SANS SECURITY AWARENESS
NEMZETI KIBERVÉDELMI INTÉZET
OUCH! | 2017. December
Havi biztonság tudatossági hírlevél mindenkinek

OUCH!

ebben a kiadásban...

- **Jelszavak**
- **Mi az a kétfaktoros autentikáció**
- **Hogyan Működik**

Biztonságos bejelentkezés

Áttekintés

Az autentikációs eljárás, vagyis annak bizonyítása, hogy ki is vagyok kulcsfontosságú a személyes információnk megvédésében, mint például az elektronikus leveleink, közösségi média- vagy online banki adataink. Nincs mindenki tudatában, hogy több módja is van annak, hogy bizonyítsuk, azok vagyunk, akinek állítjuk magunkat. Ilyen lehet például a tudás vagy ismeret alapú azonosítás – tudok valamit, pl.: jelszó, a birtoklás alapú azonosítás – van valamim, pl.: igazolvány, és a tulajdonság alapú azonosítás, például az ujjlenyomat azonosítás. Mindegyik fentebb felsorolt módszernek vannak előnyei és hátrányai. A legjobban elterjedt azonosítási mód a jelszavas azonosítás, amit bizonyára mindenki ismer. Sajnos, a jelszavak használata az elmúlt időszakban egyre inkább megbízhatatlannak bizonyult. Ebben a hírlevélben bemutatjuk, hogyan védhetjük meg magunkat, és hogyan tehetjük hatékonyabbá az egyszerű jelszó használatnál a bejelentkezési adataink védelmét a kétfaktoros autentikációnak nevezett eljárás segítségével.

A szerzőről
Tiffany Schoenike a Nemzeti Kiberbiztonsági Egyesület (**@staysafeonline**) Kampányok és Kezdeményezések igazgatója. Tiffany Schoenike 2016-ban dolgozott a Fehér Háznak, az USA kormányzatának és együtt dolgozott az ipar szereplőivel is annak érdekében, hogy elindítsa a Biztonságos Bejelentkezés, ÁLLJ! GONDOLKOZZ! CSATAKOZZ! figyelemfelhívó információs hadjáratát a kétfaktoros autentikáció témakörében.

A jelszó többé nem elég

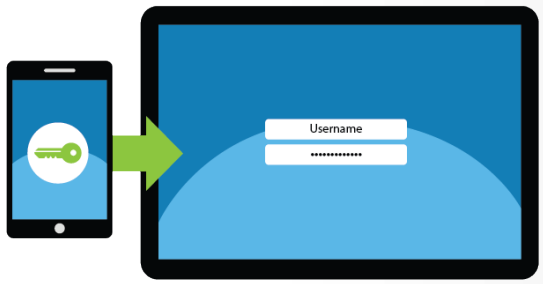
A jelszavak az ismereteinkre alapozva bizonyítják kilétünket. De ha valaki kitalálja, vagy más módon hozzáfér a jelszavunkhoz, eljátszhatja, hogy Ő mi vagyunk, és máris hozzáfér minden információnkhoz. A jelszó kompromittálódás az egyik vezető okává vált a felhasználói fiókok sikeres feltörésének. Ezért tanították régebben, hogy jelszavak helyett használjunk olyan jelmondatokat, amiket nehéz kitalálni, minden fiókhoz használjunk különböző jelszót, és sohase osszuk meg jelszavainkat mássokkal. Bár ezek a tanácsok ma épp annyira érvényesek, mint korábban, a jelszavas védelem ma már nem elégséges és nem elég hatékony. Szerencsére van egy egyszerű módja annak, hogy megtartsuk az irányítást a felhasználói fiókjaink felett, és biztonságban tartsuk a személyes adatainkat: ezt hívjuk kétfaktoros autentikációnak.

Mi az a kétfaktoros autentikáció?

A kétfaktoros autentikáció (más néven: kétlépéses autentikáció, több-faktoros autentikáció vagy 2FA) sokkal megbízhatóbb, mint a jelszavas védelem önmagában történő használata. Úgy működik, hogy az azonosítás során a felhasználónak

Biztonságos bejelentkezés

nem egy, hanem két különböző módon kell bizonyítani, hogy valóban az, akinek mondja magát. Jó példa erre a bankkártya: amikor készpénzt veszünk fel a bank automatából, a pénzfelvétel során igazából kétfaktoros autentikációt használunk. Ahhoz, hogy hozzáférhessünk a pénzünkhöz két dolog szükséges: a bankkártya (birtoklás), és a PIN kód (ismeret). Amennyiben a bankkártyánk elvész, vagy ellopták, mások nem tudnak pénzt felvenni a bank automatából anélkül, hogy tudnák a kártyához tartozó PIN kódunkat is. Egy tolvajnak egyszerre kell fizikailag hozzáférnie a bankkártyánkhoz és kell ismernie a hozzá tartozó PIN kódot is. A kétfaktoros autentikáció ugyanezt a koncepciót használja.



Tegyük biztonságosabbá a bejelentkezésünket kétfaktoros autentikáció alkalmazásával, amikor csak lehetséges, ez az egyik legerősebb lépés, amit tehetünk saját online védelmünk érdekében.

Hogyan működik

A kétfaktoros autentikácó széles körben elérhető a legtöbb nagy bank, levelezés-szolgáltató, közösségi média oldalán, illetve más oldalakon is. Továbbá, ezen oldalak legtöbbje egyszerű, lépésről-lépésre követhető tanácsokat is ad, hogy miként lehet bekapcsolni a kétfaktoros azonosítást (további információkért kérjük, tekintse át a hírlevelünk végén felsorolt forrásokat). Amint sikeresen bekapcsoltuk a kétfaktoros azonosítást, az a következőképpen fog működni. Először is, a szokásos módon kezdeményezzük a belépést: megadjuk a felhasználói nevünket és a jelszavunkat. Ez az első a két faktor közül – az ismeret alapú azonosítás. Ezt követően egy egyedi kódot kapunk, legtöbbször SMS formájában a mobil telefonszámunkra. Ezt a kódot kell beírnunk az oldal megfelelő mezőjébe. Ez a második faktor – kell, hogy legyen egy telefonunk, amire a kód kiküldésre kerül, azaz birtoklás. Innentől a felhasználói fiókunk valóban védetté vált. Még ha egy kiberbűnöző meg is szerzi az adott fiókhoz tartozó jelszavunkat, nem fér hozzá a felhasználói fiókunkhoz mindaddig, míg a telefonunkat is meg nem szerezte.

Ahelyett, hogy egy egyedi kódot kellene SMS-ben fogadnunk, telepíthetünk egy speciális azonosítást végző alkalmazást is az okos telefonunkra. Ez a program minden egyes bejelentkezési kísérlethez egyedi kódot generál nekünk. A mobil alkalmazás használatának előnye, hogy ez még biztonságosabb, mint az SMS, mert az egyedi kód a program által generálódik, és nem kerül kiküldésre szöveges üzenetként. Ez a megoldás kényelmesebb is, mivel a kód generálásához nem szükséges, hogy a telefonunk csatlakozva legyen egyik mobilhálózathoz sem. Az alkalmazás folyamatosan generálja nekünk a belépéshez használható új kódokat.

Biztonságos bejelentkezés

Ugyan a kétfaktoros autentikáció használata első ránézésre több felhasználói interakciót követel meg, a személyes adataink sokkal nagyobb biztonságban lesznek. Ne várjunk addig, míg az egyik felhasználói fiókunkat feltörik, tegyük biztonságossá a bejelentkezési folyamatot a kétfaktoros autentikáció használatával. Ezt a megoldást a legfontosabb fiókjaink védelmére használjuk - mint a levelezés, online bankolás, vagy közösségi média fiókjaink - és élvezzük a nyugalmat, tudván, hogy adataink biztonságban vannak.

További információ

Iratkozzon fel a havi OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a securingthehuman.sans.org/ouch/archives weboldalon.

Magyar Kiadás

A Nemzeti Kibervédelmi Intézet (NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. A Nemzeti Kibervédelmi Intézet rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a magyar kibertér biztonságának erősítéséhez. További információ az Intézetről a http://www.govcert.hu/ és a http://neih.gov.hu oldalon olvasható.

Hivatkozások

Jelmondatok:	https://securingthehuman.sans.org/ouch/2017#april2017
Oldalak, amik támogatják a kétfaktoros autentikációt:	https://twofactorauth.org
Állj|Gondolkozz|Csatlakozz:	https://www.lockdownyourlogin.org
Google két lépéses azonosítás:	http://www.google.com/landing/2step/

Szerkesztette: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Fordította: Tikos Anita

