Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadásban...

- **A tárgyak internete**
- **Problémák**
- **Védekezés**

A Tárgyak Internete

Mit nevezünk a tárgyak internetének?

A múltban a technológia viszonylag egyszerű volt. Csatlakoztattunk egy számítógépet az internetre, és azt használtuk a napi ügyeink intézésére. Azonban a technológia nem állt meg itt. Megérkeztek a hordozható eszközök (jellemzően okostelefonok és táblagépek formájában), amik képesek egy asztali számítógép képességeit a zsebnyi méretű eszközbe sűríteni. Azonban hiába a könnyű hordozhatóság, ezeknek az eszközöknek is megvannak a maguk biztonsági problémái. A technológiai fejlődés következő lépcsőfoka a tárgyak internete, ami a gyakorlatban azt jelenti, hogy a mindennapi használati tárgyainkat is rákötjük az internetre. A kapucsengőtől és a villanykörtéktől kezdve egészen a játék babákig és a termosztátig. Ilyen módon sokkal egyszerűbbé tehetjük a saját életünket – példának okáért a világítás automatikusan felkapcsolódik, amikor a mobiltelefonunk azt érzékeli, hogy már közel vagyunk a lakásunkhoz. A tárgyak internete folyamatos változásban van, szinte hetente találkozhatunk újabb és újabb fejlesztésekkel, amik nagyszerű lehetőségeket hoznak el számunkra. Azonban hasonlóan az okostelefonunkhoz, ezeknek a dolgoknak is megvannak a maguk biztonsági problémái. E havi hírlevelünkben útmutatót adunk azzal kapcsolatban, hogy milyen veszélyek leselkednek ránk, és hogy milyen lépéseket tegyünk ezen veszélyek elkerülésének érdekében.

A szerzőről

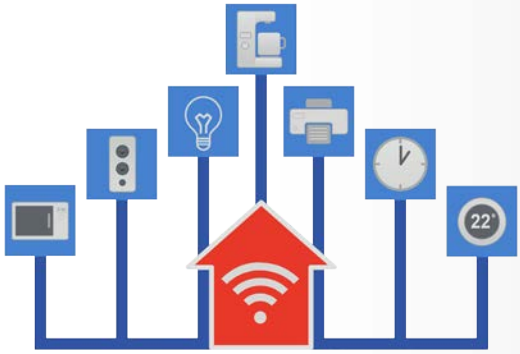
James Lyne (**@jameslyne**) a Sophos biztonsági kutatásokért felelős vezetője. Saját bevallása szerint elvetemült „geek”, akinek a technikai tudása számos területet lefed. A SANS Intézet minősített oktatója, és a különböző biztonsággal foglalkozó konferenciák vezető előadója.

A problémák

A tárgyak internetének előnye, hogy a csatlakozó eszközök egyszerűek. Például bekapcsoljuk a kávéfőző gépet, és utasíthatjuk arra, hogy csatlakozzon a Wi-Fi hálózathoz. Azonban az egyszerűségnek ára van. A legnagyobb probléma ott van, hogy sok olyan cég gyárt ilyen dolgokat, amelyeknek semmilyen tapasztalata sincs a biztonság terén, mivel a profiljuk a háztartási gépek gyártásában merül ki. Esetleg a gyártó egy friss start-up cég, aminek a célja a leghatékonyabban és leggyorsabban előállítani egy terméket. Az ilyen cégek célja a profit szerzése, a kiberbiztonságra nem ügyelnek. Ennek következtében a legtöbb ilyen eszköz egyáltalán nem vagy csak nagyon gyenge biztonsági megoldásokat használ. Például az eszközben nem lehet megváltoztatni az alapértelmezett jelszót, amit egyébként az internet segítségével bárki megismerhet. Ezen kívül

A Tárgyak Internete

gyakori, hogy egyáltalán nem lehet konfigurálni az eszközt. Hogy a dolgok még rosszabbak legyenek, nem egyszerű frissíteni, már ha egyáltalán van rá lehetőség. Ennek következtében az ilyen eszközök hamar elavulttá válnak a nem javított sérülékenységek miatt, amiken keresztül mi válunk sebezhetővé.



The Internet of Things

Tudd, hogy milyen eszközt csatlakoztatsz a hálózatra, hozz létre ezek számára egy saját hálózatot, ha van rá lehetőség, tartsd őket naprakészen, és védd erős jelszóval!

Védekezés

Tehát mi tehetünk? A célunk egyértelműen az, hogy hatékonyan és biztonságosan használjuk ezeket az eszközöket, mivel olyan előnyöket biztosítanak számunkra, amelyek kényelmesebbé teszik az életünket, pénzt és időt spórolnak meg számunkra, és akár a lakásunk is nagyobb biztonságban lesz a használatuk következtében. Ezeken túl pedig a technológia fejlődésével lassan nem lesz más választásunk, mint ilyen eszközöket beszerezni és használni. Az alábbi tanácsok segíthetnek abban, hogy hogy megvédjük az eszközöket és rajtuk keresztül saját magunkat:

- **Csak szükség szerint csatlakoztassuk**: a védekezés legegyszerűbb módja az, hogy ne kössük az internetre azt az eszközt, aminél nincs szükség online eléréshez.
- **Szeparáljuk a Wi-Fi hálózatot**: ha nem akarjuk online elérni az eszközöket, akkor alakítsunk ki egy belső Wi-Fi hálózatot csak azok számára! A legtöbb Wi-Fi eszköz képes egy másodlagos, ún. vendég Wi-Fi hálózatot kezelni. Esetleg vásárolhatunk egy második Wi-Fi router-t, kizárólag ezen eszközök számára. Bármelyik megoldást is választjuk, segít abban, hogy egy izolált hálózatban legyenek a háztartási berendezések, így nem lehet azokat arra használni, hogy segítségükkel támadják meg a számítógépünket vagy mobil készülékünket (amik tulajdonképpen a céljai a mindenkori támadóknak).
- **Frissítsünk, ha lehetőség van rá**: pont úgy, mint a számítógépek vagy mobil eszközök esetén, kapcsoljuk be az automatikus frissítést, ha van rá mód!
- **Erős jelszó**: válasszunk egyedi, erős jelszavakat, jelmondatokat, amiket csak mi ismerünk! Ha nehézséget okozna ezek megjegyzése, használjunk egy jelszókezelő alkalmazást!
- **Adatvédelmi lehetőségek**: ha egy eszköz lehetőséget ad arra, hogy adatvédelmi beállításokat módosítsunk rajta, akkor a lehető legkevesebb adat megosztását válasszuk! Akár ki is kapcsolhatjuk ezt a lehetőséget.

A Tárgyak Internete

- **Gondoskodjunk a cseréről**: eljöhet az a pont, hogy már túl sok sérülékenység vált ismertté az adott eszközzel kapcsolatban. Ilyenkor érdemes lecserélni az adott eszközt egy olyanra, amely sokkal nagyobb biztonságot biztosít számunkra.

Nincs minden igényt kielégítő eszköz, ezért javasolt mindig ellenőrizni és utánaolvasni a kiszemelt választásnak, hogyan és mennyire lehet biztonságossá tenni. Sajnos a legtöbb eszközt úgy fejlesztették, hogy a kiberbiztonság nem volt a szempontok között, így a gyártók nem is biztosítanak túl sok információt. Azonban napjainkban a biztonsági tudatosság egyre nagyobb teret kap, így reméljük, hogy a gyártók is nagyobb figyelmet fordítanak erre a területre a jövőben.

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
A jelszókezelőkről:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_hu.pdf
Új tablet biztonságáról:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_hu.pdf
Az otthoni hálózat 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