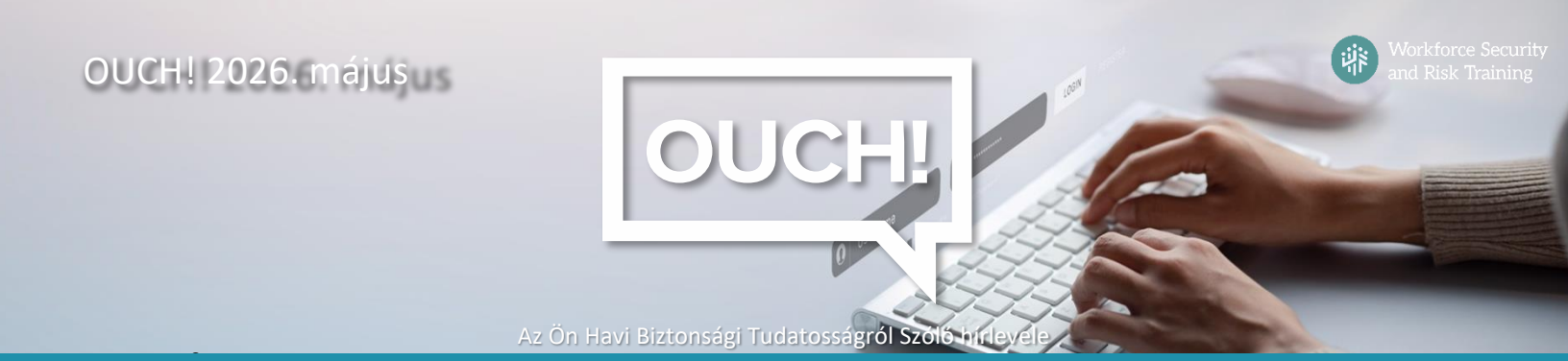

A jelmondatok ereje: miért jobb a hosszabb, mint az okosabb?

Egy egyszerű jelszó, egy hatalmas probléma

Daniel mindig is járatosnak érezte magát a számítógépek világában. Gyakran vásárolt online, digitálisan kezelte pénzügyeit és a közösségi médián keresztül tartotta a kapcsolatot barátaival. Mint sokan mások, ő is egy sok éve használatos jelszóval védte személyes e-mail fiókját. Rövid volt, könnyen megjegyezhető, és egy szimbólumon és számjegyen felül a kedvenc sportcsapatának nevét is tartalmazta. Úgy gondolta, elég jó.

Egy reggel Daniel számtalan értesítésre ébredt. Jelszó-visszaállítási e-mailek, sikertelen bejelentkezési kísérletek, valamint üzenetek barátoktól, amelyekben azt kérdezték, miért küld nekik furcsa linkeket. Az éjjel folyamán e-mail fiókját feltörték. Miután bejutott, a támadó visszaállította a jelszavakat a közösségi média, vásárlási és felhőalapú tárhelyfiókjain. Néhány órán belül hamis üzeneteket küldött a kapcsolatai számára, vásárlásokat hajtott végre a nevében, és privát fényképeket is letöltött.

Az egész oka nem egy bonyolult hackelés volt, vagy egy szofisztikált malware. A legvalószínűbb ok a gyenge, több helyen újrahasznált jelszava volt, amely vagy egy másik weboldalon történt adatszivárgás során került nyilvánosságra, vagy a támadó automatizált eszközei egyszerűen kitalálták. Egyetlen gyenge jelszó kulcsot adott a kiberbűnöző kezébe Daniel egész digitális életéhez.

Miért hagynak minket cserben a jelszavak?

A jelszavak továbbra is a leggyakoribb módjai online fiókjaink védelmének, ugyanakkor biztonságunk egyik leggyengébb pontját is jelentik. A kiberbűnözők általában nem egyesével próbálgatják a jelszavakat, mint a filmekben. Ehelyett automatizált eszközöket használnak, amelyek rendkívül gyorsan képesek akár több millió vagy milliárd jelszókombinációt is kipróbálni. Emellett nagymértékben támaszkodnak a korábbi adatszivárgásokból származó, lopott jelszólistákra is. Ha újrahasználjuk a jelszavakat, vagy rövid és kiszámítható jelszavakat választunk, a támadók már eleve előnyből indulnak.

Az erős jelszavak az egyik legalapvetőbb eszközt jelentik fiókjaink és online digitális életünk védelmében. Az összetett jelszavakkal azonban az a probléma, hogy nehéz őket megjegyezni és hiba nélkül begépelni. Egy még jobb módja az erős és biztonságos jelszó létrehozásának egy úgynevezett „jelmondat” kitalálása. A jelmondat egész egyszerűen egy több szóból álló jelszó, amelyet néha egy rövid kifejezéssé kapcsolunk össze. Ezek nem pusztán az összetettségük miatt erősek, hanem a hosszúságuk révén is. Például:

Itt az ideje egy jó erős kávénak!
eltévedt-csiga-csúszkál-a-strandon

A hosszabb jelmondatok jelentősen nehezebben törhetők fel automatizált eszközökkel, miközben továbbra is könnyen megjegyezhetők és begépelhetők maradnak. Bizonyos esetekben előfordulhat, hogy némi összetettséget is hozzá kell adnunk a jelmondatunkhoz, például szimbólumok, nagybetűk vagy számok beillesztésével.

Legyenek eredeti jelmondataink

A hossz önmagában még nem elég. A jelmondatainknak egyedieknek is kell lenniük minden egyes fiókunkhoz. Ha ugyanazt a jelszót vagy jelmondatot több oldalon is újrahasználjuk, már egyetlen fiók kompromittálódása is veszélybe sodorhatja az összes többi fiókunkat. A támadók rutinszerűen próbálják ki az ellopott hitelesítő adatokat e-mail, banki és közösségi platformokon az úgynevezett "credential stuffing" nevű folyamat során.

Tároljuk biztonságosan jelmondatainkat

Nem tudja megjegyezni az összes hosszú, egyedi jelmondatát minden egyes fiókjához? Erre is van megoldás: a jelszó menedzserek. Ezek speciális számítógépes programok, amelyek egy titkosított tárolóban biztonságosan megőrzik az összes jelszavunkat, egy mesterjelszóval védve. Ahhoz, hogy hozzáférjünk a tárolóhoz, csak a mesterjelszavunkat kell megjegyeznünk. A jelszómenedzser automatikusan elő tudja hívni a jelszavainkat, amikor szükségünk van rájuk, és automatikusan be is jelentkeztet minket a különböző weboldalakon. A jelszókezelők mára további funkciókkal is bővültek, beleértve a titkos kérdésekre adott válaszok tárolását, figyelmeztetést, ha újrahasználunk egy adott jelszót vagy ha hamis weboldalra kerülünk, valamint olyan generátorokat, amelyek erős jelszavakat vagy jelmondatokat hoznak létre számunkra. A legtöbb jelszókezelő biztonságosan szinkronizálható szinte bármilyen számítógép vagy eszköz között, így függetlenül attól, milyen rendszert használunk, könnyen és biztonságosan hozzáférhetünk az összes jelszavunkhoz.

Vigyük még egy lépéssel tovább

Még a legerősebb jelmondat sem feltétlen elég. Ezért minden lehetséges helyen érdemes engedélyeznünk a többfaktoros hitelesítést (MFA). Az többfaktoros hitelesítés egy további védelmi réteget ad azáltal, hogy megkövetel valamit, amivel rendelkezünk, például egy másik eszközre küldött egyszer használatos kódot, vagy valamit, ami mi magunk vagyunk, például biometrikus azonosítást. Ez azt jelenti, hogy még ha el is lopják a jelmondatunkat, a támadó akkor se tud belépni.

Egyszerű szokások, erős védelem

Daniel története egészen másképp is alakulhatott volna, ha hosszú, egyedi jelmondatot használ, és esetleg még a többfaktoros hitelesítést is engedélyezi. A gyenge vagy újrahasznált jelszavak továbbra is nagyon gyakoriak, és lehetővé teszik a kiberbűnözők számára, hogy célba vegyenek minket, függetlenül attól, hogy egyébként mennyire vagyunk óvatosak vagy tapasztaltak.

Vendégszerkesztő

Tarun Preetham Bulla kiberbiztonsági oktató és szakember, aki többéves iparági tapasztalattal rendelkezik az incidenskezelés, a digitális forenzika és a fenyegetésészlelés területén. Tarun kiberbiztonsági kurzusokat oktat alapképzéseken, kiberlaborokat irányít, szakdolgozati projekteket mentorál, és arra összpontosít, hogy a hallgatókat a munkaerőpiacra készítse fel azáltal, hogy a valós iparági tapasztalatokat beépíti az oktatásba.

Források

Tegyük könnyebbé a jelszókezelést: használjunk megbízható jelszószéfet: https://www.sans.org/newsletters/ouch/stop-password-pain-reliable-password-manager
A Misztikum Feloldása: Hogyan lopják el a jelszavakat a kiberbűnözők?: https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords/
Passkey - A bejelentkezés egyszerűbb és biztonságosabb módja: https://www.sans.org/newsletters/ouch/passkeys-simpler-safer-way-sign-in

A Közösség számára fordította: Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ NKI)

Többet találhat az Ouch!-ból A következő linken: https://www.sans.org/newsletters/ouch