Focus on Security

Ausgabe 08, August 2015

SECURITAS

Inhalt

Anschläge ... 3
Baustellensicherung ... 3
Biogasanlagensicherheit ... 3
Brandschutz ... 3
Cloud Computing ... 5
Corporate Security Officer (CSO) ... 5
Falschgeld ... 6
Gefährdungshinweise Türkei ... 6
Industrie 4.0 ... 6
IT-Sicherheit ... 7
IuK-Kriminalität ... 9
Korruption ... 11
Krankenhaussicherheit ... 12
Mobile Endgeräte ... 12
Netzsicherheit ... 13
Notruf- und Service-Leitstellen ... 13
Organisierte Kriminalität ... 13
Raub ... 14
Raubkopien ... 14
Sicherheitsgewerbe ... 14
Spionage ... 15
Steuerhinterziehung ... 15
Transportdiebstahl ... 15
Verfassungsschutz ... 16
Videoüberwachung ... 16
Zutrittskontrolle ... 17

Anschläge

In der Nacht zum 17. Juli haben Unbekannte drei Firmenwagen in Berlin angezündet. Die Polizei gehe von linksextremistisch motivierten Taten aus, meldet tagesspiegel.de am 17. Juli. Zwei der angezündeten PKW gehörten der Carsharing-Tochter Flinkster der Deutschen Bahn. Flinkster-Autos seien in den vergangenen Jahren vor allem in Stuttgart angezündet worden. Ferner sei ein PKW der Marke Skoda im Stadtteil Fennpfuhl angezündet worden, der dem Sicherheitsunternehmen WISAG gehört habe. Auch diese Firma sei schon mehrfach von Linksextremisten angegriffen worden.

Der ASW berichtet am 29. Juli, die Berliner Polizei sei am 11. Juni über ein brennendes Fahrzeug der Deutschen Telekom und am 13. Juli über den Brand an einem Firmenwagen von Siemens informiert worden. Zu beiden Bränden sei am 13. Juli eine anonyme Selbstbezichtigung erfolgt.

Baustellensicherung

Sebastian Höcke, EFB Elektronik, befasst sich in der Ausgabe 4-2015 der Zeitschrift Security insight (S. 40/41) mit der **Videoüberwachung** von Baustellen per SIM-Karte übers Mobilfunknetz. Es sei eine Vielzahl von UMTS-fähigen Kameras verfügbar, die keinen direkten Netzwerkanschluss mehr benötigen. Stattdessen sendeten sie die Videodaten einfach mittels SIM-Karte übers Mobilfunknetz. Dadurch könnten sie einfacher installiert werden und ließen sich flexibel und ortsunabhängig einsetzen. So werde beweiskräftiges Bildmaterial erstellt. Kommt es zu auffälligem Verhalten, etwa nächtlicher Bewegungen auf der Baustelle, meldeten die Kameras dies per http-Befehl an den zentralen Aufzeichnungsserver. Dieser ändere daraufhin die Abrufeinstellungen für einen definierten Zeitraum auf einen hochauflösenden Videostream mit einer Pixeldichte von mindestens 160 Pixeln pro Meter. Ergänzend zur automatisierten Streaming-Einstellung bestehe zudem die Möglichkeit, dass die Kamera im Alarmfall eine automatische E-Mail an den zuständigen Administrator generiert. Notwendig sei es, einen eindeutigen Zugang zu realisieren, über den der Kamerazugriff auch bei wechselnder IP-Zuweisung kontinuierlich sichergestellt ist.

Biogasanlagensicherheit

Schadenverhütung bei Biogasanlagen thematisiert Dipl.-Ing. Martin Paproth, öffentlich bestellter und vereidigter Sachverständiger, in der Fachzeitschrift s+s report, Ausgabe 2-2015, S. 57–59). Schon 2009 habe die Kommission für Anlagensicherheit (KAS) nach Auswertung von Sachverständigenberichten festgestellt, dass ca. 80 Prozent aller Biogasanlagen schwere technische Mängel aufweisen. Neben sicherheitstechnischen Mängeln seien vor allem Bedienungsfehler und Instandhaltungsdefizite als besonders häufige Ursachen im Schadengeschehen identifiziert worden. Bedeutung hätten auch ungeeignete Anlagenkomponenten, die dem Betrieb und den Prozessmedien nicht gewachsen sind. Bereits im April 2015 sei die Technische Regel Gefahrstoffe (TRGS) 529 in Kraft getreten, die den Umgang mit Gefahrstoffen bei Tätigkeiten in Biogasanlagen konkret regelt. Zumindest durch die inhaltliche Verzahnung der TRGS 529 mit dem Brand- und Explosionsschutz ergebe sich daraus auch eine Wirkung für die Schadenverhütung.

Brandschutz

Ausgabe 2-2015 der Fachzeitschrift s+s report enthält mehrere Beiträge zu Brandschutzthemen. Thomas Timke, Karlsruher Institut für Technologie, befasst sich mit der

Sicherheit von Lithiumionen-Batterien (S. 8/9). Schädigungen wie Überladung oder Tiefentladung verursachten in den Zellen irreversible Schäden, die sofort oder nach weiterem Betrieb zur Freisetzung leicht entzündlicher Gase oder direkt zum Brand führen können. Der Transport von Lithiumionen-Batterien in der Größe von PV-Heimspeichern falle immer unter das Gefahrgutrecht mit der Gefahrgutklasse 9. Das Gerücht, Lithium-Eisen-Phosphat-Zellen könnten nicht brennen, nicht überladen werden oder seien sogar komplett eigensicher, stimme nachweislich nicht. Jeder Schritt – Transport, Installation und Betrieb bis zur Entsorgung – müsse verstanden werden. Für Einkäufer und Kunden seien entsprechende Standards in Sicht, die eine Orientierung erlaubten.

Stefan Kratzmeir, VdS Schadenverhütung, erläutert die Richtlinien VdS 3188 für **Wassernebel-Systeme** (S. 14–16). Die seien für ganz bestimmte Anwendungen eine mögliche Alternative zu Sprinkler-, Sprühwasser- oder Gaslöschanlagen. Basis hierfür seien die in Kürze erscheinenden Richtlinien für Planung und Einbau von Wassernebel-Sprinkler und -Löschanlagen (VdS 3188). Zusammen mit dem jeweiligen systemspezifischen P&E-Handbuch würden Planern, Betreibern und Herstellern damit kompakte und transparente Richtlinien für Planung, Einbau, Betrieb und Instandhaltung geboten. Neue VdS-Richtlinien für Planung und Einbau von **Gaslöschanlagen** behandelt Marcel Mager, VdS Schadenverhütung (S. 18–23). Zurzeit existieren insgesamt vier VdS-Regelwerke für Planung und Einbau, die sich mit dem Aufbau und der Auslegung von Gaslöschsystemen beschäftigen: VdS 2380, 2381, 2093 und 3518. Als wesentliche Änderung bei der Überarbeitung der Richtlinien VdS 2380 und 2381 habe VdS durch ein Klassifizierungssystem die Flexibilität der Richtlinien erhöht. Der Autor beschreibt die Klassifizierungsmöglichkeiten Aufstellung der Flaschenbatterie, elektrische Blockierung und Betriebsmittelabschaltung. Zusammenfassend ließen sich die Änderungen wie folgt beschreiben: inhaltliche Überarbeitung (Einführung der Klassifizierung, neues Schutzkonzept, neue und überarbeitete Kapitel) sowie übergreifende Strukturanpassung (Bausteine ähnlich zur VdS CEA 4001 und gleicher Aufbau innerhalb der Gasregelwerke). Die **Ansteuerung von Feuerlöschanlagen** thematisiert André Lickefett, Minimax Viking Gruppe (S. 26–33). Die Ansteuerung und die damit zusammenhängende Erkennung von Bränden folgten einem ganzen Kompendium von Regelwerken. Unterteilen ließen sich diese im Wesentlichen in die vier Bereiche Komponenten, Fachkompetenz, Planung/Einbau und Betrieb. Die Leitrichtlinie für die Ansteuerung von Löschanlagen sei die VdS 2496, 2014 als Neufassung publiziert. Gegenüber der vorhergehenden Fassung gebe es grundsätzliche Änderungen, die der Autor erläutert. Er befasst sich ferner mit technischen Varianten der Steuereinrichtungen, dem typischen Aufbau elektrischer Steuereinrichtungen, der Standardschnittstelle Löschen, mit Kooperation und Verantwortlichkeiten, Informationsfluss und Dokumentation, mit technischen und physikalischen Einflussfaktoren, Fehlern zum Beispiel bei der Energieversorgung, bei der Abschaltung von Betriebsmitteln und deren Vermeidung.

Den Brandschutz in **Einrichtungen zur Betreuung bzw. Pflege** von Personen mit Pflegebedürftigkeit oder Behinderung behandelt Bernd Manning, VdS Schadenverhütung (S. 24/25). In der VdS-Publikation 3402 würden anhand der Risikomerkmale von Betreuungseinrichtungen Maßnahmen des baulichen, anlagentechnischen und auch organisatorischen Brandschutzes beschrieben, ebenso werde auf den abwehrenden Brandschutz eingegangen. Für mehr Sicherheit bei **Heißarbeiten** plädiert Ing. Mag. Gerald Netal, Risks Experts Risiko Engineering GmbH (S. 34–37). Brandgefahren könnten auftreten durch: offene Schweißflammen, elektrische Lichtbögen, Lötflammen, Schweiß-, Schneid- und Schleiffunken, abtropfendes glühendes Material, Wärmeleitung durch stark erhitzte

Metallteile oder heiße Gase, Wärmestrahlung und Widerstandserwärmung. Die Richtlinien VdS 2047, Sicherheitsvorschriften für feuergefährliche Arbeiten, verlange:

- Gefährdungsbeurteilung vor Beginn der Arbeiten
- Ausführung feuergefährlicher Arbeiten in feuergefährdeten Bereichen nur von entsprechend ausgebildeten Personen über 18 Jahre
- Festlegung spätestens vor Beginn der Arbeiten, wer den Brandposten und eventuell erforderliche Brandwache stellt
- Unterweisung von Personen, die für den Brandposten vorgesehen sind.

Cloud Computing

Nach einem Bericht in der FAZ am 11. Juli nutzen derzeit 56.000 Unternehmen das browserbasierte Anwendungspaket von **DATEV**, mit dem sich kaufmännische Aufgaben in der Cloud erledigen lassen. Die DATEV-Angebote rund um die Kernanwendung zur Online-Belegarchivierung würden rund 112.000 Unternehmen verwenden. Die Datenzentren und technischen Systeme der DATEV gehörten zu den sichersten, die es in Europa derzeit gibt. Die Techniker von DATEV überwachen auch per Video und Computer die eigenen Glasfasernetze. Darüber hinaus hätten sie mehrschichtige Identifikationsverfahren für sämtliche Nutzer der Systeme und spezielle Verschlüsselungsmethoden für den Datenverkehr eingeführt. In den Rechenzentren der DATEV seien elektronische Quarantäne-Stationen eingerichtet, die Datenpakete in tagelangen Verfahren auf Trojaner, Viren und Würmer untersuchen.

IT-Abteilungen sollten auch am Wochenende gegen Angriffe von außen gewappnet sein, schreibt die FAZ am 20. Juli. Sobald Cloud-Dienste von Beschäftigten beruflich eingesetzt werden, werde es kritisch. Kundeninformationen und Kundendaten schwirrten durch die Unternehmenswolke ebenso wie Produktionspläne oder Prozessabläufe. Manche IT-Abteilungen würden nicht einmal zehn Prozent der Cloud-Services kennen, die von ihren Mitarbeitern genutzt werden. Vereinfacht ausgedrückt bedeute das, manche Unternehmen hätten keinen blassen Schimmer, ob und was Mitarbeiter in der Datenwolke mit sensiblen Daten tun. Im Jahr 2014 habe einer der großen Cyberangriffe den Onlinehändler Ebay gezwungen, 145 Mio. Nutzer zur Änderung ihrer Passwörter aufzufordern. Der Diebstahl solcher Daten könne somit auch der Sicherheit in den Unternehmen schaden. Nach Schätzungen von Skyhigh böten lediglich sieben Prozent der analysierten Cloud-Dienste notwendige strenge Sicherheits- und Compliance-Standards. Nach der Skyhigh-Analyse speicherten lediglich 14 Prozent der mehr als 12.000 Dienste die Daten innerhalb der EU, wo die strengsten Datenschutz-Richtlinien der Welt verfolgt und angewendet werden müssen.

Corporate Security Officer (CSO)

Jasmin Engel, Alina Lauber und Dr. Christian Rosen sehen den CSO in einer neuen Rolle (Security insight, Ausgabe 4-2015, S. 52/53). Er entwickele sich mehr und mehr zum global denkenden Business-Partner, der Teams mit Mitarbeitern unterschiedlicher Kulturen und Mentalitäten führt. Der „neue" CSO baue weltweit tätige Sicherheitsorganisationen auf, steuere Prozesse über verschiedene Abteilungen und Standorte hinweg und kooperiere mit Partnern unterschiedlicher Unternehmensbereiche und Hierarchieebenen. Ausgehend von diesem Bild habe der Verband für Sicherheit in der Wirtschaft Nordrhein-Westfalen zusammen mit weiteren Partnern von Hochschulen und einer Personalberatung einen „Kompetenzatlas" zusammengestellt. Das Handbuch zeige auf, über welche er-

folgskritischen Kompetenzen ein CSO künftig verfügen muss und welche Veränderungen daraus für sein Anforderungsprofil resultieren. Grundlage sei eine Studie zur Rolle des CSO in der aktuellen Praxis. Es zeige sich, dass für den modernen CSO vor allem eine starke Ausprägung der Ergebnis- und der Kundenorientierung sowie der teamorientierten Zusammenarbeit und Beeinflussung gefragt ist.

Falschgeld

Die Zahl der sichergestellten gefälschten Banknoten hat im ersten Halbjahr 2015 den höchsten Stand seit Einführung des Euros erreicht, meldet die FAZ am 18. Juli. Rund 50.500 falsche Euronoten seien registriert worden – ein Anstieg um 31 Prozent im Vergleich zum Vorjahreszeitraum. Allerdings liege das Falschgeldaufkommen noch immer auf einem niedrigen Niveau. Alle Blüten zusammen hätten nur einen Nennwert von rund 2,2 Mio. Euro (Bargeldumlauf mehr als 17 Mrd. Euro). Am beliebtesten bei den Fälschern seien 50- und 20-Euroscheine. Im gesamten Euroraum seien nach Angaben der EZB etwas mehr als 450.000 Blüten gefunden worden. Die Masse der in Deutschland beschlagnahmten Blüten stamme aus Fälscherwerkstätten aus der Umgebung von Neapel.

Gefährdungshinweise Türkei

Spiegel.de weist am 29. Juli darauf hin, dass die Bundesregierung weitere Anschläge in der Türkei befürchte, insbesondere auch in Istanbul. Nachdem das Auswärtige Amt (AA) bereits vor möglichen Terroranschlägen gewarnt hätte, habe es seinen Reisehinweis erneut verschärft. Es gebe Hinweise auf mögliche Anschläge auf die U-Bahn und Bushaltestellen in Istanbul. Laut AA bestehe für Reisende in der Nähe der Grenze zu Syrien „die Gefahr von weiteren terroristischen Anschlägen und Entführungen von ausländischen Staatsangehörigen". In zahlreichen Provinzen bestehe ein erhöhtes Risiko für Reisende.

Industrie 4.0

In der FAZ am 23. Juli schreibt die Bundesministerin für Bildung und Forschung, Johanna Wanka, eines der drängendsten Probleme sei die Datensicherheit. Gerade bei KMU sei die Sorge vor Schadsoftware und anderen Hackerangriffen weit verbreitet. Nach einer repräsentativen Umfrage sei für 90 Prozent der KMU die Sicherheit von Daten und Computern gegenwärtig das größte Hemmnis auf dem Weg zur Industrie 4.0. Es werde die Gefahr von Produktionsausfällen gesehen. Weniger bekannt sei, dass es für viele Probleme schon gut funktionierende Lösungen gibt. Größere Schwierigkeiten schaffe die für Industrie 4.0 notwendige Vernetzung unterschiedlicher Systeme. Viele für den herkömmlichen IT-Betrieb genutzte Lösungen würden unverändert in Produktionsanlagen eingebaut. Nicht immer würden dabei aktuelle Sicherheitsstandards beachtet. Das BMBF fördere ein Nationales Referenzprojekt für IT-Sicherheit in der Industrie 4.0, das im Schulterschluss von 14 Unternehmen sowie 7 Forschungseinrichtungen und Universitäten realisiert werde. Darüber hinaus habe das BMBF zwölf Projekte gestartet, die anwendungsnahe Abwehrstrategien gegen Cyberangriffe auf Produktionsanlagen, Leitzentralen und industrielle Kontrollsysteme entwickeln. Auch hier stünden KMU im Fokus, die Lösungen bräuchten. Die größte Herausforderung sei die Verkopplung von Produktion und Unternehmenssoftware, die eine umfassende Sicherheitsstrategie verlange. Ein Thema für die Industrie 4.0-Plattform werde deshalb auch sein, wie sich ein sicherer Datenaustausch zwischen Unternehmen organisieren lässt. Hier sei die Initiative der Fraunhofer Gesellschaft zu einem geschützten Industrial Data Space zu nennen.

IT-Sicherheit

„Die große **digitale Sorglosigkeit des Mittelstands**“ titelt die FAZ am 3. Juli. Deutsche Spitzenpolitiker würden zwar immer wieder darauf verweisen, dass es keine Hinweise auf Industriespionage seitens der Amerikaner gebe. Doch unter den Unternehmen wachse die Sorge, zumal sie bislang eher mehr schlecht als recht vor Online-Attacken geschützt sind. Eine repräsentative Umfrage von BitKOM unter mehr als 1.000 Sicherheitsverantwortlichen habe große Defizite offengelegt. Die Unternehmen verfügten über einen guten Basisschutz, investierten aber noch zu selten in umfassende Sicherheitsmaßnahmen. Jenseits der Grundfunktionen werde es dürftig. Nicht einmal jedes zweite Unternehmen verschlüssele Daten auf Festplatten oder anderen Datenträgern. Auch im Umgang mit E-Mails herrsche Sorglosigkeit. Nur 40 Prozent der Unternehmen setzten auf eine Verschlüsselung ihres E-Mail-Verkehrs. Bislang verfügten nur 29 Prozent über Technologie zur Data Leakage Prevention (DLP). Nur 23 Prozent hätten Intrusion-Detection-Systeme gegen Attacken von außen installiert. Auch noch relativ selten im Einsatz seien erweiterte Verfahren zur Benutzeridentifikation wie eine Zwei-Faktor-Authentifizierung oder biometrische Merkmale. Nur jedes vierte Unternehmen nutze sie. Und nur jedes fünfte teste die Sicherheitskonzepte mit Hilfe von Penetrationstests. Vor allem kleine Unternehmen hätten in Sachen Sicherheit aus Sicht der Fachleute Nachholbedarf. Die Hälfte der Unternehmen mit mehr als 500 Mitarbeitern nutze aufwendige Authentifizierungsverfahren, aber nur ein Fünftel der kleinen mit zehn bis 99 Beschäftigten.

Wie heise.de am 30. Juni berichtet, hätten sich Vertreter des EU-Parlaments und der EU-Mitgliedsstaaten auf Grundzüge eines Kompromisses für die geplante **Richtlinie für Netzwerk- und Informationssicherheit** verständigt. Er sehe vor, dass Angriffe auf „wesentliche“ Infrastrukturen oder Dienste sowie Sicherheits- und Datenschutzpannen bei den zuständigen Behörden gemeldet werden müssen. In Deutschland wäre dafür das BSI zuständig. Die Mitgliedsstaaten sollen die betroffenen Unternehmen anhand vorgegebener Kriterien auswählen. Dabei gehe es vor allem um „kritische Infrastrukturen“ für Energie, Verkehr, Banken, Finanzmarkt und Gesundheit. Computer Security Incident Response Teams (CSIRTs) in den Ländern sollten die bereits bestehenden CERTs ergänzen oder ersetzen. Einmal im Jahr sollten die Ansprechpartner in den Ländern einen anonymisierten Bericht über erhaltene Hinweise und daraufhin eingeleitete Maßnahmen an eine EU-Kooperationsgruppe schicken.

In keinem großen europäischen Land würden die Risiken für IT-Sicherheit so sehr unterschätzt wie in Deutschland. Das gehe aus Umfragen unter 300 IT-Managern in europäischen Unternehmen hervor, meldet die FAZ am 9. Juli. Nach der Studie von Intel Securities werden im Vergleich zu Frankreich und Großbritannien die Mitarbeiter in deutschen Unternehmen am wenigsten zu IT-Sicherheitsrisiken geschult. Die durch Softwarelücken, Computerhacker, Datenspione und Cyberkriminelle aller Art verursachten Schäden beliefen sich nach Einschätzung des Cyber-Sicherheitsrats auf mittlerweile rund 50 Mrd. Euro im Jahr, Tendenz steigend.

TECCHANNEL skizziert am 4. Juli sechs Maßnahmen, die jedes Unternehmen auf dem Weg zu einer ausgereiften Cybersecurity umsetzen sollte: Sicherheitsprüfung und -plan; Unterstützung durch die Führungsebene; Aufstellung von Sicherheitsstandards und Richtlinien, um die Informationssicherheit langfristig zu steuern, zu kontrollieren und zu optimieren; Aufbau eines Security Operation Center; Entwicklung und Integration von Internetsicherheitskontrollen sowie Überprüfung eines Business Continuity-Plans.

In der Ausgabe 2-2015 von s+s report

(S. 10–13) nehmen die IT-Experten Mark Semmler und Michael Wiesner Stellung zu den **VdS-Richtlinien 3473 – Cyber-Security für kleine und mittlere** Unternehmen. Deren drei Grundsätze würden lauten: „Mache es so einfach wie möglich – aber nicht einfacher. Setze das Paretoprinzip um, nach dem 80 Prozent der Ergebnisse in 20 Prozent der Gesamtzeit eines Projekts erreicht werden. Gib dem Unternehmen möglichst großen Gestaltungsspielraum." Die VdS 3473 verpflichteten ein Unternehmen, einen Basisschutz zu implementieren und sich dann den wirklich kritischen Teilen seiner IT-Infrastruktur zu widmen.

Für eine **IT-Security-Plattform** zum Schutz gegen Cyberkriminelle plädiert TECCHANNEL am 11. Juli. Unternehmen benötigten mehrere, in eine Sicherheitsplattform integrierte Funktionen zur Bedrohungsabwehr, die sie in jeder Phase des Angriffszyklus schützen. Mit dem richtigen Schutz aus Next Generation Firewall, cloudbasierter Analyse-Plattform und Endpunktsicherheit könne der Lebenszyklus von Cyberangriffen durchbrochen werden. Diese Verteidigungsstrategie mache zudem teure manuelle Prozesse überflüssig und sorge dafür, dass Unternehmen den neuesten Angriffstechniken einen Schritt voraus sind.

TECCHANNEL stellt am 14. Juli den **„EICAR Minimum Standard für Antimalware-Produkte"** vor. Mit ihm sollen solche Produkte ausgezeichnet werden, die die Minimalanforderungen nicht-amerikanischer Hersteller an die IT-Sicherheit erfülle. Dazu würden die Einhaltung von Datenschutzbestimmungen, Transparenz über die Kommunikationen der Produkte zu den Herstellern und eine Versicherung, dass die Produkte nicht manipuliert sind, zählen. EICAR, die European Expert Group für IT-Security, setze sich weitestgehend aus unabhängigen Vertretern aus den Bereichen Forschung und Entwicklung, Akademie sowie Industrie zusammen. Die EICAR-Anwender erarbeiteten gemeinsam IZT-Sicherheitslösungen, um Bewusstsein für und Vertrauen in solche Produkte zu verbessern. Der Standard sei unterhalb der Evaluation nach Common Criteria (CC) angesiedelt. IT-Hersteller wollten unkompliziertere, einfacher zu erreichende und vor allem preisgünstigere Gütesiegel als es CC sei.

Nach einer Studie des IT-Dienstleisters Unisys vertreten 77 Prozent der befragten Bürger die Ansicht, dass Kriminelle immer einen Weg finden werden, persönliche Daten zu hacken, die bei Unternehmen gespeichert sind, meldet silicon.de am 13. Juli. Junge Menschen gehen sogar zu 85 Prozent davon aus, dass Daten nicht effektiv vor unberechtigtem Zugriff geschützt werden können. Dieses Misstrauen halte die Verbraucher dennoch nicht davon ab, Online zu einzukaufen oder Bankgeschäfte vom PC aus zu erledigen.

Ein Hackerangriff lege die **Verwundbarkeit vernetzter Autos** offen, berichtet die FAZ am 23. Juli. Zwei amerikanische Sicherheitsexperten hätten sich aus der Ferne Kontrolle über einen fahrenden Geländewagen der Marke Jeep verschafft und ihn manipuliert. Das sei nicht aus bösem Willen geschehen, sondern mit der Absicht, auf solche Sicherheitsdefizite hinzuweisen. Die Hacker hätten sich nicht nur Kontrolle über das Unterhaltungssystem verschafft, sondern auch über Belüftung, Schlösser, Lenkung, Getriebe und Bremsen. Sie nutzten offenbar eine Schwachstelle im Unterhaltungs- und Navigationssystem Uconnect. Fiat Chrysler habe vor wenigen Tagen ein Sicherheits-Update für seine Software herausgebracht, was nach Angabe des Unternehmens die Verwundbarkeit beseitigt.

Mit **Fernwartung** befasst sich TECCHANNEL am 22. Juli. Die Ausnutzung offener Kommunikationswege sei eine der erfolgreichsten Varianten, um sich Zugang zu fremden Rechnern und Unternehmensnetzen zu verschaffen. Größte Aufmerksamkeit sollte deshalb auf den eingesetzten Remote-Managementlösungen liegen. Eine Verizon-Studie aus dem

Jahr 2013 habe aufgedeckt, dass finanziell motivierte Lauschangriffe am häufigsten über Desktop-Sharing oder Remote-Access-Dienste erfolgen. Sechs Maßnahmen sollten davor schützen: Sicherheitsmaßnahme Nummer eins sei, Standardeinstellungen und -passwörter grundsätzlich zu vermeiden. Das „Durchgangsproblem" lasse sich allerdings auch an der Wurzel packen, wenn eine Remote-Support-Lösung zum Einsatz kommt, die keine offenen Listening-Ports einsetzt. Unabhängig von der eingesetzten Lösung empfehle es sich in jedem Fall, die Logdateien häufiger zu durchforsten, um den Einsatz von Remote Access-Tools zu überwachen. Weitere Sicherheitsmaßnahmen seien: Zuständigkeiten nachverfolgen: Systemzugriffe unter Kontrolle halten; alle Aktivitäten der Support-Sessions protokollieren; Support-Technologie standardisieren; gesamte Kommunikation verschlüsseln.

Microsoft habe für August 2015 die **Sicherheitssoftware Advanced Threat Analytics** (ATA) angekündigt, berichtet silicon.de am 23. Juli. Unternehmen sollten mit ATA in der Lage sein, zielgerichtete Angriffe abzuwehren. Die Software identifiziere und analysiere mithilfe von maschinellem Lernen normales sowie anormales Nutzerverhalten. Darüber hinaus setze die Lösung rollenbasierte Analyse ein, um auch fortschrittliche Angriffe in Echtzeit zu entdecken. ATA könne aber auch bekannte Fehler in der Sicherheitskonfiguration aufspüren. Microsoft wolle die Software als Standalone-Lösung und auch als Teil der Enterprise Mobility Suite und der Enterprise Client Access License anbieten.

silicon.de weist am 27. Juli darauf hin, dass am 25. Juli das **IT-Sicherheitsgesetz in Kraft getreten** ist. Es beinhalte unter anderem Mindeststandards für die IT-Sicherheit. Außerdem müssten Betreiber sogenannter „kritischer Infrastrukturen" wie Banken, Krankenhäuser oder Energieunternehmen, dem Gesetz zufolge Sicherheitsvorfälle an das BSI melden. Bei Verstößen drohten Bußgelder in Höhe von bis zu 100.000 Euro. Das IT-Sicherheitsgesetz erweitere darüber hinaus die Kompetenzen für das BSI sowie die Bundesnetzagentur. Auch das BKA erhalte im Bereich der Computerkriminalität mehr Ermittlungszuständigkeiten.

IuK-Kriminalität

silicon.de berichtet am 30. Juni, EUROPOL habe einen internationalen **Cybercrime-Ring zerschlagen**. Dieser soll Malware zum Ausspionieren wertvoller Finanzdaten entwickelt und verbreitet haben. Ermittler aus Deutschland, Estland, Lettland, Moldawien, Polen, der Ukraine und den USA hätten in einer gemeinsamen Aktion fünf Verdächtige festgenommen. In vier ukrainischen Städten hätten sie außerdem bei acht Hausdurchsuchungen Computerausrüstung als Beweismaterial beschlagnahmt. Mit der Operation hätten EUROPOL und EUROJUST insbesondere die Hintermänner von Zeug und SpyEye aus dem Verkehr ziehen wollen. Die beiden Malware-Familien seien bekannte Banking-Trojaner. Sie verbreiteten sich weltweit über Botnetze und Phishing-Kampagnen. Die Cyberkriminellen hätten ihre hochentwickelten Banking-Trojaner mit der Zeit angepasst, um die von Banken eingesetzten Sicherheitsvorkehrungen zu umgehen. Jeder Cyberkriminelle hätte ein Fachgebiet und die Gruppe sei darin verwickelt, Malware zu programmieren, Computer zu infizieren, Bankanmeldedaten zu sammeln und das erbeutete Geld über sogenannte Money-Mule-Netzwerke zu waschen. Zu den Zielen des Cybercryme-Rings hätten in der Folge einige große Banken gehört. Die Ermittler würden den verursachten Schaden auf mindestens zwei Mio. Euro schätzen.

Wie silicon.de am 8. Juli berichtet, hat Symantec eine extrem professionelle Hackergruppe mit dem Namen **Morpho** entdeckt. Sie soll es ausschließlich auf Unternehmen abgesehen haben. In den vergangenen drei

Jahren hätten sie dem Sicherheitsunternehmen zufolge Firmen aus Europa, Kanada und den USA ausspioniert. Die Konzerne stammten aus dem Internet-, Rohstoff-, Pharma- und dem Technologiesektor. Apple, Facebook, Microsoft und Twitter haben einem Symantec-Blog zufolge bereits Angriffe bestätigt. Morpho verfüge über großes technisches Wissen sowie äußerst umfangreiche Ressourcen. Die Gruppe bestehe aus weniger als zehn Leuten und entwickle maßgeschneiderte Malware für Windows und Apple. Diese soll kaum Spuren hinterlassen. Bei den Angriffen entwendeten sie vor allem wertvolle Firmengeheimnisse und verkauften sie wahrscheinlich an den Höchstbietenden.

Nach einem Bericht der FAZ am 11. Juli haben sich Hacker mit Cyberangriffen auf die amerikanische Regierung zum Teil heikle persönliche Daten von 22 Mio. Amerikanern besorgt. Die abgeschöpften Datenbanken enthielten nicht nur die üblichen persönlichen Angaben, sondern auch die Auswertungen von Sicherheitsüberprüfungen der einzelnen Personen. Der Angriff habe eine ungekannte Dimension. Die US-Regierung hege den Verdacht, die chinesische Regierung stecke hinter den Angriffen. Die entwendeten Daten enthielten die Sozialversicherungsnummern, Adressen, Fingerabdrücke, Passwörter, die Gesundheitszeugnisse, die polizeilichen Führungszeugnisse, Lebensläufe und Informationen über Angehörige.

In einer Pressemitteilung vom 8. Juli erläutert das Bayerische Landeskriminalamt den sogenannten **Verschlüsselungstrojaner**: „Plötzlich kann man nicht mehr auf die Dokumente und Dateien auf seinem PC zugreifen. Stattdessen befindet sich eine Textdatei auf dem Rechner, die einem erklärt, alle Daten seien verschlüsselt worden. Es folgt eine Anleitung, wie man den Zugriff auf seine Daten wieder zurückerhält. Natürlich nur nach einer vorherigen Geldzahlung." Und das LKA gibt Tipps zur Abwehr solcher Angriffe: Öffnen Sie niemals ungeprüft Dateianhänge. Klicken Sie niemals auf Links in unaufgefordert zugesandten E-Mails. Seien Sie in Sozialen Netzwerken kritisch mit dem Klick auf angeblich aufsehenerregende Videos oder andere Mitteilungen. Installieren Sie regelmäßig die vom Hersteller bereitgestellten Sicherheitsupdates für Ihr Betriebssystem und die von Ihnen installierten Programme. Setzen Sie ein Virenschutzprogramm ein und aktualisieren Sie dieses regelmäßig. Achten Sie darauf, dass Sie nicht mit Administratorenrechten im Internet unterwegs sind. Legen Sie sich einen „Benutzer" mit Standardbenutzerrechten an und nutzen Sie diesen für das Surfen im Internet. Sichern Sie Ihre Daten regelmäßig auf einem externen Medium.

Nach einem Bericht in der FAZ am 17. Juli haben Europol und FBI in einer international konzertierten Aktion einen der großen Marktplätze für Viren, Trojaner und andere Schadsoftware ausgehoben. Dabei seien nach Angaben des US-Justizministeriums rund 70 Personen in den USA, Europa und Asien festgenommen worden. Es gelte, die Kommunikations- und Handelswege frei von Raub und Erpressung zu machen und milliardenschwere Schäden von der Wirtschaft abzuwenden. Computerkriminelle hätten jahrelang auf der als **Darkode** bekannten digitalen Plattform zahlreiche Instrumente für Angriffe auf Fremdcomputer entwickelt und ausgetauscht. Damit konnten sie in die Geräte eindringen, die dort gespeicherten Daten auslesen, manipulieren und sabotieren. Die materiellen Schäden hätten sich über die Jahre hinweg auf Hunderte Mio. Euro belaufen. Zu den Opfern zählten Dutzende Banken und Finanzhäuser, Unternehmen wie Sony und Millionen privater Internetnutzer. Das Netzwerk habe seit 2007 bestanden. Vorübergehend seien hier 200 bis 300 kriminelle „Spitzenhacker" aus der internationalen Szene aktiv. Derzeit seien etwa noch 800 vergleichbare Plattformen bekannt. Darkode sei eine der größten gewesen. An der Spitze habe ein Schwede gestanden, der auch ein Netzwerk geschaffen haben soll, das vorüber-

gehend Hunderttausende Rechner umfasste und so die Leistungsfähigkeit eines kleinen Hochleistungsrechners hatte und in die Netzwerk- und Mainframerechner großer Bankhäuser eindringen konnte. Den illegalen Zugang zu den virtuellen Tresoren von etwa 250 Bank- und Finanzhäusern habe er für Eintrittspreise zwischen 80 und 1.000 Dollar verkauft. Die Plattform habe auch eine Hackergruppe namens Lizard Squad genutzt. Sie sollte Unternehmen wie Sony angreifen, die Netzwerke der Playstation attackieren und vorübergehend lahmlegen. Auch seien die Daten von Millionen Sony-Kunden abgegriffen worden.

Das LKA Rheinland-Pfalz informiert durch eine Pressemitteilung vom 9. Juli über die **Manipulation elektronischer Rechnungen**. Täter würden Geschäftsdaten ausspähen oder sie fingieren, um sie für manipulierte Rechnungen zu verwenden, die sich kaum von Originalrechnungen unterscheiden. Gemäß den allgemeinen Geschäftsabläufen erhielten Unternehmen nach einer Warenbestellung auf elektronischem Weg eine Rechnung über die georderten Waren, die vor Warenauslieferung zu begleichen ist. Nach geleisteter Vorkasse bleibe jedoch der Wareneingang aus. Auf den Konten des Partnerunternehmens sei kein Zahlungseingang zu verzeichnen. Das LKA gibt eine Reihe von Ratschlägen, rät vor allem, die Möglichkeiten verschlüsselter oder signierter E-Mails und Kommunikation zu nutzen, Geschäftsgeheimnisse durch verschlüsselte Datenablage zu schützen und mit den Geschäftspartnern entsprechende Ablaufprozesse zu vereinbaren.

Die FAZ weist am 28. Juli auf eine Studie von Ernst & Young hin, für die Geschäftsführer sowie Führungskräfte aus IT-Sicherheit und Datenschutz von 450 deutschen Unternehmen befragt worden seien. 81 Prozent gingen von einer wachsenden Bedrohung aus dem Netz aus. Dabei gehe die größte Gefahr aus Sicht der Manager von China aus: 46 Prozent nennen das Land als Region mit dem höchsten Risikopotenzial, dahinter folgten Russland (33 Prozent) und die USA (31 Prozent). Dennoch habe sich am Sicherheitsgefühl der Unternehmen nichts geändert. Wie schon vor zwei Jahren hielten 82 Prozent der Manager die präventiven Maßnahmen gegen Datenklau in ihrem Unternehmen für ausreichend. Jeweils mehr als 80 Prozent setzen weiter nur auf Firewalls, Antivirensoftware und gute Passwörter. Die Unternehmen seien allerdings auch tatsächlich unterschiedlich stark vom Datenklau betroffen – je nach Größe und Branche. So würden Unternehmen der Energie- und der Finanzbranche am häufigsten Opfer von Spionage und Datenklau.

Korruption

Die Bundesregierung solle **Korruption im Gesundheitswesen** per Gesetz bekämpfen, kündigt das Handelsblatt am 8. Juli an. Laut Zentralstelle zur Bekämpfung von Vermögensstraftaten und Korruption im Gesundheitswesen versickern jährlich mehr als eine Mrd. Euro in dunklen Kanälen. Nach dem derzeitigen Entwurf aus dem BMJ blieben allerdings fragwürdige Bereiche verschont. Einer davon: die von der Pharmaindustrie veranstalteten oder gesponserten Ärzte-Fortbildungen. Nach einer Untersuchung der Deutschen Gesellschaft für Hämatologie und Medizinische Onkologie von 2013 werden geschätzt 60 bis 70 Prozent aller medizinischen Fortbildungsveranstaltungen von der Industrie bezahlt. Der Gesetzentwurf enthalte keinen Hebel, um das indirekte Beeinflussen von Medizinern zu unterbinden. Das Regelwerk sehe bisher nur die Bestechung eines Arztes als Straftatbestand vor, nicht aber eine an die Vorteilsnahme angelehnte Strafvorschrift. Das sei ein kleiner, aber feiner Unterschied. Während Bestechung eine konkrete Unrechtsvereinbarung verlangt, will die Vorteilsgewährung schon die „allgemeine Landschaftspflege“ unterbinden. Denn genau das sei das Hauptproblem. Die Pharmakonzerne sähen sich als Wohltäter im

Gesundheitssystem und verwiesen auf die Fortbildungspflicht der Mediziner, an der sich die Pharmaindustrie um der Volksgesundheit willen beteilige.

In der Ausgabe 4-2015 von Security insight (S. 18/19) befasst sich Susanne Fehleisen, Mag. (FH), mit **Rechtfertigungsstrategien bei Korruptionsvorwürfen.** Bei einer empirischen Untersuchung seien die Leugnung des Schadens beziehungsweise die Leugnung der Opfer und die Leugnung der Verantwortung besonders häufig genannt worden. Als Ansatzpunkte für die Korruptionsprävention ließen sich aus den Ergebnissen der Untersuchung ableiten: die Rolle der Führungskraft als integeres Vorbild, Sensibilisierung durch Schulungen; Förderung der Eigenverantwortung; Etablierung einer „neuen" Fehlerkultur; Null-Toleranz-Strategie; offener Diskurs und ein wertschätzendes Miteinander in Teams; Wissensvermittlung zu Folgen und Schäden aus Korruption und Erhöhung des Aufdeckungsrisikos.

Krankenhaussicherheit

Die Fachzeitschrift Security insight enthält in Ausgabe 4-2015 mehrere Beiträge zur Krankenhaussicherheit. Hagen Zumpe stellt das **elektronische Zutrittsmanagement** im Evangelischen Krankenhaus Mülheim vor (S. 24/25). Über das dort angewandte Sicherheits-Managementsystem Aeos von Nedap seien neben der Zutrittssteuerung auch Videoüberwachung und Einbruchmeldung vernetzt. Neben unterschiedlichen Türarten (automatische Türsysteme, Glas-, Brandschutz-, Paniktüren) sollten auch Patientenschränke, Personalspinde sowie mobile Container und Rollwagen elektronisch gesichert werden. Technologisch basiere die Zutrittslösung auf dem „Salto Virtual Network" mit patentierter Scheib-Lese-Funktionalität und verschlüsselter Datenübertragung. In einem weiteren Beitrag wird ein **flexibles Berechtigungsmanagement** für Zutrittsmedien und andere Gegenstände beschrieben (S. 25/26). In einer elektronischen Übergabestation würden nicht nur die Zutrittsmedien (Schlüssel, Ausweise) verwahrt, disponiert und übergeben, sondern auch Betäubungsmittel. Grundlage sei ein flexibles Berechtigungsmanagement. Nach Rückgabe der Zutrittsmedien werde kontrolliert, ob sie tatsächlich wieder ordnungsgemäß im Automaten hinterlegt wurden. Der Vorgang erfolge per RFID-Technologie: Jedes Depot erkenne sein ihm zugewiesenes Objekt. Das Risiko von Verlust und Missbrauch von Zutrittsmedien sei dadurch minimal. Thematisiert werden ferner **spezielle Mobiltelefone für Kliniken** (S. 28/29). Moderne Mobiltelefone für den Klinikbereich könnten auch Alarm auslösen, wenn sie eine definierte Zeit lang nicht mehr bewegt oder gekippt werden. Mit moderner Kommunikationstechnik lasse sich das Notfallgeschehen auch lokalisieren und automatisiert weiterverfolgen. Laufend würden Positionsdaten an die Zentrale geschickt. Geht ein Notruf ein, erscheine auf dem Alarm-PC eine akustische und visuelle Meldung. Diese werde automatisch als Gruppennachricht an definierte Endgeräte übermittelt.

Mobile Endgeräte

10 Tipps für mehr Sicherheit bei der Smartphone-Nutzung geben in der Ausgabe 3-2015 der Zeitschrift WiK (S. 26) Stefan Schaffner und Janis Kinast, ASS it-systemhaus GmbH:

- das Gerät niemals aus den Augen lassen
- nur die notwendigen Daten speichern
- E-Mail-Kommunikation verschlüsseln
- Mitlesen verhindern
- Vorsicht bei der Nutzung von WLAN
- nur vertrauenswürdige Apps nutzen
- Schnittstellen im Blick behalten
- Backup- und Remote-Löschung
- Zugriff erschweren
- wirksamen Virenschutz gewährleisten

IT-Spezialist Marcus Rogge erläutert in der Ausgabe 4-2015 der Zeitschrift Security insight (S. 54/55), **wie man sein Smartphone schützt.** Es sei sehr zu empfehlen, vom Hersteller bereitgestellte System-Updates zeitnah einzuspielen. Vor der Installation einer App solle man prüfen, wie nützlich die App ist und ob ihre Nutzung auch die Rechte erfordert, die sie einfordert. Fremde Hotspots als WLAN würden immer ein Risiko bergen. Deshalb sollte man Verbindungen mit Bedacht wählen. Ein sinnvoller Sicherheitsmechanismus sei die PIN für SIM-Karten. Das Backup sollte man zusätzlich auf einem externen Medium sichern.

Netzsicherheit

Dass die rechtzeitige Vorbereitung auf Next Generation Network (NGN) Probleme bei der **Umstellung von analoger auf IP-Technik** erspart, erläutert Dipl.-Wirtschaftsjurist (FH) Sebastian Brose, VdS Schadenverhütung, in der Ausgabe 2-2015 von s+s report (S. 50/51). Insgesamt würden über 20 Mio. Anschlüsse auf IP-Basis migriert. Schon heute nutzten mehr als fünf Mio. Kunden in Deutschland die neuen Anschlüsse der Telekom. Für den Endkunden sei im Regelfall nicht erkennbar, dass die Umstellung seines Telefonanschlusses auf NGN Auswirkungen auf die Funktion seiner Übertragungseinrichtung hat. VdS empfehle Errichtern und Sicherungsdienstleistern, alle Kunden, die noch nicht über IP-basierte Übertragungseinrichtungen verfügen, so schnell wie möglich zu informieren und umzurüsten. Als die unter dem Aspekt der Zukunftssicherheit am besten geeignete Variante erscheine die Kombination aus drahtgebundener IP-Verbindung (DSL) und funkbasierter IP-Verbindung (GPRS/UMTS oder LTE).

Notruf- und Service-Leitstellen

Den Begriff **„Effizienz bei der Gefahrenabwehr",** wie er erstmalig in der neuen VdS 3138-1 (Anforderungen an NSL) auftauche, erläutert Wolfgang Wüst, BSG-WüST GmbH, in der Ausgabe 2-2015 der Fachzeitschrift s+s report (S. 44–47). Wesentliche Grundlage für einen effizienten Alarm- und Interventionsdienst sei die schutzobjektspezifische Planung einer angemessenen Gefahrenabwehr. Sie beinhalte mindestens:

- Erfassen der schutzobjektspezifischen Sicherheitssituation
- Erfassen, Bewerten und regelmäßiges Aktualisieren der schutzobjektrelevanten Sicherheitsinformationen
- Erkennen und Identifizieren konkreter Gefahren
- Ermitteln der erforderlichen Maßnahmen und Priorisieren dieser Maßnahmen für eine schnellstmögliche Gefahrenabwehr
- Erfassen, Bewerten und Verknüpfen von Informationen zur Alarmverifizierung
- Festlegen und regelmäßiges Bewerten der bestmöglichen Alarmbearbeitungs- und Interventionsmaßnahmen und der hierfür erforderlichen Einsatzmittel.

Organisierte Kriminalität

Nach einer Meldung der FAZ vom 8. Juli hat die Polizei im Landkreis Konstanz acht italienische Staatsangehörige festgenommen, denen vorgeworfen werde, der kalabrischen Mafia-Organisation anzugehören. Die italienische Staatsanwaltschaft spreche von der „außerordentlichen Fähigkeit der kalabrischen 'Ndrangheta, sich im Ausland zu reproduzieren". Es sei der Mafia im Grenzgebiet zwischen Baden-Württemberg und der Schweiz gelungen, ein fast identisches Netz aufzubauen wie in der süditalienischen Heimat. Es gebe verschiedene Zellen, die zwar einerseits

autonom seien, andererseits aber eine direkte Verbindung zur Heimat unterhielten. Die Mafia nutze Deutschland und die Schweiz nicht nur als Rückzugsraum für „Schläfer", sie wasche dort auch Geld, handle mit Menschen und Rauschgift und sei auf dem Immobiliensektor aktiv.

Raub

Ausgabe 2-2015 des Fachorgans DSD enthält eine Übersicht über die Anzahl der **Raubüberfälle auf Wertdienstleister** in europäischen Staaten nach der jeweiligen Polizeilichen Kriminalstatistik 2014: Großbritannien 223, Frankreich 34, Italien 30, Irland 19, Portugal 13, Schweden 13, Griechenland 11, Deutschland 4, Tschechische Republik 4, Schweiz 4.

Raubkopien

Wenn ein Arbeitnehmer auf seinem Dienstcomputer private CDs und DVDs kopiert, kann er fristlos entlassen werden. Das hat das BAG im Fall eines Mannes entschieden, der am OLG Naumburg für die IT verantwortlich war. Auf seinem Rechner fanden sich mehr als 6.400 Bild-, Audio-, Video- und e-book-Dateien. Zudem war ein Programm zur Umgehung des Kopierschutzes installiert. Es sei unerheblich, ob sich der Beschäftigte dabei wegen Verstößen gegen das Urheberrecht strafbar gemacht hat (Az: 2 AZR 85/15).

Sicherheitsgewerbe

Dr. Berthold Stoppelkamp, BDSW, zählt in der Ausgabe 2-2015 des DSD auf, dass von den fast 190.000 Beschäftigten der Sicherheitswirtschaft fast 130.000 Aufgaben zur Prävention und Gefahrenabwehr wahrnähmen und dabei die Polizeien mit ihren rund 240.000 Kräften entlasteten:

- 65.000 schützen Wirtschaftsunternehmen bzw. öffentliche Einrichtungen
- 16.000 nehmen Luftsicherheitsaufgaben wahr
- 12.000 schützen Veranstaltungen
- 11.000 schützen Geld- und Werttransporte
- 10.000 führen Revier- und Kontrolldienste durch
- 5.000 schützen den Öffentlichen Personenverkehr
- 5.000 schützen militärische Liegenschaften
- 2.000 arbeiten in Notruf- und Serviceleitstellen
- 1.500 schützen kerntechnische Anlagen.

Das **Lünendonk-Trendpapier 2015 „Wie viel Sicherheit darf es sein?"** liefert Einkäufern, Fachabteilungen und interessierten Marktbeobachtern Hintergrundinformationen und spricht Empfehlungen aus, wie qualitativ hochstehende Sicherheitsdienstleistungen ausgeschrieben und vergeben werden können. Im ersten Teil wird das Themengebiet theoretisch behandelt. Der Einkauf von Sicherheitsdienstleistungen unterliege erschwerenden Besonderheiten (besondere Charakteristika von Dienstleistungen, latente Interessenkonflikte zwischen Entscheidungsgremien in größeren Organisationen und neuerdings eine etwas andere Sichtweise auf die Mindestlohnproblematik). Der Dreh- und Angelpunkt letztendlicher Beurteilung bleibe aber die Qualität sowie das Wertversprechen. Grundlegende Anforderungen an Leumund, finanzielle Zuverlässigkeit sowie Zertifizierungen und die Beibringung von Unterlagen zur wirtschaftlichen und finanziellen Leistungsfähigkeit seien sozusagen die Präqualifikation bei der Auswahl eines Anbieters. Damit seien aber die Güte des Angebots und die Qualität der versprochenen Dienstleistung weder gesichert noch verhandelt. Der technische Wert eines Angebots für die Erbringung von Sicherheitsdienstleistungen sollte in vier Schlüsselbereichen überprüft werden: Wachpersonal (Erfahrung, Kenntnisse und Fähigkeiten, Auswahl, Einstellung und Überprüfung,

Arbeitsbedingungen, vom Auftraggeber definierte Kriterien), Auftragsmanagement und operative Führung (Managementteam, Auftragsmanager vor Ort, Gestaltung der Dienstpläne, unterstützende Dienstleistungen, vom Auftraggeber definierte Kriterien), Auftragsinfrastruktur (Ausrüstung, technische Unterstützung, vom Auftraggeber definierte Kriterien) und Unternehmensleistungsstärke (Struktur und Organisation, Sicherheitswesen, Qualitätswesen, Personalmanagement, Referenzen, Zertifikat und Auszeichnungen, vom Auftraggeber definierte Kriterien). Zu den Trends für den Markt für Sicherheitsdienstleistungen gehörten:

- Bei den Anbietern vollziehe sich eine Marktkonsolidierung.
- Normungs- und Standardisierungsprozesse in der Sicherheitswirtschaft würden immer bedeutsamer.
- Der aktuell viel diskutierte Einsatz von Sicherheitstechnik erhöhe die Produktivität.
- Die Verlagerung von hoheitlichen Aufgaben der öffentlichen Hand an private Dienstleister werde weiter zunehmen.

Der zweite Teil der Trendstudie illustriert das Thema anhand von Fachbeiträgen sowie mit anschaulichen Referenzen.

Spionage

Wie die Tageszeitung Libération am 30. Juni auf der Basis von Wikileaks-Dokumenten berichtet, habe die NSA rund 100 **französische Unternehmen ausspioniert**. Sie solle Verträge oder Vertragsverhandlungen über einen Wert von mehr als 200 Mio. Dollar ausspioniert haben. Eine breite Palette von Branchen habe das Interesse der NSA geweckt, darunter Telekommunikation, Elektrizität, Gas, Erdöl, Atomkraft und erneuerbare Energien. Auch Umwelttechnologien und die Gesundheitsbranche seien ausgeforscht worden. In Frankreich seien nach Angaben der französischen Behörde für IT-Sicherheit ANSSI rund hundert Unternehmen regelmäßig Opfer von Spionageangriffen. Informationen würden aufgrund historischer Verbindungen häufig mit Großbritannien, Kanada, Neuseeland und Australien geteilt.

Steuerhinterziehung

Steuerhinterziehung sei **in der Gastronomie** weit verbreitet – Betriebsprüfer würden sie aber künftig noch schwerer aufdecken können, berichtet die FAZ am 23. Juli. Der Bundesfinanzhof (BFH) habe die Verwendung einer gebräuchlichen Kontrollmethode eingeschränkt: den Zeitreihenvergleich. Besonders in Restaurants, Imbissstuben und Kneipen ließen sich damit viele verschwiegene Einnahmen aufdecken. Der BFH habe eingeräumt, dass elektronische Kassensysteme durch Umprogrammierung in nahezu beliebiger Weise manipulierbar sind. Dennoch gehe den Steuerrichtern der Einsatz der Schätzungsmethode zu weit. Sie führe „denklogisch" immer zu einem Mehrergebnis gegenüber der Buchführung des Gastronomen. Maßgabe des BFH dürfe die Finanzverwaltung künftig nur noch dann einen Zeitreihenvergleich anstellen, wenn das Verhältnis von Wareneinkäufen und Erlösen das ganze Jahr über weitgehend konstant war. Wenn der Verdacht auf inhaltliche Unstimmigkeiten bestehe, hätten andere Schätzmethoden – etwa eine „Geldverkehrsrechnung" – Vorrang. Ist ein Zeitreihenvergleich überhaupt zulässig, dürfe er allenfalls einen Anhaltspunkt für verheimlichte Erlöse bilden.

Transportdiebstahl

Der Bundesverband ASW meldet folgende Tatorte aktueller Planen-Schlitzereien und sonstiger Ladungs-Diebstähle:

- 22./23. Juni: A2, Kloster Lehnin, Parkplatz Grebser Heide zwischen AS Brandenburg

und Netzen, Fahrtrichtung Potsdam
- 6. Juli: Betriebsgelände Spornitz
- 6. Juli.: A2 Peine, Autohof Peine
- 7./8. Juli: A2, Rasthof Buckautal
- 10./11. Juli: Industriegebiet Klöcknerstraße in Castrop-Rauxel
- 12. Juli: A9, Niemegk, Raststätte Fläming-Ost, Richtung Autobahndreieck Potsdam
- 15./16. Juli: A2, Lehrte, Parkplatz Lehrter See-Süd
- 16. Juli: Wolfhagen-Niederelsungen, Rasthof

Verfassungsschutz

Laut dem am 30. Juni veröffentlichten **Verfassungsschutzbericht für 2014** wurden in diesem Jahr insgesamt 32.700 politisch motivierte Straftaten in Deutschland registriert. Das ist gegenüber dem Vorjahr ein Anstieg um vier Prozent. In dieser Zahl sind 3.368 Taten der politisch motivierten Gewaltkriminalität zuzuordnen, ein Zuwachs von 13,8 Prozent gegenüber 2013. Rechtsextremistisch motiviert waren 16.559, linksextremistisch motiviert 4.424 Straftaten. Im Phänomenbereich „politisch motivierte Ausländerkriminalität" (ohne islamistisch motivierte Aktionen) wurden 2.014 Straftaten erfasst, 270 Prozent mehr als 2013. Hauptakteure der gegen Deutschland gerichteten Spionageaktivitäten seien nach wie vor die Russische Föderation, die Volksrepublik China und die Islamische Republik Iran. Die bestehenden strengen deutschen und europäischen Exportkontrollbestimmungen hätten zu einer Veränderung des Einkaufs- und Beschaffungsverhaltens proliferationsrelevanter Staaten geführt, den sogenannten Umgehungsausfuhren. Eine Zusammenfassung des Verfassungsschutzberichts 2014 unter Hervorhebung der Abschnitte Spionage, Proliferation und Wirtschaftsschutz enthält die Website von Securitas (News/Sicherheitslage).

Videoüberwachung

Eduard Lehmann, Siemens Schweiz AG, befasst sich in Ausgabe 3-2015 der Zeitschrift Sicherheitsforum (S. 29–31) mit der Vernetzung der Videoüberwachungssysteme über Internet Protocol und der rasanten **Entwicklung der Videotechnik**. Sensible Sicherheitsanlagen sollten grundsätzlich vom Internet getrennt sein, sodass Hacker sich keinen Zugriff verschaffen können. Die Central Processing Units würden stetig stärker und besser, was wiederum eine höhere Intelligenz der Kamera ermögliche. In der Kamera sei ein Rechner integriert, auf welchem man wiederum Zusatzfunktionen installieren könne. Diese übernähmen ganz spezifische Teilaufgaben: So gebe es zum Beispiel eine Funktion für die Bildanalyse oder bei einer Wärmebildkamera eine für die Feuererkennung. Ein in die Kamera integriertes Mikrofon nehme die Geräusche auf und analysiere sie. Moderne Videomanagementsysteme (VMS) böten zunehmend umfangreichere Funktionen, welche die tägliche Arbeit des Sicherheitspersonals in den Zentralen erleichtere. Neben weiteren Trends wie Personenzählungen, virtuelle Stolperdrähte oder die Detektion von Rauch in Tunnels arbeiteten heutige VMS mit ausgemessenen Bildern und Georeferenzdaten, sodass sich die Kameras in 3D steuern ließen. Eine entsprechende Software könne Objekte verfolgen und metergenau lokalisieren. Außerdem könne man nach Belieben in Bereiche hineinzoomen und automatisch Symbole platzieren. Die Zustände könnten dynamisch dargestellt und die Alarmzonen der Analyse eingeblendet werden. Schwenk-/Neige-Kameras würden automatisch von Algorithmen gesteuert und verfolgten ein Objekt wie das menschliche Auge.

Sascha Puppel, öffentlich bestellter und vereidigter Sachverständiger für Gefahrenmeldeanlagen, befasst sich in der Ausgabe 2-2015 von s+s report (S. 38–42) mit typischen Fehlern bei der **Errichtung von Videoüber-**

wachungsanlagen. Durch die umfangreiche Überarbeitung der Norm DIN EN 50132-7 mit Stand 04/2013 (Alarmanlagen – CCTV-Überwachungsanlagen für Sicherungsanwendungen – Teil 7: Anwendungsregeln) sei ein umfangreiches Hilfsmittel und Werkzeug für Planer, Errichter und Betreiber geschaffen worden. Der Autor geht ein auf Schwierigkeiten für Errichter und Auftraggeber, auf richtige Geräte am falschen Ort, auf Einwirkungen von Wind und Wetter, auf die Gefahr von Detektionslücken, auf fehlenden Schutz vor Sabotage oder Manipulation, auf zu geringe Verlege- bzw. Trennungsabstände und häufige Defizite bei der Dokumentation.

Zutrittskontrolle

In der Ausgabe 1/2015 des ssi Bulletin (Beilage zur Ausgabe 3-2015 des Sicherheitsforum) beantwortet Markus Baumann, Amstein + Walthert Sicherheit AG, die Frage nach der Notwendigkeit eines Zutrittskontroll-Konzepts. Es sei in jedem Fall wichtig, um alle Wünsche, Aspekte und Schnittstellen aufzuzeigen und zu planen. Der Autor befasst sich mit dem Ermitteln des Bedrohungsbildes, dem Festlegen der Schutzziele, dem Maßnahmen-Grobkonzept und dem Sicherheitskonzept mit Zonenplänen. Es müsse klar definiert und visualisiert werden, ob das Zutrittskontrollsystem die Einbruchmeldeanlage steuert oder „der Lead" von ihr übernommen wird. Grundsätzlich empfehle es sich, beim Erarbeiten eines Zutrittskontrollkonzepts Bereiche, Personen oder Funktionen in Gruppen aufzuteilen.

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