secorvo
security consulting

Secorvo Security News

Januar 2019

Protokoll

Ein Protokoll ist die Niederschrift einer Ereignisabfolge – oder die Beschreibung eines festgelegten Ablaufs. In der Kommunikationstechnik spielen Protokolle eine zentrale Rolle: Als standardisierte Ablaufbeschreibungen für den Austausch von Daten zwischen Endsystemen.

Eine der größten Herausforderungen der Kryptografie ist die Entwicklung „sicherer" Protokolle – Ablaufbeschreibungen für einen Datenaustausch, der bestimmte Sicherheitseigenschaften (authentisch, vertraulich, verbindlich etc.) besitzt und resistent gegen Angriffe ist. Dabei genügt es nicht, lediglich einzelne kryptografische Mechanismen zu kombinieren: Ohne eine enge Verzahnung der Mechanismen haben Angreifer leichtes Spiel. Ein Beispiel: So reicht eine (gar einseitige) Authentifikation der Endsysteme zu Beginn des Protokolls nicht aus, denn ein Angreifer kann sich später als „Man-in-the-Middle" in die Verbindung einklinken. Die Authentifikation muss gegenseitig erfolgen und mit weiteren Mechanismen über alle Datenpakete aufrechterhalten werden. Wie komplex und fehleranfällig das im Konkreten sein kann, haben viele erfolgreiche Angriffe auf kryptografische Protokolle gezeigt. Dafür verstehen Protokoll-Designer inzwischen einigermaßen, worauf es ankommt.

Ähnliches gilt für Abläufe im echten Leben. Zahlreiche Angriffe wie die Skimming-Attacken an Geldautomaten oder die automatische Überwindung von Captchas, die Angreifer auf Erotik-Seiten weiterleiten, um sie dort von Menschen lösen zu lassen, sind nichts anderes als „analoge" Man-in-the-Middle-Angriffe. Auch das 2018 erstmals aufgetretene „Job Scamming" gehört in diese Kategorie: Mit falschen Stellenangeboten werden Bewerber zur Versendung fotografierter Ausweispapiere oder zu einem Video-Ident-Verfahren verleitet – und diese vom Angreifer für die Eröffnung eines (Geldwäsche-) Kontos verwendet.

Dabei könnte man inzwischen von den Protokoll-Designern lernen.

Inhalt

secorvo
security consulting

Security News

Schwarzer Tag für die Biometrie

Alle Jahre wieder beschert der Chaos Communication Congress zwischen Weihnachten und Neujahr einige interessante Angriffe. So kippten Julian und Starbug am 28.12.2018 auf dem 35c3 mit ihrem Vortrag „Venenerkennung hacken“ (Video) einen der letzten Hoffnungsträger biometrischer Systeme: die Venenerkennung.

Handvenen sind ein in Hochsicherheitsumgebungen (wie beispielsweise der Zentrale des BND in Berlin) beliebtes biometrisches Authentifikationsmerkmal, da ihre Analyse bisher als eines der sichersten Verfahren galt. Da die Systeme berührungslos arbeiten sind sie zudem für öffentliche Anwendungen wie Geldautomaten oder Hygienebereiche wie Krankenhäuser besonders gut geeignet. Die Sicherheitsforscher konnten jedoch zeigen, dass ein Foto einer Hand, aufgenommen mit einer Kamera ohne Infrarotfilter aus mehreren Metern Entfernung, und etwas Nachbearbeitung genügen, um mittels eines Laserdruckers und einfachem Bienenwachs eine Attrappe zu erstellen, die von Handvenenscannern akzeptiert wird. Getäuscht wurden auf diese Weise sowohl die Handflächen- als auch die Fingervenenerkennung. Trotz der (vom Hersteller behaupteten) Lebenderkennung der Zutrittskontrolllösung wurde die Attrappe nicht zurückgewiesen.

Die Forscher skizzierten weitere Angriffsszenarien wie einen in einem berührungslosen Handtrockner eingebauten Raspberry Pi mit Kameramodul, der ausreichend gute Bilder für einen erfolgreichen Angriff liefert. Damit werden sichere Biometrieverfahren langsam knapp.

PKI in Entwicklungsumgebungen

Wer PKI-Anwendungen nicht nur nutzt sondern auch selbst entwickelt oder in einer Testumgebung betreibt, steht gleich vor einem doppelten Dilemma: Einerseits sind Test- und Entwicklungssysteme oft nicht sicher genug – sie werden nicht auf dem gleichen Sicherheitsniveau betrieben wie Produktivsysteme. Schlüssel zu Zertifikaten sind dort weniger geschützt, Sperrprozesse oft nicht sorgfältig umgesetzt, und daher kann das Vertrauensniveau einer produktiven PKI leiden.

Andererseits sind produktive PKIs oft zu sicher – Zertifikate für Test und Entwicklung werden „auf Zuruf“ benötigt; sorgfältige manuelle Validierungsschritte bremsen die Entwicklungsarbeit aus. Hinzu kommt, dass fehlerträchtige Ereignisse wie die Sperrung oder der Ablauf eines Zertifikats in einem verglichen mit dem späteren Produktivbetrieb kurzen Entwicklungszeitplan meist nicht auftreten – Test-Zertifikate sollten daher eine deutlich kürzere Gültigkeit haben als in einer Produktivumgebung.

Eine schlechte Lösung für dieses Dilemma ist, bei Test- und Entwicklung mit selbstsignierten Zertifikaten und den üblichen, „wegzuklickenden“ Meldungen zu arbeiten. Eine aufwändige ist es, eine separate zweite PKI zu betreiben, deren Root-CA nur in der Entwicklung und für Tests vertraut wird.

Einen Mittelweg geht das von einem Google-Entwickler am 07.01.2019 veröffentlichte Paket mkcert. Es bietet einen einfachen Zugang zu einer ad-hoc erstellten OpenSSL-CA und platziert deren Zertifikat in alle gängigen lokalen Root-Stores. Eine künftige Version soll auch eine Zertifikatsbeantragung per ACMEv2 unterstützen. Für viele Test- und Entwicklungsumgebungen könnte dies die gesuchte Lösung sein.

Drum prüfe, wer sich ewig bindet

Aller europäischen Vereinheitlichung zum Trotz gibt es – nach wie vor – auch außerhalb der DSGVO und des neuen BDSG Datenschutzbestimmungen. Am 18.12.2018 hat das Bundessozialgericht (BSG) auf Grundlage des § 284 SGB V eine datenschutzrechtliche Entscheidung zu elektronischen Gesundheitskarten getroffen.

Die Versicherten (ausgenommen Kinder und Personen, die dazu außerstande sind) müssen den Krankenkassen Passbilder zur Ausstellung der elektronischen Gesundheitskarte zur Verfügung stellen. Wie dies zu geschehen hat ist gesetzlich nicht geregelt. Nach dem Urteil des BSG steht nun fest, dass die Krankenkassen die Bilder nach der Ausstellung der Karte unverzüglich zu löschen haben.

Dies entspricht dem Grundsatz der Zweckbindung und der Datensparsamkeit. Es ist zu begrüßen, dass die Bilder nicht dauerhaft, etwa zur Ausstellung von Ersatzkarten o. ä. gespeichert werden dürfen, auch wenn ganz offensichtlich ist, dass dies sowohl für die Kassen als auch für die Versicherten einen Mehraufwand bedeutet, wenn eine Karte abgelaufen, verloren gegangen oder auf andere Weise abhandengekommen ist.

Anderes gilt bei Ausweispapieren wie dem Reisepass, Personalausweis oder der Fahrerlaubnis. Hier liegen der Speicherung andere gesetzliche Ermächtigungen (PassG, PAuswG, StVG) zugrunde, die es den Behörden erlauben, die Bilder auch nach Erstellung der Ausweisdokumente weiter zu speichern.

Dabei dürfen die Daten im Fahrerlaubnisregister nach § 61 Absatz 4 StVG nur bis zur Vollendung des 110. Lebensjahres gespeichert werden dürfen. Was auch immer mit dieser Begrenzung bezweckt wurde – sie könnte sich eines Tages noch rächen...

secorvo
security consulting

Patchen ist gut...

...zum Schutz vor (bekannten) Sicherheitsschwachstellen. Das haben wir alle seit Jahren immer wieder gehört (und weitergesagt). Aber Patchen aus einer verlässlichen, integren Quelle ist besser. Das mussten all jene schmerzlich lernen, die im Zeitraum zwischen (vermutlich) Juli 2018 und Januar 2019 Software vom „PHP Extension and Application Repository“ (PEAR) auf ihrem Webserver installiert haben. Denn wie die Betreiber des Repositories am 19.01.2019 mitteilten, war mindestens eines der Installationspakete in diesem Zeitraum mit Schadsoftware bestückt.

Während immer mehr kommerzielle Softwarehersteller ein ISO 27001-Zertifikat für ihr Security Management vorweisen, scheinen manche Open-Source-Softwarequellen zwar mit viel Enthusiasmus zu arbeiten, aber dem sicheren Betrieb noch immer wenig Aufmerksamkeit zu widmen.

Angesichts geradezu inflationärer Security-Labels und -Zertifizierungen wäre ein Label für professionell sicher betriebene und regelmäßig auditierte Open Source Repositories ein deutlicher Fortschritt. So wie einige große OpenSSL-Anwender das am 21.01.2019 veröffentlichte Security Audit der TLS-1.3-Implementierung von OpenSSL mitfinanziert haben fänden sich bestimmt Sponsoren, denen die Integrität der von ihnen genutzten Softwarepakete am Herzen liegt.

Eine für alle

Die französischen Datenschutz-Aufsichtsbehörde CNIL hat am 21.01.2019 ein 50 Millionen Euro schweres Bußgeld gegen Google verhängt. Nach dem mit der DSGVO eingeführten „One-Stop-Shop“-Prinzip soll es bei grenzüberschreitenden Verarbeitungen für betroffene Unternehmen nur einen einzigen Ansprechpartner in Europa geben, die sogenannte „federführende Aufsichtsbehörde“, falls eigentlich mehrere verschiedene Aufsichtsbehörden zuständig wären. Dann müssen Unternehmen nur mit einer Behörde kommunizieren, es gibt nur ein Bußgeld – und damit zugleich mehr Rechtssicherheit. Die federführende Behörde muss sich mit den anderen zuständigen Datenschutzbehörden abstimmen.

Vor diesem Hintergrund stellt sich die Frage, was in Deutschland passiert, wenn es zwar keinen grenzüberschreitenden, wohl aber einen Verstoß gibt, der mehrere Bundesländer betrifft. Denn dann sind bis zu 18 Datenschutzbehörden zuständig. Zwar bezieht sich die Regelung in der DSGVO auf grenzüberschreitende Verstöße, aber die EU-weit geltenden Maßstäbe müssten auch innerhalb des Bundesgebietes angewendet werden, so dass sich die Landesdatenschutzbehörden untereinander und mit der federführenden Behörde abstimmen müssten, also derjenigen, in deren Bundesland das gegen die DSGVO verstoßende Unternehmen seinen Sitz hat.

Secorvo News

Secorvo Seminare

Im März 2019 starten wir mit einem PKI- (**18.–21.03.2019**), T.I.S.P.- (**25.–29.03.2019**) und „IT-Sicherheit heute“-Seminar (**02.–04.04.2019**) in die Weiterbildungs-Saison 2019. Die vollständigen Programme und eine Möglichkeit zur Online-Anmeldung finden Sie unter www.secorvo.de/seminare. Wir freuen uns auf Ihre Teilnahme!

Teamzuwachs

Ab dem 01.02.2019 verstärkt Jannis Pinter das Secorvo-Team. Als Informatiker mit mehreren Jahren Erfahrung in der IT-Sicherheit bringt er insbesondere vertiefte technische Kenntnisse über Public Key-Infrastrukturen mit.

Gut gehört und schon gehackt.

Oder: Wie Sennheiser das TLS-Protokoll aushebelte. Leser der Security News kennen die Hintergründe (SSN 10/2018): Ein klitzekleiner „Workaround“ der Entwickler wuchs sich im vergangenen Herbst zu einem Sicherheits-Desaster für alle betroffenen Systeme aus. Eine Design-Schwachstelle im Zertifikatsmanagement der Software Sennheiser Head-Setup unterhöhlte ohne Wissen der Nutzer die Sicherheit aller TLS-Verbindungen – für die Beseitigung der Schwachstelle war die Mitwirkung von Microsoft erforderlich. Dass ein solches Desaster überhaupt möglich war, hatte allerdings mehrere Ursachen, für die nicht ausschließlich Sennheiser verantwortlich gemacht werden sollte.

Beim Jahresauftakt-Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 21.02.2019 zeigen die Secorvo-Experten André Domnick und Hans-Joachim Knobloch, wie durch die Schwachstelle ein Man-in-the-Middle-Angriff auf TLS gelingt, stellen dar, gegen welche lang bekannten Design-Prinzipien für sichere Software verstoßen wurde und wie eine sichere Lösung hätte aussehen können.

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

Veranstaltungshinweise

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

Februar 2019	
06.-07.02.	26. DFN-Konferenz "Sicherheit in vernetzten Systemen" (DFN-CERT Services GmbH, Hamburg)
20.-21.02.	29. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
21.02.	Gut gehört und schon gehackt. (KA-IT-Si, Karlsruhe)
März 2019	
13.-14.03.	secIT 2019 (Heise Medien GmbH&Co.KG, Hannover)
14.-15.03.	Future Security 2019 (Fraunhofer VVS, Nürnberg)
18.-21.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
25.-29.03.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
29.03.	SECMGT-Workshop: IoT – ein Thema für den CISO? (GI-Fachgruppe SECMGT, Frankfurt/Main)
April 2019	
02.-04.04.	IT-Sicherheit heute – praxisnah, aktuell, kompakt (Secorvo, Karlsruhe)
09.-10.04.	Datenschutztage 2019 (FFD Forum für Datenschutz, Wiesbaden)
11.-12.04.	Security Forum 2019 (Hagenberger Kreis zur Förderung der digitalen Sicherheit, Hagenberg/AT)
24.-26.04.	DFRWS EU Conference (DFRWS, Oslo/NOR)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Hans-Joachim Knobloch, Friederike Schellhas-Mende

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 2019

Datenschützer auf der Erbse

Es war einmal ein Unternehmer, der wollte einen Datenschützer bestellen. Aber das sollte ein wirklicher Datenschützer sein. Da reiste er in der ganzen Welt herum, um einen solchen zu finden, aber überall fehlte etwas. Datenschützer gab es genug, aber ob es wirkliche Datenschützer waren, konnte er nie herausfinden. Immer war da etwas, was nicht ganz in Ordnung war. Da kam er wieder nach Hause und war ganz traurig.

Eines Tages brach plötzlich der Umsatz des Unternehmens ein, es war ganz entsetzlich. Da klopfte es am Haupteingang, und der Unternehmer ging hin, um aufzumachen. Es war ein Datenschützer, der draußen vor dem Tor stand. Wie hatte ihn der Konjunktureinbruch gebeutelt! Das Wasser lief ihm in die Schuhe hinein und zu Löchern wieder hinaus. Aber er sagte, dass er ein wirklicher Datenschützer sei. ‚Ja, das werden wir schon erfahren!' dachte der CIO, aber er sagte nichts, ging in das Rechenzentrum, löschte alle personenbezogenen Daten und versteckte in einem Verzeichnis eine Geburtstagsliste. Dann nahm er hundert beliebige Dateien, legte sie in demselben Verzeichnis ab und verschob das Verzeichnis in eines von hundert Unterverzeichnissen.

Den ganzen nächsten Tag ließ er den Datenschützer nach Datenschutzverstößen suchen. Am Abend fragte er ihn, wie er das Datenschutzniveau bewerte. „Oh, entsetzlich schlecht!" sagte der Datenschützer. „Ich habe etwas Grässliches entdeckt! Eine Geburtstagsliste ohne Einwilligung. Es ist ganz entsetzlich!" Daran konnte man sehen, dass er ein wirklicher Datenschützer war, da er in einem von hundert Verzeichnissen mit hundert Dateien die Geburtstagsliste entdeckt hatte. So feinfühlig konnte niemand sein außer einem echten Datenschützer. Da bestellte ihn der Unternehmer, denn nun wusste er, dass er einen wirklichen Datenschützer gefunden hatte. Und die Geburtstagsliste kam zur Warnung in einen Schaukasten, wo sie heute noch zu sehen ist, wenn sie niemand gestohlen hat.

Inhalt

secorvo
security consulting

Security News

Encryption – Back to the Roots

Schon bevor 1977 die öffentliche Standardisierung von Verschlüsselungsverfahren mit dem DES Fahrt aufnahm suchten neben den Geheimdiensten auch kommerzielle Unternehmen nach effizienten und zugleich sicheren Algorithmen. So basierte der DES auf der einige Jahre zuvor bei IBM von Horst Feistel entwickelten Chiffre Lucifer, und bei der Wahl des DES-Nachfolgers AES wurde ausdrücklich auch auf eine gute Performance auf einfachsten CPUs geachtet.

Dennoch wäre die Verschlüsselung des kompletten Speichers eines TV-Sticks oder Billig-Handys per AES auch heute noch recht langsam. Daher werden bspw. unter Android Geräte mit einer AES-Leistung unter 50 MB/s nicht verschlüsselt – trotz der seit Version 6 obligatorischen Data Storage Encryption.

Am 07.02.2019 präsentierten Google-Forscher nun unter dem Namen Adiantum einen Algorithmus, mit dem der Datenspeicher eines Geräts ohne AES-Beschleuniger-Hardware etwa fünf Mal schneller verschlüsselt werden kann als per AES. Dazu kombinierten sie die von Daniel Bernstein und anderen unabhängigen Forschern entwickelten Algorithmen ChaCha12, Poly1305 und NH mit AES – zu einem Feistel-Netzwerk. Damit gibt es immer weniger Argumente für Gerätehersteller, den Speicher nicht zu verschlüsseln.

TLS 1.3 auf dem iPhone

Die jüngste Version des TLS-Protokolls – TLS 1.3 – wurde im August 2018 standardisiert. Während die meisten Browserhersteller das neue Protokoll bereits in ihren Produkten nachgerüstet haben, sieht es bei den Betriebssystemplattformen hingegen dürftig aus.

Apple kündigte am 29.01.2019 als erster Mobilplattformbetreiber an, dass die kommende Version 12.2 des Mobilbetriebssystems iOS TLS 1.3 unterstützen wird. Apps, Browser und E-Mail-Clients können dann ohne weiteres Zutun Verbindungen mit dem neuen Protokoll aufbauen, sofern die Gegenstelle dieses ebenfalls anbietet. Von Google und Microsoft fehlt bisher die Ankündigung, wann mit einer Unterstützung von TLS 1.3 durch das Betriebssystem gerechnet werden kann.

Im Februar 2019 hatte TLS 1.3 auf den Servern der populärsten 150.000 Webseiten bereits eine Verbreitung von über 11,6% – beachtlich für ein Protokoll, das seit gerade einmal sechs Monaten standardisiert ist. Derweil mehren sich die Stimmen, ältere Protokollversionen abzuschalten. So wollen Mozilla, Google, Apple und Microsoft die Unterstützung für TLS 1.0 und TLS 1.1 in ihren Browsern ab März 2020 einstellen. Webseitenbetreiber sollten bis dahin sicherstellen, dass ihre Webserver mindestens TLS 1.2 beherrschen.

Grundschutz-Kompendium 2019

Am 18.02.2019 veröffentlichte das BSI eine überarbeitete Version des IT-Grundschutz-Kompendiums. Anders als die Ergänzungslieferungen zu den IT-Grundschutz-Katalogen wird die Version nun als „Edition" mit der jeweiligen Jahreszahl bezeichnet. Einige Bausteine wurden ergänzt und zum Teil Überarbeitungen der Inhalte der „Edition 2018" vorgenommen. Gut gefallen hat uns, dass auch geringfügige Änderungen explizit ausgewiesen sind, so dass man mit wenig Aufwand Änderungsbedarf an ggf. bereits durchgeführten IT-Grundschutz-Checks erkennen kann. Die klare Unterscheidung nach Bausteinen (= Soll-Anforderungen) und Umsetzungshinweisen (= Möglichkeiten zur Erfüllung der Anforderungen) wurde beibehalten. Auch mit der zweiten Ausgabe des Kompendiums ist damit aus unserer Sicht die 2017 begonnene Modernisierung des IT-Grundschutzes gelungen.

Datenkrake mit App-Zertifikaten

Zwar ist es unter Apples iOS, anders als in Googles offenem Android-Ökosystem, nicht ohne weiteres möglich, Apps aus anderen Quellen als dem offiziellen App Store zu installieren. Eine Ausnahme macht Apple jedoch: Unternehmen, die am Apple Developer Enterprise Program teilnehmen, können mit Hilfe eines speziell für sie ausgestellten Unternehmenszertifikats eigene In-House-Apps signieren und auf den iOS-Geräten ihrer Mitarbeiter installieren. Genau solch ein Unternehmenszertifikat hat Facebook nun missbraucht, um eine datenschutzrechtlich höchst bedenkliche Marktforschungs-App unter dem Titel „Facebook Research" am App Store vorbei an iOS-Nutzer zu verteilen. Damit nicht genug: Die App erfordert die Installation eines Root-Zertifikats im Trust Store des Geräts, so dass Facebook sogar verschlüsselte Kommunikation mitlesen konnte.

„Wir bessern uns" war wenige Tage vor Bekanntwerden dieses neuerlichen Skandals die Kernaussage des öffentlichen Auftritts von Facebook-Vizechefin Sheryl Sandberg Ende Januar in München. Schon kurz darauf musste jedoch Apple einschreiten und widerrief unverzüglich das Unternehmens-Zertifikat von Facebook. Damit waren nicht nur Facebooks „Research App" sondern auch sämtliche Facebook-internen Apps nicht mehr lauffähig. Inzwischen darf Facebook seine eigenen Apps

wieder signieren, die zukünftig hoffentlich innerhalb des Unternehmens bleiben und nicht erneut dazu genutzt werden, Nutzer im Namen der „Marktforschung“ auszuspionieren.

Kartellamt macht Datenschutzaufsicht

Das Bundeskartellamt schützt als unabhängige Bundesbehörde den Wettbewerb in Deutschland. In dieser Funktion hat es sich nun in die Verarbeitung von Nutzerdaten bei Facebook eingeschaltet, da Facebook eine marktbeherrschende Stellung unter sozialen Netzwerken in Deutschland innehabe. Es unterliege daher auch dem Verbot der missbräuchlichen Ausnutzung einer marktbeherrschenden Stellung nach § 19 Abs. 1 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB), insbesondere, da der Umgang mit personenbezogenen Daten für die Stellung des Unternehmens im Wettbewerb maßgeblich ist.

Bislang war die Nutzung von Facebook nur möglich, wenn einer weitreichenden Sammlung von Daten auch außerhalb der Facebook-Seite mit Zuordnung zum Nutzeraccount zugestimmt wurde. Diese Drittquellen umfassen sowohl zum Facebook-Konzern zugehörige Gesellschaften (z. B. WhatsApp, Instagram) als auch bei der Nutzung von Apps und Drittwebseiten anfallende Daten, z. B. Facebook Business Tools wie der „Like“-Button.

Ein Zusammenführen dieser Daten ist nach der Entscheidung des Kartellamts nur zulässig, wenn der Nutzer darin (freiwillig) einwilligt – was außerdem bereits aus Art. 7 Abs. 4 DSGVO folgt.

Dieser Entscheid muss als Präzedenzfall für Online-Medien angesehen werden: Der Datenverarbeitung sind sowohl datenschutzrechtliche als auch kartellrechtliche Grenzen gesetzt.

Steinige Anpassung

Nach der Stellungnahme des Bundesrats vom 19.10.2018 hat der Bundestag das Zweite Datenschutz-Anpassungs- und Umsetzungsgesetz (2. DSAnpUG EU) am 08./09.11.2018 an verschiedene Ausschüsse überwiesen. Eine endgültige Fassung gibt es daher weiterhin nicht. Der gegenwärtige Entwurf der Bundesregierung ändert in 155 Artikeln auf 553 Seiten 154 Gesetze. Dementsprechend unübersichtlich ist das Anpassungsvorhaben, zumal nun weitere Änderungsvorschläge der Ausschüsse zu berücksichtigen sind. Darunter auch – vom Bundesrat abgelehnte – Vorschläge zu einer Lockerung der Bestellpflicht von Datenschutzbeauftragten.

Angepasst werden Datenschutzregelungen in den Sozialgesetzbüchern und in Gesetzen über Dateien und Register, zahlreiche medizinrechtliche Bestimmungen, zahlreiche Gesetze des besonderen Verwaltungsrechts, das BSI-Gesetz und das Strafgesetzbuch. Vielfach werden dabei die Betroffenenrechte aus Art. 12-22 DSGVO nach Art. 23 DSGVO eingeschränkt. Nicht berücksichtigt werden bisher das Telekommunikations- und das Telemediengesetz, deren Status damit bis zur Verabschiedung der europäischen ePrivacy-Verordnung weiter unklar bleibt.

Eine öffentliche Diskussion zu den Vorschlägen blieb bislang weitgehend aus. Die zahlreichen Anpassungen werden die Rechtslage jedenfalls nicht einfacher machen, zumal die speziellen Einschränkungen der DSGVO-Pflichten Zweifel an der Reichweite der Öffnungsklauseln nach sich ziehen werden.

Secorvo News

Weiterer Black Belt

Unser Penetrationstester Michael Knöppler ist jetzt ebenfalls Träger eines „Black Belt“: Anfang Januar bestand er die OSCP-„Gürtelprüfung“ – eine weitere fachliche Verstärkung unseres Pentest-Teams.

Nächste Seminare

Wir freuen uns auf Ihre Teilnahme am kommenden PKI- (**18.–21.03.2019**) oder T.I.S.P.-Seminar (**25.–29.03.2019**) – die vollständigen Programme und eine Online-Anmeldung finden Sie unter www.secorvo.de/seminare.

Kaltblütig.

Zum Schutz von Daten vor unberechtigtem Zugriff ermöglichen Microsofts BitLocker und Apples FileVault deren Verschlüsselung – für mobile Geräte im geschäftlichen Umfeld oft eine Compliance-Anforderung. Nur wer das Passwort kennt, kommt an die Daten heran. Dass dies ein Irrglaube ist, haben Sicherheitsforscher bereits 2008 gezeigt: Hatten sie physischen Zugriff auf einen angeschalteten oder „schlafenden“ (Bereitschaftsmodus) Computer, konnten sie das Passwort aus dem Arbeitsspeicher auslesen. Zehn Jahre nach dieser Entdeckung sind die sogenannten Cold-Boot-Angriffe noch immer möglich. Beim nächsten KA-IT-Si-Event am **11.04.2019** werden Andreas Sperber und Daniel Matesic (aramido) live einen solchen Angriff auf einen Computer mit Festplattenverschlüsselung zeigen.

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

Veranstaltungshinweise

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

März 2019	
13.-14.03.	secIT 2019 (Heise Medien GmbH&Co.KG, Hannover)
14.-15.03.	Future Security 2019 (Fraunhofer VVS, Nürnberg)
18.-21.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
25.-29.03.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
29.03.	SECMGT-Workshop: IoT – ein Thema für den CISO? (GI-Fachgruppe SECMGT, Frankfurt/Main)
April 2019	
09.-10.04.	Datenschutztage 2019 (FFD Forum für Datenschutz, Wiesbaden)
11.-12.04.	Security Forum 2019 (Hagenberger Kreis zur Förderung der digitalen Sicherheit, Hagenberg/AT)
24.-26.04.	DFRWS EU Conference (DFRWS, Oslo/NOR)
Mai 2019	
06.-09.05.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
13.-17.05.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
19.-23.05.	Eurocrypt 2019 (IACR, Darmstadt)
21.-23.05.	16. Deutscher IT-Sicherheitskongress (BSI, Bonn)
22.-23.05.	20. Datenschutzkongress (EUROFORUM Deutschland SE, Berlin)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Stefan Gora, Hans-Joachim Knobloch, Michael Knopp, Sarah Niederer, Jannis Pinter, Christian Titze

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 2019

Die Heuristikfalle

Computer lösen Aufgaben deterministisch: vorhersehbar und wiederholbar. Dafür füttern wir sie mit Lösungsalgorithmen. Für viele Probleme des echten Lebens (man könnte sagen: für alle, die diesen Titel verdienen) gibt es jedoch keine Lösungsalgorithmen. Da helfen uns bestenfalls *Heuristiken*: Dicker-Daumen-Regeln, die meist zum Ziel führen, aber nicht immer. So hindert uns die Heuristik "meide Unbekanntes", giftige Früchte zu verzehren, lässt uns aber auch vor Menschen mit fremdländischem Äußeren zurückweichen.

Nicht anders funktioniert künstliche Intelligenz, die uns jetzt allerorten begegnet. In vielen Fällen genügen da heuristische Ergebnisse - eine überwiegend richtige Übersetzung ist besser als keine, und auch für eine zu 80% zutreffende Rechtschreibkorrektur sind wir dankbar.

Aber es gibt auch Probleme, die heuristische Erfolgsquoten nicht gut vertragen. So veröffentlichte die Bundespolizei am 11.10.2018 eine Studie über die sechsmonatige Erprobung biometrischer Gesichtserkennung von Straftätern durch Videoanalyse am Bahnhof Berlin-Südkreuz. Drei Gesichtserkennungssysteme, die mit Fahndungsfotos trainiert worden waren, erreichten dabei eine durchschnittliche Trefferquote von bis zu 91,2%; die Falschakzeptanzrate (Anteil der fehlerhaft als "Gesuchter" erkannten Personen) lag bei 0,34%.

Würde das System für ein Jahr an allen Bahnhöfen eingesetzt und mit Fahndungsfotos der 175.000 per Haftbefehl gesuchten Personen gefüttert, dann könnte es - sofern die Gesuchten an wenigstens einer dieser Kamera vorbeieilen – fast 160.000 davon entdecken.

Eine beeindruckende Zahl. Allerdings würden auch 0,34% der Bahnreisenden fälschlich als Täter identifiziert: Bei jährlich 4,669 Milliarden Reisenden wären das etwa 15.875.000 Fehlidentifikationen. Die Erkennungsrate läge damit unter 1% aller Identifizierten – keine grandiose Systemleistung. Und in einer freiheitlichen Ordnung eine wohl kaum erträgliche „Unschärfe“.

Inhalt

secorvo
security consulting

Security News

Office 365 und der Cloud Act

Microsoft bietet mit Office 365 Dienste wie Sharepoint, OneDrive, Teams und Exchange sowie Anwendungen wie Outlook, Word oder Excel für Privatanwender und Unternehmen an. Zur Sicherstellung von Datensicherheit und Datenschutz verpflichtete sich Microsoft zur Umsetzung wirksamer Maßnahmen. Ab Ende 2019 wird Microsoft seine Cloud-Dienste aus Deutschland in neuen Cloud-Regionen bereitstellen, die als „deutsche Region" Teil der globalen Cloud-Umgebung von Microsoft Office 365 sein werden. Damit wird das bisherige Modell von Microsoft Office 365 Deutschland abgekündigt. In den neuen Regionen mit Rechenzentren in Berlin und Frankfurt soll die Speicherung in Deutschland erfolgen, während die Cloud-Dienste aber auch an Microsofts weltweites Cloud-Netzwerk angebunden sind. Für Dienste aus seinen neuen Rechenzentrums-Regionen verspricht Microsoft die Einhaltung der DSGVO und will sich dazu vertraglich verpflichten. Wahrscheinlich wird Microsoft durch dieses Vorgehen unter den am 23.03.2018 in Kraft getretenen Cloud Act fallen (Clarifying Lawful Overseas Use of Data Act), der US-amerikanischen Ermittlungsbehörden Zugriff auf Daten einräumt, die US-Unternehmen auf europäischen Servern speichern. Es erscheint zweifelhaft, dass sich damit die Anforderungen der DSGVO erfüllen lassen.

Reverse Engineering – powered by NSA

Am 05.03.2019 stellte Robert Joyce (NSA) auf der RSA Conference („Come Get Your Free NSA Reverse Engineering Tool!") das Reverse-Engineering-Werkzeug Ghidra vor. Das Tool, dessen Existenz 2017 mit den Wikileaks-Enthüllungen Vault 7 bekannt geworden war, steht nun unter der Apache License 2.0 zur Verfügung. Es konkurriert mit seinem Funktionsumfang und der grafischen Benutzeroberfläche mit dem kommerziellen Werkzeug IDA des Herstellers Hex-Rays, dessen Lizenzkosten jenseits der tausend Euro liegen. Natürlich drängt sich bei einer Anwendung, die die NSA entwickelt hat, sofort die Frage nach Hintertüren auf. Innerhalb weniger Stunden nach Veröffentlichung wurden auch erste gravierende Schwachstellen in Ghidra entdeckt – keine Ausnahme bei „jungen" Open-Source-Projekten –, aber bisher keine Hintertüren. Die Bugs betreffen den Umgang mit dem Debug-Server und das Laden nicht vertrauenswürdiger Extensionen. US-Regierungsstellen haben bereits 32 Projekte im Quellcode im Rahmen ihrer Initiative zum Technologietransfer publiziert; sie erhoffen sich davon eine Beteiligung der Community an der Weiterentwicklung. Zwar sollte man mit dem Einsatz von Ghidra in sensiblen Bereichen noch vorsichtig sein – dennoch ist die Veröffentlichung eine Bereicherung, denn bisher stand kein freies Werkzeug mit ähnlichem Funktionsumfang zur Verfügung.

Löchrige Container

Software ohne Abhängigkeiten ist in der heutigen Zeit kaum noch vorstellbar. Wie problematisch das aus Sicherheitssicht ist, belegt das Unternehmen Snyk in seinem diesjährigen „The State of Open Source Security Report" mit konkreten Zahlen: Die Überprüfung von mehr als einer Million Open-Source-Projekten ergab, dass 78 % der dabei erkannten Schwachstellen auf indirekte Abhängigkeiten zurückzuführen sind. Indirekte Abhängigkeiten sind solche, die von explizit eingebundenen Komponenten benötigt und automatisch mitinstalliert werden. Ein Großteil der Abhängigkeiten in Paketverzeichnissen wie npm, Maven Central oder Ruby Gems sind solche indirekten Abhängigkeiten. Deshalb ist ein klarer Blick auf die Abhängigkeiten eigener Software von großer Bedeutung. Erkennen kann man bekannte Schwachstellen in den Abhängigkeiten z. B. mit dem Scanner von Snyk.

Wenn es – wie bei Containerlösungen – darum geht, die Bibliotheken und Programme eines gesamten Betriebssystems als Abhängigkeiten für den Container zu nutzen, zeichnet sich eine ähnliche Problematik ab: Laut Snyk besitzt jedes der Top 10 Docker Images mindestens 30 bekannte Schwachstellen. Sie gehen meist auf veraltete Bibliotheken im verwendeten Docker Base Image zurück. Als Gegenmaßnahme hilft in der Regel ein Upgrade, in vielen Fällen reicht sogar ein einfacher Rebuild. Auch der Einsatz von minimalen Base Images wie z. B. Alpine Linux trägt zu einer grundlegenden Sicherheits-„Hygiene" bei.

ACME wird Standard

Automatic Certificate Management Environment (ACME) ist ein von der Internet Security Research Group (ISRG) entwickeltes Protokoll zum automatisierten Bezug von TLS-Serverzertifikaten. Es wurde am 11.03.2019 in RFC 8555 als IETF-Standard veröffentlicht. Die ISRG ist die Dachorganisation hinter dem gemeinnützigen Trustcenter Let's Encrypt, das seit 2015 über das ACME-Protokoll kostenfreie, öffentlich gültige TLS-Serverzertifikate ausstellt.

ACME-Clients mit Internet-Zugang beantragen, installieren und erneuern ihre TLS-Serverzertifikate selbsttätig und reduzieren so den Administrationsaufwand erheblich. Auch der Nachweis, dass der Antragsteller berechtigt ist, ein öffentlich gültiges

DV-Zertifikat für den gewünschten Host-Namen zu erhalten, ist im ACME-Protokoll bereits vorgesehen.

Die nun verabschiedete Protokollversion (ACMEv2) schafft Planungssicherheit für die Entwickler alternativer Client- und Server-Implementierungen sowie für andere Trustcenter, die es ihren Nutzern ermöglichen wollen, ohne Änderung der bereits etablierten Prozesse und der Client-Software die Zertifizierungsstelle zu wechseln. Proof of Concept: Let's Encrypt selbst hat über ACMEv2 bereits mehr als 70 Millionen TLS-Serverzertifikate ausgestellt.

DSFA leicht gemacht?

Zum 01.03.2019 hat der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) einen Hinweis auf das PIA-Tool (Privacy Impact Assessment) der französischen Datenschutzbehörde CNIL veröffentlicht. Das Tool ist nicht neu, aber inzwischen auch in deutscher Sprache verfügbar und soll Verantwortlichen die Durchführung von Datenschutz-Folgenabschätzungen (DSFA) erleichtern. Die Oberfläche ist recht benutzerfreundlich und man kann die Folgenabschätzung Schritt für Schritt vornehmen. Die CNIL bietet weitere Hinweise zum Tool samt Youtube-Erklärvideo in englischer Sprache. Allerdings gibt es auch andere, teils komplexere Ansätze als die Methodik der CNIL zur Durchführung von DSFAs.

Eine Herausforderung wird durch die Software jedoch nicht gelöst: die Schwellwertanalyse, mit der vor der Durchführung einer DFSA geprüft wird, ob es sich bei dem abzuschätzenden Prozess tatsächlich um eine „Hochrisikoverarbeitung" handelt. Häufig werden DSFA daher vorsorglich durchgeführt. Um diesen Prozess zu erleichtern, hat der BayLfD eine überarbeitete Orientierungshilfe für Datenschutz-Folgenabschätzungen inklusive Prüfschema veröffentlicht. In der Theorie ist eine DSFA samt Vorprüfung also gar nicht so schwierig – ob sich dies auch so einfach in die Praxis umsetzen lässt, muss sich erst noch erweisen.

OWASP ASVS 4.0

Am 01.03.2019 hat das Open Web Application Security Project (OWASP) Version 4 des Application Security Verification Standard herausgegeben. Im Vergleich zur Vorversion haben sich viele Änderungen ergeben; die inhaltlich bedeutendste ist der Bezug auf NIST 800-63-3 Digital Identity Guidelines für die Abschnitte zu Authentisierung und Session Management, sowie PCI DSS – ein Audit nach ASVS Level 1 deckt die Anforderungen in Abschnitt 6.5 aus PCI-DSS 3.2.1 Abschnitt 6.5 ab. Neu ist auch der Bezug aller Prüfpunkte auf die Common Weakness Enumeration Identifier (CWE) – sehr nützlich für Tester, denn die einzelnen Prüfpunkte werden (wie in den vorangegangenen Versionen) nicht näher erläutert, obwohl einige dieser Punkte durchaus erklärungsbedürftig sind. Darüber hinaus wurde der Abschnitt zu Mobile Security gestrichen, da mittlerweile ein eigener Mobile Application Security Verification Standard (MASVS) existiert. Ebenfalls gestrichen wurde Level 0 ("Cursory"). Mit dem ASVS 4 wurden alle Punkte neu durchnummeriert; zusätzlich wurde eine neue Gliederungsebene eingeführt, da einige Abschnitte im Laufe der Zeit stark angewachsen und unübersichtlich geworden sind. Leider wurde auch die farbliche Unterscheidung der Punkte nach zugehörigem Level abgeschafft; für die Zuordnung eines Prüfpunkts zum Level muss man jetzt genauer hinsehen. Dennoch haben diese Überarbeitungen, vor allem die Anbindung an andere bekannte Werke, dem ASVS sehr gut getan und dürften die Akzeptanz bei Auftraggebern und Testern weiter erhöhen.

Secorvo News

T.I.S.P. und T.P.S.S.E.

Mit deutlich über 1.000 Absolventen ist der T.I.S.P. inzwischen eine nicht nur anerkannte, sondern auch weit verbreitete Berufsqualifikation für IT-Sicherheitsexperten. Das nächste T.I.S.P.-Seminar mit anschließender Zertifikatsprüfung bieten wir Ihnen am **13.–17.05.2019**. In der Woche davor (**06.–09.05.2019**) haben Sie die Gelegenheit, sich als T.P.S.S.E. (TeleTrusT Professional for Secure Software Engineering) zu qualifizieren.

Die detaillierten Seminarprogramme und eine Möglichkeit zur Online-Anmeldung finden Sie hier.

Kaltblütig.

Zum Schutz vor unberechtigtem Datenzugriff bieten Microsofts BitLocker und Apples FileVault deren Verschlüsselung – für mobile Geräte im geschäftlichen Umfeld oft eine Compliance-Anforderung. Nur wer das Passwort kennt, kommt an die Daten heran. Dass dies ein Irrglaube ist, haben Sicherheitsforscher bereits 2008 gezeigt: Hatten sie physischen Zugriff auf einen lediglich gesperrten oder „schlafenden" (Bereitschaftsmodus) Computer, konnten sie das Passwort aus dem Arbeitsspeicher auslesen. Zehn Jahre nach dieser Entdeckung sind die sogenannten Cold-Boot-Angriffe noch immer möglich. Beim nächsten KA-IT-Si-Event am **11.04.2019** werden Andreas Sperber und Daniel Matesic (aramido) live einen solchen Angriff auf einen Computer mit Festplattenverschlüsselung vorführen.

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

Veranstaltungshinweise

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

April 2019	
11.-12.04.	Security Forum 2019 (Hagenberger Kreis zur Förderung der digitalen Sicherheit, Hagenberg/AT)
24.-26.04.	DFRWS EU Conference (DFRWS, Oslo/NOR)
Mai 2019	
06.-09.05.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
13.-17.05.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
19.-23.05.	Eurocrypt 2019 (IACR, Darmstadt)
21.-23.05.	16. Deutscher IT-Sicherheitskongress (BSI, Bonn)
22.-23.05.	20. Datenschutzkongress (EUROFORUM Deutschland SE, Berlin)
26.-30.05.	OWASP AppSec Tel Aviv 2019 (OWASP Foundation, Tel Aviv/ISR)
Juni 2019	
03.-05.06.	Entwicklertag 2019 (VKSI, GI, ObjektForum, Karlsruhe)
03.-04.06.	DuD 2019 (COMPUTAS Gisela Geuhs GmbH, Berlin)

Fundsache

Über 140 Mal taucht „ji32k7au4a83“ in Datenbanken kompromittierter Passwörter auf. Was auf den ersten Blick verwundert, hat eine simple Erklärung: Im taiwanesischen Zeichenschema lautet der vermeintliche Zufallsstring übersetzt „Mein Passwort“.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Dr. Safuat Hamdy (Gastautor), Hans-Joachim Knobloch, Sarah Niederer, Jannis Pinter, Friederike Schellhas-Mende, Christian Titze

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

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 2019

High Noon

Zweifellos eine Sternstunde der Filmgeschichte: das Duell zwischen Recht und Verbrechen, vertreten durch Marshal Will Kane (Gary Cooper) und den Banditen Frank Miller. Fred Zinnemanns Film erzählt auch eine Geschichte von Feigheit und Pflichtbewusstsein, Treue und Mut – aber darum geht es hier nicht. Es ist die Unausweichlichkeit, mit der sich die Handlung von der ersten Filmminute an auf das große Finale hinbewegt, die an amerikanische Cloud-Anbieter denken lässt. Denn ganz ähnlich spitzt sich seit Jahren die Spannung zwischen ihnen und dem europäischen Datenschutzrecht zu.

Es begann mit kleinen Scharmützeln wie der Auseinandersetzung um Google Analytics (wenig überzeugend gelöst durch den AV-Kompromiss des Hamburgischen Datenschutzbeauftragten) oder den gerade vor dem EuGH verhandelten Social Media Plug-ins. Dann kamen 2013 die Enthüllungen Edward Snowdens, die das EU-Parlament zur Verabschiedung der Datenschutz-Grundverordnung (DSGVO) motivierten und dazu beitrugen, das Safe Harbor-Abkommen zu kippen – mit einem EuGH-Urteil, dessen Begründung auch den Standardvertragsklauseln den Boden entzog.

Nun drohen die Cloud-Geschäftsmodelle von Microsoft und Amazon am europäischen Datenschutzrecht zu zerschellen. Zwar reagierte Microsoft schnell: mit einem irischen Rechenzentrum, ausgereiften Verträgen und der Weigerung, einer richterlichen Anordnung Folge zu leisten, die Zugriff auf in Irland gespeicherte Daten verlangte. Da fiel ihnen am 23.03.2018 der US CLOUD Act in den Rücken, der amerikanische Unternehmen verpflichtet, im Ausland gespeicherte Daten auch ohne Rechtshilfeabkommen an US-Behörden herauszugeben – ein Verstoß gegen Artikel 48 der DSGVO. Am 07.11.2018 stellte daher die Datenschutzfolgenabschätzung der niederländischen Aufsichtsbehörde die DSGVO-Konformität von Office 365 in Frage. Fehlt noch, dass der US-EU Privacy Shield (erwartungsgemäß) vor dem EuGH scheitert. Dann ist High Noon. Mit offenem Ausgang.

Inhalt

secorvo
security consulting

Security News

Firmenprofile in Social Networks

Die für den 11.04.2019 angekündigte Entscheidung des Bundesgerichtshofes (BGH) in der Sache I ZR 186/17 („Facebook“) mutierte zu einem Aussetzungsbeschluss: Der BGH will zunächst das in Kürze fällige Urteil des EuGH über Social Media Plug-ins (namentlich: Facebook Like Buttons) abwarten. Die bereits am 19.12.2018 veröffentlichten Schlussanträge des Generalanwalts Bobek lassen erwarten, dass der EuGH von einer gemeinsamen Verantwortung ausgehen wird – was dann analog auch für Firmenprofile in Social Networks zutrifft. Solche Profile müssen daher wie Webseiten mit einem Impressum und einer Datenschutzerklärung versehen sein – mindestens als Verlinkung der entsprechenden Erklärungen der Unternehmenswebseite.

Altlasten und Seitenkanäle I

Seit 2005 kann TLS nicht nur mit Zertifikaten, sondern auch mit einem vorab vereinbarten symmetrischen Pre-Shared-Key (PSK) genutzt werden. Israelische Sicherheitsforscher haben am 05.04.2019 einen *Selfie Attack* getauften Angriff auf TLS-PSK (1.3) veröffentlicht, bei dem ein Client durch einen aktiven MITM-Angriff zum „Selbstgespräch“ veranlasst wird – was zu erheblichen Problemen auf höheren Anwendungsschichten führen kann. Entwickler (und Nutzer) betroffener Anwendungen sollten die empfohlenen Schutzmaßnahmen ergreifen oder, besser noch, TLS ausschließlich mit Zertifikaten einsetzen.

Bereits am 06.02.2019 hat eine Forschergruppe um Adi Shamir einen Angriff auf den RSA-Schlüsselaustausch in TLS beschrieben, der Seitenkanäle wie das Cache-Timing nutzt, um trotz diverser Gegenmaßnahmen in neueren Browsern und TLS-Versionen das 1998 von Daniel Bleichenbacher publizierte adaptive Angriffsschema gegen das RSA-Padding nach dem veralteten PKCS#1 v1.5 umzusetzen. Zwar ist ein solcher RSA-Schlüsselaustausch in TLS 1.3 nicht mehr zulässig. Unterstützt ein Server aber auch ältere Protokollversionen mit RSA-Schlüsselaustausch, ist ein Downgrade-Angriff auch gegen TLS 1.3 möglich. Schutz bieten eine komplette Umstellung auf TLS 1.3 oder die Nutzung von Zertifikaten auf Basis von ECC-Verfahren.

Zweifel an Office 365

Bereits am 07.11.2018 hat die niederländische Datenschutzaufsichtsbehörde eine umfangreiche Datenschutz-Folgenabschätzung zu Microsoft Office 365 veröffentlicht. Darin wurden zahlreiche Punkte beanstandet und Microsoft aufgefordert, diese bis April 2019 zu beheben. Die Probleme umfassen nicht nur technische Aspekte wie z. B. die Beobachtung, dass umfangreiche Telemetriedaten „nach Hause gefunkt“ werden, ohne dass die Nutzer dies wissen. Problematisch ist auch, dass Unternehmen mit Sitz in den USA den US-Behörden im Falle von Ermittlungsverfahren aufgrund des CLOUD Act Zugriff auch auf (Cloud-) Server in Europa gewähren müssen, selbst wenn die Voraussetzungen des Art. 48 DSGVO nicht vorliegen.

Nach einer Pressemitteilung des europäischen Datenschutzbeauftragten werden nun auch die vertraglichen Beziehungen zwischen Microsoft und den EU-Behörden überprüft. Ziel ist es herauszufinden, ob hier – wie in den Niederlanden – Datenschutzverstöße festzustellen sind und ob die Datenübermittlungen im Einklang mit Art. 48 DSGVO stehen.

Unternehmen aus Drittstaaten, die Cloud-Dienste in Europa DSGVO-konform anbieten wollen, könnten diese von einem europäischen Anbieter als Treuhänder erbringen lassen, ohne selbst Zugriff auf die Daten zu haben. Aber auch hier steckt der Teufel im Detail: Betreibt der europäische Partner eine Niederlassung in den USA, könnten die US-Behörden durch diese Hintertür zugreifen.

Altlasten und Seitenkanäle II

Auch im neuen WLAN-Sicherheitsstandard WPA3-Personal (SSN 01/2018) haben Sicherheitsforscher mehrere Mängel entdeckt und am 10.04.2019 unter dem Namen *Dragonblood* veröffentlicht, die eine Rekonstruktion des WLAN-Pre-Shared-Key ermöglichen.

WPA3-Personal ersetzt den gegen Offline-Wörterbuchangriffe anfälligen Vier-Wege-Handshake von WPA2-Personal durch SAE – auch als Dragonfly bekannt –, das derartige Angriffe verhindern soll. Um den Übergang zum neuen Protokoll zu erleichtern, definiert WPA3 einen „Transition Mode“, in dem sowohl WPA3- als auch WPA2-Clients unterstützt werden. In diesem Mischbetrieb lässt sich jedoch ein Downgrade auf WPA2 provozieren, wodurch der Angriff wieder möglich wird. Zwei weitere Dragonblood-Angriffe bedienen sich eines Timing- bzw. Cache-Seitenkanals, um den PSK über einen Wörterbuchangriff zu ermitteln. Schließlich wurde ein Downgrade-Angriff entdeckt, der das Sicherheitsniveau auf die schwächste von Client und Access Point unterstützte Diffie-Hellman-Gruppe absenkt.

Einige der Schwächen lassen sich per Software entschärfen; entsprechende Sicherheitsupdates sollten zügig installiert werden. Ein Mischbetrieb von WPA3/WPA2 sollte unbedingt vermieden werden.

secorvo
security consulting

Europäische Hilfestellung

Der Europäische Datenschutzausschuss hat am 09.04.2019 Richtlinien zur Datenverarbeitung bei Diensten der Informationsgesellschaft verabschiedet und zur öffentlichen Konsultation gestellt. In dem 14-seitigen Papier erläutert der Ausschuss seine enge Auslegung des Art. 6 Abs. 1 b) DSGVO: Mit der Erforderlichkeit zur Vertragsdurchführung sollen nur solche Verarbeitungen personenbezogener Daten legalisiert werden, ohne die der Vertrag nicht erfüllt werden kann. Dabei seien auch die Erwartungen der Betroffenen zu berücksichtigen.

Analysen des Nutzerverhaltens, Sicherheitslogs, Speicherungen zu Gewährleistungszwecken oder aufgrund von Aufbewahrungspflichten seien nicht von Abs. 1 b) umfasst, sondern erforderten andere Rechtsgrundlagen. Zweifellos eine zutreffende Klarstellung. Daraus folgt jedoch, dass die Betroffenen gemäß Art. 12 ff DSGVO über diese zu informieren sind. Exzessive Verarbeitungen werden sich so kaum verhindern lassen – die Laienverständlichkeit der Datenschutzerklärung dürfte jedoch leiden.

Hambacher Manifest

Die 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat am 03.04.2019 unter anderem Anforderungen an die datenschutzgerechte Entwicklung von KI-Anwendungen unter dem Titel „Hambacher Erklärung zur Künstlichen Intelligenz“ verabschiedet. Die Anforderungen starten mit dem Grundsatz aus Art. 22 DSGVO, rechtlich relevante Entscheidungen nicht ausschließlich auf automatisierte Prozesse zu stützen sowie auch für Trainingsdaten das Zweckbindungsgebot zu beachten. Datenminimierung, die Entwicklung technischer und organisatorischer Standards, die klare Festlegung von Verantwortlichkeiten sowie der Anspruch, die Entwicklung auch politisch zu steuern und die regelmäßige Durchführung von Datenschutz-Folgenabschätzungen sind weitere Anforderungen.

Kein revolutionärer Wurf – zumal das Mantra der Transparenz nicht kritisch hinterfragt wird. Gerade bei KI-Anwendungen sind Zweifel angebracht, ob diese tatsächlich kurz, verständlich und für den Betroffenen nachvollziehbar dargestellt werden können – und ob dies der richtige Ansatz zum Schutz der Betroffenenrechte ist.

Secorvo News

200 Security News

Sie lesen gerade die 200. Ausgabe der Secorvo Security News. 800 Seiten mit rund 1.500 Nachrichten, die wir für Sie recherchiert, ausgewählt und formuliert haben, ungezählte fachliche Diskussionen und Tassen Kaffee liegen hinter uns. Die Security News haben mehr Leser als die meisten deutschen Fachzeitschriften im Gebiet Informationssicherheit und Datenschutz – und darauf sind wir auch ein kleines bisschen stolz.

Wir würden uns freuen, wenn Sie die Jubiläumsausgabe zum Anlass nähmen, uns in einem kurzen Kommentar zu verraten, was Sie uns schon immer einmal sagen wollten… Unter allen Einsendern verlosen wir die ersten zehn Exemplare der in Kürze erscheinenden dritten Auflage unseres Fachbuchs „Datenschutz und Informationssicherheit“.

T.I.S.P.-Zertifizierung

Kurzentschlossene können sich noch einen Platz auf dem T.I.S.P.-Seminar am **13.–17.05.2019** sichern. Die (über)nächste Gelegenheit zur Zertifizierung Ihrer Kenntnisse in der Informationssicherheit bieten wir am **14.–18.10.2019** (Achtung: nur noch vier freie Plätze, baldige Anmeldung empfohlen).

Wie souverän ist der Souverän?

Angesichts der wachsenden Komplexität von IT-Systemen, dem Eindringen der IT in immer mehr Lebensbereiche und der Zunahme der Verarbeitung personenbezogener Daten ist "digitale Souveränität" nicht mehr lediglich von mangelnder Medienkompetenz bedroht. Beim kommenden KA-IT-Si-Event am **06.06.2019** in Kooperation mit der Initiative Smart Ettlingen zeichnet Dirk Fox die Entwicklung des Internet vom "Schaufenster" zu einer Überwachungsinfrastruktur nach und zeigt auf, welche Verantwortung für die Erhaltung (oder womöglich die Wiederherstellung) von digitaler Souveränität auf die Softwareentwickler von heute und morgen zukommt – und welche Schritte dafür erforderlich sind. Im Anschluss folgt eine Diskussion zum Thema "Digitale Souveränität im internationalen Kontext". Danach haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking" (Anmeldung).

11. Tag der IT-Sicherheit

Für die Keynote des bereits elften Karlsruher „Tag der IT-Sicherheit“ konnten wir die polnische IT-Security-Expertin Paula Januszkiewicz („*Think and Act Like a Hacker to Protect Your Company's Assets*“) gewinnen. Die Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, KASTEL und dem CyberForum e.V. findet am **11.07.2019** im Saal Baden der IHK Karlsruhe statt. Das vollständige 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

Mai 2019	
06.-09.05.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
13.-17.05.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
14.-17.05.	European Identity & Cloud Conference 2019 (KuppingerCole Ltd., München)
19.-23.05.	Eurocrypt 2019 (IACR, Darmstadt)
21.-23.05.	16. Deutscher IT-Sicherheitskongress (BSI, Bonn)
22.-23.05.	20. Datenschutzkongress (EUROFORUM Deutschland SE, Berlin)
26.-30.05.	OWASP AppSec Tel Aviv 2019 (OWASP Foundation, Tel Aviv/ISR)
Juni 2019	
03.-05.06.	Entwicklertag 2019 (VKSI, GI, ObjektForum, Karlsruhe)
03.-04.06.	DuD 2019 (COMPUTAS Gisela Geuhs GmbH, Berlin)
05.-06.06.	BvD-Verbandstage 2019 (BvD e.V., Berlin)
13.-14.06.	Annual Privacy Forum 2019 (ENISA, EC DG Connect, Universität Wien, Rom/I)
17.-19.06.	4rd IEEE European Symposium on Security and Privacy (IEEE Computer Society, Stockholm/SWE)
24.-25.06.	T.I.S.P. Update Schulung (isits AG, Bochum)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Hans-Joachim Knobloch, Michael Knopp, Jannis Pinter, Friederike Schellhas-Mende.

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 2019

Kognitive Verzerrungen

Eine der an Einsichten reichste Lektüre der vergangenen Jahre war für mich die Veröffentlichung des Wirtschaftsnobelpreisträgers 2002, Daniel Kahneman: ‚Thinking, fast and slow' (‚Schnelles Denken, langsames Denken', 2011). Darin deckt der Psychologe Wirkmechanismen des menschlichen Denkens auf, die viele Wunderlichkeiten des Homo Rationalis (von ihm „kognitive Verzerrungen" genannt) verständlich machen.

Ein zentraler Mechanismus ist das Denken in Relationen. Wir kennen das von optischen Täuschungen: Identische Objekte erscheinen im Kontext kleinerer bzw. größerer Objekte unterschiedlich groß – selbst wenn wir um ihre gleiche Größe *wissen*, können wir sie nicht gleich groß *sehen*. Diese Relativität durchzieht unser gesamtes Denken. Der Mechanismus wird besonders offensichtlich bei Entscheidungen in Geldfragen: Nicht der absolute Preis, sondern das Verhältnis zu anderen Preisen ähnlicher Güter entscheidet. Das gilt vor allem, wenn eine Ware oder Leistung keinen allgemein anerkannten, „typischen" Preis besitzt: Eine Uhr für 1.400 € erscheint teuer neben einer für 99 €, aber günstig neben einer für 4.500 €.

Umgekehrt fällt es Menschen schwer, den Wert vieler „abstrakter Güter" wie Bildung, Gesundheit oder Freiheit einzuordnen. Damit erscheinen sie „unvergleichbar", denn sie lassen sich vom menschlichen Gehirn nicht in Relation zu anderen Gütern oder Werten setzen. Wie wertvoll ist unsere Privatsphäre? Und wie hoch der Verlust, wenn z. B. unsere E-Mail-Adresse bekannt wird?

Das ändert sich sofort, wenn ihnen ein Preis zugeordnet wird. Und vielleicht wird dies eines Tages das größte Vermächtnis der DSGVO sein: Über die von den Aufsichtsbehörden verhängten Ordnungsgelder erhält unsere Privatsphäre einen Wert, der sie vergleichbar macht. So wissen wir nun: Die Preisgabe von E-Mail-Adressen in einem Verteiler kostet 2.000 €. Fast so viel wie zwei iPhone XS.

Inhalt

secorvo
security consulting

Security News

ZombieLoad und Firmwareschwachstellen

Gleich zwei Mal machte der Chiphersteller Intel im Mai durch Schwachstellen auf sich aufmerksam. Am 14.05.2019 veröffentlichte Intel das Security Advisory INTEL-SA-00213, in dem mehrere kritische Schwachstellen in der Firmware beschrieben werden. Am selben Tag wurde eine neue Schwachstellenkategorie namens Microarchitectural Data Sampling (MDS) bekannt: Wird der Prozess eines Angreifers auf dem gleichen Kern wie ein Opferprozess ausgeführt, so kann der Angreifer Speicherbereiche des Opfers lesen. Im Kontext von Hyper Threading funktionieren derartige Angriffe besonders gut. Die Fallout, RIDL und ZombieLoad genannten Schwachstellen folgen den Schwachstellen Spectre und Meltdown: Schon wiederholt wurden Schwachstellen sowohl in den Intel CPUs als auch in den Management-Technologien (z. B. der Intel Management Engine) entdeckt. Ursache dieser Schwachstellen sind eine immer höhere Komplexität und Leistungsoptimierung auf Kosten der Sicherheit. So bringen moderne Plattformen diverse schlecht oder gar nicht dokumentierte Features mit, die die Angriffsfläche erhöhen. Für die aktuellen Schwachstellen stehen Sicherheitsupdates bereit, die unverzüglich eingespielt werden sollten.

Spyware Hook

Am 14.05.2019 wurde bekannt, dass die israelische Firma NSO Group eine kritische Schwachstelle in WhatsApp nutzte, um Spyware auf iOS- und Android-Smartphones zu installieren. Dazu genügte ein telefonischer Verbindungsversuch, der nicht einmal in der Anrufliste erscheint.

Kunden der auf Cyberwarfare spezialisierten Firma sind – eigenen Angaben zufolge – Regierungen und deren Sicherheitsbehörden, die damit Terrorismus bekämpfen. In jüngster Vergangenheit wurden Angriffswerkzeuge der NSO Group aber auch gegen Menschenrechtsaktivisten, Journalisten und mindestens einen Anwalt eingesetzt. Meldungen über ähnliche Angriffe, die ebenfalls in Verbindung zur NSO Group stehen, gab es bereits im August 2018.

Aber ganz unabhängig vom Geschäftsmodell des Unternehmens bleibt zu fragen, was von einem Unternehmen zu halten ist, dass entdeckte Sicherheitslücken zu eigenen Geschäftszwecken geheim hält – und damit wissentlich Milliarden Endgeräte weiter potentiellen Angriffen aussetzt.

Log-Password-Leaks

Passwörter sollen nur mit einer geeigneten Hash-Funktion und einem individuellen Salt geschützt gespeichert werden – das ist Best Practice, wie man u. a. beim NIST nachlesen kann. Auch Facebook, GitHub, Google und Twitter wissen das. Trotzdem hatten alle vier Unternehmen in jüngerer Vergangenheit Schwierigkeiten, das beim Umgang mit Nutzerpasswörtern zu beherzigen, wie zuletzt am 21.05.2019 von Google gemeldet: So wurden die eingegebenen Passwörter als „Beifang“ in Log-Dateien des Anbieters protokolliert. Bei Facebook hatten mehr als 20.000 Facebook-Mitarbeiter Zugriff auf diese Protokolle.

Zur Fehlerbehebung ist das Protokollieren von Anfragen äußerst nützlich, aber Passwörter haben darin nichts verloren und dürfen niemals im Klartext gespeichert werden. Dem Endnutzer bleibt nur darauf zu vertrauen, dass die Anbieter in dieser Hinsicht keine Fehler machen. Weil das aber ganz offensichtlich selbst bei großen Anbietern keine Selbstverständlichkeit ist, sollten Endnutzer für jeden Dienst ein anderes Passwort verwenden. Und gegen Vergessen hilft ein Passwortmanager.

Angreifbare Altlasten

Eine Standardinstallation von Windows 10 umfasst neben dem Edge-Browser noch heute den immer weniger gepflegten Internet Explorer (IE). Eine am 28.03.2019 veröffentlichte XXE-Schwachstelle beim Umgang mit MHTML-Dateien (*.mht) erlaubt es Angreifern, über eine manipulierte MHTML-Seite Dateien vom System des Opfers zu laden.

Aus dem Internet heruntergeladene Dateien werden unter Windows mit dem so genannten „Mark of the Web“ (MOTW) versehen – einem speziellen Attribut, welches eine Datei als nicht vertrauenswürdig einstuft und die weitere Verarbeitung einschränkt. Dadurch würde der Angriff normalerweise verhindert, doch der Mechanismus funktioniert nicht ordnungsgemäß beim Download mit Edge, da dieser die Zugriffsberechtigungen der heruntergeladenen Datei durch ein nicht dokumentiertes Sicherheits-Feature so verändert, dass niedrig privilegierte Prozesse wie die des IE die Dateiattribute nicht mehr lesen können. Anstatt die Datei in einem solchen Fall als „nicht vertrauenswürdig“ einzustufen, macht der IE das Gegenteil.

Offizielle Patches für diese Probleme gibt es bisher nicht und Microsoft kündigte lediglich an, dass eine Lösung in einer zukünftigen Version des Internet Explorers „in Erwägung gezogen“ werde. Bis dahin kann man sich vor solchen Angriffen nur schützen, indem man MHTML-Dateien standardmäßig mit einem anderen Programm als dem IE öffnet (z. B. einem Texteditor) oder den Internet Explorer deaktiviert. Alternativ hilft auch der Drittpartei-Patch von 0patch (ohne Gewähr).

secorvo
security consulting

Automatisieren statt Aufpassen

Anfang Mai konnten Firefox-Anwender weltweit keine Add-ons mehr ausführen, weil deren Code-Signatur als ungültig erkannt wurde: Das Zertifikat einer Intermediate-CA im Zertifikatspfad der Code-Signing-Zertifikate für Add-on Entwickler war am 04.05.2019 abgelaufen. Die Mozilla-Entwickler hatten als Validierungszeitpunkt den Termin gewählt, an dem das betreffende Add-on geladen wird – und nicht den Zeitpunkt, zu dem die Code-Signatur angebracht wurde. Microsofts Authenticode Code-Signaturverfahren nutzt dazu korrekter Weise Timestamps.

Noch blamabler ist, dass das Intermediate-CA-Zertifikat ohne eine rechtzeitige Erneuerung ablaufen konnte – zumal Mozilla das gleiche Malheur bereits drei Jahre zuvor unterlaufen ist. Dabei sollte die Erneuerung von Zertifikaten und CRLs wo immer möglich automatisiert und der Gültigkeitsstatus aktiv überwacht werden. Besser Aufpassen war noch nie eine gute Empfehlung.

Arbeitszeiterfassung und Leistungskontrolle

Mit Urteil C-55/18 vom 14.05.2019 verpflichtet der EuGH Arbeitgeber, die tägliche Arbeitszeit der Arbeitnehmer zu messen. Was der einen (insbesondere Gewerkschaften und Co.) Freud, da nun endlich die geleisteten Überstunden erfasst werden, ist der anderen Leid: Die Arbeitgeber fürchten einen Rückfall in Stechuhrzeiten, den Wegfall flexibler Arbeitszeitmodelle und Schwierigkeiten im Hinblick auf die Ruhezeiten. Datenschutzrechtlich stellt die Einführung von Systemen zur Zeiterfassung kein großes Problem dar: § 26 BDSG bietet dafür die notwendige Rechtsgrundlage.

Zugleich erwägen viele Unternehmen, Client-Monitoring-Systeme einzuführen, mit denen oft auch eine sehr einschneidende Kontrolle insbesondere der Arbeitnehmerleistung möglich ist. Da solche Systeme häufig automatisiert Entscheidungen treffen, wird nicht nur die Rechtsgrundlage des § 26 BDSG verlassen, sondern auch der Anwendungsbereich des Art. 22 DSGVO mit weitreichenden datenschutzrechtlichen Konsequenzen eröffnet. So müssen die Arbeitnehmer mindestens in die Verarbeitung einwilligen – ein stacheliges Unterfangen, da die Freiwilligkeit einer Einwilligung im Arbeitsverhältnis regelmäßig in Frage steht.

Damit ist klar, dass die EuGH-Entscheidung keineswegs als Freibrief für die Einführung von Leistungskontrollen missverstanden werden darf.

Secorvo News

Neu: Der PKI-Blog

Wer sich seit über fünfunddreißig Jahren mit Public Key Infrastrukturen (PKI) beschäftigt, hat einiges erlebt: Von den ersten RSA-Implementierungen auf PCs und Smartcards über das „Web of Trust" von Phil Zimmermans „Pretty Good Privacy" bis zur gesetzlichen Regulierung von „elektronischen Signaturen" und den manchmal bizarren Auswüchsen bei der praktischen Umsetzung. Inzwischen sind PKIs das Rückgrat vieler Sicherheitsmechanismen – und daher bei Fehlern auch gelegentlich Ursache weit reichender Sicherheitsprobleme. Seit Kurzem gewährt der Secorvo-PKI-Experte Hans-Joachim Knobloch einen Einblick in seine Erfahrungen und Erlebnisse rund um PKIs – in seinem eigenen PKI-Blog. Lesenswert.

Wie souverän ist der Souverän?

Angesichts der wachsenden Komplexität von IT-Systemen, dem Eindringen der IT in immer mehr Lebensbereiche und der Zunahme der Verarbeitung personenbezogener Daten ist „digitale Souveränität" nicht mehr lediglich von mangelnder Medienkompetenz bedroht. Beim kommenden KA-IT-Si-Event am **06.06.2019** in Kooperation mit der Initiative Smart Ettlingen zeichnet Dirk Fox die Entwicklung des Internet vom „Schaufenster" zu einer Überwachungsinfrastruktur nach und zeigt auf, welche Verantwortung für die Erhaltung (oder womöglich die Wiederherstellung) von digitaler Souveränität auf die Softwareentwickler von heute und morgen zukommt – und welche Schritte dafür erforderlich sind. Im Anschluss folgt eine Diskussion zum Thema „Digitale Souveränität im internationalen Kontext". Danach haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (Anmeldung).

11. Tag der IT-Sicherheit

Für die Keynote des bereits elften Karlsruher „Tag der IT-Sicherheit" konnten wir die polnische IT-Security-Expertin Paula Januszkiewicz (‚Think and Act Like a Hacker to Protect Your Company's Assets') gewinnen. Die Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, KASTEL und dem CyberForum e.V. findet am **11.07.2019** im Saal Baden der IHK Karlsruhe statt. Das vollständige 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 2019	
03.-05.06.	Entwicklertag 2019 (VKSI, GI, ObjektForum, Karlsruhe)
03.-04.06.	DuD 2019 (COMPUTAS Gisela Geuhs GmbH, Berlin)
05.-06.06.	BvD-Verbandstage 2019 (BvD e.V., Berlin)
06.06.	Wie souverän ist der Souverän? (KA-IT-Si, Karlsruhe)
13.-14.06.	Annual Privacy Forum 2019 (ENISA, EC DG Connect, Universität Wien, Rom/I)
17.-19.06.	4rd IEEE European Symposium on Security and Privacy (IEEE Computer Society, Stockholm/SWE)
Juli 2019	
11.07.	11. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
14.-17.07.	DFRWS USA 2019 (DFRWS, Portland/US)
16.-20.07.	PETS 2019 (University of Minnesota, Stockholm/SWE)

Fundsache

Der am 09.04.2019 veröffentlichte Mindeststandard des BSI zur Verwendung von Transport Layer Security (TLS) hätte besser acht Tage früher erschienen sollen: Streicht man von den kompakten neun Seiten die Formalia (Deckblatt, Adressangabe, Vorwort, Inhaltsverzeichnis, Beschreibung, Literaturverzeichnis, Abkürzungsverzeichnis) und die überflüssige Grafik, bleibt nur Seite sechs übrig. Und es ginge noch kompakter: "Mindeststandard: Wenn TLS verwendet wird, dann müssen die Vorgaben aus BSI TR-02102-2 eingehalten werden." Aha.

Impressum

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

ISSN 1613-4311

Autoren: André Domnick, Fabian Ebner, Dirk Fox (Editorial), Stefan Gora, Hans-Joachim Knobloch, Jannis Pinter, Friederike Schellhas-Mende, Christian Titze

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 2019

Der Wert des Flüchtigen

Wenn ich dieses Editorial verfasse weiß ich nicht nur, dass es viele Menschen lesen werden. Ich weiß auch, dass ich nicht wissen kann, wer genau es lesen wird – oder anders herum: Ich muss damit rechnen, dass es jeder Mensch lesen könnte. Auch Menschen, die mich nicht kennen, meine Äußerungen nicht in den Gesamtkontext einordnen werden oder können, vielleicht Sätze aus dem Zusammenhang reißen. Daher werde ich mich besonders um Unmissverständlichkeit bemühen, um die korrekte Verwendung von Begriffen und die Klarheit meiner Überlegungen. Das muss nicht gelingen – aber vor der Veröffentlichung werde ich überzeugt sein, dass ich es nicht klarer und unmissverständlicher schreiben konnte. Umgekehrt wird jeder Leser genau das wissen. Und mir daher jeden Satz und jede Äußerung auch zurechnen. Einmal in der Welt lässt sich ein solcherart veröffentlichter Gedanke nicht mehr zurücknehmen. Das ist auch bedeutsam, denn erst diese Ernsthaftigkeit verleiht ihm das nötige Gewicht.

Daneben (besser: davor und dahinter) gibt es aber auch das nichtöffentliche, gesprochene Wort: Dem kann dieses Gewicht nicht beigemessen werden. Und darf es nicht. Es muss zurücknehmbar bleiben, vorläufig und flüchtig. Dieser Schutz vor unerwarteter oder unerwünschter Kenntnisnahme durch Dritte ist essentiell: Denn wir benötigen den Raum des Vorläufigen und Flüchtigen, damit Gedanken und Überzeugungen im Diskurs reifen können. Der öffentliche Umgang mit privaten Äußerungen von Politikern (die hinsichtlich aller ihrer Äußerungen natürlich in einer besonderen Verantwortung stehen) macht manchmal vergessen, wie bedeutsam diese Flüchtigkeit für eine freie Gesellschaft ist.

Wer daher den Zugriff auf Daten von Sprachassistenten fordert, hat nicht nur den Datenschutz und die Unverletzlichkeit der Wohnung, sondern auch das Fundament einer freiheitlichen Ordnung nicht verstanden.

Inhalt

secorvo
security consulting

Security News

Magische Technologien

Ransomware ist derzeit eine der größten digitalen Gefahren für Unternehmen und Behörden. Sind die Daten erst einmal verschlüsselt, hilft in der Regel nur eine gelebte Disaster-Recovery-Strategie. Oft fehlt sie – und die Opfer wenden sich verzweifelt an Datenwiederherstellungs-Experten. Doch ohne bekannte Schwachstellen in der Ransomware hilft auch das nicht, denn die verwendeten starken Verschlüsselungsalgorithmen können nicht gebrochen werden. Mehrere US-amerikanische Data-Recovery-Firmen verfügen jedoch nach eigenen Angaben über „proprietäre Technologien", um die Daten zu entschlüsseln – wie kann das sein?

Wie Pro Publica am 15.05.2019 publizierte, besteht die magische „proprietäre Technologie" darin, unter der Hand das Lösegeld zu bezahlen... Die Firmen bieten den Opfern einen risikofreien Weg aus der Ransomware-Falle. Ransomware-Entwickler umwerben diese Firmen offenbar als vertrauenswürdige Mittelsmänner und bieten ihnen Vergünstigungen, Rabatte und Verlängerungen von Deadlines an. Lesson learned: „Magische Technologien" mag es geben – allerdings nicht in der Kryptografie.

Dem Trustcenter ausgeliefert

Auch Schadsoftware kann mit einer gültigen Code-Signatur versehen werden. Forscher veröffentlichten am 22.05.2019 eine auf den Daten von VirusTotal basierende Top-25-Liste der Trustcenter, mit deren Zertifikaten mutmaßliche Malware signiert wurde. Ganz oben: die Comodo CA. Deren neuer Betreiber Sectigo sperrte daraufhin am 24.05.2019 127 betroffene Zertifikate.

Wie am 30.05.2019 bekannt wurde, war darunter jedoch mindestens ein Code-Signing-Zertifikat eines legitimen Sectigo-Kunden, dessen CAD-Software von fünf der 70 Virenscanner fälschlich als Malware klassifiziert wurde. Nach der Sperrung beschwerten sich Anwender zuhauf beim Hersteller, dass ihre CAD-Software nicht mehr lief. Sectigo hat formal korrekt gehandelt: Nach Kapitel 4.9.1 der Baseline Requirements des CA/Browser-Forums muss ein Trustcenter ein Zertifikat nach spätestens fünf Tagen sperren, wenn „*The CA obtains evidence that the Certificate was misused*". Wie sorgfältig die Indizien zu prüfen sind, ist nicht genauer spezifiziert. Eine Haftung für fälschliche Sperrung ist nicht vorgesehen. Zwar hätten fünf Tage wohl gereicht, um den Sachverhalt mit dem betroffenen Kunden zu klären – das aber ist in diesem Fall offenbar unterblieben. Wer Zertifikate für geschäftskritische Zwecke nutzt, sollte also besser regelmäßig selbst den Sperrstatus der eigenen Zertifikate prüfen.

Crypto Wars 2.0

Verwendet man TLS mit Perfect Forward Secrecy (PFS) ist es auch bei Kenntnis des privaten Schlüssels unmöglich, aufgezeichnete TLS-Sitzungen nachträglich zu entschlüsseln. Aus Compliance-Gründen (Network Monitoring in internen Netzen) unterstützt das vom Europäischen Institut für Telekommunikationsnormen (ETSI) entwickelte ETS-Protokoll (vormals eTLS) PFS nicht. MITRE listet es daher seit dem 26.02.2019 auf Betreiben der Electronic Frontier Foundation (EFF) offiziell als Schwachstelle (CVE-2019-9191). Der Bankensektor, insbesondere die Industriegruppe BITS, versuchte schon während der Standardisierung TLS 1.3 durch die Entfernung von PFS zu schwächen. Webbrowser können ETS und TLS 1.3 nicht unterscheiden, da ETS PFS mit statischen Diffie-Hellman-Schlüsselpaaren realisiert.

Eine von derzeit vielen Bestrebungen, Krypto-Protokolle zu schwächen. So sollen beispielsweise Messenger-Dienste gesetzlich verpflichtet werden, Strafverfolgungsbehörden in Verdachtsfällen einen Zugriff auf die entschlüsselte Kommunikation zu ermöglichen. Keine neue Diskussion – und es gilt noch immer, was auch der Bundesverbandes IT-Sicherheit e.V. (TeleTrusT) am 12.06.2019 publizierte: Backdoors schwächen nicht nur das Vertrauen der Nutzer in IT-Systeme, sondern können auch missbräuchlich genutzt werden. Keine gute Idee.

Certificate Transparency

Damit Zertifikate von Google Chrome als gültig anerkannt werden, müssen öffentlichen Zertifizierungsstellen diese seit dem 30.04.2018 vor der Ausstellung als *Precertificate* in mehrere öffentliche Certificate-Transparency-Protokolle schreiben. Ein echter Sicherheitsgewinn für die Web-PKI, denn nun kann jeder diese Protokolle durchsuchen – beispielsweise durch die Website crt.sh –, fehlerhafte Ausstellungen erkennen, melden und eine rasche Sperrung veranlassen.

So wurde am 16.04.2019 aufgedeckt, dass die französische Zertifizierungsstelle Certinomis unter anderem Zertifikate für nicht registrierte Domains und solche mit ungültigen Object Identifiers (OIDs) ausgestellt hatte. Wegen mehreren Verstößen gegen Baseline Requirements wird sie nun aus dem Root-Programm von Mozilla Firefox Version 69 entfernt; Certimonis-Zertifikate sind damit nicht mehr vertrauenswürdig. Auch die Zertifizierungsstellen Sectigo, SECOM und DigiCert sind betroffen: Sie haben Extended-Validation-Zertifikate (EV), die nur nach besonders sorgfältiger Überprüfung des Antragstellers ausgestellt werden dürfen und daher im Browser mit einer „grünen Adressleiste" belohnt

werden, teilweise mit „Default City“ als Städtenamen oder „Some-State“ als Staatsnamen ausgestellt. Die betroffenen Zertifikate wurden gesperrt.

Vielleicht gelingt es ja auf diesem Weg, das angekratzte Vertrauen in die Web-PKI zu kitten.

Private Videoüberwachungen

Das Bundesverwaltungsgericht hat am 27.03.2019 bestätigt, dass die Regelung zur Videoüberwachung im neuen § 4 BDSG mangels Reichweite der Öffnungsklausel der DSGVO nicht für private Stellen gilt. Private Videoüberwachungen sind allein nach Art. 6 Abs. 1 f) DSGVO (Rechtsgrundlage) und insbesondere Art. 13/14 DSGVO (Informationspflichten) zu beurteilen.

Die Entscheidung in der Sache – rechtswidrige Live-Überwachung einer Zahnarztpraxis – erging noch zur alten Rechtslage (§ 6b BDSG aF). Bei den Aussagen zu § 4 BDSG nF handelt es sich also streng genommen eher um ein *obiter dictum*: Das Gericht prüfte, ob eine Pflicht der Aufsichtsbehörde zur Überprüfung der Umsetzung besteht. Nach Überzeugung des Gerichts gelten die Öffnungsklauseln in Art. 6 Abs. 2, 3 DSGVO nur für hoheitliche Verarbeitungen. Für die Prüfung der Erforderlichkeit und Angemessenheit einer Überwachung dürfte es trotz der spezifischeren Ausführungen des § 4 BDSG weitgehend bei den bisherigen Maßstäben bleiben.

Sysmon 10

Das am 14.06.2019 aktualisierte Microsoft-Werkzeug Sysmon (v10.1) unterstützt mit 21 spezifischen EventIDs die Aufzeichnung detaillierter Logs des Laufzeitverhaltens eines Windowssystems (Server wie Clients). Für EventIDs 1 (ProcessCreate) und 7 (ImageLoad) wurde die Eigenschaft „Original FileName“ hinzugefügt, wodurch nun der aufrufende PE-Originaldateiname aufgezeichnet und nachvollziehbar wird. Die EventID 22 (DNSEvent DNS query) wurde ergänzt; sie wird erzeugt, wenn ein Prozess eine DNS-Abfrage ausführt, unabhängig davon, ob das Ergebnis erfolgreich ist oder fehlschlägt: sehr hilfreich bei der Vorfallsanalyse von Anomalien, Schadsoftware oder Datenexfiltrationen, da eine DNS-Protokollierung mit einer spezifischen Prozesszuordnung auf Urheber und Securityidentifier (SID) hinweist.

Diese Erkenntnisse gewinnt man allerdings nur, wenn Sysmon produktiv installiert ist. Mit einem eigenen Symon-Config-File lassen sich die laufenden Ereignisse (Events) in einer zentralen Logauswertung sammeln und auswerten.

Alte Antwort, neue Bedeutung

Am 13.06.2019 hat der Europäische Gerichtshof (EuGH) im Streit zwischen Google und der Bundesnetzagentur entschieden, dass GMail kein elektronischer Kommunikationsdienst nach § 3 Nr. 24 TKG bzw. RL 2002/21/EG ist. Definitionsmerkmal eines Kommunikationsdienstes sei, dass der Dienst ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze besteht. Unstreitig übertragen E-Mail-Provider und andere Anbieter von vergleichbaren Internetdiensten (wie Messengerdienste) die Signale jedoch nicht selbst, sondern bedienen sich der durch Access-Provider angebotenen Infrastruktur.

Die Bedeutung der Entscheidung wird eingeschränkt durch die bevorstehenden Neuregulierungen der bereits bis Dezember 2020 umzusetzenden RL 2018/1972/EU und der ePrivacy-Verordnung. Beide Gesetzgebungen schaffen Rechtsrahmen, die direkt auf E-Mail-Dienste und vergleichbare Angebote zielen. In der Übergangszeit beschränkt das Urteil zwar einerseits u. a. staatliche Zugriffsrechte, andererseits verschärft es die Unsicherheit: Bisher wurde bezüglich des Telekommunikationsgeheimnisses und des Umgangs mit Verbindungsdaten regelmäßig Telekommunikationsrecht angewendet. Zugleich verdrängen die sehr allgemeinen DSGVO-Bestimmungen die Datenschutzbestimmungen des Telemediengesetzes – eine Situation, die der Gesetzgeber baldmöglichst klären sollte.

Secorvo News

Secorvo@itsa

Vom **08. bis 10.10.2019** ist Secorvo wieder auf der it-sa in Nürnberg vertreten. Am Stand 10.1-630 zeigen wir Ihnen u. a. ISMS ready2go und DSMS ready2go, unsere Lösungen für das Informationssicherheits- und Datenschutz-Management. Sie sind herzlich eingeladen, bereits vorab einen Termin mit uns zu vereinbaren. Gerne schicken wir Ihnen auch einen Registrierungscode, mit dem Sie Ihr kostenfreies E-Ticket (Tageskarte) ausdrucken können.

11. Tag der IT-Sicherheit

Für die Keynote des bereits elften Karlsruher „Tag der IT-Sicherheit“ konnten wir die polnische IT-Security-Expertin Paula Januszkiewicz (‚Think and Act Like a Hacker to Protect Your Company's Assets‘) gewinnen. Die Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, KASTEL und dem CyberForum e.V. findet am **11.07.2019** im Saal Baden der IHK Karlsruhe statt. Das vollständige 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

Juli 2019	
11.07.	11. Tag der IT-Sicherheit (IHK Karlsruhe, CyberForum, KASTEL, KA-IT-Si)
14.-17.07.	DFRWS USA 2019 (DFRWS, Portland/US)
16.-20.07.	PETS 2019 (KTH Royal Institute of Technology, Stockholm/SWE)
August 2019	
03.-08.08.	Blackhat USA 2019 (Blackhat, Las Vegas/US)
08.-11.08.	DEF CON 27 (DEFCON, Las Vegas/US)
11.-13.08.	SOUPS 2019 (usenix, Kalifornien/US)
14.-16.08.	28th USENIX Security Symposium (usenix, Santa Clara/US)
18.-22.08.	Crypto 2019 (IACR, Santa Barbara/US)
September 2019	
17.09.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
23.-26.09.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
24.-27.09.	heise devSec 2019 (dpunkt-Verlag, Heidelberg)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Hans-Joachim Knobloch, Michael Knöppler, Michael Knopp, Jannis Pinter, Jochen Schlichting, Christian Titze

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 2019

Modell und Wirklichkeit

Seit Jahrhunderten erforschen Menschen die Welt. Sie erfanden die Gravitation, den Magnetismus und das Sonnensystem, um damit fallende Äpfel, ausgerichtete Kompassnadeln und kreisende Monde zu erklären und mathematisch zu beschreiben. Stieß dieses Wirklichkeitsmodell (z. B. durch den Nachweis der Konstanz der Lichtgeschwindigkeit) an Erklärbarkeitsgrenzen, wurde es flugs erweitert (Relativitätstheorie). Bis heute wissen wir jedoch nicht, ob es die Welt korrekt beschreibt. Die uneingeschränkte Geltung physikalischer Gesetze ist daher nur in diesem Wirklichkeitsmodell gesichert.

Ganz Ähnliches gilt für technische Lösungen. Sie lösen nie ein Wirklichkeitsproblem, sondern funktionieren nur in einem eingeschränkten Modell: So ist ein Auto nur unter bestimmten Voraussetzungen ein Fortbewegungsmittel – nicht unter Wasser, nicht in der Luft, nicht auf dem Mond (zumindest mit Verbrennungsmotor), und selten ohne Fahrweg oder bei Steigungen von über 30%. Leider vergessen wir das gelegentlich und wundern uns, wenn aus solchen Einschränkungen Risiken erwachsen. So zeigte eine israelische Forschergruppe am 23.06.2019, wie eine Drohne durch Vortäuschung von Verkehrszeichen ein Advanced Driver Assistance System (ADAS) beeinflussen kann. Und wenn das ADAS eines Tesla wie zuletzt am 01.03.2019 die Plane eines querenden LKW nicht als Hindernis erkennt, ist die Ursache höchstwahrscheinlich kein Programmierfehler, sondern eine Beschränkung des zu Grunde liegenden Wirklichkeitsmodells. Diese ergeben sich häufig implizit durch die Wahl einer technischen Komponente – so benötigt eine Bildauswertung Licht und Kontrast, ein Lasersensor nicht.

Dasselbe passiert mit Sicherheitslösungen, die oft versteckte Annahmen über das Angreiferverhalten enthalten. Skimming und Keyless-Go-Angriffe zeigen, dass diese nicht immer realistisch sind. Wir sollten daher von den Naturwissenschaften lernen und beginnen, die Wirklichkeitsmodelle unserer Lösungen präziser zu beschreiben.

Inhalt

secorvo
security consulting

Security News

Was man nicht aufgibt...

Die vor über 12 Jahren für Webserver eingeführten Extended Validation (EV) Zertifikate sollten Anwendern durch besonders gründlich geprüfte Zertifikatsanträge wieder Vertrauen in die durch Hacking-Vorfälle und Schludrigkeit in Verruf gekommene Web-PKI vermitteln. Dazu stellten Browser bei EV-Zertifikaten den geprüften Firmen- oder Organisationsnamen grün hinterlegt neben dem Vorhängeschloss in der Adresszeile dar („grüner Balken").

Doch schon seit iOS 12 (17.09.2018) heben Browser auf Apple-Mobilgeräten den Namen aus EV-Zertifikaten nicht mehr gesondert hervor. Auch Google Chrome wird ab Version 77, die am 10.09.2019 erscheint, die Hervorhebung komplett entfernen – seit Version 69 wird sie nur noch in grau statt grün dargestellt. EV-Zertifikate unterscheiden sich für den Endnutzer nicht mehr von DV- oder OV-Zertifikaten; der Mehrwert entfällt damit für Nutzer dieser Browser.

Diese Entwicklung entspricht der verbreiteten Einschätzung, dass EV-Zertifikate die in sie gesetzten Erwartungen nicht erfüllt haben und kein Plus an Sicherheit bieten. Google setzt stattdessen schon länger auf Certificate Transparency (SSN 6/2019). Auch durch die zunehmende Nutzung von Apps anstelle eines Browsers entfällt die Notwendigkeit der Darstellung von EV-Informationen. Statt EV-Zertifikate besonders zu kennzeichnen schlägt Mozilla mit Firefox Version 70 eine andere Richtung ein und brandmarkt unverschlüsselte HTTP-Webseiten als unsicher. HTTPS wird damit für Webseitenbetreiber endgültig zur Pflicht; die Mehrkosten für EV-Zertifikate kann man sich jedoch sparen.

Angst beflügelt den eilenden Fuß

Am 18.07.2019 schlug eine Schwachstellenmeldung Wellen: Fach- und Allgemeinpresse berichteten über eine kritische Sicherheitslücke im VLC Media Player, die einem Angreifer das entfernte Ausführen von Code ermöglichen würde. Untermauert wurde die Kritikalität durch einen CVSSv3 Score von 9.8. Losgetreten hatte sie CERT-Bund, die im BSI angesiedelte zentrale Anlaufstelle für Computersicherheitsvorfälle, nachdem MITRE den Schwachstellen-Identifier CVE-2019-13615 zugewiesen hatte. Wie sich herausstellte, handelte es sich gar nicht um eine Schwachstelle in VLC, sondern um eine in der von VLC verwendeten Bibliothek „libEBML", die bereits am 20.04.2018 mit Version 1.3.6 behoben worden war. VLC wird schon seit dem 29.05.2018 (Version 3.0.3) mit einer korrigierten „libEBML" ausgeliefert. Der Entdecker der Schwachstelle hatte eine Ubuntu-Version verwendet, die keine aktuelle Version der Bibliothek bereitstellte (deren Maintainer das Problem schnell behoben).

Ein Sicherheitsforscher, der eine nicht aktuelle Software analysiert, zwei offizielle Institutionen (MITRE und CERT-Bund), die ohne gründliche Prüfung eine kritische Schwachstelle anerkennen, Medien, die ohne tiefere Recherche voneinander abschreiben und die Community einer Linux-Distribution, die Sicherheitsaktualisierungen nicht zeitnah verfügbar gemacht hat – ein gefährlicher Cocktail, der Unternehmen vermeidbare Aufwände beschert hat.

Selbst die Änderung der Kritikalität der Schwachstelle ist nur schwer nachvollziehbar: Allein das NIST pflegt in der NVD eine umfängliche Änderungshistorie. CERT-Bund beschreibt die Änderungen vollkommen unzureichend und MITRE führt erst gar keine Historie. Und die Moral: Trau' keiner Nachricht, die Du nicht selbst überprüft hast...

Die Geister, die ich rief...

Das deutsche Vorratsspeicherungsgesetz ist nach den Urteilen des EuGH und der deutschen Obergerichte derzeit ausgesetzt und wird es auch noch auf absehbare Zeit bleiben. Allerdings hat sich der Europarat am 27.05.2019 für eine Vorratsdatenspeicherung zum Zwecke der Kriminalitätsbekämpfung ausgesprochen. Offenbar speichern Internet- und Telefonanbieter jedoch trotz der einschlägigen Rechtsprechung über Monate hinweg nicht abrechnungsrelevante Daten ihrer Kunden.

Um den Schutz des Fernmeldegeheimnisses aus Art. 10 Abs. 1 Grundgesetz zu gewährleisten, muss diese Art von Vorratsdatenspeicherung unterbunden werden. Wie wichtig das ist, zeigt ein aktueller Vorfall aus Dänemark: Das dänische Justizministerium gab am 02.07.2019 bekannt, dass ein IT-Fehler bei der Vorratsdatenspeicherung möglicherweise dazu geführt hat, dass Unschuldige verurteilt und Täter fälschlich freigesprochen wurden. Insgesamt müssen 10.700 Fälle von der inzwischen eingesetzten Expertenkommission überprüft werden.

Freiheit und Gerechtigkeit können auch unter die Räder einer gefährlichen Mixtur aus unkritischem Glauben von Strafverfolgern an die Verlässlichkeit technischer Nachweise und vorauseilendem Gehorsam bei Telekommunikationsanbietern hinsichtlich der, rechtsstaatliche Grenzen überdehnenden, Speicherung von Verbindungsdaten geraten.

Was lange währt...

Nach über sechsmonatiger Beta-Phase wurde am 28.06.2019 Version 2.1 der Burp Suite veröffentlicht. Als Proxy zwischen Web-Browser und -Server erlaubt sie das Mitschneiden, Analysieren und Mani-

pulieren von HTTP-Verkehr – ein unverzichtbares Werkzeug für Sicherheitsexperten und Web-Entwickler. Die lang erwartete Runderneuerung enthält sowohl in der (kostenfreien) Community- als auch in der Professional-Edition zahlreiche Verbesserungen: Der neue Crawler und die neue Scanning-Engine vereinfachen zusammen mit der dynamischen JavaScript-Analyse insbesondere automatisierte Tests. Auch das User Interface wurde an einigen Stellen stark überarbeitet – so wurden ein neues Dashboard und ein alternatives dunkles Farbschema integriert. HTTP-Antworten werden nun dank einer neuen Rendering-Ansicht unter Berücksichtigung von Stylesheets dargestellt. Die Burp Suite kann jetzt auch über eine REST-API aus anderen Anwendungen angesprochen werden, um beispielsweise Scans zu initiieren. Schließlich wurde auch die Performance verbessert.

Stets ist die Sprache kecker als die Tat

Datenschutzaufsichtsbehörden, Datenschutzkonferenz, Europäischer Datenschutzausschuss und Datenschutzverbände überschütten Unternehmen, Datenschutzbeauftragte und Verantwortliche derzeit mit Hinweisen, Orientierungshilfen und Stellungnahmen. Dabei hapert es aber gelegentlich an der inhaltlichen Konsistenz. Zwei aktuelle Beispiele:

Die Argumentation der Stellungnahme des HDBI vom 09.07.2019 zur Unzulässigkeit des Einsatzes von Office 365 in Schulen lässt sich durchaus auf Arbeitgeber übertragen. Als Lösung wird auf on-premise Angebote verwiesen. Zwar haben Rechtsbedenken gegen Office 365 durch das Ende der Deutschland-Cloud (SSN 3/2019) und eine niederländische Prüfung vom 07.11.2018 (SSN 4/2019), die erhebliche Datenschutzrisiken benennt (Zugriff auf personenbezogene Daten auf Grundlage des US Cloud Acts und ungeklärte Verwendung von Telemetrie-Daten durch Microsoft), neue Nahrung erhalten. Eine grundsätzliche Rechtswidrigkeit wurde bisher jedoch nicht festgestellt – und erscheint auch vor dem Hintergrund der geltenden EU-US Privacy Shield Vereinbarung juristisch fragwürdig.

Die neuen FAQ der bayerischen Landesdatenschutzaufsicht enthalten einen informationellen Rundumschlag – und verblüffen mit der Aussage, dass einerseits Google Maps, Google Fonts und allgemeine Captchas, sofern in der Datenschutzerklärung darüber informiert wird, in Webseiten eingebunden werden dürfen, andererseits aber ein rechtmäßiger Einsatz von Google Recaptcha eine Darlegung der Nutzerdatenverarbeitung durch Google erfordert. Die Zulässigkeit von Facebook Fanpages (SSN 4/2019) wird uneingeschränkt verneint.

Die Beispiele hinterlassen den Eindruck, dass die Aufsichtsbehörden sich mit einer eindeutigen Positionierung insbesondere zu amerikanischen Cloud-Angeboten schwer tun – und gelegentlich liebgewonnene Feindbilder die Argumentation überlagern.

Secorvo News

Easy – Certificates ready2go

Auch in internen Netzen wird immer häufiger TLS eingesetzt. Die Einrichtung und Erneuerung von Serverzertifikaten kann inzwischen auch ohne eigene PKI über eine Clientsoftware vorgenommen werden, die kompatibel mit öffentlichen Trustcentern ist. Mit Certificates ready2go, einer Entwicklung von Secorvo, übernimmt ein ACME-Proxy (SSN 3/2019) die Domain-Validierung und ermöglicht so auch Servern im gesicherten internen Netz den vollautomatisierten Bezug und die Erneuerung von Zertifikaten, beispielsweise von Let's Encrypt. Mit dem zugehörigen Dashboard Easy behalten Sie dabei den Überblick über den Status aller Ihrer internen Zertifikate. Zu sehen auf der it-sa 2019.

Nächste Seminare

Nach der Sommerpause startet das Seminarangebot von Secorvo in der letzten Septemberwoche (**23.–26.09.2019**) mit dem Zertifizierungsseminar TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.), gefolgt von T.I.S.P. (**14.–18.10.2019**, schnelle Anmeldung empfohlen) und IT-Sicherheit heute (**22.–24.10.2019**). Programme und die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Hallo, hier spricht Deine Zahnbürste.

Ob zu Hause, in Fahrzeugen, Industrieanlagen oder Agrarbetrieben: IoT-Anwendungen sind heute nicht mehr wegzudenken und halten in nahezu allen Bereichen Einzug in unser Leben. Bis 2020 sollen laut Gartner 20 Milliarden vernetzte Geräte im Einsatz sein. Das Internet of Things eröffnet vielfältige Chancen, jedoch mangelt es häufig an Bewusstsein für Sicherheitsaspekte. Die sichere Kommunikation der unzähligen vernetzten Dinge untereinander ist dabei die größte Herausforderung.

Warum es für Unternehmen existentiell ist, ihre IoT-Devices und den Zugriff auf ihre IoT-Plattformen abzusichern und welche aktuellen Technologien dafür zur Verfügung stehen, erläutert beim kommenden KA-IT-Si-Event am **19.09.2019** Thorsten Gahrmann von der Nexus Group. Im Anschluss an den Vortrag haben Sie – wie gewohnt – Gelegenheit zum fachlichen und persönlichen Austausch bei unserem „Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

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

August 2019	
03.-08.08.	Blackhat USA 2019 (Blackhat, Las Vegas/US)
08.-11.08.	DEF CON 27 (DEFCON, Las Vegas/US)
11.-13.08.	SOUPS 2019 (usenix, Kalifornien/US)
14.-16.08.	28th USENIX Security Symposium (usenix, Santa Clara/US)
18.-22.08.	Crypto 2019 (IACR, Santa Barbara/US)
September 2019	
17.09.	Anwendertag IT-Forensik (Fraunhofer Institut SIT, Darmstadt)
19.09.	Hallo, hier spricht Deine Zahnbürste. (KA-IT-Si, Karlsruhe)
22.-24.09.	FIfFKon 2019 (FIfF e.V., Berlin)
23.-26.09.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
24.09.	Datenschutztag 2019 (COMPUTAS, Köln)
24.-27.09.	heise devSec 2019 (dpunkt.verlag, heise Developer, heise Security, Heidelberg)

Fundsache

Das NIST hat im Juni einen Entwurf für ein White Paper zur sicheren Softwareentwicklung veröffentlicht. Das White Paper hilft dabei, einen Software Development Life Cycle (SDLC) um Praktiken der sicheren Softwareentwicklung zu ergänzen. Kommentare können noch bis zum 05.08.2019 eingereicht werden.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Kai Jendrian, Michael Knopp, Jannis Pinter, Friederike Schellhas-Mende, Christian Titze

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 2019

Digitale Blockwarte

Manchmal kommen selbst dramatische Paradigmenwechsel verhuscht um die Ecke. So wissen wir zwar längst, dass ein Gerät, das seinen Standort über Satellitenortung oder WLAN-Accesspoints bestimmen kann, diese Information auch gelegentlich weitergibt. Natürlich dient das nie der Erstellung von Bewegungsprofilen, sondern ausschließlich anderen, unverdächtig nützlichen Zwecken, wie der Bestimmung der Verkehrsdichte, der exakten Berechnung der richtigen Kochzeit für das Frühstücksei oder der behütenden Aufsicht über den Nachwuchs. Charmant obendrein: Ortungsfunktion oder Gerät lassen sich ausschalten (ja, tatsächlich!), und schon sind wir zurück in steinzeitlicher Freiheit.

Damit könnte es allerdings bald endgültig vorbei sein. Wenn die Idee hinter Apples „Apple Tag" (angekündigt für iOS 13 auf der Entwicklerkonferenz am 03.06.2019) Schule macht, ist die Steinzeit abgelaufen. Und die Freiheit mit ihr. Wie so oft kommt die Überwachung im Schafspelz daher: Elektronische Geräte ohne Ortungs- und Mobilfunk-Chipsatz sollen von anderen, kommunikations- und GPS-fähigen Geräten via Bluetooth kontaktiert, die übermittelte Geräte-ID mit aktueller Ortsinformation angereichert und an Apple geschickt werden – damit verlorene oder gestohlene Devices einfacher und schneller wiedergefunden werden.

Welch zauberhafte Vorstellung: Dank Millionen digitaler Blockwarte müssen wir unsere Schlüssel, Hunde, Zahnbürsten oder Rasierapparate nie mehr suchen oder uns über entwendete Gadgets grämen – einfach ins Netz gucken, und schon wissen wir, wo sie sind. Und auch der Standort der Blockwarte ist jederzeit dokumentiert.

Schade nur, dass die Entwicklung ziemlich genau 30 Jahre zu spät kommt. Wie viel volkswirtschaftliches Vermögen hätte man damit im Ministerium für Staatssicherheit sparen können...

Und die Geschichte wäre vielleicht ganz anders verlaufen.

Inhalt

secorvo
security consulting

Security News

Bluetooth-Downgrade

Ex- und Import von Verschlüsselungslösungen stießen in den 90er Jahren noch auf zahlreiche Restriktionen. Daher verwenden Bluetooth-Verbindungen bis heute getrennte Schlüssel für Integritätsschutz und Verschlüsselung. Während ersterer immer 128 bit lang ist, kann letzterer auf bis zu 8 bit verkürzt werden. Fast 20 Jahre dauerte es, bis ein internationales Forscherteam eine diesen Umstand nutzende Downgrade-Attacke entdeckte und am 14.08.2019 veröffentlichte: Ein Angreifer, der sich in die Schüsselaushandlung einschaltet, kann die Kommunikationspartner dazu bringen, einen 8 Bit Schlüssel zu verwenden und so die übertragenen Daten entschlüsseln.

Wer vertrauliche Daten (wie die Anschläge einer Tastatur oder Dokumente zum Drucken) und nicht nur die aktuelle Playlist via Bluetooth überträgt, sollte prüfen, ob die Hersteller beider Geräte Patches bereitstellen – oder doch zu einer kabelgebundenen Übertragung zurückkehren.

Kreditkarten-Upgrade

Auch bei einem am 29.07.2019 veröffentlichten Kreditkartenangriff mischt sich der Angreifer in die Aushandlung seiner beiden Opfer ein. So ermöglicht Visa inzwischen, am Point-of-Sale durch einfaches Auflegen der Kreditkarte zu bezahlen. Das Missbrauchsschäden bei gestohlenen Karten begrenzende Zahlungslimit (in Großbritannien £ 30) kann dabei durch die Man-in-the-Middle-Attacke auf ein Vielfaches erhöht werden.

Trotz des Proof-of-Concept will Visa nicht sofort etwas gegen die Schwachstelle unternehmen. Zwar kann ein Einzelschaden leicht im drei- oder vierstelligen Bereich liegen, doch dass organisierte Kriminelle zahlreiche Komplizen mit der erforderlichen Elektronik vor Ort auf „Einkaufstour" schicken, erscheint eher unwahrscheinlich. Daher dürfte Visa erst bei einem ohnehin fälligen Wechsel von Karten und Terminals eine sicherere Version ausrollen.

Heiße Schwachstelle

Eingebettete Systeme sind die jüngste Achillesferse der IT-Sicherheit. Da liegt es nahe, Betriebssysteme zu verwenden, die mit Fokus auf Sicherheit und Zuverlässigkeit entwickelt wurden, wie beispielsweise Wind Rivers marktführendes VxWorks. Umso schockierender ist daher eine Nachricht wie die vom 09.08.2019: Elf Schwachstellen wurden in VxWorks 6.9 gefunden, veröffentlicht unter anderem unter CVE-2019-12256. Besonders schlimm: Anwender wissen häufig gar nicht, ob sie betroffen sind oder nicht, denn bei vielen Lösungen wird das genutzte Betriebssystem nicht genannt.

Von vielen Herstellern werden bereits Updates zur Verfügung gestellt. Sie sollten, sofern die Systeme über Netzwerke erreichbar sind, dringend eingespielt werden. Und bei der Beschaffung neuer IoT-Geräte sollte zukünftig auf die Angabe der verwendeten IT-Komponenten geachtet werden.

Komplexinetes

Von Oktober bis Dezember 2018 wurde Version 1.13.4 der Open-Source-Anwendung Kubernetes einem Sicherheitsaudit unterzogen. Den Abschlussbericht veröffentlichte Kubernetes am 06.08.2019 im GitHub-Repository. Code-Qualität und Dokumentation der Container-Orchestrierungs-Lösung erhalten darin keine besonders gute Bewertung. So wurde beispielsweise die gleiche Programmlogik wiederholt implementiert anstatt auf zentrale Mechanismen zu setzen. Insgesamt wird Kubernetes als sehr komplex und reich an Abhängigkeiten eingestuft, was den Code wiederum besonders fehleranfällig macht. Daher überrascht es wenig, dass die Auditoren 37 Sicherheitslücken entdeckten, von denen fünf als hoch kritisch eingestuft wurden.

Das Beispiel zeigt erneut, dass übermäßig komplexe Lösungen ein Sicherheitsrisiko darstellen – und dass Open Source nicht automatisch bedeutet, dass existierende Schwachstellen von der Community selbst aufgedeckt werden. Korrekturen, die die Komplexität der Anwendung signifikant verringern, sind nachträglich nur schwer umsetzbar, da jene häufig aus grundsätzlichen Entwurfsentscheidungen resultiert. Ein Grund mehr, Security-Aspekte schon beim Design zu berücksichtigen.

EuGH-Trend

Der Europäische Gerichtshof (EuGH) hat am 29.07.2019 über die Verantwortung bei der Einbindung von Social Media Plugins entschieden (Rs. C-40/17). Ein Webseitenbetreiber war wegen eines Facebook Like-me Buttons und der daraus resultierenden Übermittlungen an Facebook Irland abgemahnt worden. Auch wenn es sich noch auf die EG-Datenschutz-Richtlinie und die Datenschutzrichtlinie für elektronische Kommunikation (RL 95/46/EG und 2002/58/EG) bezieht, bestätigt das Urteil einen bereits in der Entscheidung C-210/16 zu Facebooks Fanpages anklingenden Trend: Veranlasst oder ermöglicht der Webseitenbetreiber eine Datenverarbeitung durch einen Plattform- oder Dienstanbieter, tendiert der EuGH zur Annahme einer gemeinsamen Verarbeitung. Die daraus folgende

gemeinsame Verantwortung soll jedoch nur die Verarbeitungsphasen umfassen, für die Mittel und Zwecke gemeinsam bestimmt werden. Beide Beteiligte benötigen eine eigenständige Rechtsgrundlage, wobei der EuGH von der Erforderlichkeit einer durch den Webseitenbetreiber einzuholenden Einwilligung ausgeht. Informieren muss der Webseitenbetreiber nur über die gemeinsam verantwortete Verarbeitung.

Die Entscheidung ist insbesondere für Tracking-Pixel hochrelevant. Für Webseitenbetreiber ist die dargestellte Verantwortungsverteilung eine gute Nachricht. Offen bleibt, wie der Social-Media- oder Tracking-Anbieter seine über die gemeinsame Verarbeitung hinausgehende Nutzung begründen kann.

Spiegelreflex-Trojaner

Am 11.08.2019 zeigte Eyal Itkin auf der Defcon, wie sich der Markt für ein funktionierendes kriminelles Geschäftsmodell vergrößern lässt. So gelang es ihm unter Kombination mehrerer Schwachstellen einen Verschlüsselungstrojaner auf die Bilder von Canon-Kameras loszulassen (Demo). Dabei nutzte er die WLAN-Verbindung und das Picture Transfer Protocol (PTP). Nutzern der betroffenen Kameramodelle mit WLAN-Schnittstelle sei daher die Aktualisierung der Firmware und die Deaktivierung der WLAN-/NFC-Schnittstelle bei Nichtgebrauch ans Herz gelegt.

DSGVO-konforme Kamerafahrten

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) informierte am 30.07.2019 über die von Apple seit Juli 2019 auch in Deutschland vorgenommenen Aufnahmen von Straßenzügen und Gebäudefronten zur Aufwertung des Apple-eigenen Kartendienstes. Die damit einhergehenden datenschutzrechtlichen Fragen wurden erstmals mit dem vergleichbaren Dienst Google Streetview vor rund 10 Jahren beleuchtet.

Zur Sicherstellung der Betroffenenrechte wurden Maßnahmen eingeführt, die nun auch bei Apple umgesetzt werden, wie bspw. die vorherige Ankündigung von geplanten Kamerafahrten, die automatische Verpixelung von Gesichtern und Kfz-Kennzeichen, die Möglichkeit der Unkenntlichmachung des eigenen Hauses, die Widerspruchsmöglichkeit gegen die Verarbeitung sowie die Angabe von Beschwerdestellen für Betroffene. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) bewertet das Vorgehen als datenschutzkonform. Eine selten gelungene datenschutzrechtliche Zusammenarbeit zwischen einem amerikanischen Unternehmen und einer deutschen Aufsichtsbehörde.

Forever Young

Backdoors sind alte Bekannte (siehe SSN 12/2007 und SSN 01/2016) – und mächtige Ansatzpunkte für Angriffe. Bereits am 03.11.2003 wurde ein spektakulärer Ansatz für eine Backdoor im Linux-Kernel öffentlich, und erst kürzlich, am 26.07.2019, berichtete Bruce Schneier über die Verurteilung eines Mitarbeiters, der bei Siemens „logic bombs“ in Code eingebaut hatte.

Am 15.08.2019 wurde nun unter der CVE-2019-15107 die Existenz einer Hintertür in den Versionen 1.900 bis 1.920 des beliebten Admin-Tools webmin bekannt. Die Besonderheit gerade dieser Schwachstelle: Sie bestand offenbar seit April 2018 – und stattete Angreifer, die sie ausnutzten, mit hoch privilegierten Rechten aus. Ein weiteres Beispiel, dass gerade verbreitete Open Source-Lösungen besonders attraktiv (und zugleich anfällig) für derartige Angriffe sind.

Secorvo News

Seminare

Nach der Sommerpause startet das Seminarangebot von Secorvo in der letzten Septemberwoche (**23.–26.09.2019**) mit dem Zertifizierungsseminar TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.), IT-Sicherheit heute (**22.–24.10.2019**) und PKI (**18.–21.11.2019**). Für den T.I.S.P. (**14.–18.10.2019**) gibt es noch einen freien Platz; das nächste T.I.S.P.-Seminar folgt in der 48. Woche (**25.–29.11.2019**). Programme und die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Hallo, hier spricht Deine Zahnbürste.

Ob zu Hause, in Fahrzeugen, Industrieanlagen oder Agrarbetrieben: IoT-Anwendungen sind heute nicht mehr wegzudenken und halten in nahezu allen Bereichen Einzug in unser Leben. Bis 2020 sollen laut Gartner 20 Milliarden vernetzte Geräte im Einsatz sein. Das Internet of Things eröffnet vielfältige Chancen, jedoch mangelt es häufig an Bewusstsein für Sicherheitsaspekte. Die sichere Kommunikation der unzähligen vernetzten Dinge untereinander ist dabei die größte Herausforderung.

Warum es für Unternehmen existentiell ist, ihre IoT-Devices und den Zugriff auf ihre IoT-Plattformen abzusichern und welche aktuellen Technologien dafür zur Verfügung stehen, erläutert beim kommenden KA-IT-Si-Event am **19.09.2019** Thorsten Gahrmann von der Nexus Group. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch bei unserem „Buffet-Networking“ – diesmal wieder mit Blick über die Dächer von Karlsruhe (zur Anmeldung).

Veranstaltungshinweise

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

September 2019	
17.09.	Anwendertag IT-Forensik (Fraunhofer Institut SIT, Darmstadt)
19.09.	Hallo, hier spricht Deine Zahnbürste. (KA-IT-Si, Karlsruhe)
22.-24.09.	FIfFKon 2019 (FIfF e.V., Berlin)
23.-26.09.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
24.09.	Datenschutztag 2019 (COMPUTAS, Köln)
24.-27.09.	heise devSec 2019 (dpunkt.verlag, heise Developer, heise Security, Heidelberg)
Oktober 2019	
08.-10.10.	it-sa 2019 (NürnbergMesse GmbH, Nürnberg)
14.10.	Night of the Living Labs (FZI, Karlsruhe)
14.-18.10.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
15.10.	Swiss Cyber Storm 2019 (Swiss Cyber Storm Association, Bern/CH)
22.-24.10.	IDACON 2019 (WEKA-Akademie, München)
22.-24.10.	IT-Sicherheit heute - praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)

Fundsache

Am 24.07.2019 hat Netflix unter dem Titel „The Great Hack“ eine Dokumentation des Cambridge Analytica / Facebook-Skandals veröffentlicht.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Stefan Gora, Hans-Joachim Knobloch, Michael Knopp, Sarah Niederer, 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

September 2019

Das Vermächtnis

Vor exakt 2.300 Tagen erwirkte das FBI einen Haftbefehl gegen Edward Snowden – seitdem ist er auf der Flucht. Ein großes Opfer für den damals knapp 30-Jährigen. Jetzt hat er seine Geschichte veröffentlicht – auf Anhieb ein Bestseller. Was aber hat Snowden tatsächlich bewirkt?

Auf den ersten Blick wenig. Ende 2013 stellte die NSA ihr Utah Data Center fertig, mit einer Speicherkapazität, die die Archivierung und Analyse der gesamten weltweiten Datenkommunikation ermöglicht. Über den US Cloud Act sicherten sich die amerikanischen Geheimdienste am 06.02.2018 den Zugriff auf die Daten ausländischer Kunden von amerikanischen Unternehmen – ein (bislang folgenloser) Affront gegen das Privacy Shield-Abkommen mit der EU vom 02.02.2016. Derweil versucht das Bundesinnenministerium, deutschen Nachrichtendiensten „technische Datenerhebungen aus Wohnungen" zu ermöglichen – schließlich verfügen immer mehr Haushalte über freiwillig installierte Abhöranlagen: Alexa, Cortana, Siri und andere Sprachassistenten lassen grüßen.

Aber es gibt auch die andere Seite. So warnen Browser inzwischen vor Webseiten, die HTTP nicht oder mit veralteten TLS-Versionen schützen – rund 90% der Webkommunikation wird inzwischen verschlüsselt. Auch dank der Initiative „E-Mail made in Germany", einer Reaktion der deutschen E-Mail-Provider auf Snowdens Veröffentlichungen, schützen heute nur noch wenige E-Mail-Server die Kommunikation nicht via TLS vor dem Zugriff Dritter. Mehrere Messenger bieten vor Geheimdiensten sichere Ende-zu-Ende-Verschlüsselung. Sogar Microsoft und Apple versuchen die Daten ihrer Kunden dem NSA-Zugriff zu entziehen, indem sie die Schlüsselgenerierung in Kundenhand legen.

Jetzt gilt es, die Spurensammlung von Google und Co. zu begrenzen – sie sind inzwischen der Ansaugstutzen der NSA im Netz. Wenn uns das nicht gelingt ist Snowdens Vermächtnis verspielt.

Inhalt

secorvo
security consulting

Security News

Sichere(re)s DNS?

Gelingt es einem Angreifer die Namensauflösung einer Domäne zu manipulieren, kann er Nutzern gefälschte Webseiten „unterschieben". Eine wirksame Gegenmaßnahme ist die Einführung von DNS over TLS oder DNS over HTTPS (DoH), doch die läuft bislang zögerlich. Am 06.09.2019 kündigte Mozilla an DoH zum Default zu machen. Der Firefox-Browser enthält bereits einen DoH-Resolver, der künftig standardmäßig alle DNS-Anfragen verschlüsselt an einenn Resolver von Cloudflare senden soll.

Für komplexere Netzkonfigurationen sind allerdings Nebenwirkungen zu erwarten, bspw. bei Split-DNS (hier wird immer die externe Namensauflösung geliefert) oder Content-Filtering Blacklists. Firefox setzt Heuristiken ein, um solche Konfigurationen zu erkennen: Beim Start versucht Firefox, eine „Canary"-Domain aufzulösen; gelingt das nicht, wird DoH abgeschaltet. Schlägt später eine DOH-Anfrage fehl, wird das Betriebssystem befragt, und ist eine Enterprise Policy im Einsatz, ist DoH standardmäßig inaktiv. Vorsicht gilt auch, falls interne Domainnamen nicht offengelegt werden sollen. Administratoren sollten DOH in Firefox erforderlichenfalls deaktivieren.

Dubiose Hotspots oder Zensur betreibende Länder können mittels der Canary-Domain die DOH-Auflösung einfach „abschalten". Und beunruhigen kann auch, dass künftig Cloudflare alle DNS-Anfragen erhält, selbst wenn der Betreiber angibt, die Daten nur für 24 Stunden zu speichern. Monopolstellungen sind immer ein Risiko – in verschiedener Hinsicht.

Identitätsdiebstahl via Auskunft

Auf der Black Hat-Konferenz stellte der Sicherheitsforscher James Pavur am 08.08.2019 einen Social Engineering-Angriff vor, der sich Fehler bei der Umsetzung der datenschutzrechtlichen Auskunftspflicht von Unternehmen zu Nutze macht. Mittels einer selbst angelegten E-Mail-Adresse gab sich Pavur gegenüber mehr als 150 Unternehmen als seine Mitautorin Casey Knerr aus und bat um Auskunft über alle zu „ihr" verarbeiteten personenbezogenen Daten. Von den Unternehmen reagierten 72%; 23% antworteten gar nicht und 5% verweigerten jede Auskunft. Von den reagierenden Unternehmen übersandten 24% die Daten ohne jede Identitätsprüfung, weitere 16% verlangten leicht zu fälschende Identitätsnachweise (wie das Ausfüllen einer schriftlichen Erklärung, tatsächlich die betroffene Person zu sein).

Dabei sollte selbstverständlich sein, dass einem datenschutzrechtlichen Ersuchen erst nach hinreichend sicherer Identitätsprüfung nachgekommen wird, z. B. durch Versand an eine authentisierte Zustelladresse, ein Login in einem bestehenden Benutzerkonto oder die Vorlage eines von einer vertrauenswürdigen Instanz ausgestellten Identitätsnachweises.

De-Anonymizer

Personenbezogene Daten sind Informationen, die sich auf eine identifizierbare natürliche Person beziehen. Dabei sind für die Identifikation in der Regel weder Name noch Adresse erforderlich: Nach einer am 23.07.2019 in „nature" veröffentlichten Studie genügen bereits 15 demografische Attribute, um 99,98% der US-Bürger zu re-identifizieren. Für eine Anonymisierung reicht es daher in der Regel nicht, in einem Datensatz lediglich den Namen und die Adresse zu löschen. Mehr noch: Je aussagekräftiger die statistischen Angaben über eine Gruppe von Personen, desto höher ist die Wahrscheinlichkeit, dass eine Re-Identifizierung Einzelner möglich ist. Mit dem wachsenden Einsatz von künstlicher Intelligenz bei Big-Data-Auswertungen dürften zukünftig vermehrt vermeintlich anonyme Datensammlungen als Verarbeitung personenbezogener Daten zu bewerten sein.

SIM-Jack

Am 12.09.2019 veröffentlichte Cathal McDaid von AdaptiveMobile Security im firmeneignen Blog einen Post über die Schwachstelle Simjacker. Darüber können sich Angreifer mittels einer präparierten SMS in der SIM-Karte einnisten. Von dort können Informationen ausgelesen oder unbemerkt Telefonverbindungen aufgebaut werden, die das Gerät in eine Wanze verwandeln. Offenbar nutzen diese Schwachstelle Angreifer mehrerer Länder schon seit mindestens zwei Jahren. Die Schwachstelle bedroht jedes mobile Endgerät, auf dessen SIM-Karte (UICC) der Netzbetreiber die Software S@T Browser, eine Alternative zum klassischen SIM Toolkit, installiert hat. Sie soll in 30 Staaten mit insgesamt über einer Milliarde Einwohnern im Einsatz sein. Immerhin: Die Netzbetreiber Telekom, Vodafone und Telefónica teilten übereinstimmend mit, dass auf ihren Karten der S@T Browser nicht installiert ist.

Die Erfahrung zeigt, dass es in komplexen IT-Systemen selten nur einen einzigen Sicherheitsbug gibt. Daher gilt (nicht nur aus diesem Grund): Gelegentliches Ausschalten hilft.

Unzulässige Kekse

Cookie-Banner finden sich inzwischen auf fast allen Webseiten – oft sind sie jedoch datenschutzrecht-

lich unzureichend. Erst am 18.09.2019 wies der Landesbeauftragte für Datenschutz- und Informationsfreiheit (LfDI) Baden-Württemberg darauf hin, dass die Nutzung der Webseite keine rechtswirksame Einwilligung darstellt. Eine Studie der Ruhr-universität Bochum zeigt, dass die meisten untersuchten Cookie-Banner nicht nur nicht DSGVO-konform sind (86%), sondern auch psychologische Tricks anwenden, um Nutzer dazu zu bringen die gewünschte Einwilligung zu erteilen. Oft wird zudem nicht darüber informiert, dass die Daten an Dritte weitergegeben werden. Das LG Dresden urteilte am 11.01.2019, dass es nicht ausreicht, die Nutzer aufzufordern, Einstellungen im Browser vorzunehmen, die das Speichern von Cookies und die Übertragung von personenbezogenen Daten verhindern – auch dies eine verbreitete Unsitte.

Bereits im Cookie-Banner muss die Möglichkeit gegeben werden, die Verwendung von Cookies abzulehnen. Hier hilft eine kurze Beschreibung, welche Cookies was an wen übermitteln. Ausführliche Hinweise und Informationen können dann in einem gesonderten Cookie-Hinweis oder in der Datenschutzerklärung folgen. Eine gute Hilfe bei der Gestaltung bieten die FAQ des LfDI Baden-Württemberg.

Renitenter Sündenbock

Ransomware-Autoren haben ein neues Angriffsziel: US-amerikanische Kleinstädte, die nicht ausreichend gegen derartige Angriffe gewappnet sind. In der Not sind sie oft bereit, das geforderte Lösegeld zu zahlen. Am 10.06.2019 wurde Lake City (Florida) Angriffsopfer – und verlor 460.000 USD (42 BTC). Daraufhin entließ man am 21.06.2019 den IT-Direktor. Brian Hawkins jedoch verklagte am 09.08.2019 die Stadt: Er habe bereits 2017 gewarnt und auf die Anschaffung eines Cloud-basierten Backup-Systems gedrängt, was aus Kostengründen abgelehnt worden sei. Nach Überzeugung von Hawkins habe die Stadt damit entschieden, das Risiko eines Cyberangriffs zu akzeptieren. Solche essentiellen Entscheidungen sind im Rahmen des Risikomanagements zu dokumentieren, sonst kann man sich später nicht darauf berufen. Im Fall von Hawkins ist dies nicht geschehen – was ihn nun in Beweisnot bringt.

Secorvo News

Secorvo@it-sa

Besuchen Sie uns vom 08. bis 10.10.2019 auf der deutschen IT-Sicherheits-Leitmesse it-sa in Nürnberg. Unseren Stand finden Sie in Halle 10, Standnummer 10.1.-630. Wir zeigen unsere „ready2go"-Managementlösungen für Informationssicherheit (ISMSr2g), Datenschutz (DSMSr2g) und die Zertifikatsverwaltung (Easy). Am 09.10.2019 spricht um 10:45 Uhr Jörg Völker im Forum M10-Management über „Die Rückkehr der ISMS-Ritter".

Sie haben noch kein Ticket? Registrieren Sie sich mit unserem Gutscheincode **A411787** und Sie erhalten ein kostenfreies Tagesticket.

3. Auflage des T.I.S.P.-Buchs

Jetzt ist sie verfügbar – die gründlich überarbeitete und ergänzte dritte Auflage des T.I.S.P.-Begleitbuchs „Informationssicherheit und Datenschutz", ein Gemeinschaftswerk des gesamten Secorvo-Teams. Wir freuen uns sehr, dass der dpunkt.verlag die Herausgabe übernommen hat. Auf der Verlagswebseite finden sich ausgewählte Leseproben des 824 Seiten umfassenden Grundlagenwerks, das nun für 84,90 € im Buchhandel erhältlich ist.

Nächste Seminare

Die letzte Gelegenheit, bei der Sie sich in diesem Jahr Ihre Qualifikation und Erfahrung in der IT-Sicherheit zertifizieren lassen können, bieten wir Ihnen in der 48. Woche mit dem nächsten T.I.S.P.-Seminar (**25.–29.11.2019**) – von über 250 Teilnehmern mit 4,35 von 5 Punkten bewertet. In der Woche davor kommen PKI-Interessierte zum Zug: In nur vier Tagen vom Einsteiger zum Experten bei unserem PKI-Seminar (**18.–21.11.2019**), Rating: 4,3. Wir freuen uns auf Ihre Teilnahme!

Alle Programme, die Seminartermine 2020 und die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Möge das ISMS mit dir sein

Die Etablierung von Informationssicherheit im Unternehmen gleicht oft dem Kampf der Star-Wars-Rebellen gegen die dunkle Seite der Macht – hier dem allzu sorglosen Umgang mit schützenswerten Informationen. Dabei hilft ein Informationssicherheits-Managementsystem (ISMS).

Damit sich der Aufbau und die Zertifizierung des ISMS jedoch nicht ähnlich lange hinziehen wie der Kampf gegen das Imperium empfiehlt es sich zielstrebig vorzugehen. Der Vortrag beim kommenden KA-IT-Si-Event am **24.10.2019** fasst die grundlegenden Anforderungen der ISO 27001 zusammen und stellt die konkrete Umsetzung und Zertifizierung beim Kirchlichen Rechenzentrum Südwestdeutschland (KRZ-SWD) vor.

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

Veranstaltungshinweise

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

Oktober 2019	
08.-10.10.	it-sa 2019 (NürnbergMesse GmbH, Nürnberg)
14.-18.10.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
14.10.	Night of the Living Labs (FZI Forschungszentrum Informatik, Karlsruhe)
15.10.	Swiss Cyber Storm 2019 (Swiss Cyber Storm Association, Bern/CH)
22.-24.10.	IDACON 2019 (WEKA-Akademie, München)
November 2019	
05.-06.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
05.-06.11.	9. Handelsblatt Jahrestagung - Cybersecurity (Handelsblatt/EUROFORUM, Berlin)
11.-15.11.	ACM CCS 2019 (ACM/SIGSAC, London/UK)
18.-21.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
20.-22.11.	43. DAFTA (GDD, Köln)
25.-29.11.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
26.-29.11.	DeepSec In-Depth Security Conference Europe (DeepSec, Wien/AT)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Benjamin Faller, Hans-Joachim Knobloch, Friederike Schellhas-Mende, Christian Titze

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 2019

Rechenmagie

Wer die Liste der seit Inkrafttreten der DSGVO verhängten Datenschutz-Bußgelder durchsieht, wird von deren Spanne überrascht: Sie reicht von gerade einmal einhundert Euro bis zu deutlich dreistelligen Millionenbeträgen (Marriott, British Airways). Unvermeidlich drängt sich der Eindruck auf, dass die Bußgeldhöhe keiner einheitlichen Systematik folgt, sondern eher Beliebigkeit entspringt.

Bei genauerem Hinsehen wird deutlich, dass dies drei Ursachen haben dürfte: die noch geringe Erfahrung vieler europäischer Aufsichtsbehörden mit diesem gestärkten Sanktionsinstrument, die bisher eingeschränkte Abstimmung der Aufsichtsbehörden untereinander und die strukturell neue Ausrichtung der Bußgelder an der Leistungsfähigkeit des betroffenen Unternehmens.

Erkennbar ist, dass mit wachsender Erfahrung der Aufsicht auch die Höhe der Bußgelder steigt. Vor wenigen Wochen haben sich nun die deutschen Aufsichtsbehörden auf ein Berechnungsschema geeinigt, das die Bußgeldhöhe aus dem Unternehmensumsatz ableitet und mit einem Korrekturfaktor die Schwere des Verstoßes berücksichtigt sowie materielle Verstöße stärker als formelle ahndet.

Eine zu begrüßende Entwicklung zu mehr Transparenz und Nachvollziehbarkeit. Dennoch führen Rechenmodelle nicht automatisch zu gerechteren Ergebnissen. Daher ist der wichtigste Teil des Konzepts der letzte Punkt – die Berücksichtigung täterbezogener und wirtschaftlicher Umstände bei der endgültigen Bußgeldfestsetzung. Das ist keine Beliebigkeit durch die Hintertür, sondern räumt einen Ermessensspielraum ein, der bei besonnener Nutzung zu mehr Einzelfallgerechtigkeit führen kann als das Rechenschema.

Unternehmen müssen sich daran gewöhnen, dass derselbe Datenschutzverstoß zu verschiedenen Bußgeldern führen kann. Und die Aufsichtsbehörden müssen aufpassen, dass sie bei aller pseudo-objektiver Rechenmagie nicht das Augenmaß verlieren.

Inhalt

secorvo
security consulting

Security News

Unauffällige Erweiterungen

Auf der CS3STHLM-Konferenz in Stockholm zeigte der Sicherheitsforscher Monta Elkins am 24.10. 2019, wie es ihm mit einem Budget von nur $200 gelang, eine Cisco ASA 5505 Firewall um eine Hardware-Backdoor zu erweitern. Der von ihm aufgelötete ATtiny85 greift über die serielle Schnittstelle die Passwortrücksetzung an und richtet eine Hintertür mit Administrationsrechten ein. Der etwa fingernagelgroße Mikrocontroller ist ohne Schaltplan kaum als zusätzliches Bauteil erkennbar. Der Angriff erinnert stark an die von Edward Snowden und Glenn Greenwald 2014 aufgedeckten Manipulationen der NSA an Cisco-Routern auf dem Postweg und Gerüchte über chinesische Hacker, die 2018 auf Mainboards des Herstellers Supermicro einen reiskorngroßen Chip ergänzt haben sollen. Derartige Manipulationen zeigen eindrucksvoll, dass zur Herstellung sicherer Produkte auch eine sichere Lieferkette gehört. Präpariert ein Angreifer originale Firewalls oder Server und verkauft sie dann beispielsweise über Amazon Marketplace, kann er manipulierte Geräte mit geringem Aufwand verbreiten.

Freie Kekswahl

Ein kollektives Stöhnen und Wehklagen der online-Werbebranche erschallte am 01.10.2019, nachdem der EuGH in der Rechtssache C-673/13 - Planet49-GmbH entschieden hatte, dass beim Besuch einer Webseite nur technisch notwendige Cookies – so genannte Session-Cookies – ohne Einwilligung gesetzt werden dürfen. Das Urteil ist EU-weit unmittelbar umzusetzen und anzuwenden. Die deutsche Umsetzung der „Cookie-Richtlinie“ im Telemediengesetz ist nicht rechtskonform und muss angepasst werden. Voreingestellte Häkchen gehören nun ebenso der Vergangenheit an wie konkludente Einwilligungen durch Weiternutzung einer Webseite mit impliziter Duldung.

Wirksame Einwilligungen setzen voraus, dass der Seitenbetreiber die Nutzer über Third-Party-Cookies, die er zu setzen wünscht, informiert. Erst wenn Nutzer die Möglichkeit haben, eine freiwillige Entscheidung für oder gegen die Cookies zu treffen, entspricht die Einwilligung den gesetzgeberischen Anforderungen. Das bedeutet für (fast) alle Unternehmen Handlungsbedarf bei der Anpassung der Cookie-Banner auf ihren Webseiten. Ansonsten geht man das Risiko ein, in das Visier der Aufsichtsbehörden und etwaiger Abmahner zu geraten. Es ist nur ein schwacher Trost, dass auch der EuGH nach Veröffentlichung des Urteils den eigenen Cookie-Banner mehrfach anpassen musste, bis er den Vorgaben des eigenen Urteils entsprach.

In Code We Trust

Der Turing-Award-Preisträger Ken Thompson illustrierte schon 1984 in seiner Dankesrede „Reflections on Trusting Trust“, wie ein manipulierter Compiler Backdoors in Programme einbauen kann, ohne dass dabei Spuren im Quellcode zurückbleiben. Die am 24.10.2019 veröffentlichte Kombination einer XXE- und einer Directory Traversal Schwachstelle im XML Language Server (aka lsp4xml) erreicht zwar nicht ganz das Ausmaß eines manipulierten Compilers. Durch die Verwendung der Komponente in XML-Plugins diverser Entwicklungsumgebungen (Eclipse, VS-Code, ...) drängt sich allerdings immer noch die gleiche Frage auf wie vor 35 Jahren: Können wir dem Code oder der Software trauen, die wir einsetzen um neue Software zu erstellen?

Ken Thompson kam zu dem Schluss, dass dies nicht möglich ist: „*You can't trust code that you did not totally create yourself.*“ Den kompletten Code inklusive Tools und Compiler selbst zu erstellen ist heute allerdings in den seltensten Fällen überhaupt und nur mit unvertretbar hohem Aufwand möglich. Allerdings sollte es zu den Minimaltugenden gehören, nur etablierte Werkzeuge mit aktuellem Versionsstand einzusetzen und niemals „blind“ Code(schnipsel) aus unbekannten Quellen zu verwenden.

Entflammbarer Brandschutz

Immer noch fordern Auditoren, Virenschutzprodukte auf Servern einzusetzen. Aber funktionieren solche Lösungen tatsächlich effektiv als Brandschutz, oder werden sie beim nächsten Feuer nicht eher zu Brandbeschleunigern? Denn eine Virenschutzlösung, die mit erhöhten Privilegien arbeitet, kann selbst zur mächtigen Bedrohung werden. Das zeigen am 19.10.2019 und 21.10.2019 gemeldete Schwachstellen (Trend Micro Anti Threat Toolkit) und Einbrüche bei Herstellern von Sicherheitslösungen (NordVPN, Avast) sowie zahlreiche zurückliegende Fälle (SSN 3/2004, SSN 5/2014, SSN 5/2016). Deshalb sollte bei der Entscheidung für eine solche Lösung die mögliche Fehlbarkeit der eingesetzten Produkte in Risiko- und Bedrohungsanalysen sowie Sicherheitskonzepten berücksichtigt werden.

Rechenhilfe

Am 16.10.2019 präsentierte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ihr Modell zur Berechnung von Bußgeldern für Verstöße nach Art. 83 Datenschutz-Grundverordnung (DSGVO). Die Bußgeldbemessung soll damit transparent, systema-

tisch nachvollziehbar und innerhalb der EU harmonisiert werden. Das Konzept nimmt die Bußgeldzumessung in fünf Schritten vor:

- Zuordnung des Unternehmens zu einer von insgesamt 20 Größenklassen
- Bestimmung des mittleren Jahresumsatzes der jeweiligen Größenklasse
- Ermittlung eines wirtschaftlichen Grundwertes (entspricht dem durchschnittlichen Tagessatz)
- Multiplikation dieses Grundwertes mit einem von der Schwere der Tatumstände abhängigen Faktor (1-6 für formelle und 1-12 für materielle Verstöße)
- Anpassung des ermittelten Wertes unter Berücksichtigung täterbezogener und z. B. wirtschaftlicher Umstände

Nach Auffassung der DSK bestärkt dieses Konzept durch die Anknüpfung an den Unternehmensumsatz die Umsetzung des Wunschs des Europäischen Gesetzgebers nach Wirksamkeit, Verhältnismäßigkeit und abschreckender Wirkung gemäß Art. 83 Abs. 1 DSGVO. Das Bußgeldmodell ist also durchaus darauf ausgelegt, den Bußgeldrahmen möglichst umfassend auszuschöpfen.

Konkretisierungen

Der Europäische Datenschutzausschuss (EDSA) hat am 08.10.2019 Version 2.0 der Richtlinie zur „Verarbeitung personenbezogener Daten im Zusammenhang mit der Bereitstellung von Online-Diensten“ veröffentlicht. Die Richtlinie enthält vor allem Vorgaben zur Abgrenzung der Erlaubnistatbestände im Bereich Marketing und Online-Dienste. Sie begrenzen die Verarbeitungserlaubnis „Vertrag“ strikt auf die Prozesse, die nach Erwartung des Betroffenen zur Vertragserfüllung erforderlich sind. Bereits die Aufbewahrung von vertragsbezogenen Unterlagen zu Buchhaltungszwecken soll bspw. vor allem nach Vertragsende transparent auf die gesetzliche Pflicht (Art. 6 Abs. 1 c) DSGVO) gestützt werden. Zwecke wie Service-Verbesserung, Werbung in Verbindung mit dem Vertragsgegenstand oder Betrugsabwehr können über das berechtigte Interesse des Verantwortlichen begründet werden, nicht jedoch über den Vertrag. Gewarnt wird davor, Verarbeitungen, die ein Vertrag erforderlich macht, auf Einwilligungen zu stützen, da sich die Rechtsfolgen bezüglich Widerspruch, Löschpflichten u. a. erheblich unterscheiden. Datenverarbeitung beispielsweise zum Zweck individualisierter Werbung als Gegenleistung für ein Leistungsangebot einzufordern ist nach Auffassung des EDSA unzulässig.

Die Richtlinie macht wie die Orientierungshilfe der Datenschutzkonferenz deutlich, dass innerhalb von Verarbeitungsvorgängen nach Zwecken und Rechtsgrundlagen sorgfältig differenziert werden muss, dass diese Differenzierungen Teil der Datenschutzinformationen sein sollen und dass die Rechtsgrundlagen nicht abhängig von der Darstellung austauschbar sind.

Secorvo News

Wissensauffrischung

Schnellentscheidern bieten wir noch zwei Gelegenheiten in diesem Jahr, ihre Kenntnisse in der Informationssicherheit aufzufrischen und zu erweitern: Bei unserem T.I.S.P.-Seminar (**25.–29.11.2019**) sowie dem viertägigen Intensivseminar PKI (**18.–21.11.2019**). Eine Übersicht über alle angebotenen Seminare, Programme und die Termine im Jahr 2020 sowie die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Geliebter Feind – Enemy Mine

Fast täglich kann man in den Medien von Wirtschaftskriminalität, Wirtschaftsspionage und Cybercrime lesen. Was aber verbirgt sich konkret dahinter? Welche Tätertypen gibt es, und warum wird ein Mitarbeiter nach vielen Jahren Betriebszugehörigkeit auf einmal delinquent? Und was meinen Begriffe wie „wirtschaftskriminologisches Belastungssyndrom“ oder „Competitive Intelligence“? Wird man im eigenen Unternehmen mit einem solchen Vorfall konfrontiert, stellen sich viele Fagen: Was ist dem „internen Ermittler“ erlaubt und was nicht? Wann sollten Strafverfolgungsbehörden eingeschaltet werden? Und warum helfen Systeme wie ein IKS nur bedingt gegen Wirtschaftskriminalität?

Auf diese Fragen gibt Andreas Schäfer (VBK) auf dem nächsten KA-IT-Si-Event am **05.12.2019** Antworten und zeigt, wie Unternehmen sich im Vorfeld schützen und – im schlimmsten Fall – verteidigen können. Im Anschluss haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ (Anmeldung).

Alice und Bob im Wunderland

Zu einer Veranstaltung der ganz anderen Art laden wir Sie herzlich zusammen mit dem Forschungszentrum Informatik (FZI) am **14.11.2019** ein. Mit einem Vortrag von Tobias Schrödel über das Darknet und zahlreichen Live-Demos präsentiert Ihnen die IT-Sicherheitsregion Karlsruhe das „Wunderland der IT-Sicherheit“ im Karlsruher Palazzo. Lassen Sie sich von einem wunderbaren Abend verzaubern... Wir empfehlen eine schnelle Anmeldung, da die Zahl der Plätze begrenzt ist.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

November 2019	
05.-06.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
05.-06.11.	9. Handelsblatt Jahrestagung – Cybersecurity (Handelsblatt/EUROFORUM, Berlin)
11.-15.11.	ACM CCS 2019 (ACM/SIGSAC, London/UK)
18.-21.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
20.-22.11.	43. DAFTA (GDD, Köln)
25.-29.11.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
26.-29.11.	DeepSec In-Depth Security Conference Europe (DeepSec, Wien/AT)
Dezember 2019	
03.12.	Black Hat Europe 2019 (Blackhat, London/UK)
05.-06.12.	8. DFN-Konferenz Datenschutz (DFN-Verein/DFN-CERT, Berlin)
10.12.	GERMAN OWASP DAY 2019 (OWASP Foundation, Karlsruhe)

Fundsache

Nachdem der Heise-Verlag im Frühjahr 2019 Opfer eines Emotet-Angriffs wurde, hat er nicht den Deckmantel des Schweigens über diesen Vorfall gebreitet, sondern ist sowohl mit einer Aufarbeitung als auch einer FAQ zu diesem Thema an die Öffentlichkeit gegangen. Die Erkenntnisse sind lesenswert.

Impressum

Secorvo Security News – ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Kai Jendrian, Michael Knöppler, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende

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 News

November 2019

Denial of Service

Für viele Prediger der Digitalisierung sind vor allem personenbezogene Daten das „Öl“ des 21. Jahrhunderts. Sehen wir einmal davon ab, dass das Bild ein wenig Schräglage hat (Daten sind keine in Jahrmillionen entstandene endliche Ressource), so ist die Botschaft doch klar: Die Rockefeller von morgen brauchen sehr, sehr viele Daten. Blöd nur, dass der ungebremsten Abschöpfung dieses Rohstoffs der Datenschutz entgegensteht. Daher forderte der damalige Bundesminister für Verkehr und digitale Infrastruktur, Alexander Dobrindt (CSU), in seinem „Strategiepapier Digitale Souveränität“ (sic!) schon im März 2017 eine „neue Datenkultur: Weg vom Grundsatz der Datensparsamkeit hin zu einem kreativen, sicheren Datenreichtum.“ Und nicht nur er.

Dabei könnte sich das Problem von selbst erledigen. Zwar dürfen Daten ohne Zustimmung der Betroffenen nur unter drei Voraussetzungen verarbeitet werden: Ihre Verarbeitung ist zur Erfüllung eines Vertrags mit den Betroffenen erforderlich, der Verarbeiter hat ein (die schutzwürdigen Bedürfnisse der Betroffenen) überwiegendes, berechtigtes Interesse oder es gibt ein Gesetz, das die Verarbeitung vorschreibt – und mit Art. 8 der EU-Grundrechtscharta vereinbar ist. Daher bleibt oft nur, die Einwilligung der Betroffenen einzuholen.

Das haben die Datenverarbeiter inzwischen verstanden. Und holen Einwilligungen ein. In jeder App, auf jeder Webseite und in jedem Vertrag – selbst dann, wenn eine der oben genannten Voraussetzungen bereits erfüllt ist. Und die Betroffenen klicken und unterschreiben, so oft und ritualisiert, dass sie nicht nur die Datenschutzerklärung ignorieren, sondern die Bestätigung der Kenntnisnahme schon als bürokratische Zumutung empfinden.

So degeneriert der Königsweg der informationellen Selbstbestimmung zum Freibrief für jede Art der Verarbeitung. Kein Science-Fiction-Autor hätte sich das besser ausdenken können: Entscheidungs-Overload durch einen Denial-of-Service-Angriff auf den freien Willen.

Inhalt

secorvo
security consulting

Security News

Doppelte Timing-Attacke

Unter dem Namen TPM-Fail publizierte ein internationales Forscherteam am 13.11.2019 eine Timing-Attacke, mittels derer sich private ECDSA-Schlüssel aus sicherheitszertifizierten Trusted-Platform-Modulen (TPMs) von Intel und STMicro extrahieren lassen. Bereits am 03.10.2019 hatten tschechische Forscher unter dem Namen Minerva eine verblüffend ähnliche Attacke u. a. gegen eine Smartcard von Athena veröffentlicht. Die Ähnlichkeit ist nicht zufällig – beide Arbeiten beziehen sich auf dieselbe Publikation aus dem Jahr 2011. Da beide Gruppen CVEs für ihre jeweiligen „Opfer" angemeldet hatten, bevor die andere Arbeit publiziert wurde, darf man von parallelen Entdeckungen ausgehen – und nicht von einem Plagiat.

Die Angriffe demonstrieren (wieder einmal), dass Sicherheitszertifikate für Produkte nur so viel wert sind wie die Sorgfalt bei deren Zertifizierung. Dabei sollte man auch das Kleingedruckte lesen: Die Anfälligkeit der Smartcard-Library gegen Seitenkanalangriffe war schon bei der Zertifizierung bekannt. Zertifiziert wurde daher nur die resistente Variante der ECDSA-Funktionen des Chip. Wenn aber ein Sicherheitschip Kryptofunktionen sowohl in einer „secure"- als auch in einer „fast"-Variante anbietet, welche wird ein Entwickler wohl nutzen?

Immerhin hat sich EdDSA als härtere Nuss im Vergleich mit ECDSA erwiesen: Die EdDSA-Erfinder erläuterten am 24.10.2018, dass dies kein Zufall ist. Gegen Seitenkanalangriffe hilft eben auch Prävention beim Entwurf des Kryptoverfahrens.

Mit OWASP wäre das nicht passiert

Am 25.10.2019 wurde eine lesenswerte Beschreibung von zwei kritischen Schwachstellen (CVE-2019-16663, CVE-2019-16662) im freien Netzwerktool rConfig veröffentlicht. Damit war es in den betroffenen Versionen möglich, aus der Ferne ohne Authentifizierung beliebige Kommandos als root-Benutzer auszuführen.

Hätten die Entwickler den schon im Herbst veröffentlichten Release-Candidate der OWASP API Security Top 10 gekannt und angewendet, wäre dieser Fehler zu vermeiden gewesen: Darin werden die API-Schwachstellen „Broken Authentication" und „Broken Object Level Authorization" behandelt, die bei rConfig ausgenutzt werden konnten.

Rechtskonformes Tracking

In enger Taktung erscheinen derzeit Nachrichten zum Thema Cookies, Webtracking und Einwilligung. Am 14.11.2019 veröffentlichten 12 Landesdatenschutzbeauftragte und der Bundesdatenschutzbeauftragte einen eindringlichen Hinweis unter der Überschrift „Personenbezogenes Webtracking nur mit Einwilligung". Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) wies in seiner Pressemitteilung explizit darauf hin, dass die „Hinweise des HmbBfDI zum Einsatz von Google Analytics" (sprich: seine eigenen) längst überholt und zurückgezogen seien: Ein Auftragsverarbeitungsverhältnis läge nach derzeitigem Sachstand dabei nicht vor.

Diese Pressemitteilungen müssen als Warnung an diejenigen verstanden werden, die sich noch nicht oder nicht ausreichend um einen DSGVO-konformen Einsatz ihrer Trackingtools und die DSGVO-gerechte Gestaltung der Cookie-Banner gekümmert haben. Am einfachsten ist es immer noch, gänzlich auf derartige Hilfsmittel – insbesondere unter Zuhilfenahme von Diensten Dritter – zu verzichten oder sie so lange abzustellen, bis ein DSGVO-konformer Einsatz gewährleistet ist.

Hungernde Haustiere

Mit der Futterstation FurryTail können Haustiere während der Abwesenheit der Bewohner per App mit passenden Futtermengen versorgt werden. Am 24.10.2019 publizierte die russische Sicherheitsforscherin Anna Prosvetova via Telegram (Account @theyforcedme) eine in fast 11.000 via Internet erreichbaren Geräten ausnutzbare Schwachstelle in der API bei der Autorisierungsprüfung, über die die Geräte von Unberechtigten ferngesteuert werden können.

Immer wieder werden in Smart-Home-Produkten elementare Schwachstellen entdeckt. Die Geräte werden möglichst billig von Drittanbietern für bekannte Marken entwickelt; auch die Tierfutterstation stammt nicht von Xiaomi selbst. Sicherheit ist dabei selten ein Qualitätskriterium. Durch die Internetanbindung solcher Geräte entstehen nicht nur neue Angriffsmöglichkeiten, sondern auch Geschäftsmodelle: Kann ein Unberechtigter die Futterausgabe remote blockieren, werden Haustierbesitzer erpressbar.

Tails 4.0

Die bereits in den SSN 06/2014 vorgestellte Distribution „Tails 1.0" für einen anonymen Internetzugriff wurde in der Zwischenzeit mehrfach überarbeitet. Am 22.10.2019 wurde die runderneuerte Version 4.0 veröffentlicht. Tails ermöglicht (wie Whonix) auch technisch weniger versierten Menschen eine einfache Nutzung des anonymen Tor-Netzwerks.

Version 4.0 verwendet Debian 10 als Plattform und aktuelle Anwendungen wie den Tor-Browser 9.0. Schwachstellen in den eingesetzten Softwarekomponenten wurden behoben. Für Nutzer ist wichtig, dass sie am System, am Browser und an den Plugins keine Veränderungen vornehmen, da sie sich sonst ggf. hierüber ungewollt zu erkennen geben. Tails kann von DVD, einem USB-Stick oder als virtuelle Maschine genutzt werden.

Teurer Datenfriedhof

Erst in den SSN 10/2019 haben wir das Thema Bußgeldbemessung bei Datenschutzverstößen thematisiert. Nun hat die Berliner Beauftragte für Datenschutz- und Informationssicherheit am 05.11.2019 gegen die Deutsche Wohnen SE das bisher höchste Bußgeld in Deutschland in Höhe von 14,5 Mio. € verhängt.

Schuld ist ein „Datenfriedhof" – und die unzureichende Trennung aufbewahrungspflichtiger von anderen personenbezogenen Daten. Werden personenbezogene Daten verarbeitet, muss jeweils geprüft werden, ob diese aufgrund steuerrechtlicher Vorgaben aufbewahrt werden müssen. Falls nicht, sind sie zu löschen, sobald sie für den Verarbeitungszweck nicht mehr erforderlich sind.

Bei der Anschaffung entsprechender Archivierungssysteme ist darauf zu achten, dass das System eine Löschung ermöglicht. Wer das versäumt, den kann die rechtswidrige Aufbewahrung wie im vorliegenden Fall teuer zu stehen kommen.

Secorvo News

Enemy Mine – Geliebter Feind

Fast täglich kann man in den Medien von Wirtschaftskriminalität, Wirtschaftsspionage und Cybercrime lesen. Was aber verbirgt sich konkret dahinter? Welche Tätertypen gibt es, und warum wird ein Mitarbeiter nach vielen Jahren Betriebszugehörigkeit auf einmal delinquent? Und was meinen Begriffe wie „wirtschaftskriminologisches Belastungssyndrom" oder „Competitive Intelligence"? Wird man im eigenen Unternehmen mit einem solchen Vorfall konfrontiert, stellen sich viele Fragen: Was ist dem „internen Ermittler" erlaubt und was nicht? Wann sollten Strafverfolgungsbehörden eingeschaltet werden? Und warum helfen Systeme wie ein IKS nur bedingt gegen Wirtschaftskriminalität?

Auf diese Fragen gibt Andreas Schäfer (VBK) auf dem nächsten KA-IT-Si-Event am 05.12.2019 Antworten und zeigt, wie Unternehmen sich im Vorfeld schützen und – im schlimmsten Fall – verteidigen können. Im Anschluss haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (Anmeldung).

Seminare 2020

Mit einem T.I.S.P.-Seminar ist Ende November die Seminar-Saison 2019 bei Secorvo ausgeklungen. Im kommenden Jahr bieten wir Ihnen wieder zahlreiche Gelegenheiten, Ihre Kenntnisse in der IT-Sicherheit zu erweitern und Ihre Qualifikation zu zertifizieren. Das vollständige Programm mit allen Terminen und der Möglichkeit zur Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Türchen für Türchen

Kinder für das Thema Datensicherheit zu sensibilisieren und ihnen dabei spielerisch Verständnis für Verschlüsselungstechniken zu vermitteln ist das Ziel des Online-Adventskalenders „Krypto im Advent". Auch für diesen inzwischen fünften Kalender haben sich die Karlsruher IT-Sicherheitsinitiative und die Pädagogische Hochschule Karlsruhe wieder spannende Krypto-Rätsel für die Vorweihnachtszeit ausgedacht: Es gilt, alte und neue Verschlüsselungstechniken zu entdecken und dabei tolle Sachpreise zu gewinnen.

Schülerinnen und Schüler der Klassen 3 bis 6 können mit den Agenten Krypto und Kryptina und dem Agentenhund Kryptix im Zirkus auf Undercover-Mission gehen; Fortgeschrittene (7. bis 9. Klasse) helfen dem Agenten-Team, den Code des internationalen Agentenregisters zurück zu ergattern. Auch Schulklassen und Profis können miträtseln, letztere allerdings außer Konkurrenz. Anmeldungen sind ab sofort auf krypto-im-advent.de möglich – die Teilnahme ist wie immer kostenlos.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Dezember 2019	
03.12.	Black Hat Europe 2019 (Blackhat, London/UK)
05.12.	Geliebter Feind – Enemy Mine (KA-IT-SI, Karlsruhe)
05.-06.12.	8. DFN-Konferenz Datenschutz (DFN-Verein/DFN-CERT, Berlin)
10.12.	GERMAN OWASP DAY 2019 (OWASP Foundation, Karlsruhe)
27.-31.12.	Chaos Communication Congress 36C3 (Chaos Computer Club, Leipzig)
Januar 2020	
20.-22.01.	Omnisecure 2020 (in TIME, Berlin)
21.-24.01.	AppSec California 2020 (OWASP Foundation, Santa Monica/US)>
31.01.-02.02.	ShmooCon 2020 (The Shmoo Group, Washington/US)

Fundsache

Das NIST Cybersecurity Framework v1.1 ist eine am 16.04.2018 publizierte Sammlung von nach Phasen (Identify, Protect, Detect, Respond, Recover) sortierten IT-Schutzmaßnahmen, die eine umfassende Hilfestellung zur Organisation der Informationssicherheit darstellt. Wertvoll sind auch die zusätzlichen Verweise, wo sich einzelne Maßnahmen in den bekanntesten Sicherheitsstandards wiederfinden.

Impressum

Secorvo Security News – ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Friederike Schellhas-Mende

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 2019

Zauberlehrlinge

Walle! Walle manche Strecke, dass zum Zwecke Software fließe, und mit reichem, vollem Schwalle in den Rechner sich ergieße.

Das haben wir weder gewollt noch gemeint, als wir in den späten 90er Jahren regelmäßige Sicherheits-Patches forderten: Wer sich heute mit dem Internet verbindet, um einige wenige Sätze lange E-Mails abzurufen, wundert sich regelmäßig über sein rapide schrumpfendes Downloadkontingent. Denn nicht selten laden Rechner und Smartphones täglich Updates für Programme („Apps“) und Betriebssystem im Umfang von mehreren Gigabyte – je Gerät in etwa das Volumen aller täglichen Twitter-Nachrichten zusammen, weltweit.

Kein Wunder, dass Bandbreiten knapp und Netze ständig überlastet sind. Herstellern und Providern kann das wohl recht sein – der ungebändigt steigende Datenhunger nährt ihre Geschäfte, und der Kunde zahlt, ohne zu bemerken, dass es gar nicht seine Nutzung ist, die den Datenverkehr verursacht. Dabei scheint das eine das andere zu befeuern: Die Frequenz, in der Apps heute aktualisiert werden, legt nahe, dass die Hersteller es mit der Sorgfalt nicht (mehr) so genau nehmen. Warum auch, wenn man schon morgen das nächste Update nachschieben und die (Sicherheits-) Tests auf den Kunden auslagern kann?

Und so sind wir dabei, das Verhältnis von Nutzdaten zum gesamten Datenvolumen rapide zu verschlechtern. Zum Glück sind da noch die Video-Streamer, sonst wären wir wohl schon deutlich unter der Ein-Prozent-Marke. Und während unsere Kinder freitags im Namen von Umwelt und Zukunft die Schule schwänzen, verbraten ihre Smartphones und die zugehörige Netzwerkinfrastruktur über 90% der Energie für die Übermittlung von Wegwerfcode, der schon bald durch ein Update ersetzt werden wird.

Diesmal ist es mit einem „*In die Ecke, Besen! Besen! Seids gewesen.*“ des Meisters wohl nicht getan.

Inhalt

Security News

Top 25 Software Errors

Neben dem bekannten CVE-System zur eindeutigen Identifizierung von konkreten, produktspezifischen Schwachstellen bietet die weniger bekannte „Common Weakness Enumeration“ (CWE) eine detaillierte Übersicht und Kategorisierung bekannter Fehler in Software. Die gefährlichsten werden in der Liste der „Top 25 Most Dangerous Software Errors“ geführt, die am 18.09.2019 zum ersten Mal seit acht Jahren neu erstellt wurde. Dafür wurden ca. 25.000 CVE-Einträge und deren Verknüpfungen zu CWE-Einträgen aus den vergangenen zwei Jahren ausgewertet. SQL Injections fielen dabei von Platz 1 auf Platz 6 zurück, während Cross-Site Scripting (XSS) und Out-of-Bounds-Speicherzugriffe (wie z. B. „Buffer Overflows“) die neue Liste anführen.

Die detaillierten Erläuterungen der Fehlertypen mit Code-Beispielen in mehreren Programmiersprachen und Vorschlägen für Gegenmaßnahmen aus unterschiedlichen Perspektiven sind eine empfehlenswerte Handreichung für jeden Software-Entwickler.

DSGVO-Erfahrungen

Am 06.11.2019 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) einen Erfahrungsbericht über die DSGVO-Umsetzung verabschiedet und Anfang Dezember veröffentlicht. Darin werden die Bereiche Informationspflichten, Recht auf Unterlagenkopien, Benennungspflicht des Datenschutzbeauftragten, Vorfallsmeldungen, Zweckbindung, Sanktionspraxis, Privacy by design, Direktwerbung, Profiling und einige eher die Zusammenarbeit der Behörden betreffende Fragen diskutiert. Zu einer Reihe von Regelungen werden Änderungsvorschläge gemacht.

Dabei wird deutlich, dass es sich um Erfahrungen der Aufsichtsbehörden handelt – der radikalste Vorschlag ist die Streichung der Meldepflicht des Datenschutzbeauftragten; die Veröffentlichungspflicht reiche aus. Der ausufernde Informationskatalog des Art. 13 f DSGVO soll bei zu erwartender Verarbeitung nur auf Verlangen erteilt werden. Weiter wird der Anstieg von Bagatellmeldungen beklagt – die in vielen Fällen entbehrliche 72-Stunden-Frist wird hingegen nicht thematisiert. Zwar wird der Bedarf eines Datenschutzmanagements festgestellt, aber dessen konkrete Ausgestaltung nicht diskutiert. Für das Profiling wird eine Verschärfung des Verbots aus Art. 22 DSGVO gefordert und für Art. 25 DSGVO (Privacy by design) eine Ausdehnung auf die Hersteller als Adressaten.

Insgesamt hätte man dem Bericht mehr Mut zur kritischen Vernunft, einen weniger eingeschränkten Blick sowie einen größeren Themenumfang gewünscht.

Responsible Disclosure

Am 09.12.2019 bat die Internet Engineering Task Force (IETF) um eine letzte Kommentierung des Drafts „A Method for Web Security Policies“. Dieser Internet-Standard spezifiziert die Informationen für Sicherheitsforscher, wie gefundene Schwachstellen bei den Betreibern gemeldet werden können. Die Ablage soll in einer Datei namens „security.txt“ erfolgen, die Webseitenbetreiber auf ihrem Webserver im Verzeichnis „/.well-known/“ ablegen. Vorgesehen sind neben den üblichen Kontaktdaten (E-Mail, Telefon) auch Bug-Bounty-Programme, und zwar sowohl solche des Betreibers als auch von Plattformen wie HackerOne oder Bugcrowd. Noch vor Verabschiedung des Standards bietet der Webdienst securitytxt.org bereits eine Funktion zum Erstellen einer solchen Datei und hilfreiche Hinweise zum Thema. Es wäre erfreulich, wenn sich diese Meldewegedokumentation in der Praxis durchsetzt.

Schuld ist immer der Andere

Am 05.12.2019 hat das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein den Volltext des Urteils des Bundesverwaltungsgerichts (BVerwG) vom 11.09.2019 veröffentlicht und in einer Pressemitteilung kommentiert. Kernpunkt war die Frage, ob der Betreiber einer Facebook Fanpage datenschutzrechtlicher Verantwortlicher ist oder nicht. Der im Rahmen des Vorabentscheidungsersuchens mit dieser Frage ebenfalls befasste EuGH hatte dies bereits am 05.06.2018 bejaht (SSN 07/2018). Das BVerwG hat nun in den Urteilsgründen klargestellt, dass es beim Betrieb der Fanpages nicht nur einen Fall der gemeinsamen Verantwortlichkeit sieht, sondern dass darüber hinaus auch der Betreiber der Facebook Fanpage verantwortlich im Sinne von Art. 2 lit. d) der Datenschutzrichtlinie ist. Weiter sei auch das BDSG alter Fassung unionsrechtskonform auszulegen, und deshalb sei auch der Betreiber einer Facebook Fanpage verantwortliche Stelle im Sinne des § 38 Abs. 5 BDSG a.F., unabhängig davon, ob im Rahmen einer gemeinsamen Verantwortlichkeit die Verantwortlichen in gleichem Maße Zugriff auf die personenbezogenen Daten haben.

Das Urteil bezieht sich allerdings auf die Rechtslage im Dezember 2011. Fanpage-Betreiber werden aber auch zukünftig Adressaten von ähnlichen Verfügungen sein können. Wie die Rechtmäßigkeit der Verarbeitungen durch Facebook nach aktueller Rechtslage zu beurteilen ist, bleibt im Urteil unbeantwor-

tet. Wer eine Facebook Fanpage betreibt, sollte sich jedoch seiner desbezüglichen Verantwortung bewusst sein und die notwendigen Maßnahmen zur Information der Betroffenen ergreifen sowie den Schutz der personenbezogenen Daten ernst nehmen.

German OWASP Day 2019

Am 10.12.2019 fand der German OWASP Day in Karlsruhe statt. Die gut besuchte und sehr gut organisierte Veranstaltung bot eine Reihe spannender und interessanter Vorträge. Besonders gut gefallen haben uns die Keynote von Christoph Kerschbaumer zu den verschiedenen Schichten der Firefox-Härtung und der von Jiska Classen sehr unterhaltsam vorgetragene Hack von Vorwerk-Staubsauger-Robotern. Empfehlenswert auch die von Franziska Bühler vorgestellte Möglichkeit von "ModDevOpsSec" – ein pragmatisches Vorgehen, wie man Security bei DevOps berücksichtigen und in das Ganze auch noch eine Web Application Firewall auf Basis von ModSecurity integrieren kann. So kann die Absicherung von Web Applikationen tatsächlich gut funktionieren.

RSA-240 faktorisiert

Am 02.12.2019 informierte eine Gruppe französischer Zahlentheoretiker um Emmanuel Thomé, dass ihnen die Faktorisierung von RSA-240 (795 bit) der RSA Factoring Challenge aus dem Jahr 1991 gelungen sei. Der Aufwand lag dank verbesserter Algorithmen rund 25% unter dem der Faktorisierung von RSA-232 (768 bit) vor ziemlich genau zehn Jahren (SSN 01/2010). Die Faktorisierungserfolge machen damit eine „Seitwärtsbewegung“ – und bleiben deutlich unter unserer Prognose aus dem Jahr 2002. Mit der Faktorisierung eines 1024-bit-Schlüssels (RSA-309) ist für das Jahr 2020 also eher nicht zu rechnen. Die Faktorisierung eines doppelt so langen, 2048-bit-RSA-Schlüssels (RSA-617) dürfte nach der Prognose nicht vor 2060 gelingen – wären da nicht die Quantencomputer, denen das (zumindest theoretisch) innerhalb von acht Stunden gelingen könnte, wie von Craig Gidney und Martin Ekera am 05.12.2019 beschrieben.

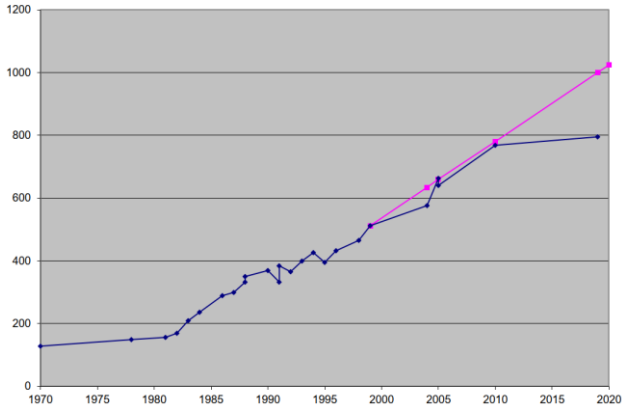

Abb.: Faktorisierungserfolge (blau), Prognose (rot)

DSGVO-konformes Win10

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat am 06./07.11.2019 ein Prüfschema zu Windows 10 veröffentlicht, das Verantwortliche in der Beantwortung der Frage unterstützt, ob Windows 10 DSGVO-konform eingesetzt wird.

Nach dem Prüfschema für Windows 10 und den zugehörigen wietergehenden technischen Hinweisen der DSK ist dafür insbesondere zu prüfen, ob eine Rechtsgrundlage für eine Übermittlung an Microsoft vorliegt. Da sich nicht alle Datenübermittlungen deaktivieren lassen, müssen erforderlichenfalls weitere technische und organisatorische Maßnahmen ergriffen werden, um unzulässige Übermittlungen zu unterbinden.

Secorvo News

... und noch nie zu fragen wagten.

Keine Novellierung des Datenschutzrechts hat eine solche Aufmerksamkeit bekommen wie die im Mai 2018 in Kraft getretene Datenschutz-Grundverordnung. Obwohl fast alles beim Alten geblieben ist, ist doch alles anders... und sind viele konkrete Fragen offen: Wann ist das Tracking von Webseitenbesuchern zulässig? Wie kann ein Unternehmen seine Informationspflichten angemessen erfüllen? Welche Datenschutzvorfälle sind meldepflichtig? Wie bestimmt sich die Höhe eines Bußgelds?

Zu diesen, weiteren und auch Ihren Fragen zur DSGVO und dem Datenschutz wird uns auf dem Jahresstart-Event der KA-IT-Si am **13.02.2019** Dr. Stefan Brink, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Rede und Antwort stehen. Wir freuen uns sehr auf diesen Termin, denn Dr. Brink ist für seine klaren Einschätzungen bekannt – und hoffen auf großes Interesse Ihrerseits.

Wir empfehlen eine frühzeitige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Januar 2020	
20.-22.01.	Omnisecure 2020 (in TIME, Berlin)
21.-24.01.	AppSec California 2020 (OWASP Foundation, Santa Monica/US)
31.01.-02.02.	ShmooCon 2020 (The Shmoo Group, Washington/US)
Februar 2020	
19.-20.02.	30. ID:SMART Workshop (Fraunhofer Institut SIT, Darmstadt)
24.-25.02.	27. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, Hamburg)
März 2020	
09.-12.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
16.-19.03.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
17.-20.03.	GI Sicherheit 2020 (Gesellschaft für Informatik, Göttingen)
25.-26.03.	secIT 2020 (Heise Medien, Hannover)

Fundsache

Das BSI bietet im Rahmen des Services BSI für Bürger eine Reihe von Erklärvideos an. Die anschaulich animierten Kurzfilme weisen auf wichtige Aspekte der IT-Sicherheit wie Backup, Browsersicherheit, Phishing und das Löschen von Daten auf Smartphones hin. Empfehlenswert.

Impressum

Secorvo Security News – ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Fabian Ebner, Stefan Gora, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Christian Titze.

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