secorvo
security consulting

Secorvo Security News

Januar 2016

Next Big Thing

Während Experten noch darüber streiten, was genau unter „Industrie 4.0“ zu verstehen ist, rauscht bereits die nächste große „IT-Sau“ auf das Dorf zu: das „Internet of Things“, kurz: IoT. Zwar ist die Idee nicht mehr ganz frisch: Sie basiert auf einem Aufsatz von Mark Weiser aus dem Jahr 1991 und dem „Ubiquitous computing“ – der Erwartung, dass die Miniaturisierung von Computern diese allgegenwärtig machen wird. Im Automobil ist das bereits Realität: Hunderte Steuerungs- und Diagnosesysteme sind darin verbaut. Dank des mit IPv6 ins Unvorstellbare (genauer: auf $3{,}4 \cdot 10^{38}$) vergrößerten Adressbereichs kann nun jedes Staubkorn auf unserem Planeten eine IP-Adresse erhalten – erst recht die immer kompakteren und leistungsfähigeren Miniaturrechner. Ausgestattet mit Sensoren vermessen diese nun unsere Welt: Das Einschalten von Geräten verrät unser Nutzungsverhalten, die Senderwahl im TV unsere Vorlieben, der Kühlschrank erlernt unsere Ernährungsgewohnheiten, die Armbanduhr erhebt unsere Vitaldaten, das Gaspedal erkennt unseren Fahrstil, den der Bordcomputer mit dem Ortsinformationen korreliert.

Damit sind Dienste möglich, die unsere Vorstellungskraft (noch) übersteigen: Nach intensiver Gerätenutzung könnten uns Neugeräte angeboten, das abendliche TV-Programm passgenau zusammengestellt, Nahrungsmittel geliefert, bevor der Vorrat zur Neige geht, Medikamente bei Bedarf automatisch zugestellt, Rasen und Falschparken direkt an die zuständigen Behörden gemeldet, Versicherungsprämien aus dem tatsächlichen Risiko (Zigaretten? Alkohol? Blutdruck? Riskanter Fahrstil?) berechnet und Verhaltensoptimierungen via App empfohlen (und deren Einhaltung überprüft) werden.

Derweil einigten sich die Datenschutzaufsichtsbehörden mit dem VDA am 26.01.2016, dass „... die bei der KfZ-Nutzung anfallenden Daten (...) jedenfalls dann personenbezogen (...) sind, wenn eine Verknüpfung mit (...) dem KfZ-Kennzeichen vorliegt“.

Inhalt

secorvo
security consulting

Security News

Firewalls mit Hintertür

Nachdem kurz vor Weihnachten Netzwerkgeräte von Juniper mit gleich zwei Hintertüren (sowohl im SSH-Zugang als auch im Zufallszahlengenerator für VPN-Verbindungen) für Aufsehen sorgten, zog am 12.01.2016 der bekannte Firewall-Hersteller Fortinet nach. Ein fest kodiertes „Managementpasswort" erlaubte es Angreifern jahrelang, sich per SSH an Fortigate-Firewalls anzumelden. Die Schwachstellen sind zwar behoben, ein ungutes Gefühl in der Magengegend bleibt jedoch. Beide Fälle zeigen, dass Netzwerkgeräte und Appliances kein uneingeschränktes Vertrauen verdienen.

Bei Penetrationstests entdecken wir in Netzwerkgeräten häufig vom Internet erreichbare Management-Zugänge wie SSH oder Web-Schnittstellen. Begründet wird der Zugang oft damit, dass so eine schnelle Remote-Fehlerbehebung ermöglicht werden solle – schließlich würden sichere Passwörter, Anmeldemechanismen und Protokolle eingesetzt. Die entdeckten Hintertüren sollten Anlass sein, solche Zugänge auf den Prüfstand zu stellen.

Abmahnrecht für Verbände

Bislang konnten Datenschutz-Verstöße in erster Linie von Betroffenen abgemahnt werden. Teilweise wurde dieses Recht auch Mitbewerbern zugesprochen. Mit dem am 17.12.2015 beschlossenen „Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts" kommen registrierte Verbände hinzu. Das UKlaG und das BGB werden angepasst.

Künftig können beispielsweise Verbraucherschutzzentralen per Unterlassungsklage gegen Unternehmen vorgehen, die aus ihrer Sicht Datenschutzverstöße mit Verbraucherbezug begehen. Während die meisten Datenschutz-Aufsichtsbehörden eher auf Einsicht von Unternehmen setzen, dürften Verbände weniger Beißhemmungen und vor allem mehr (personelle) Kapazitäten haben.

Besonders Betreiber von Web-Shops dürften die Auswirkungen spüren. Bisher konnten fehlende oder falsche Klauseln in AGB und Datenschutzerklärungen abgemahnt werden; nun kommen tatsächliche Datenverarbeitungen hinzu. Die Verbände werden sich Vorgänge wie Bonitätsprüfungen oder Retargeting vermutlich sehr genau anschauen. Unternehmen sollten das Gesetz zum Anlass nehmen, ihre Web-Shop-Prozesse von ihrem betrieblichen Datenschutzbeauftragten überprüfen zu lassen.

OpenSSH-Schwäche

Für das weit verbreitete OpenSSH Projekt begann das neue Jahr am 14.01.2016 mit einer gravierenden Client-Schwachstelle (CVE-2016-0777). Sie ermöglicht es, unter Ausnutzung der (experimentellen) Roaming-Funktionalität mit einem manipulierten Server-Dienst bei einer Authentisierung mit privatem Schlüssel diesen auszulesen. Damit können sich Angreifer, die einen Server übernehmen konnten, die Schlüssel der Administratoren verschaffen. Da letztere oft das gleiche Schlüsselpaar für eine große Anzahl von Servern nutzen, erhalten die Angreifer so die Credentials für alle diese Server.

Gegen derartige Angriffe können sich Nutzer durch das Deaktivieren des Roaming Supports oder durch das Einspielen eines gepatchten SSH-Clients schützen. Eine präventive Maßnahme wäre die Verwendung eines Schlüsselpaars pro Zielsystem oder der Einsatz von Smartcards gewesen.

Wie bei Heartbleed hatte hier eine Schwachstelle in einer praktisch nicht genutzten, experimentellen Funktion gravierende Auswirkungen auf die Sicherheit des gesamten Systems. Vor allem bei derart sicherheitskritischen Werkzeugen sollte man sich auf den Grundsatz besinnen: Weniger ist mehr!

Freunde finden

Der Bundesgerichtshof hat am 14.01.2016 die Funktion „Freunde finden" von Facebook für rechtswidrig erklärt und damit das Berufungsurteil des Kammergerichts Berlin vom 24.01.2014 bestätigt. Facebook verschickte über diese Funktion mittels der aus den Adressbüchern neu registrierter Nutzer ermittelten E-Mail-Adressen automatisch Einladungen zur Registrierung auch an Nicht-Mitglieder des Netzwerks. Der Verbraucherzentrale Bundesverband (VZBV) war 2010 hiergegen vorgegangen. Der BGH hat nun bestätigt, dass darin eine unzulässige, belästigende Werbung i. S. von § 7 Abs. 1 und 2 Nr. 3 UWG sowie eine Täuschung der Nutzer über die Verwendung ihrer Adressbuchdaten gelegen habe. Das Ergebnis der Revision ist wenig überraschend. Die Praxis, Adressbuchdaten ungefragt zu nutzen, hat Facebook inzwischen längst aufgegeben.

Zahlreiche weitere Soziale Netzwerke, z. B. auch Xing, bieten den Nutzern ähnliche Funktionen, um Einladungen an ihre Adressbuchkontakte zu verschicken. Nach den Kriterien des bestätigten Berufungsurteils führt die bloße technische Hilfestellung durch den Netzwerkanbieter jedoch nicht zu unerlaubter Werbung. Offen ist allerdings noch, wie der BGH automatisch generierte Erinnerungen an eine solche Einladung bewertet.

Cross Device Tracking

Dass smarte Software „nach Hause telefoniert“, um ihren Hersteller mit Nutzungsdaten zu versorgen, ist nicht neu. Neu ist, dass besonders smarte Software über Device-Grenzen via Ultraschall miteinander kommuniziert – und so ihr Wissen über das Nutzungsverhalten an PC, Smartphone, Tablet und TV verknüpfen kann. Am 16.10.2015 hatte das Center for Democracy and Technology (CDT) in einem öffentlichen Brief an die US-amerikanische Federal Trade Commission zu diesem seit mindestens Mitte 2014 bekannten Verfahren Stellung genommen.

Marktführer ist demnach die indische Firma SilverPush, die für das menschliche Ohr nicht wahrnehmbare Tonsequenzen in TV- und Browser-Werbung einblendet, die von einem in bereits mehr als 67 Apps versteckten SDK empfangen und ausgewertet werden können. Angeblich kontrolliert SilverPush auf diese Weise schon mehr als 18 Mio. Smartphones – und erfährt so, wie lange eine Anzeige oder eine TV-Werbung sichtbar ist oder ob sie weggeklickt wird. Offenbar gehören auch Google, Nestle und McDonalds zu den über 150 Kunden von SilverPush, wie Jai Vardhan am 11.11.2015 berichtete.

Tatsächlich entzieht sich diese Art des Trackings jeder technischen Gegenmaßnahme – und ist zudem nicht ohne weiteres feststellbar. Wer sich davor schützen will, dem bleibt nur, das Mikrofon seines Smartphones abzukleben – oder die „Aus“-Taste zu suchen (und zu betätigen).

Secorvo News

Wer druckt, der bleibt

Bei unserem kommenden KA-IT-Si-Event am **02.02.2016** (ausnahmsweise einem **Dienstag**) wird Ihnen Hendrik Herberger (Modox - Modern Documents GmbH) in seinem Vortrag „Übersehen und unterschätzt - Live Hacking von Druckern“ die Gefährdung Ihrer Daten durch moderne Drucker und Kopierer aufzeigen und konkrete Empfehlungen geben, wie sich diese Risiken minimieren lassen.

Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“. Anmeldung unter www.ka-it-si.de.

Das T.I.S.P.-Zertifkat

Am 29.02.2016 startet die erste T.I.S.P.-Schulung 2016. Sie schließt mit der Prüfung zum T.I.S.P.-Zertifikat ab. Die Schulung gibt Ihnen einen umfassenden und themenübergreifenden Überblick über die wichtigsten Gebiete der Informationssicherheit. Vorab erhalten Sie zur Vorbereitung das Begleitbuch „Zentrale Bausteine der Informationssicherheit“. Mehr als 800 IT-Sicherheitsexperten belegen ihre Qualifikation bereits mit dem anerkannten T.I.S.P.-Zertifikat. Termin: **29.02.-04.03.2016** in Karlsruhe. Es gibt nur noch wenige freie Plätze.

Das T.E.S.S.-Zertifikat

System Security Engineering betrachtet die Sicherheit komplexer Systeme. Diese hängt nicht nur von den Sicherheitseigenschaften der beteiligten Komponenten, sondern auch von deren Zusammenwirken und den verwendeten Schnittstellen und Protokollen ab. In der Schulung T.E.S.S. lernen Sie das Zusammenspiel aller Faktoren so zu gestalten, dass das resultierende Gesamtsystem Ihren Sicherheitsanforderungen genügt. Mit dem Erwerb des T.E.S.S.-Zertifikats (TeleTrusT Engineer System Security) dokumentieren Sie Ihre Qualifikation. Termin: **04.-07.04.2016** in Karlsruhe

PKI für Experten

Wer für die Konzeption, den Aufbau oder Betrieb einer PKI zuständig ist, sei unser Praxis-Seminar-Klassiker wärmstens ans Herz gelegt. Fast 300 positive Teilnehmerbewertungen belegen, dass die Expertise und Erfahrung aus 19 Jahren PKI-Praxis ankommt. Termin: **19.-22.04.2016** in Karlsruhe

Detailbeschreibungen unserer Seminarangebote und die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite.

Krypto im Advent

In Zusammenarbeit mit der Pädagogischen Hochschule Karlsruhe realisierten wir den interaktiven Online-Adventskalender „Krypto im Advent“. Mehr als 1.100 Schülerinnen und Schülern der Klassen 3 bis 7 machten sich im Dezember 2015 täglich an die Lösung einer Knobelaufgabe aus der Welt der Kryptologie. Dabei gab es zahlreiche gesponserte Sachpreise zu gewinnen. Aufgrund der großen und begeisterten Resonanz werden wir das Adventsrätsel auch 2016 anbieten. Zum Üben gibt es alle Aufgaben aus dem vergangenen Jahr (und die Lösungen) zum Download.

Veranstaltungshinweise

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

Februar 2016	
02.02.	Wer druckt, der bleibt (KA-IT-Si, Karlsruhe)
09.-10.02.	23. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
17.-18.02.	25. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)>
29.02.-04.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
März 2016	
08.-11.03.	Java Security (Secorvo, Karlsruhe)
21.-24.03.	1st IEEE European Symposium on Security and Privacy (IEEE, Saarbrücken)
29.03.-01.04.	2nd DFRWS EU Conference (DFRWS, Dublin/IE)
April 2016	
04.-07.04.	T.E.S.S. - TeleTrusT Engineer System Security (Secorvo, Karlsruhe)
11.-14.04.	CPSSE - Certified Professional for Secure Software Engineering (Secorvo, Karlsruhe)
19.-22.04.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)

Fundsache

Der Informatiker Carsten Eilers hat am 28.01.2016 ein (kostenfreies) E-Book veröffentlicht, in dem er alle 2015 bekannt gewordenen Router-Schwachstellen zusammengefasst hat. Eine hilfreiche Checkliste.

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

secorvo
security consulting

Secorvo Security News

Februar 2016

Trägheitsprinzip

Das Trägheitsprinzip ist ein zentrales Axiom der Physik *Sir Isaac Newtons* (1642-1726), auch bekannt als das im Jahr 1687 publizierte „Erste Newtonsche Gesetz". Formuliert wurde es bereits im Jahr 1638 von *Galileo Galilei* (1564-1641): Jeder Körper behält seinen Ruhe- oder Bewegungszustand bei, solange keine auf ihn einwirkende Kraft ihn zur Änderung dieses Zustands zwingt.

Wie wir heute wissen, lassen sich mit diesem Prinzip nicht nur die Bewegungen der Himmelskörper erklären, sondern auch das Verhalten von elektromagnetischen Feldern. Verfolgt man aufmerksam die Nachrichten, kann man sich außerdem des Eindrucks nicht erwehren, dass auch das menschliche Verhalten diesem Prinzip gehorcht.

Wie anders ließe es sich auch erklären, dass nach einer Analyse von 35 Millionen Authentifikationsdaten durch das Hasso-Plattner-Institut im Jahr 2015 das meistgenutzte Passwort der Welt „123456" lautet? Dass gut 15 Jahre nach dem I-Love-You-Virus noch immer angeklickte E-Mail-Anhänge das Haupteinfallstor für Schadsoftware sind? Dass auch heute noch Mitarbeiter ihre Rechner am Arbeitsplatz in der Regel ohne Aktivierung einer Zugangssperre verlassen? Dass Mitarbeiter sich mit Händen und Füßen gegen den Entzug von Administratorrechten für ihren lokalen Rechner wehren?

Sicherheit könnte viel einfacher sein – etwas mehr Einsicht bei den „Gurtmuffeln" des 21. Jahrhunderts vorausgesetzt. Derweil üben sich die Verantwortlichen in Selbsttäuschung: Nach dem am 17.11.2015 veröffentlichten „Cyber Security Report" des Instituts für Demoskopie Allensbach (im Auftrag der Deutschen Telekom) halten die befragten Führungskräfte deutscher Unternehmen das Schadensrisiko durch einen Hackerangriff für eher gering (60 %) und sehen ihr Unternehmen „so gut wie möglich vorbereitet" (60 %).

Offenbar müssen wohl auch hier erst externe Kräfte einwirken, damit sich der Zustand ändert.

Inhalt

secorvo
security consulting

Security News

Und Krypto funktioniert doch ...

... zumindest bei aktuellen Erpressungs-Trojanern (*Ransomware*) wie Teslacrypt. Ließen sich von Teslacrypt 2 verschlüsselte Dateien noch mit dem TeslaDecoder wiederherstellen, weil der verwendete AES-Schlüssel rekonstruierbar im Header der Datei versteckt wurde, ist dies bei dem am 12.01.2016 in Umlauf gebrachten Teslacrypt 3 nicht mehr möglich. Auch ältere Erpressungs-Trojaner wie Cryptowall (seit 01.11.2014 bekannt) setzen inzwischen so gute kryptographische Verfahren ein, dass das FBI empfiehlt, die erpresste Summe zu zahlen.

Gegen derartige Angriffe hilft eine Kombination aus technischen und Sensibilisierungs-Maßnahmen für die Benutzer. Werden E-Mail-Anhänge abgefangen oder solche mit Schadsoftware gar nicht erst geöffnet, wird damit die Infektion unterbunden – das ist wirkungsvoller als ein Virenschutz, der neue Varianten der Trojaner ohnehin zunächst nicht erkennt. Um den Schaden einer Infektion zu begrenzen helfen restriktive Berechtigungen, sodass nur wenige (Benutzer-) Dateien und nicht komplette Netzlaufwerke unerwünscht verschlüsselt werden. Und eine angepasste und strikte Backup-Strategie hilft im Fall der Fälle bei der Wiederherstellung der Daten.

Minimierung per Verordnung

Das Bundesinnenministerium hat am 13.01.2016 einen Referentenentwurf der Verordnung (BSI-KritisV) zum am 25.07.2015 in Kraft getretenen IT-Sicherheitsgesetz vorgelegt, der insbesondere näher festlegt, welche Anlagen als kritische Infrastrukturen gelten und damit dem Gesetz unterfallen.

Der Entwurf zählt die Anlagenkategorien aus den Bereichen Energie, Wasserversorgung, Telekommunikation und Ernährung auf und umfasst einen Anhang mit branchenspezifischen Schwellenwerten. Beispielsweise fallen Stromerzeugungsanlagen ab 420 MW installierter Leistung und Serverfarmen mit im Jahresdurchschnitt mindestens 25.000 laufenden Instanzen unter die Regelungen.

Der Aspekt des Gefährdungspotentials für die öffentliche Sicherheit (§ 2 Abs. 10 Nr. 2 BSI-Gesetz) wird dabei vollständig ausgeblendet. Auch die im Gesetzestext enthaltenen Sektoren Gesundheit, Transport und Verkehr oder Finanz- und Versicherungswesen sind (bis Ende 2016) ausgespart. Nach der Begründung sind in Deutschland insgesamt 650 Anlagen betroffen, deren Betreiber jährlich mit einem Aufwand von sieben Vorfallsmeldungen à 660 Euro pro Anlage rechnen müssen. In der Gesetzesbegründung war noch von 2000 Betreibern und einem nicht quantifizierbaren Aufwand für die Maßnahmenumsetzung die Rede. Offenbar ist ein ISMS in Deutschland zurzeit günstig zu haben.

Arbeitnehmerkontrolle

Das Landesarbeitsgericht Berlin-Brandenburg hat am 14.01.2016 entschieden, dass Arbeitgeber die Internetnutzung ihrer Mitarbeiter – auch bei in Pausen ausnahmsweise gestatteter privater Nutzung – ohne Einwilligung der Betroffenen anhand der Browserprotokollierung überprüfen dürfen. Die Protokolle haben zudem Beweiskraft im Streit über eine außerordentliche Kündigung wegen exzessiver Internetnutzung.

Die Datenschutz-Aufsichtsbehörden sehen dies v. a. bei erlaubter Privatnutzung kritischer und haben ihre Einschätzung gerade erst in einer am 30.01. 2016 veröffentlichten Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz dargestellt.

Das Landesarbeitsgericht Berlin-Brandenburg hat bereits im Jahr 2011 vertreten, dass der Arbeitgeber selbst bei erlaubter Privatnutzung nicht zum Telekommunikationsdiensteanbieter wird. Ob dieses jüngste Urteil in ähnlicher Weise rechtliche Streitstände vertieft, wird jedoch erst die Urteilsbegründung verraten.

Transparenz ist Pflicht

Fast jede Webseite verfügt heute über eine Anbieterkennzeichnung gem. § 5 TMG, meist zu finden unter dem Link „Impressum“. Eine korrekte Datenschutzerklärung nach § 13 TMG fällt vielen Seitenbetreibern schon viel schwerer. Dabei hatte das OLG Hamburg bereits im Juli 2013 entschieden, dass fehlende oder fehlerhafte Datenschutzerklärungen einen abmahnfähigen Wettbewerbsverstoß darstellen.

Dieser Entscheidung folgt das LG Köln mit seinem Beschluss vom 26.11.2015 und erließ eine entsprechende einstweilige Verfügung gegen einen Webseitenbetreiber. Unter anderem wurde auf der Seite das Remarketing-Tool Google Adwords eingesetzt. Webseitenbetreiber sollten den Beschluss als Ermahnung nehmen, ihre Datenschutzerklärung auf Aktualität und Vollständigkeit zu überprüfen – oder umgehend eine zu erstellen.

Grünes Licht für Cookie-Opt-out

Das OLG Frankfurt hat am 17.12.2015 entschieden, dass eine Opt-out-Möglichkeit beim Einsatz eines Webanalyse-Dienstes ausreicht. In dem Urteil über die Klage eines Verbraucherschutzverbands ging es um eine Gewinnspiel-Einwilligung, die aufgrund

undifferenzierter Verlinkung auf 59 Kooperationspartner nicht rechtswirksam war.

„Nebenbei" beantwortet das Urteil jedoch die Frage, ob die so genannte Cookie-Richtlinie der EU und deren Vorgabe zur Einwilligung beim Einsatz von Cookies in Deutschland unmittelbar anwendbar ist. Diese Frage ist seit Jahren heiß diskutiert und umstritten. Das OLG hat nun klargestellt, dass die entsprechenden datenschutzrechtlichen Vorschriften keine Einwilligung (in Gestalt eines Opt-in-Verfahrens) vorschreiben. Die Zustimmung gilt als erteilt, wenn der Nutzer einen bereits gesetzten Haken nicht entfernt (Opt-out-Verfahren).

Grenzen der Werbeflut

In seiner Urteilsbegründung zu der bereits am 15.12.2015 ergangenen Entscheidung über Werbung in Eingangsbestätigungs-E-Mails ist der Bundesgerichtshof (BGH) auf die Reichweite der von ihm angenommenen Persönlichkeitsrechtsverletzung eingegangen. Im verhandelten Fall hatte der Kläger auf einen Werbewiderspruch eine automatische Eingangsbestätigungs-E-Mail mit Werbeinhalt erhalten. Der § 7 UWG war in diesem Fall nicht anwendbar, da es sich beim Kläger um einen Verbraucher, nicht um einen Wettbewerber handelte. Ein elektronisches Postfach sei jedoch Teil der Privatsphäre, das allgemeine Persönlichkeitsrecht vermittle das Recht „in Ruhe gelassen zu werden".

Ob das Einwilligungserfordernis aus Art. 13 Abs. 1 der EU-Datenschutzrichtlinie für elektronische Kommunikation bei Verstößen stets zu einem Eingriff in das Persönlichkeitsrecht mit resultierendem Unterlassungsanspruch führt, ließ der BGH jedoch offen. Dies gelte jedenfalls regelmäßig für einen Werbewiderspruch.

Werbezusätze in E-Mails dürfen nach dieser Rechtsprechung nur noch bei Einwilligung oder bei bestehender Geschäftsbeziehung eingesetzt werden – vom E-Mail-Server automatisch angehängte Marketing-Footer können zukünftig teuer werden.

Secorvo News

Call for Paper für die T.I.S.P.-Community

Vom **10. bis 11.11.2016** treffen sich in Frankfurt Absolventen des T.I.S.P.-Zertifikats auf dem „10. T.I.S.P. Community Meeting" zum Erfahrungsaustausch. Von TeleTrusT wurde ein Call for Paper für diese Veranstaltung veröffentlicht: Bis zum 18.04. 2016 können Sie Beitragsvorschläge einreichen.

Das CPSSE-Zertifikat

Werden bei der Entwicklung von Software-Sicherheitsanforderungen systematisch berücksichtigt, dann ist das nicht nur ein wichtiger Schritt zu einer höheren Softwarequalität, sondern auch ein Gewinn für die IT-Sicherheit aller Kunden. Wie das gelingt, zeigt die Schulung zum Certified Professional for Secure Software Engineering (CPSSE) vom **11. bis 14.04.2016** in Karlsruhe. Ein Teilnehmer schrieb uns dazu: „*Secure Software Engineering: alles andere als nur Theorie: Informatives und interaktives Seminar mit einem sehr guten Verhältnis von Theorie und Praxis.*"

PKI für die Praxis

Über 300 PKI-Experten haben sich bisher auf einem unserer PKI-Seminare mit aktuellem Know-how versorgt. Eine Teilnehmerstimme: „*Das gesamte Seminar war beeindruckend strukturiert aufgebaut und umfasste alle wesentlichen Themen wie Grundlagen, Standards und praktische Umsetzung. Unter kompetenter Begleitung durch spezialisierte Dozenten hat mich der abschließende Workshop für die schrittweise Vorgehensweise sensibilisiert […]. Eine wohltuende Atmosphäre um das Seminar […].*" Die nächste PKI-Schulung, die Expertise und Erfahrung aus 20 Jahren aktiver Gestaltung von PKIs bündelt, findet vom **19. bis 22.04.2016** in Karlsruhe statt.

Detaillierte Seminarinhalte, weitere Angebote und die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite.

Dumm. Dümmer. DAU?

In der IT gilt die alte Weisheit, stets den „Dümmsten Anzunehmenden User" (DAU) im Blick zu behalten. Doch was heißt das eigentlich? Und warum verhält sich der DAU so „dumm"? Und was kann man daraus lernen?

In seinem Vortrag „Psychologie der Sicherheit: Ist der DAU wirklich dumm?" beim nächsten KA-IT-Si-Event am **21.04.2016** um 18 Uhr erläutert Christoph Schäfer (Secorvo Security Consulting GmbH), wie Entscheidungsprozesse im menschlichen Gehirn ablaufen und welchen systematischen Fehlern Menschen bei der Entscheidungsfindung unterliegen.

Dabei wird deutlich, welche Bedeutung dem „Faktor Mensch" in der IT-Sicherheit zukommt – und was man daraus lernen sollte. Anschließend haben Sie wie gewohnt die Gelegenheit zum „Buffet-Networking". Anmeldung unter www.ka-it-si.de.

Save the Date: APP #4

Merken Sie sich bereits den 29.04.2016 vor – den Termin unserer vierten Anti-Prism-Party im Karlsruher ZKM.

Veranstaltungshinweise

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

März 2016	
14.-15.03.	9. GDD-Fachtagung „Datenschutz International“ (Gesellschaft für Datenschutz und Datensicherung e.V., Berlin)
21.-24.03.	1st IEEE European Symposium on Security and Privacy (IEEE, Saarbrücken)
April 2016	
04.-07.04.	T.E.S.S. - TeleTrusT Engineer System Security (Secorvo, Karlsruhe)
11.-14.04.	CPSSE - Certified Professional for Secure Software Engineering (Secorvo, Karlsruhe)
19.-22.04.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
21.04.	Dumm. Dümmer. DAU? (KA-IT-Si, Karlsruhe)
27.-28.04.	17. Datenschutzkongress (EUROFORUM, Berlin)
29.04.	Anti-Prism-Party 4. Staffel (KA-IT-Si, Karlsruhe)
Mai 2016	
30.05.-01.06.	IFIP SEC 2016 (IFIP, Hamburg)

Fundsache

Am 28.01.2016 hat der Rat der Europäischen Union die deutschsprachige Fassung der am 15.12.2016 beschlossenen Datenschutz-Grundverordnung veröffentlicht, die die EU-Richtlinie aus dem Jahr 1995 ablöst.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, 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

secorvo
security consulting

Secorvo Security News

März 2016

Rettungsleck

Vor einigen Jahren nahmen wir an einer Wildwasser-Fahrt im Schlauchboot teil. Als mein Blick bei der Einweisung auf die Boote fiel, staunte ich nicht schlecht: im Boden klaffte jeweils ein großes Loch. „Damit das Wasser herauslaufen kann“, erläuterte uns der Bootsführer grinsend. Kaum im Wasser klärte sich das vermeintliche Wunder: Der Auftrieb der Luftkammern hielt das Boot so weit über der Wasseroberfläche, dass das hereinschwappende Wasser tatsächlich durch das Loch ablief – ohne Loch hätte das Boot tief und schwerfällig im Wasser gelegen.

An dieses Erlebnis musste ich am 09.03.2016 denken, als ein Verschlüsselungstrojaner unter Verwendung der Ransomware EDA2 die Runde machte. Dessen Autor Utku Sen hatte eine Entschlüsselungs-Hintertür in EDA2 eingebaut, die eine Rekonstruktion der Schlüssel ermöglichte – etwa 700 Betroffene kamen daher ohne Lösegeldzahlung wieder an ihre unerwünscht verschlüsselten Daten.

Das klingt nach einem guten Argument für das FBI, das derzeit von Apple den Einbau von Entschlüsselungs-Hintertüren in iPhones fordert. Aber wie beim Loch im Wildwasser-Schlauchboot gilt auch hier: Nicht jede Speziallösung eignet sich als generelles Konzept. Denn nachweislich ist ein Loch im Rumpf normalerweise kein wirksamer Sinkschutz.

Ein Verschlüsselungsverfahren ist nur dann ein sicheres Verfahren, wenn es keine Hintertür besitzt. Solche Verschlüsselungsverfahren sind bei einem Ransomware-Angriff zweifellos unerfreulich – sie sind jedoch nicht die Ursache des Problems. Auch die „Klick-nicht-auf-den-Anhang“-Empfehlung nimmt allein den Auslöser ins Visier. Der Schaden von Ransomware ist hingegen meist deshalb so groß, weil die betroffenen Benutzer Schreibrechte auf zu vielen Daten besitzen – und die zugehörigen Backups zu alt sind für eine verlustarme Wiederherstellung. Hier stecken die eigentlichen Hausaufgaben.

Inhalt

secorvo
security consulting

Security News

DROWN-Angriff: ein SSL-Krimi

Der von einer Gruppe von Sicherheitsexperten am 01.03.2016 publizierte jüngste Angriff auf TLS/SSL (DROWN – *Decrypting RSA using Obsolete and Weakened eNcryption*) liest sich wie ein Krimi: Eine Gemengelage aus Crypto War-Relikten, Protokoll-Designfehlern, fehlerhafter Konfiguration und Bugs. Er basiert auf der verbreiteten, aber irrigen Annahme, dass es ungefährlich sei, wenn ein Server das „ausgestorbene" Protokoll SSLv2 nicht deaktiviert. Anfang März 2016 unterstützten allein sechs Millionen HTTPS-Server SSLv2. Anfällig für DROWN sind weitere Millionen Server, die andere SSL-basierte Protokolle nutzen oder mit einem SSLv2 unterstützenden Server das Zertifikat teilen.

DROWN nutzt die schwachen Export-Chiffren von SSLv2 aus den 90er Jahren mit nur 40 bit langen symmetrischen Schlüsseln (RC2 bzw. RC4) für einen *Chosen-Ciphertext*-Angriff, um den Sitzungsschlüssel einer mitgeschnittenen TLS-Verbindung zu berechnen und damit die Daten nachträglich zu entschlüsseln. Kryptographisch basiert DROWN auf dem *Padding Oracle*-Angriff von Daniel Bleichenbacher aus dem Jahr 1989.

Um einen HTTPS-Server vor DROWN zu schützen, reicht das Entfernen der Export-Chiffren in der Serverkonfiguration nicht aus: Es müssen SSLv2 serverseitig deaktiviert und aktuelle TLS/SSL-Bibliotheken (z. B. für OpenSSL) eingespielt werden.

Zum Testen der Verwundbarkeit eines HTTPS-Servers bietet die Webseite „The DROWN Attack" ein Check Tool und eine wunderbare FAQ.

Quadratur des Kreises

Nach erfolgloser Abmahnung hat die Verbraucherzentrale Nordrhein-Westfalen am 29.02.2016 Microsoft vor dem LG München I (AZ. 12 O 909/16) auf Unterlassung verklagt. Grund ist die nach Auffassung der Verbraucherzentrale schwer verständliche und unklare Datenschutzerklärung zu Windows 10, auf deren Grundlage jeder Windows-Nutzer in zahlreiche Datenübertragungen einwilligen soll.

Die Datenschutzerklärung von Microsoft differenziert nach Diensten und verlinkt jeweils auf unterschiedliche Informationsquellen. Dabei ist für den Nutzer kaum zu erkennen, welche Datenkategorien zu welchen Zwecken unter welchen Umständen erhoben und verarbeitet werden. Andererseits handelt es sich bei Windows 10 um ein komplexes System von verschiedensten Diensten und Funktionen; sämtliche hierbei anfallenden Datenerhebungen in einer kurzen, hervorgehobenen Erklärung darzustellen und dabei alle einwilligungsrelevanten Informationen zu vermitteln dürfte der Quadratur des Kreises gleichkommen.

Auch wenn ein gesteigerter Sanktionsdruck bezüglich der Verarbeitungstransparenz wünschenswert ist, so ist in diesem konkreten Fall jedoch auch zu hoffen, dass er nicht zum Auftakt einer Abmahnwelle wird, die auf konfligierenden Gesetzesanforderungen fußt und auch bemühte Anbieter erfasst.

Hackers Contest

Im Rahmen der von TippingPoint im Jahr 2005 gegründeten Zero Day Initiative, die Security-Forscher mit Preisgeldern für gefundene Schwachstellen belohnt, fand am 16. und 17.03.2016 der Pwn2Own-Contest 2016 in Vancouver statt. Dabei lobten HP und Trend Micro hohe Preise für diejenigen aus, denen es gelingen sollte, Systeme über die aktuellen Versionen von Google Chrome, Microsoft Edge, Adobe Flash oder Apple Safari mittels *Zero Day Exploits* zu übernehmen. Die Teilnehmer deckten insgesamt 21 kritische Sicherheitslücken auf – und reisten mit Prämien in Höhe von insgesamt 460.000 $ ab. Allein 145.000 $ strich der erfolgreichste Teilnehmer, der Südkoreaner Jung Hoon Lee ein: Ihm gelang die Übernahme von Google Chrome in weniger als zwei Minuten. Schon im vergangenen Jahr war er als Sieger aus dem Contest hervorgegangen und mit einer Gesamtprämie in Höhe von 225.000 $ zurückgekehrt.

Der Wettbewerb zeigt den Herstellern jährlich die Grenzen ihrer Softwareentwicklung auf – und macht eindrucksvoll deutlich, dass es, allen Anstrengungen zum Trotz, mit deren Qualität noch längst nicht zum Besten bestellt ist.

No-Spy-Klausel

Am 16.03.2016 hat der IT-Planungsrat – das zentrale Gremium zur Koordination der Informationstechnik zwischen Bund und Ländern nach Art. 91c GG – in ihre Standard-Beschaffungsverträge die Zusicherung des Auftragnehmers aufgenommen, dass erworbene Hardware „frei von Funktionen ist, die die Integrität, Vertraulichkeit und Verfügbarkeit der Hardware, anderer Hardware und/oder Software oder von Daten gefährden". Eine entsprechende Formulierung hatte der IT-Planungsrat bereits am 16.07.2015 in die Vertragsbedingungen für die Beschaffung und Pflege von Standardsoftware aufgenommen.

Ein wichtiger Schritt um Softwarehersteller dazu zu bewegen, Sicherheitsaspekten eine höhere Priorität einzuräumen.

Datenschutz via Kartellrecht

Am 02.03.2016 teilte das Bundeskartellamt mit, dass ein Verfahren gegen Facebook Inc., Facebook Ltd. und Facebook Germany GmbH wegen „Konditionenmissbrauchs" eingeleitet wurde: Es bestehe ein Anfangsverdacht, dass Facebook seine marktbeherrschende Stellung auf dem Gebiet der sozialen Netzwerke zur Durchsetzung rechtswidriger Datenschutzklauseln verwendet. Anlass ist die Einwilligung in die Datenverarbeitung bei der Nutzerregistrierung, die sich auf die als Fragenkatalog gestalteten Datenschutzrichtlinien bezieht. Darin wird nur sehr ungenau beschrieben, welche Daten in welchem Umfang verarbeitet und an Dritte weitergegeben werden.

Das Kartellamt kann nach eigener Auffassung selbständig datenschutzrechtliche Verstöße feststellen und Anordnungen zur Beseitigung oder Bußgelder von bis zu 10% des Jahresumsatzes verhängen.

Ob es tatsächlich zu einem Bußgeld kommt und dieses auch einen anschließenden Rechtsstreit übersteht, ist noch eine offene Frage. Im Erfolgsfall ist der Ansatz jedoch angesichts der Sanktionsmöglichkeiten des Kartellamtes (§ 32 ff GWB) ein starkes Druckmittel, Transparenz und die Einhaltung von Datenschutzgrenzen bei großen, internationalen Anbietern zu erzwingen. Voraussetzung dafür ist jedoch eine sorgfältige Marktdefinition, um deren marktbeherrschende Stellung bei bestimmten Angeboten nachzuweisen.

Secorvo News

CfP T.I.S.P. Community Meeting

In Frankfurt treffen sich vom **10. bis 11.11.2016** 150 IT-Sicherheitsexperten der deutschen Wirtschaft zum Erfahrungsaustausch beim 10. *T.I.S.P. Community Meeting*. Noch bis zum 18.04.2016 können Vortragsvorschläge eingereicht werden.

PKI für Praktiker

Unsere PKI-Schulung vom **19. bis 22.04.2016** bündelt die Expertise und Erfahrung aus 19 Jahren aktiver Gestaltung von Public Key-Infrastrukturen. Hier die Einschätzung eines der über 300 Teilnehmer: „*Das PKI-Seminar bei Secorvo hat mir durch seine thematische Breite bei gleichzeitig gut durchdachter Struktur alle notwendigen Kenntnisse und Werkzeuge an die Hand gegeben, die mich in die Lage versetzen, auch künftigen PKI-Anforderungen unserer Organisation zu begegnen.*" Wir freuen uns, Sie auf dem Seminar zu begrüßen (Anmeldung).

CPSSE-Zertifikat

Auf unserer Schulung zum Certified Professional for Secure Software Engineering (CPSSE) vom **11. bis 14.04.2016** in Karlsruhe lernen Sie, wie Sie bereits bei der Code-Entwicklung Schwachstellen gezielt vermeiden. Dazu eine Teilnehmerstimme: „*Ich kann das Seminar nur weiterempfehlen. Hervorheben möchte ich neben der Kompetenz der Vortragenden die angenehme und inspirierende Atmosphäre und die dadurch ermöglichten Diskussionen, die wesentlich zum Verständnis der Problematik beitragen und motivieren, sich weiter mit dem Thema auseinanderzusetzen.*" Wir freuen uns auf Ihre Anmeldung.

T.I.S.P.-Zertifikat

Vom **06. bis 10.06.2016** gibt Ihnen die Schulung zum T.I.S.P. einen umfassenden und themenübergreifenden Überblick über die aktuell wichtigsten Gebiete der Informationssicherheit. Mit der anschließenden Prüfung können Sie das anerkannte T.I.S.P.-Zertifikat erwerben und damit Ihr Expertenwissen dokumentieren.

Anti-Prism-Party #4

Zum Abschluss der Ausstellung „Global Control and Censorship" des ZKM | Karlsruhe lädt die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) zusammen mit dem Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL) und dem CyberForum e.V. am **Freitag, 29.04.2016 ab 16 Uhr** zur 4. Staffel der Anti-Prism-Party (Eintritt frei).

Dort zeigen Experten, wie Sie sich vor Ausspähung im Internet schützen können. Es gibt Live-Vorführungen zu den Themen „Sicheres Surfen", „Sicher kommunizieren" und „Sichere Kommunikation im Karlsruher Public WLAN". Vertiefte IT-Kenntnisse sind nicht erforderlich, um den anschaulichen Vorführungen folgen zu können. Sie können sich von Experten individuell beraten lassen und die Erläuterungen im Workshop „E-Mail-Verschlüsselung" direkt am eigenen Laptop umsetzen. Derweil werden Ihre Kinder in der Spion-Schule von der Pädagogischen Hochschule Karlsruhe zu Verschlüsselungsexperten ausgebildet.

Um 18:30 Uhr schließt die Veranstaltung mit einem offenen Diskussionsforum unter Mitwirkung des Datenschutz-Aktivisten Malte Spitz. Nähere Informationen und das Programm zur 4. Staffel der Karlsruher Anti-Prism-Party finden Sie auf der Webseite www.anti-prism-party.de.

Veranstaltungshinweise

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

April 2016	
04.-07.04.	T.E.S.S. - TeleTrusT Engineer System Security (Secorvo, Karlsruhe)
05.04.	Security Sells (CyberForum, Karlsruhe)
11.-14.04.	CPSSE - Certified Professional for Secure Software Engineering (Secorvo, Karlsruhe)
19.-22.04.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
21.04.	Dumm. Dümmer. DAU? (KA-IT-Si, Karlsruhe)
27.-28.04.	17. Datenschutzkongress (EUROFORUM, Berlin)
29.04.	Anti-Prism-Party 4. Staffel (KA-IT-Si, Karlsruhe)
Mai 2016	
30.05.-01.06.	IFIP SEC 2016 (IFIP, Hamburg)
Juni 2016	
06.-10.06.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
13.-14.06.	DuD 2016 (Computas, Berlin)
22.06.	8. Tag der IT-Sicherheit (KA-IT-Si, Karlsruhe)

Fundsache

Das Nationale IT-Lagezentrum des BSI hat angesichts der zunehmenden Verbreitung von Ransomware am 11.03.2016 ein Dokument mit Empfehlungen zur Prävention und Reaktion herausgegeben. Inhaltlich wenig Überraschendes, aber eine gute Zusammenfassung.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Dr. Yun Ding, Michael Knopp.

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

secorvo
security consulting

Secorvo Security News

April 2016

Time is money

Die ungebremste Beschleunigung unserer Arbeitswelt, die inzwischen sogar unser Privatleben vereinnahmt, beklagen wir nicht erst seit der Verbreitung des Smartphones (nanu, da ist ja ein „Aus"-Knopf?!). Sie erfasst nun auch die dunkle Seite des Internet: Cyber-Angriffe werden zum stressigen Unterfangen. Die internationale Kooperation und die Nachrüstung von Strafverfolgungsbehörden, Richtern und Staatsanwälten in Sachen IT-Know-How beginnen offenbar Früchte zu tragen. Wer eine Attacke startet, muss heute mit koordinierter und energischer Gegenwehr rechnen: Maliziöse Systeme werden vom Netz getrennt, kriminelle Gruppen ausgehoben.

Zwar lässt sich mit *flux networks*, in denen durch schnelle Änderungen der IP-Konfigurationen das Abkoppeln der Angriffssysteme erschwert wird, etwas Zeit gewinnen – doch wie im echten Leben gilt es nun auch im virtuellen Raum, den kriminellen Zugriff möglichst kurz zu halten. Oft bleibt nur ein Zeitfenster von wenigen Stunden, manchmal sogar Minuten, um von einem Phishing-, Verschlüsselungs- oder DoS-Angriff zu profitieren. Während der Vorbereitungsaufwand für einen erfolgreichen Angriff steigt, sinkt mit der Verkleinerung des Zeitfensters dessen Profitabilität.

Sicherlich darf man trotzdem in naher Zukunft nicht darauf hoffen, dass blanke Not die Cracker zu Gutmenschen mutieren lässt. Denn noch finden sie ausreichend Nahrung: Lange nicht jedes Unternehmen hat seine Hausaufgaben ordentlich gemacht. Und ist erst der gesamte Fileserver verschlüsselt, steigt die Zahlungsbereitschaft meist mit Lichtgeschwindigkeit.

Sollte die Entwicklung so weitergehen, könnte sich dennoch am Horizont ein wenig Licht abzeichnen. Vielleicht genügt es ja eines Tages, nicht jede ankommende E-Mail sofort zu öffnen.

Das wäre zugleich ein kleiner Beitrag zur Entschleunigung – der vielleicht auch einfach mal so gut tun würde.

Inhalt

secorvo
security consulting

Security News

Anti-Ransomware

Fast täglich tauchen neue, immer ausgeklügeltere Varianten von Verschlüsselungstrojanern (*Ransomware*) auf – auch in kritischen Infrastrukturen, wie heise.de am 18.02.2016 berichtete. Anti-Viren-Programme helfen nicht dagegen: Die Schadsoftware wird oft erst Tage später erkannt.

Was lässt sich dagegen tun? Neben einem Backup, das im Katastrophenfall die Wiederherstellung unzugänglich verschlüsselter Daten erlaubt, erreicht man nachhaltigen Schutz nur durch einen zurückhaltenden Umgang mit Schreib- und Ausführungsrechten. Will man den Schaden für Dateien auf Fileservern begrenzen, benötigt man ein differenziertes und restriktives Rechte- und Rollenkonzept, das Benutzern nur die Schreibzugriffe einräumt, die sie tatsächlich benötigen. Auch sollten Anwender nie mit administrativen Rechten auf externe Daten (Webseiten, E-Mail-Anhänge, USB-Stick-Inhalte) zugreifen.

Zusätzlich ist zu empfehlen, via AppLocker über Gruppenrichtlinien einzuschränken, welche Dateien ausgeführt werden dürfen, und das Aktivieren von Ransomware auf allen Systemen zu unterbinden. Auch eine Einschränkung von Skriptsprachen wie Powershell oder CScript sollte in Betracht gezogen werden. Zum Schutz vor Office-Makros bietet sich auch die Verwendung vertrauenswürdiger Speicherorte an. Nicht zuletzt sollten die Anwender mit geeigneten Security Awareness-Maßnahmen für die Risiken sensibilisiert werden, damit sie in Zweifelsfällen fragen, bevor sie eine Schadsoftware aktivieren.

Volksverschlüsselung über Nacht

Am 05.04.2016 poppte in WhatsApp-Chats auf Millionen Smartphones die Nachricht auf: Ab sofort seien alle Nachrichten und Anrufe mit dem Gesprächspartner Ende-zu-Ende verschlüsselt.

Bei aller berechtigter Kritik an WhatsApp muss man vor dieser Maßnahme den Hut ziehen. Unter der Annahme, dass die Implementierung der Verschlüsselung ordentlich erfolgt ist (derzeit gibt es keinen Grund etwas Anderes anzunehmen – sie basiert auf dem anerkannten TextSecure-Protokoll), wurde über Nacht ein immenser Gewinn für die Privatsphäre von Millionen Menschen geschaffen. Die Umsetzung ist unkompliziert: Schlüsselerstellung und -austausch erfolgen automatisch. Zusätzlich kann eine Sicherheitsnummer (QR-Code) abgeglichen werden, um den Gegenüber zu authentifizieren. Diese Funktion ist allerdings stiefmütterlich platziert – offenbar sind die Entwickler zu der (realistischen?) Einschätzung gelangt, dass die Authentifizierung die User ohnehin nicht interessiert.

Allerdings fallen nach wie vor Metadaten zuhauf an (wer kommuniziert wann mit wem?). Und weiterhin synchronisiert WhatsApp automatisch das Adressbuch – im Unternehmensumfeld in der Regel ohne Rechtsgrundlage. Daher sollten Unternehmen nicht dem Irrglauben verfallen, die geschäftliche Nutzung von WhatsApp sei durch die Verschlüsselung unbedenklich geworden.

Paranoia als Sorgfaltspflicht?

Geht es nach der Rechtsprechung steigt die Awareness der Durchschnittsnutzer offenbar stetig. Das Amtsgericht Frankfurt a. M. hat mit Urteil vom 24.03.2016 das Hereinfallen auf eine Phishing-Mail, die zur Mitteilung der Telefon-Banking-PIN verleitete, als grobe Fahrlässigkeit gewertet. Verschiedene Instanzgerichte und 2012 auch der Bundesgerichtshof haben die Herausgabe von TANs und PINs bereits als vom Nutzer zu verantworten qualifiziert, wenn die Bank zuvor auf die Gefahren durch Phishing hingewiesen und klargestellt hat, dass sie zu bestimmten Verhaltensweisen nicht auffordern wird. Bis Oktober 2009 haftete der Bankkunde bereits bei einfacher Fahrlässigkeit, danach wurde § 675v Abs. 2 BGB auf grobe Fahrlässigkeit beschränkt. Sie liegt vor, wenn die erforderliche Sorgfalt in besonders schwerem Maß verletzt wird und selbst naheliegende Überlegungen nicht angestellt werden. Angesichts der steigenden Qualität der Angriffe darf man jedoch bezweifeln, dass vom Durchschnittsnutzer generell erwartet werden kann, eine Phishing-Mail zu erkennen.

Forensische Jagd

Das Google Rapid Response Framework (GRR) ist ein bewährtes forensisches Werkzeug für die Analyse von Apple-, Windows- und Linux-Systemen. Im aktuellen Release 3.1 vom 16.04.2016 wurde die Möglichkeit ausgebaut, eine umfassende Jagd (*hunt*) über eine Gruppe von Zielsystemen durchzuführen, um die Existenz eines spezifischen Artefakts zu prüfen und optional auch Gegenmaßnahmen einzuleiten. Unter der Haube des GRR wurde die forensische Echtzeitanalyse in das am 05.04.2016 fertig gestellte Rekall V1.5 integriert, das jetzt auf den Capstone Disassembler umgestellt hat und dadurch ein sehr viel weiter gehendes Bild über die Ablaufstrukturen von Programmfunktionen liefert als das, was man bisher von einem forensischen *Incident Tool Framework* erwarten durfte. Wer GRR testen möchte, dem seien der aktuelle Docker Build oder die pre-build Binaries empfohlen. *Happy Hunting*!

Standardisiertes Löschen

Die „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“ ist am 08.04.2016 als DIN 66398 erschienen und kann nun beim Beuth Verlag bezogen werden. Die Weiterentwicklung der Leitlinie Löschkonzept zu einer DIN-Norm wurde seit Ende 2013 von den Unternehmen Deutsche Bahn, Blancco, DATEV, Secorvo und Toll Collect gefördert (SSN 2/2014, SSN 1/2015 und SSN 9/2015). Ein großer Schritt für den Datenschutz: Nun gibt es einen Standard für die Festlegung von Löschfristen.

Durch Wiederholung richtig?

Das Landesarbeitsgericht Berlin-Brandenburg hat anlässlich eines Falls exzessiver Internetnutzung eines Arbeitnehmers sein Urteil von 2011 bekräftigt und die Stellung des Arbeitgebers als Telekommunikationsanbieter verneint. So sei der Arbeitnehmer bei erlaubter Privatnutzung kein Dritter, und es läge keine Erbringung von Telekommunikationsdiensten vor (§ 3 Nr. 10 TKG). Die Zulässigkeit der Auswertung des Browserverlaufsprotokolls stützt das Gericht auf § 32 BDSG. Die Speicherung sei zur Missbrauchskontrolle zulässig. Da der Arbeitnehmer das Protokoll beliebig löschen kann, ist allerdings bereits die Eignung fraglich.

Insgesamt überzeugt die Begründung des Gerichts auch bei dieser neuen Entscheidung nicht, da sich das Urteil weder argumentativ mit der Dritteigenschaft von Arbeitnehmern noch vollständig mit der datenschutzrechtlichen Qualifizierung von Browserverlaufsdaten auseinandersetzt. Unternehmen sollten daher auch weiterhin bei erlaubter Privatnutzung die Pflichten eines Telekommunikationsdiensteanbieters erfüllen.

Datenschutzgrundverordnung

Am 14.04.2016 hat als letzte Instanz auch das Europäische Parlament die Datenschutzgrundverordnung verabschiedet, die damit nach Veröffentlichung im Europäischen Amtsblatt in Kraft tritt und ab Mitte 2018 europaweit gelten wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich bereits am 07.04.2016 mit der Anpassung der deutschen Datenschutzgesetze auseinandergesetzt. Die Datenschutzbeauftragten fordern u. a. die Einführung eines Beschäftigtendatenschutzgesetzes (oder die Beibehaltung von § 32 BDSG), Beschränkungen für Gesundheitsdaten, die Normierung der Schutzziele Datensparsamkeit, Vertraulichkeit, Integrität, Verfügbarkeit, Nichtverkettbarkeit, Transparenz und Intervenierbarkeit und die Beibehaltung des § 4f Abs. 1 BDSG zur Bestellpflicht eines bDSB.

Die Erklärung macht deutlich, dass auch mit der Grundverordnung noch lange keine Klarheit über die 2018 eintretende Rechtslage und die zu erwartenden Auswirkungen für Unternehmen besteht.

Secorvo News

Zertifikat für Experten

Wir können Ihnen noch einige wenige freie Plätze auf dem kommenden T.I.S.P.-Seminar vom **06. bis 10.06.2016** anbieten. Mit Ihrer Anmeldung erhalten Sie das T.I.S.P.-Begleitbuch zur Vorbereitung. Die nächste Gelegenheit zur Zertifizierung bieten wir dann erst wieder im November – der frühe Vogel bekommt den Platz …

Programm und Online-Anmeldung unter
http://www.secorvo.de/college

Auslaufmodell Datenschutz?

Zum Abschluss der Ausstellung "Global Control and Censorship“ lädt die KA-IT-Si zusammen mit dem ZKM | Karlsruhe, KASTEL und dem CyberForum e.V. am **Freitag, 29. April 2016 ab 16 Uhr** zur größten Anti-Prism-Party Europas (4. Staffel) ins ZKM (Eintritt frei). Experten zeigen in Live-Vorführungen und an Beratungsständen, wie Sie sich vor Ausspähungen im Internet schützen können; begleitet von Führungen durch die Ausstellung. Derweil können sich Ihre Kinder in der Spion-Schule der Pädagogischen Hochschule Karlsruhe zum Verschlüsselungsexperten ausbilden lassen.

Gibt es überhaupt Chancen, der allgegenwärtigen Überwachung zu entgehen? Ist das Konzept „Datenschutz“ gar ein Auslaufmodell? Diese Fragen möchten wir um **18:30 Uhr** im Medientheater des ZKM mit Ihnen und dem Datenschutz-Aktivisten Malte Spitz in einer Publikumsdiskussion erörtern.

Programm: https://www.anti-prism-party.de

Save the date - 8. Tag der IT-Sicherheit

Auf dem „Tag der IT-Sicherheit“, einer Veranstaltung von KA-IT-Si, IHK Karlsruhe und CyberForum, zeigen wir einmal jährlich aktuelle IT-Sicherheitsbedrohungen für Unternehmen auf und informieren über Präventionsmöglichkeiten. Unser diesjähriger *Keynote Speaker* ist Tobias Schrödel, IT-Sicherheitsexperte und erster Comedyhacker. Das Programm finden Sie auf unserer Webseite. Merken Sie sich den **22.06.2016, 14 Uhr** schon jetzt in Ihrem Terminkalender vor.

Wir empfehlen eine frühzeitige Anmeldung.

Veranstaltungshinweise

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

Mai 2016	
08.-12.05.	Eurocrypt 2016 (IACR, Sofia/BG)
30.05.-01.06.	IFIP SEC 2016 (IFIP, Hamburg)
Juni 2016	
06.-10.06.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
10.06.	IT-Sicherheitsrisiken managen: Hürden und Möglichkeiten (Fachgruppe SECMGT der GI, Frankfurt)
10.-11.06.	AREA41 Security Conference (DC4131 DEFCON Switzerland, Zürich/CH)
13.-14.06.	DuD 2016 (Computas, Berlin)
15.-17.06.	Entwicklertag 2016 (VKSI, GI, ObjektForum, Karlsruhe)
22.06.	8. Tag der IT-Sicherheit (KA-IT-Si, Karlsruhe)
27.06.-01.07.	OWASP AppSec EU 2016 (OWASP Foundation, Rom/I)
Juli 2016	
30.07.-04.08.	Blackhat USA 2016 (Blackhat, Las Vegas/US)
August 2016	
04.-07.08.	DEF CON 24 (DEFCON, Las Vegas/US)
07.-10.08.	16th Annual DFRWS Conference 2016 (DFRWS, Philadelphia/US)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Dr. Volker Hammer, Kai Jendrian, Michael Knopp, Christoph Schäfer, Jochen Schlichting

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

secorvo
security consulting

Secorvo Security News

Mai 2016

Vom Aushalten

Ein Login ohne Passwort? Eine EC-Karte ohne Geheimnummer? Online-Banking ohne PIN/TAN? Informationstechnik ohne Schutzmaßnahmen ist heute undenkbar.

Beim Zugriff auf Daten von Kriminellen wird aus dem Schutz jedoch ein Ermittlungshindernis. Am 21.04.2016 gestand Direktor James Comey der Washington Post, dass das Knacken des Smartphones des San-Bernardino-Mörders dem FBI über 1,3 Mio. US$ wert war – mit einem Programm, das eine Schwachstelle im iOS ausnutzte, die nur beim iPhone 5c funktionierte. Da selbst das FBI (Etat: 8,7 Mrd. US$) Hacks auf alle Smartphone-Modelle (sofern überhaupt möglich) nicht bezahlen könne, fordert Comey von den Herstellern direkten Datenzugriff. Wie könnte das funktionieren? Zwei Ansätze gibt es dafür: Entweder durch eine Hintertür in der Software oder durch Hinterlegung der kryptografischen Schlüssel.

Beide Ansätze sind keine gute Idee. Informationen über Hintertüren verbreiten sich rasch – die Listen der BIOS-Master-Passwörter zur Umgehung des Bootschutzes sind legendär. Das weiß auch das FBI: Seit Mitte 2015 kursieren 3D-Druckvorlagen der sieben Master-Schlüssel für TSA-Kofferschlösser, die angeblich nur Zollbeamten zugänglich sind. Auch gelingen immer wieder Angriffe auf hinterlegte Schlüssel – wie die Kompromittierung des SecureID-Root-Keys von RSA vor fünf Jahren (SSN 03/2011). Der 1993 von der Clinton-Regierung entwickelte *Escrowed Encryption Standard*, nach dem die Verschlüsselungsschlüssel verschlüsselt mitgesendet bzw. -gespeichert werden sollten, scheiterte an einem Protokollfehler. Die Erfahrung lehrt: Sichere Verschlüsselung muss frei von Hintertüren sein – und Schlüssel dürfen nicht zentral gespeichert werden.

Wenn wir die Sicherheit unserer Informationstechnik insgesamt nicht aufs Spiel setzen wollen, bleibt uns daher nur, es auszuhalten, dass auch Kriminelle Daten so verschlüsseln können, dass kein Strafverfolger darauf zugreifen kann.

Inhalt

secorvo
security consulting

Security News

Wette auf fallende Kurse

In letzter Zeit häufen sich wieder Meldungen zu Schwachstellen in Sicherheitssoftware: Betroffen waren u. a. Virenschutzprogramme von Symantec, (16.05.2016), SSL-Proxies von Jugendschutzfiltern mehrerer Hersteller (20.12.2015) und die Management-Software von Lenovo (26.04.2016). Diese Programme sollen die Sicherheit verbessern – schaffen aber durch Schwachstellen selbst neue Angriffspunkte.

Generell gilt: Ganz gleich, welche Art von Software man einsetzt, immer erhöht man dadurch die Wahrscheinlichkeit von Schwachstellen. Bei Sicherheitssoftware stellen sie meist eine besondere Gefahr dar, da diese oft mit privilegierten Rechten arbeitet. So mancher Benutzer wiegt sich daher mit solchen Programmen in trügerischer Sicherheit.

Schon vor zwei Jahren berichteten wir über Schwachstellen, die man sich durch den Einsatz von Virenschutz- und Monitoring-Agenten erst einhandelt (SSN 05/2014). Manchmal ist weniger mehr: Ein wenig Awareness dafür, worauf man bei der Internetnutzung achten sollte, ist womöglich eine bessere Investition als ein technischer Filter – der neue Viren ohnehin erstmal nicht erkennt und zudem womöglich Schwachstellen enthält.

Das dabei gesparte Geld sollte man vielleicht Gewinn bringend auf fallende Aktienkurse ausgewählter Hersteller von Sicherheitssoftware setzen.

Kritische Anlagen

Weitgehend unverändert ist der Referentenentwurf der ersten Verordnung zum Anwendungsbereich des IT-Sicherheitsgesetzes am 03.05.2016 in Kraft getreten. Ergänzt wurde die Behandlung von miteinander verbundenen kritischen Anlagen. Das Prinzip, den Versorgungsgrad als Maß für die Kritikalität einer Anlage heranzuziehen (SSN 02/2016), ist geblieben – die Gefährdung der öffentlichen Sicherheit durch Fehlfunktion einer Anlage bleibt bei der Einstufung weiterhin ausgeblendet.

Die Verordnung zu den Sektoren Finanzen, Transport, Verkehr und Gesundheit soll Anfang 2017 folgen. Zur Unterstützung der Entwicklung branchenspezifischer Sicherheitsstandards hat das BSI im Dezember eine Orientierungshilfe publiziert; bisher wurde jedoch noch kein Standard veröffentlicht.

Die Umsetzungsfrist für die Betreiber von in den Anhängen der Verordnung benannten Infrastrukturen läuft bis zum 03.05.2018. Bis dahin sind Investitionen in Anbieter rund um ISM-Systeme sicher keine schlechte Kapitalanlage.

Ad-hoc-Meldung

Am 03.05.2016 wurde gleich eine Handvoll schwerer Schwachstellen in der beliebten Bildbearbeitungssoftware ImageMagick veröffentlicht. Brisant sind diese Schwachstellen nicht nur wegen der Möglichkeit, beliebigen Code ausführen zu können, sondern auch, weil der ImageMagick-Code in zahlreichen Bibliotheken verwendet wird, ohne dass dies den Entwicklern bekannt sein dürfte: Nicht nur dort, wo ImageMagick draufsteht, ist ImageMagick drin.

Wer Anteile an ImageMagick hält, sollte sie nicht gleich abstoßen – denn bekanntlich ist auch schlechte Publicity gute Publicity. Aber man sollte den Fall zum Anlass nehmen, neben einem funktionierenden Patch-Management dafür zu sorgen, dass die in der Entwicklungsabteilung verwendeten (Open-Source-) Bibliotheken inventarisiert und der Umgang mit dazu veröffentlichten Schwachstellen geregelt wird.

Spionagetools statt Gold

Spätestens seit der Veröffentlichung der Panama Papers sind kreative neue Möglichkeiten der Geldanlage gefragt. Die Bundesnetzagentur will helfen und sagte am 25.04.2016 Spionagekameras den Kampf an: Seitdem ist es verboten, WLAN-Kameras anzubieten oder zu besitzen, die in Alltagsgegenständen wie beispielsweise Kugelschreibern oder Rauchmeldern versteckt sind. Die BNetzA geht gegen Hersteller, Verkäufer und Käufer vor und verlangt die Vernichtung der Gegenstände – nach eigenen Angaben bisher in rund 70 Fällen.

Nicht bekannt ist, ob auch Organisierte Kriminalität und Nachrichtendienste zu den Betroffenen zählen – und warum andere „hilfreiche" Tools wie sendende Keylogger oder spionierende Hotspots nicht unter den Bann fallen.

Dennoch ist jetzt der richtige Zeitpunkt, um schnell noch in Restbestände von Spionagekameras zu investieren und diese vom benachbarten Ausland über einschlägige, nicht-deutsche Online-Shopping-Plattformen zu vertreiben.

Investition im Keksmarkt

Cookies sind ein geliebtes Feindbild des Datenschutzes – kein Grund allerdings, Investitionen im Keksmarkt zu reduzieren. Denn die am 24.05.2016 in Kraft getretene Datenschutz-Grundverordnung (Verordnung (EU) 2016/679, DSGVO) bringt keineswegs die vielerorts erhoffte Klarheit.

Während der Bundesinnenminister mehr Flexibilität fordert, da personenbezogene Daten schließlich „nicht um ihrer selbst willen schützenswert“ seien, weisen Experten auf strukturelle Probleme der DSGVO hin, u. a. ihre Unterkomplexität. Es bleibt eine große Unsicherheit, denn die in zwei Jahren unmittelbar geltenden Regelungen enthalten eine Vielzahl von Öffnungsklauseln. Manche stellen einen konkreten Handlungsauftrag an den nationalen Gesetzgeber: Das BDSG wird durch ein Nachfolgegesetz ersetzt werden müssen. Umgekehrt werden viele Regelungen, die Datenverarbeitungen bisher legitimieren, aufgrund fehlender Öffnungsklauseln schlicht wegfallen, so z. B. Teile des § 28 BDSG zur werblichen Nutzung personenbezogener Daten.

Da viele Datenschützer den Besuch eines der unzähligen Seminarangebote zur DSGVO einer Lektüre der 187-seitigen Broschüre der BfDI vorziehen dürften, ist in den nächsten Monaten mit einem Anstieg des Kekskonsums zu rechnen – Cookies hin oder her. Wer sich die Seminarkosten angesichts der herrschenden Unklarheit über die finale Rechtslage spart, sollte daher über eine Aufstockung seiner Investitionen im Keksmarkt nachdenken.

Haftung bleibt

Folgt man der Euphorie der Medien, ist die Störerhaftung für offene WLANs schon so gut wie begraben. Tatsächlich hat sich die Bundesregierung am 10.05.2016 auf eine Entschärfung eines vom September 2015 stammenden Gesetzesentwurfs zur Änderung des Telemediengesetzes geeinigt.

§ 8 Abs. 4 des ursprünglichen Entwurfs sah verschiedene Pflichten für Anbieter von WLAN-Hotspots vor. Diese sollen nun entfallen und Anbieter offener WLANs vollständig Zugangsanbietern gleichgestellt werden, die bereits heute nach § 8 TMG ein Haftungsprivileg genießen. Ursache des Sinneswandels ist unter anderem der Schlussantrag des Generalanwalts am EuGH vom 16.03.2016, der diese Gleichstellung auf Basis von Art. 12 der E-Commerce-Richtlinie vornimmt.

Der Schlussantrag lässt jedoch genau wie das BGH-Urteil vom 26.11.2015 den Weg zu Sperranordnungen offen. Die Rechtsprechung wendet das Haftungsprivileg zudem bislang nicht auf zukunftsgerichtete Unterlassungsansprüche an. Daran ändert auch die neue Einigung nichts. Der Schlussantrag kommt allerdings zu dem Ergebnis, dass Anbietern keine Abmahnkosten auferlegt werden dürfen. Von einer Abschaffung der Störerhaftung kann also kaum die Rede sein.

Investitionen in Musik- und Filmverlage sollte man daher nicht gleich abstoßen – hingegen lohnt es weiterhin, in Anbieter von Sperrsoftware und auf Urheberrechtsfragen spezialisierte Rechtsberatungen zu setzen.

Secorvo News

Aktuelle Entwicklungen

Auch die Informationssicherheit wird von der Schnelllebigkeit technischer Entwicklungen nicht verschont. Auf dem Seminar „IT-Sicherheit heute“ (**27.-29.09.2016**) greifen wir aktuelle Entwicklungen und neue Themen auf, um eine Hilfestellung beim Nachjustieren von Sicherheitskonzepten und Schutzmaßnahmen zu bieten. Das Programm des Seminars wird ständig aktualisiert.

T.I.S.P.

Anfang des Jahres 2017 dürfte die 1.000er-Marke fallen – so viele IT-Sicherheitsexperten haben inzwischen das T.I.S.P.-Zertifikat zum Nachweis ihrer fachlichen Qualifikation erworben. Der Erfolg des T.I.S.P. lässt sich nicht nur an der großen Nachfrage ablesen, sondern auch an der Bedeutung, die Stellenanzeigen im Bereich der IT- und Informationssicherheit dem Zertifikat einräumen.

Wer das T.I.S.P.-Seminar bei Secorvo besucht, erhält zur Vorbereitung das Begleitbuch zum T.I.S.P., ein 700seitiges Lehr- und Lernbuch sowie Nachschlagewerk zu den zentralen Themen der Informationssicherheit. Das nächste T.I.S.P.-Seminar mit freien Plätzen findet vom **21. bis 25.11.2016** statt. Programm und Online-Anmeldung unter https://www.secorvo.de/college.

8. Tag der IT-Sicherheit

Der Karlsruher Tag der IT-Sicherheit, den die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) in Zusammenarbeit mit dem CyberForum e.V. und der IHK Karlsruhe austrägt, beschäftigt sich in diesem Jahr zum achten Mal mit aktuellen IT-Sicherheitsherausforderungen für Unternehmen. Er macht deutlich, wie wichtig ein professioneller Umgang mit den Themen IT-Sicherheit und Datenschutz ist und informiert über Präventionsmöglichkeiten. Diesjähriger Keynote Speaker ist Tobias Schrödel, IT-Sicherheitsexperte und erster „Comedyhacker“. Die Fachvorträge beschäftigen sich u. a. mit den Themen Cybercrime und Industrial Security im Produktionsumfeld. Das Programm schließt mit einem Live-Hacking und bietet Gelegenheit zum fachlichen Gedanken- und Erfahrungsaustausch mit Referenten, Teilnehmern und Ausstellern.

Die Veranstaltung findet am **22.06.2016** im Saal Baden der IHK Karlsruhe statt. Das Programm sowie die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite www.tag-der-it-sicherheit.de.

Veranstaltungshinweise

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

Juni 2016	
06.-10.06.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
10.06.	IT-Sicherheitsrisiken managen: Hürden und Möglichkeiten (Fachgruppe SECMGT der GI, Frankfurt)
10.-11.06.	AREA41 Security Conference (DC4131 DEFCON Switzerland, Zürich/CH)
13.-14.06.	DuD 2016 (Computas, Berlin)
15.-17.06.	Entwicklertag 2016 (VKSI, GI, ObjektForum, Karlsruhe)
22.06.	8. Tag der IT-Sicherheit (KA-IT-Si, Karlsruhe)
27.06.-01.07.	OWASP AppSec EU 2016 (OWASP Foundation, Rom/I)
Juli 2016	
30.07.-04.08.	Blackhat USA 2016 (Blackhat, Las Vegas/US)
August 2016	
04.-07.08.	DEF CON 24 (DEFCON, Las Vegas/US)
07.-10.08.	16th Annual DFRWS Conference 2016 (DFRWS, Philadelphia/US)

Fundsache

Der Landesbeauftragte für den Datenschutz Baden-Württemberg hat am 22.04.2016 einen 27-seitigen Leitfaden für Datenschutzeinstellungen bei Windows 10 herausgegeben, der empfehlenswerte Grundkonfigurationen Schritt für Schritt erläutert.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, 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

secorvo
security consulting

Secorvo Security News

Juni 2016

Glückliche Sklaven

Während sich der von der Safe-Harbor-Entscheidung des EuGH vom 06.10.2016 aufgewirbelte Staub langsam legt, die ersten Aufsichtsbehörden Bußgeld-Bescheide verschicken und sich die EU beeilt, via Privacy Shield-Abkommen eine neue Rechtsgrundlage für die Übermittlung personenbezogener Daten in die USA zu zimmern, erreicht die heimliche Überwachung neue Dimensionen.

Anfang der 2000er Jahre schossen sich Datenschützer auf die Nutzung von Cookies als Tracking-Instrument ein. Darauf reagierte die EU am 25.11.2009 mit der Verabschiedung einer (wenig universellen) „Cookie-Richtlinie“, die eine Einwilligung der Benutzer fordert. Sie ist bis heute in vielen EU-Staaten nicht umgesetzt; Verstöße werden nicht geahndet. Derweil wichen Google & Co. auf andere, weit ergiebigere Methoden zur Gewinnung von Internet-Nutzungsdaten aus: Mit „kostenlosen“ Service-Angeboten spannten sie Webseitenbetreiber vor ihren Karren. Mit Erfolg: Das Webseiten-Analysetool Google Analytics erreichte einen Marktanteil von über 90%, bevor es in den Fokus von Datenschützern geriet, denen die Datensammelei von Marketingabteilungen ohnehin ein Dorn im Auge war.

Während sich Datenschützer an Google Analytics und Social Media Plugins festbissen, zündeten Google & Co. ein Feuerwerk an Angeboten für Webentwickler, die diese bereitwillig in ihren Code einbetteten. Kaum eine Webseite, die kein Javascript- oder CSS-Framework und keinen Web-Font nachlädt – und dabei die Nutzerdaten bei Facebook, Google oder Twitter abliefert. Schließlich erfand Google die Safe Browsing-API, die jeden Seitenaufruf anhand einer Google-Blacklist auf enthaltene Schadsoftware prüft. Inzwischen Teil von Firefox, Safari und Chrome meldet die API jeden Webseitenaufruf von einer Milliarde Nutzern an Google. Microsoft wollte da nicht zurückstehen führte im IE8 den SmartScreen-Filter ein. Ein genialer Coup. Denn die erbittertsten Feinde der Freiheit sind bekanntlich die glücklichen Sklaven.

Inhalt

secorvo
security consulting

Security News

Heimlich, still und leise

Google Analytics und Social-Media-Plugins sind immer wieder für eine Aufregung gut – wie zuletzt anlässlich der Bußgeldbescheide der Datenschutz-Aufsichtsbehörde Hamburg vom 06.06.2016. Technisch sind beide inzwischen Nebenkriegsschauplätze der großflächigen Erhebung von Metadaten. Die erfolgt mittlerweile – heimlich, still und leise – durch Web-Entwickler-Tools, die sich bisher weitgehend der Wahrnehmung von Datenschützern und Aufsichtsbehörden entziehen:

Bootstrap: Das von Twitter angebotene CSS-Framework erfreut sich großer Beliebtheit bei Webseitenbetreibern. Wird es jedoch nicht auf dem eigenen Server installiert, bekommt Twitter beim Online-Download die Nutzerdaten (IP-Adresse, besuchte Webseite und Zugriffszeitpunkt) frei Haus.

jQuery/Ajax: Eine Webseite zu finden, die ohne den Einsatz der freien JavaScript-Bibliothek auskommt, gleicht schon fast einem Wunder. Werden dabei die jQuery-Bibliotheken von Google nachgeladen, erhält Google die Nutzerdaten.

AngularJS: Genauso verhält es sich mit Googles JavaScript-Webframework. Eine lokale Installation ist aus Datenschutzgründen anzuraten, doch welcher Webdesigner macht das schon?

React: Facebook bietet mit React eine Alternative zu Angular – ein Webframework, das beim Nachladen die Nutzerdaten an Facebook übermittelt.

Web-Fonts: Annähernd jede moderne Webseite nutzt Web-Fonts von Google oder Adobe. In der Regel werden die Fonts dabei erst beim Seitenbesuch nachgeladen. Dabei wäre eine lokale Installation der Fonts problemlos möglich.

Kartendienste: Beliebt ist es auch, auf der Kontakt-Seite die Kartendienste von Google oder Bing Maps einzubinden. Auch hier liefert man dem Anbieter die Nutzungsdaten seiner Seitenbesucher. Mangels einer ähnlichen Lösung wie für die Social-Media-Plugins würde hingegen ein Link zum Kartendienst genügen – sofern man nicht gleich auf die freie Alternative OpenStreetMap setzen möchte.

No CAPTCHA reCAPTCHA: In den SSN 12/2014 berichteten wir über die Google-Version des Turing-Tests, bei der die IP-Adresse übermittelt und Mausbewegungen ausgewertet werden. Zumindest die DENIC setzt nach harscher Kritik im Netz inzwischen wieder auf eine alternative Lösung.

Viele Webseiten-Entwickler erliegen heute den Verlockungen kostenfreier Frameworks, Schriften etc. Die Übermittlung der Nutzungsdaten der Webseitenbesucher in die USA ist nach der Entscheidung des EuGH (SSN 10/2015) jedoch ohne einen Vertrag nach EU-Standardvertragsklauseln oder eine wirksame Einwilligung der Betroffenen rechtswidrig. Zumindest eine lokale Installation der Dienste ist daher geboten – auch wenn man sich anschließend selbst um das Patching kümmern muss.

Versteckter Tracing Code

Dank eines Beitrags im Diskussionsforum reddit wurde am 10.05.2016 bekannt, dass der C++-Compiler von Visual Studio 2015 ungefragt *Tracing Code* in kompilierte Anwendungen einbaut. Dabei handelt es sich um Telemetriedaten wie bestimmte Events und Zeitstempel, die an die Systemkomponente ETW (*Event Tracing for Windows*) weitergeleitet werden. Daraufhin sah sich Microsoft zu einer Stellungnahme gezwungen, in der angekündigt wurde, diese Funktion mit dem nächsten Update zu entfernen.

Auch wenn diese Daten nur lokal auf dem System gespeichert werden und nicht unmittelbar abfließen, ist es schon bedenklich, dass derartige Funktionen im Verborgenen injiziert werden. Schließlich ist es nahezu unmöglich nachzuvollziehen, ob das kompilierte Programm tatsächlich nur die gewünschte Funktionalität enthält. Beim Vertrauen in die eigesetzten Werkzeuge ist besondere Vorsicht geboten, wie schon Ken Thompson in seinem 1984 erschienenen Paper „Reflections on Trusting Trust“ aufzeigte.

Smart Spy

Groß war die Aufregung, als heise am 25.01.2014 SmartTVs als potentielle Spione im Wohnzimmer entlarvte. Über den Datendienst HbbTV können TV-Sender den Fernseher anweisen, eine bestimmte URL abzurufen – und zwar genau dann, wenn man den Sender einschaltet: Der Zählpixel der TV-Welt, mit dem sich das Fernsehverhalten der Nutzer protokollieren lässt. Eine senderübergreifende Auswertungsmöglichkeit mit Google Analytics versteht sich von selbst – Cookies finden nicht nur im PC, sondern auch im Fernseher Verwendung.

Neben den TV-Sendern lassen sich inzwischen auch die Hersteller smarter Fernsehgeräte mit Daten über den Nutzer beglücken. In einem Musterklageverfahren gegen die deutsche Samsung-Tochter konnte nun die Verbraucherzentrale Nordrhein-Westfalen am 10.06.2016 einen kleinen Sieg beim Landgericht Frankfurt am Main erringen (Az. 2-03 O 364/15): Auch wenn man die AGB und die über 56 Bildschirmseiten lange Datenschutzerklärung gele-

sen und abgelehnt hat, übermittelt ein Samsung-SmartTV die IP-Adresse des Nutzers an Samsung.

Das LG akzeptierte die Datenschutzbestimmungen wegen ihrer Länge und Unübersichtlichkeit nicht als wirksame Einwilligung. Da die Datenübermittlung jedoch nicht an die beklagte deutsche Samsung-Tochter, sondern an die Muttergesellschaft erfolgt, muss Samsung Deutschland nur seine AGB nachbessern. „Ob die Datenübermittlung in der konkreten Art und Weise rechtmäßig war, hatte die Kammer (...) nicht zu entscheiden" – schließlich gilt das BDSG nicht für Südkorea.

Unsichere Updates

Automatische Updates von Software beugen der Ausnutzung von Schwachstellen in veralteten und verwundbaren Programm-Versionen vor und stellen damit eine immer wieder empfohlene Schutzmaßnahme dar. Allerdings setzen viele Software-Hersteller ihre Nutzer durch automatische Update-Mechanismen unnötigen Gefahren aus, wenn der sensitive Update-Prozess über unverschlüsselte HTTP-Verbindungen erfolgt. So geschehen z. B. bei Intels Driver Update Utility (19.01.2016), ebenso bei Dell (23.11.2015) und bei Lenovo (31.05.2015). Sogar Sicherheitssoftware wie Keepass 2 (02.03.2016) ist verwundbar.

Erfolgt der Download nicht über TLS, können Angreifer mit einem Man-in-the-Middle-Angriff die übermittelten Updates *on the fly* mit Schadsoftware „anreichern". Die dafür benötigten Werkzeuge sind frei im Web verfügbar. Für die Nutzer ist die Manipulation eines Updates praktisch nicht zu erkennen. Wirksam schützen kann man sich davor nur, indem man unverschlüsselte Updates ausschließlich im eigenen, vertrauenswürdigen Netz zulässt.

Seitenkanäle im PC

Angriffe über so genannte Seitenkanäle, also nicht intendierte Informationswege wie das physische Verhalten eines Systems (Zeit, Stromverbrauch oder Arbeitsgeräusche), sind nichts grundsätzlich Neues. So wurden in der Vergangenheit Funker an der „Handschrift" ihrer Morsezeichen identifiziert oder Inhalte von Röhrenmonitoren über deren elektromagnetische Abstrahlung rekonstruiert.

Neu ist, dass über die Auswertung des Stromverbrauchs, des elektromagnetischen Felds oder der Geräuschentwicklung nicht nur geheime Schlüssel einer SmartCard (Paul Kocher, 1996), sondern auch aus einem modernen PC gewonnen werden können. Das belegen Daniel Genkin, Lev Pachmanov, Itamar Pipman, Adi Shamir und Eran Tromer in ihrem am 04.06.2016 in der Juni-Ausgabe der Communications of the ACM erschienenen Beitrag am Beispiel von Angriffen auf GnuPG – zwar unter optimierten Bedingungen, aber mit preiswertem Equipment aus gut 10 m Entfernung.

Will man Krypto-Software wirksam vor solchen Seitenkanalangriffen schützen, führt kein Weg an den bei Krypto-Hardware bereits üblichen Schutzmechanismen wie „Blinding" vorbei. Eine neue Herausforderung für Softwareentwickler.

Secorvo News

IT-Sicherheit heute

Für das Herbstseminar „IT-Sicherheit heute" sind noch letzte Plätze frei. Vom **27. bis 29.09.2016** bringen wir Sie auf den aktuellen Stand in den Bereichen Informationssicherheit, IT-Sicherheit und Datenschutz.

Neben Themen wie dem IT-Sicherheitsgesetz und der EU-Datenschutz-Grundverordnung stehen aktuelle Bedrohungen im Fokus: Gleich zu Seminarbeginn schlüpfen Sie in die Rolle von Angreifer und Verteidiger. Am dritten Seminartag (Hacking Day) zeigen Ihnen unsere Experten in Live-Hacks Angriffe mit Ransomware und PowerShell. Auch klassische Angriffsmethoden wie Spoofing und Man-in-the-Middle werden vorgestellt und es wird auf die Sicherheitslücken von Web-Anwendungen eingegangen. Zum Abschluss des Seminares dürfen Sie selbst Hand anlegen: Im WebGoat-Workshop nähern Sie sich Schritt für Schritt der Web-Security.

Wichtig für alle T.I.S.P.-Absolventen: Das Seminar wird als Weiterbildung für die Re-Zertifizierung anerkannt. Wir freuen uns auf Ihre Anmeldung.

Who is who?

Bei der Anmeldung an Ihrem Arbeitsplatzrechner müssen Sie sich authentisieren, d. h. Ihre Identität gegenüber dem System nachweisen. Das erfolgt heute in den meisten Fällen über die Eingabe Ihres Passworts.

Doch sind Passwörter noch zeitgemäß? Immer mehr Unternehmen setzen auf eine Zwei-Faktor-Authentifizierung (2FA). Bei unserer kommenden KA-IT-Si-Veranstaltung am **14.07.2016**, diesmal in den Räumen der Nexus Technology GmbH in Ettlingen, stellen Petra Barzin (Secorvo), Sandra Bialinski und Michael Leuchtner (Nexus) vor, welche 2FA-Alternativen es gibt und welche Stärken und Schwächen diese Lösungen besitzen.

Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking". Weitere Infos und die Möglichkeit zur Anmeldung auf www.ka-it-si.de.

Veranstaltungshinweise

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

Juli 2016	
14.07.	Who is who? (KA-IT-Si, Karlsruhe)
30.07.-04.08.	Blackhat USA 2016 (Blackhat, Las Vegas/US)
August 2016	
04.-07.08.	DEF CON 24 (DEFCON, Las Vegas/US)
07.-10.08.	16th Annual DFRWS Conference 2016 (DFRWS, Philadelphia/US)
10.-12.08.	25th USENIX Security Symposium (Usenix, Austin/US)
14.-18.08.	Crypto 2016 (IACR, Santa Barbara/US)
September 2016	
07.-08.09.	Annual Privacy Forum 2016 (ENISA, EC DG Connect, Goethe Universität, Frankfurt)
13.-15.09.	Future Security 2016 (Fraunhofer VVS, Berlin))
19.09.	Sommerakademie (ULD Schleswig-Holstein, Kiel)
26.-27.09.	D • A • CH Security (Gemeinsame Arbeitskonferenz von GI, OCG, BITKOM, SI, TeleTrusT, Klagenfurt)
27.-29.09.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)

Fundsache

Wer angesichts der zahlreichen Passwort-Leaks auf einen Passwort-Manager umsteigen will, dem sei dieser am 22.06.2016 veröffentlichte ausführliche Vergleich der wichtigsten Lösungen empfohlen.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Kai Jendrian, 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

secorvo
security consulting

Secorvo Security News

Juli 2016

Wir täuschen uns vielleicht

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, (...) kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden“ (Volkszählungsurteil vom 15.12.1983). Wie wahr. Man stelle sich vor, ein Gesprächspartner kenne alle irgendwo über uns gespeicherten Daten: Die bargeldlosen Zahlungen mit Datum/Uhrzeit, die Bewegungsmuster, die das Navi übermittelt, die Schlüsselworte, nach denen wir gegoogelt und die Webseiten, die wir je besucht haben. Wir trösten uns damit, dass diese Daten ohne Weiteres nicht zugänglich sind. Und täuschen uns vielleicht.

Unseren Namen erfährt man über die Fahrzeughalterauskunft, die Adresse über das Einwohnermeldeamt und die Teilnahme an einer Sportveranstaltung über die Ergebnislisten im Internet. Wir trösten uns damit, dass selbst öffentlich zugängliche Daten in der Regel nur mit höherem Aufwand zu erfahren sind, den wohl kaum jemand auf sich nimmt. Und täuschen uns vielleicht.

Denn es gibt Menschen, die sich den Aufwand leisten – um zum Beispiel (Privat-)Insolvenzen über eine App in Google Maps sichtbar zu machen. Oder um zu zeigen, welcher Arzt unseres Vertrauens Zahlungen von Pharmaunternehmen erhält. Diese Apps ließen sich rechtskonform aufwerten, indem man die Vorstandstätigkeiten in Vereinen, die veröffentlichungspflichtigen Leitungsfunktionen in Unternehmen, die Jahresgehälter und Pensionsverpflichtungen von AG-Vorständen und Aufsichtsräten sowie die von ihnen verkauften Aktien ergänzte. Dazu die Einblendung eines aktuellen Fotos aus Facebook, die Angabe des Hochzeitstags aus der Bestellung des Aufgebots und Verweise auf die nächsten Verwandten z. B. aus einer Online-Traueranzeige. Wir trösten uns damit, dass der Gesetzgeber dem schon einen Riegel vorschieben wird. Und täuschen uns vielleicht.

Inhalt

secorvo
security consulting

Security News

Malware Virenschutz

Wie erneut ein aktueller Fall vom 28.06.2016 zeigt (siehe SSN 5/2014), verstecken sich auch in Virenschutzprodukten (diesmal: Symantec) Schwachstellen. Virenschutzsoftware muss man daher inzwischen auch als eine potentielle Gefährdung ansehen, zumal Angreifer über solche Schwachstellen privilegierte Rechte erhalten. Hinzu kommt, dass neue Schadprogramme erst mit mehreren Tagen Verzögerung erkannt und Heuristiken von geschickten Angreifern umgangen werden.

Werden Datenträger konsequent auf Viren geprüft und erfolgt die Datenübermittlung über zentrale Content Filter, sollte man daher darüber nachdenken, auf Fat-Clients und Servern ganz auf Virenschutz zu verzichten.

Wem die Virenfreiheit von Systemen zu bestimmten Zeitpunkten wichtig ist, sollte einen (schreibgeschützten und Firmware-signierten) „Virenschutz-Stick" z. B. mit dem vom heise-Verlag veröffentlichten Desinfec't verwenden, um damit stichprobenhafte Prüfungen durchzuführen.

Ganz klein gelandet

Am 17.06.2016 hat das zweite Gesetz zur Änderung des Telemediengesetzes den Bundesrat passiert. Die Änderungen nach fast 12-monatigem Gesetzgebungsverfahren und noch längerer Vordiskussion umfassen eine WLAN-Definition und § 8 Abs. 3, der klarstellt, dass Anbieter öffentlicher WLANs dem Haftungsprivileg für Access-Provider unterfallen. Ein geplanter Abs. 4, der auch Unterlassungsansprüche ausschließen sollte, wurde nicht aufgenommen.

Hotels und Anbieter von Gäste-WLANs oder Hotspots müssen nun keine Erklärungen ihrer Nutzer mehr einholen und auch keinen verschlüsselten Zugang anbieten. Abmahnungen wegen Rechtsverletzungen der Nutzer können den Anbieter jedoch weiter treffen, denn nach bisheriger Rechtsprechung sind diese vom Haftungsprivileg nicht umfasst. Dem steht nur die unverbindliche Gesetzesbegründung entgegen. Unsicherheit wird weiter die Frage schaffen, was ein zur Unterlassung verpflichteter Anbieter denn tun soll, um erneute Rechtsverstöße über sein WLAN zu verhindern.

PKI unter Zeitdruck

Erfolge erschaffen bekanntlich Neider - und finden oft Nachahmer. So veröffentlichte die israelische Firma StartCom Ltd. am 06.06.2016 ihr Produkt StartEncrypt, das viele Ähnlichkeiten mit dem sehr erfolgreichen Projekt LetsEncrypt aufweist. Kurz darauf wurden allerdings gravierende Sicherheitsprobleme aufgedeckt, sodass der Service am 04.07.2016 wieder eingestellt wurde – vorübergehend, wie es heißt, da man aus Zeitdruck nicht ausreichend getestet habe. Ein für ein Sicherheitsunternehmen besonders peinliches Eingeständnis.

Gut gemeint

Die Volksverschlüsselungs-Software, die die Fraunhofer Gesellschaft mit Unterstützung der Deutschen Telekom am 29.06.2016 in der aktuellen Version zum Download bereit gestellt hat, um Ende-zu-Ende E-Mail-Verschlüsselung auf Grundlage von S/MIME und PGP mit kostenlosen Zertifikaten für private Endanwender tauglich zu machen, ist gar keine Verschlüsselungslösung – sie kümmert sich allein um die Erzeugung und Einbindung des Public-Private-Schlüsselpaars.

Keine ganz neue Idee: Schon Anfang der 2000er Jahre hatte TC Trustcenter kostenlose S/MIME- und PGP-Zertifikate für Privatnutzer im Angebot.

Vor allem aber kombiniert sie die Nachteile offener und geschlossener PKIs: den aufwändigen Registrierungsprozess einer jedermann offenstehenden PKI mit der Beschränkung auf „mitspielende" Kommunikationspartner wie bei einer geschlossenen PKI.

Vielleicht sollte man lieber die vereinfachte Benutzerschnittstelle der Open-Source Volksverschlüsselungs-App mit einem Open-Source E-Mail-Client wie bspw. Thunderbird kombinieren – und auf die ebenfalls kostenlosen E-Mail-Zertifikate öffentlicher Trust Center wie Comodo oder StartCom zurückgreifen.

Stand der Technik

In Gesetzten und Verträgen wird von IT-Sicherheitsmaßnahmen häufig die Erfüllung eines „Stands der Technik" gefordert. Doch welche Maßnahmen genügen diesem Kriterium? Dieser Fragestellung hat sich der TeleTrusT-Arbeitskreis Stand der Technik angenommen. Am 26.05.2016 legte er eine "Handreichung zum Stand der Technik" im Sinne des IT-Sicherheitsgesetzes vor, die im Detail aufzeigt, welche Produkte und Technologien als etabliert betrachtet werden können.

Das mit viel Engagement erstellte Dokument bietet eine recht vollständige Aufstellung und erscheint nur in einzelnen Bereichen (wie den konkreten Anforderungen an sichere Softwareentwicklung oder die Sicherheit von Web-Applikationen) ergänzungswürdig, während das Thema „Datendiode" etwas überbewertet erscheint. Dennoch eine klare Leseempfehlung.

Datenschutz-Workaround

Die Europäische Kommission hat am 12.07.2016 ihre hoch umstrittene Angemessenheitsentscheidung (Art. 25 Abs. 6 Datenschutz-Richtlinie) zur Datenübermittlung in die USA auf Basis des sog. *EU-US Privacy Shield* erlassen. Diese Antwort auf die Safe-Harbor-Entscheidung des EuGH besteht aus mehreren Regelungsdokumenten, die die EU-Kommission mit verschiedenen US-Ministerien ausgehandelt hat, darunter Datenverarbeitungsprinzipien, Schiedsverfahren, Betroffenenrechte und ein erläuternder Anhang zur Datenschutz-Rechtslage in den USA. Zentraler Mechanismus ist weiter die freiwillige Selbstzertifizierung der US-Unternehmen, die personenbezogene Daten importieren; sie unterliegt staatlicher Aufsicht und Verstöße sollen sanktioniert werden.

Die Entscheidungsbegründung geht nur auf Basis der US-Darstellungen auf die Überwachungs- und Rechtsschutzpraxis ein; eine vom EuGH geforderte eigenständige Prüfung der objektiven Rechtslage ist kaum erkennbar. Auch der Privacy Shield dürfte daher vor dem EuGH landen und der Prüfung mit hoher Wahrscheinlichkeit nicht standhalten. Wer als Rechtsgrundlage seines Datenverkehrs in die USA gerade erst Verträge mit Standardvertragsklauseln abgeschlossen hat, sollte es erst einmal dabei belassen. Allerdings werden auch diese Gegenstand eines EuGH-Verfahrens.

Lawful Access

Wie ein Damokles-Schwert schwebte seit zwei Jahren ein Gerichtsverfahren vor einem New Yorker Bezirksgericht über den US-amerikanischen Cloud-Anbietern: Die US-Regierung hatte im Rahmen eines Drogenermittlungsverfahrens eine Verfügung gegen Microsoft erwirkt, um an Daten eines E-Mail-Accounts zu gelangen, die im Microsoft-Rechenzentrum in Irland gespeichert sind. Microsoft wehrte sich mit allen juristischen Mitteln. Unterstützung erfuhren sie dabei nicht nur von anderen IT-Giganten wie AT&T, Apple, Cisco und Verizon und Bürgerrechtsorganisationen wie der Electronic Frontier Foundation (EFF) als Amicus Curiae – auch die irische Regierung schaltete sich ein. Die umstrittene Verfügung wurde nun am 14.07.2016 durch ein Bundesberufungsgericht aufgehoben. Der Stored Communications Act (SCA) von 1986, auf den sie gestützt wurde, sei im Gegenteil dazu da, Daten vor dem Zugriff des Staates zu schützen, und dies gelte auch für ausländische Server eines US-Unternehmens.

Der Microsoft-Chefjurist Brad Smith äußerte sich frenetisch. Gewonnen ist jedoch lediglich ein Kampf in der großen Schlacht um die Datenhoheit. Eine große Hürde für amerikanische SaaS-Anbieter ist aus dem Weg geräumt – aber FBI & Co. werden zweifellos weiter nach kreativen juristischen Wegen für den Datenzugriff suchen.

Secorvo News

Spätsommerseminar

Unser rundum erneuertes Seminar „IT-Sicherheit heute“ (**27.–29.09.2016**) erfreut sich großer Nachfrage – damit sind interessante Diskussionen und ein lebhafter Erfahrungsaustausch schon garantiert. Das Programm reicht von aktuellen Rechtsthemen wie dem IT-Sicherheitsgesetz oder der Datenschutz-Grundverordnung der EU bis zu einem „Hacking Day“ mit WebGoat-Workshop.

Schnell Entschlossene bekommen noch einen Platz (Programm und Online-Anmeldung).

Penetrationstests

Das Angebot von Penetrationstests erfordert eine ständige Weiterentwicklung, da sich Angriffsmethoden und Tools permanent verändern. Daher haben sich unsere Pentester der renommierten OSCP-Zertifizierung unterzogen, unseren Pentest-Werkzeugkasten weiter ausgebaut sowie typische Leistungspakete (wie die Untersuchung von Webanwendungen, der DMZ-Systeme oder des WLAN-Zugangs) geschnürt, die den Leistungsumfang transparenter machen.

Durch standardisierte Arbeitsabläufe und die Ergänzung von Einzelanalysen konnten wir die Aussagekraft unserer Berichte weiter verbessern – was den Mehrwert der Penetrationstests nochmal deutlich erhöht. Eine Übersicht unseres Pentest-Leistungsangebots finden Sie in unserem neuen Produktflyer.

Encryption as a Service (EaaS)

Wie real ist die Gefahr, sich mit einer Ransomware zu infizieren? Welche Infektionswege verwenden die Angreifer? Wie arbeitet ein solcher Verschlüsselungstrojaner? Und welche Schutzmaßnahmen helfen dagegen?

Auf diese Fragen gibt auf dem nächsten KA-IT-Si-Event am **22.09.2016** der Vortrag von Tobias Häcker (Leitwerk AG) Antworten. Er wirft einen Blick hinter die Kulissen moderner Ransomware, beleuchtet deren Funktionsweise und stellt Abwehrmaßnahmen vor. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking" – mit Blick über die Dächer von Karlsruhe. Wir freuen uns auf Ihre Anmeldung.

Veranstaltungshinweise

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

August 2016	
04.-07.08.	DEF CON 24 (DEFCON, Las Vegas/US)
07.-10.08.	16th Annual DFRWS Conference 2016 (DFRWS, Philadelphia/US)
10.-12.08.	25th USENIX Security Symposium (Usenix, Austin/US)
14.-18.08.	Crypto 2016 (IACR, Santa Barbara/US)
September 2016	
07.-08.09.	Annual Privacy Forum 2016 (ENISA, EC DG Connect, Goethe Universität, mobile business, Frankfurt)
13.-15.09.	Future Security 2016 (Fraunhofer VVS, Berlin))
19.09.	Sommerakademie des ULD Schleswig-Holstein (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel)
22.09.	EaaS – Encryption as a Service (KA-IT-Si, Karlsruhe)
26.-27.09.	D • A • CH Security (Gemeinsame Arbeitskonferenz GI, OCG, BITKOM, SI, TeleTrusT, Klagenfurt)
27.-29.09.	IT-Sicherheit heute - praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
Oktober 2016	
04.-07.10.	Java Security (Secorvo, Karlsruhe)
11.-14.10.	OWASP AppSec USA 2016 (OWASP Foundation, Washington DC/US)
18.-20.10.	it-sa 2016 (NürnbergMesse GmbH)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, 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

secorvo
security consulting

Secorvo Security News

August 2016

Digitalisierung 5.0

Die Welt wird digital. Das ist nicht neu – auch wenn es einige Menschen erst jetzt zu bemerken scheinen. Rechner bestimmen schon seit Jahrzehnten unser Leben, und vieles bekämen wir ohne sie nicht mehr hin. Vielleicht bewundern wir deshalb Michelangelos David oder Leonardos Mona Lisa, obwohl jeder mit 3D-Drucker und Smartphone selbst perfekte Abbilder der Wirklichkeit erzeugen kann.

Vor einigen Jahren hat jedoch eine neue Phase begonnen, die weit über das „Internet der Dinge“ und „Industrie 4.0“ hinausweist. Ich will sie „Digitalisierung 5.0“ nennen. Es ist eine Phase der Selbstbezüglichkeit: Computer beginnen, sich selbst zu gestalten. Und es ist die IT-Sicherheit, die diese Entwicklung befeuert. So akzeptieren wir (wenn auch nicht immer klaglos), dass unsere Rechner sich via Virenscanner ständig selbst untersuchen, eigenständig die Signaturdatenbank aktualisieren und unsere E-Mails von Spam befreien. Programm- und Betriebssystem-Updates erfolgen inzwischen ohne Freigabe der Benutzer, die Suche nach Programmfehlern übernehmen automatisierte Prozesse und Tools – nicht nur bei Softwareentwicklern, sondern auch als Cloud-Service. Längst arbeiten Angreifer mit Systemen, die systematisch Exploits durchprobieren, kombinieren – und die Zielsysteme sogar auf noch unbekannte Schwachstellen abklopfen. Die Antwort heißt IDS oder SIEM: die automatische Analyse von Netzverkehr und Log-Dateien auf Angriffsspuren.

Nicht mehr lange, und unsere Rechner nehmen sich in Quarantäne, säubern sich gegenseitig von Schadsoftware und setzen sich neu auf. Sie werden ihre Erfahrungen anderen Rechnern über Wissensdatenbanken zugänglich machen, ihre Leistungen womöglich in selbst „geschürften“ Bitcoin bezahlen und die robustesten Kollegen zu Entscheidern wählen. Nutzen könnte man sie wahrscheinlich nicht mehr – wozu aber auch: Schließlich brauchen die Rechner uns, damit wir gelegentlich defekte Festplatten ersetzen oder das RAM erweitern.

Inhalt

secorvo
security consulting

Security News

Abgehörte Tastaturen

In ihrer Veröffentlichung zum KeySniffer-Hack vom 27.07.2016 zeigen die Forscher von Bastille, was sich mit Angriffen wie MouseJack und Keysweeper bereits abzeichnete: Zahlreiche kabellose Tastaturen und Mäuse bekannter Hersteller wie HP oder Toshiba aber auch Logitech und Microsoft sind für das Abhören oder die Injektion von Tastatureingaben anfällig. Angreifer können so an Passwörter oder Kreditkartennummern gelangen oder sogar das Zielsystem übernehmen.

Die Schwachstelle liegt bei den Herstellern der betroffenen Geräte, die eigene Übertragungsprotokolle und Sicherheitsmechanismen entwickelten anstatt auf bewährte Standards zu setzen. Mit einer Behebung der Schwachstelle ist eher nicht zu rechnen, da ein Einspielen neuer Firmware in die Dongles und Eingabegeräte nicht möglich ist oder der Aufwand von den Herstellern als zu hoch eingeschätzt wird.

Grundsätzlich sind kabelgebundene Tastaturen und Mäuse kabellosen Geräten vorzuziehen. Muss es dennoch eine kabellose Variante sein, so sollte man auf den Bluetooth-Standard setzen, der ein sicheres Kommunikationsprotokoll verwendet, das Authentifikation und Verschlüsselung umfasst.

Leitfaden zum EU-U.S. Privacy Shield

Seit dem 01.08.2016 liegt der EU-U.S. Privacy Shield als Garantie angemessenen Datenschutzes für U.S.-Unternehmen vor. Begleitend hat die EU-Kommission einen Leitfaden für Betroffene zu den Rechten aus den Privacy Shield Principles veröffentlicht.

Darin werden die Verpflichtungen von Privacy-Shield-Unternehmen, die diesbezüglichen Betroffenenrechte, die Beschwerderechte, die möglichen Adressaten sowie der für den gesamten EU-U.S.-Datenverkehr anwendbare Ombudsmann-Mechanismus ausführlich erläutert.

Eine Beschwerde kann an die verarbeitende U.S.-Gesellschaft, an eine von dieser einzusetzenden unabhängigen Beschwerdestelle und an die nationale Aufsichtsbehörde beim Department of Commerce oder der Federal Trade Commission gerichtet werden. Arbeitnehmer können sich stets an die nationale Aufsichtsbehörde wenden.

Scheitert eine Beschwerde, kann ein Schiedsverfahren verlangt werden. Dieses findet in den USA statt. Es besteht aber ein Recht auf Hilfestellung durch die nationale Aufsichtsbehörde, die Möglichkeit, per Videokonferenz teilzunehmen und ein Recht auf kostenlose Übersetzungen. Die Kosten werden von einem Fonds getragen.

Der vorerst nur in englischer Sprache verfügbare Leitfaden bietet datenschutzkundigen Betroffenen eine gelungene Übersicht über die grundsätzlichen Möglichkeiten. Er dokumentiert aber auch, dass der praktische Nutzen des Privacy Shields für einen einzelnen Betroffenen nur sehr schwer realisierbar sein dürfte.

IT-Grundschutz-Modernisierung

Am 08.08.2016 hat das BSI den Entwurf für einen modernisierten Baustein der IT-Grundschutzkataloge veröffentlicht. Ein weiterer Baustein folgte am 09.08.2016. Die wesentliche Neuerung ist, dass bei den modernisierten Bausteinen deutlich zwischen einem Anforderungsteil und sogenannten Umsetzungshinweisen unterschieden wird. Letztere weisen einen höheren Detaillierungsgrad auf als die eigentlichen Bausteine und ähneln den bisherigen Katalogen, stellen jedoch nur noch eine Möglichkeit zur Umsetzung dar.

Die neuen Bausteine stellen nun in kompakter Form die Vorgaben zusammen. Auf eine umfassende Gefährdungsdarstellung wurde verzichtet; die wesentlichen Maßnahmen, die aus Grundschutz-Sicht umgesetzt werden müssen, sind übersichtlich auf wenigen Seiten aufgeführt. Aus unserer Sicht eine deutliche Flexibilisierung und der richtige Weg, um die Umsetzung von IT-Grundschutz in der Praxis handhabbarer zu machen.

Vorratsdatenspeicherung revisited

Der Generalanwalt am Europäischen Gerichtshof hat am 19.07.2016 seine Schlussanträge in zwei verbundenen Rechtssachen zu nationalen Vorratsdatenspeicherungsregelungen gestellt.

Bereits 2014 hat der EuGH im Verfahren Digital Rights Ireland Ltd die Richtlinie zur Vorratsdatenspeicherung für ungültig erklärt. Die deutsche Umsetzung in § 113a ff. TKG a.F. war zuvor schon vom Bundesverfassungsgericht für verfassungswidrig erklärt worden (seit Dezember 2015 ist eine bis 2017 umzusetzende Nachfolgeregelung in Kraft).

In seinen Schlussanträgen leitet der Generalanwalt aus der Grundrechtscharta der Europäischen Union strenge Anforderungen an nationale Pflichten zur Vorratsdatenspeicherung ab. Sie dürfe nur der Bekämpfung schwerer Kriminalität dienen und müsse hierfür absolut notwendig sein. Die Anforderungen an den Schutz der Daten des vorausgegangenen Urteils müssten erfüllt und die mit der Vorratsdatenspeicherung verbundenen Gefahren dürften nicht unverhältnismäßig zu ihrem Nutzen sein.

Sollte der EuGH dem Antrag folgen, bleibt eine verfassungsgemäße Vorratsdatenspeicherung möglich. Der Nachweis der Verhältnismäßigkeit vor nationalen Gerichten wird aber angesichts vorliegender Studien schwierig. Den Vorschlägen des deutschen Innenministeriums, die Vorratsdatenspeicherung zu reanimieren und auf Telemedien auszudehnen, dürfte das Urteil jedoch einen Dämpfer setzen.

BSI-Zertifizierung nach TR

Mit der ISO 27001-Zertifizierung auf Basis von IT-Grundschutz darf man die am 12.08.2016 vorgestellte Zertifizierung nach TR in Verbindung mit ISO 27001 nicht verwechseln: Hier geht es, aufbauend auf einer ISMS-Zertifizierung nach ISO 27001, um die Zertifizierung konkreter, in den Technischen Richtlinien (TR) des BSI definierten Maßnahmen für ganz bestimmte Einsatzzwecke. In Vorbereitung ist derzeit eine Zertifizierung nach TR-03108 Secure E-Mail Transport für E-Mail-Provider.

Wir haben Ihren PC aktualisiert

Seit dem 02.08.2016 verteilt Microsoft das drei Gigabyte große Anniversary Update, mit dem die Strategie des „Windows as a Service" fortgesetzt wird: Jeder Windows-Nutzer soll stets die aktuellste Version des Betriebssystems verwenden – Apple lässt grüßen. Home-User können diesen „Service" nicht verweigern.

Neben einigen optischen und funktionalen Anpassungen sowie dem nachhaltigen Aushebeln von Secure Boot, holt das Thema Datenschutz mal wieder Microsoft ein (vgl. SSN 8/2015). Die US-Bürgerrechtsorganisation EFF sowie die französische Datenschutzaufsicht CNIL kritisieren Microsoft deutlich. Im Zentrum steht das Windows-Assistenzsystem Cortana, das nun zur Standardsuche in Windows 10 wird – bislang konnte man es deaktivieren. Cortana ist sehr kommunikativ: Es überträgt zahlreiche persönliche Informationen an Microsoft, darunter den Standort, Text-, Sprach- und Touch-Eingaben, Webseitenbesuche sowie Nutzungsstatistiken. Details zu den übertragenen Telemetriedaten sind bisher nicht bekannt. Firmenkunden können Cortana immerhin per GPO abschalten, Home-User müssen dafür zu regedit greifen. Da wünscht man sich glatt Karl Klammer zurück – der war zwar nervig, aber wenigstens verschwiegen.

Nach erfolgreichem Update wird man von seinem aufgefrischten Windows mit „Hallo. Wir haben Ihren PC aktualisiert." begrüßt. Besser lässt sich der Hoheitsverlust über den eigenen Rechner nicht zusammenfassen - Realsatire as a Service.

Secorvo News

PKI Check-up

In den vergangenen Jahren haben viele Unternehmen und Organisationen interne Public-Key-Infrastrukturen (PKI) aufgebaut. Viele Betreiber fragen sich jedoch, ob ihre PKI noch angemessen sicher, praxistauglich und für künftige Herausforderungen gerüstet ist. Als Abhilfe hat Secorvo daher einen PKI Check-up entwickelt, der PKI-Prozesse, -Architektur und -Dokumentation an bewährten Best Practices und Standards misst, bewertet und Optimierungspotenzial aufzeigt.

Fast ausgebucht

Noch drei letzte freie Plätze gibt es auf unserem rundum erneuerten Seminar „IT-Sicherheit heute" (**27.–29.09.2016**). Das Programm reicht von aktuellen Rechtsthemen wie dem IT-Sicherheitsgesetz und der Datenschutz-Grundverordnung bis zu einem „Hacking Day" mit WebGoat-Workshop – und ist als Weiterbildung zur T.I.S.P.-Re-Zertifizierung anerkannt. Schnell Entschlossene erwischen noch einen Platz (Programm und Online-Anmeldung).

Zertifikate

Im November (**21.–25.11.2016**) bieten wir die nächste Möglichkeit zur T.I.S.P.-Zertifizierung. Nach Ihrer Anmeldung erhalten Sie, frühzeitig vor Seminarbeginn, unser T.I.S.P.-Buch zur Vorbereitung: ein systematischer Zugang zur Informationssicherheit in 26 Kapiteln auf 700 Seiten, verfasst von Experten für Experten.

Software-Architekten und -Entwickler bereiten wir im Oktober (**24.–27.10.2016**) auf die Zertifizierung zum *Certified Professional for Secure Software Engineering* (CPSSE) vor. Auch hier empfehlen wir eine frühzeitige Anmeldung.

Cloud Encryption

Wie real ist die Gefahr, sich mit einer „Ransomware" zu infizieren? Welche Infektionswege verwenden die Angreifer? Wie arbeitet ein solcher Verschlüsselungstrojaner? Und welche technischen und organisatorischen Schutzmaßnahmen wirken dagegen? Auf diese Fragen gibt am **22.09.2016** ab 18 Uhr Tobias Häcker (Leitwerk AG) im Rahmen des nächsten KA-IT-Si-Events im Panoramasaal der IHK Karlsruhe Antworten und wirft einen Blick hinter die Kulissen aktueller Erpressungstrojaner. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" – mit Blick über die Dächer von Karlsruhe.

Wir freuen uns auf Ihre Anmeldung.

Veranstaltungshinweise

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

September 2016	
07.-08.09.	Annual Privacy Forum 2016 (ENISA, EC DG Connect, Goethe Universität, mobile business, Frankfurt)
19.09.	Sommerakademie des ULD Schleswig-Holstein (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel)
22.09.	EaaS – Encryption as a Service (KA-IT-Si, Karlsruhe)
26.-27.09.	D • A • CH Security (Gemeinsame Arbeitskonferenz GI, OCG, BITKOM, SI, TeleTrusT, Klagenfurt/AT)
26.-30.09.	Informatik 2016 (Gesellschaft für Informatik, Klagenfurt/AT)
27.-29.09.	IT-Sicherheit heute – praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
Oktober 2016	
04.10.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
11.-14.10.	OWASP AppSec USA 2016 (OWASP Foundation, Washington DC/US)
18.-20.10.	it-sa 2016 (NürnbergMesse GmbH)
19.10.	Swiss Cyber Storm 6 (Swiss Cyber Storm Association, Luzern/CH)
24.-27.10.	CPSSE – Certified Professional for Secure Software Engineering (Secorvo, Karlsruhe)
24.-28.10.	Conference on Computer and Communications Security (CCS) (CASED/Fraunhofer SIT, Wien/AT)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, 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

secorvo
security consulting

Secorvo Security News

September 2016

Die Tür

Wer in den vergangenen Jahren die Nachrichten verfolgt, dem drängt sich leicht der Eindruck auf, dass gegen alle diese Cracks – ob in staatlichem Auftrag, aus krimineller Motivation oder schlichtem Spieltrieb – einfach kein Kraut gewachsen ist. Warum also überhaupt diesen ganzen Aufwand treiben? Wieso nicht einfach alle Daten in die billigste Cloud verlegen, jede hilfreiche App auf das preisgünstigste Smartphone laden – und das gesparte Geld statt in Schutzmaßnahmen in Aktien investieren? Wenn der Datengau ohnehin früher oder später jeden trifft, dann hat man bis dahin wenigstens am Vermögen gearbeitet... So ähnlich klang kürzlich der Fatalismus zwischen den Zeilen eines Gesprächspartners, dem der Schreck über einige von mir vorgestellten Angriffswege noch anzusehen war.

Da kam mir eine Geschichte in Sinn, die schon einige Jahre zurückliegt. Bei unseren Nachbarn war eingebrochen worden – am hellichten Tag, mit nicht mehr als einem langen Schraubenzieher als Hebel. Es wurde wenig entwendet, aber der Schock saß tief.

Unvermeidlich unterzog ich unsere Haustür einem kritischen Blick – und musste feststellen, dass auch sie einem solchen Angriff nicht standgehalten hätte. Also holte ich mir Rat bei einem erfahrenen Kriminalisten. Der besah sich die Tür und beäugte mich amüsiert, als ich ihn fragte, was ich tun müsste, um so einen Einbruch zu verhindern. Falsche Frage, meinte er: „Es geht nicht darum, *ob* jemand einbrechen kann – sondern *wie lange* er dafür braucht." Genau das sei der Punkt. Jede Tür ließe sich öffnen – oft mit überraschend wenig Aufwand, und wenn es sein muss, mit schwerem Gerät. Entscheidend sei der Aufwand: Je mehr Zeit ein Einbrecher benötige und je mehr Lärm er verursache, desto größer sei die Entdeckungsgefahr. Wie bei der IT-Sicherheit: Je aufwändiger und langwieriger ein Angriff, desto höher Kosten und Risiko. Darum helfen Schutzmaßnahmen – gegen Einbrecher ebenso wie gegen Cracker.

Inhalt

secorvo
security consulting

Security News

Flüsterangriff auf Smartphones

Auf dem diesjährigen 25th USENIX Security Symposium wurde am 11.08.2016 ein unkonventioneller Angriff auf Smartphones vorgestellt: Ein Smartphone mit aktivierter Spracherkennung lässt sich von für ein menschliches Ohr unverständlichen Sprachbefehlen steuern. Denn die Geräuschfilterung ist erstaunlicherweise so gut, dass ein Smartphone manche Befehle wie "Öffne URL xyz" erkennt und ausführt, während der Besitzer dies aufgrund von Umgebungsgeräuschen nicht mitbekommt. Bei Tests wurde ein verschleiertes "OK Google" zu 95% vom Smartphone, aber nur von 22% der Probanden verstanden.

Einige Beispiele solcher „Hidden Voice Commands" für Android-Smartphones haben die Autoren auf ihrer Webseite zusammengestellt. Dort finden sich auch Tests, bei denen den Forschern Details zum Spracherkennungssystem vorlagen. Wer sicher gehen möchte, dass sein Smartphone keine Fremdsteuerung ermöglicht, sollte die Sprachsteuerung deaktivieren – oder zumindest so konfigurieren, dass sie im gesperrten Zustand nicht reagiert.

Hacker-Stecker

Ein einheitlicher Micro-USB-Stecker ist bei Smartphones (bis auf wenige Ausnahmen) mittlerweile Standard – und ab 2017 gesetzlich vorgeschrieben. Neben dem Laden des Akkus und dem Datenaustausch mit einem Computer bietet der Anschluss dank OTG meist nahezu die gleichen Möglichkeiten wie jeder USB-Port eines Computers. Durch den immer größeren Funktionsumfang der Schnittstelle entstehen jedoch auch neue Angriffsflächen, wie Brian Markus auf der Hacking-Konferenz DEF Con vom 04. bis 07.08.2016 demonstrierte. Bei seinem als „VideoJacking" bezeichneten Angriff wird ein externer Monitor oder ein Aufnahmegerät über einen Splitter mit dem Ladekabel verbunden. Darüber kann das auf dem Smartphone angezeigte Bild gespiegelt und abgegriffen werden. Betroffen sind alle mit dem Feature *Mobile High-Definition Link* (MHL) ausgestatteten Smartphones.

Für einen Nutzer ist grundsätzlich nicht ersichtlich, ob das über den Micro-USB-Port angeschlossene Gerät auch das ist, was es zu sein vorgibt. Fremde Ladegeräte sollten daher gar nicht oder nur mit einer dazwischen gesteckten Datenaustauschsperre (wie z. B. dem USB-Kondom) genutzt werden.

WLAN-Haftung

Der rechtliche Rahmen für Hotspots und Gäste-WLANs ist seit langem umstritten und mit großer Unsicherheit behaftet. Nach dem Vorstoß des deutschen Gesetzgebers (siehe SSN 7/2016) hat nun der EuGH am 15.09. 2016 sein Urteil im Fall Tobias McFadden ./. Sony Music verkündet. Der Beklagte hatte in seinen Verkaufsräumen ein ungesichertes WLAN betrieben und sich anlässlich einer Abmahnung von Sony wegen einer Urheberrechtsverletzung auf Art. 12 der Richtlinie 2000/31/EG und deren deutsche Umsetzung in § 8 TMG (das „Providerprivileg") berufen. Der EuGH hat nun entschieden, dass eine Schadensersatzhaftung des Anbieters gegen die Richtlinie verstoße und von dem Anbieter keine über die Richtlinie hinaus gehenden Maßnahmen verlangt werden dürften. Der Anbieter könne aber auf Unterlassung in Anspruch genommen werden und müsse hierfür die Kosten tragen. Er dürfe zum Schutz des WLANs durch ein Passwort und zur Nutzeridentifikation verpflichtet werden.

Die (ohnehin voreilige) Euphorie über den neuen § 8 Abs. 3 TMG dürfte damit verflogen sein. Die Richtlinie lässt die Störerhaftung in Art. 12 Abs. 3 ausdrücklich zu, das Urteil ist daher nachvollziehbar. Passwortschutz und Identifikation alleine reichen jedoch zur Umsetzung des Unterlassungsanspruchs nicht aus, daher hat das Urteil nicht zur Klarheit über die tatsächlichen Pflichten des Anbieters beigetragen – ein weiteres in der langen Reihe unglücklicher WLAN-Entscheidungen.

IoT-Krypto-Camouflage

Am 06.09.2016 veröffentlichte das Unternehmen SEC Consult eine Untersuchung der Sicherheit der Implementierung kryptographischer Verfahren in IoT-Geräten. Schon im November 2015 war SEC Consult in eine Studie zu dem Ergebnis gekommen, dass die Verwendung von privaten Schlüsseln in verbreiteten Geräten bei weitem nicht dem Stand der Technik entspricht. Die aktuellen Ergebnisse legen nahe, dass sich die Situation in den vergangenen neun Monaten eher verschlimmert hat. Vielfach erlauben falsch verwendete Schlüssel und Zertifikate Zugriff auf Geräte oder vertrauliche Informationen. Betroffene Schlüssel und Zertifikate wurden inzwischen auf Github veröffentlicht; darunter finden sich auch einige Schlüssel von AVM Fritzboxen. Auf die offizielle Meldung des US CERTs reagierte offenbar bisher fast keines der betroffenen Unternehmen. Der Kauf von billiger Kryptographie kann die Nutzer also teuer zu stehen kommen.

OPM-Hack

Fast wie ein Krimi lesen sich die 217 Seiten des am 07.09.2016 veröffentlichten offiziellen Untersuchungsberichts mit dem prägnanten Titel „The OPM

Data Breach: How the Government Jeopardized Our National Security for More than a Generation“ zu den Angriffen auf das *U.S. Office of Personnel Management* (OPM) in den Jahren 2014 und 2015, bei denen sehr persönliche Daten aus Sicherheitsüberprüfungen, darunter auch Fingerabdrücke, von mehr als 21,5 Millionen Amerikanern entwendet wurden. Das OPM war Ende 2014 als die Behörde mit den schwächsten Authentifikationsverfahren gerügt worden und betrieb zentrale Server (die später kompromittiert wurden) vorschriftswidrig ohne Security Assessment. Bereits im März 2014 war das OPM vom US-CERT auf einen Hackerangriff hingewiesen worden; die Aktivitäten des Hackers wurden vom OPM jedoch lediglich über zwei Monate beobachtet. Mangelhafte Schutzmaßnahmen, unvollständige Logs und unangemessene Reaktionen sieht der Bericht als Ursachen des (verhinderbaren) Datenabzugs. Ein abschreckendes Beispiel für falsche Prioritätensetzung beim Umgang mit Informationssicherheit.

Smart-Meter-Regulierung

Am 01.09.2016 ist das am 08.07.2016 vom Bundesrat verabschiedete Gesetz zur Digitalisierung der Energiewende im Bundesgesetzblatt veröffentlicht worden und am 02.09.2016 in Kraft getreten. Kernstück ist das ‚Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen‘ (Messstellenbetriebsgesetz – MsbG). Es regelt den Übergang zu modernen Messstellen in zukünftigen Energienetzen.

Technische Vorgaben an die Datensicherheit werden in den §§ 19 ff. MsbG geregelt. Konkrete Anforderungen an Interoperabilität und Anbindungssicherheit vor allem der Smart-Meter-Gateways finden sich in bereits vorliegenden technischen Richtlinien. Die Erfüllung der Anforderungen durch die Geräte ist mit einer Zertifizierung nachzuweisen. Nicht den Anforderungen entsprechende Geräte dürfen nur noch bis Ende 2016 verbaut und anschließend maximal acht Jahre genutzt werden.

Die Datenerhebung und –verarbeitung wird umfangreich in 25 Paragraphen (§§ 49 ff. MsbG) geregelt, darunter finden sich auch Löschpflichten und sogar konkrete Löschfristen. Die aus Datenschutz- und Datensicherheitsanforderungen resultierenden Umsetzungspflichten sind komplex und umfangreich; sie werden von Herstellern und Betreibern mehr als einen Blick über den Tellerrand erfordern, um den Zertifizierungsanforderungen genügen zu können.

Secorvo News

Von und für Experten

Vierzig Jahre liegt die wegweisende Veröffentlichung von Whitfield Diffie und Martin E. Hellman („New Directions in Cryptography“) inzwischen zurück – und noch immer sind Aufbau und Betrieb einer PKI eine Herausforderung. Wie so oft liegt der Teufel in den Details – Zertifikatsgültigkeiten, Key Usage, Prozesse und Policies sind geeignet festzulegen und umzusetzen. Wie das geht, zeigen wir in Theorie und Praxis auf unserem PKI-Seminar vom **14. bis 17.11.2016** (Programm und Anmeldung).

Bis Mitte des Jahres 2016 wurden 850 T.I.S.P.-Zertifikate ausgestellt. Sofern Sie drei Jahre Berufserfahrung im Gebiet Informationssicherheit mitbringen, können Sie noch in diesem Jahr Teil dieser schnell wachsenden Experten-Community der *Information Security Professionals* werden: Vom **21. bis 25.11.2016** findet in Karlsruhe die nächste T.I.S.P.-Schulung mit anschließender Zertifikatsprüfung statt, durchgeführt von den Autoren des T.I.S.P.-Buchs (detaillierte Agenda und Online-Anmeldung).

Live Hacking

Kaum etwas ist wirkungsvoller als die Anschauung – das gilt auch für die IT-Sicherheit. Daher haben wir in den vergangenen Monaten zahlreiche Live-Hacking-Vorführungen entwickelt, die verbreite Einfallstore zeigen. Alle Live Hacks kommen ohne „Hokuspokus“ wie Spezialversionen einer anfälligen Soft- oder Hardware aus; gezeigt wird, was ohne größere Investitionen in die Ausrüstung heute möglich ist. Wenn Sie einen solchen Live Hack buchen möchten, nehmen Sie bitte mit uns Kontakt auf.

IT-Grundschutz-Zertifizierung

Zertifizierung eines großen Rechenzentrums – nach IT-Grundschutz? Kann das mit vertretbarem Aufwand und in überschaubarer Zeit funktionieren? Sascha Grund, IT Compliance Manager der Globalways AG, stellt auf dem kommenden KA-IT-Si Event am **10.11.2016, 18 Uhr** in den Räumen des CyberForum e.V. vor, dass und wie das geht – und gibt praktische Tipps zur Umsetzung.

Im Anschluss an den Vortrag haben Sie wie gewohnt die Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“. Anmeldung und weitere Informationen unter www.ka-it-si.de.

Veranstaltungshinweise

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

Oktober 2016	
04.10.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
11.-14.10.	OWASP AppSec USA 2016 (OWASP Foundation, Washington DC/US)
18.-20.10.	it-sa 2016 (NürnbergMesse GmbH)
19.10.	Swiss Cyber Storm 6 (Swiss Cyber Storm Association, Luzern/CH)
26.-28.10.	IDACON 2016 (WEKA-Akademie, München)
November 2016	
01.-04.11.	Black Hat Europe 2016 (Blackhat, London/UK)
08.-11.11.	DeepSec In-Depth Security Conference 2016 Europe (DeepSec, Wien/AT)
10.11.	IT-Grundschutz-Zertifizierung (KA-IT-Si, Karlsruhe)
10.-11.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
14.-17.11.	PKI (Secorvo, Karlsruhe)
17.-18.11.	40. DAFTA (GDD, Köln)
21.-25.11.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Fundsache

Die 40seitige Publikation „Offenes Geheimnis – Mythen und Fakten zu Überwachung und digitaler Selbstverteidigung“ der Rosa Luxemburg Stiftung gibt eine Übersicht über Hintergründe und Schutzmöglichkeiten für Endanwender.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp.

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

secorvo
security consulting

Secorvo Security News

Oktober 2016

Freiwillige Cyberwehr

Es ist kein guter Stil, Salz in offene Wunden zu streuen. DIE ZEIT und netzpolitik.org haben sich bereits ausführlich über die freiwillige Cyberwehr ausgelassen, und via Twitter wurde das BSI mit Spott übergossen. Doch das Thema ist zu wichtig, um es unkommentiert zu lassen. Worum also geht es?

Bereits Anfang Juni 2016 wurde bekannt, dass das BSI ein 20-köpfiges „Mobile Incident Response Team" aufbauen will, das ab 2017 Betreiber kritischer Infrastrukturen bei einem IT-Sicherheitsvorfall unterstützen soll. So weit, so gut. Offenbar bekam das BSI nun jedoch Respekt vor der eigenen Courage und entwarf rasch eine Kooperationsvereinbarung für eine „freiwillige Cyberwehr", die Anfang Oktober publik wurde. Das Konzept: Kooperierende Unternehmen stellen eigene Fachkräfte für IT-Sicherheit ab, die bei einem IT-Sicherheitsvorfall der „Cyberwehr" des BSI unterstellt werden und bis zu drei Tage Soforthilfe leisten. Die Unternehmen sichern ein vom BSI abrufbares Einsatzkontingent von jeweils bis zu 20 Personentagen jährlich (zuzüglich Reisekosten, Übungen und Fortbildungen) zu – unentgeltlich, versteht sich – und besetzen eine rund um die Uhr erreichbare Kontaktstelle für die Alarmierung.

Eine wenig beruhigende Vorstellung: IT-Sicherheitsvorfälle in kritischen Infrastrukturen werden zukünftig von einer bunten, auf Zuruf zusammengetrommelten Truppe freiwilliger Cybercops unter BSI-Leitung bekämpft. Sieht man einmal von der Frage ab, ob Unternehmen bereit sein werden, ihre hoch bezahlten Fachkräfte für solche Einsätze abzustellen – professionell klingt das nicht.

Wollte man Schäden wirksam begrenzen und den Umgang mit Vorfällen professionalisieren, müsste den immer ausgefeilteren Angriffsmethoden eine intensiv trainierte, hoch kompetente und eingespielte schnelle Eingreiftruppe gegenüberstehen. Wer schon einmal eine IT-Notfallübung durchgeführt hat, weiß, dass es dabei mit drei Tagen „Schlauch draufhalten" nicht getan ist. SEKs sind schließlich auch keine spontan einberufenen Grisu-Teams.

Inhalt

secorvo
security consulting

Security News

Risikomanagement erneuert

Am 19.10.2016 hat das BSI die "Community Draft"-Version des neuen Risikomanagement-Standards 200-3 veröffentlicht. Die reichlich formale und in der Praxis selten hilfreiche Vorgehensweise des Vorgängers 100-3 wurde erheblich überarbeitet.

Zum einen wurden die noch als Ergänzung zum 100-3 definierten ‚Elementaren Gefährdungen' nun als wesentliche Komponente für Risikoanalysen integriert, ein für die Praxis durchaus sinnvoller Schritt. Zum anderen ist nun ein kompletter Prozess für das Risikomanagement von Informationssicherheitsrisiken beschrieben. Und der rockt. Praxistauglich, pragmatisch und, wenn man noch die Beispiele kürzt und den nicht wirklich belastbaren Begriff der Eintrittswahrscheinlichkeit durch eine (subjektive) Wahrscheinlichkeitseinschätzung ersetzt, ein wirklich brauchbares Grundlagenwerk. Ein kleiner Schritt in der Versionsnummer, aber ein großer Schritt in Richtung praktikablen IT-Grundschutzes.

Datenübermittlung auf der Kippe

Wer glaubt, mit dem EU-U.S. Privacy Shield (SSN 07/2016, 08/2016) sei der Datentransfer außerhalb der EU wieder in trockenen Tüchern, der wiegt sich in trügerischer Sicherheit. Nach dem erfolgreichen Vorgehen gegen Facebooks Datenübermittlung auf Basis von Safe Harbor hat Max Schrems im Mai 2016 auch die Prüfung EU-Standardvertragsklauseln bei der zuständigen irischen Datenschutzbeauftragten (DPC) initiiert. Diese Klauseln dienen als Rechtsgrundlage einer Datenübermittlung in jedes Drittland (nicht nur den USA) und werden vielerorts als „bessere Alternative" zu Safe Harbor verstanden. Am 28.09.2016 informierte die DPC über den Verfahrensstand: Nach ihrer Überzeugung verstoßen die Klauseln gegen europäisches Recht, denn EU-Bürgern stehen in den USA keine wirksamen Rechtsbehelfe zur Verfügung. Die Argumentation stützt sich auf die Entscheidungsgründe im Safe-Harbor-Urteil des EuGH.

Anfang 2017 wird der Austausch mit dem High Court abgeschlossen sein – und dieser kann kaum etwas anderes tun, als die Frage nach der Rechtmäßigkeit der Klauseln dem EuGH vorzulegen. Folgt dieser seinen eigenen Argumenten, wird er die Standardvertragsklauseln für unwirksam erklären. Damit bliebe für die Datenübermittlung in die USA nur noch der Privacy Shield, den die europäischen Datenschutz-Aufsichtsbehörden zunächst auf ein Jahr befristet beobachten wollen, um dann zu entscheiden, ob sie ihn als rechtmäßig ansehen.

Unendliche Geschichte

Mit seinem Urteil in Sachen Breyer ./. BRD hat der EuGH dem alten Streit um den Personenbezug der IP-Adresse am 19.10.2016 ein neues Kapitel hinzugefügt. Einerseits wird der Personenbezug dynamischer IP-Adressen erneut bejaht, wenn auch nicht uneingeschränkt. Daneben wurde die Frage, ob die Protokollierung von Webseitenzugriffen zu Sicherheitszwecken zulässig ist, gegen die in Deutschland herrschende Meinung entschieden: Nach Auffassung des EuGH ist sie regelmäßig erlaubt.

An der IP-Adresse entzündet sich immer wieder der Streit um ein objektives oder relatives Verständnis der Personenbeziehbarkeit: Reicht es, dass ein Dritter den Betroffenen ermitteln kann oder muss dies dem Dateninhaber selbst möglich sein?

Der EuGH sieht die Personenbeziehbarkeit auch gegeben, wenn der Dateninhaber die Zuordnung nicht allein vornehmen kann, aber die rechtliche Möglichkeit hat, die Zuordnungsdaten zu erlangen. Das ist im Umkehrschluss ein Brückenschlag zur „relativen Theorie". Außerdem stünde die RL 95/46/EG einer Regelung entgegen, die eine Datenverarbeitung ohne jegliche Abwägungsmöglichkeit kategorisch verbiete. Beide Aussagen gehen deutlich über das Telemediengesetz hinaus. Mit der Öffnung zur relativen Theorie sind beispielsweise Pseudonyme rechtlich neu zu bewerten. Die neue Entscheidungslage hat jedoch ein Verfallsdatum, denn mit der Datenschutz-Grundverordnung entfallen ab Mai 2018 wesentliche Teile der Wortlautargumente des EuGH – und der Streit wird wohl von vorne beginnen.

6. Deutscher IT-Sicherheitspreis

Der „Deutsche IT-Sicherheitspreis", gestiftet von Dr. Horst Görtz, dem Gründer des ersten großen deutschen IT-Sicherheitsunternehmens, zeichnet seit 2006 alle zwei Jahre drei herausragende Entwicklungen im Gebiet der IT-Sicherheit aus. Mit einem Preisgeld von insgesamt 200.000 € ist dies einer der höchsten privat gestifteten Preise in Deutschland. Am 06.10.2016 wurden in Darmstadt die diesjährigen Gewinner ausgezeichnet. Den ersten Preis erhielt die Analysesoftware Harvester der Forschungsgruppe um Professor Eric Bodden, die eine Schadsoftwareerkennung auch in obfuskierten Android-Apps erlaubt. Preis zwei ging an die Plattform Octopus zur Schwachstellensuche der Forschungsgruppe um Professor Konrad Rieck, die mit Methoden des Pattern Matching und des maschinellen Lernens beeindruckende Analyseerfolge mit einer Minimalzahl an „False Positives" vorweisen kann. Ein deutliches Signal, welcher Stellenwert der

Bekämpfung von Schadsoftware und Schwachstellen inzwischen eingeräumt wird – und welche überraschende Fortschritte in diesem Bereich noch möglich sind.

Microsoft Edge-VM

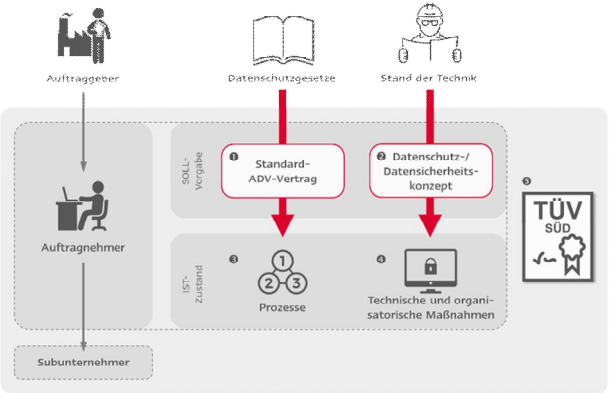
Microsoft plant, den Microsoft-Internetbrowser Edge in der nächsten Version von Windows 10 in eine virtuelle Umgebung zu verfrachten. Die *Windows Defender Application Guard* genannte Technologie startet beim Aufruf von nicht vertrauenswürdigen Seiten eine schlanke virtuelle Windows-Instanz, in welcher der Browser selbst bei infizierten Webseiten Angriffsmöglichkeiten auf das eigentliche Betriebssystem und die Benutzerdaten unterbindet. Im Intranet wird Edge „ganz normal" gestartet und kann auch auf die internen Daten zugreifen. Ein viel versprechender Ansatz, den Zugriff auf Webseiten sicherer zu machen.

Secorvo News

Das Standard-ADV-Modell

Wie lassen sich Auftragsdatenverarbeiter systematisch und kontinuierlich, zugleich aber effizient und effektiv auf die wirksame Umsetzung geeigneter technischer und organisatorischer Maßnahmen (TOM) zum Schutz der verarbeiteten personenbezogenen Daten prüfen? Die Verantwortung für die Verarbeitung liegt beim Auftraggeber: Er muss regelmäßig prüfen, ob geeignete Maßnahmen zu deren Schutz getroffen wurden und die gesetzlichen Anforderungen erfüllt sind.

Eine Zertifizierung kann aufwändige Einzelprüfungen durch ein standardisiertes Verfahren ersetzen. Doch warum hat sich bisher kein Standard etabliert? Genau mit dieser Frage haben sich Secorvo und der TÜV SÜD beschäftigt. Daraus ist das Standard-ADV-Modell mit Zertifizierung entstanden, das Auftragnehmer von Auftragsdatenverarbeitungen beim Nachweis der Eignung und Angemessenheit der getroffenen Maßnahmen gegenüber ihren Auftraggebern mit dem Prüfzeichen und Zertifikat „Zertifizierte Auftragsdatenverarbeitung" unterstützt. Mit einer nach wenigen Monaten bereits zweistelligen Zahl erfolgreicher Zertifizierungen könnte das Konzept ein Erfolgsmodell werden.



Eine ausführliche Darstellung des Modells und des Zertifizierungsverfahrens haben Christoph Schäfer und Dirk Fox in Ausgabe 11/2016 der Fachzeitschrift DuD veröffentlicht.

T.I.S.P.-Zertifikat

Eine letzte Möglichkeit, Ihre Kenntnisse und Qualifikation in der Informationssicherheit noch in diesem Jahr zu zertifizieren, bieten wir mit unserem T.I.S.P.-Seminar im November (**21.–25.11.2016**). Das Begleitbuch erhalten Sie zur Vorbereitung auf das Seminar unmittelbar nach Eingang Ihrer Anmeldung. Programm und Online-Anmeldung sowie die Termine und Seminarangebote für 2017 finden Sie unter www.secorvo.de/seminare.

Mit Brief und Siegel

Zertifizierung eines großen Rechenzentrums – nach IT-Grundschutz? Kann das mit vertretbarem Aufwand und in überschaubarer Zeit funktionieren?

Der Globalways AG ist das mit einem pragmatischen Ansatz bei der Vorbereitung und Umsetzung der IT-Grundschutzmaßnahmen auf effiziente Weise gelungen. Die Erfahrungen, Herausforderungen und „Lessons Learned" im Zertifizierungsprozess, von der Vorbereitung bis zum Zertifikat, stellt der CISO Sascha Grund bei unserer nächsten KA-IT-Si Veranstaltung am **10.11.2016, 18 Uhr** vor. Dabei wird vor allem auf das Zusammenspiel der eingesetzten Werkzeuge und deren Verwendung im Informationsverbund eingegangen.

Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking". Die Möglichkeit zur Anmeldung finden Sie unter www.ka-it-si.de.

Krypto im Advent 2016

Nach dem großen Erfolg im Advent 2015 bietet die KA-IT-Si gemeinsam mit der Pädagogischen Hochschule Karlsruhe im Dezember 2016 wieder den interaktiven Online-Adventskalender „Krypto im Advent" an, bei dem Schülerinnen und Schüler die Welt der Verschlüsselung und Geheimsprachen kennenlernen und tolle Preise gewinnen können. Auch ältere, an Ver- und Entschlüsselungsverfahren Interessierte sind herzlich eingeladen mitzumachen – allerdings außer Konkurrenz.

Veranstaltungshinweise

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

November 2016	
01.-04.11.	Black Hat Europe 2016 (Blackhat, London/UK)
08.-11.11.	DeepSec In-Depth Security Conference 2016 Europe (DeepSec, Wien/AT)
10.11.	Mit Brief und Siegel (KA-IT-Si, Karlsruhe)
10.-11.11.	T.I.S.P. Community Meeting (TeleTrusT, Frankfurt am Main)
17.-18.11.	40. DAFTA (GDD, Köln)
21.-25.11.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
21.-22.11.	6. Handelsblatt Jahrestagung - Cybersecurity (Handelsblatt/EUROFORUM, Berlin)
29.-30.11.	5. DFN-Konferenz Datenschutz (DFN-Verein/DFN-CERT, Hamburg)
Januar 2017	
13.-15.01.	ShmooCon 2017 (Shmoo Group, Washington/US)
16.-18.01.	OmniSecure 2017 (inTime, Berlin)
23.-25.01.	AppSec Cali 2017 (OWASP Foundation, CA/US)

Fundsache

Valerie Tischbein hat am 22.08.2016 auf Netzpolitik.org eine Übersicht der von Facebook erhobenen 98 Datentypen zur Schaltung zielgenauer Werbung und den korrespondieren Datenschutzeinstellungen veröffentlicht, basierend auf einer Analyse der Washington Post.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, 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

secorvo
security consulting

Secorvo Security News

November 2016

Reichtum

Zuerst verwirren sich die Worte.
Dann verwirren sich die Begriffe.
Und schließlich verwirren sich die Sachen.
(Chinesische Weisheit)

Oft beginnt es mit ungenauen Begriffen. Wenn wir „Datenschutz" sagen, meinen wir „Schutz der Persönlichkeitsrechte". Gesprächspartner verstehen aber meist „Schutz der Daten" – und assoziieren unvermeidlich „IT-Sicherheit". Eine wichtige Ursache für das verbreitete Unverständnis, dem Datenschützer begegnen – geschuldet einer irreführenden Bezeichnung.

Schlimmer noch als ungenaue Begriffe sind falsche Metaphern. Das hat viel damit zu tun, dass unser Gehirn „in Bildern denkt": Assoziationen bilden wir nicht in Gestalt abstrakter Begriffe, sondern als visuelle Vorstellungen. Eine starke Veranschaulichung überlagert daher alle denkbaren Bedeutungsnuancen mit unseren damit verbundenen Emotionen und Vorurteilen. Daher sind Metaphern starke argumentative Waffen: Sie fokussieren, vereinfachen und können wahre Bedeutungen sogar überdecken oder verdrängen.

Manchmal jedoch schlägt eine solche argumentative Metapher unerwartet zurück. So sprechen wir seit Jahren von Daten als neuer „Währung", mit denen wir unentgeltliche Leistungen im Internet bezahlen. Der Friedenspreisträger des deutschen Buchhandels von 2014, Jaron Lanier, schlägt sogar vor, dass Nutzer für die Preisgabe ihrer Nutzungsdaten ein Entgelt erhalten. Gar keine schlechte Idee, Daten einen Wert beizumessen, oder? Zweifellos steigt damit ihre Schutzwürdigkeit – wollen wir nicht genau das?

Tatsächlich aber untergräbt die Währungs-Metapher den Wesensgehalt des Datenschutzes. Was macht man mit einer Währung? Man versucht, möglichst viel davon zu akkumulieren. Das Ergebnis ist Reichtum – das Gegenteil von (Daten-) Sparsamkeit (war das nicht die Tugend von Armen und Geizigen?). Kein Wunder, dass Verkehrsminister Dobrint nach „Datenreichtum" ruft – und Datenschützer zurückrudern. Hätten wir bloß diese Metapher verhindert.

Inhalt

secorvo
security consulting

Security News

Attacks are getting better...

... oder wie man mit einer Sonnenbrille zu George Clooney wird: Am 27.10.2016 haben Forscher der Carnegie Mellon University auf der 23rd ACM Conference on Computer and Communications Security vorgestellt, wie sich Gesichtserkennungssysteme in die Irre leiten lassen. In ihrem Vortrag zeigten sie anschaulich, wie sie von theoretischen Überlegungen zu Schwächen in Gesichtserkennungssystemen zu praktischen Angriffen kamen, die die Eignung solcher Systeme als Sicherheitsmaßnahme zweifelhaft erscheinen lassen: Es gelang ihnen – wenn auch unter Laborbedingungen – durch die Verwendung spezieller Brillen Gesichtserkennungssystemen vorzutäuschen, sie seien eine beliebige andere Person, die das System kennt. Mit dem Einsatz von Gesichtserkennungssystemen in Hochsicherheitsbereichen sollte man sich also noch zurückhalten.

AppSec Practice

Am 03.11.2016 veröffentlichte die Firma Veracode eine Studie mit dem Titel *How IT Professionals are approaching AppSec today*. Die Erkenntnisse der Umfrage unter über 300 Verantwortlichen für Softwaresicherheit sind womöglich nicht überraschend, aber dennoch erschreckend: Als Hauptgründe für unzureichende Sicherheit von Softwarelösungen wurden externer und interner Druck sowie die wachsende Komplexität angegeben. Häufig würden Schutzmaßnahmen verwendet, die erwiesenermaßen nicht optimal sind. Dass dies auch praktische Konsequenzen hat, zeigen beispielsweise die im *Verizon 2016 Data Breach Investigation Report* vom 19.05.2016 dokumentierten Fälle.

Leider beschränkt sich der Bericht auf die Problembeschreibung und zeigt keine konkreten Auswege auf. Wir empfehlen die Beachtung konstruktiver Hilfestellungen wie beispielsweise die des OWASP oder aktueller Publikationen wie des CSA-Whitepapers zur Absicherung von IoT-Devices.

Poison Pi

Je leistungsfähiger Microcontroller-Boards wie der Raspberry Pi werden, desto mehr eignen sie sich auch als preiswertes Angriffs-Tool. Der amerikanische Sicherheitsforscher Samy Kamkar veröffentlichte am 16.11.2016 ein auf einem 5 US$ teuren Raspberry Pi Zero implementiertes, Streichholzschachtel großes Angriffswerkzeug (PoisonTap), das sich (sogar gegenüber einem mit Passwort gesperrten PC) als lokales USB-Ethernet ausgibt und den gesamten Netzverkehr über den Raspberry Pi umleitet. Als „Man-in-the-Middle" kann es Login-Daten mitschneiden, Schadsoftware unterschieben, Daten abfließen lassen oder verfälschen – mehr als einen freien USB-Anschluss in einem laufenden PC mit offenem Browser benötigt es dafür nicht.

Neben einer regelmäßigen Überprüfung der USB-Anschlüsse am PC kann man Client-seitig wenig tun – ein gestarteter Browser genügt PoisonTap. Webserver-seitig hilft HTTPS *Strict Transport Security* (HSTS, RFC 6797), da es HTTPS-Verbindungen erzwingt, die PoisonTap nur unter Inkaufnahme einer TLS-Fehlermeldung aufbrechen kann.

Engineering Reversed

Der reinen Lehre zufolge sollten für neue Kryptoprotokolle zunächst die genauen Sicherheitsziele festgelegt, dann die Verfahren formal definiert und ihre Sicherheit analysiert werden, bevor man sie implementiert und unter das Volk bringt. Beim Kryptoprotokoll des Messengers Signal ist diese Reihenfolge gehörig durcheinander gekommen: Seine wesentlichen Elemente wurden bereits in den Messenger-Anwendungen von WhatsApp, Facebook & Co. genutzt, bevor eine unabhängige Forschergruppe aus England, Australien und Kanada in einer am 01.11.2016 veröffentlichten Analyse das Protokoll und seine Anforderungen formalisiert und basierend auf einer bereits vor 15 Jahren etablierten formalen Beweismethodik untersucht hat.

Für ihre Analyse mussten die Forscher sogar Details aus dem Open Source Quellcode rekonstruieren. Inzwischen wäre das nicht mehr notwendig, denn zwischen dem 20.10. und 20.11.2016 haben die Signal-Autoren schließlich selbst das Protokoll und die Sicherheitseigenschaften in drei Teilen dokumentiert. Die gute Nachricht für eine Milliarde Messenger-Nutzer: Das Protokoll wurde in der formalen Analyse für gut befunden. Auch, wenn das Vorgehen nicht empfohlen werden kann – ob das Protokoll nach Lehrbuch entworfen wurde, interessierte am Ende niemanden mehr.

Privacy Leaks

Greenpeace und der Spiegel veröffentlichten am 25.11.2016 verschiedene Verhandlungsdokumente des internationalen Abkommens über den freien Handel mit Dienstleistungen (*Trade in Services Agreement* – TiSA). Den vorliegenden Dokumenten nach wird dieses geheim verhandelte Abkommen europäisches Datenschutzrecht tangieren. So fordert das „Non-Paper on data flows", Beschränkungen für den Datenfluss auch personenbezogener Daten nicht zuzulassen, wenn dadurch Dienstleistungsanbieter ungerechtfertigt diskriminiert werden. Immerhin enthält der Entwurf eine Ausnahmeklausel für Maßnahmen zum Datenschutz

(Art. I-9 (c) (ii)), und der Annex zum E-Commerce sieht die Berücksichtigung nationalen Verbraucherschutzrechts vor. Allerdings darf kein Vertragsstaat als Bedingung für den Marktzugang die Nutzung von Rechenzentren im eigenen Territorium verlangen – das beißt sich mit geltendem Datenschutzrecht.

Zwar sind die Entwürfe noch deutlich von einer Endfassung entfernt, doch enthalten die Regelungsvorschläge zahlreiche Konfliktpunkte mit den gerade erst neu erlassenen europaweiten Datenschutzbestimmungen.

Orientierungssuche

Die Übermittlung personenbezogener Daten ins außereuropäische Ausland beschäftigt derzeit die Datenschutz-Aufsichtsbehörden: Die Behörden der Länder Bayern, Berlin, Bremen, Hamburg, Niedersachsen, NRW, Rheinland-Pfalz, Saarland und Sachsen-Anhalt haben am 03.11.2016 in Pressemitteilungen bekannt gegeben, 500 zufällig ausgewählte Unternehmen verbindlich zur Beantwortung eines diesbezüglichen Fragebogens auffordern zu wollen. Darin wird u. a. nach Übermittlungen in die USA und weitere Drittstaaten, nach der Rechtsgrundlage (u. a. auch Safe Harbor), nach der Überprüfung der tatsächlichen Privacy-Shield-Unterwerfung und nach typischen Auslagerungen oder Cloud-Diensten mit außereuropäischem Bezug gefragt. Zum weiteren Vorgehen machten die Aufsichtsbehörden hingegen keine Angaben.

Nun ist wenig gegen Versuche der Aufsichtsbehörden einzuwenden, einen Überblick über die Praxis der Datenübermittlung zu gewinnen. Dass den Unternehmen bei den Angaben zahlreich Gelegenheit gegeben wird, sich diverser Datenschutzverstöße selbst zu bezichtigen, hinterlässt jedoch einen schlechten Beigeschmack – während die Aufsichtsbehörden an anderer Stelle ihre Unsicherheit bei der Beurteilung der derzeitigen Rechtslage betonen.

Secorvo News

ISMS-Verstärkung

Angesichts der wachsenden Bedeutung, die Unternehmen inzwischen dem systematischen Umgang mit Informationssicherheit beimessen, haben wir uns um Verstärkung bemüht: Seit dem 01.11.2016 zählt Fabian Ebner zum Secorvo-Team. Er bringt neben praktischer Erfahrung einen Bachelor-Abschluss in Unternehmens- und IT-Sicherheit mit – und damit ein breites Grundlagenwissen über alle Gebiete der Informationssicherheit hinweg.

Ebenfalls im November hat Stefan Gora die Qualifikation eines ISO 27001:2013-Lead-Auditors erlangt – als vierter im Secorvo-Team.

IT-Sicherheit in der Produktion

Am **08.12.2016** führen wir in Kooperation mit der Innovationsallianz Karlsruhe unsere letzte KA-IT-Si-Veranstaltung in diesem Jahr zum Thema „IT-Sicherheit in der Produktion“ durch.

Als besonderes „Schmankerl“ starten wir diesmal mit einer Führung durch das IT-Sicherheitslabor des Fraunhofer IOSB. Im Anschluss zeigt das Fraunhofer ISI das wachsende Gefährdungspotential durch Industrie 4.0 und stellt Handlungsvorschläge zur Verbesserung der IT-Sicherheit vor. Das IOSB präsentiert das „Smart Factory Web“, eine Verbindung von Modellfabriken in Südkorea und Deutschland.

Schließlich gewährt die Firma HOMAG einen Einblick in das nationale Referenzprojekt zur IT-Sicherheit für „Industrie 4.0“. Im Anschluss an die Fachvorträge haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking". Die Möglichkeit zur Anmeldung finden Sie unter www.ka-it-si.de.

24 Krypto-Rätsel

Am 1. Dezember beginnt unser diesjähriges Adventsrätsel „Krypto im Advent“ für Schülerinnen und Schüler der Klassen 3-9. Der in Zusammenarbeit mit der Pädagogischen Hochschule Karlsruhe entwickelte interaktive Adventskalender entführt in die Welt der Verschlüsselung und Geheimsprachen. Diesmal gilt es, drei Spione zu stoppen, die es auf die Weihnachtsgeschenke abgesehen haben... Wer alle Aufgaben richtig beantwortet, kann einen der zahlreichen, von unseren Sponsoren beigesteuerten Preise gewinnen.

Auch ältere, an der Kryptologie Interessierte sind herzlich eingeladen mitzumachen – allerdings außer Konkurrenz.

Veranstaltungshinweise

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

Dezember 2016	
08.12.	IT-Sicherheit in der Produktion (KA-IT-Si, Innovationsallianz, Karlsruhe)
16.12.	Sicherheit oder Datenschutz: Ein falscher Gegensatz? (GFT, ZKM, GI Karlsruhe)
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	
14.-15.02.	24. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
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), Kai Jendrian, Hans-Joachim Knobloch, 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

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