Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadásban...

- A WiFi hálózat
- Eszközök

Az otthoni hálózat biztonsága

Áttekintés

Néhány évvel ezelőtt az otthoni hálózatok viszonylag egyszerűek voltak. Általában egy vezeték nélküli (WiFi) hozzáférési pontból és a hozzá csatlakozó egy vagy két számítógépből álltak, amiket böngészésre, online vásárlásra vagy játékra használtunk. Mára azonban ezek sokkal összetettebbé váltak, mivel manapság már sokkal több eszközzel csatlakozunk a hálózatra, és azokat több mindenre használjuk, mint egyszerű internetezés vagy médiafogyasztás. Az OUCH! e havi kiadásában bemutatjuk, hogyan tudunk az egész család számára biztonságos otthoni hálózatot létrehozni.

A szerzőről

Cheryl Cloney a Lockheed Martin biztonsági oktatással és tudatossággal foglalkozó csoportjának vezetője. Az általa irányított „The I Campaign™" oktatási kampány több mint 100 ezer emberhez jutott el, amely magába foglal több szervezeten belüli szövetséget és érdekképviseleti csoportot és egy adathalászat elleni programot is. A Twitter-en **@conleychera** néven találhatjuk meg.

A WiFi hálózat

Szinte minden otthoni hálózat vezeték nélküli hálózat (WiFi). Ennek segítségével bármilyen alkalmas eszközt vezeték nélküli technológia segítségével lehet csatlakoztatni az Internetre, kezdve a laptop-októl és tablet-ektől egészen a játékkonzolokig és TV készülékekig. A legtöbb otthoni WiFi hálózatot egy internet kijárattal rendelkező router felügyeli, azaz ezen keresztül el lehet érni az Internetet. Azonban bizonyos esetekben előfordulhat, hogy egy különálló eszközön – ún. WiFi csatlakozási ponton (Access Point) – keresztül csatlakozunk a szolgáltató által biztosított modemhez vagy routerhez. Függetlenül attól, hogy nálunk melyik megoldás van, alapvetően ugyanúgy működik a rendszer: a vezeték nélküli hálózat rádiójeleket sugároz a lakásban és annak környezetében, és a különböző eszközök ezeknek a rádiójeleknek segítségével csatlakoznak a hálózathoz és azon keresztül az Internethez. Ez pedig azt jelenti, hogy a WiFi hálózat biztonsága alapvető fontosságú az otthonunk védelmében. Ezért az alábbi lépések megtételét javasoljuk:

- Változtassuk meg a WiFi router vagy csatlakozási pont alapértelmezett adminisztrátori jelszavát, amivel az egész hálózatot felügyelni lehet! Az adminisztrátor felhasználóval az egész hálózatot lehet konfigurálni. A probléma az, hogy a legtöbb ilyen központi eszköz üzembe helyezéskor már használ egy alapértelmezett adminisztrátori jelszót, és ezt az Internet segítségével bárki pillanatok alatt megtudhatja. Ezért nagyon fontos, hogy ezt egy olyan erős, egyedi jelszóra cseréljük, amit csak mi ismerünk.
- Változtassuk meg a WiFi hálózat alapértelmezett elnevezését (gyakran nevezik SSID-nek is)! Ezt a nevet látják a WiFi hálózatot kereső eszközeink. Adjunk olyan nevet a hálózatunknak, ami egyedi és könnyen azonosítható, de

Az otthoni hálózat biztonsága

mégsem tartalmaz semmi személyes információt! A WiFi hálózatunkat beállíthatjuk rejtettnek is (az eszköz ebben az esetben nem „reklámozza”, azaz sugározza a hálózat megnevezését), de ennek ellenére a legtöbb WiFi kereső eszköz vagy egy képzett támadó könnyedén fel tudja deríteni.

- Gondoskodjunk arról, hogy csak olyan emberek tudjanak csatlakozni a WiFi hálózatunkhoz, akikben megbízunk, és az ő kapcsolatuk is titkosítva legyen! Ezt úgy érhetjük el, ha erős titkosítást állítunk be – erre a legjobb megoldás jelenleg a WPA2 titkosítás használata. Ha engedélyezzük azt az opciót, akkor a WiFi router-hez történő kapcsolathoz jelszó lesz szükséges, ezután már titkosított adatforgalom zajlik az eszköz és a router között. Győződjünk meg arról, hogy nem használunk régi, elavult titkosítási eljárásokat (pl. WEP), vagy, hogy egyáltalán nem használunk semmilyen titkosítást! A nyílt hálózatok lehetőséget adnak bárki számára, hogy előzetes hitelesítés nélkül csatlakozzanak az adott hálózathoz.

Az otthoni hálózatunk védelmének kulcsa a WiFi kapcsolatos biztonságos beállítása, valamint a frissített és erős jelszóval védett eszközök.

- A WiFi router-en keresztüli internet csatlakozás jelszava legyen kellően összetett és egyedi, tehát mindenféleképpen különbözzön a WiFi router adminisztrátori jelszavától! Tartsuk észben, hogy általában csak egyszer kell megadni a jelszót, mert a készülékek képesek eltárolni azt!
- A legtöbb WiFi hálózat támogatja az ún. vendég hálózat (guest network) létrehozását. Ennek használatával lehetővé válik az, hogy a vendégek eszközei úgy csatlakozzanak az Internetre a WiFi router-en keresztül, hogy közben azok nem látják a hálózatunkra csatlakozó saját rendszereinket, eszközeinket. Amennyiben létrehozunk egy ilyen vendég hálózatot, akkor itt is állítsunk be egy egyedi jelszót valamint a WPA2 titkosítást a csatlakozáshoz!
- Kapcsoljuk ki a WiFi Protected Setup vagy hasonló funkciókat, amelyek lehetővé teszik, hogy új eszközök csatlakozzanak a hálózatra a jelszó és konfigurációs paraméterek ismerete nélkül!
- Ha nehezen tudjuk csak megjegyezni a jelszavakat, akkor használjunk egy jelszókezelő programot azok biztonságos tárolásához!

Amennyiben bizonytalanok vagyunk a fenti beállításokat illetően, akkor kérjünk segítséget az internetszolgáltatónktól, nézzük át a router vagy hozzáférési pont dokumentációját, illetve ellenőrizzük azok gyártóinak weboldalát is.

Eszközök

A következő lépés az, hogy mindig legyünk tisztában vele, hogy milyen eszközök képesek csatlakozni a hálózathoz, és gondoskodjunk azok biztonságáról. Ez nagyon egyszerű volt akkor, amikor még csak néhány csatlakozott eszközről volt

Az otthoni hálózat biztonsága

szó. Manapság viszont szinte követelmény, hogy az eszközök képesek legyenek állandó kapcsolatot fenntartani (ide értve az olyanokat, mint például a TV készülékek, játékkonzolok, bébi monitorok, hangszórók, termosztátok vagy akár az autók is). Amennyiben meg akarjuk tudni, hogy éppen milyen eszközök vannak felcsatlakozva a hálózatunkra, akkor használjunk hálózat szkennelő programokat (például Fing). Az ilyen alkalmazásokat telepíthetjük számítógépre vagy mobil eszközre is, majd pedig át tudjuk vizsgálni a WiFi hálózatunkat a felcsatlakozott eszközök után. Miután azonosítottuk az összes ilyen eszközt, győződjünk meg arról, hogy mindegyik biztonságosan be van állítva. Erre a legjobb módszer az, hogy mindegyik eszközön a legfrissebb szoftvereket és firmware-eket használjuk. Ahol lehetséges, engedélyezzük az automatikus frissítést, használjunk bonyolult, egyedi jelszót. Végezetül pedig ne felejtsük el meglátogatni az internetszolgáltatónk weboldalát, mivel a szolgáltatók is gyakran nyújtanak segítséget a saját hálózatunk biztonságosabbá tételében ingyen letölthető szoftverek formájában.

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

A jelmondatokról:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_hu.pdf
Jelszókezelő programok:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_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