OUCH! | 2016. június

Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadásban...

- **Mit nevezünk titkosításnak?**
- **Mire használhatjuk a titkosítást?**
- **Csináljuk jól!**

Titkosítás

Mit nevezünk titkosításnak?

Mindannyian hallhattuk már azt a kifejezést, hogy titkosítás, illetve azt is, hogy ennek segítségével hogyan kellene megvédenünk magunkat és adatainkat. Azonban a titkosítás nem biztos, hogy mindenki számára egyértelmű, és tisztában kell lennünk a technológia lehetőségeivel és határaival. A mostani hírlevelünkben egyszerű kifejezésekkel mutatjuk be, hogy mi az a titkosítás, hogyan véd meg bennünket, és hogyan használhatjuk megfelelően.

A szerzőről

Francesca Bosco (**@francibosco**) kutató, kiberbiztonsággal, kiberbűnözéssel és a technológiai visszaélésekkel kapcsolatos projekteken dolgozik az ENSZ Interregionális Bűnügyi és Igazságügyi Kutató Intézeténél, ahol társalapítója a Tudományos és Jogi Központnak.

Hatalmas mennyiségű személyes információt tárolunk a különböző eszközeinken dokumentumok, képek, email-ek formájában. Ha volt már példa arra, hogy elhagytuk vagy ellopták a mobil eszközünket, akkor az összes személyes információnkat megszerezhették azok, akik hozzáfértek a készülékhez. Ráadásul akár az elvégzett online banki műveletek vagy webshop-os vásárlások bizalmas információi is – mint például a bankszámla vagy bankkártyaszám is – illetéktelen kézbe kerülhet. A titkosítás segíthet az ilyen esetekben azzal, hogy idegenek nem tudják elolvasni vagy módosítani az információkat.

A titkosítást már évezredek óta használjuk. A ma használatos módszerek már nagyon kifinomultak, de végeredményben ugyanazt a célt szolgálják – üzenetet küldeni egyik helyről a másikra, miközben biztosak lehetünk abban, hogy csak az tudja elolvasni, akinek eredetileg is szántuk. A nem titkosított információt egyszerű szövegnek, más néven „plain-text”-nek nevezzük. Ez azt jelenti, hogy bárki könnyedén hozzáférhet, és el tudja olvasni. A titkosítás ezt az egyszerű szöveget átalakítja egy nem olvasható formára, amit titkosított szövegnek, más néven „cipher-text”-nek hívunk. A manapság használt titkosítások összetett matematikai műveleteket és egy egyedi kulcsot használnak a titkosított szövegek előállításához. A kulcs az, ami „nyitja” vagy „zárja” a titkosítással védett adatot, ez pedig a legtöbb esetben egy jelszó vagy jelmondat.

Mire használhatjuk a titkosítást?

Alapvetően kétféle információt kell titkosítással védeni: azt, amit a telefonon tárolunk, illetve azt, ami épp úton van egyik pontból a másikba (például üzenet küldünk vagy épp fogadunk).

Titkosítás

A mobil eszközön tárolt adatok titkosítása életbevágó arra az esetre, ha elvesztenénk vagy ellopnák tőlünk a készüléket. A ma használatos eszközökön már hatalmas mennyiségű személyes és más bizalmas információ gyűlhet össze, viszont nagyon könnyű elveszíteni. Ezen felül más típusú hordozható eszközök (pendrive, külső merevlemez) is tartalmazhatnak olyan információkat, amiket nem szeretnénk mások kezében látni. A teljes lemeztitkosítás (Full Disk Encryption - FDE) egy széles körben használt titkosítási technológia, amely a teljes merevlemezt titkosítja. Ez azt jelenti, hogy minden automatikusan titkosításra kerül a rendszeren, tehát nem kell nekünk dönteni arról, hogy mi legyen, és mi ne legyen titkosítva. Manapság a számítógépek többsége már teljes mértékben támogatja a teljes lemeztitkosítást, bár azt még nekünk kell eldöntenünk, hogy be legyen-e kapcsolva. A Mac gépeken ezt FileVault-nak, a Windows-os rendszereken pedig Bitlocker-nek vagy eszköztitkosításnak (Device Encryption) nevezik. A legtöbb mobil eszköz szintén támogatja az FDE-t. Az iOS és iPad készülékek automatikusan bekapcsolják, amint első alkalommal beállítjuk a jelszavas védelmet. Az Android 6-os verziójától (Marshmallow) kezdődően a Google megköveteli az FDE bekapcsolását, amennyiben a készülék hardvere teljesíti a minimum elvárásokat.

A titkosítás megfelelő módszer az adataink biztosítására, de csak annyira erős, amennyire a használt kulcs is az.

Az információ akkor is veszélyben van, amikor elküldjük valahova, így amennyiben nincs titkosítva, könnyedén le lehet hallgatni, vagy akár módosítani is lehet. Ezért szükséges titkosítani minden bizalmas adatot és kommunikációt. Az online adatok titkosításának leggyakoribb módszere a HTTPS, ami azt jelenti, hogy minden adat, ami a böngészőnk és a weboldal között halad, az titkosításra kerül. Ha egy zárt lakat ikont látunk a https:// mellett, esetleg az egész címsor (ahova az URL-t írjuk) zöldre vált, akkor titkosított adatkapcsolat jött létre. Egy másik példa lehet, ha email-t küldünk vagy fogadunk. A legtöbb levelezőprogramnak megvan a képessége a titkosításra, de lehet, hogy engedélyeznünk kell azt. Vagy például ott vannak a chat alkalmazások, mint az iMessage, Wickr, Signal, WhatsApp vagy Telegram. Az ilyen alkalmazások is képesek arra, hogy a két végpont közti adatátvitelt titkosítsák, így harmadik fél nem képes hozzáférni ahhoz, vagyis csak a küldő és a fogadó képes elolvasni az üzeneteket.

Csináljuk jól!

Annak érdekében, hogy valóban jól működő titkosítást használjunk, érdemes betartani az alábbi szempontokat:

- A titkosítás pontosan olyan erős, mint a használt kulcs. Ha valaki kitalálja vagy megszerzi a kulcsunkat, hozzá fog férni minden adatunkhoz. Védjük meg a kulcsot! Ha jelszót használunk, akkor az legyen kellően erős és egyedi! Minél

Titkosítás

hosszabb a jelszó, a támadónak annál több időbe kerül feltörnie azt. Azonban ha elfelejtjük a jelszót, akkor többé nem fogunk hozzáférni a saját adatainkhoz. Használjunk jelszókezelő programot, a jelszavak biztonságos tárolásához.

- A titkosítás erőssége függ magától az eszköz biztonságosságától is. Ha egy támadó feltöri, vagy káros szoftverrel fertőzi meg az eszközt, akkor lehetősége nyílik megkerülni a titkosítást. Ezért nagyon fontos, hogy megtegyük az olyan megfelelő lépéseket a készülék biztonságossá tételéhez, mint például a víruskereső program és erős jelszó használata, valamint az eszköz folyamatos karbantartása, frissítése.
- Manapság már sok mobil vagy számítógépes alkalmazás tudja használni a modern titkosítási módszereket az adatok és a kommunikáció védelme érdekében. Amennyiben az általunk használtak nem képesek erre, érdemes alternatív megoldások után kutatni.

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a securingthehuman.sans.org/ouch/archives 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

A titkosításról:	http://www.biztonsagosinternet.hu/hu/tippek/61
A jelmondatokról:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_hu.pdf
Jelszókezelő programokról:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_hu.pdf
A káros szoftverekről:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_hu.pdf
Az új tablet biztonságáról:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201601_hu.pdf

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

