OUCH! | 2014. január

Havi biztonságtudatossági hírlevél számítógép-felhasználók számára

OUCH!

Ebben a kiadványban...

- **Vezeték nélküli hálózat**
- **OpenDNS**
- **Eszközök**

Az otthoni hálózat védelme

Áttekintés

Évekkel ezelőtt az otthoni hálózatok meglehetősen egyszerűek voltak, mivel jellemzően egy vezeték nélküli hozzáférési pontból (access point) és a hozzákapcsolódó egy, esetleg két számítógépből álltak, melyekkel a felhasználók szörföltek a neten, illetve online játékokkal játszottak. Mára azonban sokkal összetettebbek lettek az otthoni hálózatok. Nem csak a kapcsolódó eszközök száma nőtt meg, hanem ezeket az eszközöket sokkal több mindenre is használjuk. Az OUCH! mostani számában bemutatunk pár egyszerű lépést, amivel biztonságosabbá tehetjük az otthoni hálózatunkat.

Vendégszerkesztő

Kevin Johnson a **MySecurityScanner.com** weboldalt működtető Secure Ideas vezetője, illetve a SANS Institue veterán oktatója. A vendégszerkesztőről további információk a **www.secureideas.com** weboldalon érhetők el.

Vezeték nélküli hálózat

Szinte minden otthoni hálózat vezeték nélküli hálózat (szokták még WiFi hálózatnak is nevezni). Ezen keresztül lehet a különböző vezeték nélküli eszközöket (laptopok, tablet-ek, játékkonzolok és televíziók) csatlakoztatni az Internetre. Ahhoz, hogy ez működjön, a vezeték nélküli hálózatnak szüksége van egy vezeték nélküli hozzáférési ponthoz. Ez egy kis elektronikus szerkezet, amely csatlakozik az Internetre kötött router-hez (de gyakran egybe van építve azzal), és olyan vezeték nélküli jelet bocsát ki, amelyet a fent említett eszközök érzékelni tudnak. Miután ezek az eszközök sikeresen csatlakoztak a hozzáférési ponthoz, ennek megfelelően az Internethez és a további, hálózaton lévő eszközökhöz. Ennek következtében nyugodtan kijelenthetjük, hogy a vezeték nélküli hozzáférési pont az otthoni hálózat egyik kulcsfontosságú eleme, így javasolt az alábbi lépések megtétele, amivel biztonságossá lehet tenni a használatát.

- A legtöbb vezeték nélküli hozzáférési ponthoz tartozó, alapértelemezetten beállított adminisztrátori felhasználónév és jelszó bárki által megismerhető, mivel ezeket az Internetről is meg lehet tudni. Ezért feltétlenül meg kell változtatni az adminisztrátor bejelentkező nevét és jelszavát, ami legyen egyedi, és nem szabad sehol máshol használni!
- Egy másik feladat, hogy be kell állítani a vezeték nélküli hálózat nevét (szokták meg SSID-nek is nevezni)! Ezt a nevet fogják látni a hálózatra csatlakozni szándékozó eszközök, miközben keresik a helyi hálózatot. Adj a hálózatnak valami olyan nevet, ami egyedi, és könnyen azonosítható, de mégsem tartalmaz semmi személyes információt! Úgy is lehet konfigurálni egy hálózatot, hogy rejtve maradjon (vagyis ne látszódjon az elérhető hálózatok között az SSID - hálózat neve), azonban tisztában kell lenni azzal, hogy a legtöbb kereső program, vagy éppenséggel egy tapasztalt hacker könnyedén fel tudja fedezni így is a hálózat részleteit!

Az otthoni hálózat védelme

- A következő lépesben azt kell megoldanod, hogy csak az általad ismert és megbízhatónak tartott emberek tudjanak hozzáférni a vezeték nélküli hálózathoz, és ők is csak titkosított kapcsolat használatával! Ezzel biztosíthatod azt, hogy se a szomszédok, se más idegenek ne tudjanak csatlakozni vagy lehallgatni a hálózatodat. Ezt úgy lehet könnyen megoldani, hogy erős titkosítást állítasz be a vezeték nélküli hozzáférési ponton. A jelenlegi legjobb választás a WPA2 titkosítás beállítása. Amennyiben ez az opció be van állítva, akkor csak jelszóval lehet csatlakozni a hálózathoz, és a kapcsolódás után az adatforgalom titkosításra kerül. Győződj meg arról, hogy a titkosításnál nem valamilyen régebbi, már elavult módszer van beállítva (például WEP), vagy ami még rosszabb, egyáltalán nincs semmilyen titkosítás beállítva (ezt hívják nyílt hálózatnak - open network)! Az ilyen nyílt hálózathoz bárki hozzáférhet hitelesítés nélkül.
- Figyelj arra, hogy a felhasználók olyan nehezen kitalálható, erős jelszóval tudjanak csatlakozni az otthoni hálózathoz, amely különbözik az adminisztrátori jelszótól! Tartsd észben, hogy csak egyszer kell beírni a jelszót minden eszközbe, mert azok elmentik, és a következő csatlakozásnál is azt fogják használni!
- Számos olyan WiFi hozzáférési pont van, amelyik ismeri az ún. vendég hálózat (Guest Network) fogalmát. A vendég hálózat lehetővé teszi a látogatók számára, hogy kapcsolódjanak az Internetre a vezeték nélküli hozzáférési ponton keresztül, de nem látják a hálózathoz csatlakozó egyéb eszközöket. Ha bekapcsolod a vendég hálózat funkcióját, akkor ahhoz is WPA2 titkosítást használj, és egy minden mástól különböző jelszót!
- Ha nem tudod fejben tartani a különböző jelszavakat, használj jelszókezelő programot ezek kezeléséhez és biztonságos tárolásához!

Az otthoni hálózat védelme érdekében használj biztonságos vezeték nélküli hálózatot, használj OpenDNS vagy más hasonló szolgáltatást, és minden csatlakozó eszköz szoftvere legyen naprakész!

OpenDNS

Miután konfiguráltad a vezeték nélküli hálózatodat, érdemes beállítani az OpenDNS használatát is (vagy valamilyen Norton ConnectSafe for Home szolgáltatáshoz hasonló dolgot). Amikor egy címet írsz be a böngésző címsorába, a DNS mondja meg neki, hogy milyen IP címre kell elküldeni a kérést az oldal letöltésére (vagy akár egy levél elküldésére). Az OpenDNS-hez hasonló szolgáltatások képesek azonosítani az ismert, fertőzött weboldalakat, és blokkolni fogják az adott oldalra vonatkozó kéréseket, így még véletlenül sem lehet meglátogatni egy káros szoftvert vagy más káros tartalmat hordozó weboldalt az otthoni hálózaton keresztül. Ezen kívül az ilyen szolgáltatások lehetőséget adnak arra, hogy blokkold a kifogásolhatónak ítélt weboldalakhoz történő hozzáférést is. Ennek a megközelítésnek az adja a hatékonyságát, hogy nem szükséges semmilyen szoftver telepítése az Internet elérésre szolgáló eszközökre, egyszerűen csak be kell állítani a hozzáférési ponton.

Az otthoni hálózat védelme

Eszközök

A következő lépés az, hogy tisztában kell lenned azzal, hogy milyen eszközök kapcsolódnak az otthoni hálózatodhoz, és meg kell győződnöd arról, hogy azok biztonságban vannak. Ez viszonylag egyszerű volt addig, amíg csak néhány ilyen eszközről beszéltünk. Napjainkra már szinte minden tud kapcsolódni az otthoni hálózathoz (TV készülékek, játékkonzolok, bébi monitorok, hangszórók, hőmérséklet szabályzók, vagy akár az autód is). Amennyiben egyszer összeírod az összes eszközt, lehet, hogy meg fogsz lepődni, hány ilyen van. A legjobb módszer ezen eszközök biztonságának megteremtéséhez az az, hogy mindig a legfrissebb operációs rendszert használod az eszközökön. Ahol lehetséges, kapcsold be az automatikus frissítést! Amennyiben erre nincs lehetőség, akkor legalább havonta nézz utána a frissítéseknek! Ezen kívül rendszeresen keresd fel az Internet szolgáltatód weboldalát, mivel ők is kínálahtnak olyan ingyenes eszközöket, amikkel javíthatsz az otthoni hálózatod biztonságán!

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

OpenDNS: http://www.opendns.org

Norton ConnectSafe: http://dns.norton.com/dnsweb/dnsForHome.do

Network security scanner: http://www.sophos.com/en-us/products/free-tools/network-security-scan.aspx

Jelszókezelők: http://www.securingthehuman.org/resources/newsletters/ouch/2013#october2013

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