Passkey a biztonság új szintje

PCLinuxOS Magazine – 2023. november

Jacob Hoffman-Andrews
Electronic Frontier Foundation (EFF) írásai nyomán
(a PCLinuxOS Magazine 2023. novemberi számában megjelent kétrészes cikk kivonata)

Mi az a Passkey?

A Passkey egy, 2023-tól elérhető új bejelentkezési technológia az adathalászat és a jelszavak többszöri felhasználásának megakadályozására.

A Passkey eszközön (telefon, laptop, biztonsági USB kulcs stb.) tárolt, egy adott weblapra bejelentkezés céljából véletlenszerűen generált 100-1400 byte hosszú, adatsor. A Passkey-t a böngésző biztonságos helyen tárolja (pl. jelszókezelő) és az adott weblapra jelszó begépelés nélküli bejelentkezéshez használja. Csak annyit kell tenni, hogy a weblap bejelentkező képernyőjénél a „Sign in with a Passkey”-t (bejelentkezés Passkey-vel) kell kiválasztani – ha van ilyen lehetőség. Ekkor a jelszókezelő kéri a megerősítést, amit nyugtázva belép. Persze ehhez a honlapnak, a böngészőnek, a jelszókezelőnek és az operációs rendszernek egyaránt támogatnia kell a Passkey alkalmazását.

Minden egyes fiókot, legyen az más, vagy egyazon honlaphoz tartozó, külön Passkey zárol. A Passkey használata gyors (két kattintás) és mellőzhető vele a szokásos kétlépcsős azonosítás (SMS, vagy biztonsági kulcs). Azért lehetséges ez, mert az adott gépen a használatához, a gépre bejelentkezéssel (PIN, arc-, vagy újlenyomat-felismerés) már eleve történt egy hitelesítés.

A kulcs tárolása és mentése

Mivel a Passkey egy adott eszközön van, némi gond lehet a használatával másik gépeken. Három lehetséges megoldás van a kulcs átvitelére:

> **1.** a jelszótárolóban titkosítva tárolt Passkey mentése felhőbe és onnan másolása más gépekre;
> **2a.** Passkey-t egy fizikai USB biztonsági kulcson készítjük és azt használjuk bejelentkezésre más gépeken. (Az ilyen Passkey nem másolható, de ehhez újfajta, Passkey-t támogató kulcs kell);
> **2b.** a Passkey fokozott biztonságú, gépbe beépített csipre kerül (pl. TMP, vagy Secure Enclave). Az ilyen kulcs sem másolható.

A 2a és 2b megoldások kevésbé kényelmesek, de biztonságosabbak, ám a megvalósításuknak költségvonzata lehet. Az 1. megoldásnál a készülék ellopása esetén a Passkey esetleg lemásolható, ha a jelszókezelő nincs megfelelően védve.

A 2a és 2b-nél, az elvesztés, vagy megsemmisülés esetére egyazon weblaphoz több Passkey-t kell készíteni más gépeken, vagy az e-mail alapú felhasználói fiókhelyreállításra kell bízni magunkat, ami biztonsági kockázatokat rejt magában.

Hogyan akadályozza meg a Passkey az adathalászatot?

A Passkey tárolja a domain nevét, amihez tartozik. Hiába hoz létre valaki beékelődve a kommunikációba egy, az adott oldalra megtévesztésig hasonlító weblapot, hasonlító domain névvel, a böngésző nem küldi el a Passkey-t. (Ám, ha normál jelszót is alkalmazunk, akkor a csaló kérheti annak begépelését azt állítva, hogy a Passkey nem működik. Ha begépeljük a jelszót, akkor sikeres lehet az adathalász. Erre figyelni kell.)

A Passkey haszna

Aki használ jelszókezelőt, annak a Passkey kevéssé fokozza a biztonságát és egyszerűsíti a bejelentkezést. Aki még nem használ jelszókezelőt, annak már a jelszókezelő használata eleve biztonságfokozó fejlesztés.

Az olyan weblapok, amik kétlépcsős azonosítást (2FA) (SMS-sel, vagy alkalmazáson keresztüli megerősítés) (2FA) alkalmaznak, sokkal jobban kitettek az adathalász támadásoknak, mint a Passkey-eljárás, mivel a hamis weblapok a kommunikációba beékelődve lekérhetik az egyszeri kódot számunkra. A biztonsági kulcsos 2FA azonosítás védett az adathalászat ellen, itt a Passkey csak kényelmesebb lehet, mert eggyel kevesebb jelszót kell megjegyezni.

A Passkey támogatása jelenleg nem teljes. Gond van az eszközök és az operációs rendszerek közötti szinkronizációval Adam Langley állítja: A Windows Hello egyáltalán nem szinkronizál. A Google Password Manager csak Androidok között, a iCloud Keychain pedig csak Apple eszközök között szinkronizál. A Passkey-támogatással bíró, harmadik fél által készített jelszókezelők tudnak szinkronizálni, de nem támogatnak minden platformot. (Pl. az 1Password nem ad teljes támogatást Androidon a Passkey-hez. Passkey kipróbálható "eldobható" passkey.io-n, vagy webauthn.io-n létrehozott fiókokon.)

Követés weblapokon át

A követés megakadályozásnak feltétele, hogy eltérő honlapokon eltérő azonosítót használva (név, e-mail-, IP-cím) ne lehessen összekötni a személyazonosságot, még ha a honlapok meg is osztják egymással az információkat a háttérben. A Passkey ezt megakadályozza, bár hagy egy kiskaput. A honlapok lekérdezhetik a használt TMP, vagy biztonsági kulcs gyártóját és az eszköz típusát. Ez nem lenne gond, de egyes gyártók régebben minden egyes eszközt egyedi azonosítóval láttak el, ami elősegíti az azonosítást. Ilyen gyártói hiba a jövőben sem zárható ki. A webalapok a jelszókezelőkkel kapcsolatos információkat szintén lekérhetik.

Egyes biztonsági kulcsok minden egyes tárolt Passkey-hez számlálót adnak. El kell kerülni, hogy a számlálókat együtt tárolják, de ez nem minden biztonsági kulcs esetén valósul meg, így a weblapok azonosságokat, korrelációt kereshetnek az beazonosításhoz.

Egyéb megfontolások

Azonosítás – Passkey használata során az eszköz (telefon, számítógép) kérhet további azonosítást (biometrikus, PIN vagy alakzat). Az azonosítót nem küldi el, csak jelzi, hogy sikeres volt.

Megosztott fiókok – normál jelszóhasználat esetén, mivel mindenki ugyanazt a jelszót használja, nem derül ki, hogy pontosan ki használja a fiókot. Passkey esetén a fiókhoz mindenkinek önálló jelszót kell készítenie, amivel a bejelentkező személye azonosítható.

Eszköz elvesztése, vagy ellopása:

- ha Passkey-t tároló biztonsági kulcsot más szerzi meg, kilistázhatja az összes Passkey-weblap párost. (Vannak olyan biztonsági kulcsok, amik PIN-kódot kérnek a használatukhoz);

- jelszókezelő használata esetén, aki fizikailag hozzáfér a géphez, feltörheti a jelszókezelőt és láthatja a Passkey adatait, nem beszélve arról, hogy be is jelentkezhet oldalakra;

- titkos fiók esetén, ha más is hozzáférhet a gépedhez, biztonságosabb lehet a jelszóhasználat, kiegészítve inkognitó, vagy privát böngészési móddal. Ilyenkor az adathalászat nem zárható ki.

Felhő-tárolás

- az operációs rendszerek beépített, felhő alapú jelszókezelője (Windows Hello; Google Password Manager; iCloud Keychain), kényelmes megoldás lehet, de használatukhoz be kell jelentkezni. A rendszer felajánlhatja további adatok „szinkronizálását” (m. böngészési előzmények, könyvjelzők stb.), amiket érdemes kikapcsolni;

- használható harmadik fél jelszókezelője, ami nem próbál meg más adatokat szinkronizálni.

Összegzés

A Passkey jelentős előrelépés lehet a biztonság szinte ingyenes megteremtése felé, de még nincs teljesen kész, van tere a továbbfejlesztésének.

Magyar forrás a téma tanulmányozásához:
https://nki.gov.hu/it-biztonsag/tanacsok/passkey-elonyok-es-hatranyok/