Az IoT eszközök valóban kényelmesek, de mennyire biztonságosak?

Sajtóközlemény – 2020.06…/PResston PR

Sok mindent megteszünk annak érdekében, hogy minél több IoT eszközt birtokolhassunk. Az általuk biztosított kényelem érdekében sokszor hajlamosak vagyunk feláldozni még a biztonságunkat, és az érzékeny adatainkat is.

Az IoT, az Internet of Things, azaz a dolgok internetének rövidítése. Azok az eszközök sorolhatók ide, amelyek képesek más eszközzel/eszközökkel kétirányú kommunikációt folytatni. Mi már a digitális világ összekapcsolt hálózatában élünk. Van intelligens ajtócsengőnk, amely segít nekünk okostelefonok révén ellenőrizni, hogy ki áll az ajtónk előtt. Vannak okos óráink, hogy felügyelhessük gyermekeink tartózkodási helyét, és fitneszalkalmazásaink, melyekkel nyomon követhetjük fizikai jólétünket. A tárgyak internetes forradalma intelligens háztartási készülékek egész sorával árasztotta el háztartásainkat. Az okos teáskannáktól, mosógépeken át, egészen az intelligens hűtőszekrényekig.

Mindez ugyan megkönnyíti az életünket, de nem jelenti azt, hogy biztonságosabbá is teszi azt. Kényelmes lehet a háztartások nagy részének okostelefonról történő irányítása, de biztonságban vannak-e az érzékeny adataink?

„Az IoT eszközök esetében a kibertámadók magukat az okos eszközöket támadják, gyakran a felhasználó bevonása vagy megtévesztése nélkül, közvetlenül kihasználva a sebezhetőségeket vagy a gyenge biztonsági megoldásokat.”- mondta **Csizmazia-Darab István, a Sicontact Kft. biztonsági szakértője**

Íme néhány olyan okos kütyü, amely használatával a kényelem oltárán áldozzuk fel a személyes adatainkat:

Gyermekfigyelő okosórák

Minden szülő életében prioritás az, hogy a gyermekeit biztonságban tudja. Annak érdekében, hogy nyomon kövessék őket ebben a digitalizált világban, néhányan olyan okosórákat választanak, melyek helymeghatározó funkciókkal is rendelkeznek, így láthatják, hol vannak a kicsik és még kommunikálhatnak is velük szükség esetén. De nem minden gyerekfigyelő jó választás – ha egy kevésbé márkás okosórát akarunk vásárolni, akkor körültekintőnek kell lennünk a választást illetően.

Sajnos egyes gyártók szerverein találhatunk biztonsági réseket, amik az áhított biztonság helyett veszélybe is sodorhatják gyermekeinket. Egy okos órákkal kapcsolatos kutatás szerint, némely gyártó nem biztosítja a szervereik biztonságos működését. Egy bizonyos okosóra esetében a biztonsági szakértők több mint 5000 gyermek helyzetéhez, telefonszámához, fényképeihez és privát beszélgetéseihez tudtak hozzáférni. Az Európai Bizottság már egy ilyen termék visszahívását is elrendelte, ugyanis nem első esetben éltek vissza érzékeny adatokkal különböző gyerekeknek készült okosórákon keresztül.

Intelligens ajtócsengő

Manapság már fel sem kell kelnünk az ágyából vagy a kanapéról ahhoz, hogy megnézzük, ki áll az ajtónk előtt, sőt bizonyos okos rendszerek esetében az ajtót is kinyithatjuk a telefonunk segítségével. Ezt a kényelmet biztosítja számunkra egy intelligens ajtócsengő vagy egy intelligens zár. Joggal gondolhatjuk, hogy a kényelem megéri az árát, ugyanis néhány okos eszköz megvásárlásával extra biztonsági funkciókat is kapunk. Ilyen például az okos ajtócsengő, amely képes rögzíteni a bejárat előtti mozgást.

Célszerű körültekintőnek lennünk mielőtt egy intelligens ajtócsengőbe invesztálunk, hiszen mindenki számára a család és otthon biztonsága a legfontosabb. A szakemberek szerint néhány okos ajtócsengő nemvárt dolgokat is produkálhat. Egy adott típus például pillanatképeket készített és töltött fel minden alkalommal, amikor mozgást érzékelt a bejárat előtt. Azt gondolnánk, hogy ez normális, ugyanakkor nem volt mód ezeket a pillanatképeket visszanézni és kideríteni, hogy hová kerülnek feltöltésre. Jobb, ha alaposan megvizsgáljuk mit is vásárolunk valójában, ezzel csökkentve a biztonsági kockázatok mértékét.

Olcsó biztonsági kamerák

A biztonság témakörénél maradva, egy másik népszerű IoT-eszköz, az intelligens biztonsági kamera. Az emberek azért telepítik ezeket, hogy nyomon követhessék, otthonaik vagy a vállalkozásaik külső-belső védelmét. Ahhoz, hogy a kamera képeihez bárhol és bármikor hozzáférhessünk, internet hozzáférés szükséges. Ebből adódóan, az adataink biztonsága a kapcsolat erősségén, illetve a kamerát működtető szerver biztonságától függ. Hogyha egy kibertámadónak sikerül meghackelni a rendszert és távoli elérést szereznie hozzá, máris egyenes út vezet számára az otthonunkba, ami a legrosszabb forgatókönyvet eredményezheti.

Sajnálatos módon az olcsó IP-kameratípusok, amelyek célja a család és a vagyontárgyak védelme lenne, a leggyakrabban feltört eszközök közé tartoznak. Mivel az olcsó eszközöket hasonló módon gyártják, a legtöbb ugyanazokkal a sebezhetőségekkel kerül forgalmazásba. Nemcsak a közvetlen támadások miatt kell az ügyfeleknek aggódniuk, hanem a működés közben fellépő programhibák miatt is. Az egyik ilyen esetben például egy Xiaomi márkájú eszköz random képeket osztott meg idegen otthonokból a többi kameratulajdonossal.

IoT eszközök közös kapcsolódási pontja : a hub

A közös hálózati kapcsolódási pontba csatlakozik az összes otthoni IoT eszköz – így metaforikus értelemben az egész rendszer agyának is nevezhetjük. Egységesíti az összes IoT eszközt - például a biztonsági kamerákat, az okos ajtócsengőt, a lámpákat -, és elősegíti, hogy ezeket kényelmesen egy helyről irányítsuk. A kapcsolódási pontok segítségével nem csak az okos otthonokat tudjuk figyelni és irányítani, hanem a vállalkozások környezetének vezérlésében is nagy szerepet játszanak.

Ezek alapján már biztosan el tudjuk képzelni, hogyan működnek az IoT eszközök. Ha a kibertámadók sebezhetőséget találnak az eszközökön, azt kihasználva teljes hozzáférést kaphatnak az okos rendszerekhez és az általuk tartalmazott érzékeny adatokhoz. Az ESET IoT Research számos súlyos sebezhetőséget talált három kapcsolódási pontban, amelyek közül néhány megnyitja a rendszert a támadások előtt.

Összefoglaló gondolatok

Ha az IoT eszközök piacáról szeretnénk beszerezni olyan eszközöket, amelyek könnyebbé és kényelmesebbé teszik az életünket, érdemes pár szabályt betartani a biztonságunk érdekében:

• Mielőtt bármit megvásárolnánk, érdemes utánajárni alaposabban az adott eszköznek. Olvassuk el a megvásárolni kívánt készülék leírását, keressünk vásárlói vélemények a termékről, illetve azt is nézzük meg, hogy ezek mennyire megbízható forrásból származnak. Keressünk rá a márkanévre, sőt a modell nevére, a „sebezhetőség" vagy hasonló szavak kombinációval együtt. Ha bármilyen biztonsági probléma felmerült a korábbiakban, ellenőrizzük, hogy ezek megoldódtak-e, és nem érintik már az eszközt.

• Tartózkodjunk a kevésbé ismert márkák vásárlásától, ha nem tudjuk ellenőrizni, hogyan biztosítják az adatok védelmét, vagy ezek hová kerülnek feltöltésre. Az olcsóbb eszközök vásárlásával később sokkal nagyobb költséget realizálhatunk, hogyha illetéktelen személyek kezébe kerülnek az érzékeny adataink.

• Miután megvásároltunk egy eszközt, mindig frissítsük a firmware-t a lehető legújabb verzióra. Ha bármilyen frissítés rendelkezésre áll, érdemes azonnal telepíteni azt, mivel ezek általában az eszköz biztonságosabbá tételét célozzák. Ellenkező esetben a kiberbűnözők könnyen visszaélhetnek az eszközök sebezhetőségével, amit megakadályozhattunk volna a frissítések telepítésével.