Fwd: AW: Confidential update

Von: [redacted] <vorzimmerpvp@bsi.bund.de> (Leitungsstab)
An: GPLeitungsstab <leitungsstab@bsi.bund.de>
Datum: 19.10.2018 10:27

LKn,

Euch zur Kenntnis.

Viele Grüße
Im Auftrag
[redacted]

_____ weitergeleitete Nachricht _____

Von: gerhard.schabhueser@bsi.bund.de
Datum: Montag, 1. Oktober 2018, 20:13:25
An: [redacted]@fb.com
Kopie:
Betr.: AW: Confidential update

> Vielen Dank und
> Beste Grüße
> Gerhard Schabhüser
>
> Mit SecurePIM gesendet
>
> Am 1. Oktober 2018 19:35, hat [redacted] geschrieben:
>
> Lieber Herr Schabhüser,
> Ich möchte Ihnen ein vertrauliches Update zu unserem Sicherheitsupdate vom
> 28. September zu einem Angriff auf unsere Systeme durch einen externen
> Akteur geben. Heute morgen haben wir auf Nachfrage dem Irish Data
> Protection Commissioner mitgeteilt, dass weniger als 5 Millionen Konten in
> der EU potenziell von dem Angriff betroffen waren. Diese Zahl wird
> voraussichtlich in Kürze veröffentlicht, aber ich wollte Sie im Voraus
> vertraulich mit Ihnen teilen. Wir arbeiten weiter an einer finalen
> Bestätigung und detaillierteren Aufschlüsselung dieser Zahl und werden
> Ihnen schnellstmöglich weitere Informationen zusenden.
>
> Wenn Sie Fragen oder Anmerkungen haben, melden Sie sich gerne jederzeit.
> Mit freundlichen Grüßen,
> [redacted]
>
> Facebook | Instagram
>
> [redacted] | Manager Public Policy
> Mobile +49 [redacted]
> E-Mail [redacted]@fb.com
> 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
>
> From: [redacted]
> Sent: Sunday, September 30, 2018 12:32 PM
> To: gerhard.schabhueser@bsi.bund.de
> Subject: Re: Weitere technische Informationen zu Hacker-Angriff
>
>
> Lieber Herr Schabhüser,
>
> hier nun die deutsche Übersetzung, die wir auch in unserem "Newsroom"

> veröffentlicht
> haben: https://de.newsroom.fb.com/news/2018/09/sicherheitsupdate/
>
> Ergänzende technische Informationen
>
> 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.
>
> Einen schönen Sonntag,
>
> [redacted]
>
> From: gerhard.schabhueser@bsi.bund.de <gerhard.schabhueser@bsi.bund.de>
> Sent: Saturday, September 29, 2018 9:33 PM
> To: [redacted]
> Subject: AW: Weitere technische Informationen zu Hacker-Angriff
>
>
> Lieber [redacted],
> vielen Dank für das Update
> Beste Grüße
> Gerhard schabhüser
>
> Gesendet von meinem BlackBerry 10-Smartphone.
> Originalnachricht

> Von: [redacted]
> Gesendet: Samstag, 29. September 2018 19:01
> An: gerhard.schabhueser@bsi.bund.de
> Betreff: Weitere technische Informationen zu Hacker-Angriff
>
> Lieber Herr Schabhüser,
>
> unten stehend sende ich Ihnen eine kurze technische Zusammenfassung, wie
> der Angriff verlaufen ist. Wir werden auch zeitnah eine deutschsprachige
> Version der Angriffsbeschreibung zur Verfügung stellen.
>
> Earlier this week, we discovered that an external actor attacked our
> systems and exploited a vulnerability that exposed Facebook access tokens
> for people's accounts in HTML when we rendered a particular component of
> the "View As" feature. The vulnerability was the result of the interaction
> of three distinct bugs:
>
> First: View As is a privacy feature that lets people see what their own
> profile looks like to someone else. View As should be a view-only
> interface. However, for one type of composer (the box that lets you post
> content to Facebook) — specifically the version that enables people to
> wish their friends happy birthday — View As incorrectly provided the
> opportunity to post a video.
>
> Second: A new version of our video uploader (the interface that would be
> presented as a result of the first bug), introduced in July 2017,
> incorrectly generated an access token that had the permissions of the
> Facebook mobile app.
>
> Third: When the video uploader appeared as part of View As, it generated
> the access token not for you as the viewer, but for the user that you were
> looking up.
>
> It was the combination of these three bugs that became a vulnerability:
> when using the View As feature to view your profile as a friend, the code
> did not remove the composer that lets people wish you happy birthday; the
> video uploader would generate an access token when it shouldn't have; and
> when the access token was generated, it was not for you but the person
> being looked up. That access token was then available in the HTML of the
> page, which the attackers were able to extract and exploit to log in as
> another user.
>
> The attackers were then able to pivot from that access token to other
> accounts, performing the same actions and obtaining further access tokens.
>
> To protect people's accounts, we've fixed the vulnerability. We have also
> reset the access tokens of the almost 50 million accounts we know were
> affected and we've also taken the precautionary step of resetting access
> tokens for another 40 million accounts that have been subject to a View As
> look-up in the last year. Finally, we've temporarily turned off the View As
> feature while we conduct a thorough security review.
>
> Beste Grüße,
>
> [redacted]
>
> Facebook | Instagram
>
> [redacted] | Manager Public Policy
> Mobile +49 [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

--
[redacted]

Vorzimmer P/VP
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 -189
53175 Bonn
Telefon: +49 228 99 9582-[redacted]
Fax: +49 228 99 10 9582-5420
E-Mail: vorzimmerpvp@bsi.bund.de
Internet: www.bsi.bund.de
www.bsi-fuer-buerger.de