SANS SECURITY AWARENESS
NEMZETI KIBERVÉDELMI INTÉZET
OUCH! | 2018. Január
Havi biztonság tudatossági hírlevél mindenkinek

OUCH!

ebben a kiadásban...

- **Vezeték nélküli hálózat**
- **Eszközök**
- **Jelszavak**
- **Biztonsági mentések**

Otthoni Informatikai Biztonság

Áttekintés

Néhány évvel ezelőtt az otthoni informatikai biztonság megteremtése egyszerű feladat volt. A legtöbb otthonban nem volt több, mint egy vezeték nélküli hálózat és néhány számítógép. Mára a technológia jóval összetettebbé vált, és életünk minden részébe integrálódott a mobil készülékektől és a játékkonzoloktól kezdve az otthoni (okos) termosztáton át a hűtőszekrényig bezárólag. Az alábbi négy lépés segítségével megteremthetjük az otthoni informatikai biztonságot.

A szerzőről

Matt Bromiley napközben incidenskezelő munkakörben dolgozik, mely során segít a különböző nagyságú ügyfeleinek megbirkózni adatbiztonsági problémáikkal. Matt ezen felül oktató a FOR508 Magas Szintű Informatikai Szakértés és Incidenskezelés című, SANS tanfolyamon is. Mattet a **@mbromileyDFIR** azonosítót bejelölve követhetjük.

Vezeték nélküli hálózat

A legtöbb otthoni hálózat rendelkezik a vezeték nélküli (vagy Wi-Fi) eléréssel– ennek segítségével csatlakozik minden eszköz az Internethez. A legtöbb vezeték nélküli hálózatot az otthoni Internetes útválasztó, vagy egy külön, vezeték nélküli hozzáférési pont vezéreli. Mindkét eszköz hasonló módon működik: vezeték nélküli jeleket sugároznak, amiken keresztül az eszközök csatlakoznak a hozzáférési ponthoz. Ez azt jelenti, hogy a vezeték nélküli hálózat biztonságosabbá tétele az otthonunk biztonságának alapköve. A következő lépéseket javasoljuk a biztonság megerősítése érdekében:

- Változtassuk meg az útválasztó, vagy a hozzáférési pont alapértelmezett adminisztrátori jelszavát – bármelyik is vezérli az otthoni hálózatot. Az adminisztrátori felhasználói fiókkal lehet a vezeték nélküli hálózat beállításait módosítani.
- Bizonyosodjunk meg arról, hogy csak azok csatlakozhatnak a hálózatunkhoz, akikben megbízunk. Ezt erős védelmi beállítások alkalmazásával érhetjük el a legkönnyebben. Jelenleg a WPA2-nek nevezett biztonsági megoldás használata a legjobb választás. A WPA2 engedélyezésével a csatlakozni kívánó felhasználóknak egy jelszót kell megadniuk, és amint sikeresen csatlakoztak, a hozzáférési pont és a felhasználók közti kapcsolat titkosított is lehet.
- Győződjünk meg arról, hogy a csatlakozáshoz megfelelően erős jelszót választottunk, valamint, hogy az a jelszó nem egyezik meg a korábban beállított adminisztrátori jelszavunkkal. Ne feledjük, hogy ezt a jelszót csak egyszer szükséges megadni minden csatlakoztatott eszköz esetében, mert az eszközök azt eltárolják és emlékeznek rá.
- A legtöbb vezeték nélküli hálózat támogatja az úgynevezett vendég hálózatokat, melyek lehetővé teszik, hogy a vendégek csatlakozzanak az internetre, miközben megvédi az otthoni hálózatunkat úgy, hogy a vendégek nem csatlakozhatnak más, a hálózathoz kapcsolódó eszközhöz. Ha vendég hálózat alkalmazását választjuk, bizonyosodjunk meg róla, hogy a WPA2 engedélyezve van, valamint ehhez a hálózathoz is állítsunk be egyedi jelszót.

Otthoni Informatikai Biztonság

Bizonytalanok vagyunk a fenti lépések megtételében? Kérjük meg az Internetszolgáltatónkat, hogy ellenőrizze a weboldalunkat, vagy tekintse át a hozzáférési ponthoz kapott dokumentációt, esetleg ellenőrizze a gyártó weboldalát.

Kövessük ezt a négy lépést az otthoni informatikai biztonságunk megteremtése érdekében: tegyük biztonságossá az otthoni Wi-Fit, engedélyezzük az automatikus frissítések letöltését, használjunk egyedi jelmondatokat, és engedélyezzük a biztonsági mentéseket.

Eszközök

A következő lépés az, hogy tudjuk milyen eszközök csatlakoznak a vezeték nélküli hálózatunkhoz, valamint, hogy bizonyosodjunk meg arról, hogy ezek az eszközök biztonságosak. Ez régebben viszonylag egyszerű volt, amikor még csak egy-két számítógépünk volt. Napjainkban már szinte minden eszköz csatlakoztatható az otthoni hálózatunkhoz, beleértve az okostelefonokat, a TV-ket, a játékkonzolokat, babamonitorokat, HIFI berendezéseket, és még talán a gépjárműveket is. Amint sikerül minden, hálózathoz csatlakoztatott eszközt azonosítanunk, meg kell győződnünk arról, hogy ezek az eszközök biztonságosak. A legegyszerűbb módja ennek az, ha minden eszközön, ahol lehetséges, engedélyezzük az automatikus frissítéseket. A kiberbűnözők folyamatosan tárnak fel újabb és újabb gyengeségeket a különböző eszközökben és operációs rendszerekben. Az automatikus frissítés engedélyezésével a számítógépünk és más eszközeink minden esetben a legfrissebb alkalmazást futtatják, ami megnehezíti, hogy bárki feltörhesse azokat.

Jelszavak

A következő lépés az erős és egyedi jelszavak használata minden eszköz, és felhasználói fiók esetében. A kulcsszavak az erős és az egyedi. Elegünk van már azokból a jelszavakból, amiket nehéz megjegyezni és leírni? Másoknak is. Használjunk inkább jelmondatokat. Ez egy olyan jelszó, ami olyan szavak sorozatát tartalmazza, amikre könnyű emlékezni, mint például “Hol van a kávém?”, vagy “elhagytam-a-mosolygós-fánkokat”. Minél hosszabb a jelmondat, annál erősebb is. Az egyedi jelszó azt jelenti, hogy minden eszközhöz és felhasználói fiókhoz más jelszót használunk. Ezzel a megoldással, még ha egy jelszavunk ki is tudódik, minden más eszközünk és felhasználói fiókunk biztonságban lesz. Nem tudjuk megjegyezni a sok erős, egyedi jelszót? Nem kell aggódnunk, mert mások sem! Ezért is javasolt, hogy használjunk jelszókezelőt, egy olyan különleges biztonsági programot, ami biztonságosan és titkosított módon tárolja el jelszavainkat egy virtuális páncélszekrényben.

Végezetül, ahol csak lehet de leginkább az online felhasználói fiókok esetében, használjunk kétfaktoros autentikációt. A kétfaktoros autentikáció sokkal erősebb: jelszavakat használ ugyan, de hozzáad egy második lépést is, mint például egy titkos kód elküldése az okostelefonra, vagy egy alkalmazás az okostelefonra telepítve, ami a kódot generálja. A kétfaktoros autentikáció valószínűleg az egyetlen, legfontosabb lépés, amit megtehetünk, hogy megvédjük magunkat online, és a használata sokkal egyszerűbb, mint gondolnánk.

Otthoni Informatikai Biztonság

Biztonsági mentések

Néha, bármilyen óvatosak is vagyunk, megtörténhet, hogy hackelés áldozatául esünk. Ebben az esetben leggyakrabban az egyetlen módja annak, hogy visszaszerezzük személyes adatainkat, hogy azokat visszaállítjuk egy biztonsági mentésből. Bizonyosodjunk meg arról, hogy rendszeresen készítünk biztonsági mentéseket a fontosnak ítélt adatainkról, és ellenőrizzük a mentett adatok visszaállíthatóságát is. A legtöbb mobil készülék támogatja a biztonsági mentések felhőbe történő mentését. A legtöbb számítógép esetében viszont előfordulhat, hogy biztonsági mentő szoftvert, vagy szolgáltatást kell vásárolnunk, ami relatíve olcsó megoldás, és a használatuk is egyszerű.

További információ

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

Magyar Kiadás

A Nemzeti Kibervédelmi Intézet (NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. A Nemzeti Kibervédelmi Intézet rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a magyar kibertér biztonságának erősítéséhez. További információ az Intézetről a http://www.govcert.hu/ és a http://neih.gov.hu oldalon olvasható.

Hivatkozások

Jelmondatok:	https://securingthehuman.sans.org/ouch/2017#april2017
Jelszókezelők:	https://securingthehuman.sans.org/ouch/2017#september2017
Kétfaktoros autentikáció:	https://securingthehuman.sans.org/ouch/2017#december2017
Biztonsági mentések:	https://securingthehuman.sans.org/ouch/2017#august2017

Szerkesztette: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Fordította: Tikos Anita

