Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

Die sichere Nutzung von mobilen Apps

Überblick

Mobile Geräte wie Tablets und Smartphones haben sich zu einer der am meist genutzten Technologien, sowohl in unserem Privatleben, als auch im beruflichen Umfeld entwickelt. Was die mobilen Geräte so vielseitig macht sind die Millionen von Apps, aus denen wir wählen können. Diese Apps erhöhen unsere Produktivität und erlauben uns schnelle, unkomplizierte Kommunikation, das Teilen von Inhalten, helfen bei Ausbildung und Erziehung - oder einfach dabei, mehr Spaß zu haben. Mit den vielfältigen Möglichkeiten gehen jedoch auch Risiken einher, weshalb wir nachfolgend einige Schritte vorstellen wollen, die Ihnen die sichere Nutzung Ihrer Apps ermöglichen.

Gastautor

Chris Crowley ist ein unabhängiger Berater, zertifizierter SANS Ausbilder und Kursautor. Er ist als **@CCrowMontance** auf Twitter und als **+ChrisCrowley** auf Google plus aktiv.

Bezug von Apps

Der erste und vielleicht wichtigste Schritt ist sicherzustellen, dass Sie Apps immer aus sicheren, vertrauenswürdigen Quellen beziehen. Jedermann kann heutzutage Apps erstellen, daher ist es wichtig darauf zu achten woher Sie diese beziehen. Cyberkriminelle haben ihre Fähigkeiten in der Erstellung und Verteilung infizierter Apps verfeinert, die vorgeben seriöse Apps zu sein. Wenn Sie eine dieser infizierten Apps installieren, können die Cyberkriminellen Kontrolle über Ihr Mobilgerät erlangen, inklusive Zugriff auf Ihre E-Mails, Nachrichten und Kontakte. Indem Sie Apps nur von bekannten, vertrauenswürdigen Quellen beziehen, reduzieren Sie das Risiko eine infizierte App zu installieren beträchtlich. Die je nach Gerät unterschiedlichen Optionen beschreiben wir im Folgenden.

Für Apple Geräte, wie iPad und iPhone, können Sie Apps nur aus dem von Apple verwalteten App Store beziehen. Der Vorteil hierbei ist, dass Apple eine Sicherheitsprüfung sowohl der Apps, als auch der Autoren vornimmt. Auch wenn Apple hiermit noch immer keine hundertprozentige Garantie für die Ungefährlichkeit geben kann, reduziert diese verwaltete Umgebung das Risiko eine infizierte App zu laden signifikant. Apple kann zudem Apps auch sehr schnell aus dem Store entfernen, wenn der Verdacht besteht, dass sie infiziert sind. Windows Phone nutzt einen vergleichbaren Ansatz zur Verwaltung von Apps.

Bei Android Mobilgeräten ist das Konzept ein anderes. Android gibt Ihnen mehr Flexibilität, indem Sie Apps von überall im Internet herunterladen können. Damit geht aber eine erhöhte Verantwortung für Sie einher: Sie müssen vorsichtiger sein, welche Apps Sie herunterladen und installieren, da nicht alle überprüft wurden. Google betreibt einen verwalteten

Die sichere Nutzung von mobilen Apps

App Store vergleichbar dem von Apple, den Google Play Store. Apps, die Sie von Google Play beziehen, wurden zumindest grundlegend überprüft, weshalb wir empfehlen Apps für Android Geräte nur von Google Play herunterzuladen. Meiden Sie es Apps von anderen Seiten zu beziehen, denn für Cyberkriminelle ist es sonst ein Leichtes, manipulierte bzw. infizierte Apps zu vertreiben und Sie dazu zu bringen, diese auf Ihrem Mobilgerät zu installieren. Als zusätzlichen Schutz können Sie eine Anti-Virus App auf Ihrem Mobilgerät installieren.

Der Schlüssel zur sicheren Nutzung von Apps ist die Installation aus vertrauenswürdigen Quellen, regelmäßiges Aktualisieren und Überprüfung der Berechtigungen.

Um Ihr Risiko noch weiter zu senken, sollten Sie brandneue Apps vermeiden, ebenso wie solche die erst sehr wenige Downloads verzeichnen oder nur wenige positive Kommentare vorweisen können. Je länger eine App verfügbar ist und umso mehr positive Kommentare sie bereits erhielt, um so wahrscheinlicher ist, dass es sich um eine vertrauenswürdige App handelt. Empfehlenswert ist zudem, nur die Apps zu installieren die Sie wirklich benötigen und benutzen. Fragen Sie sich immer, ob Sie eine App wirklich benötigen. Neben neuen Verwundbarkeiten bringen selbst Apps aus vertrauenswürdigen Quellen auch immer neue Privatsphärefragen mit. Wenn Sie eine App nicht länger benutzen, deinstallieren Sie sie auf Ihrem Mobilgerät - Sie können sie später leicht wieder installieren, wenn Sie sie benötigen.

Um dieses Kapitel abzuschließen, möchten wir noch auf das Thema Jailbreak bzw. rooten von mobilen Geräten eingehen. Dies bezeichnet den Prozess, gezielt bestimmte Sicherheitsfunktionen des mobilen Betriebssystems zu deaktivieren. Ziel ist meist eine Erweiterung des Funktionsumfangs des mobilen Betriebssystems bzw. die Möglichkeit zu erhalten, Apps (meist nicht für den App Store zugelassene) mit weitergehenden Möglichkeiten zu installieren. Wir raten hiervon vehement ab, da dies teils grundlegende Sicherheits- und Schutzfunktionen der Geräte außer Kraft setzt und darüber hinaus oft auch Garantien und Supportverträge beeinflusst.

Berechtigungen

Sobald Sie eine App aus einer vertrauenswürdigen Quelle installiert haben, sollten Sie die sichere Konfiguration und die Gewährleistung Ihrer Privatsphäre sicherstellen. Die Installation setzt häufig schon voraus, dass Sie einer App bestimmte Berechtigungen einräumen. Fragen Sie sich vor dem Erteilen jeder Berechtigung, ob die App diese wirklich für ihre beworbene Funktion benötigt. Einige Apps benötigen beispielsweise Geolokationsdienste. Wenn Sie einer App erlauben fortwährend Ihren Standort abzufragen, ermöglichen Sie es möglicherweise ihrem Ersteller Ihre Bewegungen nachzuverfolgen und diese Daten womöglich sogar weiterzuverkaufen. Wenn Sie die von einer App angeforderten Berechtigungen nicht erteilen wollen, sehen Sie sich im Store nach einer anderen App mit vergleichbarem Funktionsumfang um - es gibt meist mehr als

Die sichere Nutzung von mobilen Apps

genug Auswahl. Apple Geräte erlauben die Änderung einiger Berechtigungen im Systemmenü unter “Einstellungen” oder in der laufenden App, wie z.B. den Zugriff auf Standortdaten. Windows und Android Mobilgeräte nutzen hier einen anderen, “alles-oder-nichts”, Ansatz. Wenn Sie einer App nicht alle angegebenen Berechtigungen erteilen wollen, können Sie die App nicht installieren.

Aktualisierung von Apps

Apps müssen, genau wie Ihr Computer oder das Betriebssystem des Mobilgeräts, immer wieder aktualisiert werden um auf einem aktuellen Stand zu bleiben. Kriminelle suchen fortwährend nach Schwachstellen in Apps und entwickeln Angriffe die solche Schwachstellen ausnutzen. Die Entwickler Ihrer Apps erstellen und veröffentlichen jedoch auch immer wieder Aktualisierungen oder neue Versionen ihrer Apps um diese Schwachstellen zu beheben und Ihre Geräte zu schützen. Je öfter Sie auf Updates prüfen und diese installieren, desto besser. Die meisten Plattformen bieten zudem eine Möglichkeit, Apps automatisch zu aktualisieren, wozu wir Ihnen raten. Wenn das nicht möglich ist, empfehlen wir Ihnen Ihre Apps mindestens alle zwei Wochen auf Aktualisierungen zu prüfen. Stellen Sie nach jeder Aktualisierung sicher, dass sie jede neue Berechtigung, die die Apps anfordern, verstanden und mit Bedacht gewährt haben.

Weiterführende Informationen

OUCH! Social Engineering:	http://www.securingthehuman.org/ouch/2014#november2014
OUCH! Entsorgung Ihres Mobilgeräts:	http://www.securingthehuman.org/ouch/2014#june2014
OUCH! Absichern Ihres neuen Tablet-Computers:	http://www.securingthehuman.org/ouch/2013#december2013
Gängige Begriffe der IT Sicherheit:	https://www.bsi-fuer-buerger.de/BSIFB/DE/Wissenswertes_Hilfreiches/Service/Glossar/glossar_node.html
SEC575: Mobile Device Security Kurs:	http://www.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 http://www.securingthehuman.org.

Deutsche Ausgabe

OUCH! wurde aus dem Englischen übersetzt von Marek Kreul und René Wiedewilt. Beide arbeiten für das CERT eines deutschen IT-Dienstleisters 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