Bild: Christophe Gateau / dpa

Kein Entkommen

Android-Apps schicken Nutzerdaten ungefragt an Facebook

Ob sie wollen oder nicht: Smartphone-Nutzer senden unzählige Daten an Facebook – selbst wenn sie keinen Account besitzen. Die Datenweitergabe ist so tief in den Apps verwurzelt, dass selbst deren Entwickler oft nicht Bescheid wissen.

Von Torsten Kleinz

Die Datensammelpraxis von Facebook steht seit Jahren in der Kritik. Zwei neue Untersuchungen zeigen, dass Nutzer nicht einmal ein Konto bei Facebook eröffnet oder die App installiert haben müssen, um dem Konzern detaillierte persönliche Informationen zu senden. Dank des in vielen Apps eingebauten Facebook-SDKs fungieren Smartphones als universelle Datensammelstelle für den Konzern und die gesamte Werbeindustrie.

Laut einer Studie der Universität Oxford vom Frühjahr 2018, bei der knapp eine Million Apps aus dem Gooogle Play Store untersucht wurden, enthalten 42,5 Prozent der Apps einen Tracker von Facebook. Damit steht der Konzern auf Platz zwei der Android-Datensammler direkt hinter Google.

Die Organisationen Privacy International (privacyinternational.org) sowie mobilsicher.de haben sich nun die Datenströme populärer Apps genauer angesehen. Dabei stellt Privacy International fest, dass knapp zwei Drittel der untersuchten Apps bereits beim Einschalten Daten an Facebook schicken – bevor der Nutzer davon in Kenntnis gesetzt und um Erlaubnis gefragt wird. Zu den Informationen gehören zumindest der Name der App, Datum und Zeit der Nutzung sowie die AAID oder „Werbe-ID“ von Android, die ein App-übergreifendes Tracking ermöglicht.

Reisepläne und Schwangerschaften

Viele Apps übertragen noch deutlich mehr Informationen. Eine Analyse des verschlüsselten Datenverkehrs mithilfe des Programms „mitmproxy“ enthüllte, dass die App der Reiseplattform Kayak beispielsweise detaillierte Reisepläne an Facebook schickte – inklusive der gebuchten Ticketklasse und mitfliegenden Kinder. Mobilsicher.de stellte fest, dass die App „Schwangerschaft+“ Details über die Schwangerschaft samt dem errechneten Geburtstermin ins Silicon Valley übermittelte. Erst nachdem die Redaktion den App-Hersteller Philips darauf aufmerksam machte, wurde die Datenübermittlung abgestellt.

Andere App-Entwickler zeigen oft jedoch wenig Problembewusstsein. „Gerade größere Anbieter kennen die Funktionalität der Facebook-Schnittstelle, bestehen auf Nachfrage aber darauf, dass die Datenübertragung anonym sei“, erklärt Miriam Ruhenstroth, Redaktionsleiterin von mobilsicher.de.

Dies ist ein verbreitetes Missverständnis. Zwar werden die Daten in der Regel ohne den Realnamen oder die Mail-Adresse eines Nutzers übertragen. Doch die von den Apps automatisch übertragene Werbe-ID ist nicht anonym, sondern pseudonym. Das heißt: Firmen können die Daten eines Nutzers zu einem vollständigen Profil zusammenzufügen. So ist es für Facebook kein Problem, die Informationen einer App mit dem Namen des Nutzers zu kombinieren, wenn dieser auf seinem Gerät die Facebook-App installiert hat.

Unbewusstsein der Entwickler

Ein möglichst reichhaltiges Datenprofil ist die Grundlage für Online-Werbung – für viele App-Anbieter eine unverzichtbare Einkommensquelle. Denn es gibt nur wenige Sponsoren, die Werbung direkt schalten. Die Werbeindustrie ist mittlerweile fast komplett auf das sogenannte „programmatische Advertising“ umgeschwenkt. Das heißt: Werbende Firmen buchen über große Netzwerke die Ausspielung ihrer Botschaften bei bestimmten Zielgruppen. Welche Werbung bei welchem Nutzer auftaucht, wird in einem ausgefeilten Auktionssystem ermittelt.

Ein Anbieter für Babynahrung will beispielsweise bevorzugt bei jungen Eltern annoncieren. Um herauszufinden, wer zu dieser Gruppe gehört, können die Werbenetzwerke viele Datenquellen heranziehen – den von einer App übermittelten Geburtstermin, den Einkaufszettel der Eltern oder das typische Schlaf- und Bewegungsmuster von einem Fitness-Tracker. Ob die Werbung dann in einer App, auf einer Website oder auf einem Smart-TV erscheint, ist für die Werbetreibenden egal. Das Tracking macht es möglich.

Für den Anwender einer App bleibt völlig unklar, welche Informationen über ihn gesammelt und welche Rückschlüsse daraus gezogen werden. So erzählte die Autorin der Studie von Privacy International, dass eine App sie als „Erwachsene“ kategorisierte, ohne ihr Geburtsdatum abzufragen. Die App habe vielleicht aufgrund einer Auswertung des Bewegungs-

sensors in ihrem Smartphone geschlossen, dass sie kein Kind mehr war, witzelte die Autorin. Die Übertragung sei zudem ungesichert, sodass sie von Dritten leicht manipuliert werden könnte.

Aber nicht nur App-Anbieter, die Werbeeinnahmen erzielen wollen, bauen Tracker wie das Facebook-SDK ein. Der Programmbaustein bietet zahlreiche weitere Funktionen: Der bequeme Log-in per Facebook-Account verspricht eine breite Nutzerbasis, die Analytics-Funktion wertvolle Hinweise zur App-Nutzung und der Zugriff auf das Graph-API von Facebook erleichtert es, Inhalte im Freundeskreis zu teilen und die App viral zu bewerben.

Mobilsicher.de fand die Facebook-Schnittstelle auch in zwei Apps von CDU und SPD. Erst nachdem die Redaktion die Parteien kontaktierte, wurde diesen bewusst, dass sie Daten ihrer Mitglieder an Facebook schickten. Die CDU deaktivierte daraufhin die Schnittstelle per Update, die SPD-Fraktion NRW nahm ihre App gar offline.

Schwarzer Peter

Facebook beteuert zwar immer wieder, keine Schattenprofile von Personen ohne Account anzulegen. Welche Daten erhoben, wie lange sie gespeichert werden und welche Rückschlüsse die Algorithmen aus ihnen ziehen, verrät der Konzern jedoch nicht. Nicht zuletzt erfährt Facebook über sein SDK und die 2013 übernommene Analysefirma Onavo, welche Apps auf welchem Smartphone wie oft genutzt werden, und kann mit diesen Informationen aufkommende Konkurrenten entweder aufkaufen oder bekämpfen.

Der Konzern schiebt die Verantwortung den App-Entwicklern zu. Diese seien für die Datenübertragung verantwortlich. Allerdings ist sie von Haus aus im SDK aktiviert. App-Entwickler müssen sie von sich aus abschalten, damit keine Daten übertragen werden. Bis zur SDK-Version 4.34, die von Facebook Mitte Juni 2018 veröffentlicht wurde, konnten Entwickler die Datenübertragung noch nicht einmal so lange verzögern, bis der Nutzer ihr nach dem Start DSGVO-konform zugestimmt hatte. Viele Apps, darunter etwa die von Spotify, setzten aber noch im Dezember 2018 ältere SDK-Versionen ohne Verzögerungsmöglichkeit ein.

Schutzlos ausgeliefert

Android und Facebook bieten im Setup recht gut versteckte Optionen an, sich aus dem Geschäft mit der personalisierten Werbung abzumelden. Für den Normalnutzer ist es aber trotzdem kaum möglich, Kontrolle über den Datenstrom zu erlangen. So hilft es beispielsweise nichts, sich in Android explizit von der persönlichen Werbeauslieferung abzumelden. Laut Privacy International übertrugen einige der untersuchten Apps dann sogar noch mehr Daten.

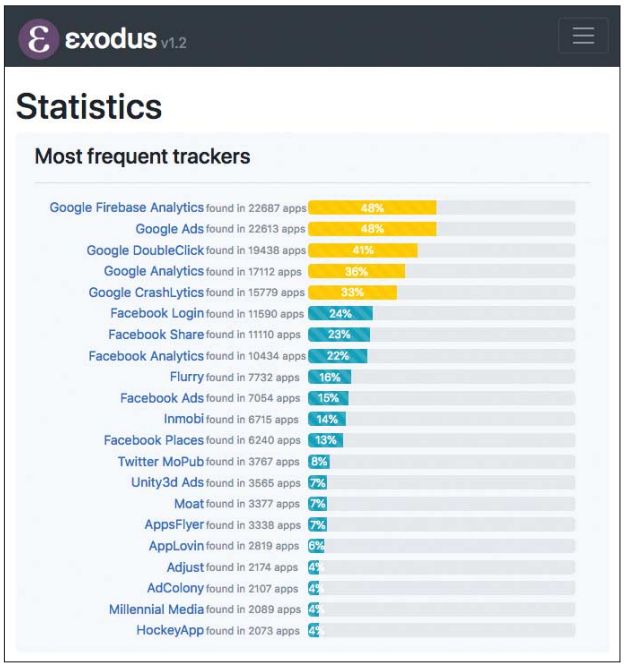
Um seine Spuren zumindest zeitweilig zu verwischen, kann man bei Android unter Einstellungen/Google/Anzeigen die Werbe-ID rotieren. Eine weitere Möglichkeit der Verschleierung besteht darin, Apps in in einem isolierten Arbeitsbereich zu separieren. Einige Android-Smartphones unterstützen das von Haus aus, sonst helfen Apps wie Shelter (siehe c't 22/2018, S. 59). Sie verhindern den Datenaustausch von Apps untereinander, jeder Bereich bekommt eine andere Werbe-ID. Damit erschwert man es den Datensammlern zumindest, ein Profil über einen längeren Zeitraum zu vervollständigen. Ganz verhindern lässt sich dies aber nicht.

Rigoroser arbeiten No-Root-Firewalls wie Netguard und AFWall+, wenn man mit ihnen eine Datenverbindung zu bestimmten Servern wie graph.facebook.com blockiert. Das ist jedoch eine Sisyphosarbeit. Manche Apps versagen dann auch ihren Dienst. Zudem existieren neben Facebook und Google unzählige weitere Datensammler. Allein die Analyse-Plattform Exodus Privacy (exodus-privacy.eu.org) führt 152 Tracker auf, die zum Teil Bewegungsprofile, Einkäufe und persönliche Vorlieben über zigtausende von Apps erheben. Für Nutzer gerooteter Android-Versionen bietet zudem Kuketz die Open-Source-App Blokada an, die die Kommunikation mit Tracking-Servern ins Leere laufen lässt.

Privacy by default

Derlei Aufwand ist normalen Anwendern jedoch kaum zuzumuten. Die Autoren der Studien fordern deshalb, Facebook und Google in die Pflicht zu nehmen. Sie müssen dem Anwender eine einfache Kontrolle darüber geben, welche Daten über ihn erhoben werden – egal ob personalisiert, pseudonymisiert oder anonymisiert. Apps und Programmierschnittstellen sollten zudem den Grundsatz „privacy by default“ befolgen und Daten erst dann sammeln und übertragen, wenn ein Entwickler oder Anwender dies von sich aus explizit wünscht.

Die Autoren betonen, dass die Daten nicht nur unter Android gesammelt werden. Apple hat zumindest in iOS 10 von sich aus die vormalige Betriebssystem-Anbindung an Facebook gekappt und räumt dem Anwender im Setup die Möglichkeit zur Abschaltung des Werbe-Trackings und die Rotation der Werbe-ID ein. Laut dem IT-Experten Klaus Rodewig haben App-Entwickler unter iOS keine Möglichkeit, die Hardware eindeutig zu identifizieren oder die Werbe-ID zu nutzen, wenn der Anwender dies nicht erlaubt. Inwieweit iOS-Apps trotzdem noch Daten an Facebook und andere Tracker übermitteln, will Privacy International im laufenden Jahr genauer untersuchen. *(hag@ct.de)* c't



Exodus Privacy listet in seiner Web-Datenbank Daten-Tracker in Android-Apps auf.