Bundesverband

Newsletter Sicherheitspolitik

KW 09/17, 03.03.2017

IN EIGENER SACHE

1. ASW Sicherheitsspiegel – Handbuch Wirtschaftsgrundschutz (Folge 3)

Wenn es um die Sicherheit geht, sehen sich viele Unternehmen vor allem vor der Herausforderung ihre IT zu schützen. Doch neben der IT Sicherheit gibt es auch heute noch viele weitere Gefahren für Unternehmen. Dazu gehören physische, prozessuale, personelle und organisatorische Gefahren, die neben informationstechnischen Herausforderungen zur Bedrohung für Unternehmen werden können. Ergänzend zum IT-Grundschutz, welches sich auf die IT-Sicherheit des Unternehmens bezieht, bietet das Handbuch Wirtschaftsgrundschutz eine weitere Orientierung für die Sicherheitspolitik des Unternehmens. Welche weiteren Aspekte das Handbuch Wirtschaftsgrundschutz beinhaltet, inwieweit es die Unternehmen bei der Gestaltung ihrer Sicherheitspolitik unterstützen kann und wie auf das Handbuch zugegriffen werden kann, erfahren Sie **hier** in der dritten Folge des ASW Sicherheitsspiegels.

2. Nächste Sitzung des Kompetenz-Centers Aus- & Weiterbildung findet am 05. April in Köln statt

Das Kompetenz-Center Aus- & Weiterbildung findet sich zur nächsten Sitzung am 05. April in Köln zusammen. Themen der Sitzungen werden u.a. Aus- und Weiterbildungsangebote für den Mittelstand, Ausbildungsmaterialien, Forschungsprojekte und Öffentlichkeitsarbeit sein. Sollten Mitglieder unserer Mitgliedsverbände Interesse an einer Teilnahme haben, kontaktieren Sie bitte die Geschäftsstelle unter info@asw-bundesverband.de für weitere Informationen.

3. ASW Bundesverband veröffentlicht Leitblatt zum Identitätsmissbrauch

Das Leitblatt beschreibt die Charakteristika von Identitätsmissbrauch, wie man dem Diebstahl und Betrug im analogen aber auch digitalen Raum vorbeugen kann und was man tun sollte, wenn man Opfer von Identitätsmissbrauch geworden ist. Beim Identitätsmissbrauch wird mit zuvor gestohlenen personenbezogenen Daten wie dem Geburtsdatum, der Adresse, Bankkonten, Kreditkartenummer, Führerschein- oder Sozialversicherungsnummern die Identität einer anderen Person angenommen. Ziel kann dabei Rufschädigung, Betrug oder auch andere illegale Aktivitäten sein, die oftmals mit hohen Schulden und Strafen für das Opfer einhergehen. Betroffen sind Privatpersonen, aber auch für die Unternehmen hat diese Betrugsform Auswirkungen: wirtschaftlicher Schaden durch Betrug im Warenhandel, Diskreditierung und Manipulation von Mitarbeitern oder dem Unternehmen selbst. Das Leitblatt steht **hier** kostenfrei zum Download zur Verfügung.


Identitätsmissbrauch

Charakteristika von Identitätsmissbrauch

Dem Diebstahl und Betrug vorbeugen

ASW Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Neue Schönhauser Straße 20 | 10178 Berlin
Telefon +49 (0)30 200 77 200 | Telefax +49 (0)30 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de

4. **Roadshow: Game over! Erfolgreich Manipulations- & Betrugsversuche abwehren**

In den Regionen findet eine ASW-Workshop-Reihe zum Thema Social Engineering statt. Durch geschickte Manipulation und Täuschung seitens der Angreifer ist das Datenleck Mensch die größte Bedrohung für Unternehmen. Sei es nun, dass durch geschickte Täuschung Geldüberweisungen (CEO-Fraud) vorgenommen werden oder unberechtigter Zugang zu IT-Systemen gewährt wird. Ziel der Workshop ist es, ohne Neuinvestitionen in kostenintensive Hard- und/oder Software vornehmen zu müssen, vorhandene „Tools", die in jedem Unternehmen als Basisschutz vorhanden sein müssen, wirkungsvoll und effektiv ein- und umzusetzen. Die Teilnahmegebühr beträgt 400€ und die ersten Termine sind die Folgenden: 15.03.2017 Stuttgart, 22.03.2017 Düsseldorf, 27.03.2017 Erfurt, 24.04.2017 Hamburg, 08.05.2017 Berlin. Informationen und die Möglichkeit zur Anmeldung finden Sie **hier**.

5. **Roadshow: Darknet Investigation Training**

Auch zum Thema Darknet gibt es eine ASW-Workshop-Reihe. Das Darknet hat massive Bedeutung in der Hacker-Community als Handelsplattform für illegale Geschäfte und ist somit zunehmend eine Bedrohung für Unternehmen. Angriffe werden dort vorbereitet. Beute wird zum Verkauf angeboten. Nur wer sich auskennt, hat die Chance, Angriffspläne schon vor der Ausführung zu kennen und sich entsprechend zu wappnen. Diese Workshops schulen wie man im Umgang mit der Parallelwelt des Internets, dem Darknet, den Straftätern bzw. Cyberkriminellen durch eigenständige Ermittlungen auf die Spur kommen kann. Die Teilnahmegebühr beträgt 400€ und die Termine für die Workshops sind die Folgenden: 11.04.2017 München, 12.04.2017 Hamburg, 18.04.2017 Erfurt, 02.05.2017 Düsseldorf, 03.05.2017 Stuttgart, 09.05.2017 Berlin. Informationen und die Möglichkeit zur Anmeldung finden Sie **hier**.

6. **ASWN: Vorstellung des Schulungskonzeptes „AGO – Awareness an Gefahrenorten" beim Deutschen Fußball Bund (DFB)**

Auf Einladung des DFB hat der Leiter Aus- und Weiterbildung der ASW Norddeutschland, Joachim M. Weger, am 22. Februar 2017 in Heidelberg im Rahmen einer Fortbildung für zertifizierte Lehrkräfte des DFB in der dortigen Hochschule das neue Schulungskonzept vorgestellt. Kern des Vortrages waren Videoaufnahmen von realen Eingangskontrollen bei zwei Fußballveranstaltungen im Dezember 2016 im hamburgischen Volksparkstadion. Die Teilnehmer, darunter auch der Einsatzleiter dieses Veranstaltungsdienstes sowie ein Beauftragter des DFB, diskutierten die sehr eindrucksvollen Aufnahmen ausführlich und teilweise kontrovers. Die Videos zeigten gestelltes auffälliges Verhalten, beispielsweise Abstellen eines Koffers in der Besucherschlange oder am Zaun, abruptes Verweigern und Entziehen der Körperkontrolle durch Flucht und die Erstreaktion der Einsatzkräfte. Weitere Informationen finden Sie in der angehängten Pressemitteilung.

INFORMATIONEN UNSERER PARTNER

1. **CSTV: SIDW mit Lars Waldow - Vernetzung von Gefahrenmanagementsystemen (Folge 26)**

Gefahrenmanagementsysteme sind Teil vieler, vor allem größerer, Unternehmen. Dabei betreffen diese nicht nur die Sicherheit, sondern auch die Kommunikation. Da die unterschiedlichen Systeme im Unternehmen auch oft von unterschiedlichen Herstellern sind, entsteht die Herausforderung alle Systeme unter eine Oberfläche zu bringen, um diese einheitlich steuern zu können. Lars Waldow von der Advancis Software & Services GmbH erklärt, welche Möglichkeiten sich zur Vereinheitlichung bieten, wie sicher ein einheitliches System ist und welche Trends in diesem Bereich zu erkennen sind. Das Video finden Sie **hier**.

2. **IBWS: Informationen zur Sicherheitslage vom 02.03.2017**
   IBWS analysiert in dieser Ausgabe einen Text, der von den „Anarchist_innen“ am 18.02.2017 anlässlich des Europäischen Polizeikongresses veröffentlicht wurde und in dem auch eine Reihe von Unternehmen namentlich genannt werden. Die gesamte Analyse finden Sie im Anhang dieses Newsletters.

SICHERHEITSVORFÄLLE

1. **Dutzende Tote bei Angriff auf Sicherheitskräfte**
   Bei einem Angriff auf zwei Standorte der Sicherheitskräfte in der syrischen Stadt Homs sind nach Angaben von Beobachtern mindestens 42 Menschen ums Leben gekommen. Unter den Toten sei auch ein hochrangiger Offizier, teilte die in Großbritannien ansässige Beobachtungsstelle für Menschenrechte am Samstag mit. Das staatliche syrische Fernsehen berichtete, es habe in den Distrikten Al-Ghuta und Al-Mohata Gefechte gegeben, bevor sich Selbstmordattentäter bei den beiden Standorten in die Luft gesprengt hätten.
   (handelsblatt) Weiterlesen

2. **Fraunhofer warnt vor Lücken in Android-Passwortmanagern**
   In verschiedenen Passwortmanagern gibt es “gravierende Sicherheitslücken”. Das Teil das Fraunhofer-Institut für Sichere Informationstechnologie (Fraunhofer SIT) mit. die Sicherheitsexperten warnen ausdrücklich vor Lecks unter anderem in LastPass, Dashlane, Keeper und 1Password. Im Anschluss an die Untersuchung durch die Fraunhofer-Experten haben die Hersteller die Lecks mittlerweile beseitigt. Nun sollten Anwender dringend auf die aktuellste Version upgraden, raten die Experten von Fraunhofer SIT.
   (silicon) Weiterlesen

3. **Mord an Kim Jong Nam - Ermittler finden starkes Nervengas an Leiche**
   Auf dem Gesicht Kim Jong Nams seien Rückstände des auch als Chemiewaffe geächteten Gases entdeckt worden, teilten die Ermittler mit. Der Stoff sei in entnommenen Gewebeproben von Gesicht und Augen des Toten enthalten gewesen. Die Untersuchung "weiterer Beweisstücke" laufe noch, sagte Polizeichef Khalid Abu Bakar.
   (focus) Weiterlesen

4. **Bundestagsnetzwerk stundenlang lahmgelegt**
   Die Internet-Server des Bundestages sind erneut stundenlang lahmgelegt gewesen. Wie die Zeitung "Die Welt" auf ihrer Website berichtete, konnten in den Abgeordnetenbüros seit etwa 15.30 Uhr keine Mails mehr empfangen oder von dort aus gesendet werden. Bundestagsmitarbeiter bestätigten die Störungen im Mail-System. Sie wichen zum Teil auf private Mail-Konten aus.
   (ntv) Weiterlesen

5. **Islamisten Al-Kaida bestätigt Tod von Vize-Chef Al-Masri**
   Der Al-Kaida-Anführer Abu Chair al-Masri ist bei einem Luftangriff der US-geführten Militärallianz in Syrien getötet worden. Zwei Al-Kaida-Ableger bestätigten den Tod der mutmaßlichen Nummer zwei des Terrornetzwerks. Berichten zufolge war der 59-jährige Schwiegersohn des getöteten Al-Kaida-Gründers Osama bin Laden am Sonntag nahe der Stadt Idlib getötet worden. Auch im Jemen bombardierten US-Kampfflugzeuge am Donnerstag mehrere Stellungen der Extremistengruppe.
   (stern) Weiterlesen

6. **Bluetooth-Skimming an der Supermarktkasse**
   Mit Teilen aus einem alten Smartphone und einem echt aussehenden Gehäuse ist es Fälschern in den USA offenbar gelungen, Daten von Kartenzahlungen abzugreifen. Es gibt ein paar Hinweise, wie Kunden gefälschte Terminals erkennen können. Die Kriminellen nutzen dabei einen kompletten, authentisch aussehenden Nachbau der Oberseite des Gerätes, der über das eigentliche Terminal gestülpt wird.
   (golem) Weiterlesen

SICHERHEITSPOLITIK

1. **Migrationssteuerung im südlichen Mittelmeerraum verzeichnet weitere Erfolge**
   Federica Mogherini, die Hohe Vertreterin der EU für Außen- und Sicherheitspolitik, und die EU-Kommission haben heute (Donnerstag) über weitere Fortschritte beim Migrationspartnerschaftsrahmen mit afrikanischen Staaten informiert. Außerdem legten sie erste Schritte zur Durchführung von Maßnahmen entlang der zentralen Mittelmeerroute fest.
   (aktiencheck) Weiterlesen

2. **Gabriel: Zwei-Prozent-Ziel der Nato «völlig unrealistisch»**
   Im Streit um höhere Investitionen in das Militär hat sich Außenminister Sigmar Gabriel (SPD) erneut vom Rüstungsziel der Nato distanziert. Sicherheit könne in dieser Welt nicht allein durch zusätzliche Verteidigungsausgaben gewährleistet werden, sagte der Vizekanzler in Estland. Die Nato-Mitgliedstaaten hatten sich 2014 in Wales darauf verständigt, ihre Verteidigungsausgaben binnen zehn Jahren auf zwei Prozent des Bruttoinlandsprodukts zu steigern.
   (stern) Weiterlesen

3. **Herrmann (CSU) weist Schulz-Kritik an Sicherheitspolitik scharf zurück**
   Der bayerische Innenminister Joachim Herrmann (CSU) hat die Kritik von SPD-Kanzlerkandidat Martin Schulz an der Sicherheitspolitik der Union scharf zurückgewiesen. "Seit Jahren vernachlässigen die SPD und ihre grünen Partner in den Bundesländern den Aufbau starker und effizienter Polizei-Sicherheitsstrukturen", sagte der CSU-Politiker dem "Tagesspiegel" (Mittwochausgabe). "Szenen wie in der Kölner Silvester-Nacht sind hausgemachte Probleme eines rot-grün regierten Bundeslandes."
   (tagesspiegel) Weiterlesen

4. **Trump kündigt nukleare Aufrüstung an – „Wollen an die Spitze“**
   S-Präsident Donald Trump will das Atomwaffenarsenal der USA ausbauen. Die USA seien hier zurückgefallen und müssten wieder „an die Spitze“ (Wortwörtlich Make us „Top of the pack“) kommen, sagte Trump am Donnerstag in einem Interview mit der Nachrichtenagentur Reuters. Im Jahr 2016 hatten die USA laut dem Jahrbuch des “Stockholmer internationales Friedensforschungsinstitut“ mit 7000 Sprengköpfen 290 weniger als Russland.
   (welt) Weiterlesen

5. **„Briten müssen mindestens 50 Milliarden Euro zahlen“**
   Auch nach dem Brexit, Großbritanniens angestrebtem Austritt aus der Europäischen Union, muss das Vereinigte Königreich für Europa zahlen. „Wir gehen von mindestens 50 Milliarden Euro aus, die Großbritanni-

en nach einem Austritt aus der EU aufgrund bestehender Verpflichtungen noch zahlen muss“, sagte Günther Oettinger, EU-Kommissar für Haushalt und Personal, am Mittwochabend in Hamburg.
(welt) Weiterlesen

6. **BSI legt Grundstein für Prüfungen gemäß IT-Sicherheitsgesetz**
Die Umsetzung des IT-Sicherheitsgesetzes (IT-SiG) läuft an: Betreiber kritischer Infrastruktur (KRITIS) der Sektoren Energie, IT+TK, Ernährung und Wasser müssen die ersten Prüfungsnachweise bereits zum 3. Mai 2018 beim Bundesamt für Sicherheit in der Informationstechnik (BSI) einreichen. In einem "Multiplikatoren-Workshop" Mitte Februar hat das BSI die Schulungsinhalte und -konzepte festgelegt, nach denen Prüfer fortgebildet werden sollen.
(heise) Weiterlesen

ANDERE SICHERHEITSTHEMEN

1. **Neuer Reisepass lässt sich per Handy auslesen**
Die deutschen Reisepässe lassen sich künftig auch über Mobilfunkgeräte auslesen. Die seit dem 1. März 2017 ausgegebenen neuen Pässe enthielten eine neue Chipkarte, die nicht nur über die sogenannte maschinenlesbare Zone (MRZ) ausgelesen werden könne, teilte das Bundesinnenministerium auf Anfrage von Golem.de mit und bestätigte damit einen Bericht von Heise.de. Dazu enthält der neue Reisepass ebenso wie bereits die Personalausweise eine sogenannte Card-Access-Number (CAN).
(golem) Weiterlesen

2. **Cog Systems will das sicherste Smartphone der Welt zeigen**
Das sicherste Smartphone der Welt? Mit diesem Versprechen geht in Barcelona die Firma Cog Systems an den Start. Bei dem Gerät handelt es sich um ein HTC A9 mit einigen Extras - etwa einem Hypervisor und fest verbautem VPN.
(golem) Weiterlesen

3. **SK Telecom stellt Chip für Quantenverschlüsselung vor**
Kommunizieren, ohne dass ein Geheimdienst mitliest: Das südkoreanische Unternehmen SK Telecom hat einen Chip vorgestellt, der das ermöglichen soll. Er ist nur wenige Millimeter groß. Vorgestellt wurde der Chip auf dem Mobile World Congress (MWC) in Barcelona.
(golem) Weiterlesen

HINTERGRUNDBERICHT

NSA-Report: eine systematische Analyse zum Schutz der Deutschen Wirtschaft

Das Cybersicherheitsteam der Corporate Trust hat in den vergangenen Monaten die Snowden-Dokumente, Wikileaks-Informationen und weitere Open-Source-Quellen gesichtet und analysiert. Dasselbe Team arbeitete zeitgleich an der IT-forensischen Aufklärung von zahlreichen Fällen von Datenspionage und Informationsabfluss in deutschen Unternehmen. Das Ergebnis ist ein umfassender Report der erstmalig die Aktivitäten der NSA nicht vor einem gesellschaftspolitischen Hintergrund, sondern im Hinblick auf die ökonomischen Interessen der deutschen Wirtschaft beleuchtet.

Die wichtigsten Ergebnisse in Kürze:

- Die Amerikaner geben mehr als 0,3% ihres Bruttoinlandsprodukts für die NSA aus. Die amerikanischen Ausgaben für die staatlichen Cybereinheiten wirken wie ein Konjunkturprogramm für Cyber-Sicherheit. Es gibt international operierende deutsche Konzerne die Ihre Sicherheitsabteilungen in den USA ansiedeln, weil man dort einfacher IT-Sicherheitsexperten rekrutieren kann.
- Betrachtet man die 90 größten Internetknoten und die 360 wichtigsten Unterseekabeln, dann kann die NSA wohl mehr als 90% dieser Internet-Kapazitäten überwachen. Selbst in Russland oder China gibt es größere Installationen von Abhörtechnologie. Auf der Weltkarte mit den Standorten wird klar wie nah die NSA ihrem erklärten Ziel ist: "global network dominance".
- Vor 10 Jahren waren Raumfahrt, Elektro-Optik, Nanotechnologie und energetischen Materialien auf der strategischen Missionsliste der NSA. Die Fallpraxis der Corporate Trust hat dies bestätigt. Heute sind bei geheimdienstlichen Spionageangriffen zusätzlich die Bereiche Biotechnologie, Getriebetechnologien und alternative Antriebe betroffen. Firmen, die solche Produkte entwickeln und produzieren sowie deren Zulieferer und Dienstleister, werden gezielt von ausländischen Diensten ausgeforscht.
- Das Cyberwaffen-Arsenal der NSA ist flexibel einsetzbar und bereits heute brandgefährlich. In der Zukunft werden Cyberwaffen mit Industrie 4.0, selbstfahrenden Autos, computergesteuerten Stromnetzen und dem „Internet of Things“ die Zerstörungskraft von Atomwaffen erreichen. Das lockt Diebe an. Und NSA Cyberwaffen in der Hand von Kriminellen oder anderen Geheimdiensten sind eine noch viel größere Bedrohung für die deutsche Wirtschaft. Erste Fälle gibt es bereits.
- Die NSA (zuständig für Spionage und Cyberabwehr) hat 40.000 Mann, das United States Cyber Command (zuständig für Angriffe) 6.000. Damit die Zusammenarbeit reibungslos funktioniert haben beide Einheiten per Dekret den gleichen Chef. In Deutschland verteilen sich die 1.300 Stellen auf die Cybereinheiten beim BND, das BSI, das Kommando digitale Kräfte bei der Bundeswehr sowie Cybermitarbeiter beim Bundesamt für Verfassungsschutz und den 16 Landesämtern für Verfassungsschutz und demnächst bei der neuen „Zentralen Stelle für Informationstechnik im Sicherheitsbereich“. Dazu kommen noch das Bundeskriminalamt und die 16 Landeskriminalämter und einige Schwerpunktstaatsanwaltschaften. Selbst für Experten ist es schwer, den Durchblick zu behalten, wer in Deutschland für was zuständig ist.
- Das NSA Organigramm zeigt: die Spionageabteilung der NSA (Hauptabteilung S) ist organisiert wie ein Wirtschaftsunternehmen: Es gibt einen Vertrieb (S1), eine Produktion – in diesem Fall das Erstellen von Analysen in Form von „Produktlinien“ (S2) und eine Forschungs- und Entwicklungsabteilung (S3) die ständige verbesserte Methoden zum Sammeln von Daten entwickelt. Dieser effizienten Organisation können derzeit weder die deutschen Sicherheitsbehörden noch die IT-Abteilungen der Industrie etwas entgegensetzen.
- Die NSA versteht sich als Werkzeug der Politik und des Militärs. Dazu gehört die Unterstützung bei Vertragsverhandlungen und internationalen Konferenzen. Kunden sind u.a. US Handelsvertretungen sowie das Finanz-, das Handels- sowie das Energieministerium. Die NSA ist ein sehr mächtiges Werkzeug in den Händen eines Präsidenten der solche Machtoptionen zu nutzen weiß. Deutschland kann da kaum mithalten.

Der komplette Report ist frei downloadbar unter: https://www.corporate-trust.de/de/portfolio-items/nsa-report

Autor: Florian Oelmaier, Corporate Trust www.corporate-trust.de

ISPSW PUBLIKATIONEN

1. **Why Border Controls won't Protect Europe Against Terrorism**

   The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute for research and consultancy. The ISPSW is objective and task oriented, and impartial to party politics. In an ever more complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, that bring major opportunities but also risks, decision makers in enterprises and politics depend more than ever before on the advice of highly qualified experts. ISPSW offers a range of services, including strategic analyses, security consultancy, executive coaching and intercultural competency. ISPSW publications examine a wide range of topics relating to politics, economy, international relations, and security/defence. ISPSW network experts have operated in executive positions, in some cases for decades, and command wide-ranging experience in their respective areas of specialization.
   (ispsw) **Weiterlesen**

ASW Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Neue Schönhauser Straße 20 | 10178 Berlin
Telefon +49 (0)30 200 77 200 | Telefax +49 (0)30 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de