OUCH! | augusztus 2018


OUCH!

SANS SECURITY AWARENESS

Havi biztonság tudatossági hírlevél mindenkinek

# Okos Otthoni Eszközök

## Mik azok az okos otthoni eszközök?

Hagyományosan csak néhány otthoni eszközünk tudott csatlakozni az internethez, mint például a laptopunk, az okostelefonunk vagy a játékkonzolunk. Napjainkban mindazonáltal egyre több eszköz csatlakozik az internethez, az okos villanykörtétől kezdve a hangszórókon keresztül akár a televíziókészülék, zárak, sőt akár az autónk is. Hamarosan szinte minden, otthoni háztartásban található eszköz csatlakoztatható lesz az internethez. Ezeket a csatlakoztatott eszközöket gyűjtőnéven a dolgok internetének (Internet of Things, IoT), vagy okos otthoni eszközöknek nevezzük. Miközben ezek az eszközök nagy szolgálatot tesznek nekünk a kényelem tekintetében, sajátos veszélyeket is magukban hordoznak.

## Mi a probléma?

Minél több eszköz csatlakozik az otthoni hálózatunkra, annál több baj történhet. A hackerek úgy programozhatják az eszközeinket, hogy azok megtámadjanak másokat, a gyártók széles körben gyűjthetnek információkat a tevékenységünkről, vagy az eszközeink megfertőződhetnek, és akár ki is zárhatnak minket magából az eszközből. A legtöbb gyártóknak, akik ezeket az eszközöket előállítják, nincs tapasztalatuk a kiberbiztonság területén, és a biztonságra csak költséghelyként tekintenek. Ennek eredményeképpen, a legtöbb eszköz amit megvásárolunk egyáltalán nem rendelkezik védelemmel, vagy csak igen alacsony szintűvel. Például egyes készülékek mások által is jól ismert alapértelmezett jelszavakat használnak, vagy az eszközök vezérlő programjait nem lehet frissíteni vagy konfigurálni.

## Hogyan védhetjük meg magunkat?

Szóval mit tehetünk? Egyértelmű célunk, hogy a csatlakoztatott eszközeinket biztonságosan tudjuk vezérelni. Ezek az eszközök csodálatos képességekkel rendelkeznek, melyek megkönnyítik az életünket. Mindezeken túl, ahogy a technológia fejlődik, nem marad más választásunk, minthogy használjuk ezeket az “okos” eszközöket. A következőekben találhatóak a legfontosabb lépések, amiket megtehetünk a biztonságunk érdekében.

**Csak azt csatlakoztassuk, amire igazából szükségünk van:** A legegyszerűbb módja egy eszköz biztonságossá tételének, ha nem csatlakoztatjuk azt az internethez. Ha nincs arra szükségünk, hogy az eszközünk online legyen, ne csatlakoztassuk azt a WiFi hálózathoz. Tényleg szükségünk van arra, hogy a kenyérpirítónk értesítéseket küldjön a telefonunkra?

**Legyünk tisztában azzal, mit csatlakoztatunk:** Milyen eszközeink csatlakoznak az otthoni hálózatunkhoz? Nem vagyunk biztosak benne, vagy nem emlékszünk rá? Kapcsoljuk ki a vezeték nélküli hálózatunkat, és nézzük meg, melyik eszközünk nem működik tovább. Lehetséges, hogy nem azonosítható így minden eszköz, de meg fogunk lepődni, mennyi eszközről feledkeztünk el.

**Mindig frissítsünk:** Éppúgy, mint a számítógép és a mobil eszközeink esetében, kritikus, hogy bármely és minden eszközünk frissítve legyen. Ha az eszközeinken van automatikus frissítési beállítás, engedélyezzük azt.

**Jelszavak:** Változtassuk meg az eszközeinken a jelszavunkat egy egyedi, erős jelmondatra, amit csak mi ismerünk. Minden valószínűség szerint csak egyszer kell ezeket a jelszavakat begépelnünk. Nem emlékszünk minden jelmondatunkra? Nem kell aggódnunk, hisz senki sem szokott! Fontoljuk meg egy jelszókezelő alkalmazás használatát, hogy biztonságosan tárolhassuk minden jelszavunkat, jelmondatunkat.

**Adatvédelmi beállítások:** Ha az eszközünk lehetővé teszi, hogy módosítsuk az adatvédelmi beállításokat, korlátozzuk az eszköz által gyűjtött vagy megosztott információk körét. Egy lehetséges megoldás, hogy egyszerűen letiltjuk az információ megosztásának lehetőségét.

**Gyártók:** Olyan cégtől vásároljunk eszközöket, melyet ismerünk, és amelyben megbízunk. Olyan terméket keressünk, ami támogatja a biztonsági beállításokat, mint például az automatikus frissítések engedélyezésének lehetősége, az alapértelmezett jelszó megváltoztatásának lehetősége, és az adatvédelmi beállítások módosítása.

**Mindig figyeljünk:** Ha egy eszköz képes szóbeli parancsokat értelmezni, akkor folyamatosan figyel. Például az Alexa vagy a Goggle Home készülékek rögzíthetik akár az érzékeny információkat tartalmazó beszélgetéseket is. Vegyük ezt figyelembe, amikor eldöntjük, hová helyezzük el ezeket az eszközöket otthonunkban, és vizsgáljuk felül az adatvédelmi beállítási lehetőségeket is.

**Vendéghálózat:** Fontoljuk meg, hogy az Otthoni Okos Eszközeinket egy külön "vendéghálózathoz" csatlakoztassuk, mintsem az elsődleges WiFi hálózatához, amihez a számítógépünk és a mobil eszközeink is csatlakoznak. Így, ha bármely okos eszköz megfertőződik, a fő hálózathoz csatlakoztatott számítógépeink vagy a mobil eszközeink biztonságban maradnak.

A telefonos csalások száma emelkedőben van. Mi magunk vagyunk a legjobb védelem az ilyen csalások felismerésben és megállításában is.

## 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.

## A szerzőről

***Robert M. Lee*** *(@RobertMLee) SANS tanúsítvánnyal rendelkező oktató, és szerzője a FOR 578 – Kiber Fenyegetés Felderítés és az ICS15 – ICS Aktív Védelem és Incidenskezelés kiadványoknak. Robert ezen kívül alapítója és ügyvezetője a Dragos nevű ipari kiberbiztonsági társaságnak.*

## Hivatkozások

| | |
|---|---|
| Jelmondatok: | https://www.sans.org/u/GEB |
| Jelszókezelők: | https://www.sans.org/u/GEG |
| Az otthoni hálózat biztonsága: | https://www.sans.org/u/GEL |