Focus on Security

Ausgabe 10, Oktober 2015

SECURITAS

Inhalt

Arbeitsschutz

Mit dem richtigen **Gehörschutz** befasst sich die Fachzeitschrift GIT in der Ausgabe 9-2015, S. 118/119. Die Deutsche Gesetzliche Unfallversicherung (DGUV) führe in ihrer Regel „Benutzung von Gehörschutz" vom Januar 2015 vier verschiedene Methoden zur Ermittlung des richtigen Gehörschutzes auf: die „Oktavband"-Methode sollte angewendet werden, wenn im Einzelfall die Schutzwirkung möglichst genau zu bestimmen ist; die HML-Methode mit ihren drei für jeden Gehörschützertyp angegebenen Dämmwerten für hohe, mittlere und tiefe Frequenzen; der HML-Check, eine Kurzform der HML-Methode; und die SNR-Methode, die einen einzigen Dämmwert verwendet. Generell unterscheide man zwei verschiedene Gehörschutzvarianten, die je nach Arbeitssituation und -umgebung ihre Vorteile haben: Gehörschutzstöpsel eigneten sich insbesondere für Arbeitsumgebungen mit hohen Temperaturen, bei langer Tragedauer, wechselnder Belegschaft sowie in Kombination mit anderer persönlicher Schutzausrüstung. Kapselgehörschützer eigneten sich besonders zum Einsatz bei schmutzigen Arbeitsbedingungen. Sie seien für Menschen mit druckempfindlichem Gehörgang eine Alternative zu Gehörschutzstöpseln und sorgten zudem für den Schutz der Ohren bei niedrigen Temperaturen.

Brandschutz

Mit **Brandmeldungs-Technologie** befasst sich Dipl.-Ing. ETH Roger Gorlero, Bosch Sicherheitssysteme, in der Zeitschrift Sicherheitsforum (Ausgabe 4-2015, S. 24–26). Die Falschalarmhäufigkeit habe man durch die Zweimelder-Abhängigkeit reduziert, dadurch aber die Ansprechgeschwindigkeit massiv verschlechtert. Diese sei durch Multisensormelder (Streulichtsensor, Temperatursensor und Kohlenmonoxidsensor) erheblich erhöht worden. Ein weiterer Optimierungsschritt sei die Einführung der Detektionsalgorithmen gewesen. Heute biete sich noch eine weitere wesentliche Möglichkeit, die Detektionsleistung zu verbessern: Der Einsatz einer zusätzlichen blauen LED verbessere das Detektionsverhalten bei offenen Flammenbränden deutlich. Insbesondere langsam anlaufende Flammenbrände würden wesentlich besser detektiert, da das blaue Licht durch die kleinen Aerosole, die bei offenen Bränden entstehen, besser gestreut werde.

s+s report weist in der Ausgabe 3-2015 auf ein neues Merkblatt der Vereinigung zur Förderung des Deutschen Brandschutzes e. V. (vfdb) zur **Planung von Brandschutzanlagen** hin. Das in ihm veröffentlichte Ablaufdiagramm zeige die notwendigen Arbeitsschritte zur Erfüllung unterschiedlicher Schutzziele in ihrer empfohlenen Reihenfolge und Verknüpfung (S. 6).

Dr. Mingyi Wang, GDV, befasst sich in s+s report (Ausgabe 3-2015, S. 14/15) mit der Richtlinie **VdS 3110.** Diese richte sich an den Brandschutzbeauftragten und enthalte ergänzende Hinweise zu Verantwortung und Hilfestellung zur Beurteilung von Brandgefahren und der Überprüfung von Brandschutzmaßnahmen. Neben dem Leitfaden zum Brandschutz im Betrieb (VdS 2000) habe der GDV zahlreiche weitere unverbindliche Empfehlungen erarbeitet, die im VdS-Verlag veröffentlicht werden.

Feuerschutzabschlüsse im Zuge bahngebundener Förderanlagen (FAA) thematisiert Torsten Pfeiffer, VdS Schadenverhütung, in der Ausgabe 3-2015 von s+s report (S. 26–31). Er gibt einen Überblick über den Aufbau von FAA (Feuerschutzabschluss, Feststellanlage, Freifahren, Gefällestrecke, Freiräumen, Einquetschen, Zerdrücken, Energieversorgung) und vor allem über Sicherheitseinrichtungen der Feststellanlage, die einen eingeleiteten Schließvorgang verzögern oder unterbrechen, wenn sich Personen oder

Gegenstände im Sicherheitsbereich des Abschlusses befinden. Er gibt ferner Hinweise zur Abnahme von FAA, erklärt die bauseitigen Voraussetzungen für die Abnahme, erläutert die Abnahme des Einbaus der Feststellanlage und der Freifahr- bzw. Freiräumeinrichtung und der Funktion des Gesamtsystems.

Compliance

„Kein eigenes Gesetz zum Schutz von Hinweisgebern" titelt der Behörden Spiegel in seiner September-Ausgabe. Der Entwurf für ein **Whistleblower-Schutzgesetz** sei im Bundestag abgelehnt worden. Wie der CDU-Abgeordnete Wilfried Oellers betont habe, enthalte die Rechtsordnung Schutznormen wie z. B. § 17 Abs. 2 Arbeitsschutzgesetz, §§ 53 ff. BImSchG, §§ 84, 85 BetrVG und § 1 Kündigungsschutzgesetz. Der von den Grünen eingebrachte Gesetzentwurf bedeute keine Verbesserungen für den Hinweisgeberschutz.

Datenschutz

Die **EU und die USA** haben sich auf ein Datenschutzabkommen geeinigt, meldet ZEIT ONLINE am 8. September. Dieses regele, wie persönliche Daten geschützt werden sollen, die Behörden zur Strafverfolgung austauschen. Das Abkommen verbiete beispielsweise die Weitergabe von Daten in Drittstaaten oder eine unnötige Speicherung. Der Kongress müsse dem Abkommen noch zustimmen. In der EU gelte die formelle Zustimmung der Mitgliedstaaten und des Parlaments als sicher. Die USA wünschten ein europäisches Fluggastdaten-Register. Auch das werde durch das Abkommen möglich.

Die **VdS-Richtlinien zur Cyber-Security** aus der Sicht von Datenschutzbeauftragten bewerten in s+s report (Ausgabe 3-2015, S. 44/45) Ralf Becker und Tobias Kafelja, zertifizierte Datenschutzbeauftragte und IT-Sicherheitsmanager. Mit dem vorgelagerten Quick-Check und dem Quick-Audit nach VdS 3474 vor der Zertifizierung nach VdS 3473 ergebe sich eine logische und absehbare Treppe. Das Management könne stückweise die Durchführung der einzelnen Schritte angehen und werde nicht verunsichert durch ein unkalkulierbar ausuferndes Projekt. Durch eine saubere Planung von Zeit und Budget könne sichergestellt werden, dass das nächste Etappenziel erreicht wird und sich der verbleibende Aufwand zur Zertifizierung nach VdS 3473, ISO 27001 oder gar als KRITIS-Betreiber stetig reduziert.

Datensicherheit

Felix Widmer, Tan Consulting & Services, behandelt in Ausgabe 4-2015 der Fachzeitschrift <kes> (S. 62/63) die Datensicherung als einen zentralen Sicherheitsbaustein. Sie müsse im Kontext der Geschäftsfortführung geplant und implementiert werden. Der tolerierte Datenverlust (Recovery Point Objective) und die maximale Wiederherstellungszeit (Recovery Time Objective) müssten verbindlich mit dem Business festgelegt und periodisch verifiziert werden. Eine Datensicherungsstrategie, Datensicherungsmethoden sowie genutzte Speichermedien und Tools könnten erst festgelegt und evaluiert werden, wenn die Anforderungen an die Datensicherung klar definiert sind.

Immer mehr Billighersteller aus China bringen nach einer Meldung der Wirtschaftswoche vom 28. August **Mobiltelefone mit fest installierter Spähsoftware** auf den Markt. Meist seien die Viren so programmiert, dass sie das infizierte Smartphone in eine Abfangstation für sensible Daten aller Art verwandeln. Bisher gebe es kein Gegenmittel. Die Spionageprogramme seien sehr tief in der Software neu ausgelieferter Smartphones chi-

nesischer Hersteller versteckt. Neben Handys asiatischer Billighersteller treffe es auch Geräte von Huawei, Lenovo und Xiaomi. Enttarnen könnten die Kunden so einen Spionageangriff, indem sie direkt nach dem Auspacken des Smartphones eine Sicherheits-App installieren und das Gerät nach Schadsoftware durchsuchen.

Im Sonderbericht Wirtschaftsschutz vom 18. September weist der BND darauf hin, dass zum 1. September in **Russland** eine Änderung im Datenschutzgesetz in Kraft getreten sei. Es sei vorgeschrieben, dass personenbezogene Daten russischer Staatsbürger auf Servern gespeichert werden müssen, die sich physisch auf dem Hoheitsgebiet der Russischen Föderation befinden. Ausländische Unternehmen, die ihr Geschäftsgebiet unter anderem in Russland haben, stünden damit vor rechtlichen, finanziellen und organisatorischen Problemen. Die Änderung legitimiere den russischen Staatspräsidenten, den westlichen Informationsfluss zu kontrollieren.

Google preist bessere Datensicherheit der **Apps for Work** an, berichtet heise.de am 22. September. Google habe einen neuen Standard in seinen Compliance-Katalog aufgenommen. ISO/IEC 27018.2014 richte sich speziell an Provider von externen Diensten und solle sowohl Kunden, als auch deren Kunden schützen. Die Funktion gebe es aber ausschließlich für professionelle Nutzer der Apps for Work und Apps for Education. Der Standard umfasse Richtlinien zum Umgang mit personenbezogenen Daten durch Cloud-Anbieter. Zum Beispiel dürfe Google danach keine Informationen des Kunden für Werbezwecke verwenden oder an Dritte weitergeben. Auch müssten Nutzer Werkzeuge erhalten, mit denen sie ihre Daten löschen und exportieren können. Zudem müsse der Provider angeben, wo er die Daten speichert. Andere Cloud-Anbieter wie Dropbox und Microsoft hätten ISO 27018 schon länger in ihren Katalog mit aufgenommen.

Einbruch

Einbruchschutz zahle sich aus, betont Harald Schmidt, Zentrale Geschäftsstelle für Polizeiliche Kriminalprävention der Länder und des Bundes, in der Ausgabe 3-2015 von s+s report (S. 34/35). Wer sein Haus saniere, könne jetzt zusätzlich von den Förderprodukten der KfW profitieren.

Dipl.-Ing. Paulus Vorderwülbecke befasst sich in der Ausgabe 3-2015 der Zeitschrift s+s report, S. 36–39, mit der Funktion, der Prüfung und den Einsatzgrenzen von **Passiv-Infrarot-bewegungsmeldern** (PIR-Melder). Sie böten für etliche Herausforderungen der Einbruchmeldetechnik eine passgenaue Lösung. Die technischen Randbedingungen des Einsatzes sowie die physikalischen Wirkprinzipien von PIR-Meldern müssten beachtet werden. Bei bestimmten Gegebenheiten sollte der Außenhautüberwachung gegenüber der fallen- oder schwerpunktmäßigen Überwachung mit PIR-Meldern Vorrang eingeräumt werden. Der Autor behandelt unter anderem den Problemfall „Tierimmunität", die Überlistung von PIR-Meldern und Möglichkeiten des Schutzes vor Überlistung. Zusammenfassend lasse sich feststellen, dass sich PIR-Melder – sofern VdS-geprüft und -anerkannt – gemäß ihrer Konstruktion bei der Gestaltung von EMA sinnvoll einsetzen lassen, wenn die Randbedingungen stimmen. Selbstverständlich müssten etwa die Überwachungsbereiche der Melder stets frei gehalten werden.

Einzelhandelssicherheit

Frank Horst, EHI Retail Institute e. V., erläutert in Ausgabe 3-2015 des Fachorgans DSD (S. 18) die **Inventurdifferenzen im deutschen Einzelhandel 2014.** Sie blieben mit 3,9 Mrd. Euro auch 2014 unverändert hoch. Mit einem Anteil von über 50 Prozent seien Ladendiebstähle nach wie vor die Hauptursa-

che. Bei den Maßnahmen zu deren Vermeidung hätten Personalschulungen, vor allem in den Bereichen Kasse, Verkauf und Wareneingang, die höchste Priorität. Auf Ladendiebstähle von Kunden seien rund 2,1 Mrd. Euro der Differenzen zurückzuführen. Den eigenen Mitarbeitern würden knapp 900 Millionen angelastet, Lieferanten sowie Servicekräften etwas mehr als 300 Millionen. Die restlichen 600 Mio. Euro entfielen auf organisatorische Mängel. Insgesamt gingen dem Einzelhandel durch Inventurdifferenzen und Investitionen zu deren Vermeidung 1,34 Prozent des Umsatzes – absolut rund 5,2 Mrd. Euro – verloren.

Elektronischer Personalausweis

Holger Funke, HJP Consulting GmbH, und Tobias Senger, BSI, beschreiben in der Ausgabe 4-2015 der Fachzeitschrift <kes> die Vorteile einer **Open Source-Lösung** zur Simulation der Chipkartenfunktionen des elektronischen Personalausweises. Es werde aufgezeigt, auf welcher Architektur der Simulator basiert, eine Einordnung des Simulators in die deutsche eID-Landschaft vorgenommen sowie das Prinzip der virtuellen Kartenleser und eine Migration auf ein Android-Smartphone mit NFC-Unterstützung dargestellt (S. 35–41). Behandelt werden die Simulation einer Java Card, die Anbindung über virtuelle Kartenleser und die Simulation auf Android mit NFC, ferner die Vorteile von Open Source, die Community der Anwender und die Community der Entwickler. PersoSim biete interessierten Anwendern und Entwicklern eine einfache und unbürokratische Möglichkeit, den elektronischen Personalausweis zu simulieren und damit eigene Implementierungen zu verifizieren. Darüber hinaus biete der Simulator die Möglichkeit, die kryptografischen Protokolle, die auf dem integrierten Chip angewendet werden, zu verstehen und nachzuvollziehen.

Endgerätesicherheit

Ein Verbot von „Bring your own device" (BYOD) komme für die meisten Firmenchefs nicht infrage, heißt es in der September-Ausgabe des Behörden Spiegel. Für Remote Wipe (Fernlöschung) böten Security-Anbieter mehrere Lösungen an. Diese müssten aber dauerhaft aktiviert sein. Je weniger Mitarbeiter auf hochsensible Firmendaten zugreifen, desto geringer sei das Risiko, dass Firmengeheimnisse verlorengehen. Der Fachbegriff laute Mobile Device Management (MDM).

Gefährdungshinweise Thailand

Der ASW weist am 11. September auf eine Analyse der EXOP GmbH zur Sicherheitslage in Thailand hin. Der **Terroranschlag auf den Erawan-Schrein** im Zentrum Bangkoks, bei dem 20 Personen starben und mehr als 120 Personen verletzt wurden, markiere den bislang größten Terroranschlag in Thailand außerhalb der konfliktreichen Südprovinzen. Größere Anschläge seien in Thailand bislang eher Einzelereignisse gewesen. Aufgrund der geringeren Vorbereitungszeit sei das Risiko kleinerer Anschläge, die wahllos an belebten Plätzen verübt werden, ungleich höher. EXOP empfehle, insbesondere folgende Risikoindikatoren im Blick zu halten, die auf eine Verschlechterung der allgemeinen Sicherheitslage hindeuteten: Zunahme terroristischer Vorfälle und entsprechender Sicherheitsoperationen außerhalb der Südprovinzen, insbesondere in Touristengebieten; wiederholte Verstöße gegen das Versammlungsverbot und die Einschränkungen hinsichtlich politischer Berichterstattung, die von der Militärregierung verhängt werden; verstärkte Hinweise auf einen Machtkampf innerhalb des königlich-militärischen Establishments; nachlassende Unterstützung für das Königshaus und Zunahme von Verstößen

gegen das Lèse-Majesté-Gesetz vor dem Hintergrund des schlechten öffentlichen Ansehens des Kronprinzen und der parteiischen Einmischung des Königshauses in den politischen Konflikt.

Gefahrenmanagement-systeme

Die Zeitschrift PROTECTOR veröffentlicht in der Ausgabe 9-2015 eine Marktübersicht über 60 Gefahrenmanagementsysteme von 34 Anbietern (S. 36). Je Produkt seien 55 Kriterien abgefragt worden.

Gefahrenmeldeanlagen

Rechtsanwältin Petra Menge nimmt in s+s report (Ausgabe 3-2015, S. 48–52) Stellung zum rechtlichen Rahmen beim **Fernzugriff und der Fernwartung** von GMA. Sie beleuchtet haftungsrechtliche Aspekte und stellt einschlägige Beispielfälle aus der Praxis vor. Einleitend erläutert sie Arten sowie die Vor- und Nachteile des Fernzugriffs. Anhand der Beispielfälle geht sie auf die vertragsrechtliche Lage, Fragen der Pflichtverletzung, von Sach- oder Rechtsmängeln, auf das Vertretenmüssen, Kausalität und Rechtsfolgen ein. Und sie gibt Tipps zur Haftungsprävention.

Industrie 4.0

Myriam Dunn Cavelty, ETH Zürich, erläutert in der Zeitschrift Sicherheitsforum (Ausgabe 4-2015, S. 34–36), was Industrie 4.0 für die **Sicherheit im Unternehmen** bedeutet. Eingebettete Systeme benutzten häufig kein Betriebssystem, oder sie arbeiteten mit speziellen Versionen von Standard-Betriebssystemen. Diese proprietären Lösungen führten oft dazu, dass Schwachstellen unter Umständen niemals untersucht, verstanden oder beseitigt wurden und dass gängige Sicherheitslösungen nicht oder nur sehr schwierig implementiert werden könnten.
Ein fixes und quantifizierbares Maß an Informationssicherheit für die Zertifizierung könne es nicht geben. Was zählt, sei vielmehr das Vorhandensein bestimmter Sicherheitsmanagementsysteme oder auch der Einsatz von soliden Krisenmanagementplänen. Die wichtigste Herausforderung für die Industrie sei die proaktive Einbettung von Sicherheit, die auf die spezifische Priorität der Schutzziele in der Produktion Rücksicht nimmt, direkt in Geräte (Security by Design). Die größtmögliche Sicherheit werde immer aus einer Kombination mehrerer Methoden erreicht werden.

Dipl.-Wirtschaftsjurist (FH) Sebastian Brose, VdS Schadenverhütung, erläutert in s+s report (Ausgabe 3-2015, S. 46/47) die Gefahr von Angriffen auf moderne Gebäudetechnik mit **KNX-Installationen** (Feldbus zur Gebäudeautomation, früher auch als Europäischer Installationsbus (EIB) bekannt). KNX sei in nahezu allen modernen gewerblichen oder industriellen Immobilien zu finden. Aufgrund der schwachen Sicherheitsarchitektur des KNX-Busses bestehe für einen Angreifer die Möglichkeit, alle Komponenten so zu „rekonfigurieren", dass diese unbrauchbar werden. Im Worst-Case-Szenario bringe ein Täter gleichzeitig eine Vielzahl von KNX-Installationen unter seine Kontrolle. Das gleichzeitige Aus- und Einschalten aller Verbraucher aller Gebäudeinstallationen würde eine Lastspitze erzeugen, durch die das Energieversorgungsnetz einer ganzen Region in kurzer Zeit zum Zusammenbruch gebracht werden könne. VdS erarbeite derzeit Richtlinien, die beschreiben, wie eine KNX-Installation sicher aufgebaut werden kann.

IT-Sicherheit

Allein die deutsche Wirtschaft beklage jährlich einen **Schaden durch Hacker** von 50 Mrd. Euro, berichtet die FAZ am 2. September. Die 102 Mrd. Euro Schaden seien in den letzten zwei Jahren entstanden durch: Umsatzeinbußen durch Plagiate (23 Mrd.), Patentrechtsverletzungen (18,8 Mrd.), Verlust von Wettbewerbsvorteilen (14,3 Mrd.), Ausfall, Diebstahl oder Schädigung von IT-Systemen und Betriebsabläufen (13 Mrd.), Imageschaden bei Kunden und Lieferanten (12,8 Mrd.), Kosten für Rechtsstreitigkeiten (11,8 Mrd.), datenschutzrechtliche Maßnahmen (3,9 Mrd.), Erpressung mit gestohlenen Daten (2,9 Mrd.) und höhere Mitarbeiterfluktuation (1,7 Mrd.). Die Standards für die hardwarebasierte Datensicherheit auf der Welt setzen nach Worten von Kurt Sievers, Vorsitzender des Fachverbandes Electronic Components and Systems im ZVEI, die drei großen europäischen Chiphersteller NXP, Infineon und ST Microelectronics. Für den ZVEI komme es auf Sicherheit in drei Bereichen an: den Schutz persönlicher Daten (Beispiel Gesundheitspass), die Sicherheit vor Manipulation (Onlinebanking) und die Hoheit der Daten (Fahrdaten des Autos). Die im Chip materiell verankerte Sicherheit sei gegen äußere Angriffe sicherer als eine reine Software-Sicherheit. Manche Chips seien so programmiert, dass sie sich bei unsachgemäßer Berührung oder bestimmter Strahlung selbst zerstören. Die deutsche Mikroelektronik habe einen großen Anteil an der Sicherheit der flächendeckend eingesetzten Kreditkarten oder auch an den heute üblichen elektronischen Wegfahrsperren in den Autos. Das elektronische Bezahlen im Einzelhandel sei so ausgereift, dass es jetzt in großem Stil und mit hoher Sicherheit der Daten eingesetzt werden könne.

Mit Schwachstellen in **Kontrollsoftware von Kraftwerken und Raffinerien** befasst sich heise.de am 31. August. Sicherheitsforscher warnten seit Jahren davor, dass Industrie-Kontrollsysteme (ICS) viel zu verwundbar für Angriffe von außen sind. Jetzt habe ein Hacker der Sicherheitsfirma Positive Technologies erneut eine ganze Reihe von Sicherheitslücken in Software offengelegt, die wichtige Aufgaben in Raffinerien, Fabriken und Kraftwerken erfüllt. Bei einem Produkt könnten Passwörter lokal im Klartext ausgelesen werden, in einem anderen Fall könnten Angreifer Passwort-Hashes abfangen und die Kontrolle über Systeme von außen übernehmen.

Durch **Differenzierung von Zugriffen,** beispielsweise in „nur Nutzer verwalten" oder „nur Audit-Einstellungen steuern", könnten potenzielle Schäden durch Eindringlinge oder durch den Administrator selbst eingegrenzt werden, heißt es in einem Verlagsspezial Consulting der FAZ am 8. September. Die erforderlichen Administrationsrechte sollten über Bereichsrollen zugewiesen werden. Einfacher Passwortschutz mit Passwörtern, die zudem nicht regelmäßig erneuert werden, sei für Angreifer aus dem Cyberspace kein Hindernis, so Mathias Hein, freier IT-Berater. Er plädiere im Rahmen einer hieb- und stichfesten Zugriffskontrolle für den Einsatz starker Authentisierungsverfahren. Nach dem Marktanalysten Gartner würden Digital Business, Cloud Computing und Mobility maßgeblich die Ausrichtung und Ausprägung der Zugriffskontrollschirme prägen. Zusätzliche Arbeitsfelder für das Security Consulting seien Identity Federation für den Austausch von Nutzer-Identitätsinformationen zwischen Sicherheitsdomänen, ein barrierefreier Single-Sign-on-gesteuerter Zugriff zwischen den Domänen und die Zuordnung von Nutzern zu Rollen im erweiterten Einsatzfeld. Anderen Akteuren – wie Cloud-Providern – sollte nur die Verwaltung eigener Daten, Anwendungen und Systeme überlassen werden, die für das Unternehmen weniger kritisch sind. In derselben Verlagsbeilage weist Olaf Baunack, Alsbridge GmbH, auf das Modell des Hybrid Sourcings hin. Hatten Unternehmen bisher lediglich die Möglichkeit, sich zwischen Offshore-, Nearshore- und Onshore-Outsourcing

zu entscheiden, erweitere Hybrid Sourcing die Möglichkeiten. So könnten zum Beispiel Rechenzentren zur Speicherung sensibler Daten regional ansässig sein. Darüber hinausgehende Services würden im Hinblick auf Personal- oder Betriebskosten in vergleichsweise kostengünstigen Regionen erbracht.

Einen Index der Gefährdungslage als „Tacho für die IT-Sicherheit" stellen Holger Himmel, Tengelmann KG, und Dr. Aleksandra Sowa, Deutsche Telekom AG, in Ausgabe 4-2015 der Fachzeitschrift <kes>, S. 14–18, vor. **Sicherheitsmetriken** über die Verwundbarkeit und Bedrohungen ließen sich zu einem aussagekräftigen Index der Gefährdungslage (Exposure Index) konsolidieren. Ziel dieses Index sei es, die aktuelle Lage der Informationssicherheit sowohl unter Berücksichtigung relevanter Bedrohungen als auch im Hinblick auf die tatsächliche Verwundbarkeit und vorhandene Schwachstellen des Unternehmens quantitativ abzubilden – konkret: die Gefährdungslage für die Grundwerte der IT-Sicherheit darzustellen, also für Verfügbarkeit, Integrität und Vertraulichkeit. Die in den Index einfließenden Metriken könnten die Aktualität von Software, Passwortstärke, Schutz vor Umwelteinflüssen, Grad der Security-Awareness, Qualität des Monitorings von Systemen oder Richtlinienkonformität betreffen. Die Autoren beschreiben Beispiele für den Verwundbarkeitsindex und für den Bedrohungsindex. Das Modell sei skalierbar. Zu seiner weiteren Entwicklung wäre die Erstellung einer Basis-Metriksammlung mit Normierungsempfehlungen für den Index der Verwundbarkeit für Unternehmen oder gar für einzelne Branchen sinnvoll.

Prof. Dr. Kai-Oliver Detken, DECOIT GmbH, befasst sich in der Ausgabe 4-2015 der Fachzeitschrift <kes>, S. 25–28, mit dem Projekt „Security Information and Event Management für kleine und mittelständische Unternehmen" (SIMU), in dem ein skalierbares **„Security Information and Event Management"-System** (SIEM) mit Nutzung einheitlicher Metadaten per „Interface for Metadata Access Points" (IF-MAP) erarbeitet wird. SIEM-Systeme seien aufwändig und daher in KMU kaum verbreitet. Aber auch in größeren Unternehmen bewirkten sie eventuell mehr Aufwand als nötig. Erste Ergebnisse des Projekts ließen sich auch in bestehenden Installationen und großen Unternehmen nutzen. Behandelt werden die SIEM-Definition, das SIMU-Projekt und das SIEM-Konzept. Den Bedürfnissen von KMUs komme unter anderem eine leichte Integrierbarkeit in eine bestehende Infrastruktur und der wartungsarme Betrieb des Systems entgegen.

Monika Schaufler, Proofpoint, befasst sich in der Ausgabe 4-2015 der Fachzeitschrift <kes> mit dem Problem, dass ein immer schneller werdender Fluss an Kundendaten, vertraulichen Informationen, Kreditkartendaten und geistigem Eigentum aus Netzwerken von Unternehmen ströme, lange bevor das Personal einen Sicherheitsbruch auch nur erkannt hat. Tatsächlich beginne beispielsweise bei nahezu 90 Prozent der Datenschutzverletzungen an Point of Sale-Terminals die Datenausschleusung bereits innerhalb von Minuten oder Sekunden nach dem Eindringen. Ob Abwehrsysteme den erwünschten Schutz und Nutzen bringen, hänge davon ab, wie gut die Informationen und Gegenmaßnahmen der verschiedenen Systeme vereint, analysiert und ausgewertet werden.

Dirk Knop, JakobSoftware, behandelt in der Ausgabe 4-2015 der Fachzeitschrift <kes>, S. 50–52, **Malware am Point of Sale.** Meldungen über Schadsoftware, die Daten von Kassensystemen abgreift, würden sich häufen. An der Kasse des Baumarkts, der Tankstelle, des Discounters fänden sich die meisten Informationen. Was läge also näher, als die begehrten Daten gleich dort zu stehlen? Der Autor beschreibt die Einfallstore. Als Sicherheitsmaßnahmen empfiehlt er: Die Netzwerke, in denen Kassen arbeiten, dürfen nicht als sicher betrachtet werden. Die Kommunikation zwischen Kasse und Server

sollte verschlüsselt ablaufen. Zudem müssten alle Standard-Passwörter in der eingesetzten Software geändert werden. Weiterhin müsse man die installierten Programme, Dienste und Betriebssysteme stets auf dem aktuellen Stand halten. Ein Virenschutz auf Clients, Servern und sogar den Kassensystemen könne eindringende Malware aufspüren und blockieren. Zudem sollte die Konfiguration der Systeme weiterreichende Sicherheitsaspekte berücksichtigen.

Bewerberportale und E-Mail-Bewerbungen könnten sich als zweischneidiges Schwert für ein Unternehmen erweisen, befürchtet Security-Engineer Ralph Dombach in Ausgabe 4-2015 der Fachzeitschrift <kes>, S. 54–57. Denn sie könnten neben Zuschriften von Kandidaten auch Angriffe transportieren. Hohe Wirkung gegen neue Schadsoftware ließe sich im virtuellen Arbeitsumfeld, durch Format-Konvertierung, Multiscannertest und Quarantäne erzielen, mittlere Wirkung durch ein alternatives Betriebssystem und die Nutzung alternativer Software. Diese Möglichkeiten werden beschrieben. Wichtig sei es, eine Lösung zu finden, die den Prozessablauf nicht unnötig verkompliziert und die Sicherheit bei der Bearbeitung von Dokumenten deutlich erhöht.

In der Fachzeitschrift <kes> (Ausgabe 4-2015, S. 44–49) bezeichnet Philipp Beck, Berater der sirosec GmbH, ein **Botnetz aus Robotern und Kampfdrohnen** als eine düstere Sci-Fi-Vision. Der Sprung vom infizierten Router zum „Internet of Things" (IoT) sei nur noch ein kleiner Schritt. Neben Entertainment und Gebäudeautomation sei die Mobilisierung des IoT ein weiteres Entwicklungsfeld. Der Autor beschreibt fremdgesteuerte Vitalfunktionen und den Keyless Access. Vieles spreche für die Adaption von „Standard-IT" durch die Industrie – nur: Die vielen Fehler in solchen Geräten und deren katastrophale Auswirkungen auf die Security sprächen eklatant dagegen. Industrieanlagen hätten eine ähnlich große Anziehungskraft wie das IoT: Die Popularität von Anlagen-Hacking nehme zu. Während es heute bei der Kriminalität mit Fokus auf IT-Systeme vornehmlich um Erpressung, Datendiebstahl, Werbung oder Betrug gehe, könne sich das Bedrohungsszenario in Zukunft schnell wandeln. Denn mit der Kontrolle über Steuerungen realer Dinge gehe auch die Kontrolle über die Unversehrtheit der realen Umwelt verloren. Bis einheitliche Security-Standards existieren, sei ein langer Prozess zu erwarten. Bis dahin werde Verantwortlichen nichts anderes übrig bleiben, als aus den Erfahrungen der „klassischen" IT zu lernen und individuelle Lösungen aus bestehenden Ansätzen zu entwickeln.

In einer Beilage zur Zeitschrift <kes>, August 2015, S. 5–8, erläutert Joern Maier, HiSolutions AG, die geplante **Überarbeitung des IT-Grundschutzes** nach BSI, der nach dem Urteil vieler zu unflexibel, zu aufwändig und den Anforderungen der heutigen Zeit nicht mehr entsprechend sei. Es solle ein Verfahren erarbeitet werden, das den Schwerpunkt auf die Implementierung der wichtigsten grundlegenden Sicherheitsmaßnahmen legt, ohne dabei einen zu großen organisatorischen Aufwand für die Erhebung und Bewertung von Informationswerten zu generieren. Ein weiteres Verfahren solle es Institutionen ermöglichen, sich in einem ersten Schritt ganz auf den Schutz besonders wichtiger Informationen zu konzentrieren. Das BSI strebe eine radikale Verschlankung der Bausteine an. Sie würden sich darauf konzentrieren, was umzusetzen ist. Wie etwas umzusetzen ist, solle in sogenannten Umsetzungshinweisen definiert werden. Insbesondere werde über eine Optimierung und Verbesserung der bisherigen Aufteilung in die fünf Schichten übergreifende Aspekte, Infrastruktur, IT-Systeme, Netze und Anwendungen nachgedacht. Die neue Struktur werde weiterhin IT- und Infrastrukturobjekte vorsehen, diese aber deutlich detaillierter untergliedern. Neben den technischen Zielobjekten würden die neuen IT-Grundschutz-Kataloge auch Prozessbausteine enthalten. Ein weiterer wichtiger Aspekt des neuen IT-Grundschutzes würden Profile sein.

Der IT-Grundschutz setze bei der ISMS-Einführung auf das **„Wasserfall"-Modell,** meinen Knut Haufe, Marcel Schulz und Knud Brandis, PERSICON AG, in der Beilage der Zeitschrift <kes> vom August 2015, S. 10–12. Langjährige Projekterfahrung zeige allerdings, dass ein alternatives Vorgehen mit einer bewussten Parallelisierung geeigneter Aufgaben größeren Erfolg verspricht und das angestrebte Informationssicherheits-Managementsystem besser mit der Sicherheitspraxis verzahnt. Eine prozessorientierte Vorgehensweise habe folgende Vorteile: IT-Grundschutz werde zum nützlichen Orientierungsrahmen mit der Folge höherer Akzeptanz und größerem Nutzen. Das ISMS werde integraler Teil der Betriebsorganisation. Der IT-Grundschutz halte mit der Dynamik typischer moderner Informationsverbünde Schritt. Er bediene sich vorhandener Ressourcen und er habe eine größere Chance, Teil der „Sicherheitskultur" in der Organisation zu werden. Eine unkontrollierte Ausweitung des Projekt-Scopes lasse sich leichter vermeiden.

In der Beilage der Zeitschrift <kes> vom August 2015 (S. 14/15) plädiert René Seydel, secunet Security Networks AG, für eine optimierte Sicherheitskonzepterstellung nach IT-Grundschutz. Fachprozesse fänden in der Methodik ebenso Berücksichtigung wie Standard-IT-Anwendungen. Das von secunet entwickelte Vorgehen werde in drei vorzugsweise parallel auszuführenden Handlungssträngen – „sichere Kern-IT", „Fachsicherheitskonzepte" und „ISMS" – gebündelt und führe zielgerichtet zu einem zertifizierungsfähigen ISMS nach IT-Grundschutz. Die Methodik sehe vor, mehrere Schritte zeitgleich zu beginnen und in den drei Handlungssträngen parallel zu verfolgen. Dadurch sei eine optimierte Zeitplanung möglich und die Gesamtprojektdauer verkürze sich.

Die BSI IT-Grundschutz-Vorgehensweise lasse viel Raum für Anpassungen, schreibt Tobias Seemann, HiScout GmbH, in der Beilage zur Zeitschrift <kes> vom August 2015 (S. 16/17). Er erklärt, warum die Individualisierung der Vorgehensweise oft sinnvoll sei, Entscheidungen nicht für die Ewigkeit seien, und wie man trotzdem **das richtige Tool** finde. Es sollte auf ein Tool gesetzt werden, das zwei zentrale Eigenschaften besitzt: Einerseits sollte es im Auslieferungszustand am BSI-Standard ausgerichtet sein, um den initialen Ein- oder Umstieg möglichst einfach zu gestalten. Andererseits sollte es durch einfache Anpassbarkeit und eine flexible Plattform in der Lage sein, spätere Erweiterungen und Anpassungen problemlos zu unterstützen.

Ein **Notfallplan** minimiert Schäden und Spätfolgen von systematischen Hackerangriffen, argumentiert Michael Klatte, ESET Deutschland GmbH, in der Beilage der Zeitschrift <kes> vom August 2015, S. 18–20. Aber jedes zweite Unternehmen besitze keinen Notfallplan. Der Security-Software-Hersteller ESET gebe fünf Tipps, mit deren Hilfe die Folgen einer Malware-Attacke auf ein Minimum reduziert werden könnten: das Ausmaß der Infektion ermitteln, den IT-Betrieb sicherstellen, die Infektion eindämmen, sie eliminieren und weitere Attacken verhindern, schließlich aus Cyberangriffen und Fehlern lernen.

Rainer Singer, Infoblox, befasst sich in der Beilage zur Zeitschrift <kes>vom August 2015, S. 22–24, mit der **Schwachstelle Domain-Name-System** (DNS), das als allgegenwärtiges „Adressbuch" des Internets überall vorhanden, aber selten geschützt sei. Angriffe zielten auf die Unterbrechung von DNS-Diensten, wie etwa DoS/DDoS-Attacken. Vor allem letztere gehörten weiterhin zu den bevorzugten und damit auch gefährlichsten Angriffen auf Unternehmen. Sowohl Umfang als auch Geschwindigkeit und Komplexität von DoS- und DDoS-Attacken seien in den letzten Jahren signifikant angestiegen. Name-Server könnten heute in der Regel so modifiziert werden, dass wiederholte Anfragen von derselben IP-Adresse mit identischem Inhalt erkannt würden.

Das **Vulnerability-Management** behandelt Dirk Schrader, Greenbone Networks GmbH, in der Beilage zur Zeitschrift <kes> vom August 2015, S. 26/27. Der überwiegende Teil aller erfolgreichen Angriffe auf die IT eines Unternehmens nutze Schwachstellen aus, die schon länger als zwölf Monate bekannt waren. Der diesjährige „Data Breach Investigation Report" beziffere diesen Anteil auf 99,9 Prozent. Ziel müsse es sein, diese Angriffsfläche deutlich zu reduzieren. Vulnerability-Management sei ein wesentliches Element der IT-Sicherheit. Konkret gehe es um den zentralen Vergleich von Ergebnissen einzelner Schwachstellenprüfungen. Das Resultat gebe Auskunft darüber, wie sich das Sicherheitsniveau entwickelt hat und werde so zu einer Erfolgskennzahl.

Neue Wege, um modernen Hackerangriffen einen Riegel vorzuschieben und sich für die Herausforderungen durch immer weiter auflösende Peripherien zu wappnen, beschreibt Sascha Pfeiffer, Sophos, in der Beilage zur Zeitschrift <kes> im August 2015, S. 28/29. Der Autor plädiert für die **Verknüpfung verschiedener Security-„Silos"** wie Netzwerk, Endpoint und Mobile und für mehr Sicherheitsintegration. Es sei an der Zeit, dass Sicherheitsprodukte zusammenarbeiten und Informationen austauschen. So erhielten Unternehmen einen Schutz, der nicht nur einfacher, sondern auch effektiver ist. Konkret sehe ein Konzept beispielsweise so aus, dass ein Unified-Threat-Management (UTM)-Appliance erkenne, wenn ein Endpoint kompromittiert wurde, den Endpoint benachrichtigt, den Administrator informiert und den Endpoint vom Internet isoliert. Ein weiteres Beispiel für eine Vernetzung bestehender IT-Lösungen wäre ein sogenanntes „Compromise Center", das verdächtige Ereignisse von mehreren Endpoints, Servern und Netzwerkgeräten zusammentragen kann.

Die FAZ meldet am 18. September, die Konzerne Allianz, Bayer, BASF und Volkswagen hätten angekündigt, gemeinsam ein **Zentrum für Computer- und Internetsicherheit** zu gründen. Es solle die deutsche Wirtschaft als Dienstleister unterstützen. Die Deutsche Cyber-Sicherheitsorganisation (DCSO) solle ihren Sitz in Berlin haben und mit dem BMI und dem BSI zusammenarbeiten. Das Angebot der Unterstützung solle sich auch an KMU richten, die ihre Sicherheitsarchitektur verbessern wollen. Die DCSO sei offen, weitere Partner mit an Bord zu nehmen. Das Projekt habe in der Branche für einige Überraschung gesorgt.

Ende Juli 2015 sei eine Sicherheitslücke bekannt geworden, die annähernd alle Versionen von Android betrifft, berichtet der BND im Sonderbericht Wirtschaftsschutz am 18. September. Die Sicherheitslücke betreffe das Multimediasystem von Android-Geräten und sei mit der Bezeichnung **„StageFright"** (Lampenfieber) veröffentlicht worden. Ein Angreifer könne unter Ausnutzung dieser Lücke mittels manipulierter Videodateien einen eigenen Programmcode mit den Rechten des Mediaplayers ausführen. Es sei davon auszugehen, dass hochrangige Cyberspionageakteure in der Lage sind, diese Schwachstelle auszunutzen. Ein sprunghafter Anstieg von Angriffen sei zu erwarten. Das Bedrohungspotenzial gegen Mobiltelefone und weitere Geräte mit Android-Betriebssystemen werde als sehr hoch eingeschätzt. Hochrangige Ziele in Unternehmen und staatlichen Einrichtungen seien vermutlich die ersten Angriffsopfer.

Dipl.-Wirtschaftsjurist (FH) Sebastian Brose, VdS Schadenverhütung, weist in s+s report (Ausgabe 3-2015, S. 43) auf die Richtlinien **VdS 3473** hin, die an den Belangen der KMU ausgerichtet seien und einen praktikablen Ansatz beschreiben würden, der schnell und gleichzeitig nachhaltig für ein vernünftiges Maß an Cyber-Security im jeweiligen Unternehmen sorge. Die Richtlinie sei dabei, sich als der Standard für Cyber-Security in KMU zu etablieren. Mit dem webbasierten Tool VdS Quick-Check könnten Unternehmen sich ein erstes Bild über den Status ihrer

Cyber-Security verschaffen. Anhand von 39 Fragen in den Handlungsfeldern Organisation, Technik, Prävention und Management werde der individuelle Schutzgrad ermittelt. Die kostenlose Auswertung gebe mit Maßnahmenempfehlungen konkrete Hilfestellung zur Verbesserung der Situation.

IuK-Kriminalität

Heise.de weist am 30. August darauf hin, dass Symantec Ende 2014 die **Ausspähungssoftware „Regin"** entdeckt hatte. Nun würden neue Untersuchungen des Unternehmens, das den Trojaner entdeckt hatte, weitere Details zu den Fähigkeiten des Programms enthüllen. Regin sei eine fünfstufige Bedrohung, die auf jeder Stufe die nächsthöhere Bedrohung nachlade und entschlüssele. Die Malware sei modular aufgebaut. Einige Module steuerten die Grundfunktionen der Malware, etwa die Vernetzung oder den Umgang mit dem eigenen verschlüsselten virtuellen Dateisystem. Andere agierten als Schadfunktionen, die die Auswirkung auf das mit Regin infizierte System bestimmen. Symantec berichte von der Entdeckung 49 weiterer Module. Doch auch mit ihnen bleibe die Liste unvollständig. Symantec habe darüber hinaus eine umfangreiche „Command and Control-Infrastruktur" (C&C) entdeckt. Die gesamte C&C-Kommunikation sei stark verschlüsselt und verlaufe zweistufig: Über einen Kanal kontaktiere der Angreifer den infizierten Computer und weise ihn an, die Kommunikation über einen zweiten zu eröffnen.

„Hacker lieben die Bahn", titelt die FAZ am 14. September. Mit zunehmender Vernetzung gerieten auch Infrastrukturen wie Stromnetze oder der Bahnverkehr ins Visier krimineller Hacker. Insgesamt seien binnen sechs Wochen gut 2,7 Mio. Zugriffsversuche auf die Simulation eines nachgebauten Eisenbahnsystems registriert worden. Sophos habe das als „Honigfalle" für Hacker konzipierte Projekt „Honeytrain" zusammen mit dem Industriedienstleister Koramis organisiert. Ungefähr in der Hälfte der Fälle sei ein Eindringen mit Hilfe von Wörterbuchattacken versucht worden. Dabei seien automatisiert lange Wörterlisten durchprobiert worden. In drei Fällen sei es den Angreifern gelungen, tatsächlich einzudringen. Zweimal seien sie in den Bereich gelangt, von dem aus in einem echten Verkehrssystem eine Zugsteuerung möglich wäre.

Holger Suhl, Kaspersky Lab, befasst sich in der Ausgabe 4-2015 der Fachzeitschrift <kes>, S. 58–62, mit **Advanced Persistent Threats** (APTs) und ihrer Abwehr. Das Ziel von APTs sei meist direkter Diebstahl oder das Ausspionieren von sensitiven und kommerziell verwertbaren Daten. APTs gingen dabei äußerst zielgerichtet vor, wollten auf keinen Fall erkannt werden, seien sehr raffiniert entwickelt und würden oft in mehreren Stufen ausgeführt. Im Visier stünden Konzerne und Organisationen, inzwischen aber auch mittelständische Firmen. Gemäß seiner Analysen gehe Kaspersky Lab davon aus, dass 67 Prozent aller Angriffsversuche auf bekannten und mit Signaturen erkennbaren Schadprogrammen basieren. Bei 32 Prozent der Cyberattacken kämen unbekannte, also noch nicht mit Signaturen gekennzeichnete, Schädlinge zum Einsatz und nur bei ein Prozent sei hochentwickelte Malware im Spiel, wie sie meistens bei APTs eingesetzt werde. Der Autor beschreibt „Duqu 2.0" (eine neue Malware-Generation), die „Equation Group", hinter der ein mächtiger Akteur zu stehen scheine, und die „Carbanak-Gang" (Kaspersky Lab, Interpol, Europol und andere Institutionen hätten im Februar 2015 einen Cyberbankraub aufgedeckt, bei dem innerhalb von zwei Jahren bis zu einer Milliarde US-Dollar von Finanzinstituten weltweit gestohlen wurde.) und bezeichnet mögliche Gegenmaßnahmen. Wichtig sei: Effektive IT-Security müsse immer vielschichtig angelegt sein – mit fortschrittlichen Anti-Malware-Lösungen im Kern und weiteren Schichten

von APT-Verhinderungs- oder Eindämmungs-Mechanismen wie Anwendungskontrolle oder Schwachstellen-Management.

Ein Lagebild der **Cybersicherheit in deutschen Unternehmen** skizziert Christian Lueg, G DATA Software AG, in der Beilage zur Zeitschrift <kes> vom August 2015, S. 32/33. Jedes dritte Unternehmen in Deutschland sei 2014 erfolgreich von Online-Kriminellen attackiert worden. Dies sei das Ergebnis der Cybersicherheits-Studie von G DATA und TNS Infratest. Insbesondere mittelständische Firmen gerieten dabei immer stärker ins Visier von Cyberangreifern. In 86 Prozent der Firmen würden Smartphones genutzt. Hierdurch würden Administratoren vor große Herausforderungen gestellt. Cyberkriminelle legten ihren Fokus immer stärker auf Mobile Devices. Allein für Android-Geräte erschienen täglich über 6.100 neue Schadprogramme. Mobile Devices müssten ebenso geschützt werden wie Desktop-PCs, Notebooks oder Server.

Im Sonderbericht Wirtschaftsschutz vom 18. September berichtet das BSI, einem Hacker-Ring sei es anscheinend gelungen, sich Zugang zu den Netzen der Fachdienste zu verschaffen, die Pressedienste börsennotierter Unternehmen an Investoren und andere Stakeholder verteilen. Auf diese Weise hätten Pressemitteilungen schon abgegriffen werden können, bevor sie der Öffentlichkeit zugänglich gemacht wurden. Die Täter hätten vorab Kenntnis von Informationen gehabt, die sich positiv oder negativ auf die Börsenkurse der Unternehmen auswirken würden, was sie zur Durchführung gewinnbringender Aktiengeschäfte befähigte. In den vergangenen fünf Jahren sollen rund 150.000 Pressemitteilungen gestohlen worden sein. Mehr als 100 Mio. US-Dollar seien anscheinend über Briefkastenfirmen mit Offshore-Konten abgewickelt worden. Neben der Cybergefährdung für Unternehmen durch Informationsabfluss zeige dieses Beispiel, dass es nicht reicht, die eigene Institution von Cybergefahren zu schützen. Vielmehr müsse ein vergleichbares Sicherheitsniveau auch bei Zulieferern, Dienstleistern und anderen Geschäftspartnern durchgesetzt werden. Bei der Sichtung von Angeboten könnten auch Zertifizierungen wie IT-Grundschutz oder ISO 27001 eine Rolle spielen.

Im Gegensatz zu Software bieten die Entwickler für **Firmware** nur äußerst selten Patches an, berichtet das BSI im Sonderbericht Wirtschaftsschutz vom 18. September. Dies führe dazu, dass viele Systeme trotz hinlänglich bekannter Sicherheitslücken ungeschützt weiter betrieben werden. Zur Unterstützung der Hersteller bei der Entwicklung eigener UEFI-Firmware habe ein Firmenkonsortium unter Beteiligung von INTEL eine Referenzimplementierung entwickelt, die stark verbreitet sei. Genau in dieser Referenzimplementierung seien nur zwei Schwachstellen entdeckt worden, durch die ein Angreifer die Firmware dauerhaft manipulieren könne. Die Lücken befänden sich im Update-Mechanismus und ermöglichten es über eine sogenannte „Privilege Escalation" für das Betriebssystem unsichtbare Rootkits einzuschleusen. Die Lücke sei bereits Ende 2014 entdeckt worden. Die unterschiedliche Herangehensweise der Hersteller mache das derzeitige Dilemma deutlich: Während sich bei den marktgängigen Betriebssystemen im PC-Bereich eine gängige Patch- und Updatekultur etabliert habe und versucht werde, bekannt gewordene sicherheitskritische Fehler zeitnah zu beheben, gäbe es bei Firmware-Updates keine allgemein anerkannte Vorgehensweise. So blieben selbst öffentlich bekannte und ausgenutzte Schwachstellen oft über Jahre bestehen. Dies gelte nicht nur für den Bereich der mobilen Geräte, sondern auch – und besonders kritisch – für viele Mikrocontroller-basierte Geräte wie zum Beispiel POS-Terminals, Kreditkartenterminals bis hin zu kompletten Industrie-Steuerungsanlagen.

Hackern sei eine erfolgreiche **Attacke gegen den App-Store** gelungen, also die

Online-Plattform von Apple, meldet die FAZ am 22. September. Es handle sich um den bislang größten Angriff auf den App-Store. Betroffen davon seien vor allem chinesische Apps, darunter Didi Kuaidi, die chinesische Version des Fahrdienstes Uber. Das auf Sicherheitsprogramme spezialisierte Unternehmen Palo Alto Networks habe mitgeteilt, es habe insgesamt 39 infizierte Apps gefunden, und mehrere hundert Millionen Nutzer könnten betroffen sein. Das Unternehmen habe die Schadsoftware als „sehr gefährlich" bewertet. Die Hacker hätten mit ihrem Angriff nicht direkt auf Apple abgezielt, sondern auf die Entwickler von Apps, und sie hätten dabei offenbar eine Schwachstelle im chinesischen Markt ausgenutzt.

Mit der Problematik von **Hackerangriffen auf vernetzte Kfz** befasst sich TECCHANNEL.de am 21. September. Der Knackpunkt im vernetzten Auto liege im CAN BUS-System. Dies sei das elektronische Herz des Connected Car. Gelinge es Angreifern, den CAN BUS zu kapern, sei der Zugriff auf die Steuergeräte meist nur noch eine Frage der Zeit. Im Regelfall seien es die Infotainment-Systeme moderner, vernetzter Autos, die als Einfallstor für Hacker dienen. Diese Systeme böten inzwischen immer häufiger zahlreiche kabellose Verbindungs- und Integrationsmöglichkeiten – etwa via Bluetooth oder WLAN. Diese Möglichkeiten zur externen Kommunikation könnten zu einem ernsthaften Problem werden, insbesondere wenn die physischen Fahrsysteme architektonisch nicht strikt von den übrigen Systemen getrennt sind.

Katastrophenschutz

Einen Überblick über Präventionsmaßnahmen gegen Hochwasser, Grundwasser und Starkniederschlag gibt Dipl.-Geologe Daniel Müller, R + V Allgemeine Versicherung AG, in der Ausgabe 3-2015 der Zeitschrift s+s report, S. 54–59. Er definiert die Gefahrenphänomene und befasst sich mit der allgemeinen Risikoerkennung, mit den Problemen eindringendes Wasser, Kanalrückstau, anschlagendes Wasser, Wasserdruck, Unterspülung und Haustechnik bei der baulichen Vorsorge, mit der Wirtschaftlichkeitsuntersuchung vor dem Bau einer Hochwasserschutzeinrichtung, mit bedarfsangepasster Gebäudenutzung, Notfallplanung und Business Continuity Management.

Logistiksicherheit

Die Fachzeitschrift GIT zeigt in der Ausgabe 9-2015, S. 70–73, wie Videokameras die Lagerlogistik optimieren. Um die Stillstandszeiten von Regalbediengeräten (RBG) in Hochregallagern möglichst gering zu halten, habe der **Hochregallager**-Anbieter Kardex Mlog seine RBG standardmäßig mit Mobotix S15D-Kameras ausgestattet. An jedem RBG sei eine S15D montiert, die links und rechts ein Objektiv besitzt. Dank Echtzeit-Monitoring entfielen aufwändige und gefährliche Vorort-Analysen. Mitarbeiter müssten nicht mehr bei jedem Störfall in bis zu 40 Meter Höhe steigen. Die Videosysteme zeichneten auch die Ereignisse vor einer Störung auf. Anhand der Videobilder könnten Störungen schnell und präzise bearbeitet werden, teilweise auch ohne dass ein Servicetechniker bei abgeschalteten Systemen die betreffende Regalgasse begehen muss. Ist eine Störungsbehebung vor Ort notwendig, lasse sich anhand der Videobilder bereits feststellen, wie viele Mitarbeiter, welche Schutz- und Hilfsmittel und welche Werkzeuge oder Ersatzteile benötigt werden.

Maritime Sicherheitswirtschaft

Mit Maritimer Sicherheitswirtschaft befasst sich Dr. Berthold Stoppelkamp im Fachorgan DSD (Ausgabe 3-2015, S. 28–32). Er weist darauf hin, dass seit Dezember 2013 nur noch vom BAFA gem. § 31 GewO zugelassene Sicherheitsunternehmen den Schutz von Seeschiffen unter deutscher Flagge ausüben dürfen. Das habe nun den nach der SeeBewachV zu erstattenden Erfahrungsbericht dem Bundestag vorgelegen (BT-Drucks. 18/5456). Der Bericht komme zu einem positiven Ergebnis. Das Zulassungsverfahren habe seine Stärke zur Qualitätssicherung gezeigt. Der Bericht enthalte nur minimale Änderungsvorschläge: Überflüssigkeit des jährlichen Personalüberprüfungsprozesses, wenn mit der Wachperson ein Arbeitsvertrag in Vollzeit abgeschlossen wurde; nähere Konkretisierung der Anforderungen an die „Auffrischungsschulungen"; Erläuterung der in der SeeBewachV aufgeführten Eskalationsstufen; Differenzierung der Ausrüstung des Teams und der einzelnen Wachpersonen. Der positiven Gesamtbeurteilung kann nach Überzeugung des Autors nicht zugestimmt werden: Die Anträge auf Zulassung seien extrem weit hinter den der Gesetzesbegründung prognostizierten Antragszahlen zurückgeblieben (nur 20 Anträge in den letzten zwei Jahren). Von den 2.700 Schiffen der deutschen Reeder würde nur in ca. 360 Fällen monatlich unter deutscher Flagge gefahren. Weltweit sei die Nachfrage nach maritimer Sicherheitsdienstleistung zurückgegangen. Die verbindliche Mindestteamstärke von vier Personen benachteilige in Deutschland ansässige Sicherheitsunternehmen im Markt. Es gäbe keinen anderen Staat, der dies gesetzlich vorschreibe. Ein weiteres großes Problem stelle die den Sicherheitsunternehmen auferlegte Pflicht dar, eine Kurzwaffe an Bord mitzuführen. Das zunächst strikte Verbot von „floating armouries" sei ein zusätzlicher Wettbewerbsnachteil. Stoppelkamp plädiert für eine Ausdehnung der Zulassungsdauer auf drei Jahre und für eine Novellierung der Regelungen der Teamstärke und der Ausrüstungsgegenstände.

Maschinensicherheit

Die Fachzeitschrift GIT behandelt in Ausgabe 9-2015, S. 102–104, neue Technologien im Explosionsschutz und beim Einsatz von sicherheitsgerichteten Funksystemen. Für den **Explosionsschutz** seien die Anforderungen an die Schaltgeräte, die für die Stellungsüberwachung von Schutztüren an Maschinen in Ex-Zonen gestellt werden, besonders anspruchsvoll – zum Beispiel bei der steute-Baureihe Ex AZ 16: ein Sicherheitsschalter mit getrenntem Betätiger. Der Maschinenbauer könne auch berührungslos wirkende Sicherheitssensoren einsetzen – zum Beispiel die Baureihe HS Si 4, die in Kombination mit einem Betätiger die Stellung von Schutztüren überwacht und sich u. a. durch besondere Schockfestigkeit auszeichne. Ebenfalls für extreme Umgebungsbedingungen, z. B. unter Tage, seien die Seilzug-Notschalter der Baureihe ZS 91 S entwickelt worden. Zu den ersten Anwendungen der neuen Geräte gehörten die Abraum-Förderbänder von Tunnelbohrmaschinen. Hier wirkten Seilzug-Notschalter als „verlängerter Not-Aus-Taster" über Distanzen bis zu 2 x 100 Meter. Auf ganz andere Anwendungen zielten Fußschalter mit sicherheitsgerichtetem Funkprotokoll. Er komme ohne elektrische Leitung aus. Der **Verzicht auf Leitung** biete den Vorteil, dass der Fußschalter flexibler zu positionieren ist, immer so, dass der Bediener beste Sicht auf den Prozess hat. Die Auswertung der Funksignale übernehme eine kompakte Kombination aus Funkempfänger und Sicherheitsrelaismodul, die im Schaltschrank eingebaut werden könne.

Trusted-Platform-Module als Tresor für Geräteidentitäten stellt GIT in der Aus-

gabe 9-2015, S. 112–115 vor. Gerade für die in Industrie 4.0-Konzepten geforderte dynamische Kommunikation komme den unverfälschten Identitäten eine besondere Bedeutung zu. Der IEEE-Standard 02 definiere sichere Geräteidentitäten. Er schreibe eine asymmetrische Kryptografie vor und unterscheide je Gerät zwischen einer initialen Identität (IDevID) sowie verschiedenen lokal signifikanten Identitäten (LDevIDs). Solche Identitäten könnten durch Trusted Platform Module (TPMs) vor dem Kopieren oder Fälschen geschützt werden. Ein TPM könne beliebig viele private Schlüssel von asymmetrischen Schlüsselpaaren so verwahren, dass diese ausschließlich von ihm verwendbar sind. Dazu enthalte jedes TPM ein individuelles Schlüsselpaar namens Endorsement Key (EK). Zum Zeitpunkt der Inbesitznahme des TPM durch einen Benutzer werde ein weiteres Schlüsselpaar im TPM generiert, der sogenannte Storage Root Key (SRK). SRK und EK würden dann im TPM gespeichert. TPMs enthielten einen hochwertigen Zufallszahlengenerator. Mit seiner Grundfunktion werde das TPM zum optimalen Tresor für Geräteidentitäten. Diese setzten sich gemäß IEEE 802.1AR aus einem asymmetrischen Schlüsselpaar mit einem Zertifikat zusammen. Die in der Automatisierungstechnik verwendeten Geräte seien in der Regel echtzeitfähig und müssten nach dem Start möglichst schnell verfügbar sein.

Near Field Communication (NFC)

Mit Sicherheitsproblemen beim Einsatz von NFC zur Zugangskontrolle, für Logistik, für elektronische Bezahlsysteme und in Ausweisdokumenten befasst sich in der Ausgabe 3-2015 von s+s report, S. 8/9, Dr. Ing. Timo Kasper, Kasper & Oswald GmbH. NFC-Karten böten keinerlei Verschlüsselungsfunktion. Der von ihm und David Oswald entwickelte Open Source **RFID-Kartenemulator Chamelion-Mini** sei ein kostengünstiges multifunktionales Werkzeug zur Prüfung der Sicherheit, Kompatibilität und Konformität von NFC-Systemen, ein frei programmierbares Gerät zur Emulation (Nachahmung des bekannten Verhaltens eines Systems durch ein anderes). Die Hardware ermögliche nebst Emulation nicht kryptografischer Karten auch die exakte Virtualisierung vieler nach ISO 14443 spezifizierter kryptografischer Karten. Der Autor erläutert weitere Eigenschaften des von ihm entwickelten Produkts.

Rechenzentrumssicherheit

Je heterogener die IT-Landschaft eines Data Centers, desto wichtiger sei ein gutes Zusammenspiel des Asset- und eines übergeordneten Infrastrukturmanagements, schreibt Uwe Bartmann, Siemens, in der Zeitschrift PROTECTOR, Ausgabe 9-2015 (S. 40/41). Neben der hohen Verfügbarkeit des Data Centers sollten auch die Mitarbeiter vor Brandgefahren geschützt werden. Hier böten Stromschienen Flexibilität für den Betrieb und eine Senkung des Brandrisikos. Tatsächlich seien Brände die häufigste Ursache für Betriebsunterbrechungen in Data Centern. Sogenannte Ansaugrauchmelder, die in den Rechnerräumen installiert werden, nähmen über ein Ansaugrohrnetz permanent Luftproben und untersuchten sie auf Rauchpartikel. Erkennt der Melder einen Brand, würden automatisch Gaslöschsysteme ausgelöst.

Die Zeitschrift PROTECTOR befasst sich in der Ausgabe 9-2015 (S. 42/43) mit der Ausfallsicherheit und **Business Continuity im Rechenzentrum.** Spannungsschwankungen könnten genauso wie Stromausfälle ohne Absicherung mit einer unterbrechungsfreien Stromversorgung (USV) die gesamte Infrastruktur und alle Prozesse in Unternehmen zum Stocken bringen. Ein USV-System fange innerhalb eines Jahres durchschnittlich mehr als 1.500 Zwischenfälle in der Stromversor-

gung ab. Das habe die Auswertung der Daten von mehr als 3.000 USV-Systemen durch Emerson Network Power ergeben. Bei der Aufstellung von Business Continuity-Plänen für Rechenzentren würden die Gefahren durch mögliche Stromausfälle oder Stromschwankungen oft erheblich unterschätzt. Um für einen Störfall optimal gerüstet zu sein, gelte es, bereits im Vorfeld grundlegende Entscheidungen zu treffen. Es müsse beispielsweise geklärt werden, ab wann die Last heruntergefahren wird oder ab wann ein zur Verfügung stehender Generator die Stromversorgung übernehmen soll. Im Business Continuity-Plan sollte auch festgelegt werden, wie viele Ersatzbatterien für den Notfall sofort verfügbar sein müssen. Um gegen Ausfälle im Rechenzentrum gerüstet zu sein, bedürfe es einer Lösung, die ein umfassendes Monitoring und Management der gesamten Infrastruktur erlaubt – also sowohl der IT- als auch der Facility-Komponenten.

In einer Beilage zur Zeitschrift <kes> vom August 2015 (S. 30/31) beschreibt Michael Leibner, Wagner Group GmbH, moderne **Brandbekämpfung** zum Schutz eines Hochsicherheits-Rechenzentrums. Für den IT-Bereich eigneten sich gasförmige Löschmittel, die rückstandsfrei einen Brand effizient bekämpften. Eine Bevorratung in Löschflaschenbatterien sei einfach und platzsparend, und im Löschfall verteile sich Stickstoff schnell und homogen ohne sichtbehindernden Nebel oder Rückstände im Raum. Das Problem, dass schnelles Einströmen des Gases durch die Löschdüsen einen Schalldruck von über 130 dB(A) erzeugte und erhebliche Schäden an Festplatten durch Vibration verursachte, habe man auf den Serverflächen des im Beitrag vorgestellten DARZ-Rechenzentrums durch den Einsatz von speziell entwickelten Schalldämpfern gelöst, die an den Löschdüsen montiert seien und den Schalldruck auf ca. 98 dB(A) verringerten. Eine weitere Besonderheit stelle die Softflutung dar. Durch Durchflussregler verringere sich die Größe der erforderlichen Druckentlastungsöffnungen erheblich.

Risikomanagement

Die FAZ berichtet im Verlagsspezial Consulting am 8. September über eine aktuelle Befragung der Prüfungs- und Beratungsgesellschaft EY unter rund 1.200 großen Unternehmen aus 63 Ländern nach der **Rangordnung von Risiken.** Eines zeige die Umfrage sehr klar: Die Unternehmen seien sensibler geworden für potenzielle Risiken und nähmen sehr viel mehr interne und externe Themen und Entwicklungen als mögliche Risiken wahr. Das sei die gute Nachricht. Das Management der Risiken könne vielerorts allerdings deutlich effizienter sein. Und die „Königsklasse" des Risikomanagements, nämlich Risiken und Chancen zu betrachten, das gelinge noch relativ wenigen Unternehmen. Ein strategisches Risiko zeichne sich dadurch aus, dass es nicht nur eine potenzielle Bedrohung beinhalte, sondern auch die Chance, bestimmte Unternehmensziele zu erreichen. Externe Risiken seien dagegen nicht wirklich kontrollierbar. Risiken zu identifizieren, zu managen und darauf zu reagieren, sollte in den täglichen Ablauf im Unternehmen eingebettet sein.

Jan Offerhaus, Risk Management Association e. V., thematisiert in der Zeitschrift PROTECTOR (Ausgabe 9-2015, S. 48/49) die **Verzahnung von Risikomanagement und Compliance.** Die Geschäftsführung des Unternehmens müsse in die Lage versetzt werden, aggregierte, einheitliche, aktuelle und schnell zu erfassende Informationen über die Gesamtorganisation zu erhalten. Dies sei Grundvoraussetzung für ein vorausschauendes Handeln im Sinne des Unternehmens. Oft stehe im Unternehmen das Risikomanagement mit dem Risikomanager auf der einen und der Bereich Compliance mit dem Compliance Officer auf der anderen Seite. Beide würden in ihrem Bereich ihr Bestes tun, aber leider nicht im Sinne eines einheitlichen Vorgehens. So bleibe das ganze Risikomanagement- und Compliance-Vorhaben bruch-

stückhaft, mit heterogenen Informationen ohne einen Gesamtzusammenhang für die Organisation und ihre Entscheider. Wichtig sei die Verknüpfung von Strukturen und Prozessen hin zu einem qualitativ hochwertigen Gesamtsystem namens Governance, Risk und Compliance (GRC).

Ansätze zur **Verankerung des Risikomanagements in Organisationen** beschreibt Andreas Wartenweiler, Helsana Versicherungen AG, in der Zeitschrift Sicherheitsforum (Ausgabe 4-2015, S. 50–53). Die Hauptzielgruppe für Sensibilisierung und Ausbildung seien Mitarbeitende und Management aus den operativen Einheiten (erste Verteidigungslinie). Mitarbeitende aus der „zweiten Verteidigungslinie" würden die erste Linie im Bewirtschaften von Risiken mit Modellen, Framework, Prozessgestaltung und -durchführung sowie Qualitätsprüfung unterstützen. Die interne Revision bilde eine unabhängige dritte Verteidigungslinie. Die Sicherheit von Organisationen, die ein hohes Gefährdungspotenzial aufweisen, aber dennoch weniger Unfälle produzierten als statistisch zu erwarten wäre, basiere gemäß Forschungsergebnissen grundsätzlich auf „achtsamem Handeln", das umschrieben werde als Zusammenspiel von Fehlertoleranz, Abneigung gegen Simplifizierung, Sensibilität für betriebliche Abläufe, Streben nach Flexibilität sowie Respekt vor fachlichem Wissen und Können. Die Luftfahrt habe die Ergebnisse dieser Untersuchungen mittels Human Factors Training in die Praxis umgesetzt. Es sei gezeigt worden, dass die gleichen Reaktionsmuster, Wahrnehmungsfehler und Kommunikationspannen sowohl in der Fliegerei als auch in Unternehmen ihre gefährliche Wirkung entfalten können. „Situational Awareness" unterstütze das Erkennen von „weak signals". Hierbei gehe es darum, frühzeitig die Situation um sich herum umfassend erfassen und einschätzen zu können, Hintergründe zu verstehen und Folgen abschätzen zu können. Einen umfassenden Schutz böten die aufgezeigten Maßnahmen allein noch nicht. Eine gewinnbringende Anwendung und Beibehaltung von Human Factors erfordere eine kontinuierliche Kommunikation, die Etablierung von Risikomanagement als Führungsinstrument im Alltag sowie die Förderung einer offenen Fehler- und Risikokultur mit konkreten Maßnahmen.

Dr. oec. Michael Phan, Kommunaler Zweckverband civitec, beschreibt in Ausgabe 4-2015 der Fachzeitschrift <kes>, S. 20–24, einen alternativen **Rechenweg für praxisnäheres Risikomanagement.** Schäden im IT-Umfeld seien meist nicht-linear und beschränkt. Die übliche einfache Risikoformel passe dazu nicht. Wer mehr Aufwand betreibt, um potenzielle Schäden zu modellieren, habe bessere Möglichkeiten, sein Risikomanagement sinnvoll zu begrenzen. Der Autor behandelt das lineare Risiko (Eintrittswahrscheinlichkeit x Höhe des erwarteten Schadens), die Ressourcenallokation zur Schadenserhebung, Schadenseintritt und -entwicklung und Maßnahmen zur Risikominderung unter Anwendung mathematischer Formeln. Der Nutzen von dynamisierten nicht-linearen Modellen zur Berechnung einzelner Schäden oder auch zur Ressourcenallokation in der Risikoberechnung könne aufgrund der Komplexität der Kalkulationen und der erforderlichen Informationsbeschaffung im Vorfeld zwar überdimensioniert erscheinen, würde sich aber gerade in Unternehmen mit einer Vielzahl deutlich unterschiedlicher Schadensszenarien empfehlen, da sich hierbei deutliche Kosteneinsparungen realisieren ließen. Leider erschließe sich die volle Wirksamkeit solcher Modelle erst dann, wenn man dazu in der Lage ist, realistische Aussagen zur maximal akzeptierten Nichtverfügbarkeit eines Systems zu treffen, die dann auch Niederschlag in Service Level-Agreements und Operational Level-Agreements finden sollten.

Schließsysteme

Die Zeitschrift PROTECTOR veröffentlicht in Ausgabe 9-2015 eine Marktübersicht über 116 mechatronische Schließsysteme von 50 Anbietern (S. 32–33). Je Produkt seien 48 Kriterien abgefragt worden.

Ein elektronisches **Schließsystem für Anlagen in Wohnhäusern und kleineren Objekten** (Blue Compact von Winkhaus) stellt die Fachzeitschrift GIT in Ausgabe 9-2015, S. 46/47 vor. Es mache vieles anders – das zeige sich bereits bei der Ersteinrichtung. Installiert und verwaltet werde das System einfach via Smartphone-App, die auf iOS und Android-Basis zum kostenlosen Download im App Store zur Verfügung stehe. Ein Tutorial erkläre dabei jeden Schritt von Anfang an. Schließanlagen mit bis zu 25 Zylindern und 99 Schlüsseln ließen sich mit dem Zutrittssystem organisieren. Informationen zwischen der App und dem Blue Compact Masterkey würden über Bluetooth übertragen. Die elektronischen Zylinder würden mittels Masterkey programmiert. Alle relevanten Daten lägen aus Sicherheitsgründen stets auf dem Masterkey.

Sicherheitsgewerbe

Reinhard Rupprecht, Berater Securitas Deutschland, plädiert im Fachorgan DSD (Ausgabe 3-2015, S. 6–9) für die **Integration von Dienstleistungen und Technik** im Sicherheitsgewerbe. Gründe für die Integration würden sich geradezu aufdrängen: die enge funktionale Verknüpfung von Sicherheitsdienstleistung und Sicherheitstechnik, deren zunehmende Effizienz, die Erzielung der im Einzelfall kostengünstigsten Lösung und der Wunsch vieler Kunden nach einer Gesamtsicherheitslösung „aus einer Hand". Der Übergang vom Angebot von Einsatzstunden für vom Kunden vordefinierte Sicherheitsfunktionen zum Angebot integrierter Sicherheitssysteme bedeute für Sicherheitsunternehmen einen Paradigmenwechsel, den das Unternehmen nur mit einem konsequenten Change-Management bestehen könne. Vorausgesetzt würde eine hohe technische Kompetenz des Sicherheitsdienstleisters, um den Kunden durch Professionalität und Zuverlässigkeit zu überzeugen. In größeren Unternehmen müsse es einen Chief Technology Officer (CTO) geben. Sicherheitstechnische Experten müssten auch in den einzelnen Niederlassungen für Sicherheits-Scans, Angebotserstellung und Kundenberatung und zur Einweisung von Einsatzkräften für den Betrieb technische Systeme zur Verfügung stehen. Ebenso wie die Sicherheitsdienstleistung optimiere und beschleunige die Digitalisierung die Infrastruktur des „neuen Sicherheitsunternehmens, Einsatzvorbereitung und -nachbereitung, Informationssammlung, -verarbeitung und -weitergabe. Die Integration der Sicherheitstechnik in das vom Sicherheitsdienstleister angebotene Leistungsportfolio werde durch Branchensegmentierungen im Sicherheitsunternehmen gefördert.

Sicherheitskultur

Dr. Johannes Wiele, Managing Security Consultant, befasst sich in Ausgabe 4-2015 der Fachzeitschrift <kes> mit **Begriff und Inhalt der Sicherheitskultur.** Es sei einer jener Begriffe, die um so stärker schillern, je genauer man sie zu fassen versucht. Der Autor versucht eine Definition, beschreibt Probleme bei der Konzeption und Umsetzung der Sicherheitskultur. Eine existierende Organisations- oder Sicherheitskultur habe ein gewaltiges Beharrungsvermögen. Will man sie ändern, müsse man die Mehrheit innerhalb der Organisation überzeugen, für eine breite Akzeptanz sorgen, die abzulösenden Praktiken mit ihren negativen Folgen exakt benennen und sie möglichst dennoch nicht vor all jenen abschätzig behandeln, welche

die entsprechenden Verhaltensweisen seit Langem aus Tradition oder „guten Gründen" gelebt haben. Um eine Kultur zu beeinflussen, sei deshalb viel Erklärungsarbeit zu leisten, und man müsse für die Ziele werben, statt sie zu verordnen.

Sicherheitsmarkt

PROTECTOR veröffentlicht in der Ausgabe 9-2015 ein **Branchenbarometer der Sicherheitstechnik,** an dem sich Interessierte seit Juni 2015 beteiligen konnten (S. 10/11). 26 Prozent der Teilnehmer erwarten in den nächsten zwölf Monaten einen Marktzuwachs von 1–2 Prozent, 27 Prozent von 3–5 Prozent, 19 Prozent von 5–8 Prozent und 15 Prozent von 5–8 Prozent. Die höchsten Wachstumsraten werden branchentypisch im Bereich Video gesehen: Über die Hälfte der Befragten sehen ein Wachstum jenseits der 5 Prozent als realistisch an. Hinsichtlich des eigenen Umsatzes erwarten 52 Prozent ein Wachstum zwischen 1 und 5 Prozent. 40 Prozent gehen von einem Wachstum von über 5 Prozent aus. 51 Prozent der teilnehmenden Unternehmen erwarten leicht fallende Preise, 49 Prozent leicht steigende Preise bis maximal 4 Prozent.

Sicherheitsplanung

Sicherheitsberater.de nennt am 3. September ein paar Beispiele, bei denen **Unsauberkeit und Unordnung** unmittelbar zu erheblichen Sicherheitsrisiken führen können: Staubfreiheit und Sauberkeit gehöre in sogenannten „Reinräumen", die der Fertigung von Halbleitern oder Lasern dienen, zur wichtigsten Produkteigenschaft. Werkschutzverantwortliche ohne ein gewisses Verständnis für Ordnung und Sauberkeit würden es schwer haben zu erkennen, dass der „provisorisch" gelagerte Sperrmüll vor dem Werkszaun auch von Einbrechern hervorragend als Kletterhilfe zu gebrauchen ist, oder dass von Chemikalienresten oder Elektrogeräten eine ernsthafte Gefahr ausgeht. In Gebäuden könnten Kisten, die Fluchttüren versperren, oder der „F-90-Keil", der ein automatisches Schließen der Brandschutztür verhindert, schnell in einer Katastrophe enden.

Spionage

„Berlin als europäische Hauptstadt der Agenten" lautet eine Überschrift in der September-Ausgabe des Behörden Spiegel. Das ehemalige Gästehaus der DDR-Regierung diene als Außensitz für die Wirtschaftsabteilung der chinesischen Botschaft. Dort befände sich die zentrale technische Einrichtung für den geheimen Nachrichtenaustausch mit Peking, aber auch die Abhöreinrichtungen für die deutsche Hauptstadt sowie die Geheimdienstabteilung, zumindest die inoffizielle. Den größten Vorteil in Berlin hätten allerdings die Russen. Sie verfügten über eine riesige Botschaftsanlage an der Straße Unter den Linden und auf der Rückseite über große Wohnkomplexe für Mitarbeiter. Jeder chinesische Student, Professor oder Geschäftsmann müsse sich spätestens nach vier Wochen in Deutschland bei der chinesischen Botschaft gemeldet haben und erhalte einen Fragebogen. Das chinesische System gelte unter allen Geheimdiensten als Erfolgsmodell. Ein ganz besonderes Kapitel seien die Israelis mit dem Auslandsgeheimdienst Mossad. Ihre Aufklärer seien auch in Deutschland überall. Neben den harten Killer-Methoden des Mossads verfüge der israelische Geheimdienst auch über smarte Varianten. Aber auch der Inlandsgeheimdienst der Israelis sei in Berlin durchaus sichtbar. Cyberspionage sei auch deswegen für viele Geheimdienste attraktiv, weil sie preiswert, ohne Sicherheitsrisiko und effektiv zu organisieren ist.

Sprachalarmierung

Mit der **akustischen Brandalarmierung** befasst sich die Fachzeitschrift GIT in Ausgabe 9-2015, S. 92–94. Der Planung von Signalisierungsbereichen und der Erstellung eines entsprechenden Alarmierungskonzeptes komme eine wachsende Bedeutung zu. Um die Wahrnehmbarkeit der Signale zu erhöhen, seien sowohl der Alarmierungston in der DIN 33404-3 als auch die Mindestschallpegeldifferenz zum Umgebungsschallpegel im gesamten zu planenden Signalisierungsbereich in der DIN VDE 0833-2 geregelt. Anforderungen an die akustischen Signalgeber an Brandmeldeanlagen würden in den Normen DIN EN 54-3 und DIN VDE 0833-2 und DIN 14675 festgelegt. Der Schallpegel und damit die Lautstärke eines Schallgebers sei nicht bei allen implementierten Tönen identisch. Zur Planung müsse deshalb immer der Schallpegel des später verwendeten Tons zugrunde gelegt werden. Konkret sei für eine Planung und Projektierung der jeweilige Signalisierungsbereich eines Gerätes zu bestimmen, der sich folglich aus dem vorliegenden Umgebungsschallpegel (Lärmkataster) in Verbindung mit der Abstrahlcharakteristik ergebe. Die Planung ausschließlich gemäß Marketingdatenblättern und/oder Erfahrungswerten führe oftmals dazu, dass in der Projektierung eine zu geringe Anzahl oder ihrer Leistung zu schwache Signalgeber eingesetzt würden. Betrachtet man die Leistungsfähigkeit der Geräte, so weise die elektromagnetische Schallerzeugung gegenüber der Piezo-Technologie einen weitaus größeren Signalisierungsbereich auf.

Wolfgang Unger, Novar, gibt in der Ausgabe 9-2015 der Zeitschrift GIT (S. 96–99) einen Überblick zum aktuellen Stand der **Normen für Sprachalarmierung.** Die DIN VDE 0833-4 sei in den letzten Jahren überarbeitet worden und in der neuen Version am 1. Oktober 2014 in Kraft getreten. Ziel dieser Überarbeitung sei es gewesen, Unklarheiten aus der Vorgängerversion zu beseitigen, Einflüsse aus der Praxis mit einzubringen und auf geänderte Rahmenbedingungen zu reagieren. Die markanteste Änderung betreffe die Ausfallsicherheit, insbesondere die Sicherheitsstufen. Für die Festlegung einer Sicherheitsstufe seien nach wie vor die möglichen Gefährdungsszenarien entscheidend. Eine Änderung bezüglich der Sicherheitsstufen beziehe sich auf das Verhalten im Fehlerfall. Bei Sicherheitsstufe 2 werde nur noch auf die Sprachverständlichkeit Bezug genommen. In der neuen Version bei den Sicherheitsstufen 2 und 3 finde man eine Anmerkung, in der auf die A-B-Verkabelung hingewiesen wird. Diese sei darüber hinaus in Kapitel 3.1.4 aufgenommen worden.
Die neue EN 50849, die „elektroakustische Notfallwarnsysteme" behandelt, ersetze die EN 60849. Die Einführung der DIN 14675 sei für die Sprachalarmierung reibungslos und unproblematisch erfolgt. Derzeit gebe es in ganz Deutschland ein flächendeckendes Netz von Planungsbüros und Errichterbetrieben für die Sprachalarmierung, die nach DIN 14675 zertifiziert sind.

Unternehmenssicherheit

Die Fachzeitschrift GIT weist in Ausgabe 9-2015, S. 24–27, auf eine von YouGov im Auftrag von Vanderbilt durchgeführte Umfrage in fünf europäischen Ländern hin. Danach habe jedes dritte deutsche KMU finanzielle Schäden, Betriebsunterbrechungen oder anderweitige Beeinträchtigungen als direkte Folge von Verstößen gegen seine physische Sicherheit oder von Cyberangriffen zu beklagen. Dabei sei die Anzahl der Verstöße gegen die physische Sicherheit mehr als dreimal so hoch wie der Anteil der virtuellen Übergriffe. Dass 39 Prozent der befragten deutschen Unternehmen keine elektronischen Sicherheitslösungen wie Zutrittskontrollsysteme, CCTV-Anlagen oder EMA im Einsatz haben, gebe Anlass zu großer Besorgnis.

Videoüberwachung

Bertrand Völckers, Flir Commercial Vision Systems, und Lothar Liebelt, Journalist, erläutern den **Perimeterschutz eines Solarparks** mit einer Gesamtfläche von über 16 Hektar in Spanien in der Zeitschrift PROTECTOR, Ausgabe 9-2015, S. 37. Es seien 21 Wärmebildkameras mit einer Auflösung von 320 mal 240 Pixeln entlang eines Drahtzauns an zwei bis drei Meter hohen Masten installiert worden. Die Kameras ließen sich über digitale und analoge Netzwerke steuern. Digital Detail Enhancement liefere unabhängig von den vorherrschenden Wetterbedingungen stets scharfe Bilder mit den dazu passenden Kontrastwerten. Die Wärmebildkameras seien mit einem Einbruchserkennungssystem gekoppelt und gemeinsam mit diesem an einer zentralen Alarmstation angeschlossen. Tiere würden vom System von vornherein als „zulässige Eindringlinge" eingestuft.

Wie GIT in der Ausgabe 9-2015 (S. 28/29) berichtet, verwendet Securitas Österreich in der Sicherheitsleitstelle die intelligente **Software des Kiwivision Video Control Centers,** die die Handhabung der Systeme unterschiedlicher Betreiber vereinfache, indem es sie in einem zentralen Gesamtsystem vereint. Das Projekt spare sowohl Zeit wie Kosten, zudem sei es wesentlich einfacher, Mitarbeiter auf ein einheitliches System zu spezialisieren und erhöhe im Ernstfall die Reaktionsgeschwindigkeit. Die künstliche Intelligenz des Systems mache es möglich, relevante Informationen simultan mit dem Geschehen herauszufiltern. Infolgedessen werde die Bilderflut, mit der die Leitstandmitarbeiter konfrontiert werden, auf das Wesentliche reduziert.

Überspannungsschutz für Videoüberwachungsanlagen thematisiert GIT in Ausgabe 9-2015, S. 74/75). Grundlage für die Planung und die Installation der Blitzschutzmaßnahmen bildeten die Blitzschutz-Normen der Reihe VDE 0185-305. Bei der Auslegung der Ableitungen des äußeren Blitzschutzes der Kamera sei darauf zu achten, dass zwischen der Ableitung der Blitzschutzanlage und der Kamera mit deren Versorgungsleitungen ein genügend großer Trennungsabstand eingehalten wird. Um Störungen der Überwachungskameras durch Blitzentladung im elektromagnetischen Feld zwischen der Überwachungszentrale und den Kameramasten zu vermeiden, sollten Überspannungsschutzgeräte zum Schutz der Versorgungsspannung und des Videosignals der Kamera eingesetzt werden.

Über einen **Leitfaden** zur Planung, Projektierung und Umsetzung von Videoanlagen berichtet Markus Groben, Groben Ingenieure GmbH, in einem im September veröffentlichten Videoüberwachung-Special von PROTECTOR (S. 34/35). Experten hätten in einem Arbeitskreis des Verbandes für Sicherheitstechnik ihre Erfahrungen zusammengetragen. Der Leitfaden könne über den VfS unter www.vfs-hh.de kostenlos bezogen werden. Der Autor skizziert die Zielsetzung, die Projektgliederung, Lastenheft und Pflichtenheft, eine Risikodefinition und eine Kosten/Nutzen-Analyse.

In dem Videoüberwachung-Special der Zeitschrift PROTECTOR vom September 2015 stellt Jie Fourmont, Digivod GmbH, maßgeschneiderte Sicherheitslösungen mit PSIM **(Physical Security Information Management)** vor (S. 36/37). Die Idee von PSIM sei es, mit unabhängiger Software samt flexibler Architektur und moderner GUI (Graphical USER Interface) die Integration von beliebigen Systemen zu ermöglichen. In einer zentralen Karte würden Kameras, Gebäude, Zugangskontrollen und Alarmsysteme hinterlegt. Die Bedienung der Sensoren erfolge per Drag und Drop und per Mausklick. Fourmont beschreibt die grafische Oberfläche, den Lageplan und die flexible Architektur. Videomanagement-Softwarelösungen mit einfacher Oberfläche und flexiblen Architekturen seien prädestiniert für Integrationen.

Mit **Speed Dome-Kameras** befasst sich in dem Special Videoüberwachung der Zeitschrift PROTECTOR vom September 2015 Volkhard Delfs, Panasonic Marketing Europe GmbH, S. 38/39. Zu den Funktionen dieser Kameras gehörten unter anderem die Möglichkeit zum nahtlosen Drehen um 360 Grad, oftmals auch sehr leistungsfähige Zoomobjektive. Die kompakte Bauform des Kamerakopfes erlaube sehr schnelle Schwenk/Neige-Bewegungen mit vernachlässigbaren mechanischen Schwingungen im Gegensatz zu andersartigen Schwenk/Neige-Köpfen. Allerdings müssten die Kameraköpfe vor gewissen Umwelteinflüssen geschützt werden, etwa vor Staub, Feuchtigkeit oder korrosiven Stoffen. Je nach Umgebungsbedingungen sollte die Kuppel ein- bis zweimal jährlich gereinigt werden. Der Nachteil der Halbkugelrundung der Kuppel, die eine direkte horizontale Ausrichtung des Objektivs kaum ermögliche, könne durch eine veränderte Kuppelgeometrie aufgehoben werden, welche die typische Halbkugel mit einem Zylinder kombiniert.

Analoge Videosysteme im IP-Zeitalter thematisiert Marcus Fiederling, UTC Fire & Security Deutschland GmbH, im Videoüberwachung-Special von PROTECTOR (September 2015, S. 40/41). Die Lösung heiße HD-TVI (High Definition Transport Video Interface), die einen schrittweisen und damit schnellen, kostengünstigen Übergang von analoger auf IP-Videotechnik ermögliche. Analoge Kameras könnten weiterhin genutzt oder stückweise durch HD-TVI Kameras ausgetauscht werden, wobei das Videosignal weiterhin über die bestehende Koax-Kabelstruktur übertragen wird. Ein HD-TVI Recorder erkenne automatisch beide Signalarten und zeichne diese auf. Der Autor beschreibt HD-TVI und die Migration.

Kamera-Kombinationen im Perimeterschutz behandelt Andreas Wolf, Dallmeier Electronic GmbH & Co. KG, in dem Videoüberwachung-Special von PROTECTOR (September 2015, S. 42/43). Durch die Kombination von Thermalkameras und Multifocal-Sensortechnologie ergäben sich neue Möglichkeiten für die Analyse, Objektverfolgung und Erkennung von Personen am Perimeter. Mit der Multifocal-Technologie seien große Distanzen überschaubar. Nach einem Alarm könne ein Objekt in mehreren Sichten automatisch visualisiert und optimal observiert werden. Der Autor erläutert die Grenzen der Thermal-Technologie und ihre Kombination mit Multisensorkameras.

Die enormen Fortschritte bei der Bildqualität führten in der Videoüberwachung zu einer substanziellen Zunahme des Datenvolumens. Pieter von de Looveren, Bosch Security Systems, sieht daher in einem intelligenten und effizienten Management sowie Technologien zur **Datenreduzierung ohne Qualitätsverlust** die Möglichkeit zu handhabbaren Videolösungen (PROTECTOR, Videoüberwachung-Special, September 2015, S. 42–44). Eine intelligente Bildanalyse trage durch Ausblenden unwichtiger Details sowie Abstrahierung zur Reduzierung des Datenvolumens bei. Bosch habe eine selektive Komprimierung entwickelt, durch die bis zu acht Bildbereiche mit unterschiedlichen Kompressions-Parametern konfiguriert werden könnten. Die Content Based Imaging Technology (CBIT) kombiniere die Informationen des Sensors, der Bildverarbeitung, des Encoders sowie der intelligenten Videoanalyse, um jede Szene in optimaler Bildqualität darzustellen. Um Vorfälle einigermaßen sicher erkennen zu können, könne bei der Durchsicht des Videomaterials maximal mit vierfacher Geschwindigkeit gearbeitet werden.

Verschlüsselung in der Videomanagementsoftware behandelt Dr. Jürgen Hösel, Accellence Technologies GmbH, im Videoüberwachung-Special der Zeitschrift PROTECTOR (September 2015, S. 48/49). Mit einer geeigneten Software mit Verschlüsselung könne zuverlässig sichergestellt werden, dass die Daten nicht von Dritten

manipuliert werden und die erforderlichen Sicherheitsstandards bei Erfordernis bereits ab der Kamera eingehalten werden. Durch eine Absicherung mittels End-to-End-Verschlüsselung sei ein Zugriff auf die Daten nur durch autorisierte Mitarbeiter möglich, die im Besitz des Dongles mit dem privaten Schlüssel sind. Bei höheren Sicherheitsanforderungen könne die Freigabe der Video- und Audiostreams zusätzlich an ein Mehraugen-Prinzip gekoppelt werden.

Timo Sachse, Axis Communications GmbH, befasst sich in dem Videoüberwachung-Special von PROTECTOR (September 2015, S. 50/51) mit dem **„Mythos Bildqualität in Zeiten von 4K Ultra HD"**. Die Ursache für den geringen Detailgrad des Bildmaterials liege zumeist in der verwendeten Kompressionsmethode. H.264, der Kompressionsstandard der Videosicherheitsbranche, sei zwar prinzipiell sehr leistungsfähig und flexibel. Jedoch ergäben sich bei falscher Anwendung Risiken. Höhere Bitraten seien eine Herausforderung. Dies beginne bereits in der Kamera: Hier sei für höhere Bitraten mehr Arbeitsspeicher und Prozessorleistung erforderlich. Auch das Netzwerk und die Datenspeicherung seien höheren Anforderungen ausgesetzt. Die künstliche Begrenzung der Bitrate durch eine sogenannte Maximale Bitrate (MBR) sei die am weitesten verbreitete Methode. Die Axis Zipstream Technologie trage der Natur der Bitrate Rechnung: Statt die Bitrate in ein Korsett zu zwingen, analysiere der Algorithmus das gesamte Bild in Struktur und Bewegungsanteilen. Überall dort, wo Bewegung in einem strukturierten Bereich vorliegt, werde die Default Kompression der Kamera nicht verändert. Sei ein Bereich statisch, werde die Kompression in den Teilen moderat angehoben, die eine Struktur besitzen, und deutlich verstärkt, wenn keine erkennbare Struktur vorliegt. Im Lowlight-Bereich helfe eine Rauschunterdrückungskomponente, die Bitrate erheblich abzusenken.

Videoüberwachung am Bahnhof ist das Thema von Cornelia Groß, Securiton GmbH, in dem Videoüberwachung-Special der Zeitschrift PROTECTOR vom September 2015, S. 52/53. Beim Einsatz von Videokameras durch die Münchener Verkehrsgesellschaft identifiziere der IPS Videomanager mithilfe intelligenter Algorithmen vom Normalfall abweichende Ereignisse. Die Bildanalysen würden den Unterschied zwischen großen Objekten wie einem Zug und kleinen Objekten, wie einer verirrten Taube oder eines Menschen erkennen, bei dem dann der Alarm auslöst. Halten sich Personen in Winkeln mit wenig Publikumsverkehr oder an sensiblen Stellen wie dem Fahrkartenautomaten auf, sorge die Loitering Detection nach einer frei definierbaren Zeitspanne für eine Echtzeit-Alarmierung. Bei der „Outdoor Detection" spiele das Zonenkonzept seine Stärken aus: Die Software erzeuge nur dann einen Alarm, wenn sich beispielsweise eine Person aus der Erfassungszone heraus und in die Alarmzone hinein begibt. Das Modul „IPS Public Transport Protection" erkenne ein- und ausfahrende Züge, analysiere das Verhalten von Fahrgästen am Bahnsteig und identifiziere Personen, die gewollt oder gar ungewollt in das Gleisbett springen bzw. fallen.

Das Special Videoüberwachung der Zeitschrift PROTECTOR vom September 2015 enthält **Marktübersichten** über 118 Kameramodelle von 41 Anbietern mit Angaben zum Videostandard, der Signalverarbeitung, der aktiven Bildelemente und der Betriebstemperatur; über 168 Netzwerkkameras von 60 Anbietern mit Angaben zum Videostandard, der Signalverarbeitung und dem Betriebssystem; über Videomanagement-Software mit 117 Lösungen von 62 Firmen und Angaben zur Audioaufzeichnung, der software-basierten Bewegungsdetektion, einem Mehrmonitorbetrieb sowie Vor- und Nachalarmspeicher; über 98 Monitorgeräte von 34 Anbietern mit Angaben zum Seitenverhältnis, der Auflösung, einem integrierten Lautsprecher und dem Gehäusematerial (S. 54–61).

„Banken wollen per Video identifizieren", titelt der Behörden Spiegel in seiner September-Ausgabe. In dem von der BaFin inzwischen genehmigten Verfahren erfolge die **Identifizierung mittels eines Videochats.** Demnach ist die (juristische) Person auch dann anwesend, wenn sie über ein Video identifiziert wird. Des Weiteren müssten sich beide Vertragspartner damit einverstanden erklären, dass das Gespräch aufgezeichnet wird. Außerdem müsse die Vor- und Rückseite des Personalausweises in die PC- oder Laptop-Kamera gehalten werden, um sich so ausweisen zu können. Bisher habe wegen der Geldwäschekontrolle und der Sicherheit insgesamt die Regel gegolten, dass zwar Bankgeschäfte online durchgeführt werden können, aber immer eine persönliche Überprüfung des Kontoinhabers – bei einer Filiale oder per Post-Identverfahren – erforderlich ist.

Impressum

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

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

Herausgeber:
Manfred Buhl, Vorsitzender der Geschäftsführung, Düsseldorf

Verantwortlicher Redakteur:
Bernd Weiler, Leiter Kommunikation und Marketing

Beratender Redakteur:
Reinhard Rupprecht, Bonn

focus.securitas.de

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

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

E-Mail: info@securitas.de