Die App als Datenschutzfalle

Serie Datenschutz (Teil 4): Tipps von der Internet-Expertin Christa Rahner-Göhring zum Thema Apps

Von unserer Mitarbeiterin
Heidrun Gehrke

Waiblingen.
Apps bereichern die modern-mobile Welt: Sie erlauben uns, unterwegs Zeitung zu lesen, eine Hotelübernachtung zu buchen, den Wetterbericht oder Staunachrichten zu empfangen oder einfach eine Runde Monopoly auf dem Smartphone zu spielen. Ein paar Dinge sollten beachtet werden, um die Kontrolle über seine persönlichen Daten und die anfallenden Kosten zu behalten.

Apps sind praktisch. Aber es gilt auch bei den Anwendungen für Smartphones und Tabletcomputern der alte Grundsatz: Trau, schau, wem! Bild: Fotolia

Apps bringen Internetseiten auf Handtaschenformat. Seiten, die für große herkömmliche Bildschirme designt wurden, werden von einer App für die Darstellung auf kleinen Bildschirmen angepasst. In der Regel werden Apps vom jeweiligen Betreiber einer Plattform erstellt und angeboten (Beispiel: Facebook), aber auch jeder findige Programmierer kann eigene Apps erstellen, mit denen er Dienste anbietet und nutzbar macht. Grundsätzlich ist es so, dass der App-Betreiber die Nutzungsbedingungen für den Dienst festlegt. Im Markt der App-Möglichkeiten lassen sich praktische Anwendungen für Reisen und Ausflüge finden, wie auch Spiele, Gesundheitsratgeber oder ein Pollenflugkalender. Der App-Markt ist groß, das Angebot wächst ständig. Gerade die Möglichkeit, dass jeder, der eine gute Idee hat, diese über eine App verbreiten kann, bereichert unsere Welt mit Vielfalt und neuen Chancen - aber auch mit Missbrauchsmöglichkeiten. Um sich selbst davor zu schützen, muss man einigen Aufwand betreiben.

Ganz wichtig: Vor dem Installieren einer App sollte man sich Informationen darüber einholen, wer die App anbietet und was die App kann. Auch nachschauen, was andere Nutzer im Internet über diese App berichten. Eine Kernfrage lautet: Bietet mir diese App genau das, was ich mir vorgestellt habe, oder gibt es bessere Alternativen? Es empfiehlt sich, möglichst nur solche Apps zu wählen, die im App-Store (wie zum Beispiel GooglePlay, AppleStore) erhältlich sind - das minimiert die Risiken, sich mit der App einen Schädling (Trojaner, Virus) auf das Gerät zu laden. Einen sicheren Schutz gibt es jedoch nicht. Die Infobrokerin Christa Rahner-Göhring rät allen, die sich für eine App entschieden haben, die Nutzungsbedingungen und die Datenschutzerklärung durchzulesen - „auch wenn es viel ist“. Denn mit jeder App geht der Nutzer einen Vertrag mit einem Anbieter ein. Hierfür sollte er seine Rechte und Pflichten kennen, damit er keine bösen Überraschungen erlebt, insbesondere für den Fall einer Reklamation. Geklärt sein müssen Kosten, die Vertragsbindung, das Rückgaberecht und die Weiterverwendung der persönlichen Daten des Nutzers.

Nun zum Praktischen: Bei der Installation jeder App wird der Nutzer darauf aufmerksam gemacht, welche Rechte sich die App auf dem Gerät nehmen will. Hier muss der Nutzer entscheiden, welche Rechte er seiner App einräumen will. Das kann bis zur kompletten Freigabe aller Vorgänge auf dem Endgerät gegenüber dem App-Betreiber gehen. Wer diese Berechtigungen nicht erteilen will, kann die jeweilige App nicht verwenden. „Aus Datenschutzgründen lohnt es sich, sehr kritisch und selektiv zu entscheiden und Kompromisse nur da zu machen, wo es nicht anders geht“, empfiehlt Rahner-Göhring.

Außer der Datenschutzfalle droht auch noch eine Kostenfalle

Viele Apps fordern mehr Rechte, als für den Betrieb der App erforderlich. Schützen kann nur eine eigene kritische Haltung vor Installation der App. In geringem Umfang können auch Einstellungen am Gerät vorgenommen werden. Außer in die Datenschutzfalle kann man auch in die Kostenfalle tappen: Oft passiert es, dass in kostenlosen Apps Werbeeinblendungen zu kostenpflichtigen Angeboten führen und versehentlich gebucht werden; die Folgen werden erst aus der nächsten Monatsrechnung ersichtlich. Oder es werden innerhalb der App einzelne Zusatzangebote kostenpflichtig, sogenannte „In-App-Käufe“. Aus diesen Verträgen dann wieder herauszukommen, ist schwierig: Über den persönlichen Telefonanbieter sollte ermittelt werden können, wo der App-Vertrag gekündigt werden kann. „Da es sich sehr häufig um Firmen mit Sitz im Ausland handelt, gestaltet sich der Vorgang in der Regel höchst unerfreulich“, sagt Rahner-Göhring. Ihr Tipp: Drittanbietersperre einrichten - über eine Vereinbarung mit dem Provider.

Das ist zu beachten

- Fünf Tipps von Christa Rahner-Göhring: **Gesunden Menschenverstand** einsetzen und App-Angebote kritisch hinterfragen, bewusst entscheiden.
- Ständig die **aktuellsten Software-Versionen** für Betriebssystem und Apps nutzen; bei den Aktualisierungen auch auf mögliche Zusatzrechte achten, die gefordert werden. Notfalls: App deinstallieren.
- Nach Installation **ungewöhnliche Veränderungen** an Stromverbrauch, Datenverkehr und nicht zuletzt Rechnungen beobachten und reagieren.
- **Virenschutz und Sicherheitsmaßnahmen** für das eigene Gerät auf dem neuesten Stand halten.
- Auf Geräten für **Kinder und Jugendliche**: Drittanbietersperre einrichten, In-App-Käufe soweit möglich unterbinden; auf geeignete Apps für Kinder achten und nur diese installieren. Nicht jede App ist für Kinder und Jugendliche auch geeignet: www.klicksafe.de/themen/kommunizieren/smartphone-und-apps/apps-fuer-kinder-und-jugendliche/.
- Zwei Angebote für geprüfte und für **geeignet empfundene Apps für Kinder:** http://de.gute-apps-fuer-kinder.de oder http://schau-hin.info/handy-smartphone-tablet/klein-bunt-mobil-antworten-auf-elternfragen-zu-apps.html.