Mit einem Klick ins fremde Facebook-Profil

3. November 2012

Henning Steier, NZZ

Nutzer des Forums «Hacker News» wollen rund 1,3 Millionen Links mittels spezieller Google-Suchanfragen im Netz gefunden haben, über die man sich direkt in Profile von Facebook-Nutzern einloggen konnte. Das Social Network versendet diese Links, welche Nutzer-ID und Passwort enthalten, an E-Mail-Adressen von Mitgliedern, um sie über Aktivitäten ihrer Freunde auf dem Laufenden zu halten. Klickt man einen Link an, läuft er ab. Allerdings sollen noch nicht alle der im Netz zu findenden Links genutzt worden sein, weswegen man fremde Konten übernehmen konnte.

Wer einen abgelaufenen Link anklickt, wird aufgefordert, das Passwort einzugeben. Spammer könnten so aber immerhin noch die E-Mail-Adressen nutzen. Mittlerweile will Facebook die Funktion abgeschaltet haben, wie Entwickler Matt Jones verlauten liess. Die Suchanfragen funktionieren in jedem Fall nicht mehr. Wie die Links in Googles Suchindex gelangten, dazu machte der Mitarbeiter von Facebooks Sicherheitsabteilung keine Angaben. Er forderte Hacker auf, sich beim nächsten Mal direkt an das Unternehmen zu wenden, um nicht zum Missbrauch solcher Entdeckungen einzuladen. Facebook zahlt Nutzern Belohnungen für das Aufspüren von Fehlern. Eine offizielle Stellungnahme des Unternehmens gab es bisher nicht.

Wert der Daten

Laut einem Forennutzer soll Googles Browser Chrome ebenso wie jedes andere Surfprogramm mit Googles Toolbar bei entsprechenden Einstellungen die eingegebenen Internetadressen anonymisiert an den Suchmaschinisten übermitteln, um die Popularität von Links zu messen. Dem hat das Unternehmen wiederholt widersprochen. Auf Googles Hilfeseite zum Browser heisst es, man benötige die Links unter anderem, um Anwendern ähnliche Websites vorschlagen zu können. Laut Matt Jones hätten die Links bewusst online publiziert werden müssen, um in Googles Index aufgenommen zu werden. Viele der ins Netz gelangen E-Mail-Adressen sollen von Anbietern wie asdasd.ru stammen, also Diensten, die vor allem zum Generieren von Wegwerf-Adressen genutzt werden – und für Suchmaschinen zugänglich sind. Das wiederum könnte den Wert der Daten gehörig verringern.

Erst vergangene Woche machte Facebook mit einem Datenschutzproblem Schlagzeilen, das wohl ebenfalls nicht ausschlieslich dem Unternehmen angelastet werden kann: Bogomil Shopov will für fünf Dollar etwa eine Million Namen und E-Mail-Adressen von Facebook-Mitgliedern erworben haben. Der Netzaktivist hat die Datensätze auf der Social-Marketing-Plattform gigbucks.com von einem User namens mertem gekauft. Einige will Shopov ihm bekannten Nutzern zugeordnet haben. Die Daten sollen von Facebook-Apps gesammelt worden sein und vor allem Nutzer aus Europa und Nordamerika betreffen.

Fall wird geprüft

Ein Facebook-Sprecher sagte auf Anfrage, man sei noch mit der Prüfung des Falles

beschäftigt. «Ich habe das Unternehmen gebeten, nach Abschluss der Untersuchung die Öffentlichkeit zu informieren, um in Zukunft solche Pannen zu vermeiden», berichtete Bogomil Shopov, «doch der Mitarbeiter hat mir versichert, dass man keine Informationen dazu veröffentlichen werde.» Wenigstens habe man ihm nicht mit einem Strafverfahren gedroht, sagte Shopov. Heute, gut eine Woche, nachdem Shopov den Fall bekannt gemacht hat, gibt es noch immer keine präzisen Angaben von Facebook, wie es zum Datenleck kommen konnte.

Dass Entwickler Nutzerdaten aus Facebook-Apps zu Geld machen, ist nicht neu. Im Zuge einer Untersuchung der Federal Trade Commission (FTC) zum Datenschutz im Social Network kam im August heraus, dass Facebooks Massnahmen, die Sicherheit von Applikationen zu verbessern, teilweise eine Farce gewesen sein sollen. Denn das im Dezember 2009 nach knapp sechs Monaten eingestellte Programm Verified Apps versprach zwar, eingereichte Anwendungen unter anderem detailliert auf unberechtigtes Auslesen von Userdaten zu überprüfen. Passiert soll dies laut FTC aber nicht sein – «jedenfalls nicht mit einem Aufwand, der über jenen für Standard-Apps hinausging». Daher soll die Formulierung, Anwendern werde zusätzliche Sicherheit bei der Nutzung jener mit dem grünen Häkchen gekennzeichneten Applikationen geboten, irreführend gewesen sein.