Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadásban...

Ha már egyszer feltörtek …

Áttekintés

Mindnyájunkat foglalkoztat a számítógépünk és mobil eszközeink biztonsága, amelynek érdekében természetesen lépéseket is teszünk. Azonban nem számít, hogy milyen biztonságosan használjuk a technológiát, előbb vagy utóbb mindenkit elérhet a végzet, amikor „feltörik” az eszközünket. E havi hírlevelünkben bemutatjuk, hogy mik utalnak arra és mit tehetünk, ha valaki sikeresen feltörte a számítógépünket vagy mobil eszközünket. Végtére is, minél hamarabb észrevesszük és minél előbb reagálunk a veszélyre, annál kisebb kárt okozhatnak a támadók.

A szerzőről

Samantha Davison (**@sam_e_davison**) az Uber biztonság tudatossági és oktatási program menedzsere, aki világszerte 350 városban felel az alkalmazottak képzéséért.

Gyanús jelek

Általában nem könnyű felismerni, ha valaki sikeresen feltörte a gépünket, mivel ennek felismerésére gyakran nincs kézzel fogható bizonyíték. Viszont a támadók számos nyomot hagynak maguk után, amelyeket indikátoroknak szokás nevezni. Minél több gyanús jelet észlelünk, annál valószínűbb, hogy feltörték azt.

- A víruskereső program jelzi, hogy a rendszer fertőzött, különösen akkor, ha azt mondja, nem tudja eltávolítani vagy karanténba helyezni a gyanús fájlokat.
- A böngésző kezdőoldala váratlanul megváltozott, vagy olyan oldalt nyit meg, amit nem akarunk.
- Olyan új felhasználói fiók van a számítógépen, amit nem mi hoztunk létre, vagy olyan programok futnak, amit nem mi telepítettünk.
- Az alkalmazások vagy akár a számítógép folyamatosan összeomlik, újraindul, ismeretlen alkalmazások ikonjai jelennek meg, vagy furcsa ablakok ugranak fel.
- Egy program engedélyt kér arra, hogy módosítást végezzen el a számítógépen, bár nem telepítettünk vagy frissítettünk semmit.
- A helyes jelszóval nem tudunk bejelentkezni a rendszerünkbe vagy egy online fiókba.
- Barátok kérdezik, hogy miért küldünk nekik kéretlen leveleket, amikor biztosak vagyunk abban, hogy semmit nem küldtünk.
- A mobil eszközünk engedély nélkül küld emelt szintű számra SMS üzenetet.

Ha már egyszer feltörtek …

- A mobil eszközünk hirtelen minden magyarázat nélkül sok adatot forgalmaz, vagy gyorsan lemeríti az akkumulátort.

Előbb vagy utóbb a mi rendszerünket is feltörik. Minél előbb ismerjük fel és reagálunk a támadásra, annál kisebb kárunk keletkezik.

Mit tehetünk?

Amennyiben úgy gondoljuk, hogy feltörték a rendszerünket, akkor a minél gyorsabb reakció a legjobb lépés. Ha a szóban forgó eszközt a munkáltató biztosította, vagy munka céljára van fenntartva, akkor ne akarjuk mi magunk megoldani a problémát. Nem csak azért, mert több kárt okozhatunk, mint hasznot, hanem azért is, mert olyan értékes bizonyítékokat tüntethetünk el, amelyek segíthetik a nyomozást. Ehelyett inkább azonnal vegyük fel a kapcsolatot az ügyfélszolgálattal vagy az informatikai biztonsági csoporttal. Amennyiben nem lehetséges felvenni a kapcsolatot a fent említettekkel, akkor a kérdéses eszközt válasszuk le a hálózatról, kapcsoljuk ki (esetleg tegyük alvó vagy hibernált módba). Még ha nem is vagyunk biztosak abban, hogy feltörték a gépünket, akkor is jelentsük az esetet! Amennyiben a készülék a saját tulajdonunk, akkor az alábbi lépéseket javasoljuk megtenni:

- **Jelszóváltoztatás**: nem csak az adott számítógép vagy mobil eszköz jelszavát kell ilyenkor lecserélni, hanem minden online felhasználói fiókét is, és ezt ne a feltört számítógépről végezzük el, hanem egy olyan másikról, amely esetében biztosak lehetünk abban, hogy elég biztonságos ehhez a művelethez.
- **Víruskereső program**: ha a szoftver tájékoztat bennünket arról, hogy fertőzött fájlt talált, kövessük a tanácsait, ami általában a fájl karanténba helyezése, megtisztítása vagy törlése. A víruskereső programok rendszerint internetes hivatkozásokat is ajánlanak, ahol többet is megtudhatunk a szóban forgó káros szoftverről. Ha kétségünk van tegyük karanténba a fájlt! Ha ez nem lehetséges, akkor töröljük!
- **Újratelepítés**: ha nem tudjuk kijavítani a fertőzés okozta károkat vagy ha teljesen biztosra akarunk menni, hogy semmilyen káros szoftver sem marad a rendszerünkön, akkor egy biztosabb megoldás az újratelepítés. Számítógép esetén kövessük a gyártó utasításait! A legtöbb esetben beépített szolgáltatások vannak a teljes újratelepítésre. Abban az esetben, ha ezek a lehetőségek nem állnak rendelkezésre (sérült, fertőzött, stb.), akkor vegyük fel a kapcsolatot a gyártóval, vagy látogassuk meg a weboldalukat! Soha ne telepítsük a rendszert egy korábbi biztonsági másolatból, mert az olyan sérülékenységeket tartalmazhat, amelyeken keresztül a támadó már sikeresen megfertőzte a rendszert. A biztonsági mentéseket csak az adatok helyreállítására használjuk! A mobil eszközök esetén kövessük a készülék gyártójának vagy a szolgáltatónak az utasításait, amiket megtalálhatunk a weboldalukon. A legtöbb esetben ez annyit jelent, hogy visszaállítjuk az eredeti gyári beállításokat. Amennyiben nem érezzük eléggé felkészültnek magunkat

Ha már egyszer feltörtek …

ehhez, vegyük igénybe szakértő segítségét! Amennyiben a számítógép vagy mobil eszköz már régi darab, lehet, hogy jobban járunk egy új vásárlásával. Végezetül pedig, ha sikeresen újratelepítettük az eszközt, kapcsoljuk be az automatikus frissítést, hogy mindig naprakészen tudjuk tartani.

- **Biztonsági mentés**: a védekezés legfontosabb lépése a rendszeres biztonsági mentés készítése, amely minél gyakoribb, annál jobb. Vannak olyan megoldások, amelyek akár óránként képesek menteni az új vagy megváltozott fájlokat. Függetlenül attól, hogy milyen megoldást veszünk igénybe, rendszeresen ellenőrizzük, hogy képesek vagyunk visszaállítani a mentésből az adatokat. Elég gyakran a biztonsági mentések visszaállítása az egyetlen mód, hogy egy betörés után helyreállítsuk a rendszert.
- **Hatóság értesítése**: ha úgy érezzük, hogy bármilyen módon fenyegetve vagyunk, értesítsük a rendőrséget!

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a http://www.securingthehuman.org weboldalon keresztül.

Magyar Kiadás

Kormányzati, távközlési és informatikai szolgáltatóként, Magyarország egyik stratégiai fontosságú gazdasági társasága a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Társaságunk kiemelt feladata a kormányzati infrastruktúra működtetése, az e-közigazgatási megoldások támogatása, valamint kormányzati szintű informatikai szolgáltatások nyújtása. További információ a http://www.nisz.hu oldalon olvasható.

Hivatkozások

Biztonsági mentés és helyreállítás: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_hu.pdf

A jelmondatokról: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_hu.pdf

A káros szoftverek: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_hu.pdf

Az új tablet és a biztonság: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201601_hu.pdf

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Fordította: Birkás Bence, Árvai Gábor, Pál Benyó