

Legújabb Facebook-hekk

Ezúttal 50 millió felhasználó oldala került veszélybe, a beszámolók szerint ebből lehet az első GDPR-es gigabírság.



A Facebook múlt pénteken számolt be arról a kivételesen súlyos adatbiztonsági incidensről, amelynek során a támadók 50 millió felhasználói profilhoz és a hozzájuk kapcsolódó adatokhoz férhettek hozzá. A bejelentés szerint a hekkerek a „view as”, vagyis a „megtekintés mint” funkciót kezelő kód hibáját használták ki, amely eredetileg azt mutatja meg a felhasználóknak, hogy mások hogyan látják az ő profiloldalukat, ebben az esetben azonban arra is alkalmas volt, hogy rajta keresztül privát információhoz férjenek hozzá.

A szóban forgó információk köre elvileg kiterjed a személyes üzenetekre, fotókra vagy posztokra is, bár a vállalat közölte, hogy egyelőre nincs rá bizonyíték, ha ezt ténylegesen ki is használták. A biztonsági tokenek működését kihasználó sérülékenység lehetőségét ad ugyan az oldalra való belépésre, de a probléma leírása alapján a hekkerek nem férhettek hozzá magukhoz a belépéshez szükséges jelszavakhoz vagy kártyaadatokhoz. Azzal kapcsolatban viszont ismét csak a maszatolás megy, hogy ezeken kívül mihez férhettek hozzá: a profilokba való belépés ugyanis elég egyértelműen utal rá, hogy körülbelül mindenhez.

A Facebook az FBI-jal közösen vizsgálja az ügyet, és biztonsági megfontolásokból összesen 90 millió

felhasználót jelentkeztetett ki. A társaság ehhez hozzátette, hogy mindazok az érintettek, akik Instagram- vagy Oculus-fiókjukat összekapcsolták facebookos profiljukkal, jobban teszik, ha ismét elvégzik a szét- és összekapcsolást. Egyben elgondolkodhatnak azon is, hogy mennyire jó ötlet az univerzális bejelentkezés, amit a Facebook évek óta mindenhol erőltet.

A gyakorlatban is lecsaphat a 4 százalékos kasza

Az érintett felhasználók számát tekintve a Cambridge Analytica botrányánál is nagyobb volumenű adatbiztonsági incidens részletei [itt](#) vagy [itt](#) olvashatók bővebben. A dolog egyik fontos – és nem technikai jellegű – vonatkozása, hogy a szabályozók és a törvényhozás képviselői is egyből rávetették magukat. A The New York Times például egy demokrata szenátort szólaltatott meg, aki szerint egy újabb indikátorról van szó abban a tekintetben, hogy a kongresszusnak lépéseket kell tennie a közösségimédia-felhasználók személyes adatainak és biztonságának védelmében.

A Wall Street Journal eközben arról ír, hogy a Facebook homályos tájékoztatása a cég európai felügyeletét ellátó ír adatvédelmi hatóság szemében is homályos, így a szervezet további tájékoztatást kért a vállalatától. A lap szerint az incidens könnyen a GDPR keretei között maximálisan kiszabható, jelen esetben 1,63 milliárd eurós bírsággal végződhet, amennyiben megállapítják, hogy a társaság nem tett meg mindent a felhasználói adatok biztosítása érdekében.

A bírság plafonja ugyanis 20 millió dollár, vagy az érintett szervezet globális éves forgalmának 4 százaléka (mindig a magasabb összeg játszik), ez pedig a Facebook esetében éppen ennyit tenne ki; ugyanakkor a bevételek további 2 százalékanak megfelelő összeget is bukhatnak, ha kiderül, hogy az adatszivárgásról nem adtak 72 órán belül megfelelő tájékoztatást az illetékes hatóságoknak.

Ez lenne egyébként a GDPR-ben foglalt büntetési plafon legelső alkalmazása; az Egyesült Államokban egyelőre nem fenyegetnek hasonló nagyságrendű büntetések, de a Facebook vezérigazgatója és operatív vezetője a Cambridge Analytica bortányt követően is kellemetlen órákat töltött szenátus bizottsági meghallgatásán, most pedig odaát is több politikus követel átfogó vizsgálatot a legfrissebb adatbiztonsági fiaskóval kapcsolatban.

Forrás: <https://bitport.hu/1-63-milliard-dollaros-buntetes-erhet-a-facebook-tortenetek-legdurvabb-adatlopasa>

Válogatta: Fonyó Istvánné