Übergriffig

Manche Smartphone-Apps verlangen scheinbar grenzenlosen Datenzugriff. Mit den aktuellen Betriebssystemen kann man dem gegensteuern.

iPhone-Nutzer haben es besser – und ebenso Besitzer eines Smartphones mit Version 6 des Android-Betriebssystems. Mit dieser wurde nämlich eingeführt, was bei Apple schon seit Jahren selbstverständlich ist: die einfache und von den Herstellern offiziell zugelassene Möglichkeit zur Kontrolle und Beschränkung der Zugriffsberechtigungen von Apps.

Wer nicht akzeptieren mochte, dass zum Beispiel eine Kalender-App oder die Fahrplanauskunft der ÖBB (Scotty) die gespeicherten Kontakte und die aktuellen Positionsdaten abrufen müssen, hatte unter Android bisher nur zwei Möglichkeiten: mit sogenanntem Root in die Gerätesoftware einzugreifen und den Verlust der Herstellergarantie in Kauf zu nehmen oder vollständig auf die Nutzung der entsprechenden App zu verzichten. Dabei war es nicht etwa so, dass es technische Hindernisse gegeben hätte. Eine vor Jahren verfügbare App, welche den Nutzern den erwünschten Zugriff gestattete, wurde – weil von Google nicht gewollt – rasch wieder aus dem Play Store entfernt.

Der Komfort leidet

Tatsache ist jedenfalls, dass viele Apps auch mit eingeschränkten Berechtigungen funktionieren, nur eben nicht so komfortabel. Leider erschließen sich Sinn und Notwendigkeit von Berechtigungen dem Nutzer oft nicht ohne nähere Erklärung (siehe auch Kasten „Datenspion Scotty?"). Wenn Scotty den aktuellen Standort oder die gespeicherte Wohnadresse eines Kontaktes nicht abfragen darf, dann muss man Ausgangs- und Endpunkt der Fahrt eben händisch eintippen. Und ähnlich verhält es sich mit den Termineinträgen im Kalender. Mehr steckt – zumindest bei seriösen Anbietern – nicht dahinter.

Die eventuell nicht ganz so seriösen, aber auch jene, die auf externe Finanzierungsmodelle für ihre kostenlosen Angebote angewiesen sind, sammeln (anonymisierte) Daten zur Erstellung von Nutzerprofilen, die sie gewinnbringend an die Werbeindustrie verkaufen. In der Regel machen sie aber keinen Hehl daraus, sondern schreiben es in ihre Nutzungsbedingungen. Sie tun damit nichts anderes als Google, Apple, Facebook oder die Anbieter von kostenlosem Virenschutz. Daten sind die eigentliche Währung des Internets. Wer ein Smartphone verwendet, hat seinen Anteil ohnehin schon auf den Markt geworfen; und wer Apps von Drittanbietern installiert, muss diesen wohl oder übel ein gewisses Grundvertrauen entgegenbringen. Mit einem aktuellen Smartphone-Betriebssystem kann man zumindest bei den App-Berechtigungen ein wenig steuernd eingreifen.

Automatisch und manuell

Bei Apps, die für Android 6.0 und höher entwickelt wurden, sowie bei iOS-Apps kann man bei der ersten Verwendung Berechtigungen erteilen oder verweigern. Ein entsprechendes Fenster wird eingeblendet. Von dieser automatischen Abfrage abgesehen, gibt es auch den (nachträglichen) Weg über die Einstellungen des Smartphones. Android 6: »Einstellungen/Apps bzw. Anwendungsmanager« und dann zum Aufrufen aller Apps »(Zahnradsymbol)/App-Berechtigungen« bzw. zur gezielten Kontrolle einer einzelnen App »(App-Name)/Berechtigungen« ; iOS: »Einstellungen/Datenschutz«. Das ist nicht nur zwecks Übersicht wichtig, sondern auch deshalb, weil eine im ersten Impuls nicht gewährte Berechtigung möglicherweise dazu führen kann, dass eine App nicht funktioniert.

Das Aktivieren und Deaktivieren von Berechtigungen erfolgt bei beiden Betriebs-

Grafik: Alhovik / Shutterstock.com Montage: Doris Seyser

Datenspion Scotty?

Aufmerksame Nutzer hinterfragten von Beginn an die von der Fahrplanauskunfts-App Scotty eingeforderten Berechtigungen. Daraufhin veröffentlichten die ÖBB zur Klarstellung nachstehende Informationen auf ihrer Website (Stand: Mai 2016). Leider sind solche ausführlichen Erklärungen, die viele offene Fragen beseitigen, die Ausnahme und üblicherweise auch nicht im jeweiligen App-Store zugänglich. Der Originalwortlaut:

„Kontaktdaten: Diese werden nur dazu verwendet, um Ihnen die Verkehrsbindung zu oder von einem Kontakt aus Ihrem Adressbuch anzuzeigen. Es werden nur Orte, Straßen und Hausnummern übertragen. Diese Daten werden durch uns nicht gespeichert (auch nicht zwischengespeichert).

Positions- bzw. Standortdaten: Nur wenn Sie das möchten, kann zur optimalen Verbindungssuche durch SCOTTY mobil Ihr aktueller Standort ermittelt werden, um von dort Reiseverbindungen zu suchen oder Stationen in der Nähe zu finden. Auch hier findet keine Zwischenspeicherung statt, somit ist auch die Erstellung von Bewegungsprofilen o.ä. nicht möglich.

Bewegungs- und Richtungssensor, Kompassfunktion: Diese Funktionalität erleichtert die Suche von Stationen in der Nähe. Diese Daten werden durch uns nicht gespeichert (auch nicht zwischengespeichert).

Kalender: SCOTTY mobil bietet Ihnen das zusätzliche Service, die Reisedaten zu Ihrer Verbindung in den Kalender Ihres Geräts zu speichern. Dieses Service ist nicht verpflichtend, sondern steht in Ihrem persönlichen Belieben. Je nach Betriebssystem beziehen sich auch die verwandten Sicherheitshinweise ‚Kalendertermine sowie vertrauliche Informationen lesen' bzw. ‚Ohne Wissen der Eigentümer Kalendertermine hinzufügen oder ändern und E-Mails an Gäste senden' auf diese Funktion. Die eigentlichen Inhalte der Kalender werden jedoch nicht gelesen.

USB-Speicherinhalte ändern oder löschen: Dieser Zugriff ist nur erforderlich, falls Sie SCOTTY mobil auf der SD-Karte speichern möchten.

Verknüpfungen installieren: Diese Berechtigung ist zum Erstellen von Shortcuts für Verbindungen und Abfahrtstafeln erforderlich.

Anrufliste lesen: Diese Berechtigung wird standardmäßig vom Betriebssystem Android angefordert, wenn Adressdaten aus den Kontakten gelesen werden können. Die Informationen der Anrufliste werden jedoch von SCOTTY mobil nicht gelesen.

Foto-, Musik- und Videobibliotheken: Diese Berechtigung wird aus technischen Gründen zum Erstellen der Live-Kachel-Grafiken (Karten) benötigt. Es werden keine privaten Daten ausgelesen und auch keine Daten geschrieben, die für andere Apps sichtbar wären.

Kamera: Fotos und Videos aufnehmen: Diese Berechtigung wird benötigt um Augmented Reality zu nutzen. Es werden keine Fotos oder Videos gespeichert.

Benachrichtigungen: Diese Berechtigung wird künftig zum Empfangen und Anzeigen von Push-Nachrichten (z.B. Verspätungsinformationen) benötigt, steht jedoch derzeit noch nicht zur Verfügung. Eine Speicherung der Daten wird aber auch mit dieser zukünftigen Funktion nicht erfolgen."

Fazit: Scotty kann unserer Meinung nach nicht wirklich als Datenspion bezeichnet werden, da gibt es andere Kaliber. So etwa den Facebook-Messenger oder WhatsApp, das ja gleichfalls zu Facebook gehört. Hier ist zwingend der Zugriff auf die Kontakte erforderlich. Aber wer würde schon daran zweifeln, wenn Mister Zuckerberg betont, dass lediglich die eingetragenen Telefonnummern genutzt werden?

systemen über die virtuellen Ein-/Aus-Schalter am Display; sie ermöglichen die einfachste und effizienteste Methode, um festzustellen, welche Berechtigungen mindestens notwendig sind: Versuch und Irrtum. Unter diesen unbedingt erforderlichen Berechtigungen können natürlich noch immer welche sein, die bei manchen Nutzern Unbehagen hervorrufen. Womit wir wieder beim Grundvertrauen wären – die einzige Alternative ist nämlich das Deinstallieren der App.

Randthema Hintergrunddaten

Ruft man unter Android die Apps wie beschrieben einzeln auf oder geht man in den iOS-Einstellungen zu »Allgemein«, dann findet man dort die »Hintergrunddaten« bzw. »Hintergrundaktualisierung«. Dies ist gleichfalls eine Berechtigung, die man gewähren oder entziehen kann, doch bringt sie nur bedingt Vorteile hinsichtlich des Datenschutzes. Die Hintergrundaktualisierung erlaubt es einer App, weiterzulaufen (z.B. Navigation), auch wenn sie geschlossen ist, oder Daten abzufragen (E-Mails, Chat-Nachrichten, Wetter, Börsenkurse, Aktualisierungen bei geräteübergreifend synchronisierten Apps etc.). Das ist einerseits praktisch, andererseits verbraucht es Strom und mobiles Datenvolumen. Ein Nebenaspekt ist, dass über die in regelmäßigen Abständen gelieferten Mobilfunkdaten auch der ungefähre Aufenthaltsort auslesbar ist, selbst wenn der Standort bzw. die Ortungsdienste via GPS blockiert wurden und die App geschlossen ist. Aber wer ein Smartphone verwendet, hat wie gesagt seine Daten ohnehin schon auf den Markt geworfen und kann nur noch ein wenig deren Umfang regulieren.

Rat und Hilfe für Verbraucher in Europa ECC-Net

Finanziell unterstützt durch die Europäische Union

Dieser Artikel entstand im Rahmen der „Action 670702 – ECC-NET AT FPA", für welche das Europäische Verbraucherzentrum Österreich Förderungen aus den Mitteln des Verbraucherprogramms der Europäischen Union (2014–2020) erhält.

Mehr zum Thema

Bisher in KONSUMENT erschienen:

Browser	1/16
Browser-Eweiterungen	3/16
Flash-Cookies und Skripte	4/16
E-Mails	5/16
Opera und Thunderbird	6/16