Focus on Security

Ausgabe 02, Februar 2016

SECURITAS

Inhalt

Anschläge

Das BKA berichtet in der Wochenlage vom 4. Januar, dass in der Nacht zum 11. Dezember unbekannte Täter in Frankfurt am Main die Reifen von sieben Kfz der **ABG Frankfurt-Holding** zerstachen und von vier dieser Fahrzeuge die schraubbaren Dachantennen entwendeten. Die Fahrzeuge seien auf dem frei zugänglichen und nicht videoüberwachten Firmengelände abgestellt und als Firmenfahrzeuge gekennzeichnet gewesen. Bei der geschädigten Firma handele es sich um die größte Wohnungsbaugesellschaft in Frankfurt. Im Themenzusammenhang Sozialpolitik/ Umstrukturierung sei dieses Unternehmen bereits in der Vergangenheit in das Zielspektrum der linken Szene geraten.

In der Wochenlage am 8. Januar berichtet das BKA über eine Brandstiftung an einem Fahrzeug der Firma **Thyssen-Krupp** in Berlin-Friedrichshain in der Nacht zum 30. Dezember. Unbekannte Verfasser hätten unter der Bezeichnung „informelle pyromanische Verschwörung" ein Selbstbezichtigungsschreiben auf der linksgerichteten Internetseite www.linksunten.indymedia.org eingestellt. Sie stellen die Tat in mehrere Begründungszusammenhänge, u. a. „Antirepression", „Antimilitarismus", „Gentrifizierung" und „Antikapitalismus".

Betrug

Der ASW geht in seinem Newsletter vom 8. Januar auf **Fake-Shops** ein. Das seien gefälschte Internet-Verkaufsplattformen, die auf den ersten Blick schwer zu erkennen seien. Sie seien teilweise Kopien real existierender Websites, wirken daher seriös und ließen beim Käufer selten Zweifel an ihrer Echtheit aufkommen. Das sei das Ziel der Betrüger: Mit aus dem Internet kopierten Produktbildern und Informationen, professionell aufgemachten AGBs und einem gefälschten Impressum wollten sie das Vertrauen der Online-Shopper gewinnen und sie so zum Kauf animieren. Ein weiteres Lockmittel sei der scheinbar besonders günstige Preis des gesuchten Produkts.

Siilicon.de befasst sich am 4. Januar mit der neuen Taktik **Business E-Mail Comprise**, vor der das FBI seit August 2015 warne. Der Betrüger fälsche eine Mailadresse und gebe sich damit als Chef oder Mitarbeiter des Unternehmens aus. Man spreche dabei auch von dem Fake President Fraud. Dabei bekämen Mitarbeiter vermeintlich vertrauliche Anweisungen, Geld zu überweisen, um heikle Geschäftsvorgänge oder Übernahmen abwickeln zu können. Die Schäden für Unternehmen könnten Millionenbeträge erreichen.

Brandschutz

Der Behörden Spiegel berichtet in der Januar-Ausgabe über das **Technische Sicherheitszentrum des Kompetenzzentrums Kritische Infrastrukturen** in Berlin-Mahlsdorf. Hier könnten Einsatzkräfte in speziellen Feuerwehr-Schulungen die Brandbekämpfung an einer Niederdruckleitung, einer Mitteldruckleitung und einer Hochdruckleitung üben. Des Weiteren könnten in der Einrichtung eine unterirdische Rohrbeschädigung, der Brand einer Gasleuchte sowie eine Gasverpuffung simuliert werden. In ganz Deutschland existierten nur zehn derartige Trainingszentren. Das Sicherheitszentrum verfüge auch über eine Baggerschadensdemonstrationsanlage und biete Schulungen für Erstsicherer im Bereitschaftsdienst, Brandschutzhelfer sowie zum sachgerechten Umgang mit Feuerlöschern an. Das Regelwerk des Deutschen Vereins des Gas- und Wasserfaches (DVGW) schreibe allen Gasnetzbetreibern vor, dass binnen 30 Minuten nach Eingang der Meldung ein Mitarbeiter an der Störungsstelle sein muss.

Cloud-Computing

Der Sicherheitsberater weist in Ausgabe 1-2016, S. 14-16 darauf hin, dass das BSI zum Cloud-Einsatz einen sehr intelligenten und passenden Ansatz entwickelt habe. In Zusammenarbeit mit PwC sei der „Anforderungskatalog Cloud Computing" vorgestellt worden. Aus IT-Sicherheits- und aus Wirtschaftsprüfungsstandards seien Kriterien extrahiert worden, die relevant für die gesuchte Beurteilung der IT-Sicherheit von Cloud-Diensten sind.

Datenschutz

Die Wochenzeitung Das Parlament befasst sich am 4. Januar mit der **Datenschutzgrundverordnung**, die im ersten Halbjahr 2018 in Kraft treten soll und europäische Vorschriften aus dem Jahr 1995 ersetzt. Damit sollen die bisherigen 28 nationalen Vorschriften abgelöst werden. In Deutschland werde das BDSG genauso obsolet wie unzählige Paragrafen, die sich in Datenschutznormen der Bundesländer befinden, aber auch im Arzneimittelgesetz und dem Telekommunikationsgesetz. Nach Schätzungen der EU-Kommission würden die Unternehmen künftig im Jahr 2,3 Mrd. Euro einsparen. Einheitliche Regeln bedeuteten aber auch, dass sich die Firmen nicht mehr den Standort mit den schwächsten Datenschutzregeln heraussuchen könnten. Gleichzeitig könnten Verbraucher sich im Heimatland beschweren, sollten sie Verstöße gegen den Datenschutz feststellen.

Internetunternehmen wie Google, Facebook und Amazon müssten künftig eine Zustimmung bei den Nutzern einholen, wenn sie deren Daten nutzen wollen. Sie könnten die Daten dann auch nur zu dem Zweck einsetzen, den sie angegeben haben. Kunden erhielten außerdem das Recht, dass ihre Daten im Internet gelöscht werden und dass ihnen Daten übergeben werden, wenn sie etwa von Facebook in ein anderes soziales Netzwerk wechseln wollten. Unternehmen drohten künftig hohe Strafen, wenn sie sich nicht an Regeln halten. Bußgelder könnten bis zu vier Prozent des weltweiten Jahresumsatzes erreichen oder maximal 20 Mio. Euro. Künftig müssten europäische Unternehmen, die in großem Stil sensible Daten verarbeiten oder das Verhalten von Verbrauchern überwachen, einen Datenschutzbeauftragten benennen. Komme es zum Verstoß eines Unternehmens, den die Datenschutzbehörden der Mitgliedstaaten unterschiedlich interpretieren, habe der Europäische Datenschutzausschuss das letzte Wort und fasse rechtskräftige Beschlüsse.

In derselben Ausgabe geht die Wochenzeitung auf das **Safe-Harbor-Urteil des EuGH** ein, mit dem das Safe-Harbor-Abkommen zwischen der EU und den USA gekippt wurde. Seit dem Jahr 2000 hätten amerikanische Unternehmen die Daten von Europäern problemlos in die USA übertragen sowie dort speichern und verarbeiten können, vorausgesetzt, sie erklärten sich dazu bereit, bestimmte Datenschutzstandards einzuhalten. Inzwischen hätten mehrere Datenschutzbehörden Zweifel daran angemeldet, ob Unternehmen auf anderer rechtlicher Grundlage Daten übertragen können, wenn sich die Rechtslage in den USA nicht ändert. Zwar verschafften die EU-Datenschutzbehörden den Unternehmen etwas Luft, indem sie der EU-Kommission und ihren amerikanischen Verhandlungspartnern bis Ende Januar Zeit geben, ein neues Abkommen auszuhandeln. Die Gespräche würden sich aber offenbar alles andere als einfach gestalten. Solange es keine Nachfolgeregelung gibt, könnten nun europäische Datenschützer Datenübertragungen in die USA auf ihre Rechtmäßigkeit prüfen und für nicht rechtmäßig erklären, falls sie sich allein auf die ungültige Safe-Harbor-Entscheidung stützen, betont die FAZ am 1. Februar. Laut Internetwirtschaftsverband Eco könnten sich Unternehmen, wenn sie

Daten nach Amerika übertragen, auch auf EU-Standardvertragsklauseln oder sogenannte Binding Corporate Rules berufen. Vertreter der deutschen Wirtschaft würden derweil anmahnen, dass es auch kurzfristig weiter möglich sein müsse, Daten in die USA zu übermitteln. Manche deutsche Unternehmen würden dagegen schon auf den Datenspeicherstandort Europa bauen. Fakt sei, dass europäische Datenschutzrichtlinien schärfer seien als amerikanische.

Diebstahl

Wie das BKA in der Wochenlage am 4. Januar berichtet, wurden seit Mai 2015 der Gemeinsamen Grundstoffüberwachungsstelle ZKA/BKA (GÜS) mehrere Fälle des Diebstahls von **Wasserstoff-Druckgasflaschen** in verschiedenen Niederlassungen eines international tätigen Gase produzierenden Unternehmens in Nordrhein-Westfalen bekannt. Die noch nicht ermittelten Täter hätten sich jeweils durch Einbruch Zutritt zum Firmengelände verschafft und die Gasflaschen mittels Klein-Lkw abtransportiert. Die Zahl der entwendeten Gasflaschen habe jeweils im zweistelligen Bereich gelegen, mit Mengen von teils mehreren Tausend Litern Gas je Diebstahlsfall. Bislang seien der Firmengruppe in den Jahren 2014 und 2015 knapp 400 Druckgasflaschen mit einer Gesamtmenge von rund 20.000 Litern Wasserstoff und einem Gesamtschaden von mehr als 200.000 Euro entwendet worden. Aus den Niederlanden seien dem BKA in den letzten Monaten vermehrt Sicherstellungen von Wasserstoff-Druckgasflaschen im Zusammenhang mit der Aufdeckung illegaler Rauschgiftlabore bekannt geworden. Von bislang 58 in den Niederlanden zum Teil in Rauschgiftlaboren sichergestellten Gasflaschen seien zehn Flaschen einem Diebstahl in Dortmund zugeordnet worden. Bei einer anderen Firma in Hessen seien im November 2015 insgesamt 14 Druckgasflaschen Chlorwasserstoff mit gleicher Tatbegehung gestohlen worden. Nach derzeitigem Kenntnisstand werde davon ausgegangen, dass eine kriminelle Gruppierung aus vermutlich niederländischen Staatsangehörigen mit gleicher Tatbegehungsweise nun auch andere Gase für die illegale Rauschgiftherstellung in den Niederlanden durch Auftragsdiebstähle in Deutschland beschafft. Die große Menge der gestohlenen Chemikalien stehe im Einklang mit dem aktuell aus den Niederlanden berichteten hohen Ausmaß der illegalen Produktion von Amphetaminen.

„Schlüssellos klaut sich famos" titelt die FAZ am 19. Januar. Den Dieben gelänge, was die Zulieferer der Systeme jedenfalls offiziell bislang für unmöglich gehalten hätten: Sie hackten sich in die Frequenz zwischen Schlüssel und Auto und verlängerten deren Funkwellen. Es werde also nicht etwa die Frequenz gehackt, sondern das Signal verlängert. So „glaubten" die Antennen im Auto, der Schlüssel sei an Bord. Deshalb blockiere die Wegfahrsperre nicht, und auch die Alarmanlage schlage nicht an, registrierten beide Sicherheitssysteme doch den rechtmäßigen Schlüssel. Die kryptologischen Verschlüsselungsverfahren würden somit außer Kraft gesetzt. Die Autoindustrie arbeite permanent daran, die Angriffe zu erschweren. Doch offenbar fehle ihr kurzfristig eine schlagkräftige Antwort. Eine Lösung sei die Übertragung im Ultra Wide Band (UWB) und die Einführung eines Hochfrequenz-Standards. Der verwende ein Datenprotokoll, das den Abstand zwischen Auto und Schlüssel misst. Unter dem Markennamen Decawave sei es einem Hersteller gelungen, den USB-Empfänger auf Chipgröße zu bringen. Bis diese Technik im Auto einsetzbar ist, werde es nach Aussagen von Zulieferern bis zum Jahr 2019 dauern. Noch weiter voraus reiche die Idee, biometrische Daten zu nutzen.

Drohnensicherheit

Das Kasseler Start-up-Unternehmen Dedrone habe ein Gerät entwickelt, das vor Drohnenangriffen warnt, heißt es in der FAZ am 1. Februar. Die **Luftschutz-Warnanlage** sehe aus wie eine vierblättrige Blumenblüte, sei bestückt mit hochsensiblen Video- und Audiosensoren und lasse sich überall und jederzeit aufbauen. Die Chips unterschieden jede Drohne von einem Vogel und hörten aus 300 Metern Entfernung das Schnurren eines kleinen Elektromotors. Sie könnten alle Signale an eine digitale Plattform weiterreichen und dort auswerten lassen.

Energieversorgungssicherheit

Das BKA weist im Sonderbericht Wirtschaftsschutz vom 15. Januar darauf hin, dass in den Jahren 2013 bis 2015 insgesamt 511 Straftaten mit linksextremistischer Motivation zum Thema „Klimaschutz" registriert worden seien. Die Aktionen/Straftaten hätten 2015 überwiegend in NRW und hier insbesondere im Zusammenhang mit den Protesten gegen die Rodung des Hambacher Forsts stattgefunden. Im Kern würden Linksextremisten das Thema „Klimawandel" mit der grundsätzlichen Kritik am „kapitalistischen System" verbinden. Aktivitäten der **Kampagne „Ende Gelände"** orientierten sich mittlerweile auch auf das Braunkohlerevier in der Lausitz und auf die Firma Vattenfall als Betreiber der dortigen Kraftwerke und der Kohleförderung. In einem Newsletter werde für 2016 unter anderem an Pfingsten zu „Massenaktionen zivilen Ungehorsams" in der Lausitz mit einem mindestens viertägigen „Camp" aufgerufen. Daneben sei im August/September ein „Klimacamp" und „Degrowth Summerschool" im Rheinland mit neuen Aktionsformen vorgesehen.

Gefährdungslage Türkei

In der Wochenlage am 28. Januar aktualisiert das BKA die Beschreibung der Gefährdungslage Türkei. Dargestellt wird die Anschlagsaktivität der PKK, sonstiger linksterroristischer Organisationen und islamistischer Terroristen. Den Verlautbarungen im IS-Onlinemagazin KONSTANTINIYYE zufolge ist zwar weiterhin primär mit terroristischen Aktivitäten des IS gegen staatliche Einrichtungen und Angehörige der Sicherheitskräfte zu rechnen. In den Metropolen der Türkei sowie in den südöstlich gelegenen Grenzgebieten zu Syrien und dem Irak ist aber auch von einem anhaltenden Anschlagsrisiko gegen nichtmilitärische Ziele auszugehen. Selbst wenn sich die türkischen Sicherheitsvorkehrungen landesweit auf einem hohen Niveau bewegten, sei aufgrund des dynamischen politischen Prozesses und angesichts in der Vergangenheit durchgeführter Anschläge militanter Gruppierungen auch gegen nicht-militärische Ziele in allen Teilen der Türkei weiterhin von einer terroristischen Gefährdung auszugehen. Insbesondere in den Metropolen sowie in den Grenzgebieten zu Syrien und dem Irak bestehe ein anhaltendes Anschlagsrisiko. Deutsche Einrichtungen und Interessen stünden hierbei nicht im unmittelbaren Zielspektrum. Ein zufälliges Mitbetroffensein sei allerdings einzukalkulieren.

Geschäftsgeheimnisse

Der Behörden Spiegel meldet in seiner Januar-Ausgabe, dass sich EU-Kommission, Rat und EU-Parlament Ende 2015 auf einen Richtlinienentwurf zum Schutz von Geschäftsgeheimnissen (Know-how-RL) geeinigt hätten. Wichtiger Bestandteil dieser Richtlinie sei die Definition des Geschäftsgeheimnisses gemäß Art. 2 des Entwurfs. Eine Information soll nur dann als Geschäftsgeheimnis geschützt sein, wenn angemessene Maßnahmen zur Geheimhaltung ergriffen

wurden. Es gehe um technische und rechtliche Schutzmaßnahmen. Mit der Abstimmung im EU-Parlament sei 2016 zu rechnen.

Geschäftsreiserisiken

Einer bisher unveröffentlichten Umfrage nach führt sich jeder Zweite bei Zwischenfällen auf Dienstreisen allein gelassen, meldet die FAZ am 23. Januar. Jeder Dritte der Befragten habe in fremden Ländern schon mit politischen Unruhen oder mit Zollproblemen zu tun gehabt. Gestiegen sei die Zahl der Unternehmen, die ihren Mitarbeitern ein professionelles Risikomanagement anbieten. 55 Prozent der Befragten habe angegeben, dass ihr Arbeitgeber etwa Rückholpläne bereitstellt. Für die Studie im Auftrag der Travel Management Companies seien mehr als 200 Manager befragt worden.

IT-Sicherheit

Techchannel.de skizziert am 7. Januar **die 25 häufigsten Netzwerkfehler** und ihre Auswirkungen, u. a.:

- Die Konfiguration wurde nicht gespeichert und geht bei einem Neustart verloren.
- Die abgespeicherten „Konfigurationen" entsprechen nicht den Unternehmensrichtlinien.
- Unnötig viele Firewall-Regeln und nicht genutzte ACL-Einträge
- Überlastung von Firewall-Verbindungen
- Datenstau an einer Schnittstelle
- Probleme mit Links und deren Stabilität
- Belastungsgrenzen des Netzwerks sind überschritten.
- Falsche serielle Bandbreiteneinstellung
- Die VOP-Qualität ist schlecht.
- Das OSPF-Protokoll ist nicht richtig konfiguriert.
- Der Datenverkehr erfolgt nur in eine Richtung.
- Die Router-Schnittstelle ist down.
- Nutzung unbekannter Switches oder Hubs im Netzwerk
- Der Port ist im fehlerhaften Status.
- Ungleichmäßig ausgelastete Etherchannel-Verbindungen.

Die FAZ geht am 11. Januar auf eine von PwC Mitte 2015 durchgeführte Befragung von 400 mittelständischen Unternehmen ein. Danach sei 2015 jedes zehnte **mittelständische Unternehmen** mindestens einmal Opfer einer Attacke aus dem Internet. Im Schnitt sei ein wirtschaftlicher Schaden von rund 80.000 Euro entstanden. Viele Mittelständler hätten den Ernst der Lage noch nicht erkannt und verfügten weder über ausreichende technische Sicherheitsmaßnahmen, noch einen angemessenen Versicherungsschutz. Bisher habe sich nur jedes fünfte Unternehmen gegen einen Cyberangriff versichern lassen. Das IT-Sicherheitsgesetz schreibe nun Betreibern kritischer Infrastrukturen vor, sich besser gegen IT-Angriffe zu wappnen. Die betroffenen Unternehmen – u. a. Transport- und Logistikunternehmen, Energieversorger und Finanzdienstleister – müssten die Vorgaben formal bis zum 13. Juni 2017 umgesetzt haben. Bislang verfüge nur ein relativ kleiner Anteil der mittelständischen Unternehmen über gute Standards zur Informationssicherheit. Deutlichen Nachholbedarf gebe es noch bei Unternehmen aus den Branchen Transport und Logistik sowie Technologie, Medien und Telekommunikation.

Der Behörden Spiegel meldet in seiner Januar-Ausgabe, dass sich die EU-Kommission Ende 2015 auf die **Richtlinie zur Netz- und Informationssicherheit (NIS**) geeinigt habe. Die Richtlinie sei Teil einer europäischen Cyber-Sicherheitsstrategie. Ziel sei es, Cyber-Angriffe auf die europäische Netz- und Informationsinfrastruktur zu verhindern. Hierfür sehe die Richtlinie unter anderem vor, dass die EU-Mitgliedstaaten eigene nationale NIS-Strategien entwickeln und beispielsweise ein IT-Notfallteam aufstellen müssen. Inhaltlich

deckten sich die Ziele mit dem IT-Sicherheitsgesetz.

Das US-Ministerium für Verkehr und Vertreter von 18 Firmen aus der Automobilindustrie haben sich nach einer Meldung von heise.de vom 17. Januar auf Maßnahmen gegen Cyber-Attacken auf **selbstfahrende Autos** geeinigt. Vereinbart worden sei ein proaktiver Dialog zwischen den Autobauern und der für die Verkehrssicherheit auf Bundesstraßen zuständigen Behörde, der National Highway Traffic Safety Administration.

IuK-Kriminalität

„Der Feind im PC" titelt die Wochenzeitung Das Parlament am 4. Januar. Cyberkriminalität nehme zu, die Attacken würden raffinierter. Der Schaden sei immens. Nach einer Studie von Corporate Trust habe jedes zweite deutsche Unternehmen in den vergangenen beiden Jahren einen Spionageangriff oder Verdachtsfall zu beklagen. Konkret seien 26,9 Prozent von einem konkreten Vorfall betroffen. Dies stelle einen Anstieg um 5,5 Prozent im Vergleich zu den Ergebnissen aus der Studie 2012 dar. Der jährliche finanzielle Schaden durch Industriespionage beträgt 11,8 Mrd. Euro. Im Fokus des Datendiebstahls stehe der Mittelstand. Nach Angaben der Wirtschaftsberatungsgesellschaft KPMG herrscht ein gravierendes Missverhältnis bei der deutschen Wirtschaft in der Einschätzung von allgemeiner und eigener Betroffenheit. Neun von zehn Unternehmen sähen allgemein ein hohes Risiko für deutsche Unternehmen, Opfer von Cyberverbrechen zu werden. Dagegen schätze weniger als die Hälfte die eigene Gefährdungslage als hoch ein. Die meisten Fälle würden nicht gemeldet. Das größte Risiko bestehe im Verlust von Kundendaten und dem folgenden Imageschaden. Hacker suchten übrigens nicht die möglichst größte Beute, sondern achteten darauf, dass sie ihre Tat möglichst einfach ausführen können. Firmen müssten also umdenken. Ein Notfallplan, so die einhellige Expertenmeinung, sei oberste Pflicht, um die Folgen eines IT-Sicherheitsvorfalls minimieren zu können. Dieser liste zum Beispiel die wichtigsten Geschäftsprozesse des Unternehmens auf und beschreibe, was im Schadensfall zu tun und wer zu informieren ist. Eine Voraussetzung für mehr Sicherheit sei verschlüsselter Datenverkehr oder die Ablage von Daten nur in geschützten Bereichen. Besonders großen Handlungsbedarf sähen das BSI und das BMI bei Sicherheitslücken von Software. Schlecht würden in dem BSI-Report über kritische Schwachstellen zum Beispiel die Programme Adobe Flash und Microsoft Internet Explorer sowie die Betriebssysteme OS X von Apple und Windows von Microsoft abschneiden. Bei ihnen seien bis September 2015 jeweils mehr als 100 kritische Schwachstellen registriert worden.

Das BKA führt seit Juni 2015 ein Ermittlungsverfahren gegen eine bosnische Gruppierung von Cyberkriminellen mit dem Pseudonym **„DD4BC" („DDoS for Bitcoin)** wegen des Verdachts der Erpressung und Computersabotage durch. Die Gruppierung ist seit 2014 weltweit mit erpresserischen DDoS-Angriffen gegen die Onlinepräsenz größerer Unternehmen vorgegangen. Auch deutsche Unternehmen waren betroffen. Die Zahl der weltweit bekannt gewordenen Schadensfälle liegt im hohen dreistelligen Bereich. Die Unternehmen wurden zur Zahlung eines bestimmten Betrages aufgefordert, damit die Täter ihre Angriffe einstellen. Gefordert wurde jeweils ein Betrag in der digitalen Währung Bitcoin, zumeist im Wert von rund 10.000 Euro. Jetzt wurde ein bosnisch-herzegowinischer Staatsangehöriger durch eine bosnische Cybercrime-Dienststelle festgenommen. Er steht in Verdacht, eine führende Rolle in der Gruppierung zu spielen. Das BKA betont, es bedürfe einer vertrauensvollen Kooperation mit der Wirtschaft, da eine strafrechtliche Verfolgung nur möglich sei, wenn betroffene Unternehmen diese Taten anzeigen (Auszug aus der

Wochenlage vom 15. Januar 2016). Ausgestanden sei die Gefahr damit nicht, argumentiert die WirtschaftsWoche am 15. Januar. Denn seit Monaten gehe die Nachfolgetruppe Armada Collective mit ähnlichen Mitteln wie DD4BC vor. In Deutschland seien von den fünf größten Banken bisher laut Experten mindestens zwei angegriffen worden. Weil die Schutzgeldsummen, gemessen am Schaden des Angriffs, relativ gering seien, zahlten viele Unternehmen. Die geringe Geldsumme spreche für die Professionalität der Täter.

Acht Prozent deutscher Unternehmen und öffentlicher Einrichtungen sind nach einer Meldung von heise.de vom 19. Januar bisher ein- oder mehrmals Opfer „hacktivistischer Angriffe" geworden. Dies gehe aus einer **Dunkelfeld-Studie des BKA** hervor, in der sich aus einer Stichprobe von 4.543 Institutionen 971 Firmen und Behörden geäußert hätten. Die meisten Betroffenen stammten aus der Branche Information und Kommunikation. Konkret hätten die Attacken überwiegend aus Spam-Wellen bestanden, gefolgt von DDoS-Angriffen und verunstalteten Webseiten. Vielfach sei das eigene System mit Schadstoffen infiziert worden und der Server ausgefallen. Daneben hätten die Angriffe auch Sachschäden, Systemabstürze, Daten- und Reputationsverluste, Umsatzeinbußen und unerwünschte Presseberichterstattungen bewirkt. Es falle auf, dass Einrichtungen, die einen Mitarbeiter-Zugriff auf das Netzwerk von außerhalb erlauben, besonders von Shitstorms und Cyberangriffen betroffen gewesen seien.Heise.de meldet am 26. Januar einen Identitätsdiebstahl bei **Car2go**-Kunden. Sie bekämen derzeit eine Phishing-SMS zugeschickt, die angeblich vom Anbieter versendet wurde. Wer eine derartige SMS erhält, sollte nicht auf den enthaltenen Link klicken. Denn dieser führe zu einer Phishing-Webseite, auf der die unbekannten Betrüger Opfer auffordern, Scans von ihrem Führerschein und Personalausweis hochzuladen. Car2go zufolge sind die Betrüger an Namen von Kunden und deren Telefonnummern gekommen. Bezahldaten sollen dabei nicht abgegriffen worden sein.

Lässt man die News, die 2015 die Security-Branche beschäftigten, noch einmal Revue passieren, dann falle auf, dass vor allem spektakuläre Hacks und Schwachstellenfunde im Gedächtnis geblieben sind, schreibt TECCHANNEL am 26. Januar. Dabei gerate leicht in Vergessenheit, dass Cyber-Kriminelle ihre Schadsoftware weiter verbessert haben. TECCHANNEL skizziert die gefährlichsten Bedrohungen und geheimen Tricks der Cyber-Kriminellen: Ransomware, Exploit Kits, CBT-Locker, Angler Exploit Kit, AAEH/Beebone, Simda, Logjam, Matsnu, CertifiGate, Sality Gambling Campaign, BrainTest, XCodeGhost. Cyber-Kriminelle lernten immer mehr und immer schneller, wie sie Barrieren umgehen können, um an ihr Ziel zu gelangen. Es gebe aber inzwischen eine Reihe von Technologien und Prozessen, die jedes Unternehmen implementieren könne, um sich gegen Ransomware, Exploit Kits und Bot-Infektionen bestens zu schützen.

Kartellrecht

Focus befasst sich in der Ausgabe 2-2016 mit der Umsetzung des Kartellrechts. Das deutsche Wettbewerbsrecht tue sich schwer, einerseits funktionierende Märkte zu gewährleisten und andererseits Wirtschaftskriminalität zielgenau zu sanktionieren. Zwar verhängten deutsche und europäische Aufseher immer wieder eindrucksvolle Bußen in Höhe von mehreren hundert Mio. bis zu einer Mrd. Euro. Doch die Zahl der Kartelle sei nicht zurückgegangen. Die Justizminister der Bundesländer hätten sich vor allem über Wiederholungstäter in klassischen Hardcore-Kartellen geärgert: Seit Jahrzehnten ertappten die Behörden immer wieder Baufirmen, Zulieferer oder Schiene und Bahn. Für Empörung habe vor einem Jahr der Wurstfabrikant Clemens Tönnies gesorgt, der das Bundes-

kartellamt raffiniert habe auflaufen lassen. Er habe die wegen Preismanipulationen verhängte Bußgeldzahlung in Höhe von 120 Mio. Euro verhindert, indem er im Handelsregister die Löschung der betreffenden Firmen erwirkte. Dabei sei das deutsche Wettbewerbsrecht eigentlich eine Erfolgsgeschichte: Seit dem Jahr 2000 habe das Bundeskartellamt dank der neu eingeführten strafbefreienden Kronzeugenregelung etliche Kartelle geknackt. 2003 habe es eine Rekordbuße von 660 Mio. Euro gegen das Zement-Kartell verhängt, das das OLG Düsseldorf 2009 allerdings halbierte. Das stringente Vorgehen sei aber in den Führungsetagen sehr aufmerksam registriert worden. So hätten die Kartellwächter mit der Brauerei Anheuser Busch als Kronzeugen das Bier-Kartell zerschlagen und Adidas, Asics oder den Rucksack- und Outdoor-Hersteller Deuter bei Preisvorgaben in die Scharanken gewiesen. Sie hätten die vermeintliche Bestpreisgarantie bei Hotelportalen untersagt und sich die Tarife der Heizungsableser Brunata und Ista vorgeknöpft. Kein deutscher Konzern kenne sich so gut aus mit Kartellen wie ThyssenKrupp. Über alle Geschäftsbereiche hinweg kümmerten sich 400 Manager darum, dass die Geschäfte sauber bleiben. 70 von ihnen überprüften die Einhaltung der Regeln sogar hauptamtlich. Seit 2011 schwanke die Zahl der jährlichen Bußgeldentscheidungen der Kartellämter in den Ländern und im Bund gerade einmal zwischen 13 und 15. In eigentlich allen Branchen fänden sich Verstöße, sobald die Wettbewerbshüter nur einmal genauer hinsähen. Die EU-Wettbewerbskommissarin Margarethe Vestager rolle ein Verfahren gegen Google neu auf und drohe mit einer Rekordstrafe von 6,6 Mrd. Euro wegen der Benachteiligung von externen Diensten in der Suchergebnisliste. Die beiden größten Verfahren drehten sich um Amazon und Apple.

Korruption

Nach der Einstufung von Transparency International (TI) hat sich Deutschland im internationalen Vergleich um zwei Plätze auf den zehnten Rang verbessert, meldet die FAZ am 28. Januar. In den vergangenen zwei Jahren habe das Land einige Hausaufgaben in der Korruptionsbekämpfung erledigt. Insgesamt gebe es mehr Länder, in denen sich die Lage 2015 verbessert habe, als Länder mit einer Verschlechterung. Am Ende der 168 Länder umfassenden Liste stünden Nordkorea und Somalia, kurz davor Afghanistan und der Sudan.

Kreditkartenbetrug

Das Chip+PIN-System aktueller Kreditkarten ist nicht sicher vor Betrügern, schreibt zeit.de am 22. Januar. Eigentlich würden Kreditkarten mit Chip+PIN-Funktion als sicher gelten, vor allem im Vergleich zum alten System mit Magnetstreifen. Recherchen von c't und der ZEIT belegten nun aber, dass Kriminelle auch solche Kreditkarten klonen, die Sicherheitsvorkehrungen austricksen, und mit den Karten einkaufen können. Eine Reihe von Daten, Programmen und Werkzeugen brauche es für den Betrug mit solchen geklonten Karten und für die Umgehung des nach Europay, MasterCard und Visa benannten EMV-Bezahlsystems: Typ, Nummer und Ablaufdaten einer Karte, die Software SDA EMV Chip Writer samt der darin enthaltenen App MacGyver.cap, Smartcard-Rohlinge, Druckmaschinen und Material für Blanko-Kreditkarten. Statt eine exakte Kopie einer Kreditkarte mit Sicherheitschip zu erstellen, sorge **die MacGyver-App der Kriminellen** dafür, dass ein Bezahlvorgang auch ohne die bei Chip+PIN eigentlich vorgesehenen Sicherheitsüberprüfungen stattfindet. Das auf der geklonten Karte installierte Protokoll sorge dafür, dass das Kartenterminal einfach

jede beliebige PIN akzeptiert. Handelsübliche Bezahlterminals in Geschäften ließen sich von MacGyver missbrauchen. Kriminelle könnten auch verschiedene Guthabenkarten aufladen. Mit einem mobilen Kreditkartenlesegerät von payleven, iZettle oder SumUp könnten die Betrüger auch gänzlich unbeobachtet abräumen. In Deutschland halte sich das Bedrohungsszenario in Grenzen, denn deutsche Banken und ihre Dienstleister prüften die Echtheit der Kreditkartenchips offenbar so, wie es das EMV-System vorsieht.

Lüftungsanlagen

Der Sicherheits-Berater weist in Ausgabe 1-2016, S. 17-19, darauf hin, dass Ende Juli 2014 die VO (EU) Nr. 1253/2014 – Anforderungen an die umweltgerechte Gestaltung von Lüftungsanlagen – in Kraft getreten ist. Seit dem 1. Januar 2016 müssten nun die dort festgeschriebenen Ökodesignanforderungen für das Inverkehrbringen oder die Inbetriebnahme von Lüftungsanlagen erfüllt werden. Festgelegt seien die Anforderungen an Nichtwohnraumlüftungsanlagen in der Verordnung in Anhang III, Nr. 1. Im Kern gehe es dabei um den Einsatz von Wärmerückgewinnungssystemen, deren Einhaltung von Mindestrückwärmezahlen und die Effizienz von Ventilatoren.

Mitarbeiterüberwachung

Silicon.de weist am 14. Januar auf ein Urteil des EGMR hin, das sich auf E-Mail- und Chat-Anwendungen auf einem Firmencomputer durch einen Mitarbeiter bezieht. Nach dem Urteil darf ein Arbeitgeber solche privaten Nachrichten seiner Mitarbeiter überwachen, um sicherzustellen, dass diese ihren arbeitsvertraglichen Pflichten nachkommen. Er hatte im konkreten Fall die Nutzung von Unternehmensressourcen zu privaten Zwecken untersagt. Der Arbeitgeber sah in der privaten Nutzung während der Arbeitszeit einen Verstoß gegen den Arbeitsvertrag und kündigte seinem Mitarbeiter. Dadurch werde das in Artikel 8 der Europäischen Menschenrechtskonvention garantierte Brief- und Telekommunikationsgeheimnis nicht verletzt. Die Identität der Personen, mit denen der Mitarbeiter kommuniziert habe, sei nicht öffentlich gemacht worden.

Schwertransportbegleitung

Um die Belastung der Polizei durch die verkehrsrechtlich vorgeschriebene Begleitung von Großraum- und Schwertransporten (GST) zu vermindern, hat das Niedersächsische Ministerium für Inneres und Sport nach einer Pressemitteilung des Ministeriums ein Konzept entwickelt, in dessen Rahmen die Wahrnehmung der Aufgaben bei der Begleitung der GST voraussichtlich ab Ende Februar auf Hilfspolizeibeamtinnen und -beamte übertragen werden kann. Niedersachsen bestelle damit als erstes Bundesland die Mitarbeiterinnen und Mitarbeiter privater Begleitfirmen zur Durchführung von GST zu Hilfspolizeibeamtinnen und -beamten. Das Pilotprojekt sei als Übergangsregelung geplant, bis der Bund eine entsprechende Regelung gefunden habe. Voraussetzung sei eine mindestens dreijährige berufliche Erfahrung. Die Hilfspolizeibeamtinnen und -beamten sollten ausnahmslos für die Begleitung bestellt werden und dementsprechend auch nur eingeschränkte Befugnisse erhalten, ausschließlich für den Bereich der Verkehrsregelung.

Seilbahnsicherheit

Dank einer neuen Technik werde der Riss eines Gondelseils unwahrscheinlicher, berichtet die FAZ am 9. Januar. In Deutschland schreiben Vorschriften der Bundesländer eine

monatliche Sichtprüfung und für Tragseile ein vierteljährliches Prüfintervall vor. Die Prüfer versuchten, an dem mit einer Geschwindigkeit von weniger als 0,5 Metern je Sekunde und in handnaher Distanz vorbeilaufenden Seil mit bloßem Auge zuverlässig Schäden und Anzeichen für Verschleiß wie Risse, Knicke, Umbrüche und Verschmelzungen der Drahtlitzen zu entdecken. Man könne sich vorstellen, welche Konzentration dies bei einer Seillänge von einigen hundert bis mehreren tausend Metern verlange. Die Winspect GmbH habe über fünf Jahre mit dem Institut für Fördertechnik und Logistik der Uni Stuttgart ein teilautomatisiertes optisches Prüfgerät entwickelt und damit die visuelle Kontrolle von Seilen stark vereinfacht. Ein Seilprüfgerät werde in eine an der Seilbahn einmalig zu installierende Vorrichtung eingehängt. Bei Zugseilen werde das vorbeilaufende Seil mit vier kreisförmig um das Seil angeordneten Kameras aus allen Blickwinkeln aufgezeichnet. Der Seilumfang sei dabei in vier Bereiche unterteilt, die mit je einer Zeilenkamera erfasst und digital gespeichert werden. Die Software „wisse", wie ein ordnungsgemäßes, technisch perfektes Seil auszusehen habe, und zeige alle entdeckten Abweichungen vom Optimalzustand. Ein großer Vorteil des Systems sei, dass es den weitaus größten Teil des Seils als „in Ordnung" auszusondern vermöge. Winspect sei mit einer Aufnahmegeschwindigkeit von 3 Metern je Sekunde zudem sechsmal schneller als das menschliche Auge. Auch die VBG betrachte die neue Technik als richtungsweisend.

Sicherheitswirtschaft

Die FAZ befasst sich am 26. Januar mit einer Stellungnahme des BDSW zu Plänen des BMA, die **Zulässigkeit von Zeit- und Werkverträgen** stärker zu regulieren. Nach dieser Stellungnahme drohe der Sicherheitsbranche womöglich sogar das Aus in ihrer bisherigen Form als eigenständiger Wirtschaftszweig. Das Ergebnis der Analyse: Unternehmen oder auch Behörden, die etwa ihren Empfang durch Mitarbeiter einer Sicherheitsfirma betreuen lassen, müssten künftig rechtlichen Ärger wegen missbräuchlichen Einsatzes von Fremdpersonal befürchten. Der einzige Weg auf sicheres Terrain wäre dann, dass sich der Sicherheitsdienstleister zum Zeitarbeitsunternehmen wandelt und seine Mitarbeiter an die Kunden verleiht. Besonders heikel sei das Thema Werkvertrag. Hier solle ein neuer Katalog aus acht gesetzlichen Prüfkriterien klären, ob die Fremdvergabe eines Auftrags als missbräuchlicher Fremdpersonaleinsatz zu werten ist. Schon ein ganz normaler Pförtner am Empfang des Kundenbetriebs erfülle den Großteil dieses Verdachtkatalogs. Der Kunde hätte dann die Mitarbeiter auf die eigene Gehaltsliste zu übernehmen. Schon deshalb sei kaum anzunehmen, dass sich ein möglicher Kunde noch auf andere Vertragsgestaltungen als einen Arbeitnehmerüberlassungsvertrag einlässt. Doch wäre Zeitarbeit keine gute Lösung. Kein Kunde wolle, dass die Sicherheitskräfte ständig wechselten – eben dies müsste aber wegen der geplanten Höchsteinsatzdauer für Zeitarbeiter spätestens alle 18 Monate geschehen.

Smart Home

Samsung versuche, Fernseher in das sogenannte „Internet der Dinge" einzubinden und sie mit einem speziellen Adapter zur Schaltzentrale für vernetzte Produkte im Haushalt zu machen, meldet die FAZ am 9. Januar. Damit solle es möglich werden, mit dem Internet verbundene Produkte wie Rauchmelder oder Alarmanlagen vom Fernseher aus zu steuern.

Spionage

Der Sicherheits-Berater weist in Ausgabe 1-2016, S. 19, darauf hin, dass die EMshield

GmbH eine neue Schutzfolie gegen das Abgehörtwerden mit Lasermikrofonen auf den Markt gebracht hat. Das Produkt dürfte für alle interessant sein, die Konferenzbereiche oder sonstige Räume gegen Abhören schützen und davon ausgehen müssen, dass es Angreifer mit hochmoderner Technik gibt.

Terrorismus

EUROPOL habe vor Terroranschlägen durch die Dschihadistenmiliz des IS in Europa gewarnt, meldet die FAZ am 26. Januar. Der IS habe „neue, gefechtsartige Möglichkeiten" entwickelt, um weltweit eine Reihe „groß angelegter Terroranschläge" zu verüben. Ein dazu erstellter Europol-Bericht komme zu dem Schluss, dass die Dschihadisten insbesondere Europa im Visier hätten. Die von EUROPOL gesammelten Informationen deuteten darauf hin, dass der IS ein Kommando für Einsätze außerhalb seines „Kalifats" in Syrien und im Irak gebildet habe.

Trends

Der Sicherheits-Berater gibt in Ausgabe 1-2016 (S. 1-12) Argumente zur Entwicklung einiger Bedrohungsphänomene und der Sicherheitswirtschaft. 2016 werde ein starker Anstieg an Brandstiftungen zu verzeichnen sein. Die bereits hohe Zahl an Einbrüchen werde weiter wachsen. Der Branchenumsatz des Sicherheitsgewerbes werde um fünf bis sieben Prozent ansteigen. Der Aufwand für die IT-Sicherheit werde 2016 stark zunehmen, die IT-Sicherheit selbst trotzdem weiter abnehmen. Grund sei die „Industrie 4.0". 2016 sei mit einem Anstieg der Ransomware-Attacken um 25 bis 40 Prozent zu rechnen. Im Bereich der Sicherheitstechnik sei die Zutrittskontrolle „ein echter Dauerbrenner". Ihr Wachstumspotenzial liege bei mindestens sechs Prozent. Im Brandschutzsektor würden Nachrüstungen immer häufiger. Daher werde die installierende Wirtschaft 2016 eine Zunahme im Bereich BMA von ebenfalls sechs bis acht Prozent erleben. Im Nachrüstungsbereich Fenster, Terrassen- oder Balkontüren sei ein Anstieg um acht bis zehn Prozent des Umsatzes denkbar. Die Zahl der Alarmempfangsstellen nach EN 50518 werde 2016 weiterhin zunehmen. Errichter könnten mit einem Umsatzzuwachs in Höhe von zehn Prozent rechnen.

Verschlüsselung

Zeit.de berichtet am 7. Januar, der US-Kryptologe David Chaum arbeite an einem Verschlüsselungssystem, das zwei Dinge vereinen soll: Nutzer sollten sicher und anonym kommunizieren können und Strafverfolgern soll es unter bestimmten Bedingungen möglich sein, die Verschlüsselung und die Anonymität einzelner Verdächtiger aufzuheben. Chaum beschreibe zunächst einmal ein Protokoll namens cmix. Es solle sogenannte Mix-Netzwerke so effizient machen, dass sie sich für Chat-Apps, Filesharing, Suchen und Veröffentlichen sowie für Bezahlsysteme eignen. Dabei solle es die Metadaten verschleiern und die Inhalte verschlüsseln. In Mix-Netzwerken würden Nachrichten nicht direkt vom Sender zum Empfänger geschickt, sondern in mehreren Schichten verschlüsselt und über mehrere Zwischenstationen geleitet. Keine Zwischenstation kenne sowohl den Sender als auch den Empfänger. Populär geworden sei das Prinzip mit dem Onion Routing im Tor-Netzwerk. Der Schutz der Anonymität lasse sich aber noch verbessern, wenn mehrere Botschaften gesammelt und ihre Reihenfolge geändert wird, bevor sie weitergeleitet werden.

Wie die WirtschaftsWoche am 8. Januar berichtet, habe es das Softwareunternehmen Virtual Solution geschafft, mithilfe von App und Smartcard den Datenverkehr zu ver-

schlüsseln. Die sensibelsten Funktionen des Gerätes, die Authentifizierung des Nutzers und die Verschlüsselung des Datenverkehrs liefen über die deutsche Smartcard, die wie ein Tresor funktioniere. Wertvolle Daten würden dort so eingeschlossen, dass nur der Besitzer sie herausholen könne. Secusmart liefere **abhörgeschützte Blackberrys**. Die Secunetz Security Networks AG verkaufe ihre für stationäre Computer entwickelte Verschlüsselungstechnik Sina inzwischen auch in Kombination mit zwei Laptops von Microsoft und Lenovo, und Rohde & Schwarz entwickele mit dem Verschlüsselungsstick TopSec Mobile eine zusätzliche externe Verschlüsselungshardware, die – über Bluetooth-Funk mit dem Handy gekoppelt – alle ein- und ausgehenden Telefonate chiffriere.

BlackBerry-Geräte, die mit PGP-Verschlüsselung kommunizieren, seien nach wie vor nicht angreifbar, teilt der Hersteller nach einer Meldung von silicon.de vom 18. Januar mit. Damit dementiere BrackBerry Berichte, wonach die niederländische Polizei die Verschlüsselung angeblich umgehen konnte. Das Netherlands Forensics Institute hatte erklärt, es sei ihm gelungen, die PGP-Verschlüsselung auf Blackberry-Smartphones zu umgehen. Der Hersteller habe noch einmal betont, dass es keine Hintertüren in seinen Geräten gebe und er die Gerätepasswörter nicht speichere. Außerdem habe sich Blackberry wiederholt gegen Vermutungen verwahrt, es gewähre gewissen Staaten Einblick in die über seine Dienste laufende Kommunikation.

Für spontane Funkverbindungen wie etwa in WLAN-Hotspots soll bald sichere Verschlüsselung möglich werden, ohne dass man am Tresen nach dem WLAN-Passwort fragen muss, meldet heise.de am 25. Januar. Mit dem neuen Ansatz Opportunistic Wireless Encryption (OWE) sollen Geräte schon bei der WLAN-Verbindungsaufnahme Parameter für den Diffie-Hellman-Schlüsselaustausch übertragen. Damit könnten sie sich auf einen geheimen Schlüssel einigen und darüber dann die eigentlichen Sitzungsschlüssel zum Chiffrieren der WLAN-Verbindung austauschen. Zwar komme OWE höchstens an das Sicherheitsniveau von WPA2-PSK heran, sei damit aber immer noch wesentlich besser als ganz ohne Verschlüsselung und ohne Zutun des Nutzers einzurichten.

Videoüberwachung

Die bei Aldi verkauften IP-Überwachungskameras der Marke **Maginon** weisen nach einem Bericht von heise.de vom 15. Januar massive Sicherheitsmängel auf. Unbefugte könnten über das Internet auf das Kamerabild zugreifen und sogar den Ton anzapfen. Zudem würden die Geräte die Passwörter für WLAN, E-Mail und FTP-Zugang ihres Besitzers verraten. Betroffen seien die Modelle IPC-10 AC, IPC-100 AC und IPC-20 C. Diese habe Aldi mit einer Firmware angeboten, die eine Nutzung des Fernzugriffs auch dann zulässt, wenn der Nutzer bei der Inbetriebnahme kein Passwort gesetzt hat. Ferner seien diese Geräte motorgesteuert schwenkbar, ein ungebetener Gast könne also den Bildausschnitt beliebig verändern. Aldi habe allerdings erklärt, dass den Nutzern bereits seit Monaten ein Firmware-Update zur Verfügung stehe, bei dem sie ein persönliches Passwort festlegen müssen. Freilich – so heise.de – sei selbst nach dem Befolgen aller Sicherheitshinweise Vorsicht geboten: Da der Fernzugriff der Kameras unverschlüsselt über http übertragen werde, könne sich ein Mitlauscher bei der Nutzung ebenfalls dauerhaften Zugang zur Kamera verschaffen.

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