Focus on Security

Ausgabe 06, Juni 2015

SECURITAS

Inhalt

Anschläge

Wie das BKA in der Wochenlage am 30. April berichtet, haben unbekannte Täter am 23. April auf einem Baustellengelände der **Goethe-Universität Frankfurt a. M.** einen Bagger in Brand gesetzt. Auf einer linksgerichteten Internetseite veröffentlichte eine „AG Wohnen für Alle" am 25. April ein Selbstbezichtigungsschreiben, in dem sie „den Umbau des ehem. Philisophicums in Luxuswohnungen" als „Skandal" bezeichnen und kritisieren, dass auf dem Gelände kein „sozialverträgliches Wohnprojekt" verwirklicht wird. Nach der Bewertung des BKA begehen Linksaktivisten im Themenzusammenhang Sozialpolitik/Umstrukturierung regelmäßig Straftaten zum Nachteil von Baufirmen oder Immobiliengesellschaften, die in der Kritik der linken Szene stehen.

Bahnsicherheit

An **Videotechnik** im öffentlichen Nah- und Fernverkehr werden komplexe Anforderungen gestellt, die eine Herausforderung für Entwickler seien, heißt es in der Fachzeitschrift PROTECTOR (Ausgabe 5-2015, S. 30/31). Durch die Verbindung zentraler Sensortechnologie, photovoltaischer Energiesysteme, Wärmebildkameras und Cloud-basierter Konnektivität über das „M2M-Netzwerk" sichere Panasonic kritische Bereiche wie unbemannte Bahnübergänge. Durch das Einrichten von Sperrbereichen oder kritischen Zonen mithilfe der Analysetechnologie in den Überwachungskameras könne zudem genau verfolgt werden, ob sich Personen gezielt verbergen oder sich in gefährlichen Wartebereichen aufhalten. Die Analysefunktion der Kameras lasse sich so einstellen, dass sie einen Alarm auslöst, sobald ein Gegenstand oder Gepäckstück über einen bestimmten Zeitraum unbeaufsichtigt abgestellt bleibt.

Betrug

Ryanair vermisse 4,6 Mio. Euro von einem Geschäftskonto, meldet heise.de am 4. Mai. Der Betrag sei elektronisch im Auftrag einer chinesischen Bank eingezogen worden. Derzeit sei nicht klar, wer dahinter steckt und wie der Betrug vonstatten ging.

Brandschutz

Den **Brandschutz in hohen Hallen** behandelt die Fachzeitschrift GIT in der Ausgabe 5-2015, S. 84/85. Die Detektion in hohen Produktionshallen stelle den Brandschutz wegen der häufig unter der Hallendecke auftretenden Wärmepolster vor besondere Herausforderungen, vor allem dann, wenn produktionsbedingt als Störgröße Staub auftritt. Bei Oehler Verpackung in Leipzig überwachen sieben linienförmige Rauchmelder ILIA von Hekatron die bis zu 19 Meter hohen Produktionshallen. Sie seien unterhalb der Wärmepolster der Decken installiert, während die Kontrolleinheit dazu in bequemer Arbeitshöhe unterhalb des Bedienfelds der Brandmelderzentrale montiert sei.

Cloud Computing

Claudio Giovanoli und Stella Gatziu Grivas, Fachhochschule Nordwestschweiz, befassen sich in der Zeitschrift Sicherheitsforum, Ausgabe 2-2015, mit **Zertifizierungen** für das Cloud Computing (S. 45–47). Gerade die Aspekte Sicherheit und Vertrauen würden als eine der größten Hürden für die Cloud gelten. Nach wie vor gebe es nicht **den** Zertifizierungsstandard für Cloud-Angebote, doch existierten einige Kandidaten hierzu: ISO 20000 und 27000 Serie. Die ISO/IEC 20000 IT-Service-Management diene als messbarer Qualitätsstandard für das IT-Service-

Management (ITSM). Der Star Audit basiere einerseits auf einem Best Practice-Ansatz. Andererseits berücksichtige er BSI, ETSI und ENISA. Dadurch solle gewährleistet werden, dass ein ganzheitliches Verständnis über den Umfang und die Wirksamkeit einer solchen Betriebsprüfung ermöglicht werden kann. Die CSA STAR-Zertifizierung sei eine unabhängige Beurteilung der Sicherheit eines Cloud Service-Providers durch Dritte. Der Prüfkatalog von TÜV Rheinland basiere auf Standards wie BSI, Studien sowie auf ausgewählten Vorschriften und Empfehlungen, konkretisiert und angepasst für die Cloud.

Datenschutz

Die Diskussion um eine EU-weite Datenschutzgrundverordnung soll im Juni zum Abschluss kommen, doch es rege sich Kritik, berichtet COMPUTERWOCHE.de am 12. Mai. Die in Deutschland gesetzlich verankerte Beratung und Kontrolle durch unabhängige betriebliche Datenschutzbeauftragte in Unternehmen werde die Verordnung zunächst nicht umfassen. In diesem Punkt habe sich Deutschland gegenüber den 28 Mitgliedsstaaten nicht durchsetzen können.

Diebstahl

„Diebstahl im Outlet" titelt die FAZ am 27. Mai. Fast alle Outlet-Geschäfte in Deutschland und erst recht die in Metzingen, der „Hauptstadt des Fabrikverkaufs", litten unter der zunehmenden Zahl von Ladendiebstählen. Trotz hohem technischem Aufwand und einer immer raffinierteren Überwachungstechnik würden in manchen Outlet-Geschäften bis zu 10 Prozent der Waren verschwinden. Für viele Diebe sei die Nähe der Outlet-Geschäfte zur alten Innenstadt ein Vorteil, nirgendwo sonst könnten sie so schnell untertauchen. Die Zahl der von Baden organisierten schweren Ladendiebstähle sei von zwei Fällen 2011 auf 32 Fälle 2014 gestiegen. Die Polizei registrierte 2014 445 Straftaten in den Outlets der Stadt, mehr als 90 Prozent Diebstahlsdelikte. Das Verhältnis zwischen Gelegenheits- und organisierten Diebstählen schätze die Polizei auf 1:15. Der Blick in die Asservatenkammer der Polizeidienststelle zeige, dass die meisten Täter hochprofessionell vorgehen. Sie kämen zum Beispiel mit einer imitierten Dolce & Gabana-Tasche in die Outlets, in die drei Anzüge passen. Weil die Tasche innen mit einer dicken Aluminiumschicht ausgeschlagen ist, piepse beim Verlassen des Ladens kein Warensicherungssystem. Andere Diebe störten die Sender hinter der Kasse mit einem mitgebrachten Peilsender. Manche lösten die elektronische Warensicherung mit einem kleinen Metallhaken und stopften die geklauten Hosen oder Hemden in eine Stretch-Radhose oder einen Bikini, den sie unter Alltagskleidung tragen. Wieder andere brächten Etikettierungswerkzeuge mit und machten aus einer 700-Euro- eine 100-Euro-Lederjacke. Viele Diebe in Metzingen kämen aus dem Ausland, aus Frankreich, der Schweiz, Rumänien, Bulgarien, Ungarn oder den Balkanstaaten. Die italienische Luxusmarke Prada habe das Problem so gelöst: Wer eine Tasche oder ein Kleid nur anfassen will, müsse das Stück von einer Theke abholen. Wer sich dafür entschieden habe, bekomme einen nummerierten Zettel. Damit hole er die kostbare Prada-Handtasche an der Kasse ab.

Drohnen

Unternehmen setzten immer häufiger Unmanned Aerial Vehicles (UAVs) ein, um neue und bessere Daten zu erhalten, berichtet TECCHANNEL.de am 14. Mai. Aber der Markt für solche Drohnen formiere sich erst. Außerdem gelte es viele Implikationen zu bedenken: rechtlicher wie technischer Art. Wenn der Markt den Prognosen von ABI

Research folge, sollten sich Firmen schnellstmöglich auf den Einsatz von Drohnen vorbereiten – und auf die vielen Daten, die diese sammeln. Der Einsatz hänge natürlich von künftigen rechtlichen Regulierungen und dem Aussehen von Drohnen in wenigen Jahren ab: Unabhängig davon könne sich die IT gar nicht früh genug auf den Umgang mit den so gewonnenen Big Data-Bergen vorbereiten.

Einbruch

Das Sicherheitsunternehmen Securitas führte am 19. Mai einen Medienworkshop durch, um den Beitrag der Sicherheitswirtschaft zur Abwehr der Einbruchskriminalität vorzustellen und zu diskutieren. Manfred Buhl, CEO Securitas Deutschland, nannte es eine gesamtgesellschaftliche Aufgabe, die steigende Tendenz zu brechen. Wohnungen, Privathäuser und der gewerbliche Mittelstand seien immer stärker betroffen. Die Flut der Einbrüche einzudämmen, werde weder der Polizei noch den Unternehmen und den Wohnungseigentümern allein gelingen. Erforderlich sei eine kluge Kooperation aller Stakeholder, und die Sicherheitswirtschaft könne dazu einen erheblichen Beitrag leisten. Das geschehe insbesondere durch eine immer intelligentere und effiziente Sicherheitstechnik, die dazu führe, dass inzwischen mehr als 40 Prozent der Einbrüche im Versuchsstadium stecken bleiben, weil die Täter abgeschreckt werden oder infolge des hohen Widerstandszeitwerts die Tat abbrechen. Vorgestellt wurde unter anderem eine Videoüberwachungsanlage, deren Software den Tatverdächtigen detektiert. Über ein Audiosystem kann der Operator in der NSL den überraschten Verdächtigen ansprechen und zum Verlassen des geschützten Bereichs auffordern. Bei den nach dem neuesten Stand der Technik ausgestatteten, zertifizierten NSL von Securitas in Berlin und Mannheim seien bundesweit 140.000 Gefahrenmelde-, Brandmelde-, Videoüberwachungs- und Aufzugsanlagen aufgeschaltet. Vorgestellt wurde ferner eine mobile Videoüberwachung (Securitas Mobile Cam) für die vorübergehend notwendige Sicherung von Räumen und Anlagen, etwa Baustellen. An einem bis zu sechs Meter ausfahrbaren Teleskopmast wird eine PTZ- und Thermalkamera mit „Rund-um-Blick" und integrierter Software zur Detektion vordefinierter Bewegungen befestigt. Außerden wurde eine Vernebelungsanlage vorgeführt, wie sie Securitas zum Schutz von hochwertigen Gütern, zum Beispiel in einem Juweliergeschäft, anbietet. Innerhalb weniger Sekunden führt die ausgelöste Vernebelung zur völligen Orientierungslosigkeit des Einbrechers oder Räubers und zwingt ihn zur Aufgabe. Aber nicht nur durch das Angebot solcher Sicherheitslösungen mit integrierter Sicherheitstechnik, sondern auch durch die Bestreifung von Wohnsiedlungen im Auftrag der Immobilieneigentümer zum Schutz der Hausrechtsbereiche und durch die Übernahme von vielfältigen Funktionen der Unternehmenssicherheit leiste das Sicherheitsgewerbe einen erheblichen Beitrag zur Abwehr von Einbrüchen.

PROTECTOR enthält in Ausgabe 5-2015 (S. 26/27) eine Marktübersicht über 75 Einbruchmeldeanlagen von 31 Anbietern. Neben allgemeinen Angaben wurde eine Vielzahl von Leistungsmerkmalen abgefragt, unter anderen die Anzahl der Sicherungsbereiche, der Meldergruppen, der Meldepunkte, der Melder, der Stichleitungen, verfügbare Melderarten, Melderadressierung, Kommunikationsmodule, Aus- und Eingänge, Schnittstellen, Zugriffsschutz, Managementsysteme.

Exportkontrolle

Compliance in der Exportkontrolle thematisiert der Behörden Spiegel in der Mai-Ausgabe (S. 12). Ziel jedes Exportunternehmens müsse es sein, ein internes Exportkontroll-Compliance-System zu entwickeln, das ein

Maximum an Regelkonformität garantiert, und es in seine Geschäftsabläufe zu implementieren. Hat die Revision ergeben, dass die Exportgeschäfte der Exportkontrolle unterliegen, seien interne Verfahrensanweisungen zu erstellen, die die jeweiligen Prüfprozesse zur exportkontrollrechtlichen Bewertung von Kundenaufträgen vorgeben. Darauf baue die Errichtung eines Exportkontroll-Managements auf. Dieses entscheide exklusiv, abschließend und verbindlich für alle exportkontrollrechtlich relevanten Fragestellungen. Sofern intern exportkontrollrechtliche Verfehlungen festgestellt werden, stelle sich die Frage, wie die Unternehmensführung damit umgehen sollte, insbesondere, ob sie diese Verstöße freiwillig gegenüber den Strafverfolgungsbehörden anzeigt. Zwar resultiere daraus kein Anspruch auf Strafbefreiung oder -milderung, doch honorierten die Verfolgungsbehörden eine solche Transparenz im Rahmen ihrer Ermittlungen.

Gefahrstoffe

Marc Eder, Denios AG, befasst sich in der Ausgabe 5-2015 der Fachzeitschrift GIT (S. 88–90) mit den Technischen Regeln für Gefahrstoffe **TRGS 407 und TRGS 725**, die die sichere und richtige Durchführung der Gefährdungsbeurteilung behandeln. Es sei nicht möglich, eine Standard-Gefährdungsbeurteilung für alle Gase zu erstellen. Jedes Gas müsse einzeln betrachtet und entsprechend den Gefährdungen bewertet werden, die sich daraus ergeben.

Dr. Martin Henn, AGS-Hugg, erläutert in der Ausgabe 5-2015 von GIT (S. 92/93) den Entwicklungs- und **Beratungsstand zur neuen Gefahrstoffverordnung** (GefStoffV). Im Rahmen der Strukturreform der Betriebssicherheitsverordnung (BetrSichV) durch die Verordnung zur Neuregelung der Anforderungen an den Arbeitsschutz bei der Verwendung von Arbeitsmitteln und Gefahrstoffen vom 3. Februar 2015 seien die Grundvorschriften zum atmosphärischen Explosionsschutz der GefStoffV überarbeitet und mit den Regelungen der BetrSichV zusammengeführt worden – auch das Explosionsschutzdokument und die Zoneneinteilung seien nun in der GefStoffV enthalten. Eine Neufassung der GefStoffV sei für Ende 2015 vorgesehen und solle bei den Anpassungen folgende Schwerpunkte umfassen: vollständige Umstellung auf die EU-CLP-Verordnung; vollständige Implementierung des Risikokonzepts; anwender- und vollzugspraktikable Gestaltung der Regelungen zu Asbest.

Industrie 4.0

Cyberbedrohungen machen nach Überzeugung von COMPUTERWOCHE.de vom 28. April vor kritischen Infrastrukturen nicht Halt. Trotzdem existierten hierzulande noch immer viele falsche Wahrheiten, **Mythen zum Thema IT-Security für industrielle Systeme,** die COMPUTERWOCHE.de widerlegen möchte. Mythos 1: Offline ist sicher. Ein durchschnittliches industrielles Steuerungssystem habe elf Verbindungen zum Internet – so eine Securelist-Untersuchung von Oktober 2012. Zudem berücksichtigten die Sicherheitssysteme des Unternehmensnetzwerks nur die allgemeinen Unternehmensprozesse und nicht die kritischen Prozesssysteme. Es seien zahlreiche Verbindungen zwischen dem Unternehmensnetzwerk und dem Internet vorhanden. Uneinheitliche Sicherheitskonzepte machten Unternehmen angreifbar. Mythos 2: Eine Firewall schützt. Firewalls schützten bis zu einem gewissen Grad, sie seien jedoch nicht unüberwindbar. Mythos 3: Hacker verstehen nichts von SCADA. In der Hackerszene würden die Themenbereiche SCADA und Prozessleitsysteme diskutiert. Dafür gebe es einen guten Grund: Cyberkriminalität sei zu einem finanziell lukrativen Geschäft geworden. Mythos 4: Ein Angriff ist unwahrscheinlich. Zunächst einmal müsse ein

Unternehmen kein direktes Ziel einer Attacke sein, um Opfer davon zu werden. Zudem seien viele Systeme bereits attackiert worden und generell angreifbar – aufgrund der unsicheren Betriebssysteme, auf denen sie basieren. Mythos 5: Sicherheitssysteme schützen vor Angriffen. Aktuelle Sicherheitssysteme könnten technische Fehler aufweisen. So nutzten viele Module der Kommunikationsschnittstellen von Sicherheitssystemen eingebettete Betriebssysteme und Protokollstapel, die bekannte Schwachstellen haben.

Industrieparksicherheit

Dr. Jan-Robert Schwark, Infraserv, gibt in der Fachzeitschrift GIT (Ausgabe 5-2015, S. 20–24) Auskunft über seine Aufgaben und Tätigkeiten im **Industriepark Höchst**, dem größten Industriepark Europas (4,6 qkm, 90 Firmen, überwiegend aus der Chemie- und Pharmabranche, mit 22.000 Mitarbeitern). Die klassischen Einheiten Unternehmenssicherheit, Werkfeuerwehr, Gefahrenabwehrmeldezentrale und Notfallmanagement bildeten das Rückgrat und die personellen Schwerpunkte (275 eigene Mitarbeiter) der Gefahrenabwehrorganisation im IPH. Das Risikoprofil habe sich in den letzten Jahren massiv verändert. Ein wichtiger Schritt sei die Einführung von Dokumentenprüfgeräten an allen Zugängen des Industrieparks gewesen. Das Notfallmanagement am Standort sei einmalig. Ein Team von Naturwissenschaftlern stelle einen 24/7-Notfallmanager-Dienst sicher. Nach Alarmierung rücke ein Notfallmanager gemeinsam mit der Werkfeuerwehr aus. Die technische Überwachung der Perimeterlinie übernehme eine intelligente Videoüberwachung. Bei den Kameras kämen aufgrund der technologiebedingten Vorteile verstärkt Wärmebildkameras zum Einsatz. Der IPH setze als Erster Geräte der Bundesdruckerei zur eindeutigen Echtheitsüberprüfung von vorgelegten Personalausweisen, Reisepässen, ID-Cards, Aufenthaltstiteln und Visa ein.

IT-Sicherheit

Die RSA-Konferenz in San Francisco habe gezeigt, dass sich die **IT-Security im Umbruch** befindet, heißt es bei COMPUTERWOCHE.de am 28. April. Doch trotz der rasant wachsenden Zahl der Sicherheitsunternehmen – die Megadatendiebstähle nähmen weiterhin zu. Die Herausforderungen für die Branche erforderten neue Konzepte. Analytics, Identity Management und Cloud Security hießen die Security-Themen der Zukunft. Das Fazit des RSA-Präsidenten laute konsequenterweise, dass wir uns daran gewöhnen müssen: Dateneinbruch und Datendiebstahl seien nicht mehr die Ausnahme, sondern der Normalfall.

Mit **IT-Sicherheit im Mittelstand** befasst sich TECCHANNEL.de am 28. April. Mit dem Microsoft Baseline Security Analyzer könnten einzelne Windows-Rechner und Server eines Netzwerks auf Sicherheitslücken und fehlende Patches überprüft werden. Auch wenn in Unternehmen bereits eine Patch-Managementlösung im Einsatz sei, schade es nicht, ab und zu die PCs im Netzwerk zu scannen, damit sichergestellt ist, dass alle Sicherheitseinstellungen durchgeführt und die Computer aktuell mit Patches versorgt sind.

In einer Beilage zur FAZ am 6. Mai bezeichnet Franz Büllingen, Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste, die **IT-Sicherheit als „Achillesferse des Mittelstands".** Gerade KMU seien mit der richtigen Umsetzung von IT-Sicherheitsmaßnahmen häufig überfordert. Dabei habe eine Studie des BMWi gezeigt, dass das Bewusstsein für Risiken grundsätzlich vorhanden ist, die Unternehmen aber nicht zwangsläufig konkrete Maßnahmen ergreifen. Spionageangriffe nähmen seit Jahren zu und hätten dabei vor allem das geistige Eigentum von KMU im Blick. Gerade deutsche Mittelständler stünden aufgrund ihres Know-how-Vorsprungs in bestimmten Märkten gezielt im Fokus von professionellen Attacken. Viele Unternehmen

unterschätzten den Faktor Mitarbeiter. Selbst simple Regeln wie zum Beispiel die Verwendung starker Passwörter für den E-Mail-Account oder die tägliche Anlage von Sicherungskopien würden oftmals nicht beachtet. Neutrale Orientierung und Hilfen erhielten Unternehmen bei den kostenlosen Schulungsangeboten des BitKOM oder durch die Förderinitiative „Mittelstand-Digital", mit der das BMWi die Digitalisierung von KMU und Handwerkern unterstützt. Durch sehr praxisnahe und leicht verständliche Informationen würden Unternehmer hier über die grundlegenden Risiken aufgeklärt, und es würden Lösungswege aufgezeigt, die einfach, schnell und kostengünstig sind. So böten 38 regionale Anlaufstellen, die sogenannte eBusiness-Lotsen, die gemeinsam das eKompetenz-Netzwerk bilden, anbieterneutrale Informationen und unterstützten bei Auswahl und Umsetzung der richtigen Sicherheitsmaßnahmen. Die Förderinitiative biete auch online eine große Auswahl von Hilfsmitteln, die mit Best Practice-Beispielen und einem Selbsttest schnell einen Überblick schaffen, welche Schritte sinnvoll und notwendig sind.

Das Sicherheitsforum weist in der Ausgabe 2-2015 (S. 48) auf eine Studie von unabhängigen Marktforschungsinstituten hin, nach der etwa die Hälfte aller deutschen Befragten (53 Prozent) die Auswirkungen, die der Einsatz mobiler Endgeräte auf die IT-Sicherheit des Unternehmens (**BYOD**) haben könnte, eher unkritisch sehe. Ein Viertel sei aber der Meinung, dass bei ihnen nicht die geeignete Technologie vorhanden ist, um außerhalb mit dem gleichen Maß an IT-Sicherheit wie im Büro zu arbeiten. Fast ein Drittel der befragten deutschen Unternehmen untersage Mitarbeitern die Nutzung persönlicher Geräte.

Unternehmen, die der IT-Sicherheit nur wenig Beachtung schenken, handelten fahrlässig und könnten für ein solches Verhalten haftbar gemacht werden, schreibt Rechtsanwalt Horst Speichert in der Ausgabe 5-2015 der Zeitschrift PROTECTOR (S. 65). IT-Sicherheit gehöre zu den **Organisationspflichten des Unternehmens**. Das Gesetz zur Transparenz und Kontrolle im Unternehmensbereich zwinge die Unternehmensleitung, ein frühzeitiges Risikomanagementsystem zu etablieren, auf dessen Grundlage die IT-Sicherheit aufbaut. Das Unternehmensrisiko könne nur begrenzt auf die unteren Ebenen, wie die der IT-Verantwortlichen, delegiert werden, denn diese hafteten nur bei grob fahrlässigem oder vorsätzlichem Verschulden persönlich.

Wie heise.de am 19. Mai meldet, verteidigte Innenminister de Maiziére auf dem 14. Deutschen IT-Sicherheitskongress das geplante **IT-Sicherheitsgesetz**. Zwar sei die Meldepflicht für die Wirtschaft ein heikler Punkt, doch ohne eine solche Regelung könne die Sicherheit für alle langfristig nicht gewährleistet werden. Der Minister habe die kürzlich bekannt gewordenen Pläne bestätigt, die IT-Netze des Bundes zu begradigen und ein Bundesrechenzentrum zu schaffen. Gleichzeitig will er auch die Einrichtung einer Bundes-Cloud voranbringen. Auch die IT-Beschaffung wolle das Innenministerium zentralisieren.

Der Behörden Spiegel berichtet in der Mai-Ausgabe (S. 50) über eine Studie im Auftrag von BitKOM, die zeige, dass in den letzten zwei Jahren bereits die Hälfte der Unternehmen in Deutschland Opfer eines Cyberangriffs wurden. Bei der Umfrage seien 1.000 Topmanager befragt worden. Der Schaden betrage jährlich 51 Mrd. Euro. Gefährdet seien vor allem jene Unternehmen, die ihr Know-how über Jahre entwickelt haben und ihre Wettbewerbsfähigkeit durch ihre hohe Produktqualität gewährleisten. Mehr Sicherheit biete ein **„Multilayer-Ansatz"** mit einer Mischung von proaktiven und reaktiven Maßnahmen. Neben den gängigen Schutzvorrichtungen sollte auch eine „Sandboxing-Technologie" zum Einsatz kommen, um unbekannte Schwachstellen zu entdecken. Ergänzend seien Antibot-Sicherheitslösungen ein wichtiger Baustein.

Den **Sicherheitsfaktor Mensch** thematisiert Erwin Recktenwald, Biners GmbH i. G., in der Mai-Ausgabe des Behörden Spiegel (S. 51). Von konkurrierenden ausländischen Unternehmen, den eigenen und ehemaligen Mitarbeitern, gehe die größte Gefahr aus. Social Engineering sei ein sehr wirkungsvoller und mit geringem Aufwand verbundener Weg, die technischen „Schutzwälle" zu umgehen. Zur Abwehr von Social Engineering sollten folgende Punkte besonders beachtet werden: 1. Die Identität und die Berechtigung des speziellen Anliegens eines Anrufers oder des Absenders einer E-Mail sollten zweifellos sichergestellt sein. 2. Bei Unklarheiten über die Echtheit des Absenders sollte auf der Basis eines „gesunden" Misstrauens eine gezielte Rückfrage erfolgen. 3. Unsicheren Quellen und unbekannten Anrufern seien unter keinen Umständen organisatorische und finanzielle Informationen und Daten zur Verfügung zu stellen. 4. Bei Verdacht auf ein gezieltes „Ausspionieren" sei die Sicherheitsorganisation umgehend zu informieren.

Das rumänische IT-Unternehmen Bitdefender hat mit **New GravityZone** die neueste Version seiner virtuellen Sicherheitskonsole vorgestellt, berichtet COMPUTERWOCHE.de am 26. Mai. Sie sei ab sofort in den Editionen für KMUs, große Unternehmen und Rechenzentren verfügbar. Sie mache zentralisiertes intelligentes Scannen für unterschiedliche physische und virtuelle IT-Umgebungen möglich – einschließlich Linux. In wenigen Minuten installiere ein einziges Paket die Konsole und schließe über die zentrale Verwaltung sämtliche Endpunkte der IT-Umgebung sowie Microsoft Exchange ein.

IuK-Kriminalität

Mit der **Attacke auf den Sender TV5 Monde** haben, so die Einschätzung im deutschen Verfassungsschutz, islamistische Cyberangriffe eine neue Qualität erreicht, heißt es in der FAZ am 5. Mai. Zu Schmierereien, Fundraising, Online-Fatwas sowie der massiven und überaus professionellen Propagandaarbeit des IS komme eine neue Dimension hinzu: Sabotage. Für Deutschland sollte das ein Warnsignal sein. Seit langem sei bekannt, dass große Teile der Infrastruktur unzureichend gegen Hackerangriffe geschützt sind. Es reiche ein fingernagelgroßer USB-Stick, um, für Augenblicke mit einem Computer verbunden, in Schaltzentralen einzudringen. Noch hielten sich solche Sabotageaktionen, mit denen deutsche Verfassungsschützer aus dem radikal-islamistischen Untergrund rechnen, im Rahmen. Die Zahl der Verknüpfungen steige exponentiell. Selbst Industrieanlagen mit zwanzig Jahren alten Computersystemen würden zunehmend mit dem Internet verbunden.

Den „Virus der verbrannten Erde" nennt heise.de am 5. Mai den **Windows-Schädling Rombertik**, der versuche, per Phishing-Spam auf die Rechner seiner Opfer zu kommen und der dann dort alles ausspioniere, was den Drahtziehern irgendwie nützlich sein könnte. Interessant werde es allerdings, wenn Virenforscher versuchen, den Schädling zu analysieren. Werde solch eine Analyse entdeckt, lösche der Schadcode den Master Boot Record und starte das System neu, sodass der PC des Opfers in einer Bootschleife gefangen sei. Gelinge dies nicht, verschlüssele er die privaten Daten des Nutzers mit einem zufälligen RC4-Schlüssel und mache sie so unbrauchbar. Ca. 80 Prozent des Schädlings bestünden aus überflüssigen Daten und wahllosem Code, der zwischen nutzlosen Funktionen hin und her springe, um eine Analyse zu erschweren. Rombertik verbreite sich über Phishing-Mails als angebliche PDF-Datei, die eigentlich ein Bildschirmschoner sei. Habe er den MBR eines Systems gelöscht, seien die Daten zwar nicht unwiederbringlich verloren. Eine Wiederherstellung sei allerdings nicht einfach.

Wie sich gezielte Angriffe abwehren lassen, beschreibt COMPUTERWOCHE.de am 6. Mai.

Heutige Attacken seien zwar selten komplexer und hinterhältiger als frühere, dafür aber um so zielgerichteter auf ein bestimmtes Netzwerk ausgelegt. Das mache sie so gefährlich. Seit mindestens zehn Jahren verschiebe sich der **Fokus** von Angreifern weg von der Betriebssystemebene hin **auf die Applikationsebene**. Die externen Web-Applikationen vieler – vor allem mittelständischer – Unternehmen seien jedoch auch heute noch mit Techniken wie SQL Injection oder Cross-Site Scripting angreifbar. Bei zahlreichen mittelständischen Unternehmen seien Web Application Firewalls nach wie vor eher selten im Einsatz und viele Firmen nähmen nicht einmal jährlich Penetrationstests vor. Kriminelle würden Schwachstellen in Hilfsprogrammen wie PDF-Viewer, Flash Player, java-Interpreter, die Office-Produkte, Webbrowser und andere Plug-ins ausnutzen. Sie würden gezielte und echt aussehende Phishing-Mails versenden und Anwender auf Webseiten mit individueller Malware locken. Die neuen Lösungen, die dieses Problem adressieren, setzten an unterschiedlichen Stellen an. Am bekanntesten sei momentan die Analyse von übertragenen Objekten in einer gesicherten virtuellen Maschine oder Sandbox in der Firewall-Umgebung, bezeichnet als „Sandbox-Analyse". Ein Sensor kopiere alle Dokumente, die von Webseiten heruntergeladen werden oder an eingehenden Mails angehängt sind. Diese Objekte würden in einer abgeschotteten Sandbox auf einem zentralen System gespeichert und dort automatisch geöffnet oder zur Ausführung gebracht. Dabei überwache ein Sicherheitssystem alle Aktivitäten in der Sandbox. Wenn nun Systemeinstellungen manipuliert würden, Codes aus dem Internet nachgeladen oder sonstiges bösartiges Verhalten erkannt werde, gehe man davon aus, dass es sich um Malware handelt. Der Wert der Erkennung sinke allerdings bereits, da die Autoren von Malware und die Kriminellen inzwischen verstanden hätten, wie eine Sandbox-Analyse funktioniert. Entsprechend ändere sich das Verhalten ihrer Angriffsprogramme.

Im Code des virtuellen Floppy Disk-Controllers „QEMU" lauere die Schwachstelle **„Venom",** meldet COMPUTERWOCHE.de am 13. Mai. Angreifer, die sich die Sicherheitslücke zunutze machen, könnten dadurch unter Umständen die vollständige Kontrolle über das Host-System erlangen. Auch andere virtuelle Maschinen auf diesem System sowie lokale Netze wären in diesem Fall bedroht.

Nach einem Bericht von TECCHANNEL.de am 21. Mai beteiligten sich 600 Experten aus Unternehmen an einer **Online-Umfrage zur Mobile Security**. Datendiebstahl, eingeschleuste Malware und Viren sowie der Verlust mobiler Geräte seien danach die drei größten wahrgenommenen Sicherheitsrisiken hinsichtlich der Nutzung mobiler Geräte und Anwendungen. 53,7 Prozent der Umfrageteilnehmer hätten einen Diebstahl von Unternehmensdaten zu den größten Security-Risiken gezählt. 44 Prozent hielten das Einschleusen von Malware und Viren in die Unternehmens-IT für eine große Gefahr. Den Verlust mobiler Geräte zählten knapp 43 Prozent zu den drei größten Sicherheitsrisiken. Beim Zugriff der Mitarbeiter auf Unternehmensdaten zeigten sich Schwachstellen. Über IT-gemanagte Mobilgeräte griffen nur 69,8 Prozent auf Daten zu. Knapp 20 Prozent der dafür eingesetzten Geräte unterlägen nach der Umfrage nicht der Kontrolle der IT-Abteilung. In 6 Prozent der Fälle würden Daten unverschlüsselt an Personen außerhalb der IT-Kontrolle gesendet. Weitere 5 Prozent speicherten Daten unverschlüsselt über Cloud Services. Weniger als 10 Prozent der Befragten auf Geschäftsleitungsebene betrachteten mobile Apps als „großes Risiko".

Kartellrechtsverletzung

Das Kartell auf dem deutschen **Schienenmarkt** sei eines der Superlative, heißt es im Handelsblatt am 19. Mai. Der über die Jahre angehäufte Schaden bei Kunden wie der

Deutschen Bahn summiere sich auf über eine Milliarde Euro. Die beteiligten Unternehmen Thyssen-Krupp und Voestalpine hätten zusammen einen dreistelligen Millionenbetrag an Bußgeldern und Schadenersatz zahlen müssen. Am Ende stehe jedoch eine bescheidene Zahl: Das LG Bochum habe das Verfahren gegen sieben Angeklagte „aus den unteren Rängen" gegen eine Geldbuße von insgesamt 290.000 Euro eingestellt.

Korruption

Zwei Drittel aller Unternehmen in Deutschland haben Antikorruptionsrichtlinien. Viele davon hätten diese in den vergangenen vier Jahren bekommen. Das sei das Ergebnis einer Umfrage unter knapp 4.000 Unternehmen in Europa, dem Vorderen Orient und Afrika durch die Beratungsgesellschaft EY, berichtet die FAZ am 21. Mai. Danach habe sich der Anteil jener Unternehmen, die gegen Korruption vorgehen, hierzulande seit 2011 auf fast 40 Prozent verdoppelt. In die Einrichtung von Antikorruptionssystemen sei viel investiert worden. Aber nach der Einrichtung erlahme häufig das Engagement. Korruptionsfreies Verhalten werde noch nicht überall bewusst genug gelebt. Es werde durch **falsche Anreizsysteme** teilweise konterkariert. Selbst die Mitarbeiter, die die Grenze zu kriminellen Handlungen überschreiten, seien aber nur selten Kriminelle im landläufigen Sinne. Ihnen fehle häufig die kriminelle Absicht. Die meisten Mitarbeiter würden die Grenze der Legalität überschreiten, weil sie dem Unternehmen etwas Gutes tun wollen. Korruption sei zwar nicht die häufigste Form der Wirtschaftskriminalität, aber die bei Weitem schlimmste. Sie unterminiere das Vertrauen in das Recht und setze die Marktwirtschaft außer Kraft. Es gebe daher bei Korruption keine Abstufung in der Schwere der Verfehlung.

Krankenhaussicherheit

Margret Jöchl und Jürgen Schreiber, Tiroler Landeskrankenanstalten GmbH, befassen sich in der Ausgabe 2-2015 der Fachzeitschrift Sicherheitsforum mit Security-Kennzahlen zur Messung des Security Managements im Krankenhaus (S. 24–27). Sie messen die Anzahl der unterschiedlichen Hilfeleistungen an einer Klinik, die Anzahl nach Wochentagen und Uhrzeiten. Bei den Diebstahlsobjekten rangierten Geldtaschen an erster, Bargeld an zweiter Stelle. Die Autoren kommen zu dem Ergebnis, Statistiken und Kennzahlen böten in Krankenanstalten ein wertvolles und taugliches Werkzeug, ohne dass das Corporate Security Management nicht umsetzbar ist. Personaleinsätze könnten von Anzahl und Zeit her präziser geplant, Sicherheitsmaßnahmen zielorientierter platziert oder Personal gezielter geschult und sensibilisiert werden. Kriminalitätsschwerpunkte würden exakt herausgefiltert, um Präventionsmaßnahmen zu entwickeln.

Kreditkartenbetrug

In jüngster Vergangenheit haben Betrüger auf bisher unbekannte Weise Kreditkartendaten ausgespäht und damit binnen kürzester Zeit entsprechende Einkäufe bei verschiedenen Online-Portalen zu Lasten der Geschädigten getätigt. Die Täter machten sich dabei oftmals die bei allen Diensten identischen Passworte der Geschädigten zunutze. In einem bei der Göttinger Polizei angezeigten Fall hatten die Täter binnen 18 Minuten 173 Kartenverfügungen weltweit veranlasst. In 43 Fällen davon waren die Verfügungen erfolgreich. In einem weiteren Fall hätten Hacker in zehn Stunden 68 Umsatzverfügungen vorgenommen (Pressemitteilung der PI Göttingen vom 11. Mai).

Krisenregionen

Am 18. Mai hat das BKA eine Gefährdungsbewertung für deutsche Interessen in **Griechenland** übermittelt. Bezüglich des in Griechenland vorhandenen extremistischen/terroristischen Personenpotenzials erscheine im Hinblick auf eine Gefährdung deutscher Interessen insbesondere das linksextremistische/anarchistische Spektrum in Griechenland relevant. Bereits im Jahr 2013 habe die „Gruppe der Volkskämpfer" durch die Anschläge auf die Residenz des Deutschen Botschafters und die Mercedes-Benz Niederlassung in Athen belegt, dass die deutsche Haltung in der Finanzkrise als Legitimation für militantes Vorgehen genutzt wird. Selbstbezichtigungsschreiben zeigten, dass entsprechende Anschläge sowohl auf staatliche als auch auf private/wirtschaftliche Repräsentanzen und Interessen Deutschlands im Bereich des Wahrscheinlichen liegen. Im Ergebnis bestehe für deutsche staatliche und privatwirtschaftliche Einrichtungen in Griechenland weiterhin eine hohe abstrakte Gefährdung, bei der militante Aktionen einzukalkulieren seien.

Luftsicherheit

Die Hinweise für die **Absturzursache des Militärtransporters A400M** im Mai diesen Jahres verdichten sich, berichtet die FAZ am 20. Mai. Ein Problem in der Steuerungssoftware für die vier Flugzeugmotoren habe wohl zum Unglück im spanischen Sevilla geführt, bei dem vier Menschen der sechsköpfigen Besatzung ums Leben kamen. Der Hersteller Airbus Defence und Space habe an seine Abnehmer die „dringliche technische Empfehlung" zur Überprüfung der elektronischen Triebwerkskontrolleinheit herausgegeben. Das Unternehmen sei zwar der Ansicht, dass die Maschine weiter geflogen werden kann, rate aber ausdrücklich zu „einmaligen Kontroll-Checks" an der Triebwerkssoftware – und das „bei jedem Triebwerk vor dem nächsten Flug". Einer der überlebenden Techniker habe nach dem Vorfall berichtet, dass sich drei der vier Triebwerke nach dem Start komplett abgeschaltet hätten. Das habe wohl an fehlerhaften Anweisungen durch die Steuerungssoftware gelegen, die offenbar von Airbus-Technikern falsch konfiguriert wurde, heiße es in Konzernkreisen.

Maschinensicherheit

Dipl.-Ing. Andreas Grimsehl, Pepperl+Fuchs GmbH, befasst sich in der Fachzeitschrift GIT (Ausgabe 5-2015, S. 104/105) mit der **Trennung der Signalübertragung** zwischen Feldgerät und Steuerung zum Schutz für Personal und Anlagenteile. Hohe Spannungen könnten im Signalkreis auftreten, sodass ohne Schutzvorrichtungen Bedienpersonal und Steuerung gefährdet seien. Signaltrenner gewährleisteten den Berührschutz und schützten Anlagen vor Zerstörung. Der Einsatz von Signaltrennern sei vor allem sinnvoll:

- in ausgedehnten Anlagen mit langen Signalwegen
- wenn die Umgebung der Signalleitung in nennenswertem Umfang elektromagnetisch belastet ist
- wenn in den Eingängen der Steuerungen keine individuellen galvanischen Trennungen vorhanden sind
- bei Messspannungen mit hohem Potenzial und bei Gefahr von hohen Potenzialen im Fehlerfall.

Netzwerksicherheit

Heutige **Unternehmensnetzwerke** seien **sehr unflexibel**, schreibt das Sicherheitsforum in der Ausgabe 2-2015 (S. 49) auf der Grundlage einer Pressemitteilung der Fraunhoferinstitute. Jede Komponente, jeder

Router oder jeder Switch könne nur die eine Aufgabe übernehmen, für die sie hergestellt wurden. Seit etwa fünf Jahren arbeiteten deshalb Experten weltweit am flexiblen Netzwerk der Zukunft, dem Software Defined Networking (SDN). Der Nachteil: Es sei anfällig für Hackerangriffe. Wie sich SDN sicher machen lässt, wüssten die Forscher vom Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC). Bis heute gebe es noch keine ausreichenden Sicherheitsstandards für die Kommunikation zwischen den einzelnen Bestandteilen eines SDN. Die Forscher am AISEC machten sich dafür stark, dass ein internationaler Standard geschaffen wird.

Organisierte Kriminalität

Der BKA-Wochenlage vom 22. Mai ist zu entnehmen, dass am 12. Mai bei einer internationalen Aktion in Deutschland, den Niederlanden und Italien im Zusammenhang mit Ermittlungen der Kölner Polizei gegen mutmaßliche Mitglieder der **Cosa Nostra** wegen Verdachts der illegalen Arbeitnehmerüberlassung bzw. Steuerhinterziehung neun Haftbefehle vollstreckt sowie insgesamt 95 Privatwohnungen und Geschäftsräume durchsucht wurden. Bei den Hauptbeschuldigten handele es sich um mutmaßliche Mitglieder der Cosa Nostra. Bereits seit den 80er Jahren verfügten verschiedene Cosa Nostra-Familien über Stützpunkte in Deutschland, die für illegale Tätigkeiten, hauptsächlich im Baugewerbe genutzt würden. Beim PP Köln würden bereits seit Jahren erfolgreich Ermittlungsverfahren gegen Mitglieder der Cosa Nostra im Bereich der illegalen Arbeitnehmerüberlassung bzw. Steuerhinterziehung geführt. Es bleibe abzuwarten, ob die kriminellen Strukturen durch erfolgreiche Vermögensabschöpfungsmaßnahmen nachhaltig zerstört werden können.

Politisch motivierte Kriminalität

Im Mai veröffentlichte das Bundesinnenministerium die politisch motivierte Kriminalität im Jahr 2014. 32.700 solcher Straftaten wurden ermittelt, 3,3 Prozent mehr als im Vorjahr. An der Spitze lagen mit 38,4 Prozent Propagandadelikte. Es folgten Sachbeschädigungen mit einem Anteil von 20,2 Prozent. Im Vorjahresvergleich ist die Zahl politisch motivierter Gewalttaten um 18,3 Prozent auf einen Höchststand gestiegen. Auch die fremdenfeindlichen Straftaten sind mit 3.945 Fällen auf einen Höchststand seit Einführung des derzeitigen Erfassungssystems 2001 angewachsen (um 21,5 Prozent gegenüber 2013). Ein Anstieg um 25,2 Prozent war bei antisemitischen Straftaten zu verzeichnen (auf 1.596). Die Aufklärungsquote liegt mit 42,6 Prozent knapp unter der des Vorjahres (44,6 Prozent).

Polizeiliche Kriminalstatistik

Nach der vom Bundesinnenminister veröffentlichten Polizeilichen Kriminalstatistik wurden 2014 in Deutschland mehr als sechs Mio. Fälle – ohne Staatsschutzkriminalität und Verkehrskriminalität – registriert, 2,2 Prozent mehr als 2013. Die Häufigkeitszahl (Fälle pro 100.000 Einwohner = HZ) lag mit 7.530 höher als in den letzten Jahren, aber deutlich unter der HZ von 1993 (8.337). Signifikant zugenommen haben gegenüber dem Jahr 2013 ausländerrechtliche Straftaten (um 41,5 Prozent) und Beförderungserschleichungen (um 15,2 Prozent). Die Kriminalitätsbelastung war am höchsten in Berlin (HZ 15.873), am niedrigsten in Bayern (5.164) und Baden-Württemberg (5.592). Die Gesamtaufklärungsquote lag 2014 bei 54,9 Prozent. Eine ausführlichere Zusammenfassung – insbesondere zu den die Wirtschaft besonders belastenden Kriminalitätsphänomenen – findet sich

auf der Webseite von Securitas Deutschland (News/Sicherheitslage).

Produktpiraterie

EUROPOL hat am 29. April den **Lagebericht 2015 zu Produktfälschungen in der EU** veröffentlicht. Obwohl die Mehrzahl der gefälschten Produkte, die in Europa im Verkehr seien, außerhalb der EU produziert worden seien, ist der Bericht darauf fokussiert, wie die EU-eigene Produktion anwachse, aus Belgien, der tschechischen Republik, Italien, Polen, Portugal, Spanien und Großbritannien. Es entstehe ein zunehmend profitables Geschäft für die organisierte Kriminalität. Es sei festgestellt worden, dass Produktfälscher, die mit signifikant geringerem Risiko tätig seien, Verbindungen mit anderen Deliktsarten wie Menschenhandel – vor allem für die Arbeitsausbeutung – und mit anderen kriminellen Gruppen hätten, die aus verschiedenen Ländern in und außerhalb von Europa stammten. Die signifikanteste Möglichkeit für den Vertrieb dieser gefälschten Waren bilde das Internet. Der Bericht erforscht hoch mobile, spezialisierte chinesische organisierte kriminelle Gruppen, die in den Vertrieb gefälschter Produkte involviert seien. Soweit sie in Italien operierten, stünden sie der Camorra nahe und arbeiteten mit ihr beim Import gefälschter Produkte zusammen. Chinesische Diaspora-Gemeinschaften seien in ganz Europa verteilt und es gebe eine Konzentration chinesischer Produktfälscher-Geschäfte in mehreren italienischen Provinzen, die alle in Verbindung stünden mit der Bekleidungs- und Modeindustrie. Nach China komme Indien die größte Bedeutung bei der Fälschung pharmazeutischer Produkte für Europa zu, ebenso die Türkei für Lebensmittel, Indonesien wegen schwacher Gesetzgebung und Korruption, die Philippinen wegen geringer Strafverfolgung.

Deutschland wird derzeit mit Imitaten geradezu überschwemmt, berichtet das Magazin Focus am 30. Mai. Knapp sechs Mio. Fälschungen, von der Bremsscheibe bis zum Turnschuh, habe der Zoll 2014 auf dem Verkehr gezogen – rund 50 Prozent mehr als 2013 (2012: 3,2 Mio., 2013: 3,9 Mio., 2014: 5,9 Mio.). Erstmals hätten sich darunter mehr Körperpflegeprodukte befunden als Textilien. Bei den Arzneimitteln habe der Anstieg sogar 61 Prozent betragen. Das bedeute Milliardenschäden für die Industrie, aber auch beträchtliche Risiken für die Verbraucher. Bis zu eine Million Menschen weltweit würden jährlich sterben, weil sie gefälschte Tabletten schlucken, schätzt INTERPOL. Der Handel mit wirkungslosen Pülverchen, imitierten Pillen und nutzlosen Cremes sei lukrativer als der Schmuggel von Heroin. Die Hälfte der Medikamente, die online gehandelt werden, seien Fälschungen. Aber 90 Prozent der Menschen in Europa hielten es einer Umfrage des Markenverbandes zufolge für unproblematisch, Plagiate zu besitzen. Gerade klage der Luxusgüterhersteller Kering, das Mutterhaus von Gucci, Brioni und Yves Saint Laurent, gegen Alibaba. Der Vorwurf: Die Chinesen böten auf ihrer Plattform ein Umfeld für eine ganze Armee von Fälschern. Der größte Teil der Plagiate komme aus China. 73 Prozent der an Europas Grenzen sichergestellten Imitate stammten aus den ostasiatischen Fälscherfabriken, habe jüngst die EU-Kommission mitgeteilt. Weltweit, so schätze die Internationale Handelskammer ICC, dürfte der Schaden durch Produkt- und Markenpiraterie 2015 kaum vorstellbare 1,7 Bio. Dollar betragen. Allein den deutschen Maschinenbau kosteten Plagiate und Patentverletzungen jährlich knapp acht Mrd. Euro.

Rechenzentrumssicherheit

Malte Gloth, Siemens-Division Building Technologie, befasst sich in der Fachzeitschrift GIT (Ausgabe 5-2015, S. 72–75) mit dem Schutz von Rechenzentren durch **intelligente Gebäudeautomation und Sicherheitstechnik**.

Integrierte Gesamtlösungen erlaubten die professionelle Steuerung und das transparente Management der komplexen Abläufe und Prozesse der Rechenzentrumsinfrastruktur. Gegen Stromausfälle müssten sich Rechenzentrumsbetreiber selbst absichern. Dafür werde die Stromverteilung redundant ausgelegt und mit USV-Anlagen und Generatoren ergänzt. Neben der Sicherstellung der hohen Verfügbarkeit des Rechenzentrums sollten auch die Mitarbeiter im Alltag geschützt und Brandgefahren minimiert werden. Hier würden Stromschienen Flexibilität für den Betrieb und eine Senkung des Brandrisikos bieten. Sogenannte Ansaugrauchmelder würden über ein Ansaugrohrnetz permanent Luftproben nehmen und sie auf Rauchpartikel untersuchen. Löst bei einem Brand in einem Rechenzentrum eine automatische Gaslöschanlage aus, könnten Festplatten Schaden nehmen. Eine Studie von Siemens habe ergeben, dass die Schäden durch den hohen Geräuschpegel ausgelöst werden, die konventionelle Löschanlagen erzeugen. Für die sichere und leise Löschung habe Siemens deshalb die Silent Extinguishing Technology entwickelt.

Risikobewertung

17 Prozent der 516 von der Allianzversicherung befragten Risikomanager aus mehr als 40 Ländern bezeichneten Cyberkriminalität, Spionage und Datenmissbrauch als das größte Geschäftsrisiko, berichtet COMPUTERWOCHE.de am 13. Mai. Unter den zehn größten Geschäftsrisiken liege IT-Sicherheit auf Platz 5. Die größte Bedrohung sehen die Manager in der Betriebs- und Lieferkettenunterbrechung (46 Prozent), gefolgt von Naturkatastrophen (30 Prozent), Feuer und Explosion (27 Prozent) und rechtlichen Veränderungen (18 Prozent).

Schließsysteme

„Combo Breaker" nenne der Hacker Samy Kamkar seinen selbstentwickelten **Schlossknacker,** meldet SPIEGEL ONLINE am 15. Mai. Die Einzelteile des Maschinchens stammten aus dem 3-D-Drucker, das Gerät könne runde Kombinationsschlösser in kurzer Zeit knacken. Zum Nachbau des Gadgets brauche man zwei Motörchen, die das Schloss drehen und prüfen, ob es sich schon öffnen lässt, einen optischen Sensor und eine Arduino-Plattform, deren Software die Arbeitsschritte koordiniert. Kamkar nutze mit seinem Roboter einen Produktionsfehler beim Schlosshersteller Master Lock aus.

Sonderschutzfahrzeug

Die Nachfrage nach Sonderschutzfahrzeugen sei in den letzten Jahren stetig angestiegen, heißt es in der Zeitschrift PROTECTOR (Ausgabe 5-2015, S. 50/51). Zur Bewertung der Widerstandsfähigkeit eines Fahrzeugs gegen verschiedene Munitionsarten und Geschosstypen existierten mehrere Normen und Richtlinien. Die aktuelle Richtlinie mit produktspezifischen Anforderungen an die Durchschusshemmung und Prüfverfahren BRV 2009 (Bullet Resistant Vehicles) weise zur BRV 1999 einige signifikante Unterschiede auf. Einsätze in Krisenländern hätten ferner den notwendigen Schutz gegenüber IEDs – Unkonventionelle Spreng- und Brandvorrichtungen – gezeigt. Daher seien in der Norm ERV 2010 (Explosive Resistant Vehicles) die Anforderungen für einen entsprechenden Schutz gegen Sprengwaffen definiert. Bei der Frage der notwendigen Panzerung dürften auch die unvermeidlichen Schwachstellen, zu denen vor allem die Übergänge wie alle Fugen, Türspalten, Stöße, Überlappungen, Verschraubungen und Verschweißungen, Kabeldurchführungen, Belüftungsdurchlässe oder Tank und Tanköffnungen gehörten, nicht

vernachlässigt werden. Letztlich müssten sich alle schützenden Komponenten bei den zivilen Ausführungen in das ursprüngliche Fahrzeugdesign harmonisch einfügen, denn von der Unauffälligkeit gehe immer noch der beste Schutz aus.

Spionage

Der NSA habe deutschen Medienberichten zufolge die Abhöranlagen des BND vor allem für **Spionage gegen europäische Staaten** benutzt, verlautet zeit.de am 29. April. Nach Angaben der Süddeutschen Zeitung, des NDR und des WDR würden von Bad Aibling aus unter anderem hochrangige Beamte des französischen Außenministeriums ausspioniert, ebenso wie Beamte des Élysée-Palastes und der EU-Kommission. Hinweise auf gezielte Wirtschaftsspionage soll es dagegen nur vereinzelt geben. Deutsche Politiker befinden sich demnach nicht auf der Liste, auch sollen kaum deutsche Unternehmen betroffen sein. Nach den bisherigen Feststellungen seien Unternehmen vor allem betroffen, weil die USA nach Hinweisen auf illegale Exportgeschäfte gesucht hätten. Die FAZ meldet am 2. Mai, die Airbus-Gruppe habe Strafanzeige gegen Unbekannt wegen des Verdachts auf Industriespionage gestellt.

Verfassungsschutz will deutschen Unternehmen helfen, titelt die FAZ am 22. Mai. Er setze auf eine engere **Zusammenarbeit mit Wirtschaftsverbänden**. Das BfV und der BDSW hätten eine Absichtserklärung unterzeichnet, um Unternehmen einen besseren Schutz gegen Wirtschaftsspionage anzubieten, diese zu sensibilisieren und zu informieren. Es gehe um Prävention und Abwehr. Das BfV und die 16 Landesämter für Verfassungsschutz bieten Schulungen und Vorträge für Multiplikatoren an, wie es Verbände sind. Für den BDSW habe das den unmittelbaren Vorteil, den Kontakt zu den eigenen Kunden zu intensivieren. Geschädigte müssten sich nicht einer Behörde offenbaren. Vielen Unternehmen sei die Bedrohung durch Wirtschaftsspionage gar nicht klar. Kleine und mittelständische Unternehmen unterschätzten oft, dass ihre Patente Kronjuwelen sind. Vor einem Jahr habe der Verfassungsschutz eine ähnliche Vereinbarung mit dem VDMA getroffen – mit positiver Resonanz. Der Verfassungsschutz sei dankbar für jedwede Information aus Unternehmen über Angriffe ausländischer Nachrichtendienste – nicht, um sie nur aufzusaugen, sondern sie an andere weiterzugeben – als Kampf gegen Spionage und Sabotage, die schwer schätzbare, aber milliardenhohe Schäden verursachten.

Die USA werfen China regelmäßig Wirtschaftsspionage vor, heißt es in der FAZ am 21. Mai. Nun gebe es einen neuen Fall, in den mehrere **chinesische Professoren** verwickelt seien. Amerikanische Behörden hätten insgesamt sechs Chinesen wegen Wirtschaftsspionage angeklagt und ihnen vorgeworfen, Betriebsgeheimnisse mehrerer amerikanischer Unternehmen gestohlen zu haben. Dies sei geschehen, um Universitäten und Unternehmen einen Vorteil zu verschaffen, die von der chinesischen Regierung kontrolliert würden. Zwei der angeklagten Professoren hätten bei zwei kleineren amerikanischen Technologieunternehmen gearbeitet und sollen dort Betriebsgeheimnisse gestohlen haben. Es handele sich um Technologien, die vor allem in mobilen Geräten zum Einsatz kommen. Die Männer hätten von den USA aus nach Partnern unter chinesischen Universitäten gesucht, um die Technologie nach China zu bringen. Die Tianjin University habe sich interessiert gezeigt. 2009 hätten die Männer ihre Posten bei den amerikanischen Unternehmen gekündigt, seien nach China zurückgekehrt und hätten Professuren an der Universität angenommen. Sie hätten dann zusammen mit der Universität ein Unternehmen namens ROFS Microsystem gegründet, das sich auf diese Technologie spezialisiert habe.

Steuerhinterziehung

Das Hauptzollamt Rosenheim teilt am 21. April mit: Zöllner kontrollierten einen Lkw, der auf der A 8 in Richtung München unterwegs war. Laut Frachtpapieren hatte der Sattelzug mit Schweizer Kennzeichen Aluprofile geladen, die von der Türkei in die Schweiz transportiert werden sollten. Bei der Durchsuchung seien dann auch mehrere Holzkisten zum Vorschein gekommen, die mit Aluprofilen befüllt zu sein schienen. Beim Öffnen der ersten Kiste hätten die Beamten allerdings festgestellt, dass es sich bei den sichtbaren Aluprofilen lediglich um eine fingierte Außenwand aus Aluminium handelte. Tatsächlich seien sämtliche Kisten mit Parfüm und T-Shirts gefüllt gewesen. Insgesamt hätten die Zöllner 590 Kartons mit fast 60.000 Parfümflaschen verschiedener Marken und 1.400 T-Shirts eines namhaften Herstellers sichergestellt. Die Transportfirma sei vor zwei Jahren gelöscht worden. Auch den Empfänger der Ware habe es nicht gegeben (Scheinfirma).

Transportdiebstahl

Der ASW hat folgende Tatorte aktueller Planen-Schlitzereien und sonstiger Ladungsdiebstähle auf Fahrstrecken im Bundesgebiet mitgeteilt:

- 17.–19. April, Chemnitz-Bernsdorf, Parkbucht Thalheimer Straße
- 20.–21. April, Nossen-Neubodenbach, Rasthof an der Straße im Industriegebiet
- Nacht zum 22. April, Peine, Heinrich-Hertz-Straße, Lkw-Parkplatz des Autohofes Peine
- 24. April, A 13, Thiendorf, Parkplatz Schönfeld
- 24.–25. April, Rathenow, Dr.-Salvador Allende-Straße
- 5./6. Mai, A 72, Plauen, Tank- und Rastanlage Vogtland Nord
- 12. Mai, A 10, Raststätte Michendorf-Nord, Fahrtrichtung Magdeburg
- 13./14. Mai, A 8, Karlsbad, Autobahnparkplatz Steinig
- Nacht zum 14. Mai, A 2, Lippetal-Lippborg, Parkplatz am Strängenbach
- 16./17. Mai, Bitterfeld-Wolfen, Parkplatz in der Anhaltstraße
- Nacht zum 19. Mai, A 6, Gemarkung Bretzfeld, Parkplatz Sommerhalden, Fahrtrichtung Öhringen
- 20. Mai, A 6, Gemarkung Bretzfeld, Parkplatz Bauernwald
- Nacht zum 21. Mai, A 13, Kasel-Golzig, Parkplatz Am Bugkgraben nahe AS Freiwalde

Unternehmenssicherheit

Durch die **Digitalisierung** komme es nicht nur zu Veränderungen von Produkten und Geschäftsmodellen, sondern auch in der Organisation von Unternehmen, heißt es in silicon.de am 27. April. Zu diesem Ergebnis komme eine aktuelle Studie von BitKOM. Sie sei repräsentativ für die Gesamtwirtschaft. Vor allem die Kommunikation mit Kunden beschleunige sich durch die Digitalisierung, hätten 79 Prozent der 505 befragten Geschäftsführer und Vorstände von Unternehmen ab 20 Mitarbeitern angegeben. Die Digitalisierung führe der Studie zufolge auch zu transparenteren Entscheidungsprozessen innerhalb von Unternehmen. Dies empfänden zumindest 52 Prozent der Befragten. In kleineren Unternehmen (20–49 Mitarbeiter) habe sich die Digitalisierung weniger stark auf organisatorische Flexibilität und die Transparenz der Entscheidungsprozesse ausgewirkt. Die Digitalisierung sei gerade für kleinere Unternehmen eine Chance, noch schneller und effizienter zu werden. Davon profitierten auch die Mitarbeiter, die besser in Entscheidungsprozesse einbezogen würden und motivierter an die Arbeit gingen.

Veranstaltungssicherheit

Die Fachzeitschrift GIT weist in der Ausgabe 5-2015, S. 18, auf den „Leitfaden für Feuerwehr, Sicherheitsbehörde und Polizei sowie Veranstalter und deren Sicherheitsdienstleister" der Berufsfeuerwehr München hin, der neu aufgelegt werde, weil das Praxiswissen durch die jährliche Bearbeitung von über 2.000 Veranstaltungen und die Prüfung von über 70 Sicherheitskonzepten jährlich ständig erweitert werde. Ziel sei es, Praxis und Wissenschaft so zu verbinden und die Ergebnisse aufzubereiten, dass das Wissen universell anwendbar, leicht verständlich und der Prozess „Veranstaltungssicherheit" damit transparent gestaltet werden könne. Der Leitfaden stehe nach dem 13. Juni zum kostenlosen Download auf der Internetseite der Berufsfeuerwehr München zur Verfügung.

Verschlüsselung

Das Gremium für Internet-Standards dokumentiert Richtlinien für den sinnvollen Einsatz der Transportverschlüsselung TLS, berichtet heise.de am 18. Mai. Der RFC enthalte gute Anleitungen, Tipps und Hinweise auf Fallstricke für jeden, der Verschlüsselung selbst einrichtet. So ächte der RFC 7525 unter anderem SSLv3, RC4 und für den Export verkrüppelte Verschlüsselung mit weniger als 112 Bit Schlüssellänge. Deren Einsatz verbiete das Dokument mit dem formalisierten „MUST NOT" der IEZF-Standards. Von der Verwendung bedenklicher und eigentlich nicht mehr erwünschter Verfahren wie 3DES für die Verschlüsselung und RSA für den Schlüsselaustausch rät die IETF mit dem schwächeren SHOULD NOT deutlich ab. Der RFC ergehe sich nicht nur in Verboten, sondern bewerbe und fordere auch den Einsatz erwünschter Techniken und Optionen. So schreibe er die Unterstützung und sogar Bevorzugung von Forward Secrecy via Diffie-Hellman vor. Insgesamt bündele der RFC tatsächlich realitätsnahe Best Practices, ohne dabei das Ziel, die aktuelle Situation deutlich zu verbessern, aus den Augen zu verlieren.

Videoüberwachung

Business Intelligence durch IP-basierte Videoüberwachung ist ein Thema in der Ausgabe 5-2015 der Fachzeitschrift GIT (S. 48/49). Business Intelligence bezeichne Verfahren zur systematischen Sammlung, Auswertung und Darstellung von Geschäftsdaten mit Hilfe IT-basierter Lösungen. Ziel sei es, Erkenntnisse zu gewinnen, die es ermöglichen, die Qualität operativer und strategischer Entscheidungen zu verbessern. Durch die so gewonnenen Erkenntnisse könnten Unternehmen ihre Geschäftsabläufe sowie Kunden- und Lieferantenbeziehungen profitabler gestalten, Kosten senken, Risiken minimieren und die Wertschöpfung steigern. Beispiele: Zapfsäulen an Tankstellen werden deaktiviert, wenn ein bekannter Benzindieb davor hält. Die Demografie von Käufern bestimmter Waren könne aus der Kombination von Kassendaten und Videobildern zu Marketingzwecken analysiert werden. Aus dem Zusammenspiel von „Video Surveillance" und „Business Intelligence" werde „Business Video Intelligence" (BVI). Die Datenbank als zentrales Element der BVI-Anwendung müsse in der Lage sein, große Datenmengen in Form von Videobildern ebenso in Echtzeit zu speichern wie eine Vielzahl einzelner Ereignisse, z. B. Buchungen oder Scan-Vorgänge. BVI erweitere den Fokus der dargebotenen Informationen. Neben objekt- und ereignisbezogenen Informationen träten aggregierte Informationen, die empirische Betrachtungen ermöglichen. Offene und einfach zu konfigurierende Schnittstellen, die die Kommunikation mit Drittsystemen und das Auslösen von Folgeaktionen ermöglichen, rundeten schließlich den Funktionsumfang einer BVI-Lösung ab.

Wohnungseinbruch-diebstahl

Die Zahl der Wohnungseinbrüche in Deutschland ist in den vergangenen fünf Jahren um ein Drittel gestiegen, heißt es in der FAZ am 7. Mai. In rund 20 Prozent der Fälle sei ein Bewohner während des Einbruchs anwesend gewesen, wie aus dem **Einbruch-Report 2015 des GDV** hervorgehe. Insgesamt seien der deutschen Versicherungswirtschaft Schäden in Höhe von 490 Mio. Euro 2015 entstanden. Der durchschnittliche Schaden habe mit 3.250 Euro auf Vorjahresniveau gelegen. Die Täter würden vorwiegend in den Herbst- und Wintermonaten aktiv. Zwischen Oktober und Januar werde fast die Hälfte aller Einbrüche verzeichnet. Nur 15 Prozent der Taten erfolgten zwischen 22 und 8 Uhr. Die Täter sähen die besten Aussichten, wenn die Opfer bei der Arbeit oder beim Einkauf sind. Von 10 Uhr an steige die Zahl der Einbrüche erheblich an. Zwischen 12 und 14 Uhr sowie zwischen 16 und 18 Uhr würden die meisten Einbrüche verzeichnet.

Zugangskontrolle

Passwörter böten zwar ein gewisses Maß an Sicherheit, wenn bestimmte Regeln befolgt werden, schreibt TECCHANNEL.de am 3. Mai, ein Restrisiko bleibe aber. Oft bestehe auch kein durchgehendes Passwort-Management, und es würden keine Richtlinien für die Erstellung und Erneuerung starker Passwörter und den korrekten Umgang damit durchgesetzt. Biometrische Verfahren würden als modernere Authentifizierungsmethode gelten. Tatsächlich hätten beide Methoden Vor- und Nachteile und könnten nicht ohne Weiteres durch die jeweils andere Methode ersetzt werden. Sie ließen sich aber so kombinieren, dass sie sich optimal ergänzen.

Zutrittskontrolle

Wer in besonders schutzbedürftige Unternehmensbereiche hinein will, müsse sich ausweisen und dürfe nur einen räumlich und zeitlich begrenzten Zugang haben, heißt es in der FAZ am 5. April. Doch zunehmend würden Kriminelle die etablierten Zugangssysteme überlisten. Sicherheitsexperten forderten daher **neue Schutztechniken für sensible Anlagen**. Indische IT-Spezialisten setzten deshalb auf Einmal-Kennwörter. Die könnten zusätzlich zu Funkchips oder biometrischen Zutrittssicherungen eingebaut werden und für eine erhebliche Steigerung des Sicherheitsniveaus sorgen. In einigen Bereichen seien sie sogar den traditionellen Zugangssicherungen überlegen. So hätten etwa die Sicherheitsfachleute des indischen Schließanlagenherstellers Godrej Windenergieanlagen mit einem Zugangssystem auf der Basis von Einmal-Passwörtern ausgestattet. Der Wartungstechniker vor Ort fordere per Smartphone ein nur einmal gültiges Zutrittspasswort für eine bestimmte Tür zu einem bestimmten Windrad an. Der Zugangsserver in der Unternehmenszentrale schicke dem Techniker daraufhin ein Einmal-Kennwort zu, natürlich verschlüsselt und über ein gesichertes virtuelles privates Netzwerk. Dasselbe Kennwort werde auch an das Zugangsgerät mit Tastatur geschickt, das der Techniker als „Schlüsselersatz" bei sich hat. Der Techniker gebe das empfangene Einmal-Kennwort in sein Zugangsgerät ein. Dort werde es mit dem vom Zugangsserver empfangenen verglichen. In Rechenzentren und anderen Hochsicherheitsbereichen könne die Zugangskontrolle via Einmal-Kennwort auch mit anderen Zugangssicherungen kombiniert werden. Gefragt seien bei solchen Kombinationslösungen biometrische Anwendungen. Das Einmal-Kennwort lasse sich mit Funkchips, Zutrittskarten oder richtigen Schlüsseln kombinieren. In Indien sei die Nachfrage nach solchen Zutrittskontrollsystemen sehr groß. In Europa hätten Sicherheitsexperten die Lösung erst neuerdings entdeckt.

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