Sicherheitsupdate

28. September 2018

Von Guy Rosen, VP Product Management

Am **Dienstagnachmittag, den 25. September**, entdeckte unser Team ein Sicherheitsproblem, das fast **50 Millionen Konten** betrifft. Wir nehmen diesen Vorfall sehr ernst und möchten darüber informieren, was passiert ist und welche Massnahmen wir ergriffen haben, um die Sicherheit der Menschen auf Facebook zu schützen.

Wir befinden uns mit der Aufklärung noch im Anfangsstadium. Allerdings ist bereits klar, dass Angreifer eine Schwachstelle im Code von Facebook im Zusammenhang mit der Funktion „Anzeigen aus der Sicht von“ (View As) ausgenutzt haben. Diese Funktion dient dazu, das eigene Profil aus Sicht einer anderen Person zu betrachten. Im Zuge des Angriffs wurden Facebook-Zugriffstoken gestohlen, mit denen anschliessend Konten übernommen wurden. Zugriffstoken sind so etwas wie digitale Schlüssel, mit denen Menschen bei Facebook angemeldet bleiben, damit sie nicht bei jedem Aufruf der App ihr Passwort erneut eingeben müssen.

Die folgenden Massnahmen haben wir bereits ergriffen:

Zunächst haben wir die Schwachstelle behoben und Behörden darüber in Kenntnis gesetzt.

Zweitens haben wir die Zugriffstoken der aktuell bekannten betroffenen Konten (knapp 50 Millionen) zurückgesetzt, um sie vor Missbrauch zu schützen. Ergänzend unternehmen wir den vorsorglichen Schritt, die Zugriffstoken für weitere 40 Millionen Konten zurückzusetzen, für die im letzten Jahr die Funktion „Anzeigen aus der Sicht von“ angewendet wurde. Infolgedessen müssen sich nun rund 90 Millionen Menschen bei Facebook oder einer der Apps, die Facebook-Login verwenden, erneut anmelden. Wenn sie sich wieder eingeloggt haben, wird ihnen oben im News Feed eine Meldung angezeigt, die den Vorfall erläutert.

Als dritte Massnahme haben wir vorübergehend die Funktion „Anzeigen aus der Sicht von“ deaktiviert, während wir parallel eine gründliche Sicherheitsüberprüfung durchführen.

Dieser Angriff nutzte das komplexe Zusammenspiel mehrerer Schwachstellen in unserem Code aus. Dies ist auf eine Änderung zurückzuführen, die wir an unserer Video-Upload-Funktion im Juli 2017 vorgenommen haben, welche sich wiederum auf „Anzeigen aus der Sicht von“ auswirkte. Die Angreifer mussten diese Schwachstelle nicht nur finden und dafür nutzen, ein Zugriffstoken zu erhalten; sie mussten darüber hinaus von diesem Konto zu anderen wechseln, um weitere Token zu stehlen.

Da wir gerade erst mit unserer Untersuchung begonnen haben, wissen wir zum aktuellen Zeitpunkt noch nicht, ob diese Konten missbraucht wurden und ob auf Informationen zugegriffen wurde. Auch wissen wir nicht, wer hinter diesen Angriffen steckt oder von wo der Angriff ausging. Wir arbeiten mit Hochdruck daran, diese Details in Erfahrung zu bringen und wir werden diesen Beitrag aktualisieren, sobald uns nähere Informationen vorliegen oder falls sich die Faktenlage ändert. Sollten wir darüber hinaus weitere betroffene Konten ausfindig machen, werden wir deren Zugriffstoken sofort zurücksetzen.

Die Privatsphäre und Sicherheit der Menschen auf Facebook ist uns sehr wichtig und wir möchten uns für diesen Vorfall entschuldigen. Wir haben umgehend Massnahmen ergriffen, um die betroffenen Konten zu schützen und die Nutzer über die Ereignisse zu informieren. Es besteht keine Notwendigkeit, das aktuelle Kennwort zu ändern. Alle Menschen, die sich nicht bei Facebook anmelden können – z. B. weil sie ihr Kennwort vergessen haben – finden in

unserem Hilfebereich Unterstützung. Ausserdem sollten alle, die sich als Vorsichtsmassnahme von Facebook ausloggen möchten, den Bereich „Sicherheit und Login“ in den Einstellungen aufsuchen. Dort werden alle Apps und Websites aufgeführt, an denen unsere Nutzer über Facebook angemeldet sind. Hier besteht zudem die Möglichkeit, sich mit einem Klick aus allen Diensten auszuloggen.

Ergänzende technische Informationen

Von Pedro Canahuati, VP Engineering, Security and Privacy

Es folgen einige zusätzliche technische Details zu dem zuvor beschriebenen Sicherheitsproblem.

Anfang dieser Woche haben wir festgestellt, dass ein externer Akteur unsere Systeme angegriffen und eine Schwachstelle ausgenutzt hat. Aufgrund dieser Schwachstelle wurden Facebook-Zugriffstoken für private Konten in HTML offengelegt, nachdem unsere Systeme eine bestimmte Komponente der Funktion „Anzeigen als“ ausgeführt haben. Die Schwachstelle ergab sich aus dem Zusammenspiel dreier unterschiedlicher Fehler:

Erstens: „Anzeigen als“ ist eine Datenschutzfunktion, die dazu dient, das Aussehen des eigenen Profils aus Sicht eines Anderen zu betrachten. „Anzeigen als“ ist als Schnittstelle ausschliesslichen als Ansichtsfunktion vorgesehen. In einem bestimmten „Composer“ (das Feld, über das Du Inhalte auf Facebook posten kannst), nämlich dem zum Verfassen von Geburtstagsglückwünschen, bot „Anzeigen als“ jedoch fälschlicherweise auch die Möglichkeit, ein Video hochzuladen.

Zweitens: Eine neue Version unseres Video-Uploaders (die Schnittstelle, die aufgrund des ersten Fehlers dargestellt wurde), die im Juli 2017 eingeführt wurde, erzeugte fälschlicherweise ein Zugriffstoken mit Zugriffsberechtigung auf die mobile Facebook-App.

Drittens: Der zusammen mit „Anzeigen als“ aktivierte Video-Uploader generierte das Zugriffstoken nicht für Dich als Betrachter, sondern für den angegebenen Nutzer, den Du in der Funktion betrachtest.

In der so beschriebenen Weise ergaben diese drei Fehler eine Schwachstelle: Beim Einsatz der Funktion „Anzeigen als“ zum Betrachten des Profils aus Sicht eines anderen Nutzers hat der Code den Composer nicht entfernt, mit denen Du Freunden Geburtstagsglückwünsche übermitteln kannst; der Video-Uploader generierte fälschlicherweise ein Zugriffstoken; und das generierte Zugriffstoken war nicht auf Dich ausgestellt, sondern auf die Person, die Du bei „Anzeigen als“ ausgewählt hattest.

Dieses Zugriffstoken konnten die Angreifer anschliessend aus dem HTML-Code der Seite extrahieren und dafür missbrauchen, um sich als ein anderer Benutzer anzumelden. Dies ermöglichte es den Angreifern, von diesem Zugriffstoken zu anderen Konten zu wechseln und durch Wiederholung dieses Vorgangs an weitere Zugriffstoken zu gelangen.

Wir haben diese Schwachstelle behoben, so dass die Konten der Menschen auf Facebook sicher sind. Zusätzlich haben wir die Zugriffstoken der fast 50 Millionen bekannten betroffenen Konten zurückgesetzt. Ergänzend haben wir vorsorglich auch die Zugriffstoken für weitere 40 Millionen Konten zurückgesetzt, auf die im letzten Jahr die Funktion „Anzeigen als“ angewendet wurde. Als letzte Massnahme haben wir vorübergehend die Funktion „Anzeigen als“ deaktiviert, während wir parallel eine gründliche Sicherheitsüberprüfung durchführen.