secorvo
security consulting

Secorvo Security News

Dezember 2016

Bescherung

Jahr für Jahr überrascht uns das Weihnachtsfest – kaum sind die warmen Tage Vergangenheit, müssen wir uns schon über passende Geschenke Gedanken machen. In diesem Jahr liegen die Festtage – wenigstens für Arbeitnehmer – besonders unpraktisch, und in der gefühlten Monatsmitte mahnt bereits der vierte Advent zur Eile.

Um Ihnen ein wenig aus der Verlegenheit zu helfen, haben wir Ihnen in dieser Weihnachtsausgabe der Security News einige aktuelle Geschenkempfehlungen zusammengestellt. Da sollte für jeden Geschmack und Bedarf etwas dabei sein.

Damit auch Sie nicht zu kurz kommen, wagen wir anlässlich des nahenden Jahresendes sogar einen Blick in die Glaskugel. Das vermeiden wir üblicherweise, um nicht weitere Prognosen in die Welt zu setzen, die niemand braucht – und über die man im Rückblick lächeln müsste, würde man sich die Mühe machen, sie ein oder zwei Jahre später auf ihren Wahrheitsgehalt zu prüfen.

Allerdings waren die Trends in Informationssicherheit und Datenschutz selten so deutlich erkennbar. So haben uns die erfolgreichen Ransomware-Angriffe sehr anschaulich demonstriert, dass saubere Backup-Prozesse und systematische Berechtigungsvergaben wichtiger sind als aktuelle Virenscanner. Nicht im Perimeter-Schutz liegt die Zukunft der Informationssicherheit, sondern in systematischen Risikoanalysen, konsequenter Schadensbegrenzung und wirksamen Incident-Response-Konzepten. Wir müssen lernen, mit Angriffen umzugehen, anstatt uns darauf zu konzentrieren, sie zu verhindern. Daher wird die professionelle Organisation der Informationssicherheit – vulgo: ISMS – signifikant an Bedeutung gewinnen.

Eine ähnliche Entwicklung ist im Datenschutz erkennbar. Hier sind jedoch nicht reale Schäden der Antrieb, sondern die (EU-)Gesetzgebung. Zertifikate und eine professionelle Organisation des Datenschutzes sind auch hier die Zukunft – das „DSMS“ lässt grüßen.

Inhalt

secorvo
security consulting

Security News

Für Schnäppchenjäger

Wer den Cent beim Weihnachtseinkauf gerne mehrmals umdreht, sollte einen Blick auf aktuelle Billig-Handys werfen. Trotz des günstigen Preises kommen sie mit kostenloser Zusatzsoftware auf den Gabentisch, die eine vollumfängliche Überwachung und heimliche Software-Updates ermöglicht. Zwar ist dieses Schnäppchen nicht ganz neu (schon 2014 haben Hersteller mit einer ähnlichen kostenlosen Dreingabe Kunden zu begeistern versucht) – aber ohne Zweifel effektvoll. Könnte von einem aufmerksamen Beschenkten allerdings, nicht ganz zu Unrecht, als Danaer-Geschenk verstanden werden.

Für Ungeduldige

Pünktlich zum ersten Advent hat das Bundesministerium des Inneren am 23.11.2016 den deutschen Unternehmen und Datenschützern mit dem neuen BDSG-Entwurf ein verfrühtes Präsent beschert. Angesichts der guten Wirtschaftslage geriet der Entwurf auch nicht knauserig: Er macht nicht nur Datenverarbeitern Geschenke, sondern spendiert ganze 79 Paragraphen – 65% mehr als das noch geltende BDSG. Darin bleiben die bisherige Bestellpflicht für betriebliche Datenschutzbeauftragte, die Regelung des § 32 BDSG für Beschäftigtendaten, der bisherige § 5 BDSG zum Datengeheimnis und die Strafvorschrift des § 44 BDSG erhalten. Die Betroffenenrechte aus Art. 12 ff DS-GVO werden hingegen über Art. 14 Abs. 5 DS-GVO hinaus eingeschränkt.

Allerdings ist auch bei diesem Entwurf fraglich, ob er die Öffnungsklauseln der DS-GVO nicht etwas sehr großzügig auslegt. Auch die zahlreichen Textwiederholungen, inzwischen ausgewiesen und reduziert, sind europarechtlich problematisch. Wer sich für dieses Geschenk entscheidet, sollte mit einem Umtausch rechnen.

Für Tablet-Fans

Kann man sich etwas Exotischeres vorstellen als ein nordkoreanisches High-Tech-Gerät? Nach dem Erfolg des Red Star OS erscheint in diesem Jahr, pünktlich zum Fest, das passende Tablet Woolim auf dem europäischen Markt. Dass das Gerät es in sich hat, werden Niklaus Schiess und Florian Grunow auf dem diesjährigen Hacker-Kongress 33c3 vom 27. bis 30.12.2016 demonstrieren. Der Funktionsumfang geht weit über den herkömmlicher Tablets hinaus: So gewährleistet das Woolim, dass die Beschenkten (und ihre Geheimdienste) nie mehr rätseln müssen, woher geteilte Bilder stammen oder wer subversive Nachrichten verfasst hat. Zur Steigerung des Benutzerkomforts nehmen außerdem intelligente Filtermechanismen dem Anwender die Entscheidung ab, welche Medien er konsumiert oder verbreitet.

Für Vergessliche

Passcodes können schon nervig sein – vor allem, wenn sich die Zeichenfolge nicht so recht im Gedächtnis einprägen will. Wer vergesslichen Zeitgenossen eine Freude machen möchte, der sollte einen Link auf das Youtube-DIY-Video vom 18.11.2016 verschenken. Darin wird gezeigt, wie sich der Passcode jedes iPhones und iPads – von iOS 8 bis iOS 10.2 – dank Siri mit wenigen Schritten umgehen lässt. Post-It-Anbietern könnte diese kleine Freundesgabe glatt das Geschäft vermasseln, sofern Apple nicht schnell Abhilfe schafft.

Für Entwickler

Sicherheitslücken in Software sind das Haupteinfallstor erfolgreicher Angriffe. Da liegt es nahe, befreundete Entwickler an Weihnachten z. B. mit einem Gutschein für ein T.P.S.S.E.-Seminar zu beglücken (siehe unten). Aber es geht auch billiger: So hat Google am 19.12.2016 eine neue Testsuite für Kryptoalgorithmen publiziert. Bisher konnte die Toolsammlung bereits über 40 Bugs in verschiedenen Implementierungen aufdecken.

Für die Jüngsten

Seit dem 06.12.2016 gibt es Produktinnovationen im Spielwarenbereich, die im Zeitalter des Internet of Things unter dem Weihnachtsbaum nicht fehlen dürfen: *My Friend Cayla* und *Hello Barbie* für Mädchen und der coole *i-Que Robot* für Jungs. Um immer die passende Antwort parat zu haben, senden diese smarten Toys die mit dem eingebauten Mikrofon aufgenommene Sprache direkt in die Cloud eines amerikanischen Unternehmens. Man darf sicher davon ausgehen, dass der Vorbehalt in den Nutzungsbedingungen für die Verwendung und Weitergabe der Sprachdaten ausschließlich der Verbesserung des Angebots dient. Bedenken könnten einen vielleicht hinsichtlich des Vokabulars beschleichen – das Unternehmen stammt nämlich aus dem Verteidigungssektor.

Für Fans von Ausgefallenem

Wer etwas Ausgefallenes für seine Liebsten sucht, der sollte auf bewährte Router der Deutschen Telekom zurückgreifen. Am Wochenende des 27.11.2016 fand eine beeindruckende Produktdemonstration statt, bei der fast eine Million Router den Dienst quittierten und die betroffenen Haushalte vom Netz der Telekom und dem Internet

trennten. Zwar hatte die Telekom noch Glück im Unglück, da die Ausfälle lediglich ein Kollateralschaden des eigentlichen Angriffs waren. Aber vielleicht sollte man dem Router unter dem Baum sicherheitshalber doch lieber eine eigene Firewall zur Seite stellen.

Für Scherzhafte

Mit ein wenig Unterhaltung wartet das Landgericht (LG) Hamburg zum Jahresende auf. Am 18.11.2016 hat es – in inhaltlicher Überdehnung eines EuGH-Urteils – eine einstweilige Verfügung wegen eines urheberrechtswidrig verwendeten Fotos auf einer Homepage beschlossen. Nur war in dem seither viel diskutierten Fall nicht der Website-Betreiber Antragsgegner, sondern ein Anbieter, der lediglich auf die Webseite eines Dritten mit diesem Foto verlinkt hat. Das LG Hamburg vertritt nun die Auffassung, dass ein auf eine Webseite verlinkender Anbieter diese zuvor auf die Rechtmäßigkeit ihrer Inhalte prüfen muss – ansonsten nähme er Verstöße bewusst in Kauf oder handele fahrlässig.

Damit hat das Landgericht zahlreichen Website-Anbietern Kopfzerbrechen bereitet. Der Heise-Verlag bat daher das LG Hamburg am 12.12.2016 vor der Verlinkung des Urteils um eine verbindliche Aussage zur Rechtskonformität seiner Website – die zu erklären das LG in einem amüsanten Schriftwechsel ablehnte. Hier eröffnet sich nun eine Vielzahl an Geschenkoptionen – von der Rechtskonformitätserklärung für Verlinkungen auf die eigene Webseite über täglich durchzuführende Prüfschritte bei allen verlinkten Webseiten bis hin zur Abmahnung Dritter wegen Urheberrechtsverstößen auf von jenen verlinkten Seiten.

Für Schneeliebhaber

Passend zum Fest liefern die Ransomware-Schmieden zwei neue Geschenke aus. Die Petya-Variante Goldeneye befreit Personaler von dem Problem unspezifischer Malware-Mails. Um dem Empfänger die Entscheidung (öffnen oder nicht öffnen?) zu erleichtern gibt sich Goldeneye als Bewerbung auf eine tatsächlich ausgeschriebene Stelle des Unternehmens aus. Welcher Personaler würde ein solches Geschenk nicht auspacken?

Eine noch kreativere Verbreitungsvariante hat Popcorn Time auf Lager. Dieser neue Ransomware-Strang stellt die kostenlose Entschlüsselung der eigenen Daten in Aussicht, wenn man seine Freunde infiziert: Entweder zahlt man 1.0 Bitcoin oder man verteilt den Trojaner an mindestens zwei Personen weiter. Wenn schon der Schnee an Weihnachten ausbleibt, sorgt man damit wenigstens für ein hübsches Schneeballsystem.

Secorvo News

T.I.S.P.- und T.P.S.S.E.-Zertifizierung

Schon bald können 1.000 deutsche Informationssicherheitsexperten ihre Kenntnisse und Erfahrungen mit einem T.I.S.P.-Zertifikat belegen. Wenn Sie auch zu diesem wachsenden Kreis von Experten zählen möchten, haben Sie vom **06. bis 10.03.2017** die Gelegenheit, Ihre Kompetenz zertifizieren zu lassen. Das einwöchige T.I.S.P.-Seminar und das Begleitbuch bereiten Sie perfekt auf die Prüfung vor.

Aber auch T.I.S.P.-Absolventen kommen im März auf ihre Kosten: Vom **14. bis 16.03.2017** bietet das Seminar „IT-Sicherheit heute“ die Gelegenheit, Ihre für die Rezertifizierung erforderliche fachliche Weiterbildung nachzuweisen.

Schließlich kommen auch Entwickler und Systemdesigner auf ihre Kosten: Das Seminar T.P.S.S.E. bereitet Sie vom **27. bis 30.03.2017** systematisch auf die Prüfung als zertifizierter Professional für sicheres Software-Engineering vor – hier lernen Sie, wie sich Security by Design in der Praxis umsetzen lässt.

Weitere Seminarangebote und die Möglichkeit zur Anmeldung finden Sie unter www.secorvo.de/seminare.

Wenn der Vorstand zweimal klingelt …

Seit einem guten Jahr gehören auch deutsche Unternehmen zu den Opfern der als „CFO Fraud“ oder „Fake President Fraud“ bekannt gewordenen Social-Engineering-Angriffe. Dabei erhalten gezielt ausgewählte Mitarbeiter mittelständischer oder großer Unternehmen E-Mails und Anrufe, die vermeintlich von der Unternehmensleitung stammen oder von ihr initiiert wurden. Unter der Vortäuschung streng vertraulicher Akquisitionen werden die Mitarbeiter dazu gebracht, große Zahlungen unter Umgehung interner Prozesse auszulösen.

Auf der Jahresauftaktveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) berichten Dr. Boris Hemkemeier und Ronny Wolf von der Commerzbank AG am **02.02.2017** über diese und andere aktuelle Cybercrimeangriffe gegen Unternehmen und zeigen, wie man sich dagegen schützen kann.

Im Anschluss haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ (zur Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Januar 2017	
13.-15.01.	ShmooCon 2017 (The Shmoo Group, Washington/US)
16.-18.01.	Omnisecure 2017 (in TIME berlin, Berlin)
23.-25.01.	AppSec Cali 2017 (OWASP Foundation, Californien, US)
Februar 2017	
02.02.	Wenn der Vorstand zweimal klingelt ... (KA-IT-Si, Karlsruhe)
14.-15.02.	24. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
15.-16.02.	27. Smart Card Workshop (Fraunhofer SIT, Darmstadt)
März 2017	
06.-10.03.	T.I.S.P. (TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
14.-16.03.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
21.-23.03.	DFRWS EU Conference (DFRWS, Überlingen)
27.-30.03.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Kai Jendrian, Michael Knopp, Christoph Schäfer.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de