Focus on Security

Ausgabe 08, August 2017

SECURITAS

Anschläge

Am 17. Juli sind vor einer Polizeiwache in Bielefeld Brandanschläge auf neun **Einsatzfahrzeuge der Bereitschaftspolizei** verübt worden, meldet das westfalenblatt.de. Sechs Fahrzeuge seien, wie die FAZ berichtet, völlig zerstört worden. Die betroffenen Transportfahrzeuge seien Wagen der Hundertschaft gewesen, die auch beim G20-Gipfel in Hamburg im Einsatz war. Der Brand sei der zweite Vorfall in Nordrhein-Westfalen innerhalb weniger Tage. Schon in der vergangenen Woche seien **Polizeiautos in Münster** erheblich beschädigt worden. Unbekannte hätten Sprüche wie „Welcome to hell" in 15 Fahrzeuge der Hundertschaft geritzt. Da auch Beamte aus Münster bei dem Gipfel im Einsatz waren, gehen die Ermittler von einem Bezug aus. Es sei ein Sachschaden in Bielefeld von etwa 300.000 Euro, in Münster von rund 70.000 Euro entstanden.

Betrug

Nach einer Meldung von heise.de vom 10. Juli warnt das BSI Unternehmen vor der „**Chef-Masche**", mit der sich Trick-Gauner in E-Mails als hochrangiges Management-Mitglied oder Handelspartner ausgeben und arglose Mitarbeiter zu hohen Überweisungen von Geschäftskonten veranlassen. Das BSI habe Kenntnis von einer Liste mit rund 5.000 potenziellen Zielpersonen. Alle Mitarbeiter, die zu Zahlungsvorgängen berechtigt sind, sollten auf diese kriminelle Methode hingewiesen und sensibilisiert werden. Vorrangig würden Mitarbeiter aus der Buchhaltung oder dem Rechnungswesen angesprochen. Generell rege das BSI an, nur allgemeine Kontaktadressen auf einer Unternehmenswebseite zu veröffentlichen. Es müsse Kontrollmechanismen geben, um ungewöhnliche Zahlungsaufforderungen sowie Absenderadressen und Plausibilität des Inhalts einer Mail zu überprüfen.

Biometrie

Ab Frühjahr 2018 müssen am Flughafen Wien alle Passagiere bei der Einreise aus einem Nicht-Schengen-Land durch eine **Gesichtserkennungsschleuse**, meldet aero.de am 21. Juli. Dabei würden Gesicht und Passbild elektronisch verglichen. Die biometrische Gesichtserkennung solle auch auf die Überwachungskameras ausgedehnt werden. Geplant sei auch eine Identifikation der Reisenden mittels Handvenenscanner.

Brandschutz

Dr. Jacob Duvigneau, Institut für Schadenverhütung und Schadenforschung der öffentlichen Versicherer, befasst sich in der Ausgabe 2-2017 von 2+2 report, S. 18–21, mit **Bränden in holzverarbeitenden Betrieben**. Schon aufgrund der Brandgefahren, die von der Holzbearbeitung mit schnelllaufenden Maschinen ausgehen, oder wenn man allein die Brandgefahr von Holzstäuben betrachtet, werde schnell nachvollziehbar, wieso holzbearbeitende und -verarbeitende Betriebe als „feuergefährdete Betriebsstätten" gelten. Der Autor beschreibt zwei im Abstand von zwei Jahren in ein und demselben holzverarbeitenden Großbetrieb entstandene Schäden, wobei zumindest dem zweiten Schaden erhebliche Planungsmängel vorausgegangen seien. Aufgrund der ohne jegliche brandschutztechnische Abtrennung (z. B. durch Schnellschluss-Schieber) vorgenommenen Einspeisung der abgesaugten Späne in das Spänesilo des Nachbargebäudes habe eine Verbindung beider Gebäude bestanden, weshalb eine Brandübertragung ermöglicht worden sei. Das sei nicht im Sinne der einschlägigen Vorschriften gewesen.

Dipl.-Ing. Christoph Benning und Dipl.-Ing. Uwe Schmies weisen in der Ausgabe 2-2017 der Zeitschrift s+s report, S. 22/23, darauf

hin, dass die Suche nach Filmen zur Vorbereitung von Brandschutzschulungen jetzt einfacher sei. Unter www.brandschutzfilme.de fänden Akteure im vorbeugenden und abwehrenden Brandschutz und im Feuerwehrwesen ab sofort Links zu mehr als 120 direkt einsetzbaren Brandschutzfilmen oder -clips in 36 Fachkategorien. Sie beschreiben den Aufbau und Nutzen der Mediathek für Brandschutz- und Feuerwehrfilme.

Dipl.-Ing. (FH) Rudi Messmer, Menzerna polishing compounds GmbH & Co. KG, befasst sich in der Zeitschrift s+s report, Ausgabe 2-2017, S. 24–26, mit der **Selbstentzündung von Polierabfällen**. Das Polieren von Aluminium berge ein nicht zu unterschätzendes Brandrisiko: Polier- und Schleifabfälle könnten sich ohne Einfluss einer Zündquelle oder von Sonnenlicht selbstständig erwärmen und in der Folge entflammen. Die Lagerung unter Wasser könne den Brand nur temporär verhindern, denn trocknet der Abfall oberflächlich, könne es wieder zur Selbstentzündungsreaktion kommen. Dank einer Neuentwicklung lasse sich der Gefahr entgegensteuern: Polierpasten mit Heat Absorbing Technology (HAT) würden das Selbstentzündungsrisiko von Aluminium-Polierabfällen um 90 Prozent senken. Der Autor beschreibt unter anderem die Rahmenbedingungen für die Wirkung des Additivs und die Vorteile für Industrieunternehmen.

Eine neue **Software für Brandschutzbegehungen** wird in s+s report, Ausgabe 2-2017, S. 60/61, vorgestellt. Für einen effektiven Brandschutz sei auch entscheidend, die Wirksamkeit aller Maßnahmen immer wieder zu überprüfen. Deshalb seien regelmäßige Begehungen der Gebäude durch den Brandschutzbeauftragten unabdingbar. Die Begehungen müssten sorgfältig protokolliert werden. Eine für die Dokumentation im Brandschutz entwickelte Software sei „Themis". Bei einer Begehung mit Themis würden alle benötigten Daten per Tablet erfasst. Die Informationen würden in die zuvor hinterlegten Gebäudepläne eingefügt. Für alle Anlagen könnten Wartungsintervalle hinterlegt und Kontrollen definiert werden. Ein weiterer großer Vorteil von Themis sei, dass es lückenlose und manipulationssichere Protokolle generiere.

Compliance

Dipl.-Wirt.-Inform. Henry M. Hanau, Berater für IT-Sicherheit, bezeichnet in s+s report, Ausgabe 2-2017, S. 50–53, IT-Sicherheit nach der VdS-Richtlinie 3473 als Instrument der IT-Compliance. **IT-Compliance** sei, richtig kommuniziert, ein geschäftsausweitendes Qualitätsmerkmal. Der Autor behandelt die Datenschutzreform der EU, neue Bedingungen für Cyberrisiko-Versicherungen des GDV und die Lösungswirkung der VdS-Richtlinie 3473. Deren Ziel sei die Schaffung eines umfassenden Bildes der aktuellen Lage, das Trennen der „kritischen" Ressourcen von solchen, die mit aufwandsärmeren Standardmaßnahmen („Basisschutz") bedacht werden können, sowie die Angabe von konkreten, der IT-Sicherheit zuträglichen Vorgehensweisen, um ein ausgewogenes IT-Sicherheitsniveau einzurichten.

Datenschutz

Der EuGH hat das von der EU und Kanada geplante Abkommen zum Austausch von **Fluggastdaten** blockiert, meldet zeit.de am 26. Juli. Die Luxemburger Richter hätten entschieden, dass mehrere der vorgesehenen Bestimmungen nicht mit den von der EU anerkannten Grundrechten vereinbar sind. Das geplante Abkommen greife in das Grundrecht auf Achtung des Privatlebens ein und stelle ferner einen Eingriff in das Grundrecht auf Schutz personenbezogener Daten dar. Zu den Fluggastdaten gehörten Informationen, die von Fluggesellschaften

im Buchungsprozess sowie beim Check-in gespeichert werden. Das seien neben dem Namen des Reisenden zum Beispiel Angaben zum Gepäck, die Sitznummer und Zahlungsdaten wie die Kreditkartennummer.

Drohnen

Die Deutsche Flugsicherung (DFS) wappne sich für den rasant wachsenden Einsatz von unbemannten Flugobjekten, berichtet die FAZ am 27. Juli. Es werde nicht mehr lange dauern, dann werde es hierzulande eine Mio. Drohnen geben, habe der Vorsitzende der DFS, Klaus-Dieter Scheurle, gesagt. Es sei nicht Aufgabe der DFS, die neue Technik zu behindern, sondern ihr „den Weg zu bereiten und Chaos zu verhindern". Mit der DHL arbeite man an einer Nutzung außerhalb der Sichtweite des Steuerers. Drohnen tauchten bisher nicht auf den Schirmen der Flugsicherung auf, weil sie klein sind und niedrig fliegen. Mit der Deutschen Telekom arbeite die DFS an einem Modul, das es erlaube, die unbemannten Flugobjekte über Mobilfunksignale zu orten. Im ersten Halbjahr 2017 habe die DFS 41 Behinderungen durch Drohnen im Luftverkehr registriert. Um Privatleuten sicheres Drohnenfliegen zu erleichtern, habe die DFS eine kostenlose Handy-App entwickelt, die für jeden Standort in Deutschland zeigt, ob die Geräte dort starten dürfen.

Einbruch

2016 seien den deutschen Versicherern 140.000 versicherte Einbrüche gemeldet worden. Dafür hätten sie 470 Mio. Euro an ihre Kunden geleistet. Das gehe aus dem **Einbruch-Report des GDV** - vor, auf den s+s report in der Ausgabe 2-2017, S. 7, hinweist. Neben der Einbruchstatistik enthalte der Report die Ergebnisse einer aktuellen Forsa-Umfrage zum Thema Einbruch. Fast 80 Prozent der Befragten meinten, dass das Einbruchsrisiko in den letzten fünf Jahren zugenommen hat. Jeder Dritte habe Angst vor Einbrechern. Das persönliche Risiko werde hingegen von vielen unterschätzt. Die Umfrage zeige auch, dass vielerorts eklatante Sicherheitslücken klaffen. Nur etwa ein Viertel der Befragten habe angegeben, dass Wohnung bzw. Haus mit abschließbaren Fenstergriffen, zusätzlichen Sicherungen an Balkon- oder Terrassentüren ausgerüstet ist. Der mechanische Einbruchschutz werde meist sträflich vernachlässigt. Mieter wollten nicht in fremdes Wohneigentum investieren.

Den möglichen Nachweis von „**Lockpicking**" thematisiert die Zeitschrift Potector im Special Zutrittskontrolle, S. 44/45. Laut Einbruch-Report des GDV seien 2016 rund 140.000 versicherte Wohnungseinbrüche mit einem Gesamtschaden von 470 Mio. Euro gemeldet worden. Insbesondere im gewerblichen Bereich würden Einbrecher auf spezielle Werkzeuge zurückgreifen, die eigentlich für Schlüsseldienste entwickelt wurden. Sehr beliebt sei der „Elektro-Pick", ein elektrisch betriebenes Rüttel- und Bewegungsgerät, das mit Aufsperrhilfsmitteln wie Schlange, Haken, Halbrund oder Diamand bestückt ist. Es sei möglich, die Stifte im Sicherheitsschloss zu manipulieren. Erfahrene Lockpicker öffneten durchschnittlich sichere Schlösser in weniger als 30 Sekunden.

Einbruchmeldeanlagen (EMA)

Frank Jesse, LKA Baden-Württemberg, weist in der Ausgabe 2-2017 von s+s report, S. 36/37, darauf hin, dass sich die Polizei Baden-Württemberg dazu entschlossen habe, nach dem Auslaufen der Konzessionsverträge zum 31. Dezember 2016 das sogenannte „ÜEA-Providermodell" einzuführen. Sie habe damit absolutes Neuland betreten. Wesentlicher Unterschied zwischen dem

bisherigen Konzessions- und dem neuen ÜEA-Providermodell sei, dass die Alarmempfangseinrichtungen nicht mehr von den bisherigen Partnerunternehmen betrieben werden, sondern von der Polizei selbst. Die regionalen Beschränkungen der klassischen Konzessionen seien weggefallen. Ziel sei eine Kostenreduzierung für den Endkunden sowie die Möglichkeit, dass ÜEA-Betreiber eine freie Auswahl zwischen den gelisteten Providern treffen können.

Zwangsläufigkeit als „Best Practice" nun **europaweit genormt**, titelt Dipl.-Ing. Günter Grundmann, VdS Schadenverhütung, in s+s report, Ausgabe 2-2017, S. 46–48. Der Autor erklärt den Ausdruck „Zwangsläufigkeit" und begründet die europäische Normung. Auf Initiative der deutschen Delegation sei eine vollständige Beschreibung aller erforderlichen Maßnahmen zur Umsetzung der Zwangsläufigkeit erstmalig in einer Technischen Spezifikation (TS), sozusagen dem Vorstadium zur Norm, aufgenommen worden. Die TS 50131-12 (Methoden und Anforderungen zur Scharf- und Unscharfschaltung von Einbruchmeldeanlagen (EMA)) benenne die Zwangsläufigkeit quasi als „Best Practice" und beschreibe sie in allen Einzelheiten. Durch die Anwendung würden sich Fehler beim Verlassen und Betreten eines überwachten Bereiches auf ein Mindestmaß verringern lassen.

Extremismus

Nach dem am 4. Juli veröffentlichten **Verfassungsschutzbericht** waren **2016** von den insgesamt 41.549 politisch motivierten Straftaten 30.958 (74,5 Prozent) mit extremistischem Hintergrund ausgewiesen, d. h. sie zielten darauf ab, Verfassungsgrundsätze zu beseitigen, die für die freiheitliche demokratische Grundordnung prägend sind. Davon waren 22.471 rechtsextremistisch, 5.230 linksextremistisch und 2.566 ausländerextremistisch geprägt. 1.600 rechtsextremistische Straftaten waren Gewalttaten. Das entspricht einem Anstieg gegenüber 2015 um 13,6 Prozent. Die Anzahl rechtsextremistischer fremdenfeindlicher Gewalttaten nahm um 29,6 Prozent auf 1.190 zu. 1.201 Gewalttaten waren 2016 linksextremistisch orientiert.

Geldfälschung

Die Zahl der sichergestellten gefälschten Geldnoten hat – wie die Bundesbank am 21. Juli mitteilte - im ersten Halbjahr gegenüber der zweiten Jahreshälfte 2016 um fast neun Prozent auf knapp 39.700 zugenommen. Fast zwei Drittel entfielen davon auf gefälschte 50-Euro-Noten. Nachdem die EZB im April einen neuen 50-Euro-Schein mit verbessertem Fälschungsschutz eingeführt hat, hoffe man im zweiten Halbjahr 2017 auf einen deutlichen Rückgang der gefälschten Fünfziger. Mit einem Anteil von 23 Prozent lag der 20-Euro-Schein unter den am meisten gefälschten Noten auf dem zweiten Rang. Die falschen Euro-Scheine hatten einen Nennwert von insgesamt 2,2 Mio. Euro. Um fast 30 habe die Zahl der gefälschten Münzen zugenommen. Mit 82 Prozent sei der größte Anteil auf die 2-Euro-Münze entfallen.

Geldwäsche

Der ASW-Newsletter vom 7. Juni weist auf eine Studie der Universität Halle hin, nach der **Immobilien** in Sachen Geldwäsche ein Hochrisiko-Segment seien. Immobiliengeschäfte würden besonders gern und häufig zur Geldwäsche genutzt. Dies betreffe fast ausschließlich den Bereich der Immobilienvermittlung, also den sogenannten Nicht-Finanzsektor, im Gegensatz zu dem Bereich Immobilienfinanzierung, der dem Finanzsektor zuzurechnen ist. Grund sei die Regulierung des Finanzsektors und die daraus resultierende gute Aufstellung im Bereich

Geldwäsche, die im Nicht-Finanzsektor bei weitem nicht so ausgeprägt sei. Die deutsche Risikoberatung GmbH biete speziell auf den Nicht-Finanzsektor zugeschnittene Schulungen und Informationsseminare an.

IT-Sicherheit

Michael Wiesner, Berater für IT-Sicherheit, befasst sich in der Ausgabe 2-2017 der Fachzeitschrift s+s report, S. 49/41, mit der **VdS-Richtlinie für industrielle Automatisierungssysteme** und mit dem ergänzenden Leitfaden VdS 3437-1, der sich vor allem an Produktionsbetriebe richte. Mit der Richtlinie VdS 3473 „Cybersicherheit für kleine und mittlere Unternehmen (KMU)" habe VdS Schadenverhütung im Juli 2015 einen generischen Ansatz für die Etablierung und Aufrechterhaltung von Informationssicherheit veröffentlicht, der sich seitdem wachsender Beliebtheit erfreue und branchenübergreifend Anwendung finde. Die fortschreitende Digitalisierung der Arbeitswelt und tägliche Schreckensmeldungen über Hacker-Angriffe würden belegen, dass Informationssicherheit längst zu einem wichtigen Aspekt der Unternehmensführung und des Risikomanagements geworden ist. Dies betreffe insbesondere das produzierende Gewerbe, das unter dem Stichwort „Industrie 4.0" mehr denn je auf eine ordnungsgemäß funktionierende IT angewiesen sei. VdS Schadenverhütung trage diesem Umstand mit dem „Leitfaden zur Interpretation und Umsetzung der VdS für industrielle Automatisierungssysteme" Rechnung. Der Autor geht vor allem auf den Aufbau des Leitfadens, auf Verantwortlichkeiten, auf Regelungen für Operatoren und Systemintegratoren sowie auf Automatisierungssysteme und Netzwerke ein.

Die FAZ thematisiert am 8. Juli nochmals den **Computervirus „Petya",** der Ende Juni auch bei deutschen Unternehmen mit seinem Datenverschlüsselungsprogramm Schaden angerichtet habe. Wie das BSI mitteile, ergaben Analysen von IT-Sicherheitsforschern, dass bereits seit April in mehreren Wellen unterschiedliche Schadsoftwarevarianten über die Aktualisierungsfunktion der in der Ukraine weit verbreiteten Buchhaltungssoftware M.E.Doc verteilt wurden. Auch Datensicherungen (Backups), die nach dem 13. April angelegt wurden, müssten als potenziell gefährlich betrachtet werden. Dem BSI lägen Informationen vor, die besagen, dass die von Petya betroffenen Unternehmen erhebliche Anstrengungen unternehmen müssten, um kritische Geschäftsprozesse wieder zum Laufen zu bringen. Das BSI rate Unternehmen jetzt, dass, sollten sie auf die M.E.Doc angewiesen sein, sie die entsprechenden Computersysteme vom Internet abschotten, verstärkt überwachen und auf Schadsoftware untersuchen.

Nach einer Meldung der FAZ vom 10. Juli schätzen 39 Prozent der **KMU** das Risiko eines Hackerangriffs oder Datendiebstahls als hoch ein, wie eine Studie der Gothaer Versicherung unter rund 1.000 deutschen Betrieben mit bis zu 500 Mitarbeitern ergeben habe. Vor zwei Jahren hätten diese Befürchtung erst 30 Prozent der Befragten geäußert. Trotz des steigenden Risikobewusstseins verzichte ein Fünftel der Unternehmen auf Virenschutzprogramme, eine Drittel nehme keine professionelle Datensicherung vor. Eine Versicherung für Cyberrisiken hätten neun Prozent der Unternehmen abgeschlossen. Nach dem globalen Hackerangriff auf Computersysteme Mitte Mai 2017 sei eine deutlich steigende Nachfrage nach Cyberpolicen zu spüren.

Der Behörden Spiegel berichtet in der Juli-Ausgabe über die Ergebnisse einer **Befragung von 556 Führungskräften**, in deren Zuständigkeit die IT-Sicherheit im Unternehmen fällt, durch die Bundesdruckerei GmbH in Zusammenarbeit mit Kantar Emnid. Acht von zehn Entscheidern würden der IT-Sicherheit eine hohe Priorität beimessen.

Dennoch würden nur in weniger als der Hälfte der Unternehmen Mitarbeiter regelmäßig zu Sicherheitsthemen geschult. Und nur jedes zweite Unternehmen habe einen festen Verantwortlichen für Sicherheitsfragen. Ernsthaften Verbesserungsbedarf bei personellen Maßnahmen sehe aber nur etwa ein Drittel der Unternehmen. Allerdings würden über 40 Prozent der Befragten deutlichen Verbesserungsbedarf auf technischer Ebene angeben. Eine Verschlüsselung erfolge nur bei etwa der Hälfte der untersuchten Unternehmen.

Peter Welchering äußert sich in der FAZ am 11. Juli zur **Abhörsicherheit von Quantencomputern**. Nachrichtendienste würden sich von Quantencomputern erhoffen, dass kein Code mehr sicher ist. In aller Welt werde fieberhaft an der Quantenverschlüsselung gearbeitet. Vom Jahr 2022 an sollten Daten abhörsicher über das Quanten-Internet gesendet werden. Bei den bisherigen Quantenkryptographiesystemen, die direkt von einem Absender zu einem Empfänger Daten verschlüsselt übertragen, habe man sich zu wenig darum gekümmert, dass die Verbindung mathematisch beweisbar sicher eingerichtet wurde. Der Sender schicke beim quantenkryptographischen Verfahren Lichtteilchen als Quantenbits über die Leitung, die vier unterschiedliche Polarisationszustände aufweisen. Quantenverschlüsselungssysteme, die seit 2007 kommerziell eingesetzt werden, hätten als sicher gegolten. Doch verschiedenen Forschergruppen sei es gelungen, Schwachstellen bei verschiedenen kommerziellen Quantensicherheitssystemen ausfindig zu machen. Ihre Angriffsstrategie ähnele den Hackerangriffen auf das Online-Banking. Der Spion fange die Quantenbits oder Photonen (Lichtquanten, aus denen ein Lichtstrahl besteht) des Senders einfach ab, manipuliere sie und schicke entsprechende Photonen weiter zum Empfänger. Damit der Empfänger die Abfangaktion nicht bemerkt, blende der Datenspion die Empfängerdetektoren regelrecht. Der Detektor im Empfangsgerät könne bedingt durch die Blendung nur noch als ganz normaler Lichtsensor arbeiten. Das nutze der Datenspion aus. Er fange einzelne Photonen vom Sender ab, rekonstruiere den Quantenschlüssel und schicke die Photonen weiter zum Empfangsgerät. Der Angreifer habe den gleichen Schlüssel wie Sender und Empfänger. Er messe die Quantenzustände, die vom Sender kommen, und könne so den Quantenschlüssel erfahren. Der Datenspion nutze also eine Schwäche der Quantenverschlüsselungsgeräte aus, welche die Hersteller dieser Systeme bei der Umsetzung des quantenkryptographischen Verfahrens übersehen haben. Den Entwicklern des Quanten-Internets reichten deshalb solche Punkt-zu Punkt-Verschlüsselungen nicht mehr. Sie wollten mehrere Quanten-Repeaterstrecken miteinander vernetzen. Bis 2022 solle eine erste Quanten-Repeaterstrecke fertiggestellt sein. Sie wäre quasi der Ausgangspunkt für ein weltumspannendes Quanten-Internet. Mit ihm wäre dann abhörsichere Kommunikation möglich. Die Datenkommunikation zwischen den Quantencomputern wäre nicht nur sicher vor den Lauschaktionen der Spione. Sie könnte auch nicht manipuliert werden. Mit heutigen Angriffsmethoden könnte niemand mehr in solche Computer einbrechen und sie als digitale Waffen missbrauchen.

Im vierten Jahr nach Snowden sei das Netz für den typischen Benutzer etwas sicherer geworden. **Verschlüsseltes Surfen** werde zusehends zur Regel, schreibt die FAZ am 24. Juli. Dieser Schub zu mehr Verschlüsselung sei messbar, so auch bei der Nutzung von https. Anders als beim unverschlüsselten Surfen über http erschwere die Nutzung von https Angreifern, unerwünschte Änderungen bei der Kommunikation zwischen Website und Browser vorzunehmen.

Öffentliche **WLAN-Netze**, die für jedermann sofort nutzbar sind, bieten auch Kriminellen und Hackern neue Möglichkeiten. Darauf weist die FAZ am 25. Juli hin. Ein einfaches Smartphone mit der passenden App reiche als Handwerkszeug für kriminelle Aktivitäten

vollends aus. Datenpakete abfangen, unverschlüsselte Kommunikation extrahieren, Sitzungs-Cookies auslesen, Accounts kapern und Man in the Middle-Angriffe starten: Das seien typische Aktionen, für die man nicht einmal ein Netzwerk-Spezialist sein muss. Wer auf Nummer sicher gehen will, müsse seinen Datenverkehr verschlüsseln und darauf achten, dass auf Smartphone und Notebook in allen Apps und Anwendungen jede einzelne Einstellung stimmt. Die komplette Sitzung müsse von Anfang bis Ende verschlüsselt sein. Dienste mit persönlichem Login, die unvermittelt auf unverschlüsselte Seiten verlinken, sollte man in öffentlichen Netzen nicht aufrufen. Deutlich sicherer als ein Web-Mailer sei es, auf dem Notebook oder Smartphone ein E-Mail-Programm zu verwenden und bereits vorab zu kontrollieren, ob für Posteingang und Postausgangsserver die Verschlüsselung aktiviert ist. Die Einstellungen würden von Fall zu Fall variieren. Gegebenenfalls müsse man eine „sichere Verbindung", SSL oder „Start TLS" nachträglich aktivieren. Wer sichergehen wolle, müsse für öffentliche Netze stets ein VPN verwenden. Das Virtual Private Network schicke den gesamten Datenverkehr in verschlüsselter Form an einen vertrauenswürdigen Server. Unternehmens-Smartphone für Führungskräfte nutzten ebenfalls die VPN-Technik.

Nach einer Meldung der FAZ vom 26. Juli beklagt der Telekommunikationskonzern BT, dass bei **mittelständischen Unternehmen** trotz einer Belegschaft von ein paar tausend Mitarbeitern die IT-Abteilung „nur eine Handvoll Leute" umfasse. Für eine online-24/7-Überwachung brauche man aber mindestens sechs Sicherheitsexperten. Der Technologieverband VDE habe eine erste Plattform geschaffen, um die Lösung von IT-Security-Problemen im Bereich Industrieautomation zu koordinieren.

Die innovative Technologie „**Patient Zero Detection"** von Retarus erzeuge zu jeder E-Mail einen eindeutigen Fingerabdruck, wodurch auch zunächst unbekannte Gefahren noch nachträglich identifiziert werden können (retarus.com vom 6. Juli). Mit dem aktuellen Update ließen sich nun neben Malware auch Phishing-Mails auf diese Weise erfassen. Zusätzlich biete die neue Version optimierte Monitoring- sowie Reporting-Möglichkeiten. Unternehmen erhielten dadurch einen besseren Überblick über Malware-Angriffe und Phishing-Versuche und könnten finanziellen Schaden durch Datenverlust oder Identitätsdiebstahl leichter abwenden. Ab sofort würden auch Hashwerte aller enthaltenen URLs in eine Datenbank aufgenommen. Sobald ein Virenscanner zu einem späteren Zeitpunkt bei einem anderen Empfänger in einem identischen Anhang Schadcode entdeckt oder ein Phishingschutz-Mechanismus eine URL als Phishing-Versuch identifiziert, informiere Retarus unverzüglich alle betroffenen Empfänger sowie deren Administratoren. Unternehmen könnten somit reagieren, noch bevor sich Malware im Unternehmensnetzwerk ausbreiten kann oder sensible Daten in die falschen Hände gelangen.

Überwachung von Arbeitnehmern nicht zulässig, titelt die FAZ am 28. Juli und verweist auf ein Urteil des BAG vom 27. Juli. Es habe die Kontrolle eines Dienstcomputers durch Keylogger – einer Spähsoftware, die Tastatureingaben speichert – verboten. Eine Überwachung halte das BAG nur in Ausnahmen für zulässig. Dann müsse allerdings der Verdacht einer konkreten Straftat durch den Mitarbeiter bestehen oder eine schwerwiegende Pflichtverletzung vorliegen. Ansonsten liege ein starker Eingriff in das Persönlichkeitsrecht des Arbeitnehmers vor.

IuK-Kriminalität

Peter Marwan weist in silicon.de am 7. Juli auf eine Untersuchung von AV-Test zur Verbreitung verschiedener Arten von **Windows-Malware** hin. Danach waren 2016

von insgesamt 600 Mio. bekannten Schadprogrammen lediglich 0,94 Prozent Ransomware. Die umfangreichste Malware-Kategorie seien 2016 mit 37,6 Prozent Viren gewesen. 25,44 Prozent ordnet AV-Test der Kategorie Würmer zu. 23,74 Prozent identifiziert das Testlabor als Trojaner. Skripte (3,42 Prozent), Passwort-Trojaner (2,74 Prozent) und Backdoors (1,00 Prozent) seien nur wenig vertreten, aber immer noch häufiger als die in den vergangenen Monaten in den Mittelpunkt des öffentlichen Interesses geratene Ransomware. Insgesamt sind laut AV-Test im vergangenen Jahr 127,5 Mio. neue Schadprogramme in Umlauf gekommen. Das seien 15 Prozent weniger als 2015. 69,96 Prozent der Malware richte sich gegen das Betriebssystem Windows. 5,65 Prozent ziele auf Android. Das seien bereits rund vier Mio. neue Schadprogramme, rund doppelt so viele wie 2015. Die meisten davon seien auch 2016 schädliche Apps mit Trojaner-Funktion gewesen. Auf Ransomware entfalle auch bei Android mit einem Anteil von 0,22 Prozent nur ein sehr geringer Anteil.

Im Vergleich zum großen Aufsehen, das Erpressungstrojaner in der ersten Hälfte 2017 verursacht haben, seien **DDoS-Attacken** eher in den Hintergrund getreten, berichtet heise.de am 17. Juli. Trotzdem hätten Anfang 2017 wieder weit mehr DDoS-Attacken auf deutsche Ziele stattgefunden als 2016. Sie hätten um zwei Drittel zugenommen. Das stelle der Anti-DDos-Spezialist Link11 in seinem aktuellen DDoS-Bericht fest. Die meisten Attacken fänden an Wochenenden und spät abends statt. Mutmaßlich, um die Techniker der Unternehmen auf dem falschen Fuß zu erwischen und die Ausfallzeit der Webseiten zu maximieren. Organisierte Banden, zu denen anscheinend auch die Stealth Ravens gehörten, würden immer häufiger. Sie erpressten meistens ihre Opfer um Bitcoin und führten immer öfter Probe-Attacken aus, um zu beweisen, dass sie es ernst meinen.

Wirtschaft und Sicherheitsbehörden warnen vor **Milliardenschäden durch Cyberattacken**, titelt die FAZ am 22. Juli. Einmal das gesamte Budget des Freistaates Bayern: So viel sollen Datendiebstahl, Spionage und Sabotage deutsche Unternehmen jährlich kosten. Das sei das Ergebnis einer Studie des Branchenverbandes Bitkom. Dabei komme die Gefahr meist nicht aus den ominösen Weiten des Cyberspace, sondern der eigenen, womöglich frustrierten, Belegschaft. Am teuersten seien nach der Selbsteinschätzung der befragten Unternehmen Ermittlungen und Ersatzmaßnahmen (21 Mrd. Euro) sowie Umsatzeinbußen durch den Verlust von Wettbewerbsvorteilen und Patentverletzungen. Der Imageschaden werde auf 15,4 Mrd. Euro geschätzt, doppelt so viel wie in der Untersuchung vor zwei Jahren. Nur 31 Prozent der Vorfälle würden durch staatliche Stellen untersucht, die meisten Fälle jedoch intern (46 Prozent). Besonders gefährdet seien KMU. Sie seien besonders innovativ, und anders als in Konzernen sei es dort nicht selbstverständlich, neben Virenschutz auch aufwändigere Gegenmaßnahmen zu ergreifen. In 62 Prozent der Fälle seien es aktuelle oder ehemalige Mitarbeiter, die sich in den vergangenen zwei Jahren an Datendiebstahl, Industriespionage und Sabotage beteiligt haben. Dass nur 37 Prozent der Angriffe aus Deutschland kamen, aber jeweils um die 20 Prozent aus Osteuropa, Russland und China, stehe nur scheinbar im Widerspruch zu diesem Befund. Der Präsident des BfV, Hans-Georg Maaßen betonte, er wundere sich, dass die Unternehmen so wenig Geld in Schulung ihrer Mitarbeiter steckten. Es brauche eine Art „human Firewall". Für die vernetzte Gerätewelt mahnte er einen Wechsel der Prioritäten an: von Preis und Komfort zur Sicherheit.

Wegen der Bedrohung durch Software-Piraterie, Hacking, Computerbetrug und -sabotage haben, wie die FAZ am 24. Juli berichtet, Hessen und elf weitere Bundesländer **Schwerpunktstaatsanwaltschaften** und Sonderdezernate zur Verfolgung von

Cyberkriminalität gegründet. Die hessische Zentralstelle bei der Generalstaatsanwaltschaft Frankfurt sei erster Ansprechpartner für das BKA, wenn Täter und Tatort einer über das Internet begangenen Straftat nicht feststehen. Unter Verwendung falscher Identitäten würden selbst Großunternehmen zur Überweisung von Geld manipuliert. Vielerorts versage die interne Absicherung, beginnend von der Buchhaltung bis hoch zur Vorstandsebene. Trotz großer Compliance-Abteilungen blieben Konzerne für Angriffe anfällig und verschlössen sich zugleich den Strafverfolgungsbehörden. Das Darknet werde als Vertriebskanal genutzt, auch von der organisierten Kriminalität. Häufig mieteten die Täter ihre kriminelle Infrastruktur und IP-Adressen mit falschen Personalien in Israel oder Georgien. Allein beim BKA seien 140 Spezialisten mit der Bekämpfung von Cyberkriminalität befasst. Man brauche eine noch engere Kooperation mit der Wirtschaft und den Verbänden. Als Rückschlag für ihre Ermittlungen sähen die Staatsanwälte die Abschaffung der Störerhaftung für öffentlich zugängliche WLAN-Zugänge.

Aus dem **„Trendreport Cyberattacken"** des finnischen Unternehmens F-Secure gehe hervor, dass sich die Gesamtzahl der Cyberattacken in Deutschland von 5,6 Mio. im ersten Quartal 2017 auf 11,3 Mio. im zweiten Quartal erhöht hat, meldet die FAZ am 28. Juli. Mehr als 90 Prozent der Attacken seien in diesem Quartal aus drei Ländern gekommen: Russland (38,6 Prozent), Deutschland (31,3 Prozent) und Amerika (21,6 Prozent). Während sich im ersten Quartal die meisten Attacken aus Deutschland noch gegen Server in Amerika gerichtet hatten, sei im zweiten Quartal Deutschland selbst das Hauptziel deutscher Cyberangriffe gewesen.

Wie silicon.de am 26. Juli meldet, hat der Sicherheitsanbieter Sophos die im Dark Web als Service erhältliche **Ransomware Philadelphia** analysiert. Das „Angebot" der Hacker stehe aus Support und Tools für die Verwaltung von Malware-Kampagnen. Unter anderem sei es möglich, sich den Standort aller bereits infizierten Computer auf einer Karte anzeigen zu lassen. Die Nutzer der Ransomware könnten so sehen, wo sie bereits erfolgreich waren und in Abhängigkeit der Region die Lösegeldforderung einzelner Opfer anpassen.

Opfer von Ransomware haben in den vergangenen zwei Jahren über 25 Mio. Dollar bezahlt, berichtet Peter Marwan am 26. Juli auf silicon.de. Das gehe aus einer Untersuchung hervor, die Forscher von Google, Chainalysis, der Universität San Diego sowie der Universität New York vorgelegt hätten. Sie hätten dazu Zahlungen in der Blockchain nachverfolgt und mit bekannten Mustern abgeglichen. Als Hilfsangebot sei 2016 das Projekt **No More Ransom** ins Leben gerufen worden. Außerdem böten auch IT-Sicherheitsfirmen zahlreiche Entschlüsselungs-Tools für Opfer von Ransomware an. Wohl auch deshalb scheine die Zahlungsbereitschaft Betroffener nachzulassen. Untersuchungen legten nahe, dass allein 2016 durch Ransomware ein Gesamtschaden von rund einer Mrd. Dollar entstanden ist.

Katastrophenschutz

ZÜRS GEP ist das Thema eines Beitrags von Svenja Welter M.A., VdS Schadenverhütung, in der Ausgabe 2-2017 von s+s report, S. 54/55. Die steigenden Schadenzahlen infolge unwetterbedingter Ereignisse schrieben Geo- und Wetterdaten eine immer bedeutendere Rolle zu. VdS GeoExpertise projektiere im Auftrag des GDV das Risikobewertungssystem ZÜRS Geo und biete mit dem Portal eine passgenaue Aufbereitung von Geodaten für die Prozesse der Versicherungswirtschaft. Im ZÜRS würden Daten aus öffentlichen und amtlichen Quellen zu einem Datensatz zusammengefügt, der eine hausnummerngenaue Abschätzung

von Hochwassergefahren sowie die direkte Visualisierung umliegender Gewässer, Überschwemmungsflächen und Schutzgebiete ermögliche. Der vom VdS im Auftrag des GDV betriebene Versicherer-Standard ZÜRS Geo und das Wetterdatenportal Meteo-Info würden zusammen mit allen weiteren Anwendungen der VdS GeoExpertise auf eine gemeinsame, einheitliche und moderne Plattform gehoben. Die neue Plattform mit dem Namen ZÜRS GEP (GeoExpertise Plattform) werde der Versicherungsbranche einen zentralen Zugang zu öffentlichen und privaten Geo-Ressourcen bieten.

Kfz-Kriminalität

Im Jahr 2016 wurden nach dem vom Bundeskriminalamt im Juli 2017 veröffentlichten Bundeslagebild 35.002 **Pkw** als gestohlen registriert. Das sind 2,6 Prozent weniger als 2015. Als auf Dauer entwendet wurden 19.194 Pkw registriert. Das ist ein Prozent weniger als im Jahr zuvor und 0,9 Prozent weniger als im Durchschnitt der vergangenen fünf Jahre. Rund ein Drittel der Tatverdächtigen hatten nicht die deutsche Staatsangehörigkeit. Bei ca. 73 Prozent der auf Dauer entwendeten Pkw handelt es sich um Fahrzeuge deutscher Hersteller. Am stärksten belastet waren die Marken bestimmter hochwertiger Fahrzeuge. Abermals wurden in Berlin mehr Pkw dauerhaft entwendet als in Nordrhein-Westfalen, dem Bundesland mit dem höchsten Zulassungsbestand. Die Belastungszahl (bezogen auf je 100.000 zugelassene Pkw im jeweiligen Land) betrug 2016 im gesamten Bundesgebiet 42, in Berlin 406, in Baden-Württemberg 11. In den östlichen Bundesländern ist wegen der im Osten Europas gelegenen Absatzmärkte eine erhöhte Belastung festzustellen. Im Jahr 2016 wurden 3.452 Sachfahndungstreffer zu deutschen Kfz-Ausschreibungen in anderen Schengenstaaten erzielt, davon fast die Hälfte (1.624) in Polen. Die Treffer lassen die Hauptverschieberoute über Polen in Richtung Osten sowie eine schwächer ausgeprägte Route über die Niederlande und Frankreich in Richtung Afrika erkennen. Gesunken ist 2016 die Zahl der auf Dauer entwendeten **Lkw** (um 4,4 Prozent auf 1.527). Die Entschädigungssumme für entwendete Lkw lag 2015 nach Angaben des GDV mit 40 Mio. Euro fast 18 Prozent über dem Betrag von 2014. Zugenommen haben Diebstähle von Spezial-Lkw, insbesondere von Betonmischern und -pumpen. Sie werden nach der Entwendung mit einer neuen Fahrzeugidentifizierungsnummer versehen und ins Ausland verbracht. Dabei treten insbesondere polnische und litauische Tätergruppen in Erscheinung. Die **internationale Kfz-Verschiebung** wird von hoch qualifizierten, spezialisierten und arbeitsteilig vorgehenden Tätergruppierungen dominiert, zumeist aus Polen. Die Überwindung von elektronischen Sicherungseinrichtungen, der Fahrzeugtransport, die Zerlegung der Fahrzeuge in Einzelteile, die Fälschung oder Verfälschung von Fahrzeugpapieren und Identifizierungsmerkmalen sowie der Absatz entwendeten Fahrzeuge erfordern offensichtlich eine umfassende Logistik und verdeutlichen die hohe Professionalität der Täter. Beispielhaft für das Eindringen in moderne Fahrzeuge ist der immer häufiger festgestellte Modus Operandi der sogenannten „Funkstreckenverlängerung". Dabei benutzen die Straftäter für den Diebstahl von Fahrzeugen, die mit einem „Keyless Entry"-System ausgestattet sind, elektronische Tools, die das unmittelbare Vorhandensein des Fahrzeugschlüssels simulieren. Ein wichtiger Transportweg für den Absatz im Nahen und Mittleren Osten sowie in Zentralasien führt durch die Türkei. Alternativ werden Lkw auch über die Häfen in Antwerpen, Rotterdam, Marseille und Triest verschifft.

Krisenregionen

Nach einem Hintergrundbericht von smartrisksolutions.de im Newsletter des ASW vom 14. Juli hat sich im Osten der Demokratischen **Republik Kongo** die ohnehin nicht gute Sicherheitslage seit Anfang Juli weiter verschlechtert. Rebellengruppen nutzten den mangelnden Einfluss der Zentralregierung. Der Rebellenführer lokaler Mai-Mai-Gruppen suche immer mehr die offene Konfrontation mit der kongolesischen Armee und habe erhebliche Erfolge vorzuweisen. Die Rebellen finanzierten sich zum einen aus dem Goldhandel, zum anderen zunehmend aus Entführungen von Ausländern. Unternehmen sollten daher bei Aktivitäten vor Ort ihre bestehenden lokalen Sicherheits- und Notfallpläne kritisch überprüfen. Firmen, die bewaffneten Schutz benötigen, müssten auf das kongolesische Militär zurückgreifen, da Sicherheitsfirmen keine bewaffneten Dienstleistungen ausführen dürfen. Empfohlen würden: eine detaillierte Risikoanalyse, „robuste" Evakuierungspläne, Rahmenverträge mit Dienstleistern, um kurzfristig Zugriff auf deren Flugzeuge und Hubschrauber zu haben, detaillierte Notfallpläne mit unterschiedlichen Szenarien, ein „High-Risk-Training" und ein gutes Netzwerk vor Ort, auch als Frühwarnsystem.

Nach Informationen der Wochenzeitung DIE ZEIT hat die türkische Regierung dem BKA eine Liste mit angeblichen Terrorunterstützern übergeben. Die Liste enthalte die Namen von zahlreichen Unternehmen wie Daimler und BASF, aber auch einen „Spätkauf"-Imbiss sowie eine Dönerbude sowie Einzelpersonen. Insgesamt enthalte die Liste 681 Einträge. In Berliner Regierungskreisen werde die Liste als „absurd und lächerlich" bezeichnet. Eine unmittelbare Gefährdung von in Deutschland ansässigen Unternehmen ergibt sich nach der Bewertung des BKA nicht. Konkrete gefährdungsrelevante Erkenntnisse in Bezug auf entsprechende Niederlassungen in der Türkei lägen derzeit ebenfalls nicht vor. (FAZ vom 20. Juli).

Das Auswärtige Amt hat am 20. Juli die **Reise- und Sicherheitshinweise für die Türkei** aktualisiert. Personen, die aus privaten oder geschäftlichen Gründen in die Türkei reisen, wird zu erhöhter Vorsicht geraten und empfohlen, sich auch bei kurzzeitigen Aufenthalten in die Listen für Deutsche im Ausland bei Konsulaten und der Botschaft einzutragen. In diesem Zusammenhang wird darauf hingewiesen, dass ungeachtet des gesetzlichen Anspruchs deutscher Staatsangehöriger auf konsularischen Rat und Beistand konsularischer Schutz gegenüber hoheitlichen Maßnahmen der türkischen Regierung und ihrer Behörden nicht in jedem Fall gewährt werden kann, wenn der oder die Betroffene auch die türkische Staatsangehörigkeit besitzt. Die Sicherheitsvorkehrungen in der Türkei befänden sich landesweit auf hohem Niveau. Angesichts von Anschlägen terroristischer Gruppierungen auch gegen nicht-militärische Ziele müsse aber in allen Teilen der Türkei grundsätzlich von einer terroristischen Gefährdung ausgegangen werden. Deutschen, die sich längerfristig bzw. dauerhaft im Land aufhalten, wird empfohlen, sich in die Krisenvorsorgeliste einzutragen und die dort hinterlegten Kontaktdaten auf dem aktuellen Stand zu halten. Von Reisen in das Grenzgebiet der Türkei zu Syrien und Irak, insbesondere in die Städte Diyarbakir, Cizre, Silopi, Idil, Yüksekova und Nusaybin sowie generell in die Provinzen Mardin, Sirnak und Hakkari wird dringend abgeraten. In den Provinzen Hatay, Kilis, Gariantep, Sanharfa, Diyarbakir, Mardin, Batman, Birlis, Bingöl, Siirt, Mus, Tunceli, Sunak, Hakkari und Van bestehe ein erhöhtes Risiko für Reisende. Alle nicht zwingend erforderlichen Reisen in diese Gebiete sollten vermieden werden. Die Türkei zeichne sich bislang als ein Land mit vergleichsweise gering ausgeprägter Gewaltkriminalität aus. Bei Zahlung mit Bank- oder Kreditkarten sei Vorsicht vor Betrügern geboten, die versuchen, unbemerkt die Bankkarte des Reisenden zu kopieren und den zugehörigen PIN-Code auszuspähen.

Öffentliche Sicherheit

„**Staatliches Hacking“** thematisiert der Behörden Spiegel in der Juliausgabe. Kurz vor Ende der Legislaturperiode habe der Staat Rechtsgrundlagen für die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) und die Online-Durchsuchung geschaffen. In beiden Fällen erfolge das Abschöpfen von Daten direkt im Endgerät der Zielpersonen und nicht beim Dienstleister (Provider). Die Geräte müssten daher heimlich technisch infiltriert werden. Der umfängliche Zugriff auf Endgeräte durch Hacking sei nur erlaubt, wenn überragend wichtige Rechtsgüter konkret in Gefahr sind. Im Einklang damit könne das BKA bereits Staatstrojaner zur Bekämpfung des internationalen Terrorismus einsetzen. Die aktuellen Neuregelungen sähen das staatliche Hacking jedoch auch für die Strafverfolgung vor. Mit der Quellen-TKÜ verfolge man die Strategie, Daten schon vor der Verschlüsselung oder nach der Entschlüsselung auf den Endgeräten abzuschöpfen. Für die Online-Durchsuchung sei erstmals eine Rechtsgrundlage geschaffen worden, weil sie Zugriff auf sämtliche Daten auf einem Endgerät erlaubt. Die Maßnahme solle daher auch nur in Fällen besonderer Schwere und nur dann angewendet werden, wenn andere Ermittlungsmaßnahmen versagen. Die Rechtsgrundlage zur Online-Untersuchung orientiere sich an den bestehenden und verfassungsrechtlich geprüften Regeln zur akustischen Wohnraumüberwachung.

Produktfälschung

Martin Schindler berichtet am 3. Juli auf silicon.de, dem EU-Amt für Betrugsbekämpfung (OLAF) sei ein großer Schlag gegen **Fälscher von wichtigen elektronischen Bauteilen** gelungen. In der europaweiten Aktion „Operation Wafers“ seien nur mehr als eine Mio. gefälschter Halbleiter sichergestellt. Diese Fälschungen könnten nicht nur finanziellen oder materiellen Schaden, etwa an Computern, verursachen, sondern auch das Leben und die Gesundheit von Menschen gefährden. Die Bauteile sollten in verschiedenen Produkten verbaut werden. Auf diese Weise hätten die fraglichen gefälschten Bauteile zu schwerwiegenden Fehlfunktionen in zivilen und militärischen Infrastrukturen führen können. Einige dieser Bauteile wie Dioden, Schaltkreise oder LEDs seien für Fahrzeuge oder Flugzeuge bestimmt gewesen, andere hätten in medizinischen Geräten verbaut werden sollen. Die beschlagnahmten Geräte und Teile sollen über Kurierdienste oder über den Postweg in die EU geschmuggelt worden sein.

Sicherheitsmarkt

Nach einem Bericht von Sicherheit.info am 25. Juli sind die Umsätze für elektronische Sicherheitstechnik laut BHE 2016 um 6,2 Prozent gestiegen. Einbruchmeldetechnik und Videoüberwachung verzeichneten Zuwächse von jeweils acht Prozent. 2016 seien von der KfW mehr als 40.000 Zuschussanträge für Einbruchschutzmaßnahmen gewährt und dadurch rund 50.000 Wohneinheiten mit Sicherheitstechnik ausgestattet worden. Die Brandmeldetechnik habe 2016 ihren Gesamtumsatz auf 1,8 Mrd. Euro steigern können (Anstieg von 6,8 Prozent gegenüber 2015). Die Umsätze für Sprachalarmsysteme seien 2016 um 5,3 Prozent gestiegen, für Zutrittssteuerungssysteme um 4,8 Prozent.

Social Engineering

In einem Leitfaden befasst sich der Bundesverband ASW mit dem Social Engineering, dem gezielten Ausnutzen menschlicher Schwächen oder Verhaltensmuster wie zum Beispiel beim **„CEO-Fraud**“. Bei den ersten

Kontaktaufnahmen gehe es ausschließlich um den Aufbau von Vertrauen. Bei späteren Kontaktaufnahmen versuche der Social Engineer, an die geheimen Informationen zu kommen. Er tarne sich zum Beispiel als: Geschäftsführer, der zu einer geheimen Finanztransaktion autorisiere; als IT Support, der wegen einer Systemumstellung Usernamen und Passwort benötige; als Mitarbeiter eines Service-Unternehmens, das Details brauche, um die Kundenzufriedenheit zu testen, als Job-Bewerber, der sich seinen zukünftigen Aufgabenbereich erklären lassen soll. Zu den Verhaltensempfehlungen, die der ASW gibt, gehören: Seien Sie niemals arglos oder gutgläubig! Lassen Sie sich nicht einwickeln, denn Hilfsbereitschaft wird gerne ausgenutzt und hinter Schmeicheleien steckt mehr!

Spionage

Der am 4. Juli veröffentlichte **Verfassungsschutzbericht des Bundes für 2016** weist darauf hin, dass sich der Modus Operandi ausländischer Nachrichtendienste verändert habe. Cyberangriffe haben sich zu einer wichtigen Methode der Ausspähung entwickelt, wodurch die Intensität der Spionageaktivitäten um ein Vielfaches gestiegen sei. **Russland und China** wurden mehrfach als Angreifer erkannt, wenngleich auch Nachrichtendienste anderer Staaten über die erforderlichen Ressourcen und Fähigkeiten zur Durchführung von Cyberangriffen verfügen. So lassen sich Cyberangriffe inzwischen auch mutmaßlich staatlichen Stellen im Iran zuordnen. Betroffen seien weltweit Regierungsstellen und Ziele in Wirtschaft und Forschung, insbesondere in den Bereichen Energietechnik, Röntgen- und Nukleartechnologie, Messtechnologie sowie Luft- und Raumfahrt. Seit dem Machtantritt Xi Jinpings habe im autoritären und repressiven politischen Systems Chinas die Bedeutung der Nachrichtendienste stetig zugenommen. Sie seien in das langfristig angelegte Programm zur Modernisierung der chinesischen Wirtschaft eingebunden. Das verlangsamte Wirtschaftswachstum und die Forderung der chinesischen Staatsführung, die Wettbewerbsposition chinesischer Betriebe auch mittels Übernahmen ausländischer Unternehmen zu verbessern, habe vermehrt zum Aufkauf deutscher mittelständischer Unternehmen aus dem Spitzentechnologiesektor geführt. Nach wie vor sei die Einbindung politischer oder wissenschaftlicher Think Tanks in nachrichtendienstliche Strategien von Bedeutung. Sie dienten auch dazu, sensible Informationen zu sammeln, nicht zuletzt auch zur Vorbereitung von Cybercrimeangriffen, sowie geeignete Zielpersonen auszuwählen und nachrichtendienstliche Aktivitäten zu tarnen. Während in der Vergangenheit fast ausschließlich chinesischstämmige Personen als Agenten rekrutiert worden waren, versuchten die Dienste mittlerweile verstärkt, Personen aus westlichen Ländern als Informanten oder Agenten zu werben. Hinzu kommen Anbahnungsversuche in sozialen Netzwerken im großen Stil. Zu den Staaten, die in Deutschland Beschaffungsaktivitäten für sensitive Güter entwickeln, zählen laut Verfassungsschutzbericht auch die beiden Atommächte Nordkorea und Pakistan sowie Syrien.

Steuerhinterziehung

Das BMF habe die Behörden angewiesen, deutlich mehr Steuergestaltungen, die unter dem Namen „**Cum-Cum"** bekannt sind, als missbräuchlich einzustufen, berichtet die FAZ am 20. Juli. Sowohl „Cum-Ex"- als auch „Cum-Cum"-Geschäfte seien Varianten des Dividendenstrippings. „Cum-Ex"-Geschäfte würden als eindeutig rechtswidrig gelten. Bei ihnen werden Aktien rund um den Dividendenstichtag gehandelt, aber die Investoren haben eine nur einmal bezahlte Kapitalertragssteuer mehrfach abkassiert. Dagegen zählten die „Cum-Cum"-Transaktionen zum Graubereich. Es gebe auch Gestaltungen,

die als legal galten. Die potenziellen Steuerausfälle, die dem Fiskus durch „Cum-Cum"-Geschäfte in den Jahren 2001 bis 2016 entstanden sind, bewegten sich laut Professor Christoph Spengel zwischen 49,2 Mrd. und 82 Mrd. Euro.

Terrorismus

Handelsblatt.com weist am 12. Juli auf eine **Umfrage des Instituts YouGov Deutschland** hin, nach der sich jeder Zweite in Deutschland nach den Terroranschlägen der vergangenen zwei Jahre unsicherer fühlt als zuvor. 84 Prozent sähen eine hohe Wahrscheinlichkeit, dass islamistische Extremisten in den nächsten zwölf Monaten in Deutschland ein Attentat verüben. Jeder Zweite rechne mit rechtsextremistischen Anschlägen. 43 Prozent hielten Gewalttaten durch Linksextremisten für möglich. Analog zu dieser Gefahreneinschätzung wünschten die Menschen vor allem mehr Maßnahmen gegen islamistische Gewalt. 70 Prozent seien der Meinung, die Bundesregierung tue nicht genug gegen den islamistischen Terror. 57 Prozent fänden, es werde nicht ausreichend gegen Gewalt von rechten Extremisten vorgegangen. 51 Prozent sähen die Maßnahmen gegen Gewalt von Links als unzureichend an. 85 Prozent befürworteten die verschärften Vorkehrungen bei Veranstaltungen. Bei möglicher Mehrfachnennung hätten 38 Prozent angegeben, dass sie die Terrorgefahr mehr bei ihrer Urlaubsplanung berücksichtigen, als noch vor zwei Jahren. 29 Prozent verzichteten auf Veranstaltungen mit vielen Menschen oder auf öffentlichen Plätzen, und 13 Prozent griffen zu Dingen wie Abwehrspray, wenn sie das Haus verlassen.

Das Arbeitspapier Sicherheitspolitik Nr.19/2017 der Bundesakademie für Sicherheitspolitik befasst sich mit **Al-Qaida** (AQ), das seit 2010 kaum noch Anschläge gegen den Westen verübt habe. Im Schatten des IS sei es AQ allerdings gelungen, ein Netzwerk zwischen Subsahara-Afrika und Indien zu erreichten, das trotz des anhaltenden Antiterror-Kampfes westlicher Staaten die Machtfülle der Organisation von 2001 weit übertreffe. AQ bestehe heute aus folgenden Gruppen: Kern-AQ, AQAP (Al-Qaida auf der Arabischen Halbinsel mit 3.500 – 4.000 Kämpfern), HAT.S (Hay'at Tahrir al-Sham – Komitee zur Befreiung Syriens), Al-Shabaab, AQIM (Al-Qaida im Islamischen Maghreb) und AQIS (Al-Qaida auf dem Indischen Subkontinent). Die ursprüngliche AQ habe in den letzten 15 Jahren eine erhebliche Transformation durchlaufen: in Ausdehnung und Wachstum, bezüglich Anhängern, Ausbildung und Bewaffnung sowie regionaler Vernetzung. Die Antwort auf die Frage, warum Anschläge ausbleiben, dürfte in der Regionalisierungsstrategie liegen, die AQ nach 2011 eingeschlagen habe. Es müsse von einer strategischen Janusköpfigkeit gesprochen werden, die sowohl durch die Kern-AQ als auch von den jeweiligen Untergruppen mit Blick auf die regionalen Gegebenheiten umgesetzt werde. So sei AQ vor allem im Jemen und in Syrien tief verwurzelt, habe Bündnisse mit lokalen Kräften geschlossen und sich durch Bereitstellung elementarer sozioökonomischer Leistungen teils auch Anerkennung in den örtlichen Bevölkerungen erworben. Eine wirksame Bekämpfung könne nur in der realistischen Abwägung der Ziele und Möglichkeiten von AQ geschehen.

Videoüberwachung

Der Behörden Spiegel berichtet in der Juli-Ausgabe über eine „Nutzergemeinschaft" von Polizei, Nahverkehrsbetreiber und Fußball-Club in **Ingolstadt**, um gemeinsam von einem Videoüberwachungssystem mit der Panomera-Technologie. Die Übertragung der Aufnahmen und Daten erfolge über das Metro-Net der COM-IN Telekommunikations GmbH, Die Verkehrsgesellschaft erhalte

aus Datenschutzgründen lediglich Zugriff auf Übersichtsbilder mit geringer Auflösung von den für den öffentlichen Nahverkehr relevanten Standorten. In ähnlicher Weise zweckgebunden seien die Nutzungsrechte der Stadion-Security beschränkt worden. Die unterschiedlichen Nutzerrechte hätten indes keine Auswirkung auf die Effektivität des Gesamtsystems. Die drei Beteiligten tauschten sich regelmäßig über ihre Erfahrungen aus.

Ein Fehler in **gSOAP** (generic XML Simple Object Access Protocol) erlaube es Angreifern, sich Zugriff von außerhalb auf vernetzte Geräte zu verschaffen, die diese Bibliothek nutzen, berichtet golem.de am 17. Juli. Entdeckt worden sei der Fehler in Sicherheitskameras des Herstellers Axis. Die Lücke und eine weitere Schwachstelle in dem verwendeten Betriebssystem erlaubten die komplette Übernahme der Kamera M3004. Axis habe bereits mit einem Update reagiert. Allerdings werde gSOAP wohl auch in Geräten anderer Hersteller verwendet. Deshalb gingen die Entdecker davon aus, dass mehrere Tausend, wenn nicht Milionen Geräte davon betroffen sind.

Wirtschaftskriminalität

Das Bundeskriminalamt hat im Juli 2017 das Bundeslagebild **Wirtschaftskriminalität (Wikri) für das Jahr 2016** veröffentlicht. Im Jahr 2016 wurden in der PKS insgesamt 57.546 Fälle der Wikri registriert, 5,6 Prozent weniger als im Vorjahr und weniger als im Durchschnitt der letzten fünf Jahre (67.015). Wegen gering ausgeprägten Anzeigeverhaltens ist von einem großen Dunkelfeld auszugehen. Der Anteil der Wikri an allen polizeilich bekannt gewordenen Straftaten betrug im Berichtsjahr 0,9 Prozent, aber die durch Wikri verursachten Schäden (2.970 Mio. Euro) erreichten 43,1 Prozent des durch die Gesamtkriminalität verursachten erfassbaren Schadens von fast sieben Mrd. Euro. Dabei ist unstrittig, dass gerade die nicht erfassbaren und quantifizierbaren immateriellen Schäden, die durch Wikri verursacht werden, wesentliche Faktoren für die Bewertung des Schadenspotenzials sind.

Die Aufklärungsquote betrug im vergangenen Jahr 94,0 Prozent (Gesamtkriminalität 56,2 Prozent). Ursächlich hierfür ist vor allem, dass Geschädigte den Täter häufig kennen. In 17,1 Prozent der Fälle von Wikri wurde 2016 das Internet genutzt. Die Nutzung dieses Tatmittels ist damit gegenüber 2015 deutlich angestiegen (um 74 Prozent), hat sich jedoch gegenüber 2012 nahezu halbiert. Der Hauptanteil der Straftaten mit Internetnutzung lag wie bereits in den Vorjahren mit 8.425 Fällen im Bereich der Wikri bei Betrugstaten.

Einzelne Deliktsbereiche	**Fallzahl 2016**	**Veränderung zum Vorjahr**
Wikri bei Betrug	29.160	- 8,3 %
Insolvenzdelikte	11.283	+ 1,2 %
Arbeitsdelikte	7.699	- 13,5 %
Anlagen- und Finanzierungsdelikte	8.566	- 6,2 %
Betrug/Untreue iVm Kapitalanlagen	7.815	- 2,6 %
Abrechnungsbetrug im Gesundheitswesen	2.465	- 49,7 %
Wettbewerbsdelikte	1.737	- 3,0 %

Eine ausführlichere Zusammenfassung des Bundeslagebildes ist auf der Website von Securitas (Presse/Sicherheitslage) zu lesen.

Wirtschaftsschutz

In dem am 4. Juli veröffentlichten **Verfassungsschutzbericht** des Bundes wird zum Ausdruck gebracht, dass der Schutz der Unternehmen vor Wirtschaftsspionage, Sabotage und anderen Bedrohungsformen eine gemeinsame Aufgabe von Staat und Wirtschaft ist. Mit der 2016 gestarteten „Initiative Wirtschaftsschutz" habe sich das BfV mit weiteren Sicherheitsbehörden und der Wirtschaft unter der Koordinierung des BMI eine Zusammenarbeitsform gegeben. Das Know-how der Initiative stehe gebündelt und kostenfrei für jedermann auf der Internetplattform www.wirtschaftsschutz.info zur Verfügung. Auch das neue „Handbuch Wirtschaftsgrundschutz", das der ASW, das BSI und das BfV herausgeben, stehe auf dieser Internetplattform zur Verfügung. Die ersten Module wurden am 10. November 2016 der Öffentlichkeit vorgestellt. Sie bilden einen handlungsorientierten Leitfaden für mehr Sicherheit in den Unternehmen. Die Inhalte entsprechen vorrangig den Erfordernissen kleiner und mittelständischer Unternehmen.

Die Komplexität der Thematik „Wirtschaftsschutz" erfordert die **Schaffung klarer Zuständigkeiten und zentraler Ansprechpartner** – auf Seiten der Wirtschaft und bei den Sicherheitsbehörden, heißt es in einem Positionspapier des Bundesverbandes ASW. Man brauche daher Wirtschaftsschutzbeauftragte mit klarem Auftragsprofil in den Unternehmen und im öffentlichen Sektor. Sie hätten im Unternehmen die Aufgabe, die gesetzlichen Anforderungen an den Wirtschaftsschutz zu überwachen. Sie seien nicht nur für die Kontrolle des Sicherheitsniveaus im Unternehmen, sondern auch für die Planung und Umsetzung des Sicherheitsmanagements verantwortlich. Das Aufgabenspektrum umfasse: die Verantwortlichkeit für alle Sicherheitsbelange der gesamten Organisation, die Entwicklung einer unternehmensweiten Sicherheitsstrategie, die kontinuierliche Analyse der globalen Sicherheitstrends und anstehenden Risiken, die Entwicklung geeigneter Präventionsstrategien, die Implementierung von Sicherheitsrichtlinien und -anforderungen, die Überführung von externem Sicherheits-Know-how in das Unternehmen, die Integration des Sicherheitsmanagements in den anderen Unternehmenseinheiten und die Überprüfung der Wirksamkeit der Sicherheitsmaßnahmen.

Der Bundesverband ASW weist im Newsletter vom 28. Juli auf folgende seiner Veröffentlichungen hin:

Leitfäden

1. Leitfäden für Ausbildung und Praxis von Sicherheitsfachkräften (Unternehmenssicherheit, Rechtskunde, Dienstkunde, Schutz- und Sicherheitstechnik, sicherheits- und serviceorientiertes Verhalten und Handeln, Personenschutz, Arbeitssicherheit, Hundeeinsatz, Waffenrecht & Waffenkunde
2. Leitfäden zur Vorbereitung auf die Sachkundeprüfung nach § 34a GewO (Grundlagen der Sicherheitstechnik, rechtliche Grundlagen, Umgang mit Menschen)
3. Leitfäden Antifraud-Management (Durchführung von internen Ermittlungen)
4. Leitfaden für Aus- und Weiterbildung (Sensibilisierungs- und E-Learning-Programm zur Security Awareness
5. Leitfaden zur Cyber-Security
6. Leitfäden zur Lage- und Reisesicherheit (Checkliste zur Sicherheit auf Geschäftsreisen, Aufbau und Struktur eines Reise-Risikomanagements)
7. Leitfaden zum Bedrohungsmanagement

Leitblätter

1. Antifraud-Management (Social Engineering, Identitätsmissbrauch, CEO-Fraud)
2. Lage- und Reisesicherung (Informationsschutz auf Reisen, Verhalten bei Angriffen und Anschlägen)
3. Wirtschaftsschutz und Spionageabwehr (islamistische Radikalisierung von Mitarbeitern)

Handbuch zum Wirtschaftsschutz mit folgendem Inhalt:

- Einführung, Glossar, Standard 2000-1 (Wirtschaftsgrundschutz), Standard 2000-2 (Aufbau und Betrieb eines Sicherheitsmanagementsystems), Standard 2000-3 (Aufbau und Betrieb eines Notfall- und Krisenmanagementsystems)
- Übergreifende Aspekte (ÜA1 – Schulung und Sensibilisierung, ÜA2 -cherheitsvorfallmanagement, ÜA3 – Notfallmanagement, ÜA4 – Krisenmanagement, ÜA5 – Umgang mit Wirtschaftskriminalität, MA1 – Reisesicherheit, MA2 – Bewerberprüfung)
- Infrastruktur (IS1 – Objektsicherheit, IS3 – Kontinuität der Gebäudedienste)
- Externe Parteien (ES1 – Integrationsprüfung externer Parteien, ES2 – Auswahl und Steuerung von Sicherheitsdienstleistungen)

Zutrittskontrolle

Nach einem Bericht von Sicherheit.info vom 27. Juli präsentieren Axis Communications und SimonsVoss ein vollständig integriertes, IP-basiertes, digitales Schließ- und Zutrittskontrollsystem. Die Online-Integration zwischen dem Axis A1001 Tür-Controller und den drahtlosen Schließkomponenten des Systems SmartIntego über den Axis Entry Manager geschehe nahtlos, da alle Produkte auf einer offenen, IP-basierten Architektur aufgebaut seien. Die integrierte Lösung erlaube die Steuerung drahtloser und verdrahteter Türen mit in Echtzeit überwachtem Zutritt und detaillierten Prüfpfaden. Die ferngesteuerten SmartIntego-Schließsysteme seien mit RFID-Lesern ausgestattet. Axis A1001 benötige kein Stromkabel, da es sich um ein Power over Ethernet-System handele.

Impressum

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

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

Herausgeber:
Manfred Buhl, Vorsitzender der Geschäftsführung, Düsseldorf

Verantwortlicher Redakteur:
Bernd Weiler, Leiter Kommunikation und Marketing

Beratender Redakteur:
Reinhard Rupprecht, Bonn

focus.securitas.de

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

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

E-Mail: info@securitas.de