Apples Kampf gegen Piraten-App-Entwickler: 2FA als Heilsbringer?

Apple will seine Entwickler dazu verpflichten, eine Zwei-Faktor-Authentisierung (2FA) zu verwenden, um dem Handel mit Entwicklerzertifikaten und damit einem Einfallstor für schadhafte Apps entgegenzuwirken. Michael Veit, Security Evangelist bei Sophos, mit einem Kommentar zu dieser Vorgehensweise.

Es ist noch nicht lang her, dass sich die beiden Giganten Apple und Facebook über eine App Namens „Facebook Research“ in den Haaren lagen. Diese Applikation war nicht für den generellen Gebrauch entwickelt worden – in der Tat war es sogar so, dass Facebook die App gar nicht Jedermann zugänglich machen konnte: im App Store war sie nämlich gar nicht zugelassen, zu viel Schnüffelpotenzial. Unter anderem spähte sie in den Traffic einiger (oder aller) Netzwerke von anderen Apps – Ziel: Facebook verbessern durch tiefere Einblicke in das Onlineverhalten der Nutzer.

Hat man im Hinterkopf, dass Apps in der iPhone-Software schon verboten sind, die weitaus weniger Funktionen und Möglichkeiten haben, zeigt sich Facebooks (geschicktes) Vorgehen in diesem Fall: das Unternehmen umging diese Restriktionen, indem es die App in einer Version mit limitiertem Zugang unter Apples „Enterprise Certificate Programme“ anbot. Ein System, das Unternehmen nutzen können, um Applikationen für ihre Belegschaft zu entwickeln und zwar ohne darauf zu warten, dass Apple diese im App Store bestätigt.

„Unbekannte Quellen“ als Dauerübel
Einfach gesagt: damit kommt Apple der Google-Funktionalität in Android „Erlaube Apps von unbekannten Quellen“ schon ziemlich nahe. Und es ist der einzige Weg Software auf einem iPhone zu installieren, ohne über Los, respektive App-Store, zu gehen.

Apples Begeisterung hielt sich darüber in Grenzen. Facebook wurde gezwungen, die Research-App zurückzuziehen. Es stellte sich jedoch heraus, dass sie nicht die einzigen waren, die den Begriff „Belegschaft“ großzügig auslegten. Auch Googles „Screenwise Meter“-App umging so Apples Richtlinien. Während Facebook die „Mitarbeiter“ mit 20 US-Dollar für die Nutzung der App lockte, bezahlte Google mit Geschenkkarten. Aber es zog seine App schneller zurück, als Apple reagieren konnte. Im Ergebnis bei beiden jedoch gleich: die Anwendung steht nicht mehr zur Verfügung.

Software Piraten auf dem Vormarsch
Preisfrage: Wer hat so frei und sorglos mit den Entwickler-Zertifikaten gespielt? Software-Piraten, wie Reuters diesen Sektor an wahllosen Verkäufern nennt. Ein Haufen von „Ersatz-Zulieferern“ haben Entwicklerzertifikate verwendet, um nicht-offizielle und illegale Versionen von etablierten Apps wie Spotify, Angry Birds, Pokémon Go und Minecraft zu signieren.
Nicht offizielle Apps lassen sich derart manipulieren, wie weder Apple noch der amtliche App-Creator es zulassen würden, also zum Beispiel Werbung ausblenden, Logins Umgehen und völlig skrupelloses Betrügen in Online Games.

Wie Reuters benennt, Apple darf nicht einfach nur die missbrauchten Zertifikate löschen, sondern muss auch die schädigenden Programmierer aus seinen Entwicklerprogrammen nehmen plus Gebühren und Wartezeit bei Neubewerbung.

2FA als Pflicht für Entwickler?
Apple geht aber noch weiter: Entwickler mit entsprechendem Zertifikat werden in Zukunft eine 2FA (Zwei-Faktor-Authentifizierung) nutzen müssen, als Teil ihrer Verantwortung, die mit diesem Privileg einhergeht.

Es lässt sich vermuten, dass Apple so eine weitaus größere Kontrolle über den Missbrauch kompromittierender Entwicklerzertifikate erhält – ein Betrüger, der dann das Passwort entwendet, wird zukünftig nicht mehr genug Informationen für den Zugang zum Account zur Verfügung haben, um Apps mit einem Zertifikat zu signieren.

Die 2FA einzufordern, könnte es abtrünnigen Entwicklern ebenfalls schwieriger machen, neue Accounts anzuheizen, wenn ihre alten stillgelegt wurden. 2FA-Codes, die an das Handy gesendet werden, können an die SIM-Karte, das Gerät oder beides gebunden sein. Das macht es komplizierter, sie für neue Accounts zu registrieren, es sei denn man tauscht die Geräte aus.

2FA als Anklagepunkt
Interessanterweise ist die 2FA nicht überall beliebt. Ein Apple-Kunde aus dem US-Bundesstaat Kalifornien strebt eine Sammelklage gegen das Unternehmen an, mit dem Vorwurf, Apple habe ihn zur 2FA „gezwungen“ und diese Tatsache habe ihm und „Millionen ähnlich gestellter Kunden“ „ökonomische Verluste“ eingebracht.
Klingt zunächst amüsant, würde es nicht so ein kläglich verworrenes Bild vom Verhältnis der Welt zur Cybersicherheit aufzeigen. Googles Nest-Abteilung kam kürzlich unter Beschuss, als ein Nest-User, dessen Zuhause gehackt wurde, öffentlich 4.000 US-Dollar Schadenersatz forderte, weil Google ihm nichts über die 2FA mitgeteilt hatte.
Allerdings erhielt keiner der beiden besonders viel Sympathie von den Lesern des Naked Security-Blogs. Auf den Punkt gebracht, halten viele Blogleser es nicht für eine schwere Last 2FA zu nutzen. Sie macht keine außergewöhnliche Mühe oder verursacht so viel Ärger, wie die Kritiker behaupten. Sie hat eine größtenteils positive Wirkung für die gesetzestreue Community und: sie ist eine Funktion, derer wir uns alle heutzutage bewusst sein sollten, selbst wenn wir uns letztlich dazu entscheiden, uns nicht damit zu beschäftigen.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de