NEMZETI KIBERVÉDELMI INTÉZET

GOVCERT

Az adatvédelem minden felhasználó alapvető érdeke, ezért a Nemzeti Kibervédelmi Intézet (NKI) az állami kibervédelem támogatásán, fenntartásán és fokozottabb működtetésén túl az egyéni felhasználók tudatosítására is egyre nagyobb hangsúlyt helyez.

Az NKI célja, hogy az IT biztonságot érintő tematikus tájékoztatói segítségével a lehető legtöbb hasznos információt jutassa el a felhasználók részére.

Nemzeti Kibervédelmi Intézet
GovCERT-Hungary
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: cert@govcert.hu

Mindennapi jelszavaink

Készült a Nemzeti Kibervédelmi Intézet megbízásából, az Ön informatikai egészségének megőrzése érdekében.

Mindennapi jelszavaink

A támadók célja, hogy a jelszavainkat megszerezve hozzáférjenek a szervezet számítógépes rendszeréhez.

A támadóknak sokszor elegendő, ha csupán egy felhasználó jelszava feltörhető a rendszerben, ezt kihasználva a teljes rendszert kompromittálhatják.

A támadók a jelszavainkat automatizált módon próbálják meg kitalálni, ennek két elterjedt módja:

brute force (nyers erő) támadással: a lehetséges karakterek kombinációiból próbálják a jelszót összeállítani.

„szótár alapú" támadással: értelmes szavakat, gyakran használt jelszavakat tartalmazó lista elemeit, azok kombinációit felhasználva próbálják meg feltörni jelszavunkat.

Mit is jelent ez a hétköznapokban?

A számítógépes rendszerekbe a felhasználónevünk és jelszavunk segítségével tudunk belépni.

Amikor az adott rendszerhez (pl.: levelezésünkhöz) hozzáférést nyerünk, a naplózó rendszer a felhasználónévhez rendelve rögzíti a tevékenységünket.

Ha valaki megszerzi a felhasználónevünket és a hozzá tartozó jelszót, minden olyan adathoz hozzáférhet, amelyhez mi is, illetve használhatja ezt a hozzáférést ugródeszkaként más rendszerek eléréséhez.

A rendszer szemszögéből ez olyan, mintha mi hajtanánk végre az adott műveleteket, így amit a támadó tesz, a mi nevünkben kerül rögzítésre a rendszer naplóállományaiban, ami alapján minket vonhatnak felelősségre.

A jelszavainkat gondosan kell megválasztanunk és körültekintően kell kezelnünk.

HOGYAN VÁLASSZUNK ERŐS JELSZÓT:

- ne legyen ránk jellemző, mert kevés infomáció birtokában is könnyen kitalálható (pl.: családtag neve + születési dátum egy rövid kereséssel a közösségi oldalakon kideríthető);
- nem szerencsés, ha a jelszó csak egy szóból áll (pl.: az "almafa" szó biztosan szerepel egy támadó által kipróbálandó jelszavak listájában);
- jó, ha a jelszó hosszú és több féle karaktert (kisbetű, nagybetű, szám, írásjel) tartalmaz, mert ezzel megnehezíti a brute force technikával való feltörést;
- a legjobb, ha néhány szóból álló jelmondatot választunk, amelyben van kisbetű, nagybetű és írásjel is. Ezt könnyű megjegyezni, azonban nehéz kitalálni, feltörni pedig szinte lehetetlen.

JELSZAVAK KEZELÉSE:

- fontos, hogy ne adjuk "kölcsön" a jelszavunkat, hiszen nem tudhatjuk, hogy az adott személy körültekintően fogja-e kezelni;
- ne írjuk fel a jelszavunkat, ez elveszhet, könnyen illetéktelen kezekbe kerülhet;
- ne használjuk mindenhol ugyanazt a jelszót, ha a támadók az egyiket megszerzik, minden más rendszerünkhöz hozzáférhetnek;
- rendszeresen változtassuk meg a jelszavunkat, a támadónak minél több ideje van próbálkozni, annál nagyobb valószínűséggel tudja megszerezni a hozzáférésünket.