~~VS-NUR FÜR DEN DIENSTGEBRAUCH~~

Einstufung wurde aufgehoben

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn

Bundesministerium des Innern,
für Bau und Heimat
Referat CI 3
Alt-Moabit 140
10557 Berlin

[redacted]

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn

POSTANSCHRIFT
Postfach 20 03 63
53133 Bonn

TEL [redacted]
FAX

referat-ck15@bsi.bund.de

poststelle@bsi-bund.de-mail.de

https://www.bsi.bund.de

Betreff: Hackerangriff auf Facebook

Bezug: Nachgang 1 zu Erlass 1647/18 CI 3
Geschäftszeichen: CK 15 – 220 00 01
Berichterstatter: [redacted]
Datum: 02.01.2018

Anlage: 1. Cyber-Lage vom 02.10.2018

Mit Bezugserlass bitten Sie um ergänzende Informationen zum Hackerangriff auf Facebook.

Hierzu berichte ich wie folgt:

1. Detaillierte Beschreibung des Zusammenwirkens der bei dem Angriff ausgenutzten drei Software-Schwachstellen im Rahmen der "View-As"-Funktionalität von Facebook und des daraus resultierenden Vorgehens des/der Angreifer.

Die Software-Schwachstelle ergab sich aus dem Zusammenspiel dreier unterschiedlicher Fehler[1]:

1. Die „View-As“-Funktion dient dazu, das Aussehen des eigenen Facebook-Profils aus Sicht eines anderen Nutzers zu betrachten. In einem bestimmten „Composer“ (das Feld, über das Inhalte auf Facebook gepostet werden können), bot „View-As“ jedoch fälschlicherweise auch die Möglichkeit, ein Video hochzuladen.

2. Eine Version des 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.

3. Der zusammen mit „View-As“ aktivierte Video-Uploader generierte das Zugriffstoken nicht für den aktuellen Nutzer, sondern für den Nutzer, aus dessen Sicht man das Profil betrachtet.

1 https://de.newsroom.fb.com/news/2018/09/sicherheitsupdate/

Mit einem solchen Zugriffstoken war es dann möglich, den Zugriff auf die nicht-öffentlichen Inhalte von Facebook-Profilen zu erhalten. Darüber hinaus wurde die Möglichkeit eröffnet, sich über die Single-Sign-On-Funktion auch bei anderen Diensten als der (kompromittierte) Nutzer auszugeben.

2. Erkenntnisse, in welchem Ausmaß deutsche Nutzer von dem Angriff betroffen sind.

Facebook teilte dem BSI am 01.10.2018 mit, dass weniger als 5 Millionen Konten in der EU potenziell von dem Angriff betroffen waren. Die Zahl soll in Kürze von Facebook veröffentlicht werden. Momentan arbeitet Facebook an einer finalen Bestätigung und detaillierten Aufschlüsselung dieser Zahl nach betroffenen Ländern und hat zugesagt, schnellstmöglich weitere Informationen dem BSI zur Verfügung zu stellen.

3. Bewertung der möglichen Hintergründe und Motive des Angriffs, bei denen es nach Presseberichten offenbar nicht zu einer aktiven Nutzung fremder Accounts gekommen ist, jedoch zu einem massenhaften Abruf von Profilinformationen wie Name, Geschlecht und Wohnort.

Hierzu liegen dem BSI keine Erkenntnisse vor.

Allerdings warnt die Australische Cybersicherheitsbehörde (ACSC) nach dem Angriff auf Facebook vor potentiell zunehmenden Phishing-Mailkampagnen. Cyberkriminelle könnten die erbeuteten Daten nutzen, um an weitere persönliche Daten von Facebook-Nutzern zu gelangen. Facebook-Nutzer sollten deshalb besonders auf die Aktivitäten befreundeter Benutzerkonten achten, weil diese für die Verbreitung von Phishing-Mails ausgenutzt werden könnten.

5. Bewertung des Einsatzes von Access Token aus Sicht der IT-Sicherheit, insb. sofern diese über lesende Zugriffe hinaus gehen.

Aus Sicht des BSI spricht nichts gegen den sicheren Einsatz von Access Token[2] Die konkrete Umsetzung von Access Tokens bzw. Single-Sign-On-Verfahren hängt letztendlich jedoch vom Betreiber des jeweiligen Dienstes ab.

Nach derzeitigem Kenntnisstand hätte der Angriff auf Facebook durch die Nutzung der 2-Faktor-Authentisierung zur Erlangung des Access Token nicht verhindert werden können.

2 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04498.html

6. Bitte um Stellungnahme, ob die durch Facebook veranlassten Maßnahmen (Schließung der Sicherheitslücken, Zurücksetzung der Access-Token alle positiv und potentiell betroffenen 90 Mio. Nutzer; vorübergehende Abschaltung der "View-As Funktion") aus Sicht der IT-Sicherheit zur Risikominimierung für die betroffenen Nutzer ausreichen, insb. angesichts der vom BSI zusätzlich empfohlenen Passwortänderung für das Facebook Nutzerkonto sowie die am Single-Sign-On-Verfahren beteiligten Drittdienste.

Facebook hat augenscheinlich schnell und professionell mit Blick auf eine Risikominimierung auf den Angriff gehandelt. Insbesondere das Zurücksetzen von Zugriffstokens unterbindet den potentiell illegalen Zugriff auf nicht-öffentliche Facebook-Inhalte sowie Inhalte von Drittanbietern. Darüber hinaus kann, neben dem Zurücksetzen der Zugriffstoken durch Facebook, die vom BSI empfohlene Passwort-Änderung eine weitere Maßnahme sein, um das Konto vor Missbrauch zu schützen, da u. a. der Angriff noch nicht vollständig aufgeklärt ist.

7. Erkenntnisse, ob über die Facebook Single-Sign-On-Funktion ein Zugriff auf Nutzerinformationen und –profile bei anderen Diensten tatsächlich erfolgt ist sowie Einschätzung der sich für die Nutzer daraus ergebenden (Gesamt-)Gefährdungslage.

Theoretisch wäre es den Angreifern möglich gewesen, über kompromittierte Accounts durch Facebook-Logins auch auf andere Dienste von Drittanbietern zuzugreifen. Ob dies tatsächlich passiert ist, kann Facebook zum gegenwärtigen Zeitpunkt nicht bestätigen. Facebook hat umgehend den Zugriff auf Dienste von Drittanbietern, mit denen sich betroffene Nutzer via Facebook-Login angemeldet haben, unterbunden (vgl. Zurücksetzen von Tokens).

8. Bitte um Mitteilung, welche Maßnahmen Facebook in Zusammenarbeit mit dem BSI zur Aufklärung des Angriffs unternommen hat sowie zu der geplanten weiteren Einbindung des BSI.

Das BSI steht im direkten Kontakt mit Facebook Deutschland, um weitere Informationen über den Angriff zu erhalten. Facebook Deutschland hat zugesagt, Erkenntnisse aus der Untersuchung dieses Vorfalls umgehend und vertraulich mit dem BSI zu teilen.

Das BSI geht zusammen mit Facebook u. a. der Frage nach, inwieweit es den Angreifern möglich war, durch die Nutzung von Zugriffstoken auch die Daten von Freunden eines betroffenen Accounts zu erheben (vgl. Cambridge-Analytica-Vorfall). Derzeit kann Facebook keine Auskunft darüber erteilen, in welchem Umfang die Angreifer Tokens für den Zugriff auf Accounts genutzt haben. Hierbei gäb es theoretisch zwei Möglichkeiten, um auf Daten von Freunden zuzugreifen:

Entweder könnte ein Angreifer auf die Daten von Freunden zugreifen, soweit diese Informationen – je nach Privatsphäre-Einstellung des Freundes – sichtbar sind (Posts, Profilinformationen und Fotoalben, etc.). Oder der Angreifer hatte Zugriff auf den Account und damit auch Zugriff zur "View -As"-Funktion, um wiederum Tokens von Freunden zu erbeuten (durch Wiederholung des skizzierten Angriffs).

Bundesamt
für Sicherheit in der
Informationstechnik

Einstufung wurde aufgehoben

Im Auftrag

Dr. Häger