Apps für eine bessere digitale Welt

Datenschutz. Nicht selten ärgern wir uns über Smartphone-Anwendungen, weil sie unseren Bedürfnissen nicht entsprechen. In Wien wurde daran geforscht, wie man Apps ethischer gestalten könnte

iNNOVATiON! FORSCHUNGS-MONTAG
KURIER-SERIE

VON **BARBARA WIMMER**

Smartphone-Apps sind einer der häufigsten Formen, wie Menschen mit dem Internet interagieren. Sei es zum Buchen oder Planen einer Reise, zum Nachsehen, wie das Wetter am nächsten Tag wird, zum Lesen seiner Lieblingszeitung oder zum Kommunizieren mit seinen Freunden und Familie: Apps begleiten uns im Alltag.

Doch nicht selten sammeln die Apps viel mehr Daten über uns, als sie für ihre Anwendung eigentlich bräuchten. Manchmal gibt es vermeintlich harmlose App-Angebote wie QR-Code-Scanner, die im Hintergrund heimlich Informationen mitlesen, die nicht für sie bestimmt sind. Auf vielen Android-Geräten sind außerdem Apps vorinstalliert, die nicht zwingend für grundlegende Funktionen erforderlich sind (sogenannte „Bloatware") und Daten an Drittfirmen übertragen *(siehe unten)*.

AFP/AFP/CHANDAN KHANNA

Smartphone-Apps sind oft sehr datenhungrig. Zwar gibt es mehr Transparenz darüber als früher, doch das reicht Experten nicht

Fakten

6
Tracker
Mit so vielen Werkzeugen werden durchschnittliche Apps derzeit überwacht

300
Tausend
Mal wurden Android-Apps heruntergeladen, die heimlich Bankdaten gestohlen haben, in dem sie auf Passwörter und Tastatureingaben zugriffen und diese heimlich mitprotokollierten

91
Prozent
So viele der auf Android-Geräten vorinstallierten Apps haben keine offizielle Sicherheitsüberprüfung von Google bekommen

Qualitätslabel

Diese Praxis ist alles andere als ethisch in Ordnung. Die Bürgerrechtsorganisation epicenter.works hat im Rahmen des Wissenschafts- und Forschungsförderungsprogramms „Digitaler Humanismus" der Stadt Wien untersucht, wie Apps und die Smartphone-Infrastruktur aussehen müssten, wenn sie ethisch, datenschutzfreundlich und nachhaltig umgesetzt würden.

„Es müsste eine Art Qualitätslabel für Apps geben, über das konkret in Symbolen ausgedrückt wird, was die Apps mit den Daten machen, ähnlich wie bei Lebensmitteln", erläutert Thomas Lohninger, Geschäftsführer von epicenter.works, dem KURIER. „Neben einer Kennzeichnung, ob eine App sich fair verhält, braucht es auch Warnsymbole, wenn Nutzerdaten in die USA übermittelt werden, oder an Drittfirmen weitergegeben werden", so Lohninger. Ein derartiges Gütesiegel dürfe nicht wie bei Lebensmitteln nur die Produkte hervorheben, die sich an bestehende Gesetze halten. „Wir wollen, dass Nutzer mehr Informationen bekommen, als sie bisher haben", sagt Lohninger.

„Wir wollen, dass Nutzer mehr Informationen bekommen, als sie bisher haben."
Thomas Lohninger
epicenter.works
FRANZ GRUBER

Verbesserungen

Seit knapp einem Jahr müssen App-Anbieter, die ihre Anwendungen über den App Store vertreiben, bei den Nutzern die Erlaubnis einholen, bevor sie deren Daten über ihre App und über die Webseite anderer Unternehmen hinweg verfolgen. Die Funktionalität der Apps bleibt dabei aufrecht, auch wenn Nutzer den Apps das Tracking verbieten. Android zog dieses Jahr nach: Seit Kurzem ist es auch im Google Play Store möglich, dass sich Nutzer ein besseres Bild darüber machen können, welche Daten zu welchem Zweck erhoben werden.

„Das ist ein guter, erster Schritt", sagt Lohninger. „Doch es reicht nicht. Nutzer brauchen die volle Wahlmöglichkeit. Es müsste jeder die Möglichkeit haben, nur Teile seines Telefonbuches zu teilen oder nur seinen ungefähren Aufenthaltsort bekannt zu geben. Ich wäre eher bereit, zu teilen, in welchem Bezirk ich mich gerade aufhalte, als den exakten Aufenthaltsort", meint Lohninger. „Man muss den Nutzern mehr Kontrolle geben als sie bisher bekommen."

Cloud-Speicher

Das betrifft etwa auch die Auswahl des Cloud-Speichers, nennt Lohninger ein Beispiel. „Hier verlieren viele Menschen die Hoheit über ihre Daten. Sie werden gezwungen, beim Back-up die Cloud des Herstellers zu verwenden, wenn sie die Daten nicht mühsam über eine Verbindung mit einem PC sichern möchten." Nutzer müssten auch die Möglichkeit erhalten, ihren eigenen, privaten Cloudspeicher auszuwählen. „Damit wären die Daten auch vor Strafverfolgungsbehörden geschützt."

Freie Software

Doch fair und nachhaltig können Apps nur sein, wenn sie auf Betriebssystemen basieren, die lange Zeit unterstützt werden. „Geräte müssen möglichst langlebig sein. Das bedeutet, wenn das Handy noch funktioniert, soll es auf jeden Fall weiter betrieben werden können, auch dann, wenn der Hersteller keine Updates mehr bereitstellt. Es müsste dann vom Hersteller ermöglicht werden, das Smartphone mit freier Software weiter zu betreiben", erklärt Lohninger. Diese Sichtweise wird auch von der Free Software Foundation (FSFE) in Europa unterstützt. Epicenter.works hat alle Punkte, die im Zuge des Forschungsprojekts erarbeitet wurden, unter *www.ethicsinapps.eu* veröffentlicht.

Für Apps, die mit Steuergeld produziert werden, sollten übrigens besonders strenge Auflagen gelten. „Der Quellcode sollte bei diesen offen im Netz verfügbar sein, ansonsten verspielt man das Vertrauen der Bevölkerung", sagt Lohninger. Bei solchen Apps sollte es zudem im Vorfeld der Gestaltung partizipative Entscheidungsprozesse geben. „Denn diese Apps sollten den Bürgern dienen, und nicht dazu da sein, der Verwaltung ihre Aufgaben zu erleichtern", meint der Datenschutzexperte.

Achtung bei vorinstallierten Android-Apps

Nicht alles, was bereits beim Kauf am Handy drauf ist, ist wirklich vertrauenswürdig

VON **BARBARA WIMMER**

Sie senden Daten, haben mehr Berechtigungen als sie sollten, und verbrauchen Speicherplatz: Vorinstallierte Apps auf Android-Handys, sogenannte „Bloatware". Außerdem sind sie ein Sicherheitsrisiko. Das haben Forscher der Universität Madrid sowie der Stony Brook Universität herausgefunden, die dazu eine Studie veröffentlicht haben.

Demnach sind 91 Prozent dieser Apps nicht im offiziellen Play Store von Google zu finden und müssen auch keine Kriterien erfüllen, die zum Schutz der Nutzerdaten dienen. Google hat mit „Play Protect" nämlich ein Siegel eingeführt, mit dem Nutzer vor betrügerischen Apps besser geschützt werden sollen. Das gilt allerdings nicht für die bereits vorinstallierten Apps, wie die Forscher in ihrer Studie bestätigen. Die vorinstallierten Apps von Googles Partnerfirmen sind meistens privilegiert gegenüber denen von anderen Anbietern, die ihre Produkte über den App Store vertreiben.

So können Nutzer bei den vorinstallierten Apps meistens nicht selbst bestimmen, ob sie den Zugriff auf Mikrofon, Kamera oder den Aufenthaltsort erlauben. Nutzer wissen auch nicht, was für Daten im Hintergrund abgegriffen werden. Bei manchen dieser Apps werden Daten in Drittstaaten, etwa nach China oder die USA, übertragen.

Mehr Nutzerrechte

Die Organisation epicenter.works sowie 50 andere Initiativen (darunter Amnesty International und die Digital Rights Foundation) fordern daher, dass jeder Nutzer in der Lage sein sollte, diese Apps zu deinstallieren. „Der Großteil der Android-Nutzer hat kaum das IT-Wissen, um Bloatware selbstständig von ihrem Handy runterzubringen", sagt Petra Schmidt, Projektbeauftragte bei „Ethical Apps". Vorinstallierte Apps sollten außerdem die gleiche Prüfung unterlaufen wie Apps aus dem Play Store. Sie sollen zudem aktualisiert werden können, was derzeit nämlich oft nicht der Fall ist. Wenn App-Hersteller versuchen sollten, unkontrolliert missbräuchlich Daten abzusaugen, sollte ihnen die Zertifizierung verweigert werden.

SKYNESHER/ISTOCKPHOTO

Hersteller liefern Smartphones bereits mit einer Reihe von vorinstallierten Apps aus