Re: Confidential update

Von: [redacted]@fb.com>
An: "gerhard.schabhueser@bsi.bund.de" <gerhard.schabhueser@bsi.bund.de>
Kopie: [redacted]bsi.bund.de>, [redacted]@bsi.bund.de" [redacted]@bsi.bund.de>
Datum: 12.10.2018 18:30

Sehr geehrter Herr Schabhüser,

ich möchte Ihnen ein Update über unsere Untersuchung des Angriffs veröffentlichen, über welchen wir Sie erstmals am 28. September 2018 informiert haben. Wie wir in unserer ersten Ankündigung erklärt haben (https://newsroom.fb.com/news/2018/09/security-update), nutzten die Angreifer eine Sicherheitslücke aus, mit der sie Facebook-Zugangstoken stehlen konnten. Zugangstoken entsprechen digitalen Schlüsseln, mit denen sich Personen bei Facebook anmelden, sodass sie ihr Passwort nicht jedes Mal neu eingeben müssen, wenn sie die App verwenden.

Wir wissen jetzt, dass weniger Menschen betroffen waren, als wir ursprünglich angenommen haben. Von den 50 Millionen Menschen, deren Zugangstoken zu der Zeit möglicherweise enthüllt worden war, wurden von ungefähr 30 Millionen Menschen die Zugangstoken tatsächlich entwendet.

Zunächst kontrollierten die Angreifer bereits eine Reihe von Accounts, die mit Facebook-Freunden verbunden waren. Sie verwendeten eine automatisierte Technik, um von Konto zu Konto zu wechseln, so dass sie die Zugangstoken dieser Freunde und Freunde dieser Freunde usw. stehlen konnten. Insgesamt etwa 400.000 Menschen weltweit. Dabei konnten die Angreifer von diesen 400.000 Menschen sehen, was diese gesehen hätten, wenn sie ihre eigenen Profile angesehen hätten. Dazu gehören Beiträge auf ihrer Timeline, ihre Freundeslisten, Gruppen, denen sie angehören, und die Namen der letzten Messenger-Konversationen. Nachrichteninhalte waren für die Angreifer mit einer Ausnahme nicht verfügbar. Wenn eine Person in dieser Gruppe ein Seitenadministrator war, dessen Seite eine Nachricht von jemandem auf Facebook erhalten hatte, war der Inhalt dieser Nachricht für die Angreifer verfügbar.

Die Angreifer benutzten einen Teil dieser Freundeslisten von 400.000 Menschen, um Zugangstoken für etwa 30 Millionen Menschen zu stehlen. Bei 15 Millionen Menschen griffen die Angreifer auf zwei Arten von Informationen zu - Name und Kontaktdetails (Telefonnummer, E-Mail oder beides), je nachdem, was die Personen in ihren Profilen hinterlegt hatten. Für 14 Millionen Menschen griffen Angreifer auf die gleichen zwei Arten von Informationen sowie auf andere Details zu, die Personen möglicherweise in ihren Profilen hinterlegt hatten. Dazu gehören Benutzername, Geschlecht, Region / Sprache, Beziehungsstatus, Religion, Heimatstadt, selbst angegebene aktuelle Stadt, Geburtsdatum, Gerätetypen für den Zugang zu Facebook, Bildung, Arbeit, die letzten 10 Orte, in denen sie eingecheckt oder getaggt wurden, Website, Personen oder Seiten, denen sie folgen, und die 15 letzten Suchen auf Facebook. Für 1 Million Menschen haben Angreifer keine Informationen entwendet.

Nutzer können in unseren Hilfebereich überprüfen, ob sie betroffen waren (https://www.facebook.com/help/securitynotice?ref=sec). In den nächsten Tagen werden wir den 30 Millionen betroffenen Personen personalisierte Nachrichten senden, um zu erklären, auf welche Informationen die Angreifer zugegriffen haben könnten und welche Schritte sie unternehmen können, um sich selbst zu schützen, einschließlich verdächtiger E-Mails, SMS oder Anrufe.

Dieser Angriff umfasst keine Messenger-, Messenger Kids-, Instagram-, Oculus-, Workplace-, Pages-, Drittanbieter-Apps oder Werbe- oder Entwicklerkonten, obwohl wir noch untersuchen, wie sich dies auf Gruppen ausgewirkt haben könnte.

Gerne stehen wir Ihnen für Rückfragen jederzeit zur Verfügung.

Mit freundlichen Grüßen,
[redacted]

Facebook | Instagram

[redacted] | Manager Public Policy
Mobile +49 [redacted]
[redacted]
Facebook Germany GmbH
“Sony Center" | Kemperplatz 1A | 10785 Berlin

Erfahren Sie mehr über Facebook in Deutschland unter: https://deutschland.fb.com/

HRB 111963 Amtsgericht Hamburg
Geschäftsführer Susan Taylor, Shane Crehan, David William Kling