Bundesverband

Newsletter Sicherheitspolitik

KW 49/17, 08.12.2017

Wir wünschen Ihnen einen schönen zweiten Advent!

INFORMATIONEN UNSERER PARTNER

1. **CSTV: "Women in Security" mit Katrin Neumann (Folge 3)**
   Katrin Neumann begleitete als Moderatorin die ASIS Germany e.V. Konferenz 2017. Als "Außenstehende" erläutert sie im Interview ihre Eindrücke von der Sicherheitskonferenz und der Sicherheitsbranche im Allgemeinen und vergleicht die Konferenz mit anderen Veranstaltungen, die sie bereits moderiert hat und die thematisch einen anderen Hintergrund hatten. Dabei geht sie insbesondere auf die Initiative "Women in Security" ein, die am zweiten Konferenztag ausgiebig diskutiert wurde. Das Video finden Sie **hier**.

2. **CSTV: SIDW mit Christian Schaaf (Folge 66)**
   Christian Schaaf präsentiert die Eckpunkte des Future Reports, in dem aktuelle Trends der Wirtschaft aufgegriffen und die im Zuge dessen entstehenden Sicherheitsrisiken analysiert werden. Für eine präzisere Analyse der auf uns zukommenden Herausforderungen wurden auch reale Schäden der letzten Jahre betrachtet. Das Video finden Sie **hier**.

3. **CSTV: Event Summary - OSPAs 2017 in Germany**
   Am 9. November 2017 fanden die dritten Outstanding Security Performence Awards, kurz OSPAs, in Berlin statt. Corporate Security TV zeigt Ihnen einige Bilder von der Preisverleihung, auf der Sicherheitsakteure aus Deutschland für ihre herausragenden Leistungen in zehn unterschiedlichen Kategorien ausgezeichnet werden. Das Video finden Sie **hier**.

4. **SIDBB: Wechsel im Vorstand des Vereins Sichere Identität Berlin-Brandenburg e.V.**
   Die Mitgliederversammlung des Vereins Sichere Identität Berlin-Brandenburg e.V. (SIDBB) hat gestern seinen neuen Vorstand gewählt. Der neue Vorstand setzt sich zusammen aus Arno Fiedler, Geschäftsführer der Nimbus Technologieberatung GmbH, Dr. Matthias Flügge, Leiter Geschäftsbereich Digital Public Services am

ASW Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Neue Schönhauser Straße 20 | 10178 Berlin
Telefon +49 (0)30 246 37 175 | Telefax +49 (0)30 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de

Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS und Antonia Maas, Bereichsleiterin Communications & Public Affairs der Bundesdruckerei GmbH. Antonia Maas folgt auf Ulrich Hamann, der seit der Gründung des SIDBB e.V. den Vorstandsvorsitz innehatte und nun in den Ruhestand wechselt. Ebenso folgt Dr. Matthias Flügge auf Gerd Schürmann, der seit 2012 zweiter stellvertretender Vorsitzender des SIDBB e.V. war und nun auch in den Ruhestand wechselt.

SICHERHEITSVORFÄLLE

1. **Malwarebytes: Crypto-Miner versteckt sich hinter Windows-Taskbar**
   Malwarebytes macht auf einen neuen browserbasierten Crypto-Miner aufmerksam, der Techniken von unerwünschter Online-Werbung übernimmt, um unbemerkt PC-Ressourcen für das Mining von Kryptowährungen zu missbrauchen. Die JavaScript-basierte Coinhive-Variante öffnet ein sogenanntes Pop-under-Fenster, das hinter der Windows Taskleiste platziert wird, um unentdeckt zu bleiben.
   (silicon) Weiterlesen

2. **Viele Mail-Programme anfällig für neue Spam-Tricks**
   Eines der zentralen Probleme von E-Mail ist, dass deren Absenderadressen nicht wirklich vertrauenswürdig sind, sondern sich sogar recht leicht fälschen lassen. Mit Hilfe von Anti-Spam-Techniken wie DMARC (DKIM/SPF) können Mail-Server solche Tricksereien jedoch mittlerweile oft entlarven und die Mails als Spam erkennen oder gleich ganz abweisen. Durch zusätzliche Tricks könnten Spammer das jedoch umgehen, demonstriert der Sicherheitsforscher Sabri Haddouche und nennt das ganze Mailsploit (angelehnt an den Exploit, der eine Sicherheitslücke ausnutzt).
   (heise) Weiterlesen

3. **Paypal: Datenleck bei TIO Networks betrifft 1,6 Millionen Kunden**
   Paypal hat bekanntgegeben, dass circa 1,6 Millionen Kunden von einem Datenleck bei TIO Networks (TIO) betroffen sein könnten. Bereits am 10. November hatte Paypal die Angebote von TIO eingestellt, um Nutzerdaten zu schützen. Zu den gestohlenen Daten zählen die persönlichen Informationen von Kunden, inklusive Bankdaten und Sozialversicherungsnummern. TIO fordert seine Kunden dazu auf, einen Service zum Schutz ihrer Identität in Anspruch zu nehmen und bietet Betroffenen ein kostenloses Credit Monitoring für das nächste Jahr an. Wer genau hinter dem Angriff steckt und wann TIO den Betrieb wieder aufnehmen kann, ist noch unklar.
   (heise) Weiterlesen

4. **Neue Version das Banking-Trojaners Ursnif entdeckt**
   Cyberkriminelle testen derzeit eine neue Version das Banking-Trojaners Ursnif. Die zur Gozi-Familie gehörende Malware nutzt nun Weiterleitungsangriffe, um Anmelde- und Bankdaten zu stehlen. Dabei soll sie Nutzern von Online-Banking sehr erfolgreich vorgaukeln, sie befänden sich weiterhin auf der Website ihres Geldinstituts, obwohl sie bereits ihre Daten an die Hintermänner von Ursnif übergeben.
   (silicon) Weiterlesen

5. **Ermittler decken riesiges Netzwerk für Phishing und Betrug auf**
   Ermittler aus Niedersachsen haben gemeinsam mit der US-Bundespolizei FBI ein globales Botnetz ausgeschaltet. Darüber war die Schadsoftware "Andromeda" verbreitet worden, die weltweit Computer ausspähte, wie es in einer Mitteilung der Polizei Lüneburg und der Staatsanwaltschaft Verden heißt. Auch die EU-Polizeibehörde Europol und Ermittler aus 25 weiteren Ländern waren beteiligt.
   (zeit) Weiterlesen

6. **Daten von Millionen Smartphone-Nutzern lagen offen im Netz**
   "Achtung", warnt das Handy-Betriebssystem nach der Installation der App "Ai.Type". Die virtuelle Tastatur könne "alle von Ihnen eingegebenen Texte, einschließlich persönlicher Daten wie Passwörter und Kreditkartennummern, sammeln." Genau das ist bei vielen Tastatur-Apps von Drittanbietern üblich - und gefährlich.
   (spiegel-online) Weiterlesen

7. **Neue Cyber-Mafia zielt auf Unternehmen**
   Seit 2015 ist die Zahl der Angriffe mit Ransomware um den Faktor 2000 gestiegen. Doch das scheint noch nicht das größte Problem zu sein. Sicherheitsexperten sprechen inzwischen von einem neuen Zeitalter des Cyberverbrechens. Denn die Kriminellen gehen immer professioneller und immer besser organisiert. Tatsächlich treten offenbar immer mehr Parallelen zwischen der Hochzeit der Mafia in den 30gern zu Tage.
   (silicon) Weiterlesen

8. **Cyberbit: Spyware aus Israel gegen äthiopische Oppositionelle eingesetzt**
   Aktivisten in Nordamerika und Europa sind das Ziel ausgeklügelter Spyware geworden, die aus Israel stammt und offenbar von Äthiopien gekauft wurde. Zu diesem Schluss kommen die Überwachungs-Analysten des Citizen Lab, die von einem Betroffenen auf die Kampagne aufmerksam gemacht wurden. Bei der anschließenden Untersuchung haben sie dann nach eigenen Angaben eine öffentlich zugängliche Log-Datei gefunden, über die sie nicht nur die Zielpersonen sondern auch die Überwacher selbst aufspüren konnten. Demnach stammt die Software von der israelischen Firma Cyberbit, die bei der Auswahl ihrer Kunden damit wohl ebenso wenig zimperlich ist, wie die NSO Group, das Hacking Team und die Gamma Group.
   (heise) Weiterlesen

9. **Trojaner Quant nimmt Kryptowährungen ins Visier**
   Forscher von Forcepoint Security Labs haben eine neue Variante des Trojaners Quant entdeckt. Ein vor kurzem veröffentlichtes Update soll die Malware um einige “beunruhigende” Funktion erweitern. Unter anderem soll sie nun in der Lage sein, die Anmeldedaten für Online-Geldbörsen von Kryptowährungen auszuspähen, um die darin enthaltenen Bitcoins zu stehlen.
   (silicon) Weiterlesen

10. **Ganz und gar nicht sicher: Immer mehr Phishing-Webseiten setzen auf HTTPS**
    Verglichen mit 2016 setzen dieses Jahr acht Mal mehr Phishing-Webseiten die Transportverschlüsselung HTTPS ein, berichten Sicherheitsforscher von Phishlabs. Damit wollen Betrüger Vertrauen wecken, um so noch mehr Opfer erfolgreich abzuzocken.
    (heise) Weiterlesen

SICHERHEITSPOLITIK

1. **Jerusalem verschärft Sicherheitsvorkehrungen zum Freitagsgebet**
   Jerusalem bereitet sich auf einen Tag mit Auseinandersetzungen vor. Zehntausende Muslime werden zum Freitagsgebet auf dem Tempelberg in der Altstadt erwartet. Nach den Auseinandersetzungen im Westjordanland am Donnerstag werden auch in Jerusalem Zusammenstöße erwartet. Palästinensergruppen hatten nach der Entscheidung von US-Präsident Donald Trump, Jerusalem als Israels Hauptstadt anzuerkennen, "Tage des Zorns" ausgerufen. Die radikalislamistische Hamas hatte sogar eine neue Intifada angekündigt.
   (sueddeutsche) Weiterlesen

2. **Spionagevorwürfe: Bundesanwaltschaft stellt Ermittlungen gegen Ditib-Imame ein**
   Die Bundesanwaltschaft hat ihre Spionageermittlungen gegen mehrere Imame eingestellt. Im Zentrum der Untersuchungen standen Geistliche, die in Moscheen des Dachverbands der türkischen Moscheegemeinden, Ditib, tätig waren.
   (sueddeutsche) Weiterlesen

3. **Grenzverletzung: China meldet Absturz von indischer Drohne**
   Eine indische Drohne ist nach offiziellen Angaben in Chinas Luftraum eingedrungen und abgestürzt. "Indiens Vorgehen hat die territoriale Souveränität Chinas beeinträchtigt, und wir sind sehr unzufrieden damit", zitierte die staatliche Nachrichtenagentur Xinhua einen zuständigen Vizedirektor für Chinas westliche Militärregion. Er sagte, der Vorfall habe sich "kürzlich" ereignet, und fügte hinzu, dass China seine "nationale Souveränität und Sicherheit" verteidigen werde.
   (spiegel-online) Weiterlesen

4. **Großbritannien: Rekord bei Festnahmen wegen Terrorverdachts**
   Noch nie sind so viele Terrorverdächtige in Großbritannien festgenommen worden wie in diesem Jahr. Etwa 400 Personen wurden in zwölf Monaten bis Ende September 2017 festgesetzt, wie das Innenministerium am Donnerstag in London mitteilte. Das sei ein Rekord seit Beginn der Statistiken im Jahr 2001.
   (handelsblatt) Weiterlesen

5. **Atomkonflikt: Nordkorea nennt Krieg unausweichlich**
   Die Militärübungen Südkoreas und der USA sowie die Drohungen des US-Präsidenten mit einem Präventivschlag machen nach Ansicht von Nordkorea einen Krieg unvermeidbar. Es sei eine "feststehende Tatsache", sagte ein Sprecher des nordkoreanischen Außenministeriums. "Die offene Frage ist jetzt: Wann wird der Krieg ausbrechen?" Nordkorea werde sich nicht verstecken, auch wenn das Land eigentlich keinen Krieg wolle.
   (zeit) Weiterlesen

6. **USA haben weit mehr Soldaten in Syrien als bisher bekannt**
   Das US-Verteidigungsministerium hat eingeräumt, dass deutlich mehr amerikanische Soldaten in Syrien im Einsatz sind, als bislang öffentlich kommuniziert wurde. Derzeit seien etwa 2000 US-Soldaten in dem Bürgerkriegsland, sagte Pentagon-Sprecher Robert Manning am Mittwoch in Washington. Bislang hatte das Ministerium die Zahl stets mit etwa 500 angegeben. Im Irak befinden sich nach Angaben Mannings etwa 5200 amerikanische Soldaten.
   (spiegel-online) Weiterlesen

7. **Regierung dementiert umfassende Spionagepläne**
   Das Bundesinnenministerium hat Medienberichte dementiert, wonach Ermittler auf Wunsch der Unions-Innenminister umfassende Möglichkeiten für einen sogenannten Lauschangriff bei Verdächtigen erhalten sollen. Innerhalb der Bundesinnenministerkonferenz werde lediglich diskutiert, das Anbringen von Abhörwanzen innerhalb und außerhalb von Wohnung besser zu ermöglichen, sagte der Sprecher des Bundesinnenministeriums, Johannes Dimroth, auf Anfrage von golem.de. Zu diesem Zweck könnten Hersteller von Alarm- und Sicherheitssystemen gesetzlich verpflichtet werden, mit den Behörden zu kooperieren und beispielsweise Warnhinweise per SMS an die Verdächtigen zu unterdrücken.
   (zeit) Weiterlesen

8. **Frankreich verkauft Kampfflugzeuge an Qatar**
   Das von mehreren Nachbarstaaten boykottierte Qatar hat mit Frankreich ein milliardenschweres Rüstungsgeschäft abgeschlossen. Bei einem Besuch von Frankreichs Präsident Emmanuel Macron in Doha wurden am Donnerstag Verträge etwa zum Kauf von zwölf Rafale-Kampfjets der Firma Dassault sowie 490 gepanzerten Fahrzeuge der Firma Nexter unterzeichnet. Qatar sicherte sich zudem den Kauf weiterer 36 Rafale-Flugzeuge. Zudem will das Scheichtum vom deutsch-französischen Airbus-Konzern 50 Flugzeuge des Typs 321neo kaufen und stellte eine weitere Bestellung von 30 Flugzeugen in Aussicht.
   (faz) Weiterlesen

9. **Berliner Polizei ließ eilige Anfrage zu Amri unbeantwortet**
   Die Berliner Polizei hat offenbar eine dringliche Anfrage aus Nordrhein-Westfalen zum Weihnachtsmarktattentäter Anis Amri unbeantwortet gelassen. Das Auskunftsgesuch erging nur wenige Wochen ehe der Tunesier am Berliner Breitscheidplatz einen Lkw in den Markt steuerte, zwölf Menschen tötete und mehr als 100 verletzte.
   (spiegel-online) Weiterlesen

ANDERE SICHERHEITSTHEMEN

1. **Britische Behörden sollen Antivirus-Software von Kaspersky meiden**
   Britische Regierungsbehörden sollen nach Meinung des britischen Zentrums für Cyber-Sicherheit NCSC (National Cyber Security Centre) keine Anti-Virus-Software der in Moskau beheimateten Firma Kaspersky Lab einsetzen. Das geht aus einem Brief von NCSC-Chef Ciaran Martin an britische Minister hervor, der auf der Webseite des Zentrums veröffentlicht wurde. Zur Begründung hieß es, Russland habe die Absicht, die britische Regierung und entscheidende Infrastruktur des Landes anzugreifen.
   (heise) Weiterlesen

2. **ZDF-Doku „Amazon – Gnadenlos erfolgreich“: Eine Wanze namens Alexa**
   Den Aufstieg des Konzerns nachzeichnen und Missstände anprangern: Daran versucht sich die ZDF-Doku „Amazon – gnadenlos erfolgreich“. Sie ist zwar überladen – dürfte bei Amazon-Kunden jedoch ein mulmiges Gefühl auslösen.
   (handelsblatt) Weiterlesen

3. **YouTube zieht sich von Amazon-Geräten zurück**
   Ein geschäftlicher Streit zwischen YouTube und Amazon zieht zunehmend die Nutzer in Mitleidenschaft. Die Google-Videoplattform zieht ihre App nun auch von Amazons Fernsehbox Fire TV zurück. Außerdem wird die Anwendung auch das Gerät Echo Show verlassen - einen smarten Lautsprecher mit Display, auf den sie gerade erst wieder zurückgekehrt war.
   (spiegel-online) Weiterlesen

4. **Verfassungsschutz hat Lizenz zur Gesichtserkennung**
   Die Abteilung für Verfassungsschutz des Landes Berlin soll technisch deutlich aufgerüstet werden. Bisher verfügte die in die Senatsverwaltung für Inneres integrierte Behörde über kein eigenes Dokumentenmanagementsystem; sie führte nicht einmal elektronische Sachakten. Dies soll mit der laufenden Umsetzung des Berliner E-Government-Gesetzes auch beim Verfassungsschutz aber anders werden: Geplant ist der baldige Aufbau eines entsprechenden Sammelsystems, um nach offiziellen Angaben "sowohl weiterhin die Betriebsbereitschaft gewährleisten als auch alle geltenden rechtlichen Regelungen und Gesetze erfüllen zu können".
   (golem) Weiterlesen

5. **YouTube will härter gegen Gewalt vorgehen**
   Googles Videoplattform YouTube will nach Kritik und politischem Druck gegen Gewalt und Extremismus vorgehen. Unter anderem werde die Zahl der Menschen, die Inhalte prüfen, im kommenden Jahr auf 10.000 erhöht, kündigte YouTube-Chefin Susan Wojcicki an.
   (zeit) Weiterlesen

6. **Bund will Windows 10 über Bundesclient sicher nutzen können**
   Mit dem Einsatz von Microsofts Betriebssystem Windows 10 in der Verwaltung stellen sich angesichts der hochgradigen Vernetzung des Systems zahlreiche Datenschutz- und -Sicherheitsfragen. Derzeit ist es beispielsweise nicht möglich, über Gruppenrichtlinien die Datenströme zwischen dem eigenen Rechner und den Microsoft-Servern vollständig zu kontrollieren, wie das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) feststellte.
   (heise) Weiterlesen

7. **Europäisches Parlament will Mediaplayer VLC sicherer machen**
   Ab sofort gibt es ein Bug-Bounty-Programm für den Mediaplayer VLC. Das Programm ist aber vorerst nicht öffentlich; nur eingeladene Sicherheitsforscher können auf Schwachstellenjagd gehen und dafür Prämien einstreichen. Das Ganze findet auf der Bug-Bounty-Plattform Hackerone statt.
   (heise) Weiterlesen

8. **Kryptowährung soll Venezuelas Wirtschaft retten**
   Im Kampf gegen die Inflation und eine drohende Staatspleite will Venezuelas Staatschef Nicolás Maduro mit einer neuen Digitalwährung die Wende herbeiführen. In seiner TV-Sendung "Domingos con Maduro" kündigte er am Sonntag völlig überraschend die Einführung einer Kryptowährung mit Namen "Petro" an - eine Kurzform für das Wort "Erdöl". Das Land hat die größten Ölreserven der Welt.
   (spiegel-online) Weiterlesen

ASW Bundesverband | Allianz für Sicherheit in der Wirtschaft e.V.
Neue Schönhauser Straße 20 | 10178 Berlin
Telefon +49 (0)30 246 37 175 | Telefax +49 (0)30 200 77 056
info@asw-bundesverband.de | www.asw-bundesverband.de

Meldungen aus der Morgenlage

1. **Neue Studie: Rauchfrei investieren – Warum Banken das tödliche Geschäft mit Tabak beenden sollten**
   Datum: 7 Dezember 2017
   Relevanz: **INVESTMENT**
   Link: http://www.facing-finance.org/de/2017/12/neue-studie-rauchfrei-investieren-warum-banken-das-toedliche-geschaeft-mit-tabak-beenden-sollten/

2. **#TRADELEAKS enthüllen den Mercosur-Deal: die EU akzeptiert laxere Kontrollen von Rindfleisch, wenn Argentinien, Brasilien, Paraguay und Uruguay ihre Zölle für Autos aus der EU absenken. Greenpeace Niederlande veröffentlicht die Geheimpapiere**
   Datum: 6 Dezember 2017
   Relevanz: **POLITIK&RECHT, Globalisierung, International**
   Link: https://twitter.com/greenpeace_de/status/938486963761541121
   https://trade-leaks.org/2017/12/06/greenpeace-netherlands-leaks-eu-mercosur-trade-papers/

3. **Jetzt am #Flughafen #Frankfurt. Demo gegen weitere grausame #Abschiebung nach #Afghanistan #RefugeesWelcome #ProAsyl #Asyl**
   Datum: 6 Dezember 2017
   Relevanz: **POLITIK&RECHT, AKTIVISMUS, Linksextremismus**
   Link: https://twitter.com/ILRheinNeckar/status/938477990090067979
   https://twitter.com/iLfrankfurt/status/938475668265988096

4. **Freunde des Fake-News-Standorts Deutschland**
   Datum: 6 Dezember 2017
   Relevanz: **UMWELT&KLIMA, Protest**
   Link: https://klima-luegendetektor.de/2017/12/06/freunde-des-fake-news-standorts-deutschland/

5. **Many US presidents protect national monuments—Trump wants to destroy them**
   Datum: 5 Dezember 2017
   Relevanz: **POLITIK&RECHT, Regierungen**
   Link: https://twitter.com/Greenpeace/status/938181404806000640
   https://twitter.com/MikeHudema/status/938080323979620352
   https://twitter.com/MartinHeinrich/status/938132311949959174
   https://netzfrauen.org/2017/12/05/54015/

6. **Largest protest mobilisation ever at Adani's rail construction site. We are growing, and will continue to grow until this project is stopped. #StopAdani #BlockadeAdani**
   Datum: 5 Dezember 2017
   Relevanz: **FOSSILE ENERGIE, Energiebranche, Protest**
   Link: https://twitter.com/FLACCoal/status/938159912617570304
   https://twitter.com/FLACCoal/status/938157657420054533
   https://twitter.com/TimBuckleyIEEFA/status/938012092464017409

ISPSW PUBLIKATIONEN

1. **The Changing Dynamics of India-China Relations Post Doklam Standoff**
   The Doklam standoff between India and China appears to have unveiled a new era of India's China policy. Even though the conflict might not have been fully resolved and the probability of recurrence in the near future remains high, a combination of determined posture and astute diplomacy can succeed in protecting India's interests vis-a-vis China's aggressive postures in South Asia and the neighbouhood. The Doklam crisis has been a watershed moment of sorts. Does this standoff mark a turning point in their relationship or will it be a continuation of the status quo? Does it portend a trend of increased belligerence and distrust that could bring the two giants on a collision course? Or will they adopt a more conciliatory approach if such incidents were to reoccur?
   (ispsw) **Weiterlesen**