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