Eine Analyse der **iOS-App-Berechtigungen**

Mobile Apps brauchen Daten, um zu funktionieren. Aus diesem Grund verlangen App-Entwickler unterschiedliche Zugriffsrechte auf die Informationen auf Ihrem Mobilgerät. In der Regel geht es darum, die Funktionalität zu verbessern, aber gelegentlich fehlt es an einer angemessenen Rechtfertigung.

App-Entwickler*innen können aus verschiedenen Gründen einen übermäßigen Zugriff auf personenbezogene Daten verlangen, z. B. um schlampigen Code zu entwickeln, Ihr Erlebnis innerhalb der App oder app-übergreifend anzupassen, Sie zu Geld zu machen, legitime Funktionen bereitzustellen oder für schändliche Zwecke (z. B. um Daten zu stehlen und ohne Ihr Wissen weiterzuverkaufen).

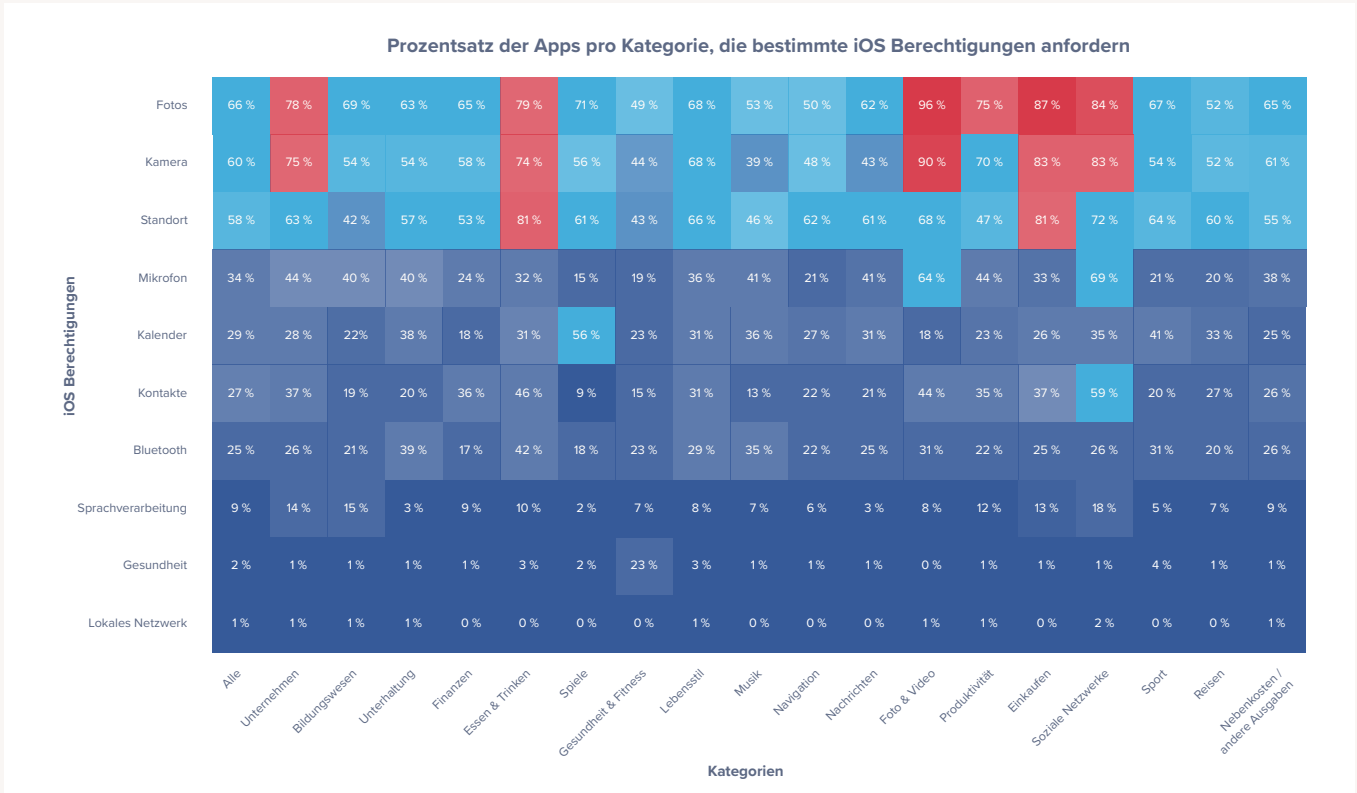
Apple und Google – die die weltweit größten mobilen App-Ökosysteme für iOS und Android betreiben - sind gegen übermäßige Datenerfassung vorgegangen. Diese beiden großen Plattformen setzen Standards durch, die App-Entwickler erfüllen müssen, um in ihren jeweiligen App-Stores aufgenommen zu werden, und sie legen die Messlatte für die Transparenz von App-Berechtigungen immer höher. Apple hat den Schutz der Privatsphäre der Nutzer sogar zum Thema einer aktuellen **Werbekampagne gemacht.**

Aber die Verantwortung für den richtigen Umgang mit Daten kann nicht allein bei Apple und Google liegen. Entwickler*innen müssen ihre Datenerfassungspraktiken überprüfen, um die möglichen Auswirkungen auf die Privatsphäre zu minimieren und gleichzeitig die Funktionalität ihrer Anwendungen aufrechtzuerhalten. Andererseits müssen sich die Verbraucher darüber im Klaren sein, dass sie mit den Informationen, die ihnen auf ihren Geräten zur Verfügung stehen, und den Kontrollmöglichkeiten, die sie zur Steuerung der Datenerfassung bieten, ihre Privatsphäre aufgeben.

Unsere Analyse der iOS-App-Berechtigungen

Um die Verwendung von App-Berechtigungen und die Informationen, die App-Entwickler zu sammeln versuchen, besser zu verstehen, haben wir die Metadaten in einer Stichprobe von fast 100.000 beliebten Apps im App Store-Katalog untersucht. Diese Stichprobe wurde anhand der Apps ermittelt, die auf den 2,5 Millionen verwalteten Geräten der Wandera-Kunden installiert sind. Wir haben die Millionen von Apps im App Store nicht berücksichtigt, die keine breite Akzeptanz gefunden haben. Diese Analyse wurde im zweiten Quartal 2021 durchgeführt.
Die in dieser Untersuchung analysierten Metadaten stammen aus zusammengefassten Protokollen, die keine persönlichen oder organisationsbezogenen Informationen enthalten.

Damit unsere Analyse aussagekräftiger ist, haben wir die Apps nach ihren App-Store-Kategorien gruppiert, sodass die Leser sehen können, wie logische Gruppen von Apps innerhalb ihrer Vergleichsgruppe gestaltet sind.



Die vier wichtigsten Genehmigungen

Unsere Analyse zeigt, dass der am häufigsten angefragte Datentyp Fotos sind, wobei mindestens die Hälfte der Anwendungen in jeder Kategorie Zugriff auf Fotos anfordert.

Die wichtigsten Kategorien von Anwendungen, die Zugriff auf die Fotobibliothek verlangen, sind:

1. Foto & Video (96%). Zu dieser Kategorie gehören Apps wie YouTube, FaceApp und Splice.
2. Einkaufen (87%). Zu dieser Kategorie gehören Apps wie Amazon, Shop und eBay.
3. Soziale Netzwerke (84%). Zu dieser Kategorie gehören Apps wie Facebook, Instagram und Twitter.

Fotos

In der Vergangenheit war der Zugang zu Fotobibliotheken entweder ganz oder gar nicht möglich. Wenn ein Nutzer beispielsweise einen Screenshot auf Twitter hochladen möchte, muss er Twitter Zugriff auf jahrzehntelange Fotos in seiner Bibliothek gewähren. Es ist nichts Ruchloses daran, dass eine Social-Media-App Zugriff auf die Fotobibliothek benötigt, aber diese Zugriffsebene ist übertrieben und könnte die Benutzer in Gefahr bringen, wenn sie mit einer schlecht entwickelten App gepaart ist. Mit iOS 14 hat Apple **mehr Kontrolle über die Fotoberechtigungen für die Verbraucher** eingeführt. Wenn eine App nun die Fotobibliothek benötigt, muss sie den Benutzer*innen die Wahl lassen, ob sie den Zugriff auf ausgewählte Fotos oder auf die gesamte Bibliothek zulassen.

Die Kamera ist die am zweithäufigsten beantragte Erlaubnis.

Die wichtigsten Kategorien von Apps, die Zugriff auf die Kamera verlangen, sind:

1. Foto und Video (90%)
2. Shopping gleichauf mit Social Networking (83 %)
3. Unternehmen (75%). Zu dieser Kategorie gehören Apps wie Zoom, Slack und WebEx.

Kamera

Die Kamera ist zwar eine weit verbreitete Erlaubnis, aber auch eine sehr riskante. Mit Zugriff auf die Kamera kann ein böser Akteur Benutzer*innen ausspionieren. Dies ist der Grund, warum streng geheime Organisationen keine Telefone mit Kameras in ihren Einrichtungen zulassen und warum einige Hersteller den Kamerazugriff deaktivieren oder ihn aus der Hardware entfernen, die sie an diese Organisationen verkaufen.

In einer **Klage aus dem Jahr 2020** wurde Instagram beschuldigt, die Kameraerlaubnis zu missbrauchen, um Benutzer*innen auszuspionieren, wenn sie die App geöffnet hatten, aber nicht mit der Kamera-Funktion interagierten. Instagram behauptet, dass es sich um einen Fehler handelte und dass keine Inhalte aufgezeichnet wurden.

An dritter Stelle der Liste der am häufigsten angeforderten Genehmigungen steht der Standort.

Die wichtigsten Kategorien von Apps, die Standortinformationen anfordern, sind:

1. Einkaufen, gleichauf mit Essen und Trinken (81%). Die Kategorie Essen & Trinken umfasst Apps wie DoorDash, UberEats und Yelp.
2. Soziale Netzwerke (72%)
3. Foto & Video (68%).

Standort

Im Jahr 2019 haben sowohl Apple als auch Google eine zusätzliche Ebene für die Wahl des Standorts durch die Verbraucher eingeführt. Vor iOS 13 gab es zwei Berechtigungen für den Standort: Bei Verwendung (im Vordergrund) und immer (im Hintergrund). Mit iOS 13 wurde die Funktion **Einmal zulassen** eingeführt, die als temporäre Autorisierung gilt.

Auch vor Android 10 hatten die Benutzer*innen zwei Möglichkeiten: Zulassen oder Verweigern. Früher bedeutete dies, **dass der Standort jederzeit** (im Vordergrund und im Hintergrund) abgerufen werden konnte, ohne dass es ein Dazwischen gab. Mit Android 10 wurde jedoch eine dreistufige Standortberechtigung eingeführt, sodass die Benutzer die Option "nur zulassen, wenn die App in Gebrauch ist" auswählen konnten.

Erfahren Sie mehr über den Missbrauch von Standortdaten in **dieser Untersuchung der New York Times**

Die viertbeliebteste App-Anfrage ist das Mikrofon.

Die wichtigsten Kategorien von Apps, die Zugriff auf das Mikrofon verlangen, sind:

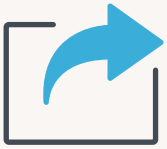
1. Soziale Netzwerke (69%)
2. Foto und Video (64%)
3. Unternehmen, gleichauf mit der Produktivität (41%) an dritter Stelle. Die Kategorie „Produktivität“ umfasst Anwendungen wie Asana, Google Calendar und TimeTree.

Mikrofon

Genau wie die Kamera kann auch der Zugriff auf Mikrofon-Apps in den falschen Händen schwerwiegende Folgen haben. Mit der Fähigkeit, das Mikrofon zu aktivieren, können Apps private Gespräche aufzeichnen und weiterleiten oder **hören, was um Sie herum vor** sich geht, um diese Informationen an Organisationen zu verkaufen. Und wenn die Erlaubnis missbraucht wurde, konnten Apps dies ohne das Wissen der Benutzer*innen tun.

Mit iOS 14 hat Apple jedoch den orangefarbenen Punkt eingeführt, der anzeigt, wenn das Mikrofon von einer App verwendet wird. So können Verbraucher leichter erkennen, ob etwas faul ist.

App-übergreifender Daten-Austausch



Der Informationsaustausch findet zu einem großen Teil außerhalb der oben genannten ausdrücklichen Genehmigungen statt. Die App-Sandbox soll verhindern, dass Apps untereinander Daten austauschen, aber verschiedene Tracking-Ansätze umgehen dies. Auch wenn die Apps nicht direkt miteinander kommunizieren, kann sich ein Werbetreibender durch die Verbindung verschiedener Backend-Dienste und Web-Interaktionen ein genaues Bild von einem Nutzer auf der Grundlage seines Online-Verhaltens machen. Hier sind einige Beispiele für die gemeinsame Nutzung von Informationen über Apps hinweg, die nicht unter die oben genannten Berechtigungen fallen:

Der Informationsaustausch von Händen (oder Apps) erfolgt über Werbekennungen, die Informationen über das Nutzerverhalten zu Werbezwecken verfolgen und weitergeben, was dem Durchschnittsnutzer wahrscheinlich nie bewusst wird. Dieser app-übergreifende Informationsaustausch zu Werbezwecken ist der Grund dafür, dass Sie, nachdem Sie bei Google nach „Sauerteig“ gesucht haben, in Ihrem Instagram-Feed plötzlich Werbung für Brotbackgeräte sehen. Kürzlich erhielten die Nutzer von Apple Geräten mehr Kontrolle über ihre Privatsphäre, als Apple mit iOS 14.5 die neue Funktion „App-Tracking-Transparenz“ veröffentlichte. Jetzt müssen App-Entwickler fragen, ob sie Ihre Aktivitäten über die Apps und Websites anderer Unternehmen hinweg verfolgen können. Hinweis: Unsere Analyse der Berechtigungen umfasst diese Berechtigung noch nicht, da sie neu ist.

Das nächste Beispiel betrifft die Fotobibliothek. Apps, die auf die Fotobibliothek zugreifen, können auch auf die in den Fotos eingebetteten GPS-Daten zugreifen, sodass Unbefugte herausfinden können, wo eine Person wann gewesen ist — und sogar, wo sie lebt und arbeitet. Standort-Daten werden nur an Fotos angehängt, wenn GPS für die Kamera aktiviert ist. Wenn Sie jedoch die GPS-Daten für die Kamera deaktivieren, verlieren Sie einige der Vorteile, die sie in der Fotobibliothek bieten. **Hier finden Sie Informationen darüber, wie Sie die Weitergabe von Standortdaten vermeiden können, wenn Sie Fotosversenden**.

Ein Fall von Datenmissbrauch kam 2020 ans Licht, als LinkedIn und TikTok beschuldigt wurden, den Inhalt der **Zwischenablage** von iOS-Nutzern zu kopieren. Das Problem wurde in der Beta-Version von iOS 14 entdeckt, als Apple eine neue Datenschutzfunktion hinzufügte, die ein kurzes Popup-Fenster anzeigte, das die Nutzer darüber informierte, dass eine App Inhalte aus der Zwischenablage gelesen hatte. Auf den ersten Blick mag dies nicht von Bedeutung sein, aber es ist nicht ungewöhnlich, dass Menschen einen Passwortmanager verwenden und die Anmeldedaten aus dem Passwortmanager in eine Website oder Anwendung kopieren.

Die wichtigsten Erkenntnisse

Trotz der Verbesserungen, die sowohl Apple als auch Google bei der Förderung des Datenschutzes vorgenommen haben, müssen die Verbraucher selbst Maßnahmen zum Schutz ihrer Daten ergreifen. Ziel dieser Untersuchung ist es, die Nutzer*innen zu ermutigen, über die Daten, die sie weitergeben, nachzudenken, bevor sie eine auf ihren Geräten erscheinende Anfrage akzeptieren. Es gibt einige Daten in dieser Analyse, die nicht überraschend sind, und einige, die es sind.

Die Mehrheit (62%) der Navigationsanwendungen verlangt beispielsweise Zugriff auf Ihren Standort. Es macht Sinn, Sie auf einer Karte zu platzieren, aber warum verlangt fast die Hälfte von ihnen (48 %) auch Zugang zu Ihrer Kamera? Das Gleiche gilt für die 83% der Shopping-Apps, die Zugriff auf Ihre Kamera verlangen. Für das Scannen von QR-Codes ist das sinnvoll, aber warum verlangen so viele (87%) auch Zugang zu Ihrer Fotobibliothek? Es lohnt sich, darüber nachzudenken, welche Funktionen eine App tatsächlich haben muss, bevor sie akzeptiert wird.

Es gibt Kategorien von Apps, die mehr Bedienungshilfen benötigen als andere. Nach unserer Analyse sind dies Foto & Video, Shopping und Social Networking. Wenn Sie eine große Anzahl von Apps in diesen Kategorien haben, sollten Sie in Erwägung ziehen, alle Anwendungen zu löschen, die Sie nicht regelmäßig verwenden, um das Risiko der Datenexposition zu minimieren.

Manche Genehmigungen sind empfindlicher als andere, und dies ist von Person zu Person unterschiedlich. Vielleicht arbeiten Sie in einer Branche, in der Sie sensible Dateien in Ihrer Fotobibliothek gespeichert haben, oder Sie haben hochrangige Kontakte in Ihrer Kontaktbibliothek. Wenn dies der Fall ist, sollten Sie alle sensiblen Berechtigungen in Ihren Einstellungen überprüfen, um die Apps, die Zugriff darauf haben, zu kontrollieren, damit Sie alle entfernen können, die ein Risiko darstellen könnten.

Empfehlungen

Um das Risiko zu minimieren, dass Ihre sensiblen Daten in die Hände Unbefugter gelangen, empfehlen wir die folgenden zusätzlichen Vorsichtsmaßnahmen:

- Lesen Sie die Genehmigungen sorgfältig, wenn sie auftauchen. Fragen Sie sich: Benötigt diese App Zugriff auf die privaten Daten um zu funktionieren? Wenn z. B. eine Wetter-App Zugriff auf Ihre Kamera oder Ihre Kontaktbibliothek verlangt, sollten Sie zweimal überlegen, bevor Sie zustimmen, und nicht zögern, den Zugriff auf Anfragen zu verweigern, die Sie nicht verstehen oder mit denen Sie nicht einverstanden sind.
- Überprüfen Sie regelmäßig Ihre App-Berechtigungseinstellungen, um zu sehen, welche Apps auf was auf Ihrem Gerät zugreifen. Worauf Sie achten sollten: (1) Apps, die Sie nicht mehr verwenden (erwägen Sie, sie zu löschen, aber wenn Sie das nicht können, entfernen Sie die Erlaubnis für sensible Daten); (2) Apps, die in den Nachrichten sind (gab es einen Ausbruch von Datenschutzaktivitäten?).
- Wenn es um Standort-Daten geht, erteilen Sie immer die Erlaubnis „nur während der Nutzung“— die sowohl auf iOS als auch auf Android verfügbar ist.
- Löschen Sie Anwendungen, die Sie nicht mehr verwenden, um das Risiko zu minimieren, dass in alten oder nicht mehr genutzten Anwendungen Fehler auftreten. Sowohl auf iOS als auch auf Android gibt es Funktionen, mit denen Sie nicht genutzte Apps auslagern/löschen können.

Wenn Sie in einem geschäftlichen Kontext Anwendungen für andere betreuen, sollten Sie Folgendes beachten:

- Führen Sie eine Sicherheitslösung ein, die eine App-Überprüfung bietet. Ein App-Überprüfungs-Tool kann Apps regelmäßig auf neue und aufkommende App-Schwachstellen in Ihrem mobilen Bestand überprüfen. App-Überprüfungs-Tools können auch eine umfassende Liste von Apps liefern, die in der gesamten Flotte mobiler Geräte verwendet werden, komplett mit Beliebtheitsbewertungen, Versionsangaben und zusätzlichen Metadaten. Dies sind genau die Art von Informationen, die IT-Administratoren dabei helfen zu bestimmen, welche Maßnahmen ergriffen werden müssen, um riskante, veraltete oder nicht konforme Anwendungen zu beseitigen.
- Halten Sie Ihren mobilen Besitz auf dem neuesten Stand. Da Apple und Google Verbesserungen an den Berechtigungseinstellungen vornehmen, sollten Sie sicherstellen, dass die Nutzer*innen davon profitieren. Verwenden Sie daher ein Sicherheitstool, das veraltete Betriebssystemversionen in Ihrem Mobilgerät erkennen kann.
- Stellen Sie sicher, dass Benutzer*innen ihre Geräte nicht mit Jailbreaks versehen, um Apps von Drittanbietern zu installieren. Die Apps von Drittanbietern stellen nicht nur ein Risiko dar, da sie nicht von Apple oder Google geprüft wurden, sondern das Jailbreaking eines Geräts hebt auch die in das Betriebssystem eingebauten Schutzmechanismen auf, wodurch das Gerät in einen sehr riskanten Zustand versetzt wird.

Mit dieser Analyse wollen wir keine Ängste schüren, sondern Sie und Ihre Benutzer über die verfügbaren Optionen aufklären und darüber, wie Sie alle Aspekte der Geräte-, Benutzer- und Unternehmensdaten am besten schützen können. Setzen Sie sich mit uns in Verbindung, um zu erfahren, wie Sie Schutzmaßnahmen ergreifen und Ihre Sicherheitslage verbessern können.

Wenn Sie mehr erfahren möchten, wenden Sie sich an Jamf.