Magyar Rendészet 2024/2. 69–88. DOI: 10.32577/mr.2024.2.4

Látható barátból láthatatlan ellenség – A kényelem ára

BÖCSKEI Renáta[1] **– TÓTH Levente**[2]

A rohamosan növekvő technikai és technológiai fejlődés következtében, valamint a digitális átalakulás és az információtechnológia terjedésével egyre népszerűbbé válnak az IoT- (Internet of Things) eszközök. Ezek ma már szinte mindenhol jelen vannak, elég csak az okosotthonokra, az önvezető autókra, az okos biztonságtechnikai eszközökre vagy épp az IoT-technológián alapuló gyártósorokra gondolni. Ma már az érték nemcsak anyagi formában létezik, és nemcsak a fizikai térben manifesztálódik, hanem létrejöhet és tárolódhat a kibertérben is. Már csak ezért is fontos tárgyalni és megismerni az eszközökkel kapcsolatos veszélyeket, amelyek megelőzésére ugyanúgy fel kell készülni mind a valós fizikai, mind pedig a kibertérben.

Kulcsszavak: *IoT, okosotthon, kiberbűnözés, DDoS, botnet, zsarolóvírus*

Információs társadalom

Jelenlegi társadalmunkat gyakran nevezik információs társadalomnak. Az információs társadalom új fogalom, amelyet társadalomtudományokkal foglalkozó kutatók és elemzők korábban egyetlen más társadalomra sem alkalmaztak. Ennek oka, hogy egyetlen korábbi populációban sem volt ilyen mértékben hatalmi tényező az információ, mint napjaink társadalmában. Az információs társadalomnak legfőbb eleme a tudás, az innováció és legfőképpen az információ, amelynek birtoklása hatalmat jelent.[3] „Az adat az új olaj”[4] – nem véletlen, hogy napjainkban még inkább aktuálissá vált ez a mottó. Ezzel együtt pedig vitathatatlan tény, hogy a 21. század egyik legnagyobb biztonsági próbatétele az egyre fokozódó mértékben jelen lévő adat- és információáradat kezelése, biztonságos felhasználása. Az információs társadalommá válás során ugyanis nemcsak a technológia fejlődik, hanem az adatok és információk megszerzésére irányuló kibertámadások is megtöbbszöröződtek.

---

[1] Hallgató, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Magánbiztonsági és Önkormányzati Rendészeti Tanszék; közbeszerzési referens, TVT Vagyonvédelmi Zrt.; értékesítési és műszaki vezető, ESDA Kft., e-mail: renatabocskei@gmail.com

[2] Tanársegéd, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Magánbiztonsági és Önkormányzati Rendészeti Tanszék; szakmai igazgató, TVT Vagyonvédelmi Zrt., e-mail: toth.levente@uni-nke.hu

[3] Belláz et al. 2020.

[4] Ezzel a címmel tartott előadást Clive Humby adatkutató 2006-ban az Association of National Advertisers konferenciáján. Beszédében Humby azt állította, hogy a nyers adatokat ugyanúgy fel kell dolgozni, mint a kőolajat, hogy az értékes legyen.

Mi az IoT?

Az

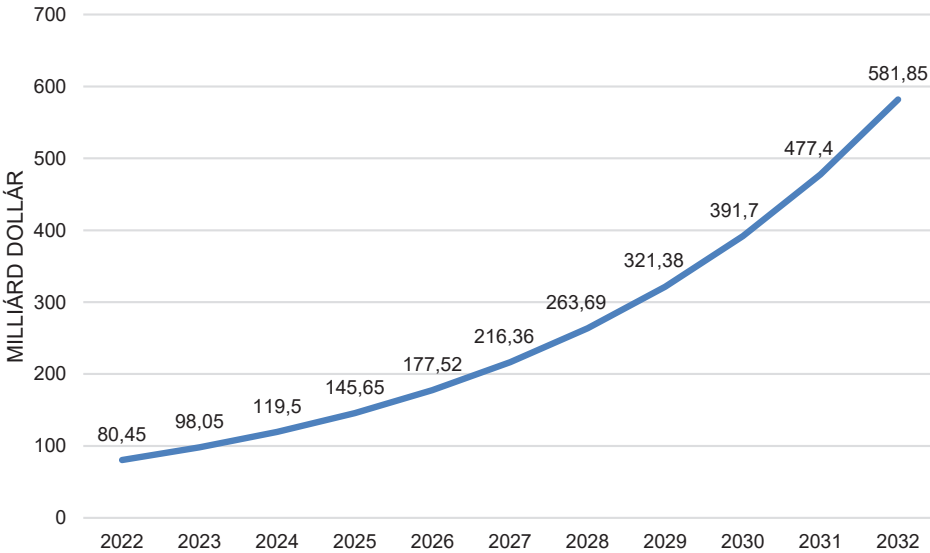
> „IoT minden olyan dolog és használati tárgy, amely egy hálózaton (általában az interneten) keresztül más gépekhez csatlakozva, általában kétirányú kommunikációval, emberi beavatkozás nélkül működik. A működés közben keletkező adatokat, információkat képesek más berendezésekre eljuttatni, és valamilyen technológia segítségével, akár netes adatbázisok, felhőalapú rendszerek révén a világ bármely pontján megosztani. Az IoT-berendezéseket sokszor nevezik »okos«-nak, vagy »smart«-nak is."[5]

Az élet számos területén találkozhatunk IoT-eszközökkel. Ilyen eszközök például az okosotthonrendszerek alkotóelemei (például okosvilágítás, okoszárak, okostermosztátok, okoskonnektorok, okoskamerák), az egészségügyi eszközök (például okoskarkötők, okosmérlegek, okos-vérnyomásmérők), az okosváros-technológiák (például okos parkolási rendszerek, légminőség-érzékelők, hulladékkezelő rendszerek), az okosközlekedési megoldások (például önvezető autók, okos közlekedési lámpák, közlekedési kamerák), az ipari IoT-eszközök (például okosszenzorok, okosgyártósorok, okos energiahatékony eszközök), valamint a mezőgazdasági IoT-eszközök (például okos-öntözőrendszerek, talajnedvesség-érzékelők, okos mezőgazdasági gépek). Összességben elmondható, hogy mára az IoT-eszközök körének gyakorlatilag csak a fantázia szabhat határt. Az IoT-technológia folyamatos fejlődése újabb és újabb alkalmazási területeket nyit meg ezeknek az eszközöknek. A technikai és technológiai fejlődés leginkább felívelőben lévő innovációi az IoT-eszközök, amelyek piaca a 2019-es 8,6 milliárd eszközről 2030-ra várhatóan 29,42 milliárdra nő.[6]

IoT-eszközök az otthonunkban

Az IoT fogyasztói és magáncélú alkalmazási területe leginkább az intelligens otthonokban mutatkozik meg, alkalmazásuk pedig évről évre növekszik, ahogy az abból származó bevételek is egyre nőnek. Míg 2022-ben 80,45 milliárd dollár volt a bevétel, addig 2023-ban 98,05, 2032-re pedig 581,85 milliárd dollárt prognosztizálnak.[7]

[5] Boda 2019: 104.
[6] Vailshery 2023.
[7] Precedence Research 2023.



1. ábra: Az okosotthon piacának bevétele világszinten 2022–2032

Forrás: a szerzők szerkesztése Precedence Research 2023 alapján

Okosotthonokban IoT-eszközök többek között a kaputelefon és -csengő, a kül- és beltéri mozgásérzékelők, a kül- és beltéri kamerarendszer, az ajtó- és ablaknyitás-érzékelők, a tűzjelző rendszer, a szén-monoxid-jelző rendszer, a fénytechnikai rendszerek, a hűtés-fűtés és légtechnikai rendszerek, fogyasztásmérő berendezések, a szórakoztatóelektronikai rendszerek és a háztartási berendezések lehetnek. Ezt a technológiát használják továbbá a garázskapuk vezérlésére, az öntözőrendszerek automatizálására, a napelemek felügyeletére, a kerti világítások kezelésére és akár az árnyékolástechnikára is.

Fontos kiemelni, hogy egy otthon nem válik automatikusan okosotthonná pusztán azáltal, hogy távolról vezérelhető eszközöket telepítünk. Attól, hogy távolról fel tudjuk kapcsolni a lámpát, el tudjuk indítani a mosógépet, vagy rá tudunk nézni a kamerarendszerre, még nem beszélhetünk okosotthonról, de az, hogy eszközeink távolról vezérelhetők legyenek, kétségkívül kihagyhatatlan lépés. Az igazi intelligencia abban rejlik, ha az eszközök képesek adatok gyűjtésére, elemzésére, összefüggések felismerésére, és ezek alapján önálló döntések meghozatalára, valamint összehangolt cselekvésre. Az intelligens otthonok irányításának kiemelten fontos kérdése az integrálhatóság: hogy az eszközöket egy platformon tudjuk egymáshoz csatolni és rendszerként működtetni. Azaz eszközeink az adatmegosztás révén egységes, organizált rendszerként tudjanak működni.

A támadók motivációi

Az internethez kapcsolódó IoT-eszközök ezzel együtt komoly biztonsági kockázatot jelentenek, ami egyéni és globális szinten is problémákat okozhat. „Minden, ami felkapcsolódik az Internetre, meghekkelhető. Az okosotthonnal a meghekkelhető otthon is létrejön, […].”[8]

Az IoT-rendszerek sérülékenysége nem csupán abban rejlik, hogy a támadó hozzáférhet az eszközeinkhez és átveheti felettük az irányítást, hanem egy pivot támadás[9] keretében az eszközünket kiindulópontként használhatja a hálózatunkon lévő más eszközök megtámadására is. A „breakout time” kifejezést a CrowdStrike 2018-as Globális Fenyegetés Jelentésében használták először.[10] Ez az időtartam az az idő, amely alatt a támadó képes bejutni egy szervezet hálózatába a belépéstől számítva. Minél rövidebb a támadási idő, annál gyorsabban tud a behatoló mozogni a hálózaton belül, adatokhoz hozzáférni és kárt okozni.

A támadás irányulhat személyes adatok, bizalmas adatok, üzleti titkok megszerzésére, a megszerzett információk felhasználhatók saját célra, egy következő, nagyobb támadáshoz, illetve továbbértékesítés, nyilvánosságra hozás vagy zsarolás céljából is. Motiváció lehet továbbá egy informatikai vagy biztonsági rendszer gyenge pontjainak felfedése. A hátráltatás is gyakori cél, itt a támadás irányulhat kritikus infrastruktúra vagy azokhoz tartozó részelemek ellen, de akár a kiszemelt személy vagy cég tekintélyének, hírnevének rombolása, szándékos károkozás, saját anyagi haszonszerzés, de egy elbocsátott vagy megsértett dolgozó bosszúvágya is. Az erőfitogtatás, hírnév, hatalomgyakorlás és mások elismerésének megszerzése is lehet támadási cél. Ez esetben a támadó uralkodik a rendszer felett, uralkodik a személy, a vállalat vagy egy adott feladat felett. A siker növeli az önbizalmat, még inkább akkor, ha ezt nyilvánosság előtt éri el. Ilyenkor élnek a rongálás és vandalizmus lehetőségével, megrongálják a webhelyeket, felülírják azokat egy saját készítésű oldallal, elrontják az arculatot, adott esetben saját névjegyüket is otthagyják.

A 2023-as SonicWall Cyber Threat Report szerint 2023 első hat hónapjában az IoT-kártevők száma világszerte 37%-kal nőtt, ami összesen 77,9 millió támadást eredményezett, szemben a 2022-es év ugyanezen időszakában mért 57 millió támadással.[11] Az adatok és információk biztonságos tárolása és kezelése tehát napjaink kihívása, azzal a ténnyel pedig, hogy az IoT-eszközök a legszűkebb magánszférában is jelen vannak, a személyes biztonság és a személyes adatok védelme, azok nem megfelelő kezelése is új próbatételt jelent, és bár számtalan felhasználó veszi ezeket az eszközöket, egyre több mindent okosít és automatizál, még sincs megfelelő képe a veszélyekről.

---

8 Bálint 2018.

9 A pivot támadás *(pivot attack)* egy olyan kiberbiztonsági támadási forma, amely során a behatoló egy már meglévő, sérülékeny eszközhöz (pl. IoT-eszköz) fér hozzá, és ezt kiindulópontként használja a hálózaton lévő más eszközök megtámadására.

10 Crowdstrike 2018.

11 Marton 2023.

A 2016-os Mirai botnet támadás

A botnet (robothálózat) gyakorlatilag zombieszközök hálózata. A megfertőzött gépeken a vírus a háttérben fut, így a felhasználó nem is értesül róla. A támadó szabadon rendelkezhet azzal, hogy mire használja az irányítása alá vett számítógépeket. A hálózat mérete folyamatosan változik, hiszen a fertőzött gép további sérülékeny eszközöket toboroz. Ennek köszönhetően egyes botnetek mérete eléri a több tízezres nagyságrendet is.[12]

A fertőzés az eszközön futó szolgáltatások sebezhetőségeinek kihasználásával történik. Egy rosszindulatú kód beszúrása a webes felületre küldött kérésekbe a sebezhetőségek kihasználásának leggyakoribb módja. Ezeknek a támadásoknak a következményei jelentősek lehetnek, például az internetszolgáltatók által a LAN-on lévő eszközök konfigurálásának automatizálására használt TR-064 protokoll megvalósításának biztonsági rése esetén. A biztonsági hiba lehetővé tette a TR-064-csomagok hitelesítés nélküli továbbítását, ami a Mirai kártevő elterjedését eredményezte; a kiberbűnözők arra használták, hogy elosztott szolgáltatásmegtagadásos (DDoS) támadásokat indítsanak vele. A szolgáltatásmegtagadásos (DoS) vagy túlterheléses támadások lényege, hogy a támadók – kihasználva a hálózat gyengeségeit vagy az eszközök biztonsági réseit – megtámadják az eszközöket vagy hálózatot úgy, hogy azok eltérjenek a normál működésüktől. Jellemzően a hálózati forgalom növekedését idézik elő, ezáltal a hálózat lelassul, megbénul, elérhetetlen lesz vagy teljesen összeomlik. Ha a támadás indításában egy eszköz vesz részt, akkor beszélünk DoS-támadásról, ha pedig egyszerre több eszköz indítja a támadást, akkor azt DDoS-támadásnak nevezzük.[13]

A támadások lényege tehát az, hogy annyi kérést küldenek egy adott weboldalra, amennyit az oldal terhelhetősége már nem bír el, nem tud kiszolgálni. Ha új látogató érkezik az oldalra, akkor szolgáltatásmegtagadással fog találkozni. Egyszerűbben fogalmazva, a botnettámadásokkal a támadó – kihasználva a biztonsági réseket – minél több eszközt céloz meg, és átveszi felettük az irányítást – zombihálózatot hoz létre –, majd az irányításuk alá került, külső utasításra cselekvő gépek egyszerre megkezdik a támadást a választott célpont ellen. A több tízezer, több százezer eszköz, bár önmagában csekély adatmennyiséggel dolgozik, összehangolt támadás esetén hatalmas adatmennyiséggel támadja a kiszemelt célpontot.

2016. 10. 21-én, a Mirai botnet több százezer IoT-eszközt fertőzött meg, és ennek köszönhetően több tucat nagyobb weboldal vált elérhetetlenné az USA-ban és Európában egyaránt.[14] A 2016-os botnettámadás következtében leállt a Spotify, a Twitter, a PayPal, a Reddit, az Amazon és az egyik legnagyobb streamingszolgáltató, a Netflix is.

[12] Nemzeti Kibervédelmi Intézet 2020a.
[13] Nemzeti Kibervédelmi Intézet 2018a.
[14] Flachner–Klág 2016.

A Mirai gyenge biztonsági védelemmel ellátott IoT-eszközöket (kamerákat és otthoni okoseszközöket) támadott meg és vett az irányítása alá, majd egy összetett DDoS-támadáshoz használták fel azokat. Már önmagában egyetlen sérülékeny IoT-eszköz is fenyegetést jelent, ha egy hacker átveszi felette az irányítást, hiszen – mivel ezek rendszerbe vannak kapcsolva – általa más IoT-eszközhöz is el tud jutni, és képes felhasználni azokat egy nagyobb volumenű támadáshoz. Elegendő egy IoT-eszközt megfertőzni rosszindulatú szoftverrel, azok pedig tovább fertőzik a többi hálózatba kapcsolt IoT-eszközt, ahogy történt ebben az esetben is.

A Mirai botnet 2016-os támadása óta a botnet több új variánsa jelent már meg. 2019-ben az Echobot,[15] a 2020–2021-es években a Dark Nexus,[16] a Kaiji,[17] a Mukashi, ami leginkább sérülékeny routereket támadott meg.[18] Az IoT-eszközökből álló botnetek, amelyeket elosztott DoS-támadásokhoz használnak, egyre elterjedtebbek a dark webes fórumokon, és nagy a kereslet a hackerek körében. 2023 első felében a Kaspersky Digital Footprint Intelligence szolgáltatáselemzői összesen több mint 700 DDoS-támadási szolgáltatások hirdetését fedezték fel különböző dark webes fórumokon. Egy ilyen szolgáltatás árát számos tényező befolyásolja. Függ a támadás összetettségétől, mint például van-e DDoS-védelem, CAPTCHA-kód vagy JavaScript-ellenőrzés az áldozat oldalán. A támadás összköltsége napi 20 és havi 10 000 dollár között változik. A hirdetéseket feladók által felszámított átlagos ár napi 63,5 dollár, vagyis havi 1350 dollár volt. DDoS-támadási szolgáltatással, gyakran infrastruktúrával és támogató segédprogramokkal ellátott IoT-malwareekkel is kereskednek ezeken a „sötét" fórumokon. Ritka esetekben az előre fertőzött eszközök hálózatai is megvásárolhatók.[19]

Jelszólopás

A jelszavak ellopása a legegyszerűbb támadási módszer, a leggyorsabban célravezető, ezért a hackerek körében a legnépszerűbb is. Több fajtája van, ilyen például a brute force támadás, amely leginkább rövid és egyszerűbb jelszavak esetén hatékony, lehetséges karakterek kombinációjából próbálják a jelszót összeállítani. A brute force egyik fajtája a leetspeak, ahol a támadók kulcsszavakat vagy korábban kiszivárgott jelszavakat kombinálnak. Gyakori módszer továbbá a password spraying, ahol a támadó a felhasználónevekhez keresi hozzá a korábban párosított vagy már használt jelszavakat.[20] A brute force támadások meglehetősen gyakoriak, mivel az IoT-eszközökön futó Telnet- és SSH-szolgáltatások általában széles körben ismert alapértelmezett jelszavakat használnak. Sajnos a felhasználók hajlamosak változatlanul

[15] Nemzeti Kibervédelmi Intézet 2019.
[16] Nemzeti Kibervédelmi Intézet 2020b.
[17] Nemzeti Kibervédelmi Intézet 2020c.
[18] Nemzeti Kibervédelmi Intézet 2020d.
[19] Kaspersky Security Services 2023.
[20] Nemzeti Kibervédelmi Intézet 2018b.

hagyni ezeket a jelszavakat. Épp ezért az okosotthonokban a vezeték nélküli hálózatok elengedhetetlen eleme lenne a titkosított csatorna, valamint az erős jelszavak, a kétlépcsős hitelesítés használata.

Mindehhez tudni kell, hogy az eszközgyártók a kétezres évek eleje óta alapbeállításokkal ruházzák fel az eszközöket, az alapértelmezett jelszavak pedig minden nehézség nélkül bárki számára fellelhetőek az interneten.[21]

Sok felhasználó ennek ellenére nem változtatja meg ezeket, vagy nem használ erős jelszavakat, kétlépcsős hitelesítést a védelem érdekében. Ennek köszönhetően a támadók az alapértelmezett jelszavak felhasználásával könnyedén hajtanak végre támadást.

1. táblázat: Alapértelmezett jelszavak és leggyakrabban használt jelszavak

Eszköz	Alapértelmezett felhasználónév	Alapértelmezett jelszó	Leggyakrabban használt jelszavak 2020-ban és 2021-ben
Dahua IP kamera	admin	admin	123456 (és változatai)
Dahua IP kamera	888888	888888	picture1
Dahua IP kamera	666666	666666	password
HIKVision IP kamera	admin	12345	111111
TP Link	admin	admin	123123
Netgear	admin	password	admin
Unifi	ubnt	ubnt	root
Axis kamera	root	pass	nc11
Cisco switch	admin/cisco/nincs	admin/cisco/nincs	user
LTS Security	admin	123456	enable
Samsung IP kamera	admin	111111	0

Forrás: a szerzők szerkesztése NordPass 2020; Le@rnCCTV 2020; Woodham 2020; Buchholz 2021 alapján

Lehallgatás

Az IoT-eszközök kezelése során igen elterjedtek a virtuális asszisztensek, azonban ezek is okozhatnak problémákat. Nemrég derült ki, hogy az Amazon Alexa hangparancsokkal működő személyi asszisztense felvette egy házaspár otthoni beszélgetését, majd elküldte azt a férj munkatársának. Az Amazon elismerte, hogy az eszköz valóban rögzítette és továbbította a hanganyagot, bár ezt a cég azzal magyarázta,

[21] Varga 2017.

hogy az asszisztens félrehallott egy parancsot – az elhangzottakat úgy értelmezte, hogy rögzítenie kell a beszélgetést, és azt el is kell küldenie.[22]

Ennél súlyosabb eset, ha egy támadó kívülről hallgat bele a beszélgetéseinkbe, azokat rögzíti, és adott esetben továbbítja is. A lehallgatás úgy tud megtörténni, hogy mivel minden eszköznek van elektromágneses kisugárzása, nagy nyereségű antenna segítségével a kisugárzás foghatóvá válik, és a támadó képes a küldött adatok lehallgatására.[23]

Néhány évvel ezelőtt az amerikai Szövetségi Nyomozó Iroda (FBI) hatósági közleményt adott ki az okostelevíziókkal kapcsolatban. Szerintük az egyik gond, hogy a TV gyártója vagy pedig az arra telepített alkalmazások fejlesztői megfigyelhetik a családot a televízión keresztül. Volt rá példa, amikor a Samsung maga szólt, hogy a privát beszélgetéseket ne a TV előtt folytassák a felhasználók, mert a készülék mikrofonja és kamerája képes – sőt nemcsak képes, de az adatvédelmi tájékoztatóban foglaltak szerint meg is teszi – rögzíteni a beszélgetést. Ezt egy távoli szerverre továbbítja, miközben a hangutasítás keresése történik. Az FBI szerint az a legnagyobb probléma, hogy a gyártók nem foglalkoznak tüzetesen a biztonsági kérdésekkel, ezáltal lehetőséget adva a kiberbűnözőknek arra, hogy az otthoni hálózatban a TV-től tovább is jussanak, és nagyobb vagy költségesebb károkat okozzanak.[24] A fenti példákon kívül pedig még számos okoseszköz használható „kémkedésre". Ilyen például az okosporszívó, ami lézeres vagy kamerás letapogatóval rendelkezik, rögzíti a lakás alaprajzát a megfelelő tisztítás céljából.

További támadási módok

Előfordul olyan is, hogy a támadó önmaga jelenik meg a kiszemelt objektumban. A támadó első körben információt gyűjt a célpontról. Ez történhet social engineering[25] módszerrel, amikor a bűnöző egy olyan személynek adja ki magát, akitől az áldozat nem tagadja meg a válaszadást.[26] Így feltérképezve az okoseszközöket lehetőség van a célzottabb támadásra és például egy rosszindulatú szoftver – malware – elhelyezésére.[27]

A malware gyűjtőfogalom: azokat a kártékony programokat takarja, amelyeket a tulajdonosai ártó szándékkal szivárogtatnak be egy sebezhető eszközre. Céljuk többnyire az, hogy olyan adatokhoz és információkhoz jussanak hozzá, amelyek szá-

[22] Crist 2018.
[23] Frész–Kálovics–Puha 2014.
[24] Balogh 2019.
[25] A social engineering a személyek pszichológiai alapokon nyugvó manipulálását jelenti olyan érzékeny információk kicsalására vagy műveletek végrehajtatására, amelyek veszélyeztetik az informatikai biztonságot.
[26] Deák 2019.
[27] Bányász et al. 2019.

mukra értéket képviselnek.[28] Egy malware-fertőzés következtében az otthon támadhatóvá válik, a célszemély akár adatlopás, akár zsarolóvírus áldozata lehet.

Amennyiben pedig sikerül behatolni az okoseszközeinkbe – akár a fent említett malware segítségével –, akkor ezeken keresztül a támadó átveheti az irányítást, például azért, hogy kikapcsolja a behatolásjelző-rendszert, kinyissa az intelligens zárakat, de betekinthet a lakásba a kamerán keresztül, vagy megszüntetheti a kameraképeket. Ezek biztonsági réseit kihasználva a behatolók a valóságban is bejuthatnak otthonunkba. A BLE-technológiát (Bluetooth Low Energy) alapvetően nem zárrendszerekhez találták ki, mégis számos gyártó alkalmazza okoszáraknál. A zár ebben az esetben felismer egy eszközt (telefon, tablet, adott esetben okosóra), és lehetővé teszi, hogy azzal kinyissa a zárat. Egy biztonsági cég Tesla autókon tesztelte ezt a fajta működést, és egy speciális eszköz segítségével lemásolta a zár és az okostelefon közötti jelet, majd gond nélkül kinyitotta az autón a zárat.[29] De gyakran hozzák fel a szakértők példaként azt, ha egy védett objektumnál – ez akár lehet az otthonunk is – a hőmérséklet-szabályzót irányítva magas hőmérsékletet idéz elő a térben, és ezzel sarkallja az áldozatot szellőztetésre. A nyitott ablakon a támadó könnyedén bejut az épületbe, ezzel megalapozva egy személy vagy vagyon elleni bűncselekmény elkövetését. Ha a biztonsági kamerák sebezhetőségét egy támadó kihasználja és hozzáfér a kameraképekhez, akkor a betekintés látja, hogy a terület mennyire őrzött, hol lehet a legkönnyebben bejutni, és így akár a komplett betörési művelet is felépíthető.

Az egészségügyben használt IoT-eszközökön keresztül a bűnözők hozzáférhetnek egészségügyi adatokhoz vagy kritikus rendszerekhez, eszközökhöz, például az IoT-alapon működő pacemakerekhez vagy egészségügyi nyilvántartásokhoz. Fennállhat annak a kockázata, hogy az orvosi beavatkozásokról hamis adatok alapján döntenek.

És mindezek mellett ne feledkezzünk meg a zsarolóvírussal kapcsolatos esetleges támadásokról sem! A Darktrace nevű kiberbiztonsági vállalat vezérigazgatója, Nicole Eagan 2018-ban beszélt egy konferencián arról az esetről, amikor bűnözők egy akváriumban elhelyezett okos-hőmérsékletszabályozón keresztül hatoltak be egy kaszinó rendszerébe, majd lopták el a sokat költő játékosok személyes adatait.[30]

A zsarolóvírus sok esetben e-mailben, csatolmánnyal jut el a célponthoz, megfertőzve ezzel a számítógépet, de az internetes bűnöző átveheti a teljes irányítást egy otthoni IoT-eszközön keresztül is, és irányíthatja például a biztonsági rendszereket, a hálózat kezelését pedig pénzért adja vissza. A zsarolóvírusos támadások a következőképpen épülnek fel:

- a kártékony szoftver segítségével a támadó titkosítja a felhasználó adatállományát;
- a képernyőn egy zsaroló üzenet jelenik meg, ami egyértelművé teszi a követeléseket. Innentől kezdve az áldozat nem fér hozzá az adataihoz, és nem képes irányítani eszközeit;

[28] Erdősi–Solymos 2017.
[29] Rodríguez 2022.
[30] Williams–Grut 2018.

- a képernyőn megjelenik egy határidő, illetve az, hogy milyen összegű váltságdíjat követelnek, és milyen fizetési lehetőségek állnak rendelkezésre;
- az adatok egy részét törlik, módosítják, saját szervereikre letöltik;
- amennyiben az áldozat nem tesz eleget a követelésnek, akkor a támadó egyre több adatot semmisít meg.[31]

2. ábra: Zsarolóvírus

Forrás: ESET 2020

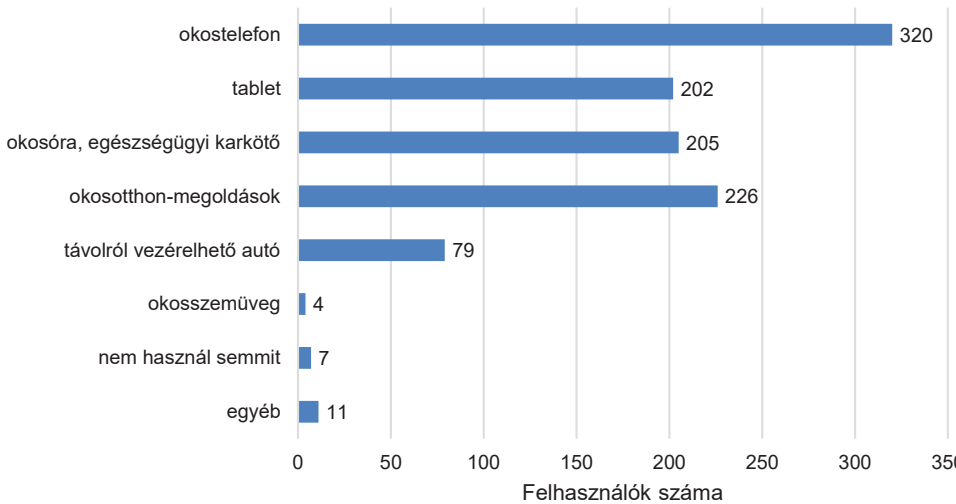
2023-ban 27%-kal növekedett a zsarolóvírus-támadás áldozatainak száma a vállalati szektorban.[32] Legfőbb okként az emberi mulasztást azonosították, így várhatóan ez a tendencia növekedni fog, hiszen a felhasználók egyre inkább teszik függővé a mindennapjaikat az IoT-eszközöktől. Az áldozatok kénytelenek tárgyalásokba belemenni a zsarolókkal, hiszen a személyes – vagy adott esetben céges, vállalati és üzleti – adatok elvesztése hatalmas károkkal járhat.

Elgondolkodtató kérdés ugyanakkor, hogy érdemes-e ilyen esetben fizetni, hiszen semmilyen garancia nincs arra, hogy a pénz kifizetése után a támadók nem értékesítik tovább a megszerzett adatokat, megágyazva ezzel egy következő zsarolásnak. Emellett, ha fizet az áldozat, akkor a befolyt pénzösszeg feltehetően további bűnözésre sarkallja a támadót, azaz, ha nem is közvetlenül, de közvetve az összeget a kiberbűnözésbe fektetik be, ezzel generálva annak növekedését.[33]

[31] Cisco 2016; Nemzeti Kibervédelmi Intézet 2022.
[32] Thales 2024.
[33] Nemzeti Kibervédelmi Intézet 2020e.

Kutatás

A kvalitatív szakirodalmi elemzés mellett fokozott figyelmet fordítottunk az IoT-eszközökről szóló, nem reprezentatív, hazai kvantitatív kutatásra is, amely 335 kitöltő válaszain alapult. A válaszadók között a legnépszerűbb IOT-eszköz az okostelefon volt, a 335 válaszadó közül 320 fő használ okostelefont, emellett nagy számban használnak okosotthon-megoldásokat (226 fő), tabletet (202 fő) és okosórát/egészségügyi karkötőt (205 fő) is.

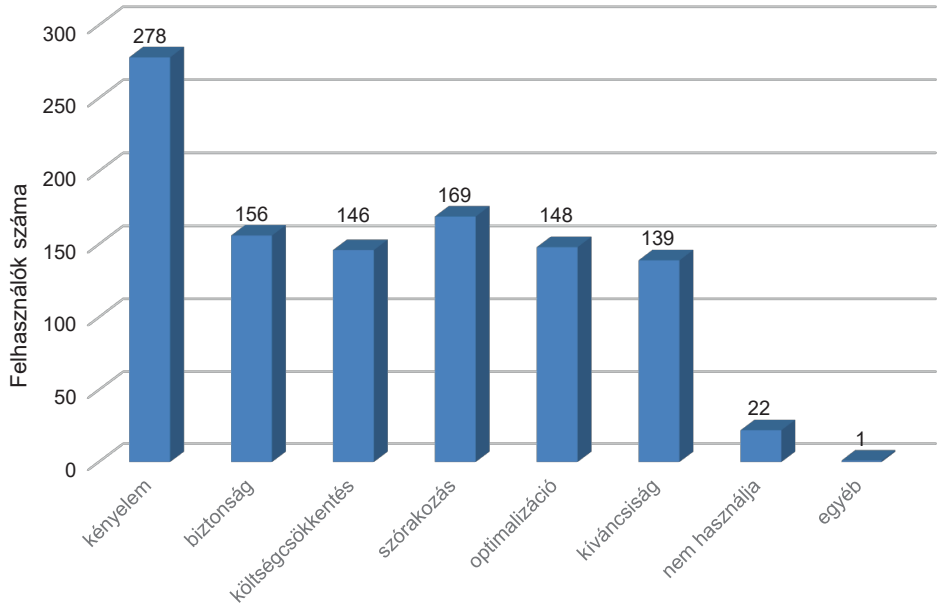


3. ábra: Alkalmazott IoT-megoldások

Forrás: a szerzők szerkesztése

Az is kiderült, hogy a kitöltők szerint a legnépszerűbb okosotthon-megoldás a szórakoztatóelektronika (a válaszadók 75,5%-a használja), második helyre a biztonságtechnika (a kitöltők 49,9%-a veszi igénybe) került, a harmadik-negyedikre pedig a világítástechnikai megoldások (48,7%) és a hűtés-fűtést biztosító berendezések (45,4%). A felmérésben részt vevők közül a jövőben 215 fő biztonságtechnikát, 189 fő a hűtés-fűtést, 186 fő a világítástechnikát és 165 fő a robotporszívót alkalmazná legszívesebben otthonaiban. Mindössze a válaszadók 6%-a nem próbálná ki egyik megoldást sem szívesen.

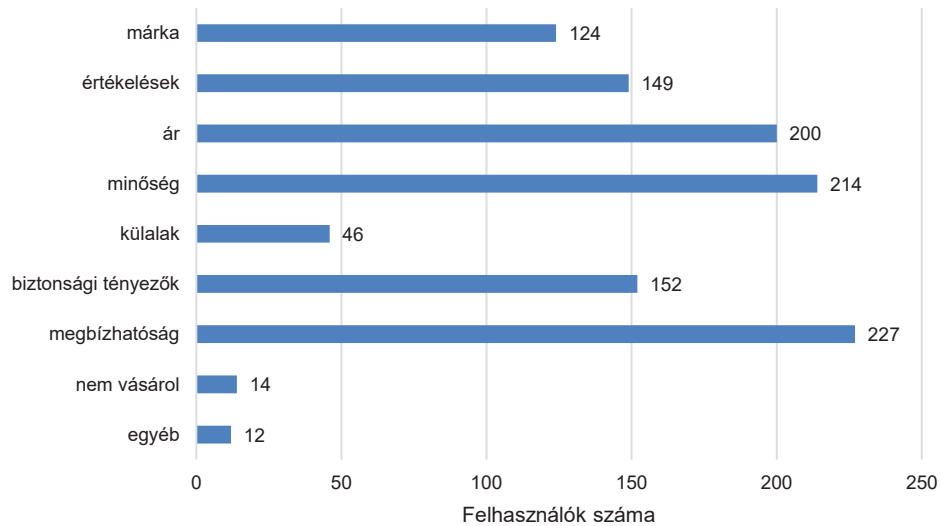
Elgondolkodtatók a használat célját, okát firtató kérdésre adott válaszok. A felhasználók legfontosabb motivációja a kényelem, ezt az opciót 278-an jelölték be, ami a megkérdezettek 83%-át jelenti. A szórakozásra a válaszadók fele (50,4%), a biztonságra a kitöltők 46,6%-a tette le a voksát.



4. ábra: Az IoT felhasználásának okai

Forrás: a szerzők szerkesztése

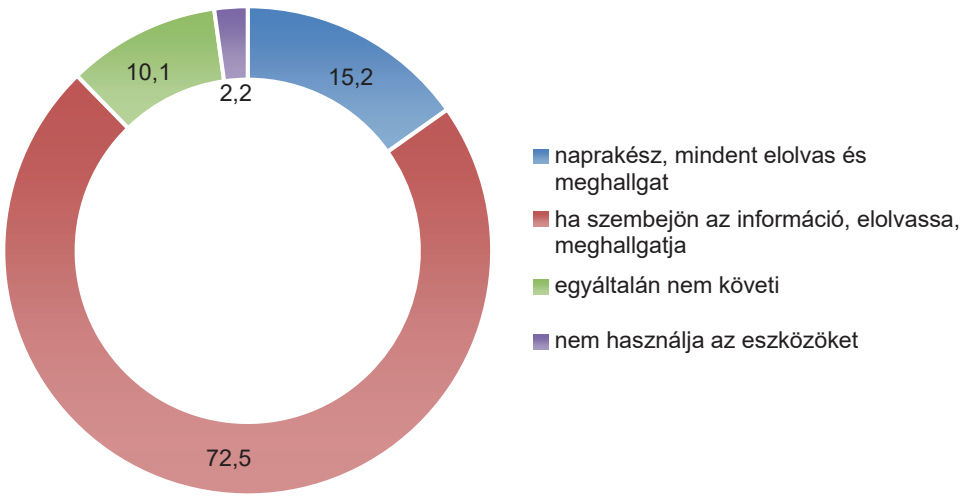
A biztonság a vásárlási szempontok között is csak a 4. helyen végzett a megbízhatóság, minőség és az ár mögött.



5. ábra: A vásárlás szempontjai

Forrás: a szerzők szerkesztése

Így már nem meglepő a felmérésnek az az eredménye, hogy csupán a válaszadók 15%-a mondhatja el magáról, hogy naprakész a biztonsági kérdésekkel kapcsolatban, nagy többségük, közel háromnegyedük (72,5%) ezzel szemben csak abban az esetben foglalkozik ezekkel az információkkal, ha szembejönnek velük. Tizedük (10,1%) pedig egyáltalán nem követi azokat.

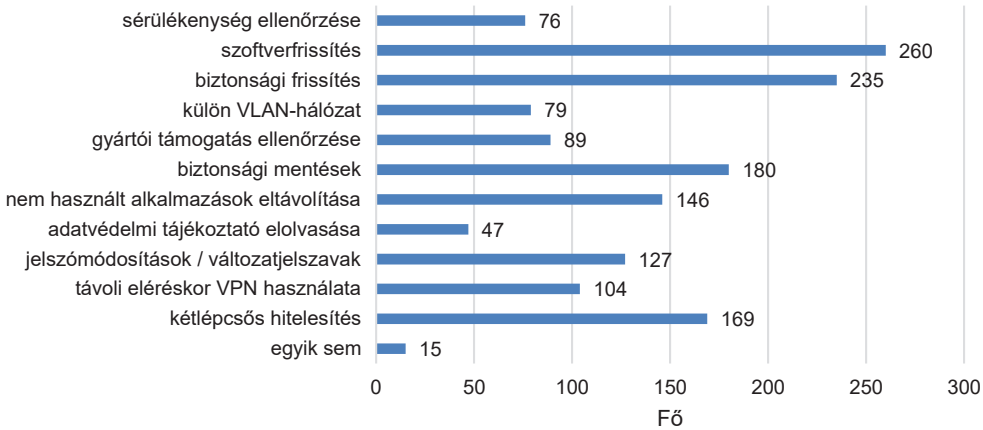


6. ábra: Az okoseszközök biztonsági kérdéseivel kapcsolatos információk követése (%)

Forrás: a szerzők szerkesztése

A legtöbb válaszadó a szoftverfrissítésekre (260 fő), a biztonsági frissítésekre (235 fő), a biztonsági mentésekre (180 fő) és a kétlépcsős hitelesítésre (169 fő) figyel oda, a legkevesebb választ (47 fő) az alkalmazások telepítése során az adatvédelmi tájékoztató elolvasása kapta. Ez igen nagy gondot jelenthet, hiszen ezek a tájékoztatók foglalják magukba azokat az információkat, hogy ki milyen módon és milyen adatunkat kezel, milyen további alkalmazáshoz fér hozzá. Ennek a tudásnak a hiányában a fogyasztók gyakorlatilag minden további nélkül lehetőséget adnak az alkalmazás kezelőjének arra, hogy adataikkal rendelkezzenek, hozzáférjenek és kezeljék azokat.

A kérdőívben 11 biztonsági intézkedést soroltunk fel, amely segíthetné az eszközök védelmét. Ezek közül mindössze kétfajta intézkedés van, amire a kitöltők nagyjából fele odafigyel, további kettő, amit a kitöltők körülbelül kétharmada elvégez. Ezek igen csekély számok. 15 fő egyébként azt az opciót jelölte meg, hogy egyik biztonsági intézkedésre sem figyel oda.



7. ábra: Figyelemmel kísért biztonsági intézkedések gyakorisága

Forrás: a szerzők szerkesztése

A kockázatok csökkentése, lehetséges védelmi megoldások és javaslatok

Tekintettel arra, hogy az IoT-eszközök rendkívül összetettek, nagy valószínűséggel a legtöbb eszköz biztonsági problémákkal rendelkezik.[34] Nem segít az sem, hogy a legtöbb gyártónak nincs kiberbiztonsági tapasztalata, és mivel a biztonsági tényezők csak pluszköltséget generálnának, ezért a forgalomban lévő eszközöket védelemmel nem, vagy csak igen csekély mértékben látják el.[35] Bizonyos intézkedésekkel ugyanakkor lehetne csökkenteni a kockázatokat.

Talán az egyik legfontosabb intézkedésnek egy egységes, nemzetközi szinten elfogadott törvényi szabályozás kialakításának kell lennie mind a biztonsági intézkedéseket, mind a büntetőjogi felelősségeket és eljárásokat érintve. A törvényalkotók mellett ugyanakkor a gyártónak és a fogyasztónak is van felelőssége. A kockázatok csökkentése érdekében a fogyasztóknak az alábbi intézkedéseket kellene megtenniük:

- vásárlás előtt ellenőrizzék a sérülékenységgel és a gyártói támogatással kapcsolatos információkat;
- ellenőrizzék magát a gyártót is;
- kerüljék el a feltűnően olcsó vagy ismeretlen gyártótól származó eszközök vásárlását;
- tartsák naprakészen az eszközt, azaz rendszeresen frissítsék azok szoftvereit, különös tekintettel a biztonsági frissítésekre;
- kövessék a sérülékenységi információkat;

[34] Bocsok et al. 2015.
[35] Lee 2018.

- az eszközöket elkülönített VLAN-hálózatokon kezeljék;
- folyamatosan készítsenek biztonsági mentéseket;
- amennyiben egy alkalmazást már nem használnak, vagy az alkalmazás elavult, távolítsák el;
- az alkalmazások telepítése során figyelmesen olvassák el az adatkezelési tájékoztatót, és csak azoknak az engedélykéréseknek tegyenek eleget, amelyek valóban szükségesek az eszköz megfelelő működéséhez;
- minden esetben más, erős jelszót használjanak, az alapértelmezett jelszavakat változtassák meg, éljenek a kétlépcsős hitelesítés lehetőségével (az interneten vannak olyan oldalak, amelyek segítségével ellenőrizhető egy adott jelszó biztonságossága, illetve az, hogy ezt egy támadó átlagosan mennyi idő alatt képes feltörni. A jelszóerősség-mérő használata célszerű. Emellett pedig például a dehashed.com oldalon ellenőrizhetők a közzétett vagy kiszivárgott információk, például telefonszámmal vagy e-mail-címmel összefüggésben is);
- távoli elérés során alkalmazzanak VPN-t.

A gyártó részéről szintén csökkenthetők a kockázatok, ha

- biztosítja a titkosított csatornán keresztüli kommunikációt, valamint a folyamatos szoftver- és biztonsági frissítéseket;
- a forgalomba hozás előtt biztonsági teszteléseket végez;
- kötelezővé teszi az alapértelmezett jelszavak megváltoztatását és annak megfelelő erősségi szintjét;
- nyomon követi az eszköz sérülékenységét, és naprakészen tájékoztatja a felhasználót ezekről (akár úgy, hogy lehetőséget ad a felhasználónak arra, hogy e-mail-üzenetet kapjon erről);
- kötelezővé teszi a vírusirtók és tűzfalak alkalmazását;
- amennyiben elavult az eszköz, cserelehetőséget biztosít;
- felhasználóbarát nyelvezet alkalmazásával folyamatosan tájékoztatja a felhasználót mindenről úgy, hogy annak megértéséhez ne legyen szükség mélyebb számítástechnikai tudásra;
- többszöri sikertelen bejelentkezési kísérlet után letiltja a felhasználót.

Ugyanakkor a fent felsorolt teendők napjainkban pusztán javaslatokként szolgálnak, ugyanis például sem Magyarországon, sem a teljes Európai Unióban egyelőre nincsen kötelező jogi szabályozás az IoT-eszközök védelmére vonatkozóan az ajánlásokon és iránymutatásokon kívül.

Ez azt jelenti, hogy jelenleg semmilyen jogszabály nem határozza meg, hogy milyen védelmi minimumkövetelményeknek kell megfelelni egy okoseszköz piacra bocsátása során, ahogy azt sem, hogy a fogyasztóknak milyen minimális biztonsági intézkedéseket, beállításokat kell megtenniük saját védelmük érdekében. Így – baj esetén – a felelősség is nehezen meghatározható.

Ugyanakkor az intelligens eszközök használatakor nem minden esetben írja elő a gyártó a felhasználó részére, hogy kötelezően változtassa meg az alapbeállított jelszót, vagy minden esetben alkalmazzon megfelelő erősségű tűzfalat, vírusvédelmi programot. Ebben az esetben már kérdéses, hogy a gyártó a felelős, aki ezt nem tette kötelezővé, avagy a felhasználó, aki ezt nem tette meg. Azt gondoljuk, hogy elengedhetetlen lenne egy egységes követelményrendszer kialakítása, ami meghatározná azokat a biztonsági előírásokat, amelyek elérése és biztosítása nélkül nem lehetne egy eszközt forgalomba hozni. Továbbá a gyártói garanciának nemcsak az eszköz fizikai vagy működésbeli meghibásodására kellene kiterjednie, hanem az eszköz védelmi mechanizmusára is.

A szabályozásnak továbbá kötelezően ki kellene térni arra is, hogy a gyártó kötelező érvényűen tájékoztassa – az átlagfogyasztó számára is érthető módon – a felhasználót, hogy neki milyen beállításokat és milyen módon szükséges elvégezni a minimális biztonsági követelményeknek való megfeleléshez. Ezenfelül a fogyasztók biztonságtudatossága sem növekszik exponenciálisan a technikai eszközök fejlődésével, pedig az ember az egyik legfontosabb tényező ezekben az új kihívásokban.

Egyöntetű vélemény, hogy a prevenciónak éppen olyan jelentősége van, mint a szankcionálásnak és bűnüldözésnek, hiszen a megelőzéssel számos kibertámadás elkövetése elkerülhető lenne. 2020-ban a Nemzeti alaptantervbe – az informatika tantárgy helyett – bekerült a digitális kultúra nevű tárgy, amelyet az általános iskola 3. osztályától tanítanak.[36] Ugyanakkor a kerettantervben meghatározott éves szintű 68 tanóra, míg például az ének-zene 132 óra,[37] igen alacsony. Pedig maga a Nemzeti Kibervédelmi Intézet is megfogalmazza, hogy az egyik legfontosabb feladatuk a biztonságtudatosság növelése mind a fogyasztók, mind a döntéshozók és üzemeltetők tekintetében, ugyanis a kibervédelem leggazdaságosabb és legeredményesebb stratégiája a felhasználók biztonságtudatosságának növelése.

Hosszú távú célként elengedhetetlen lenne, hogy mind a jogalkotás, mind az oktatási rendszer gyorsan reagáljon a technológia fejlődés adta kihívásaira. A Nemzeti alaptantervbe magasabb óraszámban kötelezően be kellene építeni a hálózati eszközök biztonságtudatos használatát, az oktatási intézményekben dolgozó, digitális kultúra tárgyat oktató tanárok folyamatos felkészítését, képzését, vizsgáztatását. Mindezeken túl kiemelten fontos a kiberbiztonság felsőfokú oktatása is. Az ilyen irányú oktatás az informatikai felsőoktatáson túl ki kell terjedjen a villamosmérnöki és a biztonságtechnikai mérnöki felsőoktatásra is.[38]

[36] Ambrus 2020.
[37] Oktatási Hivatal 2020.
[38] Tóth 2018.

Összegezés

Életünk számos területének szerves része az intelligens eszközök használata, ugyanakkor a felhasználók nincsenek tisztában a valós veszélyekkel, illetve azzal, hogy milyen alapvető biztonsági intézkedéseket kellene megtenniük annak érdekében, hogy a kockázatokat csökkentsék. Illetve, ha tisztában is vannak a veszélyekkel, nem tesznek meg minden tőlük telhetőt a saját védelmük érdekében. Az viszont elengedhetetlen, hogy ne csak teljes természetességgel használják ezeket az intelligens eszközöket, hanem a védelmi megoldások ismerete és alkalmazása is ugyanilyen természetességgel legyen jelen a mindennapokban. Ehhez nagyban hozzájárulna az is, ha az IoT-eszközök gyártása és piaci forgalmazása egységes nemzetközi szabályozás alapján működne, ha a gyártói garancia részét képezné az eszközök biztonságosságának szavatolása is, valamint ha a felhasználókat több csatornán keresztül szólítanák meg – már az oktatási rendszer keretein belül is. Továbbá segítené ezt az is, ha a magánbiztonsági szereplők magas szakértelmük miatt nagyobb szerepet tölthetnének be akár a preventív, akár a bűnüldözési, nyomozati, feltáró munka során, különböző együttműködési megállapodások keretében.

A technikai vívmányok, ezáltal a támadók, támadási felületek egyre szélesebb körben és rohamos tempóban változnak és növekednek. A virtuális térben keletkező, mérhetetlen adathalmaz értékéből fakadó kockázatok miatt elengedhetetlen, hogy ezzel egyidejűleg növekedjen ezek biztonságtudatos használata és a biztonságos adatgenerálás is az egyén szintjén, döntéshozói és törvényhozói szinteken egyaránt. Mivel az IoT-eszközök összetett működésűek, számos támadási felületet rejtenek magukban, mind a mobilalkalmazások, mind a használt webes felületek, mind a kommunikációs csatorna, de a felhőszolgáltatás is számos lehetőséget biztosít a támadók részére.

A támadók felismerték az IoT-eszközökben rejlő támadási réseket és potenciálokat, és ahogy az esettanulmányokból kiderült, szívesen ki is használják ezeket. Az IoT-eszközök a támadó szempontjából alkalmasak adatszerzésre, lehallgatásra, fizikai támadáshoz szükséges információk megszerzésére, de a felhasználók akár zsarolóvírus vagy rosszindulatú szoftver áldozatai is lehetnek, továbbá, és nem utolsósorban, az IoT-eszközök bizonyítottan alkalmasak egy nagyobb és komplexebb DoS- vagy DDoS-támadás megindításához.

Az IoT-eszközök felhasználási és felhasználói körének egyre szélesebb skálája miatt folyamatosan növekszik a potenciális áldozatok száma a kibertérben, a végfelhasználók feláldozzák biztonságukat a kényelem és az automatizáció oltárán.

Felhasznált irodalom

Ambrus Balázs (2020): Az érvényesülés kulcsa a digitális problémamegoldás. *Új Köznevelés*, 7. Online: https://folyoiratok.oh.gov.hu/uj-kozneveles/az-ervenyesules-kulcsa-a-digitalis-problema-megoldas

Bálint Krisztián (2018): Okos otthonok – a XXI. század információbiztonsági kihívásai a mindennapokban. In Rajnai Zoltán (szerk.): *Kiberbiztonság*. Budapest: Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 355–366.

Balogh Csaba (2019): Milyen tévéje van otthon? Figyelmezetést adott ki az FBI. *HVG*, 2019. december 3. Online: https://hvg.hu/tudomany/20191203_okos_tevekeszulek_lehallgatas_megfigyeles_fbi

Bányász Péter et al. (2019): A social engineering jelentette veszélyek napjainkban. In Zsámbokiné Ficskovszky Ágnes (szerk.): *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében*. Budapest: Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozata, 12–37. Online: https://doi.org/10.37372/mrttvpt.2019.1.1

Beláz Annamária (2020): Az ökoszisztémák fogalma és jelentősége az információs társadalomban. In Sasvári Péter (szerk.): *Rendszerelmélet*. Budapest: Dialóg Campus, 159–178. Online: https://doi.org/10.36250/00734.00

Bocsok Viktor et al. (2015): *A dolgok internete Technológiai háttér, információbiztonsági és adatvédelmi aspektusok*. Online: https://fornax.hu/wp-content/uploads/2016/09/Informa%CC%81cio%CC%81biztonsa%CC%81g-e%CC%81s-adatve%CC%81delem-az-IoT-vila%CC%81ga%CC%81banv02jav.pdf

Boda József főszerk. (2019): *Rendészettudományi szaklexikon*. Budapest: Dialóg Campus. Online: http://hdl.handle.net/20.500.12944/14690

Buchholz, Katharina (2021): The Most Popular Passwords Around the World. *Statista*, 2021. február 9. Online: www.statista.com/chart/16922/most-popular-passwords-2017-and-2018/

Cisco (2016): *Minden, amit a zsarolóvírusokról tudni kell*. Online: www.cisco.com/c/dam/global/hu_hu/solutions/security/ransomware/pdf/ransomware-everything-you-need-to-know_hun.pdf

Crist, Ry (2018): Alexa Sent Private Audio to a Random Contact, Portland Family Says. Online: www.cnet.com/home/smart-home/alexa-sent-private-audio-to-a-random-contact-portland-family-says/

CrowdStrike (2018): 2018 CrowdStrike Global Threat Report. Online: https://go.crowdstrike.com/2018ThreatReport.html

Deák Veronika (2019): Social engineering alapú információszerzés a kibertérben megvalósuló lélektani műveletek során. *Hadtudományi Szemle*, 12(3), 95–111. Online: https://doi.org/10.32563/hsz.2019.3.6

Erdősi Péter Máté – Solymos Ákos (2018): *IT biztonság közérthetően*. Budapest: Neumann János Számítógép-tudományi Társaság (NJSZT). Online: http://hdl.handle.net/20.500.12944/7212

ESET (2020): *Három éves minden idők legdurvább zsarolóvírusa*. Online: www.eset.com/hu/hirek/harom-eves-minden-idok-legdurvabb-zsarolovirusa-2020/

Flachner Balázs – Klág Dávid (2016): Lehalt a fél internet. *Index*, 2016. október 21. Online: https://index.hu/tech/2016/10/21/internet_hiba_kibertamadas/

Frész Ferenc – Kálovics Tamás – Puha Gábor (2014): *Hálózatok biztonsága*. Budapest: Nemzeti Közszolgálati Egyetem. Online: https://kti.uni-nke.hu/document/vtkk-uni-nke-hu/halozatok-biztonsaga.original.pdf

Kaspersky Security Services (2023): *Overview of IoT Threats in 2023*. Online: https://securelist.com/iot-threat-report-2023/110644/

Kovács László (2018): *A kibertér védelme*. Dialóg Campus.

Le@rnCCTV (2020): *IP Camera Default Password List (2020)*. Online: https://learncctv.com/ip-camera-default-password/

Lee, M. Robert (2018): *Okos otthoni eszközök*. Online: https://nki.gov.hu/wp-content/uploads/2019/03/201808-OUCH-August-Hungarian.pdf
Marton, Anna (2023): IoT Malware Attacks up by 37% in the First Half of 2023. Online: https://iotac.eu/iot-malware-attacks-up-by-37-in-the-first-half-of-2023/
Nemzeti Kibervédelmi Intézet (2018a): *Elosztott szolgáltatásmegtagadásos támadás (DDoS)*. Online: https://nki.gov.hu/it-biztonsag/tudastar/elosztott-szolgaltatasmegtagadasos-tamadas-ddos-2/
Nemzeti Kibervédelmi Intézet (2018b): *Így védekezhetsz az 5 leggyakoribb jelszó elleni támadás ellen*. Online: https://nki.gov.hu/it-biztonsag/tanacsok/igy-vedekezhetsz-az-5-leggyakoribb-jelszo-elleni-tamadas-ellen/
Nemzeti Kibervédelmi Intézet (2019): *Rengeteg célpontja van egy új botnet hálózatnak*. Online: https://nki.gov.hu/it-biztonsag/hirek/rengeteg-celpontja-van-egy-uj-botnetnek/
Nemzeti Kibervédelmi Intézet (2020a): *Robothálózat (botnet)*. Online: https://nki.gov.hu/it-biztonsag/tudastar/robothalozat-botnet-2/
Nemzeti Kibervédelmi Intézet (2020b): *Új IoT botnet felemelkedőben*. Online: https://nki.gov.hu/it-biztonsag/hirek/egyszemelyes-iot-botnet-hadsereg-felemelkedoben/
Nemzeti Kibervédelmi Intézet (2020c): *Kaiji: Új IoT malware a láthatáron*. Online: https://nki.gov.hu/it-biztonsag/hirek/kaiji-uj-iot-malware-a-lathataron/
Nemzeti Kibervédelmi Intézet (2020d): *Zyxel NAS-ok veszélyben: Új köntösben csap le a Mirai botnet*. Online: https://nki.gov.hu/it-biztonsag/hirek/zyxel-nas-ok-veszelyben-uj-kontosben-csap-le-a-mirai-botnet/
Nemzeti Kibervédelmi Intézet (2020e): *Zsarolóvírusok*. Online: https://nki.gov.hu/wp-content/uploads/2020/07/Zsarol%C3%B3v%C3%ADrusok-1.pdf
Nemzeti Kibervédelmi Intézet (2022): *Mit tegyünk, ha zsarolóvírus támadás ér bennünket?* Online: https://nki.gov.hu/wp-content/uploads/2022/03/ransomware_CTI_jelentes-1.pdf
NordPass (2020): *Top 200 Most Common Passwords*. Online: https://nordpass.com/most-common-passwords-list/
Oktatási Hivatal (2020): *Kerettanterv az általános iskola 1–4. évfolyama számára*. Online: www.oktatas.hu/kozneveles/kerettantervek/2020_nat/kerettanterv_alt_isk_1_4_evf
Thales (2024): *2024 Thales Data Threat Report Reveals Rise in Ransomware Attacks, as Compliance Failings Leave Businesses Vulnerable to Breaches*. Online: www.thalesgroup.com/en/worldwide/security/press_release/2024-thales-data-threat-report-reveals-rise-ransomware-attacks
Precedence Research (2023): *Smart Home Market*. Online: www.precedenceresearch.com/smart-home-market
Rodríguez, José (2022): Researchers Break Into a Tesla and Drive Away Using Bluetooth Vulnerability. *Jalopnik,* 2022. május 17. Online: https://jalopnik.com/researchers-break-into-a-tesla-and-drive-away-using-blu-1848938417
Tóth Attila (2018): A biztonságtechnikai tervezők helyzete. *Bolyai Szemle,* 27(1), 45–53. Online: https://real-j.mtak.hu/27242/1/bolyai_szemle_2018_27_1.pdf
Vailshery, Lionel Sujay (2023): *Number of Internet of Things (IoT) Connected Devices Worldwide from 2019 to 2023, with Forecasts from 2022 to 2030*. Online: www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
Varga Péter János (2017): Az okos otthonok vezeték nélküli alkotóelemeinek biztonsága. *Közteс-Európa,* 9(1–2), 83–87. Online: https://ojs.bibl.u-szeged.hu/index.php/vikekke/article/view/12743
Williams-Grut, Oscar (2018): Aquarium Thermometer Enables Casino Hack. *PI,* 2018. április 15. Online: https://privacyinternational.org/examples/2559/aquarium-thermometer-enables-casino-hack
Woodham, Wilbur (2020): Default Passwords for IoT Devices. Why You Should Change Them. Online: https://howtofix.guide/default-password/

ABSTRACT

Visible Friends Become Invisible Enemies – The Price of Convenience

Renáta BÖCSKEI – Levente TÓTH

The rapidly growing technical and technological development, as well as the digital transformation and the spread of information technology, have made IoT (Internet of Things) devices increasingly popular. Today, these devices are present almost everywhere, from smart homes and autonomous cars to smart security devices and IoT-based production lines. Value no longer only exists in material form and is not only manifested in the physical space but can also be created and stored in cyberspace. For this reason alone, it is important to discuss and understand the risks associated with these devices, and to be prepared to prevent them, both in the real physical space and in cyberspace.

Keywords: *IoT, smart home, cybercrime, DDoS, botnet, ransomware*