Der monatliche Security Awareness Newsletter für Jedermann

OUCH!

IN DIESER AUSGABE...

Sichere Nutzung mobiler Apps

Überblick

Mobilgeräte wie Tablets, Smartphones und Smartwatches sind beruflich wie auch privat die meistgenutzten Geräte. Was sie so vielseitig macht sind die Millionen verschiedenen Apps, aus denen wir wählen können. Diese Apps ermöglichen uns einen Produktivitätsgewinn, sichern unsere Erreichbarkeit und die Möglichkeit, Inhalte mit anderen zu teilen, oder einfach mehr Spaß zu haben. Die mächtigen Fähigkeiten dieser Geräte gehen jedoch auch mit Risiken einher. Hier sind einige Schritte die Sie unternehmen können, um Apps sicher zu verwenden und den größtmöglichen Nutzen daraus zu ziehen.

Gastautor

Joshua Wright ist Technischer Direktor von Counter Hack und langjähriger Tutor für das SANS Institute. Er ist Autor der Kurse SEC575: Mobile Device Security and Ethical Hacking, und Hacking Exposed: Wireless. Sie finden Josh auf Twitter als **@joswr1ght**.

Bezugsquellen mobiler Apps

Der wichtigste Schritt besteht darin, dass man Apps nur aus sicheren, vertrauenswürdigen Quellen lädt. Cyberkriminelle haben längst ihre Fähigkeiten in der Erstellung und Verteilung manipulierter mobiler Apps perfektioniert, so dass die Apps absolut legitim erscheinen. Wenn Sie eine dieser infizierten Apps installieren, können Kriminelle die vollständige Kontrolle über Ihr Gerät übernehmen. Indem Sie Apps nur von bekannten, vertrauenswürdigen Quellen installieren, reduzieren Sie das Risiko eine infizierte App zu installieren. Die Marke Ihres Mobilgeräts spielt bei den verfügbaren Quellen für den Bezug mobiler Apps eine große Rolle.

Apple Geräte wie iPad und iPhone können Apps nur aus dem Apple App Store laden. Der Vorteil hierbei ist, dass Apple eine Sicherheitsprüfung aller Apps durchführt, bevor sie im Store verfügbar gemacht werden. Apple kann nicht alle Infektionen erkennen, aber diese starke Kontrolle über den kompletten App-Installationsprozess minimiert das Risiko für die Installation einer infizierten App signifikant. Sobald Apple nachträglich bemerkt, dass eine App infiziert ist, wird es sie sehr schnell löschen. Windows Phone nutzt einen ähnlich strikten Ansatz für das Management von Apps.

Android Mobilgeräte sind hier anders. Android gibt Ihnen mehr Flexibilität, indem es Ihnen die Möglichkeit bietet Apps aus dem ganzen Internet herunterzuladen. Mit dieser Flexibilität geht aber auch eine höhere Verantwortung für Sie

Sichere Nutzung mobiler Apps

einher. Sie müssen vorsichtiger sein, welche Apps Sie herunterladen und installieren, da nicht alle vorab überprüft werden. Google betreibt einen verwalteten Appstore ähnlich dem von Apple, genannt Google Play. Apps die Sie von Google Play laden haben zumindest einige rudimentäre Sicherheitsüberprüfungen durchlaufen. Wir empfehlen Ihnen daher, Apps für Android Geräte nur von Google Play zu laden. Vermeiden Sie das Herunterladen von anderen Webseiten, da jeder - Cyberkriminelle eingeschlossen - einfach infizierte mobile Apps erstellen und verteilen kann, und Sie dazu überlisten kann diese auf Ihrem Mobilgerät zu installieren. Als zusätzlichen Schutz sollten Sie, wenn möglich, eine Anti-Virus-App auf Ihrem Mobilgerät installieren.

Die Schlüssel zur sicheren Nutzung von mobilen Apps sind die Installation aus vertrauenswürdigen Quellen, die schnellstmögliche Aktualisierung, und die Beschränkung auf unbedingt notwendige Berechtigungen.

Unabhängig davon welches Gerät zu nutzen kann ein weiterer Schritt darin bestehen, neue, noch unbewertete und selten heruntergeladene Apps zu meiden. Je länger eine App im Appstore verfügbar war, je mehr Nutzer sie heruntergeladen und positiv bewertet haben, desto wahrscheinlicher ist, dass es sich um eine vertrauenswürdige App handelt. Installieren Sie zudem nur die Apps, die Sie auch wirklich benötigen und nutzen. Fragen Sie sich bei jeder App, ob Sie sie wirklich verwenden werden. Jede weitere App bringt nicht nur zusätzliche Verwundbarkeiten auf Ihr Mobilgerät, sondern auch neue Bedrohungen für den Datenschutz. Wenn Sie eine App nicht länger verwenden, löschen Sie sie von Ihrem Mobilgerät (Sie können sie später jederzeit wieder installieren wenn Sie sie doch wieder benötigen). Und zu guter letzt: Unterlassen Sie es, Ihr Mobilgerät einem “Jailbreak” zu unterziehen oder es zu “rooten”. Damit beschreibt man einen Vorgang, die Sicherheitsfunktionen des Geräts außer Kraft zu setzen, um nicht freigegebene Apps zu installieren oder eingebaute Funktionen zu manipulieren. Doch hiermit deaktivieren oder übergehen Sie nicht nur viele der bordeigenen Sicherheitsmaßnahmen, sondern verletzen häufig auch die Garantiebestimmungen des Geräts.

Berechtigungen

Wenn Sie eine App aus einer vertrauenswürdigen Quelle installiert haben, sollten Sie noch sicherstellen, dass diese sicher konfiguriert ist und Ihre Privatsphäre wahrt. Denken Sie nach, bevor Sie einer App Zugriff auf Ihre Daten einräumen: möchten Sie wirklich die Berechtigung erteilen, die die App erfragt? Benötigt die App die Berechtigung wirklich? Einige Apps nutzen z.B. Ortungsdienste. Wenn Sie einer App erlauben, Ihren Standort abzufragen, gestatten Sie dem Ersteller der App möglicherweise, all Ihre Bewegungen nachzuverfolgen, und diese Informationen vielleicht sogar an Dritte zu veräußern. Wenn sie die Berechtigung nicht erteilen wollen, lehnen Sie die Anfrage der App ab oder sehen Sie sich nach

Sichere Nutzung mobiler Apps

einer anderen App mit vergleichbarem Funktionsumfang um, die Ihre Anforderungen erfüllt. Bedenken Sie, dass Sie aus einer großen Fülle wählen können.

Apps aktualisieren

Mobile Apps müssen, genau wie Ihr Computer oder das Betriebssystem der Mobilgeräte, aktualisiert werden um auf dem aktuellen Stand zu bleiben. Kriminelle suchen und finden fortwährend Schwachstellen in Apps. Sie entwickeln dann Angriffe, die diese Schwachstellen ausnutzen. Die Entwickler, die Ihre App programmiert haben, erstellen und veröffentlichen aber auch regelmäßig Aktualisierungen, um die entdeckten Schwachstellen zu beheben und die Geräte abzusichern. Je häufiger Sie auf neue Aktualisierungen prüfen und diese installieren, um so besser. Die meisten Geräte ermöglichen es Ihnen, das System so einzustellen, dass Aktualisierungen für Apps automatisch eingespielt werden - wir empfehlen Ihnen, dies zu aktivieren. Wenn es keine derartige Einstellung gibt, sollten Sie mindestens alle zwei Wochen prüfen, ob Aktualisierungen für Ihre mobilen Apps herausgegeben wurden. Wurden Ihre Apps aktualisiert, prüfen Sie immer, ob sie ggf. neue, erweiterte Berechtigungen anfordern.

Weiterführende Informationen

Social Engineering:	https://securingthehuman.sans.org/ouch/2017#january2017
Entsorgung Ihres Mobilgeräts:	https://securingthehuman.sans.org/ouch/2016#december2016
Absicherung Ihres neuen Tablets:	https://securingthehuman.sans.org/ouch/2016#january2016
OUCH Archive & Übersetzungen:	https://securingthehuman.sans.org/ouch/archives
Kurs zur Mobilgerätesicherheit:	https://sans.org/sec575

Informieren Sie Sich

Abonnieren Sie den monatlichen OUCH! Security Awareness Newsletter, greifen Sie auf die OUCH! Archive zu und lernen Sie mehr über SANS Security Awareness Angebote unter securingthehuman.sans.org/ouch/archives.

Deutsche Ausgabe

Diese OUCH! Ausgabe wurde von Marek Kreul und René Wiedewilt aus dem Englischen übersetzt. Beide arbeiten für das CERT eines DAX-Konzerns und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley