Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadásban...

- Áttekintés
- Jelszavak
- A kétlépcsős hitelesítés

A kétlépcsős hitelesítés

Áttekintés

Az információink védelmében kulcsfontosságú az a folyamat, amikor igazoljuk, hogy kik is vagyunk – ezt nevezik hitelesítésnek. Az erős hitelesítési eljárások célja, hogy csak mi férjünk hozzá saját adatainkhoz, mint például az email-ekhez, fotókhoz vagy banki adatokhoz. Három különböző módszer létezik, amellyel bizonyítani tudjuk, kik is vagyunk: van, amit tudnunk kell – jelszó; van, amivel rendelkeznünk kell – például vezetői engedély; és van, ami mi magunk vagyunk – például az ujjlenyomat. Mindegyik módszernek vannak előnyei és hátrányai. A leggyakoribb megoldás a jelszó. E havi hírlevelünkben megmutatjuk, hogyan tudjuk megvédeni magunkat a kétlépcsős hitelesítés segítségével, amely sokkal biztonságosabb, mint a jelszó, és manapság már nagyon egyszerű a használata. Azonban a kétlépcsős hitelesítés könnyebb megértése miatt előbb a jelszóval kell kezdenünk.

A szerzőről

Keith Palmgren már több mint 30 évnyi tapasztalatot szerzett az informatikai biztonság területén. A SANS Institute minősített oktatója, a SANS SEC301 (5 napos bevezetés az információ biztonságba) kurzus szerzője. Az oktatás mellett tanácsadásban, illetve projektek szervezésben is szerepet vállal. A Twitter-en **@kpalmgren** néven találhatjuk meg.

Jelszavak

A jelszavak segítségével úgy igazoljuk önmagunkat, ha ismerünk bizonyos információkat. A jelszavak azért veszélyesek, mert egyedi hibapontként szolgálhatnak. Ha valaki kitalálja vagy megszerzi a jelszavunkat, akkor úgy tud tenni, mint ha mi lennénk a gépnél, és így hozzáférhet minden olyan információhoz, amelyet az adott jelszóval védtünk. Ezért tanultuk meg korábban azt, hogy erős jelszót használjunk, amit nem lehet könnyen kitalálni. Mindenhol más és más jelszót adjunk meg, illetve hogy soha ne osszuk meg másokkal a jelszavainkat. Bár ezek a tanácsok még most is érvényesek, azt látnunk kell, hogy a jelszavak mára elavult megoldásnak számítanak, nem felelnek meg a kor követelményeknek: a legújabb technológiákkal a kiberbűnözők már könnyen fel tudják törni a jelszavakat. Amire manapság szükségünk van, az egy könnyen használható, biztonságosabb, erős hitelesítő eljárás. Szerencsére már rendelkezésre áll olyan általános megoldás, amit úgy nevezünk, hogy kétlépcsős hitelesítés.

A kétlépcsős hitelesítés

A kétlépcsős hitelesítés (néha szokták kétfaktorosnak is nevezni) sokkal biztonságosabb módszer, mint a jelszó. Úgy működik, hogy nem egy, hanem két azonosítási módszert is használunk önmagunk hitelesítése érdekében. Vegyük például

A kétlépcsős hitelesítés

az ATM-nél használt bankkártyákat. Amikor pénzt veszünk fel egy automatából, gyakorlatilag kétlépcsős hitelesítést használunk, hiszen szükségünk van magára a kártyára (valamire, ami a birtokunkban van), illetve a PIN kódra (valami, amit tudunk). Ha elhagyjuk a kártyát, attól a pénzünk még biztonságban van. Bárki is találja meg a kártyát, a PIN kód nélkül nem férhet hozzá a pénzünkhöz (kivéve azt az esetet, ha ráírjuk a kártyára, de ez nagyon rossz ötlet). Ugyanez igaz akkor is, ha valaki megtudja a PIN kódot, de nincs nála a kártya, mivel a támadónak mindkettőre szüksége van ahhoz, hogy hozzáférjen a bankszámlához. És pontosan ez a kétrétegű eljárás teszi sokkal biztonságosabbá a kétlépcsős hitelesítést.

Használjunk kétlépcsős hitelesítést amikor csak lehetséges, mert ez az egyik legerősebb módszer az adataink védelmére.

A kétlépcsős hitelesítés használata

Ezt a fajta hitelesítést egyesével kell minden egyes felhasználói fiókhoz beállítani, de szerencsére most már számos online szolgáltatás kínál ilyet. Az egyik legismertebb ilyen szolgáltató a Google. A Google fiókok a kiberbűnözők számára elsődleges célpontok, az általuk nyújtott széleskörű ingyenes szolgáltatások miatt, amiket világszerte emberek milliói használnak. Ennek következtében a Google-nél felmerült az igény, hogy erősebb hitelesítést vezessenek be, így az elsők között volt, akik elérhetővé tették a legtöbb ingyenes szolgáltatásukhoz a kétlépcsős hitelesítést. Ha megértjük, hogyan működik a Google által használt kétlépcsős hitelesítés, akkor érteni fogjuk a többi világszerte ismert weboldalnál használt megoldásokat is (Facebook, Instagramm Twitter, Apple, de számos bank is).

Elsőként engedélyeznünk kell a Google fiókban a kétlépcsős hitelesítést, majd ezután regisztrálni kell a telefonszámunkat. Miután ezzel megvagyunk, a következőképpen fog működni. Belépünk a fiókunkba felhasználói névvel és jelszóval ugyanúgy, ahogy már korábban is. Ez a két lépcső közül az első – ez az, amit tudnunk kell. A Google küld egy SMS-t mobiltelefonunkra, amely egy egyedi kódot, egy 6 karakter hosszúságú üzenetet tartalmaz. Ezt pedig ugyanúgy, mint a jelszót, be kell írni a weboldalon. Ez a második lépcsőfok. Tehát ahhoz, hogy sikeresen be tudjunk jelentkezni, szükségünk van a jelszóra (ezt kell tudnunk), és szükség van a mobiltelefonra (ezt pedig birtokolnunk kell), hogy megkaphassuk az egyedi kódot. Még ha egy támadó meg is tudja szerezni a jelszavunkat, nem férhet hozzá a Google fiókunkhoz a mobiltelefonunk nélkül. A teljesebb körű biztonság érdekében a Google minden egyes bejelentkezéshez egy új és egyedi azonosítót küld számunkra.

A kétlépcsős hitelesítés

A Google és számos más weboldal is ajánl másik lehetőséget, hogy kétlépcsős hitelesítést használjunk. Az SMS-ben küldött egyedi kód helyett, egy az okostelefonra telepített alkalmazás generálja le azt minden egyes bejelentkezés előtt. Ennek előnye, hogy nincs szükség hálózatra csatlakozott telefonra, mert az helyben generálja le az egyedi kódot, amit így nem is lehet lehallgatni a küldés közben.

Ne felejtsük el, hogy a kétlépcsős hitelesítés alapértelmezetten nincs engedélyezve, azt nekünk kell bekapcsolni! Bár elsőre úgy látszik, hogy több vele a munka, mégis erősen ajánljuk, hogy mindenki engedélyezze, ahol csak lehetséges, különösen az olyan kritikus szolgáltatásoknál, mint az email, online bankolás vagy személyes fájlok Interneten történő tárolása. A kétlépcsős hitelesítés sokkal jobb megoldás az adatok védelmére, mint az egyszerű jelszó.

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a http://www.securingthehuman.org weboldalon keresztül.

Magyar Kiadás

Kormányzati, távközlési és informatikai szolgáltatóként, Magyarország egyik stratégiai fontosságú gazdasági társasága a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Társaságunk kiemelt feladata a kormányzati infrastruktúra működtetése, az e-közigazgatási megoldások támogatása, valamint kormányzati szintű informatikai szolgáltatások nyújtása. További információ a http://www.nisz.hu oldalon olvasható.

Hivatkozások

A jelmondatokról: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201504_hu.pdf

A kétlépcsős hitelesítést támogató weboldalak: https://twofactorauth.org

Google kétlépcsős hitelesítés: http://www.google.com/landing/2step/

SANS napi biztonsági tipp (angolul): http://www.sans.org/tip_of_the_day.php

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Fordította: Birkás Bence, Árvai Gábor, Pál Benyó

