N-ABLE™

PASSPORTAL

Jelszavak világnapja

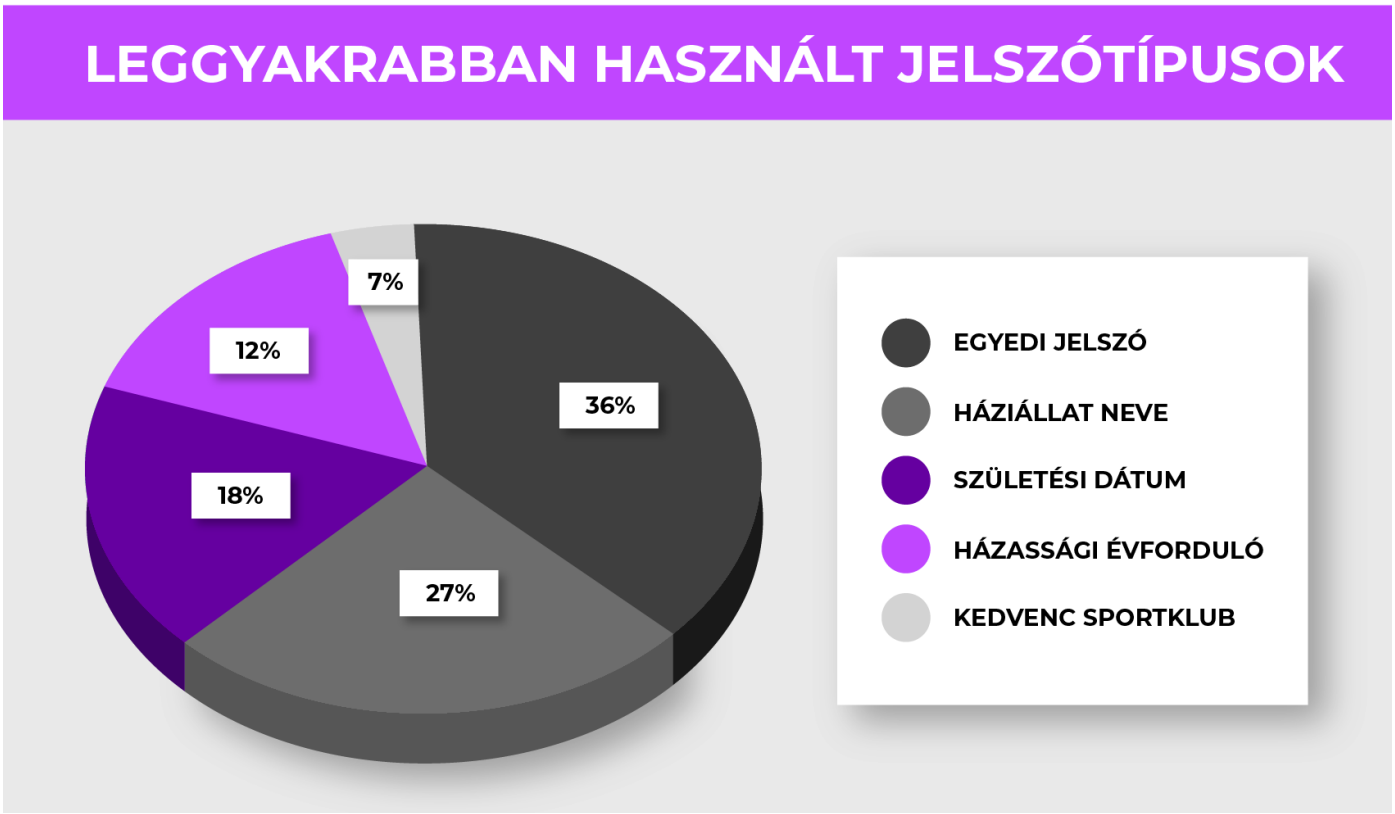
2022

A jelszavak világnapja alkalmából az N-able szakértői összeszedték a legfontosabb jelszóval kapcsolatos tippjeiket és gondolataikat. Egy dologban mindannyian egyetértettek: a jelszavakat ki kell egészíteni MFA-val (Multi-Factor Authentication – többfaktoros azonosítás) vagy minimum 2FA-val (Two-Factor Authentication – kétfaktoros azonosítás).

Fontos tények:

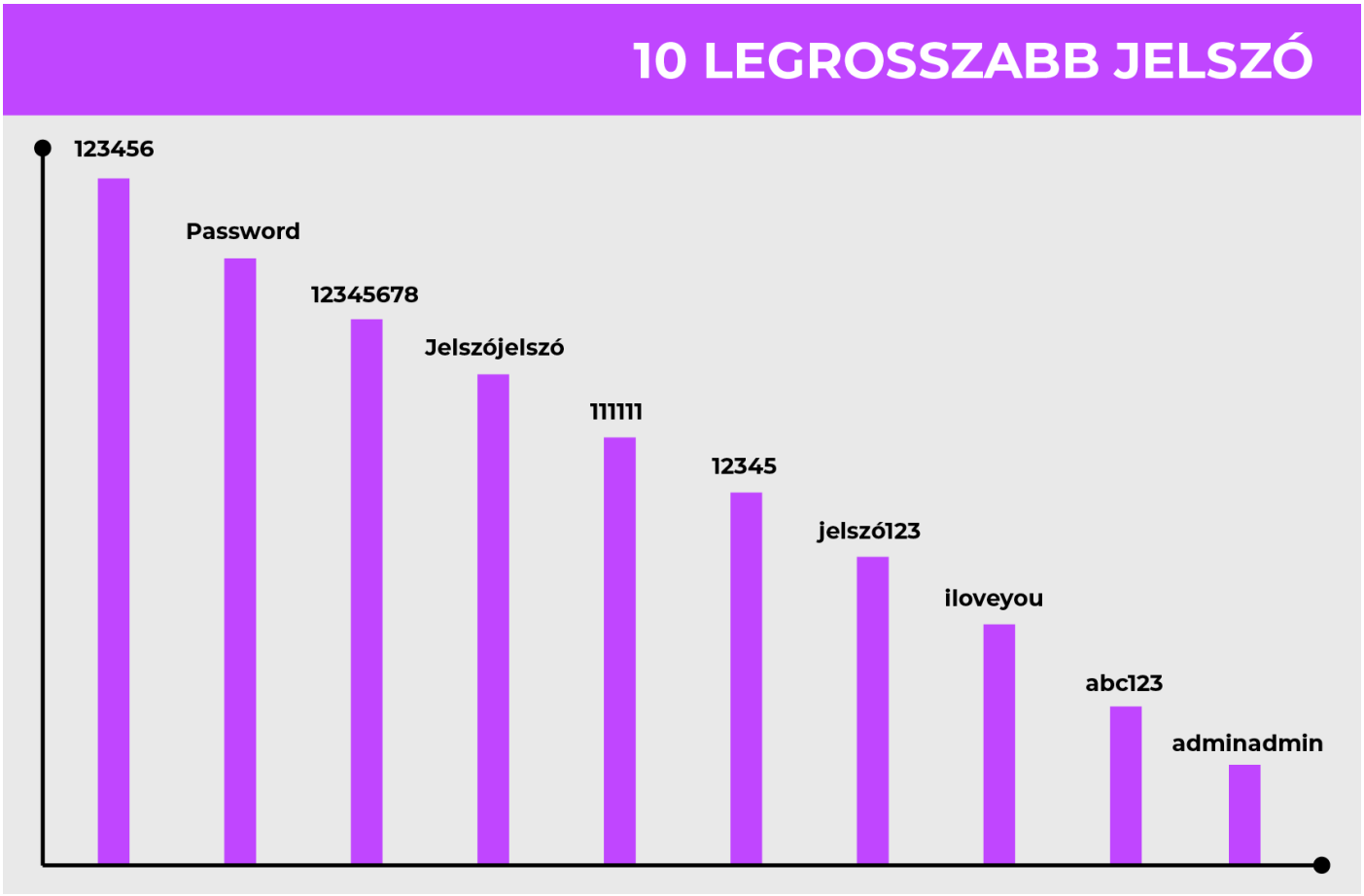
Az adatlopások közel 80%-át lopott, feltört jelszavakkal követik el. Természetesen léteznek más típusú támadások is - a rosszindulatú programoktól a social engineeringig -, de ez is mutatja, hogy a jelszavak központi szerepet játszanak bárki biztonsági helyzetében. Ezért kiemelten fontos, hogy a felhasználók mind otthoni, magán, mind pedig munkahelyi környezetükben is megfelelő jelszavakat használjanak, kiegészítve az előbb említett MFA-val vagy 2FA-val. Sőt, az sem árt, ha jelszómenedzsereket, jelszószéfeket alkalmaznak. A cégeknek pedig olyan remek megoldások állnak rendelkezésre, mint az N-able által nyújtott Passportal szolgáltatás, ami az automatizált, felhőalapú jelszókezelést és a hitelesítő adatok titkosított formában történő tárolását biztosítja.

Aggasztó például, hogy még mindig rengetegen használják jelszóként a házi állatuk nevét, vagy éppen a születési dátumukat. Az N-able adatai alapján kijelenthető, hogy az emberek nagy része még mindig nem használ egyedi, erős jelszavakat.



Még aggasztóbb tény az N-able szerint, hogy a Fortune 1000 alkalmazottak nagyjából 76%-a használta ugyanazt a jelszót a vállalati e-mail címéhez és másik fiókjaihoz is. Ez azt mutatja, hogy még az erős biztonsági intézkedéseket megengedni tudó nagyvállalatoknál is széles körben elterjedt jelszóproblémák vannak.

De még ennél is aggasztóbb, hogy a leggyakrabban használt jelszavak listája évről-évre ugyanazokat a jelszavakat tartalmazza. Ami önmagában nem lenne nagy baj. A gond az, hogy ezeket a jelszavakat rendszeresen használják is az emberek. Íme a top 10 legrosszabb jelszavak listája.



Tippek a sziklaszilárd jelszó eléréséhez.
A legfontosabb, hogy a felhasználók győződjenek meg az alábbiakról.

- Alkalmazzanak egyedi, erős jelszavakat. Legyenek eredetiek és kreatívak, akár használhatnak jelmondatokat is. Lényeg: legalább 8, de inkább még több karakterből álljon az alfanumerikus és speciális karaktereket tartalmazó jelszó.

- Az egyedi jelszavakhoz csak az adott illetékes személynek legyen hozzáférése.
- Használjanak többfaktoros (MFA) vagy kétfaktoros (2FA) hitelesítést.
- Ne jelentkezzenek be (vagy adják meg a hitelesítő adataikat) nem megbízható/ügyfél által használt eszközökről.
- Ne írják fel sehova sem a jelszavakat.
- Használjanak jelszókezelőt, jelszószéfet.
- Minden bejelentkezési felületen más jelszót használjanak.
- Alkalmanként cseréljék a jelszavakat.
- A régi jelszavakat NE használják fel újra.
- Időnként ellenőrizzék, hogy jelszavaik kompromittálódtak-e.
- A használatban lévő eszközök alapértelmezett jelszavait változtassák meg.
- Kerüljék a nyilvános wi-fi hálózatok használatát. Ha mégis csatlakoznak egy ilyenre, akkor ne lépjenek be olyan oldalakra, ahol a belépéshez jelszót kell megadni. Nyilvános hálózatok használata esetén kényes, például online banki tevékenységeket ne végezzenek.
- Frissítsék a böngészőjüket. A régi böngészőverziókban biztonsági rések lehetnek, így édemes azonnal frissíteni, amint felajánlja a böngésző azt.

Pár jótanács a cégeknek:

- A cégek alkalmazzák a zero trust elvét.
- Korlátozzák a root/admin /superuser/biztonsági tisztviselő szerepkörök számát.
- Használjanak többfaktoros (MFA) hitelesítést a szervezeten belül.
- Alkalmazzanak megfelelő jelszóválasztási kritériumokat. A kellően egyedi és hosszú jelszó / jelmondat mellett fontos, hogy a munkavállalók kerüljék a számok használatát a jelszó végén - ez egy meglehetősen gyakori minta, és a bűnözők könnyen felismerik. A számok és szimbólumok lehetőleg a jelszó elején szerepeljenek.
- Emellett próbáljanak meg olyan szabályt bevezetni, amely megköveteli a munkavállalóktól, hogy rendszeresen változtassák meg jelszavaikat. Ez lehetővé teszi a jelszófrissítési szabályok naprakészen tartását, és biztosítja, hogy a felhasználók a legújabb irányelveket kövessék, ugyanakkor korlátozza a kárt, ha a kiberbűnözők ellopnak néhány jelszót.
- Használjanak jelszókezelő alkalmazásokat. Ha a cégek nem teszik viszonylag egyszerűvé a munkavállalók számára a megfelelő jelszókezelést, akkor valószínűleg nem fogják követni a legjobb kiberhigiéniai gyakorlatokat.

Olyan eszközöket kell biztosítaniuk számukra, amelyek megkönnyítik ezeket a helyes gyakorlatokat.

- ◊ Mindezek a tippek még fontosabbá válnak MSP-k esetében. A jó jelszó- és dokumentációkezelés kritikus fontosságú, ha több ügyfél több rendszerét kell kezelnie. Az N-able Passportal megoldása segíthet ennek hatékony kezelésében, növelve a technikusok hatékonyságát azáltal, hogy a privilegizált jelszavakat és az ügyfélismereteket kéznél tartják.
- ◊ A cégek bizonyos időközönként szervezzenek IT biztonsági oktatásokat, képzéseket. A munkavállalók tudatosságra nevelése nagy szerepet játszik egy-egy cég biztonsági helyzetében.

A jelszavakkal kapcsolatos legnagyobb kihívás az, hogy egyszerűen macerás a kezelésük. Sokan természetesen a kényelmet választják a biztonság helyett, ezért fontos, hogy megpróbáljuk megkönnyíteni az életüket. Ezért olyan fontos egy jó jelszókezelő megoldás használata. A felhasználók egyszer bejelentkezhetnek a fő jelszavukkal, majd egyetlen kattintással bejelentkezhetnek számtalan fiókjukba egy automatikusan generált jelszóval. Nincs szükség végtelen kreativitásra az új jelszavak kitalálásához, és nincs szükség fotografikus memóriára ahhoz, hogy megjegyezzék azokat. Ráadásul egy olyan **jelszókezelő eszközzel, mint az N-able Passportal**, jelszókövetelményeket állíthat be a végfelhasználók számára, szükség szerint automatizálhatja a jelszófrissítést, és szükség szerint engedélyezheti vagy visszavonhatja a fiókokhoz való hozzáférést. **A Passportal, az MSP-k számára tervezett jelszókezelő lehetővé teszi, hogy automatikusan jelszavakat generáljon, és szükség esetén könnyen engedélyezhető és visszavonható egy-egy hozzáférés.**