Meghackelt mackó, kémkedő baba: hogyan szűrhetjük ki a nem biztonságos okosjátékokat ajándékvásárláskor?

Az intelligens pacemakerektől az okosórákig, a hangasszisztensektől az okos kapucsengőkig a technológia segít életünket egészségesebbé, kényelmesebbé, és szórakoztatóbbá tenni - ez a dolgok internete (Internet of Things – IoT), mely egyúttal lehetővé teszi a gyártók számára, hogy új, izgalmas játékokat dobjanak piacra. Az okosjátékok globális piacán kétszámjegyű százalékos növekedés várható, és 2027-re ez meghaladhatja a 24 milliárd dollárt. Amikor viszont a hálózati kapcsolat, az adatok és a számítástechnika találkozik, adatvédelmi és biztonsági aggályok is felmerülhetnek - az ESET szakértői most, a karácsonyi vásárlások kezdetekor az ebben rejlő veszélyekre hívják fel a figyelmet.

Valószínűleg mindannyiunkban felmerült már a gondolat, hogy beszerzünk gyermekeink számára egy okosjátékot, mely ösztönzi a tanulást és fejleszti a kreativitást. Az ESET kiberbiztonsági szakértői szerint az adatok és a magánélet védelme (plusz a gyermekek biztonsága!) érdekében érdemes némi előzetes kutatást végeznünk, mielőtt kiválasztjuk az eszközt. Amennyiben pedig laptopot, számítógépet készülünk ajándékozni, mindenképp gondoskodjunk vírusvédelmi szoftverről is, amit most az **ESET karácsonyi "2 az 1-ben" akciójában** kedvezményesen vásárolhatunk meg.

Mik azok az okosjátékok és melyek a kiberkockázatok?

Okosjátékok már évek óta léteznek. Mint minden IoT-eszköz esetében, itt is az a cél, hogy a világhálóra való csatlakoztathatóság és az intelligens eszköz segítségével még magával ragadóbb és interaktívabb élményt nyújtsanak. Ezek a játékok olyan eszközöket használhatnak, mint:

- mikrofonok és kamerák, a videó és a hang továbbítására,
- hangszórók és képernyők, amelyek hangot és videót közvetítenek a gyermekeknek,
- Bluetooth, amely által a játékot egy mobil alkalmazással kapcsolják össze,
- internetkapcsolat az otthoni Wi-Fi routerrel.

Ezek az okoseszközök merőben eltérnek azoktól a játékoktól, amelyekkel legtöbben gyermekkorunkban töltöttük az időt. Képesek arra, hogy az interakcióval bevonzzák a legkisebbeket is, és újabb és újabb funkciókat tudnak elsajátítani az internetről letölthető kiegészítők révén.

Sajnos az ESET szakértői úgy tapasztalják, hogy számos esetben a gyártók a piacért folyó versenyben spórolnak a biztonsági intézkedéseken. Ennek eredményeként termékeik szoftversebezhetőségeket tartalmazhatnak illetve engedélyezhetik a nem biztonságos jelszavak használatát. Előfordulhat, hogy adatokat rögzítenek, és azokat titokban elküldik egy harmadik félnek, vagy érzékeny adatokat kérnek a szülőktől, amelyeket nem biztonságosan tárolnak.

Amikor a játékok veszélyessé válnak

Korábban több olyan eset is történt, amikor az okosjátékok veszélyessé váltak:

- A Fisher Price okos játékmackót 3-8 éves gyermekek számára tervezték, mint “egy interaktív tanuló barátot, amely beszél, figyel, megjegyzi, amit mondanak neki, sőt, válaszol is, ha megszólítják”. A csatlakoztatott okostelefon-alkalmazás hibája azonban lehetővé tette a hackerek számára, hogy jogosulatlanul hozzáférjenek a felhasználói adatokhoz.
- A CloudPets segítségével a szülők és gyermekeik hangüzeneteket oszthattak meg egymással egy plüssállaton keresztül. A jelszavak, e-mail címek és üzenetek tárolására használt háttértárat viszont nem biztonságosan tárolták a felhőben. Az adatállomány nyilvánosan, jelszóvédelem nélkül volt elérhető az interneten.
- A My Friend Cayla egy intelligens technológiával rendelkező játékbaba, amelynek a gyermekek kérdéseket tehetnek fel, és választ is kapnak az internet segítségével. A kutatók azonban felfedeztek egy biztonsági rést, amely lehetővé teszi a hackerek számára, hogy a babán keresztül kémkedjenek a gyermekek és a szülők után. Mindez arra késztette a német távközlési felügyeletet, hogy az adatvédelmi aggályok miatt a játék kidobására szólítsa fel a szülőket. Hasonló helyzet állt elő 2019-ben a Safe-KID-One nevű okosóra esetében is.

Az NCC Group biztonsági cég 2019 karácsonya előtt próbaképpen megvizsgált hét okosjátékot, amelyeknél összesen 20 problémát talált. Ezek közül kettőt magas kockázatúnak, hármat pedig közepes kockázatúnak minősített. A leggyakrabban az alábbi problémákkal találkoztak:

- Nincs titkosítva a fiók létrehozása és a bejelentkezési folyamat, így a felhasználónevek és jelszavak nyilvánosságra kerülhetnek.
- Nem lehetséges már meglévő felhasználó fiókot törölni, megszüntetni.
- Gyenge jelszószabályzat, azaz a felhasználók könnyen kitalálható bejelentkezési adatokat választhatnak.
- Homályos adatvédelmi irányelvek, cookie-k és más nyomon követésre alkalmas információk passzív gyűjtése.
- Az eszköz párosítása egy másik játékkal vagy alkalmazással gyakran mindenfajta hitelesítés nélkül történt Bluetoothon keresztül. Ez lehetővé teszi, hogy a hatótávolságon belül bárki sértő vagy felkavaró tartalmakat közvetítsen, illetve manipulatív üzeneteket küldjön a gyermeknek.
- Bizonyos esetekben (például a walkie talkie-n keresztül) egy idegen is képes lehet kommunikálni a környéken lévő gyerekekkel azáltal, hogy egy ugyanolyan játékot vásárol magának.
- A támadók képesek lehetnek az okosotthonok meghackelésére egy audiofunkciókkal rendelkező intelligens játék feltörése által, akár úgy, hogy hangüzenetet küldenek az otthoni hangasszisztenseknek (például: “Alexa, nyisd ki a bejárati ajtót”)

Hogyan lehetséges csökkenteni az okosjátékokban rejlő adatvédelmi és biztonsági kockázatokat?

Mivel az okosjátékok bizonyos fokú biztonsági és adatvédelmi kockázatot jelentenek, **Csizmazia-Darab István**, az ESET kiberbiztonsági megoldásait forgalmazó Sicontact Kft. szakértője szerint érdemes megfontolni az alábbi gyakorlati tanácsokat ajándékvásárláskor:

- **Tájékozódjunk vásárlás előtt:** Ellenőrizzük, hogy találunk-e negatív hangvételű hírt vagy kutatást az adott eszköz biztonságával kapcsolatban.
- **Legyen biztonságos az otthoni routerünk**. Ez az eszköz az otthoni hálózat központi eleme, és az összes internetre csatlakoztatott eszközünkkel kommunikál, ezért érdemes ezt erős jelszóval védeni, és a legfrissebb biztonsági hibajavításokkal ellátni.

- **Kapcsoljuk ki az eszközöket:** Ha nem használjuk a készüléket, a kockázatok minimalizálása érdekében kapcsoljuk ki.
- **Ismerjük meg alaposan a játékok működését:** Egyúttal gondoskodjunk arról, hogy a kisebb gyermekek csak felügyelet mellett használják az eszközöket.
- **Ellenőrizzük a frissítéseket:** Ha a játék képes frissítéseket letölteni, győződjünk meg róla, hogy az már a firmware (elektronikai eszközök működését biztosító belső program) legújabb verzióját futtatja.
- **Válasszunk biztonságos kapcsolatot:** Gondoskodjunk arról, hogy az eszközök a Bluetoothon keresztül történő párosításkor hitelesítést kérnek, és wifin pedig titkosított kommunikációt folytatnak az otthoni routerrel. Erről netes keresésekkel tudunk előzetesen tájékozódni, ha elérhető a részletes felhasználó útmutató, a tapasztalatokat megosztó fórumok oldalain a felhasználók hozzászólásaiból, illetve biztonságtechnikai szakcikkekből.
- **Legyünk tisztában azzal, hogy az eszközök pontosan hol tárolják az adatokat,** és megbízható híre van-e a játékot forgalmazó vállalatnak a biztonság terén.
- **Használjunk erős és egyedi jelszavakat** a fiókok létrehozásakor.
- **Csökkentsük minimálisra a megosztott adatok mennyiségét:** Ez csökkenti a kockázati kitettséget, ha az adatokat ellopják és/vagy a vállalatot megtámadják.

Az okosjátékok valóban jó eszközei lehetnek a tanulásnak és a szórakozásnak. De csak akkor, ha gondoskodtunk arról, hogy elektronikus eszközeink mindig védve legyenek.