oft schon ist eine nicht gelebte Kultur im Nirwana des Unverbindlichen verschwunden. Die nachhaltige Lösung liege zwischen Corporate Governance und Risikomanagement und heiße Risk Government. Risk Governance sei erstens eine Philosophie. Im Kern strebe sie eine proaktive Risikosteuerung von innen heraus an. Als Katalysator für Themen der Risikosteuerung „mit Biss" brauche sie eine Stimme nach oben in die Unternehmensleitung sowie Durchsetzungskompetenz in alle anderen betrieblichen Funktionen. Risk Governance sei zweitens ein Bündel aus vier konkreten Aufgaben: Zunächst gehe es um das Design von Risikomodellen, also um die laufende (Neu-) Festlegung der Art der Risikowahrnehmung, -priorisierung und -aggregation vor dem Hintergrund der spezifischen Stakeholderbedingungen. Hinzu komme die Bestimmung der Modellrisiken als systematisches Ausschließen fehlerbehafteter Risikomodelle und permanentes Rekontextualisieren der Risikosteuerung. Risk Governance sei drittens eine wertschöpfende Unternehmensfunktion. Risk Governance sei schließlich mehr denn je strategische Notwendigkeit. Sie sei entscheidend für die Sicherung und Verbesserung der inneren Substanz eines Unternehmens und funktioniere wie ein Schutzschirm für das Unternehmen vor sich ändernden Risiken.

Schließsysteme

PROTECTOR stellt in der Ausgabe 7/8-2016, S.16/17, eine mechatronische Schließanlage vor. Die große Menge an unterschiedlichen Nutzern öffentlicher Gebäude erhöhe das Sicherheitsrisiko. Hier seien außerdem IT-Systeme gefragt, die ohne Probleme in bestehende Anlagen integriert werden könnten und multifunktional erweiterbar seien. Mit modernen Chipausweisen sei das möglich. Sie sorgten nicht nur für eine sichere Begehung der Räumlichkeiten, sondern verschlankten auch den Verwaltungsaufwand. Das Hochbauamt habe sich im konkreten Fall für eine

mechatronische Schließanlage entschieden. In den mechatronischen Zylinder sei eine intelligente Datenverschlüsselung integriert. Eingesetzt worden sei auch eine neue und moderne vernetzte Fluchtwegsteuerung von Assa Abloy Sicherheitstechnik. Sie koppele die automatische Steuerung der Türtechnik mit der Sicherheitsfunktion der Notausgangsverriegelung.

Stadionsicherheit

PROTECTOR berichtet in der Ausgabe 7/8-2016, S. 20, über die grundlegende Modernisierung der Videoanlage eines Stadions. Das eingesetzte Dallmeier Security Management System Semsy nutze eine virtuelle Matrix, also eine netzwerkbasierte Technologie. Die virtuelle Matrix ermögliche es, flexible Monitorwände zur Anzeige der Kamerabilder in verschiedenen Formaten zu errichten. Die Bediener könnten ihre Bildschirme beliebig konfigurieren, außerdem könnten Remote-Zugriffe und zusätzliche Nutzer eingerichtet werden. Mit Semsy und den Encodern sowie Video-Appliances von Dallmeier hätten die 96 im Stadion installierten analogen Kameras „wiederbelebt" und gleichzeitig der Kontrollraum mit einer modernen Plattform ausgestattet werden können. Werde aus Kosten- oder aus Sicherheitsgründen ein Austausch der bestehenden analogen Kameras und die Einführung neuer IP-HD-Technologie erforderlich, sei dies nun problemlos und ganz einfach zu realisieren. Außerdem seien die zunehmenden Probleme durch Bengalos, Rauchbomben und dissoziales Verhalten in den Gäste-Fanblöcken in Angriff genommen worden. Aus diesem Grund sei die Multifocal-Sensortechnologie **Panomera** von Dallmeier speziell für den Gäste-Fanbereich des Stadions getestet worden. Keine andere Technologie auf dem Markt der Multifocal-Sensortechnologie habe Panomera „das Wasser reichen können".

Terrorismus

In der Wochenlage am 22. Juli nimmt das BKA zu den Auswirkungen der **Amokfahrt in Nizza** Stellung. Es seien 84 Menschen getötet und mehr als 300 verletzt worden. Der Täter sei tunesischer Staatsangehöriger gewesen. Sollte sich eine islamistische Motivation bestätigen, belege der Anschlag in Nizza die Einschätzungen der Bundessicherheitsbehörden, dass auch Anschläge durch Einzeltäter und Nutzung von einfach zu beschaffenden Tatmitteln zu befürchten seien. Der Anschlag habe bislang keine Auswirkungen auf die Gefährdungslage in Deutschland. Es bestehe weiterhin eine hohe, aber abstrakte Gefahr dschihadistisch motivierter Gewalttäter.

Am 18. Juli griff ein 17-jähriger afghanischer Staatsangehöriger mehrere Fahrgäste in einem fahrenden **Regionalzug bei Würzburg** mit einer Axt und einem Messer an, meldet das BKA in der Wochenlage vom 22. Juli. Vier Reisende seien schwer verletzt worden. Auf seiner Flucht verletzte der Täter eine Fußgängerin schwer. Das Attentat stelle den ersten Anschlag in Deutschland dar, zu dem sich der IS bekannt habe. Mit der Veröffentlichung des Tätervideos habe der IS die Gewalttat propagandistisch genutzt. In der Gesamtbetrachtung unterstreiche der Vorfall nachhaltig die bestehende Gefährdungslage aus dem Phänomenbereich des islamistischen Terrorismus. Deutschland werde von terroristischen Organisationen als Gegner wahrgenommen und stehe weiterhin in deren erklärtem Zielspektrum. Dementsprechend bestehe für Deutschland eine anhaltend hohe Gefahr dschihadistisch motivierter Gewalttaten durch Einzeltäter, autonom agierenden Gruppen wie auch terroristische Organisationen, insbesondere durch den IS und dessen Sympathisanten. Der Vorfall zeige, dass bei islamistisch motivierten Taten grundsätzlich die gesamte Bandbreite möglicher Begehungsweisen einzukalkulieren sei und zunehmend „weiche"

Ziele in die direkte Auswahl genommen würden. Tatimpulse könnten beliebige Ereignisse, Äußerungen oder Handlungen und dschihadistische Internetpropaganda sein.

Der bayerische Innenminister Joachim Herrmann berichtete nach einer Meldung der FAZ vom 28. Juli von einem Chatverlauf, der belege, dass jemand mit dem Ansbacher Attentäter Mohammad C. unmittelbar vor der Zündung der Bombe in Ansbach in Verbindung gestanden habe. Im Internet sei ein Nachruf auf den Täter veröffentlicht, den der „Islamische Staat" (IS) verfasst haben soll. Der Täter sei in Syrien für den IS auf den Bau von Bomben spezialisiert gewesen und habe sich später zu einem Anschlag in Deutschland entschlossen.

Türkei

In der Wochenlage des BKA vom 22. Juli wird die Sicherheitslage nach dem Putschversuch in der Türkei dargestellt. In mehr als 40 deutschen Städten sei es zu spontanen Versammlungen und Aufzügen gekommen. Da sich die Lage in der Türkei weitgehend stabilisiert habe, sei davon auszugehen, dass die Zahl der Versammlungen in Deutschland rückläufig sein werde.

Veranstaltungssicherheit

Jede Großveranstaltung stelle ihre eigenen Anforderungen an die Verantwortlichen, das Risiko eines Schadens für die Teilnehmer so gering wie möglich zu halten, argumentiert PROTECTOR in der Ausgabe 7/8-2016, S. 14–16. Eine seit einigen Jahren gängige Möglichkeit, das tolerierbare Risiko zu bestimmen, sei die Verwendung von Simulationen. Je genauer die Grunddaten sind, mit denen die Simulation angereichert wird, desto besser und realitätsnäher werde das Ergebnis. Dies beinhalte auch das Verhalten der „Agenten", die virtuellen Personen, die sich in einer Simulation nach festgelegten Parametern bewegen. Moderne Simulationen könnten mittlerweise auch nicht lineares Verhalten von Agenten abbilden, was bedeute, dass sich diese nicht einfach automatisch zielgerichtet auf definierte Ausgänge gleichmäßig hin bewegten.

Verfassungsschutz

Die FAZ berichtet am 29. Juni über den am 28. Juni veröffentlichten **Verfassungsschutzbericht 2015**. Politisch motivierte extremistische Gewalt habe in Deutschland 2015 massiv zugenommen und neue Dimensionen im Internet erreicht. Das BfV spreche vor allem von einem „drastischen Anstieg" rechtsextremistisch motivierter Gewalttaten – sie seien um mehr als 42 Prozent auf 1.408 Fälle angestiegen. Zudem habe es einen starken Anstieg linksextremistischer Gewalt gegeben; diese Taten seien auf 1.608 gestiegen, davon fast zwei Drittel „Gewalt gegen Polizei und Sicherheitsbehörden".
Im rechtsextremistischen Spektrum sei die politisch motivierte Kriminalität insgesamt auf fast 22.000 Fälle – von rund 16.600 im Jahr 2014 – gestiegen. Die fremdenfeindlichen Gewalttaten hätten sich dabei fast verdoppelt (von 512 auf 918 Fälle). Vor allem die Straf- und Gewalttaten gegen Asylbewerberunterkünfte seien dramatisch angestiegen. Während 2014 insgesamt 170 Straftaten (darunter 25 Gewalttaten) registriert wurden, waren es 2015 mehr als fünf Mal so viele: 894 Straftaten, darunter 153 Gewalttaten. Die Zahl rechtsextremistisch motivierter Brandanschläge gegen Flüchtlingsunterkünfte sei von fünf auf 75 Fälle angestiegen. Zur Bedrohung durch islamistischen Terror habe der Verfassungsschutz mitgeteilt, es gebe einen „ungebrochenen Zulauf" für islamistische Gruppierungen in Deutschland: besonders stark gestiegen seien die Anhängerzahlen des Salasfismus (von 7.000 auf 8.350).

Vermögensabschöpfung

Das BKA befasst sich in der Wochenlage vom 22. Juli mit der strafrechtlichen Vermögensabschöpfung. Mit einer **Reform der strafrechtlichen Vermögensabschöpfung** wolle die Bundesregierung die Entschädigung von Verbrechensopfern erleichtern. Ein am 13. Juli vom Kabinett verabschiedeten Gesetzentwurf solle dafür sorgen, dass Gerichte und Staatsanwaltschaften durch kriminelle Handlungen erlangtes Vermögen wirksamer einziehen können. Im Mittelpunkt der Reform stehe eine deutliche Vereinfachung der bislang äußerst aufwändigen Entschädigung von Verbrechensopfern. Die vorläufige Sicherstellung von rechtswidrig erlangten Wertgegenständen werde erleichtert. Zudem könnten Vermögenswerte künftig auch nachträglich abgeschöpft werden. Der Staat erhalte nach dem Entwurf Zugriff auf Vermögen unklarer Herkunft. Bestünden keine vernünftigen Zweifel daran, dass Vermögen aus kriminellen Handlungen herrühre, könne es nunmehr auch dann eingezogen werden, wenn die konkrete Straftat, aus der es stammt, nicht nachgewiesen werden könne. Bei konsequenter Anwendung der neu geschaffenen Rechtsinstrumente sollte die Zahl der vorläufigen Sicherungsmaßnahmen und der gerichtlichen Einziehungsentscheidungen deutlich steigen.

Verschlüsselung

Der Behörden Spiegel befasst sich in der Juli-Ausgabe mit der von der Deutschen Telekom und dem Fraunhofer Institut für Sichere Informationstechnologie angebotenen **Ende-zu-Ende-Versschlüsselung**. Der Beauftragte der Bundesregierung für Informationstechnik, Staatssekretär Vitt, begrüßt das neue Angebot zur kostenfreien und nutzerorientierten Ende-zu-Ende-Verschlüsselung durch die Deutsche Telekom als einen wichtigen Beitrag für Deutschland als Verschlüsselungsstandort. Das Programm könne mit dem Internet Explorer von Microsoft, Google Chrome und Mozilla Firefox genutzt werden. Ein Ausbau des Angebots für die Betriebssysteme MacOS, iOS und Android sei geplant, sodass die Verschlüsselungslösung auch auf mobilen Endgeräten genutzt werden könne.

Videoüberwachung

Die FAZ stellt am 1. Juli die **Alarmanlage Arlo von Netgear** vor. Die Arlo-Kameras weisen etliche Besonderheiten auf. Sie lassen sich einzeln verwenden oder als maximal 15 Stück zählende Gruppe. Die Optik im Plastikgehäuse sei wasser- und staubgeschützt nach der Schutzklasse IP, lasse sich also draußen anbringen, benötige kein Stromkabel, sondern Batterien und funke ihr Bild per WLAN zur Alarmzentrale. Die ovale Kamera habe vorn ihr optisches Auge samt Bewegungsmelder, im Gehäuseinnern seien 4 CR 123-Einwegfotobatterien einzusetzen, die im laufenden Betrieb zwischen vier und sechs Monaten halten sollen. Zehn Stück würden 15 Euro kosten. Ein LAN-Kabel verbinde die Kamera mit dem Router. Sie habe ein externes Netzteil, und es dürfen maximal 90 Meter zwischen ihr und den einzelnen Kameraaugen liegen. Das „Sahnehäubchen" seien die Optionen für die Konfiguration des Alarmsystems. Hinweise auf eine Bewegung im Blickfeld der Kamera würden per E-Mail oder Push-Nachricht zugestellt. Die Kameras ließen sich benennen, ihre Erkennungsgenauigkeit sei einstellbar und die Aufnahmelänge des Videos ebenfalls. Innovativ sei jedoch die Option, das Smartphone und einen Geozaun zum Scharfstellen oder Ausschalten verwenden zu können.

Jörg Schulz, von zur Mühlen'sche GmbH, thematisiert im Video Security Special des Sicherheitsforum (Juni 2016, S. 6–9) die Entwicklung der Videotechnik. Die

Videosensorik bringe Kameras an ihre Grenzen. Insbesondere Kombinationen von gleichzeitiger Maximalauflösung und Maximal-Bildwiederholrate und im weiteren intelligente Videosensorik würden ein System an seine Grenzen bringen. Problematisch werde es an den Knotenpunkten, wo auf einmal viele Videostreams zusammengeführt werden müssen. Hier müsse hoch performante aktive Technik vorhanden sein, die die Daten dann auf ebenso hoch performanten Backbone-Strukturen zu Speicher- und Anzeigesystemen schickt. An zentraler Stelle der skizzierten Kette stehe das Server- und Speichersystem. Dieses habe die Aufgabe, die Daten so vorzuhalten, dass eine Bildrecherche auch mit vernünftigen Reaktions- und Bearbeitungszeiten durchgeführt werden könne. Je größer die Datenflut, desto höher sei der Aufwand, der für Speicher- und Recherchefunktionen durchzuführen ist. Ein weiterer wichtiger Grundsatz sei, dass Videosysteme nicht nach dem maximal am Markt verfügbaren technischen Möglichkeiten auszulegen sind, sondern immer getreu der Überwachungsaufgabe und den Schutzzielen.

HTL Ing. Elektrotechnik, Guido Simak, Simak Consulting, erläutert im Video Security Special der Zeitschrift Sicherheitsforum, Juni 2016, S. 15–17, die Video Security Norm EN 50132-7. Sie sei eine Norm für Praktiker. Sie unterstütze Betreiber, Errichter und Benutzer einer Video Security-Anlage bei der Aufstellung ihrer Anforderungen sowie die Planer bei der Festlegung von geeigneten Anlagenteilen. Die Norm stelle aber auch Mittel für die objektive Bewertung einer Videoanlage zur Verfügung. Der Autor thematisiert die Leistungsbeschreibung, die Definition des Prüfplans, die in der Norm geregelten Verantwortlichkeiten und technische Besonderheiten. In der Norm sei der gesamte Prozess zur Errichtung einer Videoüberwachungsanlage, beginnend mit der Idee bis zur Übernahme und Wartung der Anlage, abgebildet. Die Norm richte sich an Auftraggeber, Fachplaner und Facherrichter und regele die Verantwortlichkeiten. Die Norm folge dem Prozess der Errichtung einer Videoanlage und biete für alle Prozessschritte fein aufeinander abgestimmte Methoden, wenngleich die verwendeten Begriffe nicht immer optimal gewählt seien.

Eidg. dipl. Telematik-Engineer Giray Aybet, Bosch Sicherheitssysteme, befasst sich im Video Security Special des Sicherheitsforums, Juni 2016, S. 24–27, mit der **mobilen Video-Übertragung**. Die Netzwerke müssten stetig steigende Auflösungen, höhere Frameraten und mehr Metadaten übertragen. Der Autor geht der Frage nach, wie das Übertragungsproblem lösbar ist. IT-Abteilungen möchten so wenig wie möglich Schnittstellen in ihren Netzwerken haben. Seit kurzem ermögliche das Dynamic Transcoding von Bosch das Streaming von Livevideos wie auch bei Bedarf den sofortigen Zugriff auf HD-Bilder selbst dann, wenn die Bandbreite dazu eigentlich nicht ausreichend ist. Dynamic Transcoding verwende einen intelligenten Algorithmus, der hochauflösende Videostreams ohne Qualitätsverlust an die verfügbare Bandbreite anpasse. Der dynamischen Transcodierung gehöre die Zukunft. Die geringere Auflösung des mobil übertragenen Bildes werde für den Benutzer unmerklich nach Bedarf durch die laufend nachladenden HD-Informationen ergänzt. Der eigentliche Kunstgriff dabei sei, dass die durch die drahtlose Übertragung limitierte Auflösung laufend so ergänzt wird, dass der Nutzer nichts von der Limitierung merkt. Die Frage, ob mobile Video-Übertragung und hohe Qualität ein Gegensatz sei, könne heute dank **Dynamic Transcoding** ganz klar mit „nein" beantwortet werden.

Mit intelligenter Videotechnik befasst sich Edi Lehmann, Siemens Building Technologies, im Video Security-Special der Zeitschrift Sicherheitsforum, Juni 2016, S. 28-31. Moderne Videomanagementsysteme gingen weit über die Aufzeichnung von Videobildern hinaus. Intelligente Algorithmen würden automatisch

Ereignisse erkennen und Metadaten sammeln, deren Auswertung riesiges Potenzial berge und das Sicherheitspersonal entlaste. Im Zusammenspiel mit Gefahrenmelde- und Sicherheitstechniken gestatte die Videotechnik eine umfassende Lagebeurteilung. **Intelligente Videomanagementsysteme** (VMS) unterstützten die Betriebsabläufe und arbeiteten Hand in Hand mit anderen Systemen. VMS hätten sich über die letzten Jahre enorm gewandelt und böten heutzutage zahlreiche Funktionalitäten – nicht zuletzt auch wegen der IP-Technologie. Das Siemens Network Video Recording (SiNVR) sei ein solch intelligentes Videomanagement für die Verwaltung, Archivierung und Anzeige von Videosignalen. Dank seiner offenen Systemarchitektur könne es alle IP-Kameras der führenden Hersteller integrieren. Mit SiNVR bestehe die Möglichkeit, ein komplexes und zugleich leicht zu wartendes VMS aufzubauen. Die Erstellung von interaktiven Lageplänen gelte als aufwendigster Teil eines VMS. Das Besondere an dieser Lösung sei, dass sie über ein eigenes Geoinformationssystem verfügt und daher unbefugte Personen und sonstige Störvorfälle auf den Meter genau identifiziert werden könnten. Auf Basis von geografischen Daten werde eine dynamische Darstellung und Bedienung der Kameras und Melder möglich. SiNVR sei offen und habe Schnittstellen zu Fremdsystemen. Somit könnten weitere Gewerke in der Sicherheitstechnik wie Zutrittskontrolle, Einbruch-, Brand- oder Evakuierungsanlagen in das System eingebunden werden.

Im Video Security Special der Zeitschrift Sicherheitsforum (Ausgabe Juni 2016, S. 32–51) präsentieren Unternehmen ihr Leistungsportfolio in der Videoüberwachungstechnik. Sie schätzen den Markt ein und stellen den Stand der Technik dar. Die Algorithmen der Videoanalyse würden in Zukunft so gut sein, dass auffällige Verhaltensmuster und „bekannte" Gesichter, sei es im Museum, sei es auf öffentlichen Plätzen oder im Luxusgeschäft, automatisch erkannt werden. Das erlaube neue Möglichkeiten für die Anwendung der Videotechnik.

Whistleblowing

Ontarios Wertpapieraufsicht „Ontarios Securities Commission" (OSC) hat nach einer Meldung von „Deutsche Inkerman Fraud Weekly" in der Ausgabe 170 das erste bezahlte Whistleblower-Programm Kanadas ins Leben gerufen. Im Rahmen des Programms biete die OSC Belohnungen von bis zu fünf Mio. kanadische Dollar (CAD) für Hinweise an, die zu einer erfolgreichen Strafverfolgung und Geldstrafe von mindestens 1,5 Mio. CAD führen. Die Tipp gebenden Personen könnten zwischen fünf und 15 Prozent der auferlegten Strafen erhalten. Das Maximum werde auf fünf Mio. CAD angehoben, wenn es der Wertpapierbehörde gelingt, im Zusammenhang mit dem Fall Strafen von mindestens zehn Mio. CAD einzukassieren.

Wohnungseinbruch

Die Soziologin M.A. Gina Rosa Wollinger und der Dipl.-Soziologe Arne Dreißigacker stellen in der Ausgabe 2-2016 von s+s report, S. 35–37, die Ergebnisse eines dreijährigen Forschungsprojekts des Kriminologischen Forschungsinstituts Niedersachsen e. V. vor, einer **Opferbefragung** zu Tatmerkmalen, der Situation der Opfer und ihre Erfahrungen mit der Versicherung sowie erste Hinweise zu wirksamen Präventionsaspekten. Die meisten Einbrüche würden tagsüber begangen. Die Urlaubsmonate im Sommer seien am niedrigsten belastet. Bei der Hälfte der untersuchten vollendeten Einbruchsfälle habe der Schaden durch gestohlene Gegenstände 2.500 Euro betragen. Bei der anderen Hälfte sei ein höherer Schaden entstanden. Am häufigsten würden Schmuck und Uhren sowie Bargeld gestohlen. Ein ebenfalls beliebtes

Stehlgut seien elektronische Kleingeräte und EDV-Geräte. In den meisten Fällen seien persönliche Bereiche durchwühlt und Kleidungsstücke herausgerissen worden. In nur 4,2 Prozent der untersuchten Fälle sei es zu einem direkten Kontakt zwischen Opfer und Täter gekommen. Noch Monate nach der Tat hätten 46,5 Prozent der Opfer angegeben, sich unsicher in der gewohnten Umgebung zu fühlen. Die meisten Opfer hätten nach dem Wohnungseinbruch ein erhöhtes Präventionsverhalten gezeigt. Nach der Tat würden vom Opfer vermehrt Beratungsmöglichkeiten genutzt, Angebote von Fachgeschäften und Versicherungen aber selten angenommen. 72,5 Prozent der Befragten hätten vor der Tat keine zusätzliche Sicherheitstechnik eingesetzt. Nach der Tat habe dies nur auf 36,2 Prozent der Befragten zugetroffen. 74,5 Prozent der Opfer seien zum Zeitpunkt der Tat durch eine Hausratversicherung versichert gewesen. 29,4 Prozent hätten nach der Tat eine Hausratsversicherung abgeschlossen. Bei der Hälfte der versicherten Opfer sei der Schaden in voller Höhe ersetzt worden, bei weiteren 43,6 Prozent habe eine teilweise Erstattung stattgefunden. 79,4 Prozent der Befragten hätten angegeben, dass ihnen der weitere Schaden, der an der Einbruchstelle oder durch Verwüstungen entstanden sei, in voller Höhe ersetzt worden sei. Es habe sich gezeigt, dass bei Betroffenen, die vor der Tat eine Präventionsberatung durch ein Fachgeschäft genutzt hatten, der Einbruchversuch deutlich häufiger misslang.

Zutrittskontrolle

Sensorschleusen thematisiert PROTECTOR in der Ausgabe 7/8-2016, S. 18/19. Um die Anforderungen der Norm ISO 27001:2013 zu erfüllen, sei der Einsatz einer Kontrollschleuse der richtige Weg. Die Slimlane Doppelflügel-Sensorschleusen zeichneten sich durch ein transparentes, elegantes Design aus. Die Türen seien im Ruhezustand nicht verriegelt und bei Stromausfall frei beweglich. Im sogenannten Egress-Modus löse die Bremse nach einer Kraft von weniger als 220 Newton gemäß EN 1125, wodurch sich die Türen in Fluchtrichtung öffnen. Parallel dazu werde mit einem Signal und einer Signalleuchte auf eine Evakuierung hingewiesen. Im Gegensatz dazu trete bei einem gewaltsamen Öffnungsversuch in Eingangsrichtung eine elektromechanische Verriegelung in Kraft, bei der die Bremsen des Systems automatisch anziehen und den unberechtigten Zugang verhinderten. Die Türen öffneten in weniger als einer Sekunde, sodass bis zu 60 Personen in der Minute passieren könnten. Dies stelle besonders zu Arbeitsbeginn einen erheblichen Vorteil dar und reduziere lange Wartezeiten auf ein Minimum.

Impressum

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

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

Herausgeber:
Manfred Buhl, Vorsitzender der Geschäftsführung, Düsseldorf

Verantwortlicher Redakteur:
Bernd Weiler, Leiter Kommunikation und Marketing

Beratender Redakteur:
Reinhard Rupprecht, Bonn

focus.securitas.de

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

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

E-Mail: info@securitas.de