OUCH! 2023. január

Az Ön Havi Biztonsági Tudatosságról szóló hírlevele

Biometria – tegyük egyszerűvé a biztonságot!

Áttekintés

Ki nem állhatja a jelszavakat? Elege van abból, hogy folyamatosan be kell jelentkeznie az új weboldalakra vagy nem emlékszik a bonyolult jelszavaira? Frusztrálja, hogy az új fiókokhoz folyton új jelszavakat kell létrehoznia, illetve, hogy a meglévő fiókok régi jelszavait le kell cserélnie? Van egy jó hírünk. Ezekre a problémákra megoldást kínál a biometria, ami könnyebbé teszi számunkra a kibervédelmet. Az alábbiakban elmagyarázzuk, hogy mik azok a biometrikus adatok, hogyan teszik könyebbé az életünket és miért fogunk velük egyre többször találkozni.

Először is, miért a jelszavak?

A jelszavak hitelesítésre szolgálnak, segítségükkel bebizonyíthatjuk, hogy kik vagyunk. Alapvetően két dologgal tudjuk igazolni a személyazonosságunkat: valamivel, amit tudunk (például a jelszavaink) és valamivel, amit birtoklunk (mint a bankkártyánk vagy a telefonunk). A hitelesítés hagyományosan jelszavakkal történik. Azért jelszavakat alkalmaztunk legelőször, mert ez az egyik legkönnyebben bevezethető hitelesítési megoldás. Az évek során azonban az életünk bonyolultabbá vált, sokkal több fiókot használunk, mint valaha. Gyakran előfordul, hogy valakinek több mint 100 jelszava van a munkahelyén és a magánéletében.

Ráadásul a kibertámadók egyre jobbak a jelszavak kitalálásában, ellopásában és feltörésében. Ezért találkozunk annyi jelszókövetelménnyel, mint például, hogy legyen hosszú (ezáltal nehezen kitalálható), használjunk egyedi jelszót minden fiókhoz (így ha az egyik fiókunkat feltörik, a többi még mindig biztonságban van). Ezek a követelmények ugyanakkor megnehezítik a kiberbiztonságot. A jelszószéfek sokat segítenek azáltal, hogy biztonságban tartják és emlékeztetnek minket a jelszavainkra, bejeletkeznek helyettünk a weboldalakra, de vajon létezik-e ennél is jobb megoldás? Itt jön képbe a biometria, amelynek segítségével egy harmadik féleképpen igazolhatjuk személyazonosságunkat – azzal, amilyenek vagyunk.

Biometrikus adatok

A jelszavakhoz hasonlóan a biometrikus adataink is a személyazonosságunk igazolására szolgálnak. A különbség az, hogy ahelyett, hogy emlékeznünk kellene valamire (például a jelszavakra), a személyazonosságunk egy elemét használjuk az azonosításhoz, például ha ujjlenyomatunkkal oldjuk fel a telefonunkat.

A biometrikus azonosítás sokkal egyszerűbb, nem kell emlékeznünk semmire, nem kell beírnunk semmit, hanem valamilyen egyedi testi jellemző alapján azonosítjuk magunkat. Számos különböző típusú biometrikus adat létezik, például a hangunk, a járásunk vagy a szivárványhártyánk (írisz) lenyomata. A két legelterjedtebb az ujjlenyomat és az arcfelismerés, különösen a mobileszközök esetében. Számtalan előnye ellenére, azért a biometriának is létezik hátránya. Az egyik legnagyobb, hogy ha a kibertámadók lemásolják az ujjlenyomatunkat vagy az arcunkat, azt nem tudjuk megváltoztatni.

Belépőkulcsok – Passkeys

Az elkövetkező hónapokban és években valószínűleg azt fogjuk majd látni, hogy a biometrikus azonosítók a jelszavakat egy úgynevezett Passkeys technológiával fogják helyettesíteni. A Microsoft, az Apple, és a Google már használják ezt a megoldást, és hamarosan még több oldalon is megjelenik majd. A jelszavak helyettesítésére szolgáló belépőkulcsok lehetővé teszik, hogy a mobileszközünkkel kombinált biometrikus adatok segítségével igazoljuk magunkat. Amikor új fiókot regisztrálunk egy weboldalon (például a Google-nél vagy az Applenél) a jelszó létrehozása helyett a mobiltelefonunkat fogjuk regisztrálni. Később úgy jelentkezünk majd be az adott webhelyre, hogy a telefon a biometrikus adatainkat – ujjlenyomatunkat, arcfelismerést – használva hitelesíti a személyünket. A weboldal megbízik az eszközünkben, a mobil pedig a biometrikus adatainkkal ellenőrzi, hogy valóban mi szeretnénk belépni. A biometrikus adataink (ujjlenyomatunk, arcunk) pedig nem kerülnek továbbításra semmilyen weboldalra, hanem biztonságosan eltárolásra kerülnek a készülékünkön. Ezek az adatok csak a „Passkey" feloldására szolgálnak, amely egy egyedi, minden egyes webhelyhez létrehozott kulcs, amelyet a készülék elküld a webhelynek, s közben védi a biometrikus azonosítóinkat. Bár nincs tökéletes megoldás, a biometria és az olyan megoldások, mint a Passkeys, egyszerűbbé tehetik és segíthetik biztonságunkat.

A szerzőről

Dr. Johannes Ullrich a SANS Technológiai Intézet dékánja. Több mint 20 éves ipari tapasztalattal rendelkezik, jelenleg a SANS Internet Storm Center üzemeltetésével figyeli az aktuális fenyegetéseket. A SEC522 (Webes alkalmazások biztonsága) és a SEC503 (Behatolás-felderítés) tárgyak oktatója.
Twitter: @johullrich & LinkedIn: https://www.linkedin.com/in/johannesullrich/.

Források

Jelszókezelők: https://www.sans.org/newsletters/ouch/password-managers/
Bővebben a belépési kulcsokról: https://www.sans.org/blog/what-is-phishing-resistant-mfa/

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)