# Tárgyak internete – tárgyak bizonytalansága

*Kanizsai Viktor*

## 1. Bevezetés

A tárgyak internetének piaca („Internet of Things" – IoT) rohamosan növekvő trendet mutat. A fogyasztók rendelkezésére már olyan háztartási készülékek állnak, amelyek informatikai hálózatra csatlakoztathatók. Annak ellenére azonban, hogy ezek az eszközök a fogyasztók körében egyre inkább elfogadottak, nem szabad figyelmen kívül hagyni, hogy az eszközök védelmére, illetve az adatbiztonságra nem fektetnek kellő hangsúlyt, s így a felhasználók különböző veszélyeknek vannak kitéve. Valamennyi hiányosság elhárítására irányuló intézkedés, amely érintheti az IoT-rendszereket, már jól ismert a biztonsági elvárások meghatározásának gyakorlatában, de ennek ellenére a mérséklési technikákat gyakran elhanyagolják ezeken az eszközökön. Az IoT szállítóinak nagyobb hangsúlyt kell fordítaniuk a biztonság megvalósítására, mielőtt ezen eszközök mindenütt jelen lesznek az otthonokban, s ezáltal emberek millióit teszik veszélyeztetetté csúcstechnológiai támadások tekintetében. A tanulmányban a szerző rámutat a leggyakoribb sérülékenységekre és támadási vektorokra, valamint meghatározza a gyártókra és fogyasztókra vonatkozó irányelveket az IoT-eszközök biztonságos fejlesztése és üzemeltetése szempontjából.

## 2. Az IoT-eszközök bizonytalanságáról általában

A tárgyak informatikai hálózatra való csatlakoztatása gazdagítja a hétköznapi és az üzleti életünket. Így például a csatlakoztatott hőérzékelők, orvosi eszközök, gépjárművek és ipari berendezések egy izgalmas környezetet biztosítanak az innovációnak és az új üzleti lehetőségeknek. Másrészt viszont ez a kiterjesztett számítógépes környezet széles körű biztonsági kérdéseket is felvet, és biztonsági fenyegetéseket hordoz. Támadók célpontjává válhatnak maguk az eszközök, az általuk kezelt adatok, illetve az őket magukban foglaló rendszerek. A támadások célja, többek között, adatszerzés, eszközvezérlés, illetve a szolgáltatás megtagadása is lehet.

A gyenge jelszavak alkalmazása gyakori jelenség az IoT-eszközökön. Ezek az eszközök többnyire nem rendelkeznek billentyűzettel, így beállításukat távolról szükséges végezni. Sajnálatos módon nem minden gyártó kényszeríti a felhasználót arra, hogy módosítsa a készülék alapértelmezett jelszavát, és sok esetben felesleges korlátozások beültetésére kerül sor, amelyek pedig ellehetetlenítik a megfelelő hosszúságú, összetett jelszavak meghatározását.

Az Open Web Application Security Project (OWASP) „Top Ten Internet of Things Vulnerabilities" listája összegzi a legkritikusabb veszélyeztetettségeket, illetve támadási vektorokat az IoT tekintetében. Ezek a következők:

- bizonytalan környezet,
- elégtelen hozzáférés-vezérlés,
- bizonytalan memória,
- nem biztonságos fizikai interfészek,
- nem biztonságos webes felület,
- bizonytalan firmware,
- nem biztonságos hálózati szolgáltatások,
- nem biztonságos adminisztrációs felület,
- bizonytalan helyi adattárolás,
- bizonytalan felhőalapú interfészek.[1]

Az IoT biztonsági elvárásai különböznek az adott rendszer kockázati besorolásától függően. Egy öntözőrendszer részét képező eszköz biztonsági igényei különböznek egy összetett, missziókritikus, kőolajkút fúrását vagy csővezeték üzemeltetését lehetővé tévő IoT-rendszer csatlakoztatott szelepeinek és szivattyúinak biztonsági igényeitől.

Kulcsfontosságú azon szempont megvizsgálása, miszerint – bármely IT-rendszer biztonságát tekintve – a rendszer nem támaszkodhat folyamatosan minden egyes elemének sértetlenségére ahhoz, hogy az egész rendszer sértetlensége biztosított legyen. Az IoT-rendszer kialakítása és annak biztonsági funkciói abból indulnak ki, hogy egyes eszközök kompromittálódhatnak (nincs 100%-os biztonság), de maga a rendszer továbbra is biztonságosan üzemelhet egy-két kompromittálódott eszközzel.[2]

## 3. Az IoT-rendszer architektúrája

Több lehetséges konfiguráció jelentkezhet az IoT-rendszerek tekintetében. Egyes IoT-rendszerek esetében az eszközök közvetlenül csatlakoznak az internetre, és minden egyes eszköz a saját biztonságáért felel. Más rendszerek esetében az eszközök helyben csatlakozhatnak egy csomóponthoz (gateway), amely aggregálja a helyi eszközök adatait. Emellett vannak felhőalapú technológiákhoz csatlakozó eszközök, peer-to-peer illetve teljes hálózati topológiát alkotó eszközarchitektúrák.

Egy további, szintén kulcsfontosságú szempont a humán erőforrás, illetve a tipikus felhasználó, fogyasztó. A felhasználónak nagyon sok minden elérhető a mobil eszközén keresztül. Így a mobil eszköz egyrészt egy ablakot képez a csatlakoztatott eszközök felé, másrészt viszont egy biztonsági gócpontot is jelent a sérülékenységekkel való visszaélés vonatkozásában.

---

[1] *OWASP Internet of Things Project*. Elérhető: www.owasp.org/index. php/OWASP_Internet_of_Things_Project (A letöltés dátuma: 2016. 11. 01.)

[2] *IBM point of view: Internet of Things Security* (2015). Elérhető: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=RAW14382USEN (A letöltés dátuma: 2018. 03. 22.)

## 4. Otthoni hálózati topológia

A mai otthoni hálózatokat jellemzően széles sávú routerek alakítják, amelyek internetes hozzáférést biztosítanak a csatlakoztatott eszközöknek wifin vagy Ethernet kapcsolaton keresztül. Leginkább laptopok, asztali gépek és további mobil eszközök (mint például okostelefonok, táblagépek) csatlakoznak az otthoni hálózatokhoz. Mindezen eszközök a helyi hálózathoz csatlakoznak, és szabadon kommunikálhatnak egymással. Az internethez való csatlakozás a központi routeren keresztül valósul meg, amely router – típustól függően – rendelkezhet alapvető tűzfalvédelemmel is.

Az IoT térhódításával egyre több eszköz csatlakozik ugyanazon számítógépes hálózathoz. Ezen eszközöket két osztályba sorolhatjuk. Az elsőbe azok tartoznak, amelyek a már meglévő hálózati technológiákat alkalmazzák, mint például a wifi vagy Ethernet – ilyen például egy TV set-top box. A másik osztályba sorolhatók azok az eszközök, amelyek különböző vezeték nélküli technológiákat alkalmaznak, mégpedig olyanokat, amelyek eleget tesznek az adott eszközök igényeinek, mint például az érzékelők csökkentett energiahasználatú kommunikációs technológiája. Sajnos nincs meghatározott szabványos kommunikációs protokoll az IoT esetében, ami önmagában is biztonsági kockázatot jelent.

## 5. Támadási felület

A támadók többféle módon hallgathatják le az otthoni okoseszközök kommunikálását, illetve módosíthatják ezen eszközök előrelátott működését. Egyes esetekben az eszközhöz való fizikai hozzáférésre van szükség, ami azonban nehezíti a támadás végrehajtását, hiszen ritkábban van alkalom fizikailag elérni a célzott eszközt. Más esetekben a támadás távolról is végrehajtható az interneten keresztül. Alábbiakban támadási vektorokat mutatunk be a támadó szükséges hozzáférési szintje szerint.[3]

### 5.1. A fizikai hozzáférés

Természetesen, a fizikai hozzáférés a legmagasabb szintű, amikor is a támadó fizikailag hozzáfér a támadni kívánt eszközhöz. Noha ez úgy tűnhet, mint egy valószínűtlen támadási felület, mégis indokolt fenyegetettségnek tekinteni. Barátok megtréfálhatják az eszköz tulajdonosát egy látogatásuk során, volt élettárs átkonfigurálhatja az eszközt, amíg el nem költözik stb.

Egy másik fenyegetettség e szinten a használt IoT-eszközök piaca. Egyesek használt eszközöket vásárolnak az interneten, hogy olcsóbban hozzájussanak azokhoz, viszont ilyenkor nincsenek tudatában annak, hogy magas a kockázata, hogy egy ilyen eszközt az eredeti tulajdonos kémkedés céljából módosított és úgy értékesített.

Megtörténhet az is, hogy az eszközök gyártóját támadják meg, és kártevő programmal fertőzik meg a rendszerét. Így minden olyan eszköz, amely a fertőzött szoftveres frissítést telepíti, kompromittálódik.

---

[3] Ballano Barcena, M. – Wueest, C. (2015): *Insecurity in the Internet of Things.* Symantec Corporation.

Az eszközhöz való fizikai hozzáférés lehetővé teszi a támadónak, hogy az eszközről részletes elemzést végezzen: sérülékenységek, hátsó kapuk, fejlesztési hiányosságok, illetve titkosítási beállítások feltárása válik lehetővé. Ezek tudatában saját maga is elkészíthet egy, az eszközt működtető rosszindulatú szoftvert (firmware-t), s telepítheti azt a kiszemelt eszközre.

Ez utóbbiak azért is lehetségesek, mert az IoT-eszközök nagy többsége nem alkalmaz titkosítást, digitális aláírást szoftvereik frissítése során.

## 5.2. Felhőalapú technológiákkal vezérelt IoT-eszközök

Ebben az esetben az otthoni okoskészülék folyamatos kapcsolatban áll a felhővel. Az eszköz ellenőrzi a felhőalapú szolgáltatáson keresztül, hogy van-e számára futtatandó parancssor vagy telepítendő frissítés, valamint feltölti a saját működési státusát.

Sajnos az eszközök nagy többsége nem végez tanúsítványhitelesítést, hogy azáltal megállapíthassa a gyártó hitelességét. Továbbá nem kerül sor az SSL/TLS kétoldalú hitelesítésére sem: a kiszolgáló hitelesítteti magát a klienssel, de ez fordítva nem érvényes. A CRL-listákat nem veszik figyelembe, így olyan tanúsítványok is felhasználhatók, amelyek már korábban kompromittálódtak.

### *5.2.1. Felhőalapú infrastruktúra*

A felhőalapú szolgáltatók többsége lehetővé teszi a felhasználónak, hogy gyenge jelszót válasszon magának a hozzáféréshez, mint amilyen például az „1234”. Továbbá a szolgáltatók gyakran különféle korlátozásokkal ellehetetlenítik az összetett, erős jelszavak beállítását. Ilyen korlátozás például, amikor csak négyjegyű PIN-kódot adhatunk meg jelszóként. A támadó, ismerve a felhasználó e-mail-címét „brute force” módszerrel felderítheti a hozzárendelt PIN-kódot, és átveheti a vezérlést az eszköz felett.

A szolgáltatók/szolgáltatások általában nem zárolják a felhasználói azonosítót meghatározott számú sikertelen bejelentkezés után, ami ugyancsak kivitelezhetővé teszi a „brute force” típusú támadást. A felhőalapú szolgáltatások nem támogatják a kétfaktorú azonosítást sem.[4]

## 5.3. Rosszindulatú szoftver

Kártevők telepítése bármely otthoni, számítógépes hálózatra csatlakozó okoseszközre, lehetővé teszi, hogy a rosszindulatú szoftverek vezérelni tudják a hálózaton lévő eszközöket, a fentiekbe foglaltak szerint. Például egy kompromittálódott okostelefon vagy számítógép egyéb eszközök megtámadására is felhasználható. A legnagyobb gond talán az, hogy a fertőzött eszköz kompromittálódva marad huzamosabb ideig, hiszen az IoT-eszközök nem

[4] Ballano Barcena–Wueest 2015.

rendelkeznek integrált biztonsági megoldásokkal, amelyek a fertőzést észlelnék, és jelezni tudnák a fogyasztó felé.

Valószínűleg már nem kell sok idő ahhoz, míg a támadók rájönnek, miként tudnának nyereséget szerezni az IoT-eszközök támadásából, így hamarosan bekövetkezhet az okostévék zsarolóvírussal való megfertőzése, vagy a hűtőszekrények felhasználása DDoS-típusú támadásokra stb.

Az IoT-eszközök vezeték nélküli kapcsolatuknak protokolljai potenciálisan többek között a következő fenyegetettségeknek vannak kitéve:

- hálózati adatforgalom lehallgatása,
- injektálás,
- változtatás/meghamisítás,
- megakadályozás,
- akkumulátor lemerítése.[5]

Az OWASP szerint az alábbiak a legkritikusabb webes sérülékenységek:

- a felhasználónév listázásának lehetősége,
- gyenge jelszavak beállítása,
- a fiókzárolás hiánya,
- titkosítatlan szolgáltatások,
- a kétfaktorú azonosítás lehetőségének hiánya,
- rosszul végrehajtott titkosítás,
- frissítés titkosítás nélküli megküldése,
- szolgáltatás megtagadása,
- tároló médium eltávolítása.[6]

Az IoT-eszközök biztonságát két szinten szükséges biztosítani ahhoz, hogy védettségük átfogó és teljes legyen. Egyik szint a biztonságos IoT-eszközök és -rendszerek tervezése/fejlesztése, a másik az IoT-eszközök üzemeltetésének biztonsága.

### *5.3.1. Az IoT-eszközök és -rendszerek biztonságos tervezése/fejlesztése*

Az IoT-eszközöket úgy kell fejleszteni, hogy azok biztonsága megvalósulhasson, és a biztonsági funkciók alapbeállításban is alkalmazhatók legyenek. Ezen célból már a tervezés során átfogó elemzést kell végezni a konkrét eszköz lehetséges támadási vektorainak szempontjából. A fejlesztési folyamat szerves részét kell, hogy képezze a fenyegetettségek azonosítása, illetve azok megvalósulási esélyeinek csökkentése.

A fejlesztőknek követniük kell a biztonsági irányelveket a programozás során, hogy így egy biztonságos környezetet alakítsanak ki az IoT-eszközök működéséhez.

Gyakran előfordul, hogy a fejlesztők nyílt forráskódot alkalmaznak, ami a gyors fejlesztést valóban serkenti, viszont sérülékenységek nagy számát jeleníti meg a rendszerben.

---

[5] Ballano Barcena–Wueest 2015.

[6] *OWASP Internet of Things Project.* Elérhető: www.owasp.org/index. php/OWASP_Internet_of_Things_Project (A letöltés dátuma: 2016. 11. 01.)

Ilyenkor nehezíti a helyzetet, hogy olyan nyílt forrású komponenseket alkalmaznak, amelyek már jól ismert sérülékenységeket hordoznak magukban, mint például az OpenSSL esetében a „Heartbleed". Éppen azért, mert jól ismert sérülékenységekről van szó, részletes dokumentáció áll rendelkezésére a támadónak magáról a sérülékenységről, illetve annak kihasználási módszereiről.[7] Összegezve, a tervezés során a következőket a legfontosabb biztosítani:

- biztonsági irányelvek követése fejlesztéskor,
- többrétegű védelmi megoldások alkalmazása,
- üzembiztos működés, még ha ez azt is jelenti, hogy alkalmanként az eszköz lekapcsolódik az informatikai hálózatról.

## 6. Adatvédelem

Az eszközök felé, illetve a tőlük irányuló adatforgalom, valamint az általuk tárolt adatok érzékeny adatok lehetnek. Egy mobil bankolási alkalmazás az okostelefonon hitelkártya-adatokat tárolhat, amelyekhez pedig hozzáférhetne egy csatlakoztatott IoT-eszköz is, ha nincs kellő védelem alkalmazva.

Az eszközökről begyűjtött adatok információt adhatnak arról, hogy ki, mikor és hol tartózkodott, és esetleg még arról is, hogy az illető milyen műveletet hajtott végre. Természetesen felvetődik a kérdés: miként kezelik ezeket az adatokat, ki fér hozzájuk, mire használhatják fel őket stb. A fejlesztőknek az IoT-eszközök tervezése során kötelezően figyelembe kell venniük az adatok titkosságának megőrzését.

Az adatvédelem egy másik szempontját az adatmegőrzés jelenti. A begyűjtött adatok mennyisége egyre csak nő, így fokozódik annak a lehetősége is, hogy valamely adatokkal visszaélés történjen. Ennek megelőzéséhez megfelelő adatmegőrzési, illetve selejtezési eljárási rendeket szükséges alkalmazni. A legjobb megoldás az lenne, ha az adatokat – amint nincs már rájuk szükség – törölnék, ha ezt a törlést a törvényi rendelkezések lehetővé is teszik az adott esetre vonatkozóan.[8] A legfontosabb irányelvek az adatvédelem tekintetében a következők:

- adatelválasztás alkalmazása,
- személyazonosításra alkalmas adatok átalakítása,
- egyedi eszközazonosítók alkalmazása,
- külön azonosítók alkalmazása az adatátvitelre, illetve -tárolásra.

## 7. Biztonsági tesztelések

A sérülékenységi tesztelések végrehajtásának gyakorlata szerves része kell, hogy legyen a beültetési folyamatoknak. Ezen tesztelések hasonlóképpen végezhetők, mint az egyéb esetekben megszokottak.

---

[7] *IBM point of view: Internet of Things Security* (2015). Elérhető: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=RAW14382USEN (A letöltés dátuma: 2018. 03. 22.)

[8] *IBM point of view: Internet of Things Security* (2015). Elérhető: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=RAW14382USEN (A letöltés dátuma: 2018. 03. 22.)

Kiemelkedő irányelv e téren a sérülékenységi tesztelések végrehajtása, valamint a forráskód elemzése, etikus hack alkalmazása.

## 8. A folyamatos fejlesztés modellje

A biztonság mindkét formája igen fontos, a megelőző és a vizsgálati is. A folyamatos fejlesztés modellje megkönnyíti a reakciót és az irányítást a korábbi mechanizmusokhoz viszonyítva, mint amilyenek például a termékkibocsátás, javítócsomag stb. A következő irányelveket határozhatjuk meg e téren: a hibák és a sérülékenységek észlelését lehetővé kell tenni, a folyamatos fejlesztés modelljét kell alkalmazni.

## 9. Az IoT-eszközök üzemeltetésének biztonsága

Akármennyire is törekednek a fejlesztők, tesztelők és gyártók arra, hogy megakadályozzák eszközük sérülékeny voltát és támadhatóságát, a gyakorlatban mindig megmarad annak esélye, hogy egy aktív sérülékenységre fény derüljön, és támadást indítsanak. A támadások elleni védelemnek is így többrétegűnek kell lennie (tűzfal, adatszűrés stb.)

A tárgyak hálózatát működtető számítógépes környezetben a routerek is támadási célpontok lehetnek. Ezeket ugyanúgy korlátoztatni kell, mint az általuk védett eszközöket, és folyamatos fejlesztési eljárási rendeket kell alkalmazni.

A következő irányelveket szükséges érvényesíteni: többrétegű védelmi megoldások alkalmazása; az alrendszerek elszigetelésének lehetősége, amennyiben kompromittálódnak.

A kommunikációs csatornák biztosításához a következőket szükséges elvégezni:

- az eszközök és rendszerek kommunikációs csatornáit védetté kell tenni,
- a külső hálózatokat bizalmatlanként szükséges kezelni,
- a kommunikációs protokollok irányelveit szigorúan be kell tartani,
- ha IP-protokollról van szó, akkor TLS-t szükséges alkalmazni.

### 9.1. Az alkalmazási szokások követése és elemzése

A számítógépes világban lehetetlen előrelátni valamennyi lehetséges támadást egy adott rendszert ellen, s főleg nehéz megakadályozni azokat. A számítógépes környezet sikeres vezérléséhez nélkülözhetetlen a rendszer felügyelete, a figyelmet igénylő esetek sikeres feltárása, és ezen esetek megfelelő kezelése. A támadásokat észlelni kell, és válaszolni kell rájuk, ha lehet, azonnal. Ilyen esetek lehetnek például a következők: sérült integritású eszközök, DDoS-támadások, folyamatos támadások az adott eszközt, illetve a hálózaton lévő valamennyi eszközt célozva. Amennyiben a rendeltetésszerű alkalmazási szokásokról mintavételezésre kerül sor a rendszerben, úgy feltárhatók lesznek az eltérések, és megfelelő intézkedésekre kerülhet sor.

Kulcsfontosságú az események nyomon követése, felügyelete, akár eszköz-, akár rendszerszinten. Aktív felügyelettel lehetséges egyedül a biztonsági események feltárása és az időbeni, megfelelő intézkedések meghozatala.[9]

A következőket szükséges megvalósítani:

- megfelelő felderítési módszertanok alkalmazása a biztonsági esetek hatékony feltárására,
- naplóelemzés alkalmazása.

## 10. A kockázatok csökkentése

Ahogy korábban már említettük, a felhasználók nem tudnak könnyen védelmi megoldásokat alkalmazni az IoT-eszközeik biztonságossá tételének tekintetében, mivel az eszközök leggyakrabban nem is támogatják ezen funkciókat. Ettől függetlenül a következők betartásával csökkenthetők a biztonsági kockázatok:

- erős jelszavak alkalmazása, mind az eszközökön, mind a wifihálózaton,
- a beépített, gyári, alapértelmezett jelszavak megváltoztatása,
- a wifihálózatokon megfelelő titkosítás alkalmazása (például WPA2),
- vezetékes hálózat alkalmazása, az összes lehetséges ponton,
- az IoT-eszközök távoli elérését kellően meg kell védeni, illetve a távoli elérés lehetőséget le kell tiltani, ha nincs rá szükség,
- kellő figyelmet kell fordítani a használt IoT-eszközök vásárlása során az eszközök sértetlenségére,
- alkalmazni kell a gyártó biztonsági funkcióit,
- le kell tiltani a nem alkalmazandó funkciókat,
- rendszeres frissítést kell alkalmazni az eszközön; az eszköz mindig legyen naprakész,
- amennyiben lehetséges, az IoT-eszközök elkülönített hálózatra csatlakozzanak,
- meg kell vizsgálni, hogy újraindítás, illetve áramkiesés után az eszközök továbbra is biztonságos üzemmódban maradnak-e,
- meg kell fontolni, hogy szükség van-e az eszköz „okosságára”, vagy pedig elegendő az adott eszköz hagyományos verzióját használni.

Ugyanakkor a gyártóknak minimum a következő intézkedéseket kell végrehajtaniuk a biztonsági kockázatok csökkentése érdekében:

- a kommunikáció során TLS-titkosítás alkalmazása szükséges,
- ellenőrizni kell a TLS-tanúsítvány hitelességét és érvényességét,
- lehetővé kell tenni az erős jelszavak alkalmazását,
- kötelezővé kell tenni felhasználónak a beépített, gyári jelszavak megváltoztatását,
- biztonságossá kell tenni a frissítések folyamatát,
- alkalmazni kell a felhasználói azonosító felfüggesztését meghatározott számú esetben tévesen beírt jelszó során,

[9] *IBM point of view: Internet of Things Security* (2015). Elérhető: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=RAW14382USEN (A letöltés dátuma: 2018. 03. 22.)

- az ismert sérülékenységeket nyomon kell követni, és az eszközöket velük szemben védeni kell,
- üzembiztos módot kell alkalmazni áramkiesés vagy (informatikai) hálózati gondok esetén.

## 11. Visszaélések (lehetőségének) példái

A tanulmányban említett és leírt hiányosságok miatt sikeren támadhatók az internetes hálózatra csatlakoztatott eszközök. A támadások lehetnek tréfajellegűek, de lehetnek igen komoly következményekkel járó esetek is. Alább olvasható néhány visszaélési példa megtörtént esete.

- Gépjármű hack – fékek megbénítása; ablaktörlő, duda, rádió stb. távoli vezérlését tette lehetővé.[10]
- Otthoni webkamerák meghackelése – illetéktelen személyek betekinthettek az adott webkamerák felhasználóinak lakásába, hálószobáiba stb.[11]
- Egészségügyi eszközök hackelése – szívritmus-szabályozó (pacemaker) elleni támadás, amely lehetővé tette, hogy a pacemaker rendkívül magas szívritmust diktáljon, illetve lemerítette a pacemaker elemét.[12]
- Kávéfőző hack – tréfajellegű támadás.[13]
- Sportkarkötők hackelése – a karkötők rendeltetésüktől elértő funkciókra való felhasználása.[14]
- DDoS-támadás térmegfigyelő kamerákkal – egy aranyművest kb. 25 ezer CCTV-kameráról indított DDoS-módszerrel támadtak meg.[15]
- Fűtőrendszer megbénítása – megbénították egy finnországi város központi fűtőrendszerét a tél közepén.[16]
- Orosz bankok elleni támadás – 2016. november második hetén DDoS-támadásra került sor öt orosz bank ellen, amely támadásban IoT-eszközöket is felhasználtak.[17]
- Az internet félnapi megbénítása [22] – 1 Tbps sebességű DDoS-támadásra került sor, amely több mint 150 ezer eszközről eredt. A támadás egy internetet működ-

[10] *Hackers Remotely Kill a Jeep on the Highway – With Me in It* (2015). Elérhető: www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ A letöltés dátuma: 2016. 11. 10.)

[11] *Russian webcam hackers spy on bedrooms and offices* (2014). Elérhető: www.cnbc.com/2014/11/20/russian-webcam-hackers-spy-on-bedrooms-and-offices.html (A letöltés dátuma: 2016. 11. 09.)

[12] *Muddy Waters Capital LLC* (2016). Elérhető: http://d.muddywatersre search.com/wp-content/uploads/2016/08/MW_STJ_08252016_2.pdf (A letöltés dátuma: 2016. 11. 09.)

[13] *Hacking the Wi-Fi IoT Coffee Machine. Pen Test Partners LLP* (2015). Elérhető: www.youtube.com/watch?v=4-WEQpiyfb50 (A letöltés dátuma: 2016. 11. 07.)

[14] *Custom Firmware Unlocks Fitness Tracker* (2016). Elérhető: http://hackaday.com/ 2016/07/03/custom-firmware-unlocks-fitness-tracker/ (A letöltés dátuma: 2016. 11. 09.)

[15] *IoT Botnet — 25,000 CCTV Cameras Hacked to launch DDoS Attack* (2016). Elérhető: http://thehackernews.com/2016/06/cctv-camera-hacking.html (A letöltés dátuma: 2016. 11. 14.)

[16] *DDoS Attack Takes Down Central Heating System Amidst Winter in Finland* (2016). Elérhető: http://thehackernews.com/2016/11/heating-system-hacked.html (A letöltés dátuma: 2016. 11. 01.)

[17] *Russian Banks Suffer Wave of Ddos Attacks* (2016). Elérhető: www.scmagazine.com/russian-banks-suffer-wave-of-ddos-attacks/article/572503/ (A letöltés dátuma: 2016. 11. 11.)

tető cég ellen irányult, így aznap emberek milliói nem tudták megnyitni kívánt oldalukat az interneten. A támadásban térmegfigyelő kamerák DVR-jei is fel lettek használva mint támadást indító eszközök.[18]

A helyzetet súlyosbítja, hogy megjelentették a kártevő forráskódját, amely felhasználásával DDoS-jellegű további támadások indíthatók.[19]

## 12. Összegzés

A tárgyak internetének piaca egyre rohamosabban növekvő trendet mutat, az informatikai hálózatra csatlakoztatott okoseszközök valósággá válnak, legyen szó akár mobil eszközökről, háztartási készülékekről, egészségügyi berendezésekről vagy implantátumokról vagy gépjárművekről, zárakról, ajtókról stb. Noha funkcionalitás szempontjából eleget tesznek a fogyasztói elvárásoknak, a védelmi mechanizmusokat rendszerint figyelmen kívül hagyják. Ennek eredménye pedig az, hogy emberek milliói vannak veszélyeztetve csúcstechnológiai támadások tekintetében az IoT-eszközök révén.

A gyártóknak, s ugyanúgy a felhasználóknak is nélkülözhetetlen a biztonsági irányelvek betartása/betartatása az IoT-eszközök biztonságos fejlesztése és üzemeltetése érdekében. A tanulmányban megfogalmazott irányelvekkel csökkenthetők a biztonsági kockázatok e téren.

## Felhasznált irodalom

*A New Approach to IoT Security* (2015). PubNub.

Ballano Barcena, M. – Wueest, C. (2015): *Insecurity in the Internet of Things.* Symantec Corporation.

*Cisco IoT System Security: Mitigate Risk, Simplify Compliance, and Build Trust* (2015). Cisco Systems, Inc.

*Custom Firmware Unlocks Fitness Tracker* (2016). Elérhető: http://hackaday.com/ 2016/07/03/custom-firmware-unlocks-fitness-tracker/ (A letöltés dátuma: 2016. 11. 09.)

*DDoS Attack Takes Down Central Heating System Amidst Winter In Finland* (2016). Elérhető: http://thehackernews.com/2016/11/heating-system-hacked.html (A letöltés dátuma: 2016. 11. 11.)

*Hackers Remotely Kill a Jeep on the Highway – With Me in It* (2015). Elérhető: www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (A letöltés dátuma: 2016. 11. 10.)

*Hacking the Wi-Fi IoT Coffee Machine. Pen Test Partners LLP* (2015). Elérhető: www.youtube.com/watch?v=4WEQpiyfb50 (A letöltés dátuma: 2016. 11. 07.)

*IBM point of view: Internet of Things Security* (2015). Elérhető: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=RAW14382USEN (A letöltés dátuma: 2018. 03. 22.)

[18] *Your DVR Didn't Take Down the Internet Yet* (2016). Elérhető: www.wired.com/2016/10/internet-outage-web-cam-dvr-botnet/ (A letöltés dátuma: 2016. 11. 10.)

[19] *Source Code for Iot Botnet Responsible for World's Largest Ddos Attack Released* (2016). Elérhető: https://thehackernews.com/2016/10/mirai-source-code-iot-botnet.html (A letöltés dátuma: 2016. 11. 14.)

*IoT Botnet — 25,000 CCTV Cameras Hacked to launch DDoS Attack* (2016). Elérhető: http://thehackernews.com/2016/06/cctv-camera-hacking.html (A letöltés dátuma: 2016. 11. 14.)

*Muddy Waters Capital LLC* (2016). Elérhető: http://d.muddywatersre search.com/wp-content/uploads/2016/08/MW_STJ_08252016_2.pdf (A letöltés dátuma: 2016. 11. 01.)

*OWASP Internet of Things Project.* Elérhető: www.owasp.org/index. php/OWASP_Internet_of_Things_Project (A letöltés dátuma: 2016. 11. 01.)

*Russian Banks Suffer Wave of Ddos Attacks* (2016). Elérhető: www.scmagazine.com/russian-banks-suffer-wave-of-ddos-attacks/article/572503/ (A letöltés dátuma: 2016. 11. 11.)

*Russian webcam hackers spy on bedrooms and offices* (2014). Elérhető: www.cnbc.com/2014/11/20/russian-webcam-hackers-spy-on-bedrooms-and-offices.html (A letöltés dátuma: 2016. 11. 09.)

*Source Code for Iot Botnet Responsible for World's Largest Ddos Attack Released* (2016). Elérhető: https://thehackernews.com/2016/10/mirai-source-code-iot-botnet.html (A letöltés dátuma: 2016. 11. 14.)

*Your DVR Didn't Take Down the Internet Yet* (2016). Elérhető: www.wired.com/2016/10/internet-outage-webcam-dvr-botnet/ (A letöltés dátuma: 2016. 11. 10.)