OUCH! 2021. szeptember

SANS SECURITY AWARENESS

OUCH!

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Egy egyszerű lépés a felhasználói fiókunk biztonságáért

Úgy érzi, hogy a kiberbűnözőknél valamiféle varázspálca lehet, amivel egy csapásra bejuthatnak az e-mailjeibe vagy bankszámláira, és semmit sem tehet az ellen, hogy megállítsa őket? Nem lenne nagyszerű, ha egyetlen lépésben megvédhetnénk magunkat a kiberbűnözőktől, és biztonságosan hozhatnánk ki a lehető legtöbbet a technológiából? Bár egyetlen lépés nem állít meg minden kiberbűnözőt, az egyik legfontosabb dolog, amit megtehetünk, hogy engedélyezzük a kétfaktoros hitelesítést (2FA, kétlépcsős azonosítás vagy többtényezős hitelesítés néven is használják) a legfontosabb fiókjainkon.

A jelszavak problémája

Ami a fiókok védelmét illeti, valószínűleg mindannyian használunk valamilyen jelszót. Számos módon azonosíthatjuk magunkat egy felhasználói fiókba történő bejelentkezéshez: valamivel, amit birtokolunk, valamivel, amit tudunk, valamivel, ami csak ránk jellemző, vagy azzal, hogy hol tartózkodunk. Ha egynél több hitelesítési módszert alkalmazunk, azzal a kiberbűnözők ellen több védelmi réteget hozunk létre, így ha a támadók fel is törik az egyiket, akkor is meg kell kerülniük a további tényezőket, ha hozzá akarnak férni a fiókunkhoz. A jelszavak az alapján azonosítanak bennünket, amit csak mi tudunk. Ugyanakkor a jelszavak veszélyt is hordoznak magukban, ugyanis kritikus meghibásodási pontot jelentenek. Ha egy kiberbűnöző kitalálja vagy ellopja a jelszavunkat, akkor hozzáférhet a legfontosabb fiókjainkhoz. Ráadásul a számítógépes bűnözők egyre gyorsabb és jobb technikákat fejlesztenek ki a jelszavak kitalálására, kompromittálására vagy megkerülésére. Szerencsére a kétfaktoros hitelesítéssel visszavághatunk.

A kétfaktoros hitelesítés

A kétfaktoros hitelesítés használata sokkal biztonságosabb megoldás, mint pusztán a jelszavakra hagyatkozni. Úgy működik, hogy nem egy, hanem két különböző módszert igényel a hitelesítéshez. Ezzel a megoldással a fiók akkor is biztonságban van, ha a jelszó kompromittálódik. Valójában akkor is kétfaktoros hitelesítési formát használunk, amikor például pénzt veszünk fel egy bankautomatából. Ahhoz, hogy hozzáférjünk a pénzünkhöz, két dologra van szükségünk: a bankkártyára (ami nálunk van) és a PIN-kódra (amit tudunk). Ha elveszítjük a bankkártyánkat, és azt valaki megtalálja, attól még nem veheti fel a pénzünket, mivel nem ismeri a PIN-kódunkat. Ugyanúgy igaz az is, hogy hiába tudjuk a PIN-kódot, ha nincs nálunk a kártya. A támadónak mindkettőre szüksége van ahhoz, hogy kompromittálja a bankszámlánkat. A koncepció hasonló a kétfaktoros hitelesítéshez; két biztonsági rétegünk van.

A kétfaktoros hitelesítés online használata

A kétfaktoros hitelesítést nekünk kell beállítanunk külön-külön minden fiókunkhoz.
Ami valójában meglehetősen egyszerű: általában nem kell mást tennünk, mint szinkronizálni a mobiltelefonunkat a fiókkal. Így, amikor be szeretnénk jelentkezni a fiókba, nem csupán a fiók felhasználónevével és jelszavával tesszük azt, hanem a telefonunkra kapott egyedi, egyszer használatos kódot is használnunk kell. Tehát a jelszó és az egyedi kód kombinációja szükséges a bejelentkezéshez. Általában ezt az egyedi kódot SMS-ben vagy e-mailben kapjuk meg a mobileszközünkre. Az is egy lehetőség, hogy egy telefonunkra telepített mobilalkalmazás (például a Google vagy a Microsoft Authenticator applikáció), hozza létre ezt az egyedi kódot. A mobilalkalmazásokat tekintik a legbiztonságosabb megoldásnak az egyedi kód előállításához.

Az teszi annyira egyszerűvé, hogy ezt általában csak egyszer kell beállítanunk a bejelentkezéshez használt eszközön. Amint a webhely vagy a fiók felismeri az eszközt, a továbblépéshez gyakran már csak a jelszó szükséges. Bármikor, amikor megpróbálunk (vagy valaki más próbál) bejelentkezni a fiókunkba más számítógépről vagy eszközről, újra kétfaktoros hitelesítést kell használni. Ez azt jelenti, hogy ha egy kiberbűnöző megszerzi a jelszavunkat, akkor sem férhet hozzá a fiókunkhoz, mivel nem fér hozzá az egyedi kódhoz.

Ne feledjük azonban, hogy a kétfaktoros hitelesítés alapértelmezés szerint általában nincs engedélyezve, ezért azt nekünk kell bekapcsolni. Bár ez elsőre bonyolultnak tűnhet, a beállítása után már nagyon könnyen használható.

A szerzőről

Lysandra Capella több, mint 15 éves tapasztalattal rendelkezik az információbiztonság és technológia területén. A SANS Intézet oktatója a SANS AUD507 képzéseken, tevékenysége elsősorban a kockázatok felmérésére és kezelésére irányul. Amikor nem oktat, Lysandra stratégiakészítéssel és biztonsági és informatikai irányítással foglalkozik. https://www.linkedin.com/in/lysandracapella/.

Források

Egyszerű jelszókezelés: https://www.sans.org/security-awareness-training/resources/making-passwords-simple/
Jelszókezelők: https://www.sans.org/security-awareness-training/resources/making-passwords-simple/