Was sollte ich beim Kauf von Apps beachten?

Autorin: Ramak Molavi

Mobile Apps machen Spaß. Sie sind in vielen Situationen nützlich: Wenn man sich in einer fremden Stadt verläuft und dank GPS-Funktion und Karte doch ans Ziel kommt; wenn man einen tollen Song hört und nicht weiß, von wem er ist. Auch sonst kann man sich mit Apps die Zeit vertreiben, beispielsweise mit Spiele-Apps, E-Books und digitalen Zeitschriften oder Musik- und Videoplayern.

Neben diesen sichtbaren haben Apps jedoch eine Reihe von nicht sichtbaren Funktionen. Je nach Programmierung und Berechtigungen gestatten sie den Entwicklern nachzuverfolgen, wie wir unser mobiles Gerät nutzen. Berechtigungen ermöglichen Apps den Zugriff auf Einstellungen und Dateien auf unserem mobilen Gerät. Die Apps können unser Surfverhalten aufzeichnen, auf unser Mikrofon zugreifen, nachverfolgen, wo wir uns aufhalten, unsere Kontaktdaten abgreifen und vieles mehr, wenn wir ihnen im Rahmen der Installation entsprechende Zugriffsrechte einräumen. Eine echte Wahl ist das aber in den seltensten Fällen: Räumt man die Zugriffsrechte nicht ein, bleibt einem normalerweise nur die App gar nicht zu installieren.

Mobile Apps sind ein Feld, auf dem viel ausprobiert wird. Zum einen testen die Entwickler aus, welche Funktionen überhaupt sinnvoll sind und von den Kunden angenommen werden. Zum anderen sind die Geschäftsmodelle dahinter oft noch in der Entwicklungsphase. Eines haben die meisten Apps gemeinsam: Sie sammeln viele Daten und können auf viele Funktionen unserer Geräte zuzugreifen, oft ohne dass Nutzer es merken.

Viele Apps brauchen aber bestimmte persönliche Daten, um zu funktionieren. Eine Taxi-App etwa benötigt unsere GPS-Koordinaten, um einen Wagen in unserer Nähe ausfindig zu machen und uns diesen vorzuschlagen. Eine Kamera-App braucht Zugriff auf die Kamera des Handys und muss in der Lage sein, Fotos in Ordner abzulegen. Auf der anderen Seite gibt es immer wieder Apps, die Zugang zum Adressbuch, zur Telefonfunktion oder anderen sensiblen Bereichen einfordern, ohne dass sie diesen Zugang für ihren Dienst wirklich brauchen.

Wie erkennt man eine unsichere App?

Leider muss man sich von dem Gedanken verabschieden, dass man jede unsichere App auf den ersten Blick erkennen kann. Zum einen liegt es daran, dass viele Prozesse, die vielleicht problematisch sind, unbemerkt im Hintergrund ablaufen. Zum anderen

kann eine zunächst sichere App durch spätere Updates unsicher werden, indem sie zum Beispiel weitere Zugriffsrechte einfordert. Nicht updaten ist aber auch keine Lösung: Denn Updates werden auch dazu genutzt, Sicherheitslücken zu schließen.

Dennoch kann man als Nutzer ein paar Vorsichtsmaßnahmen ergreifen, um möglichst keine unsicheren Apps zu installieren, die die eigenen Daten missbrauchen oder Malware oder Viren ins System einschleusen:

- **AGB und Datenschutzerklärung lesen oder zumindest überfliegen:** Die allgemeinen Geschäftsbedingungen (AGB) geben in den meisten Fällen Auskunft darüber, wie das konkrete Geschäftsmodell der Apps aussieht und ob bzw. in welchen Fällen Kosten anfallen. In der Datenschutzerklärung (die in Apps oft auch Privacy Policy genannt wird) muss jeder Anbieter auflisten, welche Daten er erhebt und was er damit macht. Ist die Datenschutzerklärung vergleichsweise kurz, so heißt es leider nicht immer, dass keine Daten erhoben werden, sondern oft nur, dass die App-Anbieter unvollständig informieren. **Das Datenschutzrecht gilt im Übrigen auch bei Anbietern aus dem Ausland!** Laut gegenwärtiger Rechtslage gilt: Hat der Anbieter seinen Sitz außerhalb der EU, bietet aber seine Dienste in Deutschland an, gilt trotzdem das deutsche Datenschutzrecht mit seinem hohen Schutzniveau. Hat der App-Anbieter allerdings zusätzlich einen Sitz in einem Land der EU, gilt das Datenschutzrecht dieses EU-Landes. Im Falle von Google und Facebook wäre das somit das Datenschutzrecht von Irland.
- **Bestenlisten/Top-Download-Listen/Bewertungen:** Bestenlisten und gute Bewertungen bei Apps können darauf hinweisen, dass die App keine gravierenden Sicherheitslücken hat und dass viele Nutzer damit gute Erfahrungen gemacht haben. Verlassen kann man sich darauf allerdings nicht. Vor allem Schwächen beim Datenschutz scheinen nicht immer dazu zu führen, dass Nutzer die Apps nicht downloaden oder sie schlecht bewerten: WhatsApp und Facebook sind aufgrund ihrer Funktionen und Leistungen regelmäßig unten den Top 5 der am meisten heruntergeladenen Apps, obwohl sie bedenklich viele Daten abgreifen, weitgehende Zugriffe auf das Gerät verlangen und fragwürdige Datenschutzbestimmungen haben.
- **Alternative App-Stores meiden:** Neben den offiziellen App-Stores, die von den großen Anbietern wie Apple (iTunes Store) und Google (Google Play) betrieben werden, gibt es vor allem für Android-Nutzer die Möglichkeit alternative Stores zu nutzen oder Apps direkt von Hersteller- oder anderen Websites herunterzuladen. Diese Apps unterliegen allerdings nicht den Kontrollen durch die Portalbetreiber, so dass die Installation hier mit größeren Risiken verbunden ist. Entsprechend empfehlen wir, nur offizielle App-Stores zu nutzen.

- **Updates installieren, aber manuell!** Regelmäßige App-Updates sind sehr wichtig, um etwaige Sicherheitslücken zu schließen. Man sollte aber auf die Einstellung „automatische Updates“ verzichten und die Updates manuell installieren. Damit kann man die Kontrolle darüber behalten, was das neue Update mit sich bringt. Besonders genau sollte geprüft werden, ob weitere Berechtigungen notwendig werden und ob diese durch neue Funktionen begründet sind. Im Zweifel kann man das Update entweder abbrechen oder die App deinstallieren.
- **Sicherheits-/Virenschutz-App installieren:** Viren gibt es nicht nur für PCs, sondern auch für mobile Geräte – Tendenz steigend. Die Malwareerkennung und -behandlung ist das wichtigste Kriterium für eine gute Security-App. Aber weitere Sicherheitsfunktionen, wie etwa Diebstahlsicherung, Verschlüsselung, Kindersicherung und Backup-Funktionen, können interessant sein.
  - **Für Android:** Offene Systeme wie Android sind sehr anfällig für Viren. Entsprechend sollte man auf Android-Geräten immer eine Virenschutz-App installieren. Hier gibt es auch kostenlose Angebote, die gut getestet worden sind (siehe zum Beispiel: www.av-test.org/de/antivirus/mobilgeraete).
  - **Für iOS/Apple:** Die Installation von Apps außerhalb des offiziellen App-Stores ist bei iOS normalerweise nicht möglich. Aufgrund dieses geschlossenen Systems ist man bei iOS vor Viren und Malware relativ gut geschützt. Wichtig ist dabei, das System aktuell zu halten, damit mögliche Sicherheitslücken schnell geschlossen werden. Man kann diese Nutzungsbeschränkungen mit einem sogenannten Jailbreak entfernen. Dabei verliert man aber die Garantie auf das Gerät (wenn man sie noch hat). In diesem Fall ist es zu empfehlen, sich zum Schutz gegen Viren auch bei Apple Geräten eine Virenschutz-App zu installieren.
- **Im Zweifel nicht installieren!** Kommt einem eine App nicht vertrauenswürdig vor – zum Beispiel, weil sie schlechte Bewertungen hat, unbegründete Berechtigungen einfordert, sehr viel Werbung enthält oder in Onlinemagazinen oder der Fachpresse schlecht besprochen wurde – so sollte man von der Installation absehen. Ab und zu sollte man sein Gerät aufräumen und nichtgenutzte Apps entfernen.

Wie schützt man sich vor unbeabsichtigtem Datenzugriff und unnötigen Berechtigungen?

In der Datenschutzerklärung, der App-Beschreibung, beim Download oder bei der ersten Verwendung (je nach Betriebssystem) wird angezeigt, welche Zugriffsberechtigungen die App fordert. Es handelt sich dabei zum Beispiel um die Erlaubnis, auf die Kontaktdaten zuzugreifen, aber auch auf andere Daten oder Funktionalitäten des mobilen Geräts (auf Ordner, die Fotos enthalten; auf Standort-Daten (GPS etc.); auf die Kamera, das Mikrofon usw.). Diese Zugriffsberechtigungen sollte man sehr genau studieren,

prüfen, ob sie für die Funktionen der App notwendig sind und dann entscheiden, ob man die Apps trotz der Forderungen installieren möchte. Ist die App schon installiert, sollte man überlegen, ob man sie bei unnötigen Erweiterungen nicht lieber löscht.

Es gibt zwar Möglichkeiten durch Apps wie „App Guard“ für das Betriebssystem Android einzelne Berechtigungen von Apps teilweise einzuschränken, doch ist dies etwas mühsam und kann dazu führen, dass die App nicht mehr richtig funktioniert. Bei iOS kann man einige Zugriffe im Betriebssystem beschränken.

Allgemein gilt bei Apps und Smartphones: Versuchen Sie nur die persönlichen Daten preiszugeben, die unbedingt nötig sind. So können Sie zum Beispiel GPS ausgeschaltet lassen, wenn Sie gerade keine App nutzen, die GPS benötigt.

Wie finanzieren sich Apps und was bedeutet das für den Schutz der persönlichen Daten?
Apps sind ausgeklügelte Software. Ihre Entwicklung und regelmäßige Aktualisierung kosten Zeit und Geld, die Vermarktung ebenfalls. Apps, die man kostenlos herunterladen und nutzen kann, müssen sich anders finanzieren. Letztendlich kostet eine App immer etwas: Wenn es nicht Geld ist, zahlt man im Zweifel mit seinen Daten.

Folgende Geschäftsmodelle sind derzeit gängig:

1. Bezahl-Apps
Bei Bezahl-Apps muss man vor dem Download einen bestimmten Betrag bezahlen und kann die App dann ohne Einschränkung nutzen. Allerdings gibt es Apps mit diesem Geschäftsmodell immer seltener. Sie machen heute nur noch maximal 10 Prozent der App-Umsätze aus. In einigen Fällen kann es sein, dass man für eine aktualisierte Version – vor allem, wenn sie für ein neues Betriebssystem angepasst wurde – noch einmal bezahlen muss.

2. Free Apps
Viele App-Anbieter möchten zunächst eine möglichst große Nutzerzahl an sich binden und veröffentlichen Apps zunächst kostenlos. Ist der Dienst so beliebt, dass viele Menschen ihn nutzen, wird er interessant für Werbekunden. Es werden dann kleine – in den meisten Fällen personalisierte (also an den Interessen des Nutzers ausgerichtete) Werbebanner geschaltet. Wenn ein Nutzer auf diese klickt, dann zahlt der Werbende einen kleinen Betrag an den App-Betreiber. Durch die Entstehung von sogenannten „Ad Networks“ wie zum Beispiel Google AdMob, Microsoft Advertising oder Apple iAd ist die Integration von Werbung in das System relativ einfach geworden.

Eine zunächst kostenlose App kann auch zur Bezahl-App werden, so wie etwa bei WhatsApp geschehen. Nachdem sich die Chat-App ausreichend verbreitet und Nutzer an sich gebunden hatte, wurde sie kostenpflichtig angeboten.

3. Freemium oder Free-to-Play (Free2Play)
Auch bei diesem Geschäftsmodell kann die App kostenlos heruntergeladen und installiert werden. Sie kann dann in einer Basisvariante oder für eine bestimmte Zeit genutzt werden. Für neue Spiellevel, besondere Ausrüstungsgegenstände oder für mehr Funktionalitäten haben Nutzer die Möglichkeit innerhalb der App Käufe durch Micropayments vorzunehmen (sogenannte In-App-Käufe) oder die Vollversion der App zu kaufen.

Je nach Nutzung können bei Freemium oder Free2Play also Kosten anfallen. Aus diesem Grund sind Anbieter daher neuerdings dazu verpflichtet, vor dem Download der App darüber zu informieren, dass In-App-Käufe möglich sind (etwa: „Diese App kann kostenlos heruntergeladen werden. Es gibt die Möglichkeit von In-App-Käufen von 0,99 Cent bis 4,59 EUR.“). Im Google-Play-Store werden Apps, die später In-App-Käufe anbieten, nicht mehr als „free“ bezeichnet. Auch beim Apple-App-Store kann man schon in der Beschreibung der jeweiligen App nachlesen, welche Kaufmöglichkeiten es gibt. Diese Transparenzregeln zu In-App-Käufen sind insbesondere zum Schutz von Kindern und Jugendlichen (beziehungsweise deren Eltern) eingeführt worden.

Free-to-Play-Apps können vor allem jüngere Nutzer dazu verleiten, regelmäßig kleinere Beträge auszugeben. So kann schnell die Übersicht verloren gehen, wie viel Geld man ausgegeben hat. Um die Ausgaben besser zu kontrollieren, kann man zum Beispiel nur Prepaid-Gutscheine nutzen – und keine Konto- oder Kreditkartennummer in den Shops speichern. Zusätzlich können Eltern In-App-Käufe mit einem Passwort schützen oder – je nach Betriebssystem – vollständig deaktivieren.

Welche Formen von Abzocke in Apps sind bekannt und wie kann man sich davor schützen?

Abofallen & WAP-Billing
Auch wenn die Apps von den Store-Betreibern überprüft werden: Die Werbung in den Apps wird es normalerweise nicht. In den Werbebannern können sich bei unseriösen Anbietern klickbare Bereiche verstecken, die man auf den ersten Blick nicht sieht. Klickt man aus Versehen auf diese Bereiche, so bestätigt man unbewusst einen Kauf

oder einen Abo-Vertrag über eine bestimmte Dienstleistung. Dieser Prozess läuft unbemerkt im Hintergrund.

Diese Verträge sind zwar rechtlich gesehen in den meisten Fällen nicht gültig. Das Problem ist aber die Zahlungsabwicklung, denn Nutzer haben nicht die Möglichkeit, die Abo-Falle samt Zahlungsaufforderung zu ignorieren. Die Zahlung erfolgt nämlich automatisch über die Handy-Rechnung.

Technisch funktioniert das so, dass beim Aufruf einer solchen Seite die individuelle Nummer der SIM-Karte im Mobiltelefon des Nutzers an den Betreiber der Werbeseite übermittelt wird. Er kann diese Nummer (MSISDN = Mobile Subscriber Integrated Services Digital Network Number) an den Mobilfunkbetreiber des Nutzers schicken und erhält sofort die Mobilfunknummer des Nutzers übermittelt. Daraufhin lässt er den Betrag auf die monatliche Handyrechnung setzen.

Schützen kann man sich davor, indem man bei seinem Mobilfunkbetreiber eine sogenannte Drittanbietersperre einrichtet. Damit können die unseriösen Anbieter keine Zahlungen über die Handyrechnung vornehmen. Der Mobilfunkanbieter O2 geht einen anderen Weg: Hier kann man zwar keine Sperre beantragen, aber der Kunde muss die Bestellung eines Mehrwertdienstes ausdrücklich bestätigen, bevor ihm der Service zum Download zur Verfügung gestellt wird.

Weiterführende Links:

- klicksafe-Bereich zu Apps (www.klicksafe.de/apps) und Smartphones (www.klicksafe.de/smartphones)
- Infos zu Apps und Berechtigungen beim Handysektor: http://handysektor.de/apps-upps.html
- Infos zu Abos und Abzocke: http://handysektor.de/abo-abzocke.html
- Elternratgeber „Smart mobil?!“ von klicksafe und Handysektor: www.klicksafe.de/materialien
- Infos zu Smartphones für Eltern beim Internet-ABC: www.internet-abc.de/eltern/kinder-smartphone.php