secorvo
security consulting

Secorvo Security News

August 2020

Vermintes Terrain

Bei manchen Gelegenheiten sollte man zurückhaltend sein, Kenntnisse in der IT-Sicherheit oder dem Datenschutz durchblicken zu lassen. Zum Beispiel beim Abendessen mit Freunden. Eine der sich nach einem solchen „Coming Out" geradezu schicksalhaft ergebenden Fragen, die jeden noch so zauberhaften Abend irreparabel pulverisieren kann, ist – pars pro toto – diese hier: „Ist Whatsapp eigentlich sicher?"

Wo soll man da anfangen – und was lieber verschweigen? Dass die Kontaktdaten des Smartphones an Whatsapp übertragen werden? Dass eine solche Übermittlung von Daten Dritter in die USA rechtswidrig ist? Dass Whatsapp sich die Rechte an allen Inhalten übertragen lässt? Dass Whatsapp nach eigenen Angaben Ende-zu-Ende-Verschlüsselung realisiert? Dass man diese Behauptung nicht sicher bestätigen kann – schließlich könnte es ja eine „Hintertür" geben? Dass verlinkte Inhalte nicht in die Verschlüsselung eingeschlossen sind? Dass Whatsapp-Videochats ohnehin unverschlüsselt übertragen werden? Dass das vielleicht gar nicht die wichtigste Frage ist, da die Verbindungsdaten ein „digitales Bewegungsbild" liefern? Dass Whatsapp zum Facebook-Konzern gehört – und dass für diesen Verbindungsdaten ohnehin wertvoller sind als Kommunikationsinhalte? Dass „ich hab' ja nichts zu verbergen" das denkbar ignoranteste Argument gegen Datenschutz ist? Dass „Soziale Netzwerke" keine Sozialkontakte ersetzen sollten? Dass Bewegung für die Entwicklung der Sprösslinge besonders wichtig ist – und zwar nicht nur für die Daumen? Und – spätestens hier werden Sie mit hoher Wahrscheinlichkeit enthauptet – dass die Vermittlung von Digitalkompetenz und der damit einhergehenden „digitalen Souveränität" wichtiger sein sollte als die Befürchtung sozialer Ausgrenzung, und es sich daher lohnt, sich dem Anpassungsdruck entgegenzustellen?

Wissen kann manchmal einsam machen.

Inhalt

secorvo
security consulting

Security News

Folgen von „Schrems II“

Nach dem Urteil des EuGH zur Ungültigkeit des EU/US Privacy-Shield (C-311/18) vom 16.07.2020 hat Google mit ersten Hinweisen zur Neugestaltung seiner Datenübermittlungen in die USA reagiert und erweitert seine Vertragsbedingungen für Werbeprodukte und Google Analytics um Standardvertragsklauseln. Zudem kann der Anwender bei Beauftragung aktuell entweder die Variante "Auftragsverarbeitung" für verschiedene Dienste, darunter Analytics, oder unabhängige Verantwortung ankreuzen. Die Einordnung als gemeinsame Verantwortung der DSK vom 12.05.2020 wird damit nicht umgesetzt. Google hält seine Anwender zudem zum Einholen von Einwilligungen der Nutzer an, stellt hierzu auch Hilfen zur Verfügung und verweist auf seine Informationen zur Datennutzung.

Diese Reaktion wird von Max Schrems und der neu gegründeten Initiative „My Privacy is None of Your Business“ als unzureichend angesehen. Um die Aufsichtsbehörden zur Urteilsdurchsetzung zu zwingen hat die Initiative daher Seiten großer Unternehmen gescannt und Beschwerden über die fortgesetzte Nutzung eingereicht; inzwischen liegen Beschwerden gegen 101 Unternehmen in 30 EU-Staaten vor.

Auch die Haltung der deutschen Aufsichtsbehörden ist eindeutig, wie u. a. die Stellungnahme des LfDI Baden-Württemberg vom 25.08.2020 belegt. „Retten“ lässt sich die Situation wohl allein durch eine technische Beschränkung der Datenverarbeitung auf Europa und eine aufklärende Erneuerung der Informationen zur Datennutzung seitens Google – oder den konsequenten Verzicht auf die Nutzung dieser Dienste.

Alt und anfällig...

E-Mails dominieren weltweit sowohl die private als auch die Unternehmenskommunikation. Das dabei verwendete „Simple Mail Transfer Protocol“ (SMTP) feierte in diesem Monat seinen 38. Geburtstag – und stammt aus einer Zeit, in der Sicherheitsmechanismen noch nicht zu den Kernfunktionen eines Protokolls zählten. Passenderweise stellten drei Forscher am 06.08.2020 auf der Blackhat USA 18 Angriffe auf E-Mail-Sender-Authentisierung vor und zeigten, wie anfällig E-Mail-Infrastrukturen auch mit nachträglich eingebauten Sicherheitsmechanismen wie SPF, DKIM und DMARC sind. Sicherheitsaufsätze stoßen auch hier an ihre Grenzen.

Angriffe mit gefälschten Absendern zählen derzeit zu den erfolgreichsten Wegen, Schadsoftware zu verbreiten, wie der unlängst wiederbelebte Emotet demonstriert. Aufgrund der veralteten Architektur wird E-Mail auch mit Sicherheitsaufsätzen auf lange Zeit unsicher bleiben. Daher müssen neben technischen Schutzmaßnahmen vor allem auch die Menschen über die Fallstricke von E-Mail aufgeklärt werden.

Qualifikation des DSB

Das Landesarbeitsgericht (LAG) Mecklenburg-Vorpommern hat am 25.02.2020 über die Abberufungsvoraussetzungen eines Datenschutzbeauftragten (DSB) entschieden. Dabei traf es eine Reihe von Feststellungen zu den erforderlichen Qualifikationen und zum Pflichtumfang des DSB. Zur Qualifikation stellt das LAG fest, dass ein Volljurist mit Rückgriff auf technisches Personal zur Klärung von Fragen ohne weiteres über die erforderliche Fachkenntnis verfügt bzw. Datenschutzrecht korrekt anwenden kann.

Bezüglich der Pflichten war streitig, ob der DSB durch eine unterbliebene Verarbeitungsbeanstandung und einen Hinweis im Januar 2018, die DSGVO könne erst mit Geltung umgesetzt werden, seine Pflichten verletzt habe. Hierzu führt das LAG aus, dass ein DSB bei mehreren Betrieben und umfangreicher Datenverarbeitung zwangsläufig Prioritäten setzen muss. Durch Schulungen, Bearbeitungen von Anfragen und Mitwirkung in entsprechenden Unternehmensgremien hat er seine Pflichten erfüllt. Für die Einhaltung des Datenschutzes ist letztlich das Unternehmen verantwortlich. Dies galt auch für die Vorbereitungen zur Umsetzung der DSGVO.

Die Position des DSB wird durch das Urteil gestärkt, gleichzeitig werden die Anforderungen an seine Tätigkeit auf eine realistische Erwartung beschränkt. Als Orientierung für die Aufgabenbeschreibung bietet das Urteil hilfreiche Bezüge.

Listen to the Key

In ihrem am 24.08.2020 als Videoaufzeichnung erschienenen Vortrag von der HotMobile 2020 stellten Sicherheitsforscher der National University of Singapore einen neuen Angriff auf physische Schließsysteme vor. Die Forscher konnten zeigen, dass Angreifer neben dem bekannten Lockpicking auch das Geräusch eines ins Schloss geschobenen Schlüssels analysieren können. Denn aus dem z. B. mittels Smartphone-Mikro aufgezeichneten Geräusch der Pins beim Einschieben lässt sich das Profil des Schlüssels errechnen und ein passender Nachschlüssel fräsen – vorausgesetzt, der Angreifer kennt den Typ von Schloss und Schlüssel und der Schlüssel wird mit gleichmäßiger Geschwindigkeit eingeschoben. Eine App, die aus einer Audio-Aufnahme automatisch Nachschlüssel erzeugt, liegt also immerhin noch in einiger Ferne.

Bei dem Angriff handelt es sich um einen typischen Seitenkanalangriff. Darüber lassen sich häufig auch gute „primäre“ Schutzmechanismen umgehen: So kann beispielsweise ein grundsätzlich sicheres Kryptoverfahren einem Angreifer über Laufzeit- oder Spannungsunterschiede bei der Berechnung die Rekonstruktion des Schlüssels oder Klartextes ermöglichen. Solche Angriffe wurden u. a. bei der Mifare DESFire-Karte gezeigt. Andere Seitenkanalangriffe sind ein Passwortdiebstahl durch Aufzeichnung der Tippgeräusche oder Wärmebildaufnahmen der Tastatur. Die Härtung gegen Seitenkanalangriffe ist allerdings eine herausfordernde Angelegenheit.

Out of Scope

Dass beauftragte Einbrüche – ob digital als Penetrationstest oder physikalisch beispielsweise als Bestandteil eines Red-Team-Assessments – immer auch mit Risiken verbunden sind, hat der Fall zweier amerikanischer Penetrationstester eindrucksvoll gezeigt. Als diese am Abend des 11.09.2019 im Rahmen eines größeren, vom Staat Iowa beauftragten Assessments zum Testen des Alarmsystems durch eine offene Tür in das Dallas County Courthouse in Iowa eingedrungen waren, verließen sie das Gebäude in Handschellen – obwohl sie die schriftliche Freigabe für das Assessment mit sich führten und sich gegenüber den Beamten identifizieren konnten. Nach mehr als fünf Monaten rechtlichen Trubels wurden die Pentester Ende Januar 2020 freigesprochen. Eine Zusammenfassung der gesamten Geschichte mitsamt „Lessons learned“ gaben die beiden nun auf der Blackhat 2020.

Hilfreich war, dass ihr Arbeitgeber Coalfire sich unermüdlich für die beiden Mitarbeiter einsetzte. Um ähnliche Vorfälle zu vermeiden, rät Coalfire Auftraggebern und Pentestern, Vereinbarungen zum Ablauf eines Assessments immer schriftlich zu dokumentieren und die zugehörigen Vertragsunterlagen im Vorfeld von Juristen überprüfen zu lassen.

Auch klassische Penetrationstests können mit ähnlichen Risiken verbunden sein, wie der Fall von Rob Fuller zeigt: Durch einen winzigen Schreibfehler im vom Kunden genannten IP-Adressblock wurde das falsche Unternehmen angegriffen. Obwohl es in diesem konkreten Fall ohne negative Folgen blieb (und sogar zu einem neuen Kunden führte), hätten auch hier rechtliche Konsequenzen drohen können. Die eindeutige Klärung des Auftragsumfangs und der Zielobjekte („In Scope“/„Out of Scope“) muss deshalb zentraler Bestandteil einer jeden Vereinbarung zu einem Security Assessment sein.

Vergissmein(nicht)?

Der Bundesgerichtshof (BGH) entschied am 27.07.2020 bezüglich zweier Verfahren, wann Suchergebnisse durch Google zu löschen sind. Im ersten Fall konnte der Betroffene nicht erreichen, dass direkt auf ihn beziehbare Daten entfernt werden, da die Grundrechtsabwägung keinen Vorrang seines Schutzinteresses ergab. Das zweite Verfahren wurde ausgesetzt und mit weiteren Fragen an den Europäischen Gerichtshof (EuGH) für eine Vorabentscheidung eingereicht. Darin muss die Frage beurteilt werden, ob Google – nach Auffassung der Kläger – inhaltlich falsche Artikel eines Unternehmens über die Betroffenen löschen muss.

Im Urteil C-507/17 vom 24.09.2019 beschied der EuGH, dass Betreiber nicht verpflichtet sind, Auslistungen in sämtlichen Versionen ihrer Suchmaschinen vorzunehmen, sondern diese auf alle mitgliedstaatlichen Versionen beschränkt werden können. Aufgrund nationaler Datenschutzstandards können die Behörden eines Mitgliedsstaates jedoch eine Löschung in allen Versionen verlangen. Auch daraus wird deutlich, dass das in Art. 17 der DSGVO verankerte Recht auf „Vergessenwerden“ immer für den konkreten Einzelfall betrachtet werden muss.

Secorvo News

KA-IT-Si-Stammtisch

Aufgrund der nach wie vor geltenden Auflagen im Veranstaltungsbereich können wir unsere KA-IT-Si-Events nicht wie gewohnt durchführen. Daher möchten wir mit unserem ersten „KA-IT-Si-Stammtisch“ am **Donnerstag, 24.09.2020**, ab 18 Uhr im Biergarten der „Ersten Fracht“ in Karlsruhe (direkt gegenüber dem Hauptbahnhof) eine Plattform für den Austausch bieten.

Dort erwarten Sie vier verschiedene Thementische mit Andreas Sperber von aramido (Penetrationstests – das Was und Wie), Dr. Ingmar Baumgart vom FZI (Vulnerability Disclosure), Dirk Fox von Secorvo (Phishing-Awareness) und Oliver Winzenried von WIBU-Systems (Karlsruher „House of IT-Security“ und die zukünftige IT-Security Coworking Area). Die Ansprechpartner werden die Diskussionen mit einer kurzen Einführung in das Thema anstoßen.

Bei Interesse reservieren wir Ihnen gerne einen Platz an Ihrem ausgewählten Thementisch. Bitte melden Sie sich dafür bis Dienstag, 22. September 2020 an (keine Teilnahmegebühr, Bewirtungskosten exklusive).

Secorvo Seminare

Eine Terminübersicht, ausführliche Programme und die Möglichkeit zur Online-Anmeldung finden Sie auf unserer Webseite.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

September 2020	
07.-11.09.	IEEE European Symposium on Security and Privacy (IEEE Computer Society, Genua/IT)
14.-17.09.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
21.-22.09.	Security of Things World (we.CONECT Global Leaders GmbH, Berlin)
21.-25.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
22.09.	Datenschutztag 2020 (COMPUTAS. Köln)
24.09.	IT-Sicherheitsrechtstag (TeleTrusT e.V., Berlin)
29.09.-01.10.	Informatik 2020 (GI Gesellschaft für Informatik, Karlsruhe)
29.09.-02.10.	Blackhat Asia 2020 (Blackhat, Singapur/SIN)
Oktober 2020	
12.-14.10.	ISSE 2020 (IEEE, Wien/A)
13.10.	Swiss Cyber Storm (Swiss Cyber Storm Association, Bern/CH
22.-23.10.	heise devSec 2020 (dpunkt.verlag, heise Developer, heise Security, Heidelberg

Fundsache

Der Vortrag My Cloud is APT's Cloud: Investigating and Defending Office 365 zeigt bekannte und weniger bekannte Angriffe auf Microsofts Cloud-Lösungen auf, die in Zeiten von Covid-19 immer mehr an Bedeutung gewonnen haben.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, 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