Secorvo Security News

Februar 2023

Leichen im Keller

Jede App, die personenbezogene Daten verarbeitet, muss diese Verarbeitung in einer Datenschutzerklärung erläutern. Nur so ist eine „faire und transparente" Verarbeitung der Daten – wie von der DSGVO gefordert – möglich, da für einen Nutzer beispielsweise nicht offensichtlich ist, ob eine App die Verarbeitung lokal durchführt oder einen Cloud-Dienst in Anspruch nimmt.

Geht die Verarbeitung über den eigentlichen Anwendungszweck der App hinaus, weil der Anbieter zusätzliche Daten für eigene (bspw. Marketing-) Zwecke erhebt, wie zur Bildung von Nutzerprofilen, oder gar Daten an Dritte (beispielsweise verbundene Unternehmen) weitergibt, ist eine Einwilligung der Betroffenen erforderlich – und die ist nur rechtswirksam, wenn sie *informiert* erfolgt. Eine am 23.02.2023 veröffentlichte Forschungsstudie der Mozilla Foundation zeigt, dass zahlreiche Unternehmen hier „Leichen im Keller" haben: Von den 40 Apps mit den höchsten Download-Zahlen des Google Play Store stimmten bei fast 80% die Angaben in der Datenschutzerklärung nicht mit den Angaben der Entwickler in Googles Data Safety Form überein, die im Google Play Store angezeigt werden. Bei 40% der Apps waren die Abweichungen gravierend – so weisen beispielsweise weder TikTok noch Twitter ihre Datenweitergaben an Werbeplattformen aus. Eine auf solchen unvollständigen Informationen beruhende Einwilligung in die Verarbeitung ist damit unwirksam – und die Verarbeitung der Daten somit rechtswidrig.

Die Zahlen sind erschreckend, denn die Studie untersuchte nur die Abweichung der Datenschutzerklärung von den Angaben der Entwickler im Play Store – welche Daten von den Apps (und den dahinter liegenden Plattformen) *tatsächlich* verarbeitet und an Dritte weitergegeben werden, wurde nicht untersucht. Nach einer Langzeitstudie von ARD und ZDF verbrachten die Deutschen 2021 rund 3,4 h pro Tag mit dem Smartphone. Die dabei anfallenden Daten liefern ein Verhaltensprofil aller Deutschen.

Security News

Tesla reagiert

Am 22.02.2023 veröffentlichte die niederländische Datenschutz-Aufsichtsbehörde (DPA) ihr Untersuchungsergebnis des „Wächter-Modus" in Tesla-Fahrzeugen. Danach hat Tesla erfreulicherweise auf die vielfach geäußerte Kritik (siehe SSN 07/2022 und SSN 08/2022) reagiert: Möchte der Fahrzeuginhaber den „Wächter-Modus" nutzen, muss er ihn nun zunächst aktivieren. Die Aufnahmen werden nur noch für die Dauer von zehn Minuten und ausschließlich im Fahrzeug gespeichert; so wird eine Dauerüberwachung der Fahrzeugumgebung vermieden. Zudem filmen die Ka-

meras nur, wenn das Fahrzeug berührt wird. Eine Anzeige im Fahrzeug und die Innenbeleuchtung signalisieren Betroffenen, dass Videoaufnahmen stattfinden. Die DPA hat deshalb von der Verhängung eines Bußgelds gegen Tesla abgesehen und weist darauf hin, dass der Fahrzeughalter datenschutzrechtlich für die Videoaufnahmen verantwortlich ist. Grundsätzlich gelten für in Fahrzeugen verbaute Kameras die gleichen Regelungen wie für jede andere Kamera.

Vorgaben für S/MIME-Zertifikate

Trust Center, die Zertifikate anbieten, die von Browsern akzeptiert werden sollen, müssen sich an die Vorgaben des 2005 gegründeten CA/Browser-Forums (CAB) halten. Am 01.01.2023 veröffentlichte das CAB nun die von einer Arbeitsgruppe über gut zwei Jahre entwickelten Mindestanforderungen an S/MIME-Zertifikate. 84 Seiten füllen die Vorgaben, die am 01.09.2023 in Kraft treten. Danach müssen Zertifikatsaussteller die Identität des Antragstellers bei Personenzertifikaten genauer prüfen und diese Prüfung dokumentieren. Die Kriterien für die Auditierung der PKI werden noch diskutiert und zu einem späteren Zeitpunkt veröffentlicht.

Die Identitätsprüfung ist bei S/MIME-Zertifikaten zweifellos ein (sicherheits)kritischer Punkt – das Vertrauen in Personenzertifikate dürfte daher durch die neuen Vorgaben steigen. Allerdings könnten auch die bestehenden Registrierungsprozesse in Unternehmen, die öffentliche S/MIME-Zertifikate beziehen, von den Vorgaben betroffen sein – schlimmstenfalls ist beim nächsten Zertifikatswechsel die Registrierung zu wiederholen.

It's not a bug

Am 08.02.2023 wurde eine kontrovers diskutierte Schwachstelle im verbreiteten Passwort-Manager KeePass behoben. Konkret ging es um eine für Automatisierungsprozesse eingebaute Funktion, mit der die Passwort-Datenbank nach dem Entsperren durch den Anwender unverschlüsselt exportiert werden kann. Das (vermeintliche) Problem: Kann ein Angreifer die Konfigurationsdatei von KeePass ändern, dann kann er diese Funktionalität ohne Wissen des Benutzers aktivieren und darüber die Passwörter auslesen.

Der Fall lässt Parallelen zur Schwachstelle Log4Shell erkennen, bei der eine Funktion, die die meisten Anwender nicht erwarteten, letztlich zu einem Sicherheitsproblem führte. Auch wenn bei KeePass die Auswirkungen deutlich geringer sind: Eine automatisierte Exportfunktion werden hier nur die wenigsten Anwender erwartet haben.

Doch ein Angreifer mit Schreibzugriff auf die Konfigurationsdatei von KeePass kann weitaus mächtigere Angriffe durchführen. Das erläutert KeePass selbst schon seit einigen Jahren auf der eigenen Website. Mit den Worten der KeePass-Entwickler: „KeePass cannot magically run securely in an insecure environment."

Die neue Version 2.53.1 verlangt nun grundsätzlich bei einem Datenbankexport die erneute Eingabe des Master-Passworts.

Leitlinien gegen Irreführung

Nach elfmonatiger öffentlicher Kommentierungsphase veröffentlichte der Europäische Datenschutzausschuss (EDSA) am 14.02.2023 seine Leitlinien zu irreführenden und DSGVO-widrigen Design-Elementen auf Social-Media-Plattformen als Version 2.0. In dem 74-seitigen Dokument werden zahlreiche Irreführungen beschrieben, mit denen Plattformbetreiber versuchen, Benutzer zu verleiten, gegen besseres Wissen ihre Zustimmung zu Tracking und anderen Datenerhebungen zu erteilen. Die verschiedenen Methoden werden in sechs Kategorien strukturiert und anhand 61 konkreter Beispiele veranschaulicht. Einige der beschriebenen irreführenden Design-Elemente finden sich auch auf anderen Plattformen.

Es ist zu erwarten, dass die im Dokument beschriebenen Methoden von den Datenschutz-Aufsichtsbehörden zukünftig bei der Prüfung von Portalen auf Datenschutzverstöße herangezogen werden.

Spyware auf Diensthandys

Nach mehreren Warnungen und dem Verbot der Installation und Nutzung von TikTok, der Videoplattform des chinesischen Bytedance-Konzerns, auf Dienst-Handys der amerikanischen Bundesbehörden haben nun die EU-Kommission (am 28.02.2023) und das EU-Parlament (am 01.03.2023) die Installation und Nutzung des Dienstes auf Dienst-Handys untersagt.

Tatsächlich sind Apps mit großer Verbreitung perfekte Einfallstore für Spionage-Software: Die Geräte sind „always on", kennen den Aufenthaltsort und die Kontaktdaten des Benutzers sowie sein Nutzungsverhalten und können, wenn der Benutzer es zulässt, auf Mikrofon und Kameras zugreifen. Zusätzliche Funktionen lassen sich (bei Bedarf sogar „zielgruppenspezifisch") in Updates unterbringen, an deren ständigen Download sich Smartphone-Nutzer bereits gewöhnt haben. Zwar verhindern Schutzmechanismen der Betriebssysteme, dass eine App auf beliebige Daten und Sensoren zugreift; die erteilten Berechtigungen genügen aber meist, um ein Smartphone in ein Überwachungsgerät zu verwandeln.

Solche Angriffe sind für einen Nutzer bestenfalls an einer kürzeren Laufzeit des Geräts oder erhöhtem Internet-Traffic zu erkennen. Zwar kann man sie temporär außer Gefecht setzen, indem man den GPS-Sensor deaktiviert und die Internet-Verbindung kappt – damit deaktiviert man allerdings auch (fast) alle anderen Anwendungen auf dem Gerät.

Da viele Anbieter nicht einmal die von ihnen verarbeiteten Daten korrekt offenlegen (siehe Editorial), bleibt derzeit nur der Rückgriff auf Apps wie Gardion, die den Netzwerkverkehr des Smartphones nach Vorgaben filtern. Denen muss man allerdings vertrauen.

E-Mail-Tracking & Profiling

In ihrem Vortrag auf der 30. DFN-Konferenz am 09.02.2023 gingen Friederike Schellhas-Mende und Christian Blaicher auf die rechtskonforme Gestaltung von E-Mail-Tracking und Profiling ein. Denn nicht nur

im Browser und in Apps wird das Nutzerverhalten analysiert, sondern zunehmend auch über Newsletter. Aber auch hier gelten UWG, DSGVO und TTDSG.

Damit bedürfen Newsletter mit Werbung nicht nur einer Einwilligung nach § 7 Abs. 2 Nr. 2 UWG. Protokollieren sie das Nutzerverhalten, benötigen sie außerdem eine Einwilligung nach § 25 TTDSG. Wenn zudem Benutzerprofile erstellt werden, ist obendrein eine Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO erforderlich. Eine Volltextveröffentlichung finden Sie auf der Secorvo-Webseite.

Da das Tracking in E-Mail-Newslettern gerne US-amerikanischen Tools (wie klaviyo und Mailchimp) überlassen wird, sollte man sich in einem solchen Fall angesichts der derzeitigen Abmahnungen besonders um eine rechtskonforme Gestaltung kümmern.

Secorvo News

Was sind „Goldene Zertifikate"?

Auf der Heise-Konferenz secIT in Hannover führten Hans-Joachim Knobloch und Oliver Oettinger am 14.03.2023 auf einem eintägigen Workshop in die Grundlagen der zertifikatsbasierten Anmeldung am Active Directory und Angriffe mit „Goldenen Zertifikaten" ein. Einen verdichteten Überblick zum Thema gab Hans-Joachim Knobloch am 15.03.2023 in seiner Keynote.

Secorvo Seminare

Tanken Sie fünf Tage geballtes Wissen und lassen Sie sich anschließend als Experte für IT-Sicherheit zertifizieren: In unserem T.I.S.P. Seminar vom **27**. bis **31.03.2023** haben wir noch letzte freie Plätze.

Von den Grundlagen bis zur Planung Ihrer eigenen PKI: Alle wichtigen Aspekte von Public Key Infrastrukturen lernen Sie im PKI-Seminar vom **24**. bis **27.04.2023** kennen. In Workshops setzen Sie die Erkenntnisse aus den Vorträgen direkt um.

Von Praktikern für Praktiker: Mit unserem 3-Tages-Seminar „BSI Vorfall-Experte – Aufbauschulung" vom **09.** bis **11.05.2023** sind Sie bestens gerüstet für die Zertifizierung zum Vorfall-Experten gemäß BSI-Curriculum.

Wir freuen uns auf Ihre Anmeldung.

Phish me, if you can

Ein weltweit agierendes Kollektiv anarchischer Hacker, getrieben von anarchistischen Freiheitsidealen, hat sich zum Ziel gesetzt, die vorherrschenden Gesellschaftsstrukturen zu destabilisieren und in totales Chaos zu stürzen. Ihr erstes Ziel: die Energiewirtschaft.

Beim Jahreseröffnungsevent der KA-IT-Si am **16.03.2023** berichtet Jan Tomasch, Information Security Awareness Manager der EnBW, in seinem Vortrag „Security Awareness Kampagne mit Gamification", wie die Mitarbeitenden der EnBW als Cyber-Interventionsteam ihre Verteidigungslinie aufbauen, um den Hackern das Handwerk zu legen.

Im Anschluss haben Sie Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Net(t)working“. Wir freuen uns auf einen kurzweiligen und interessanten Abend mit Ihnen – und empfehlen eine zügige Anmeldung, da die Teilnehmerzahl auf 150 beschränkt ist.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

März 2023	
14.-16.03.	secIT 2023 (Heise Medien, Hannover)
16.03.	KA-IT-Si Event Phish me, if you can (KA-IT-Si, Karlsruhe)
21.-24.03.	DFRWS EU 2023 (DFRWS, hybrid)
27.-31.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
April 2023	
23.-27.04.	Eurocrypt 2023 (IACR, Lyon/FR)
24.-27.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
25.-27.04.	Datenschutztage 2023 (WEKA, virtuell)
25.-26.04.	Security Forum 2023 (Hagenberger Kreis, Hagenberg/AT)
Mai 2023	
09.-10.05.	BvD Verbandstag 2023 (BvD, Berlin)
09.-11.05.	BSI Vorfall-Experte - Aufbauschulung (Secorvo, Karlsruhe)
09.-12.05.	Blackhat Asia 2023 (Blackhat, Singapur/ASE)
09.-12.05.	European Identity and Cloud Conference 2023 (KuppingerCole, Berlin, hybrid)
10.-11.05.	19. Deutscher IT-Sicherheitskongress (BSI, virtuell)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Stefan Gora, Kai Jendrian, Oliver Oettinger, Friederike Schellhas-Mende, 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

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.