

36. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2023. április 18-20.
Nemzeti Közszolgálati Egyetem
Rendészettudományi Kar

**Látható barátból láthatatlan ellenség
– AZ IOT eszközök veszélyei a személyes térben**

Jelige: *Publikus privátszféra*

Pályamunka lezárásának időpontja: 2022. szeptember 29.

2023.

TARTALOMJEGYZÉK

BEVEZETÉS	4
1. INFORMÁCIÓS TÁRSADALOM.....	6
2. IOT-ESZKÖZÖK KIALAKULÁSA, ALKALMAZÁSA	9
2.1 Alkalmazása a biztonságtechnikában.....	11
2.2 Alkalmazása a kereskedelembe.....	11
2.3 Alkalmazása az egészségügyben.....	12
2.4 Alkalmazása a közlekedésben.....	12
2.5 Alkalmazása az épületautomatizálásban	12
3. AZ IOT-ESZKÖZÖK MŰKÖDÉSE.....	13
4. A KOMMUNIKÁCIÓS CSATORNÁK ÉS A FELHŐSZOLGÁLTATÁSOK.....	16
4.1 Felhőszolgáltatások	16
4.2 Kommunikációs csatornák	17
5. IOT-ESZKÖZÖK AZ OTTHONUNKBAN	21
6. IOT-ESZKÖZÖK ELŐNYEI AZ OKOS OTTHONOKBAN.....	24
6.1 Kényelem, szórakoztatás, megtakarítás	24
6.2 Biztonságtechnika	24
6.3 Egészség.....	25
7. AZ IOT-ESZKÖZÖK VESZÉLYEI - HOGYAN LESZ LÁTHATÓ BARÁTBÓL LÁTHATATLAN ELLENSÉG?	26
7.1 Az IOT-eszközök erősségei, gyengeségei, lehetőségei, veszélyei, SWOT analízis ..	27
7.2 Esettanulmányok	28
7.2.1. Az okos akvárium és a kaszinó	28
7.2.2. A 2016-os Mirai Botnet támadás	30
7.2.3. A Nest bébiőr és az alapértelmezett jelszavak	32
7.2.4. Lehallgatás	35
7.2.5. További támadási módok.....	36
8. A TÁMADÓK MOTIVÁCIÓI ÉS TÍPUSAI	39

9. A KOCKÁZATOK CSÖKKENTÉSE, LEHETSÉGES VÉDELMI MEGOLDÁSOK ÉS JAVASLATOK	43
10. A KÉRDŐÍV KIÉRTÉKELÉSE: AZ IOT-ESZKÖZÖK A MINDENNAPJAINKBAN	47
ÖSSZEFOGLALÁS	61
ÁBRAJEGYZÉK	63
IRODALOMJEGYZÉK	65
MELLÉKLET: KÉRDŐÍV	70

BEVEZETÉS

Dolgozatom témájának az IOT (Internet of Things) eszközök veszélyeit választottam. Az IOT betűszó az angol Internet of Things elnevezésből adódik, magyarra fordítva a Dolgok internetét jelenti. Az IOT-eszközök ma már szinte mindenhol jelen vannak: az iparban, a gyártásban, a biztonságtechnikában, az egészségügyben, és még számos területen. Éppen ezért fontosnak tartom tárgyalni és megismerni az IOT-eszközök veszélyeit, az eszközökkel kapcsolatos támadási módszereket és motivációkat, mert a jelenben és a jövőben ezekre ugyanolyan mértékben fel kell készülni, mint a fizikai térben leselkedő veszélyekre.

Az Y, Z és Alfa generáció a digitális világ nemzedéke, ők azok, akik hatalmas mennyiségű digitális adattal és információval rendelkeznek. Mind az Y, mind a Z, mind az Alfa generáció tagjai számára a digitális eszközök az élet szerves részei, magánéletük és munkahelyi életük nagy részét internetes platformokon töltik: ott beszélgetnek egymással, ott olvasnak híreket, és egyebek mellett a vásárlásaikat is interneten keresztül bonyolítják le. A technológia számukra természetes. Ugyanakkor sem az oktatási rendszer, sem a jogszabályi rendszer nem változott olyan mértékben, mint ahogy maga a technológia fejlődik és terjeszkedik. Ami már csak azért is veszélyes, mert ha a fiatal felhasználókat nem tájékoztatják és/vagy képzik a digitális léttel járó veszélyekről, akkor egyrészt ők maguk is könnyedén potenciális áldozatokká válhatnak, másrészt nem tudják támogatni idősebb hozzátartozóikat - akik ma már szintén igen gyakran használnak interneten alapuló eszközöket.

Dolgozatom egyrészt támaszkodik az általam felkutatott és feldolgozott szakirodalomra: az okos otthonokban használt IOT-eszközök veszélyeiről szóló tanulmányokra, továbbá az információbiztonság és kiberbiztonság területén született tudományos igényű publikációkra. Segítségemre voltak emellett a témában íródott cikkek, illetve az információbiztonsági kérdésekkel foglalkozó weboldalak, valamint saját primer kutatásom. Több, mint 300-an válaszoltak az általam összeállított kérdőív kérdéseire, melyek arra irányultak, hogy a felhasználók körében milyen mértékű az intelligens eszközök alkalmazása, és mennyire vannak tisztában azok veszélyeivel.

A dolgozat első fejezeteiben az információs társadalom fogalomkörét és az IOT-eszközök kialakulását mutatom be, majd ezen eszközök architektúráját, működését, felhasználási körét és azt, hogy milyen előnyökkel rendelkeznek. Ezt követően esettanulmányokon keresztül mutatom be a támadások lehetséges fajtáit, majd pedig a támadók fajtáit és azok motivációit.

Végül javaslatot teszek arra vonatkozóan, hogy mit tehet a fogyasztó, és mit tehet a gyártó a biztonsági kockázatok csökkentése érdekében, és hogy milyen változtatásokra van szükség annak érdekében, hogy az IOT-eszközök a felhasználók számára biztonságosabbak legyenek. Továbbá ismertetem a kérdőíves kutatásom eredményeit.

HIPOTÉZIS 1: az IOT-eszközök működésükből fakadóan veszélyesek a felhasználókra nézve, akik nincsenek tisztában az IOT-eszközök veszélyeivel

HIPOTÉZIS 2: a támadók egyre inkább kihasználják az IOT-eszközök biztonsági réseit

HIPOTÉZIS 3: az IOT-eszközök felhasználási és felhasználói körének egyre szélesebb skálája miatt folyamatosan növekszik a potenciális áldozatok száma, a végfelhasználók feláldozzák biztonságukat a kényelem és az automatizáció oltárán.

1. INFORMÁCIÓS TÁRSADALOM

Társadalmunk úgynevezett információs társadalom. *“Egy új típusú társadalom, amelynek átalakulása és fejlődése mögött az információs (és nem az anyagi) javak termelése a hajtóerő...”* (Yoneji Masuda, 1981, *Information Society as Post-industrial Society. World Future Society*) (Z. Karvalics, 2007) Egy olyan társadalmi forma, amelynek a legfőbb eleme a tudás, az innováció és legfőképpen az információ, amelynek birtoklása hatalmat jelent. Az információs társadalom új fogalom: annak ellenére, hogy valamilyen szinten minden társadalomban megjelent az információ fontossága, egyik korábbi társadalmat sem hívták még a társadalomtudományokkal foglalkozó kutatók és elemzők információs társadalomnak. Ennek az az oka, hogy egyetlen korábbi populációban sem volt ilyen mértékben hatalmi tényező az információ, mint napjaink társadalmában. A rohamosan növekvő technikai és technológia fejlődés maga után vonja az információ mennyiségének növekedését is.

Az információ-központú társadalomban előnnyel rendelkeznek azok a résztvevők, akik képesek létrehozni, összegyűjteni, feldolgozni, elemezni és használni az információt. Akinél az adat van, annál van a hatalom is. *„Az adat az új olaj”* – nem véletlenül ez napjaink egyik mottója. (Beláz, 2020) Társadalmunk tehát információs társadalommá alakult át. Ezzel együtt pedig vitathatatlan tény, hogy a XXI. század egyik legnagyobb biztonsági próbatétele az egyre fokozódó mértékben jelen lévő adat-és információáradat kezelése, biztonságos felhasználása.

A biztonság tulajdonképpen egy veszélyektől mentes, zavartalan állapotot jelent, egy olyan állapotot, amikor az állampolgárok biztonságban tudhatják a szeretteiket, az értékeiket, a vagyontárgyaikat, és nyugodtan foglalkozhatnak a napi teendőikkel.¹ (dr. Christián, 2018) Ma már az érték nem tárgyasult forma, és nem pusztán a fizikai térben létezik, hanem a kibertérben is. Éppen ezért biztonságunkat itt is meg kell védenünk. Az információs társadalommá válás során nem csak a technológia fejlődik, hanem az adatok és információk megszerzésére irányuló kibertámadások is megtöbbszörözödtek, illetve jelentősen megváltoztak az elmúlt évtizedekben.

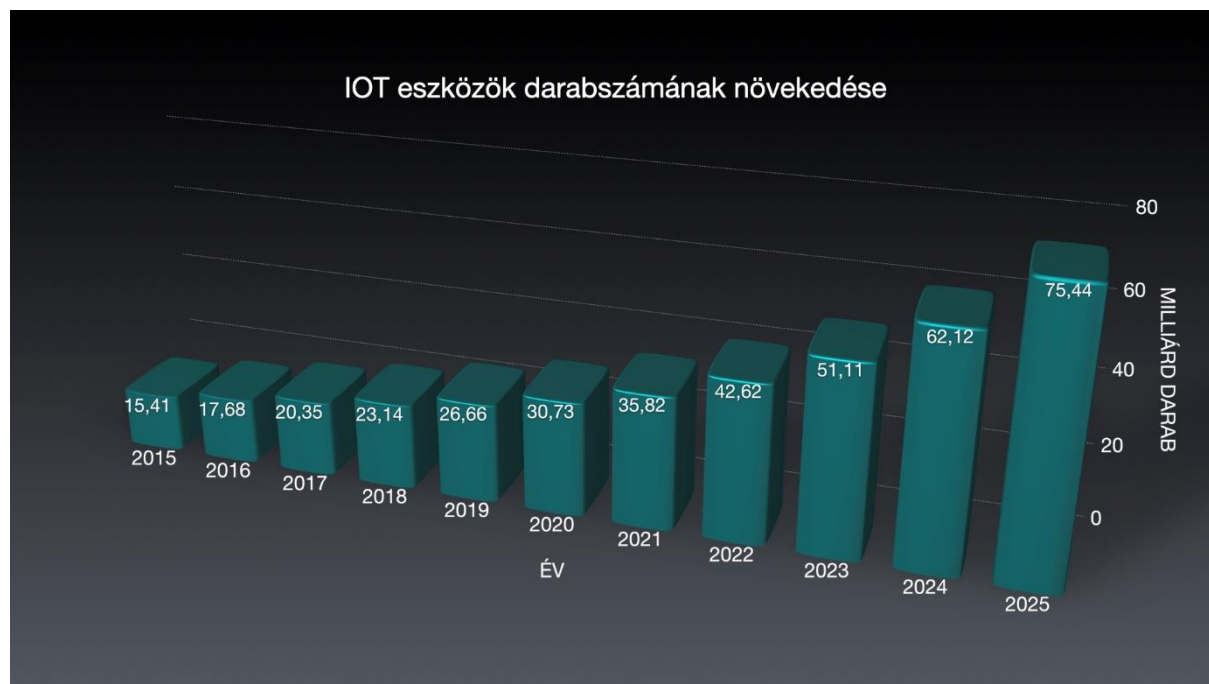
Korábban egy hackertámadás „csak” egy kihívás volt a támadó szemszögéből, egyfajta önigazolást, önmegvalósítást jelentett, ma viszont a támadások célja gyakran az anyagi vagy a nem

¹ “A "biztonság" a latin "securus" szóból (se = nélkül, cura = félelem) ered, jelentése félelem nélküli. A biztonság, az állampolgárok szemszögéből némileg leegyszerűsítve egy zavartalan állapotot jelent, amikor mindenki nyugodtan élheti mindennapjait, teheti a dolgát, mert biztonságban tudhatja saját magát, családját és szeretteit, valamint ingó és ingatlan vagyonát. A biztonság egy kézzel nem megfogható állapot, helyzet, amelyet hajlamosak vagyunk természetesnek venni, éppen ezért csak akkor gondolkodunk el rajta, amikor azt veszélyeztető tényezők, körülmények merülnek fel..”

materiális haszonszerzés, mint például az információ megszerzése, a biztonsági rések, sebezhetőségek feltárása, politikai vagy vallási ideológiák terjesztése, és napjainkban már kereskednek is az illegálisan megszerzett adatokkal.

A technikai és technológiai fejlődés egyik leginkább felívelőben lévő innovációi az IOT-eszközök. Az IHS előrejelzése szerint az IOT-eszközök piaca a 2015-ös 15,4 milliárd eszköztől 2025-re 75,4 milliárdra nő. (Columbus, 2016)

1. diagram: IOT-eszközök darabszámának növekedése



Forrás: a szerző saját szerkesztése (Columbus, 2016) alapján

A hétköznapi ember számára a leglátványosabb technológiai fejlődés az otthonaik IOT-eszközökkel való felszerelése, tehát “okosítása”, vagyis az okos otthon. Egy évtizeddel ezelőtt még az okos telefonok használata is ritkaságszámba ment, mára viszont egyre többen vannak azok, akik környezetüket és otthonaikat, mindennapi tevékenységeiket IOT-eszközök segítségével automatizálják. (Statista, Statista, 2022)

Az IOT-eszközök olyan eszközök, amelyek internetes hálózaton keresztül képesek érzékelni, értelmezni az információt, és a hálózaton keresztül képesek további eszközökkel kommunikálni. (Boda, 2019)²

² 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

Azt gondolhatjuk, hogy az IOT-eszközök teljes mértékben biztonságosak, és nem okozhatnak semmilyen problémát - sőt, nem csak a kényelmünket biztosítják, de a ránk, illetve a vagyontárgyainkra, otthonunkra leselkedő veszélyek kockázatát is csökkentik. Bár ezen eszközök célja az lenne, hogy kiszolgálják az embereket, nem pedig az, hogy kiszolgáltatottá tegyék, a valóság sokszor egészen mást mutat. Hasznosságuk ugyan vitathatatlan, hiszen felhasználásukkal számos tevékenység kényelmesebbé válik, nem kérdéses továbbá a segítségükkel elérhető költség-optimalizálás, időmegtakarítás, valamint a munka hatékonyságának növelése sem, azonban számos eset bizonyította, hogy az IOT-eszközök nem veszélytelenek, és az elmúlt évek kibertámadásainak ismeretében nem is biztos, hogy az IOT-ra épülő megoldásokat az egyre kifinomultabb, fejlettebb és széleskörűbb kibertámadásokkal szemben valaha teljesen biztonságossá lehet tenni.

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.”

2. IOT-ESZKÖZÖK KIALAKULÁSA, ALKALMAZÁSA

Bár az IOT-eszközök használata a XXI. században terjedt el igazán, az első intelligens eszközt az 1980-as évek elején készítette a Carnegie Mellon Egyetem néhány technikusa. Az egyik hallgató, David Nichols úgy ítélte meg, hogy túl messze van a tanszéktől a Coca-Cola automata, és számtalanszor előfordult, hogy átsétált az automatahoz, de az már üres volt, vagy csak meleg üdítő volt benne. Nichols írt néhány barátjának az ötletéről, miszerint megoldható lenne, hogy távolról nyomon kövesse a gép tartalmát, és végleg véget vessen ennek. Hamarosan két másik diák – Mike Kazar és Ivor Durham –, valamint az egyetem kutatómérnöke, John Zsarnay kezdett el vele dolgozni, hogy az a műszaki megoldás, miszerint távolról is meg lehet állapítani, hogy van-e kóla a gépben és az hideg is, megvalósuljon.

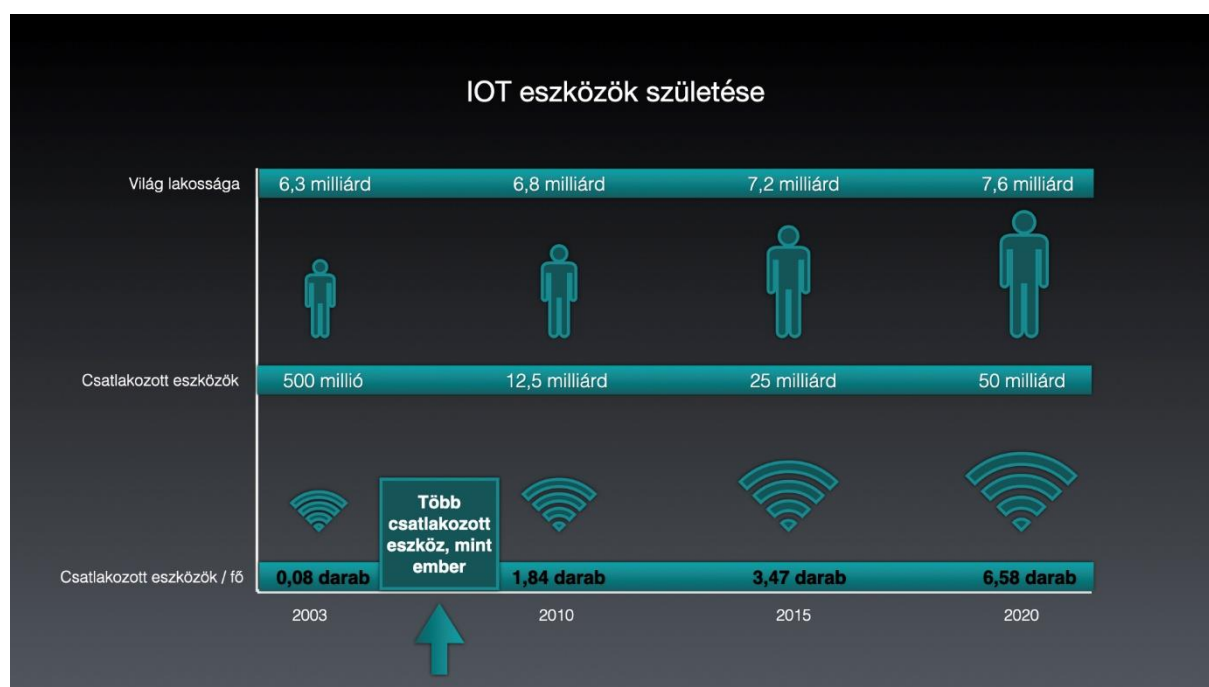
A programot az évek során tovább fejlesztették, amelynek köszönhetően a fogyasztók ezután már néhány egyszerű gombnyomással ellenőrizhették, hogy van-e kóla a gépben, és ha igen, akkor az hideg-e. A program gyorsan népszerűvé vált. Akkor egyébként nem gondolták, hogy évtizedekkel később ezt az eszközt úttörőként emlegetik majd, Kazar úgy nyilatkozott, hogy az IOT által uralt világ *“távoli fantáziának tűnt.”* (Teicher, 2018) Az IOT kifejezést egyébként először Kevin Ashton, a Procter & Gamble marketingmenedzsere használta 1999-ben, aki a cég egyik termékéért, egy rúzsért volt felelős. A termék váratlanul elfogyott a boltok polcairól, és Ashton ennek okát kutatva kiderítette, hogy a probléma az volt, hogy nem szóltak időben a boltok arról, hogy a termék el fog fogyni, azaz az egyes árnyalatok mennyiségi termékkövetése nem megfelelő. E probléma megoldásának keresése arra készítette, hogy megvizsgáljon egy technológiát, az RFID-technológiát (Radio Frequency Identification, azaz rádiófrekvenciás azonosítás).

A technológia ma már széles körben elterjedt, használják például a készletkezelésben: a gyártósoron a legyártott, RFID címkével ellátott végtermék elhalad az olvasó előtt, az olvasó leolvassa a címkét, majd a beérkező adatokat továbbítja a központ felé, így a központ valós adatokat lát a legyártott termékek és a meglévő készletének mennyiségével kapcsolatosan. (Kovács, 2018)

A technológiát korábban így mutatták be: *„Az RFID technológia egy előreutató megoldás, amelynek segítségével egy termék „élete” végig kísérhető a gyártástól egészen a megsemmisítéséig. Az RFID technológia forradalmasíthatja az áruátvételeket, a raktározást, a bolti lopás elleni védekezést, a termékhamisítást, a jótállási idővel történő manipulációt (átcímkézés) stb.* „ (Tóth & Tóth, 2014)

Ashton azt akarta elérni, hogy a cég vezesse be az RFID-t a termékek, a készlet mozgásának követésére. Később az MIT-nál, azaz a Massachusetts Institute of Technology-nál az RFID kutatásával és fejlesztésével foglalkozó Auto-ID Center vezetője lett. Ashton e munkája során több száz előadást tartott vállalati vezetőknek az RFID technológia lehetőségeiről és arról, hogy ezek a chipek hogyan tudtak más gépekkel kommunikálni vezeték nélküli hálózaton. Előadásainak az Internet of Things nevet adta. (Elder, 2019) Annak ellenére, hogy Ashton előadásai-
ban számtalanszor elhangzott a kifejezés, akkoriban mégsem terjedt el. Ennek oka, hogy az internet alapú eszközök 2008-2009-ben robbantak be igazán.

Ezt megelőzően az IOT-eszközök száma a világ lakosságához képest alacsony volt: 6,3 milliárd ember élt a bolygón, és 500 millió internethez csatlakozott eszköz volt. 2010-re viszont az IOT-eszközök száma 12,5 milliárdra nőtt a 6,8 milliárd fős emberiséghez képest. Ez azt jelentette, hogy a bolygó minden egyes emberére majdnem 2 ilyen eszköz jutott (pontosan 1,84). (Evans, 2011)

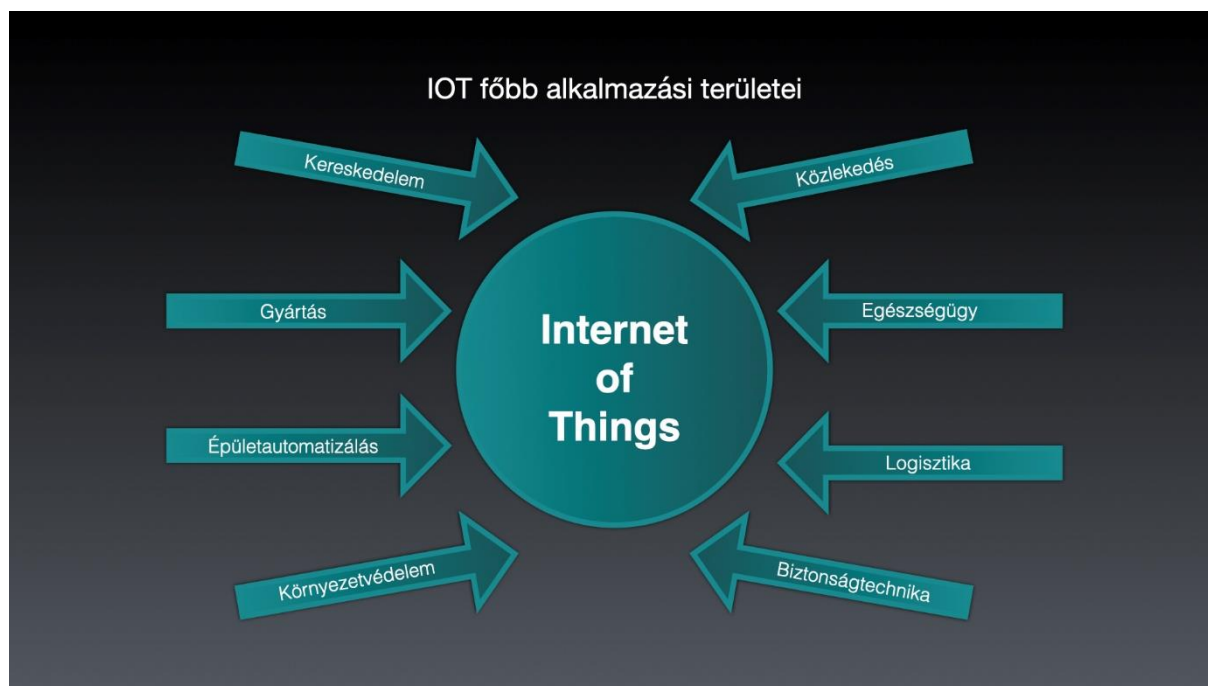


1. ábra: IOT-eszközök születése

Forrás: a szerző saját szerkesztése (Evans, 2011) alapján

2011-ben a Gartner piacelemző cég az IOT-t a feltörekvő technológiák közé sorolta, 2014-ben pedig a Google felvásárolta a Nest Labs céget, amely WiFi-képes, szenzoros eszközöket fejlesztett. Ezzel a Google is elkötelezte magát az IOT-eszközök mellett. (Portfolio, 2014) A cég fő profilja a házak és lakások fűtését automatikusan vezérelhető eszközök gyártása.

Az első igazán ismert okos otthon eszköz a Nest termosztátja volt, ami igazodott a felhasználók felkelési és lefekvési szokásaihoz, az időjáráshoz, illetve ahhoz, hogy a felhasználók mikor vannak otthon. Ennek fényében automatikusan szabályozta a fűtést és hűtést. (Perry, 2021) Mára az IOT-eszközök körének gyakorlatilag csak a fantázia szabhat határt. Alkalmazásuk jelen van és kulcsszerepet játszik többek között a biztonságtechnikában, a kereskedelemben, a közlekedésben, az épületautomatizálásban és az egészségügyben is.



2. ábra: IOT főbb alkalmazási területei

Forrás: a szerző saját szerkesztése (Lueth, 2020) alapján

2.1 Alkalmazása a biztonságtechnikában

A biztonságtechnika vonatkozásában az otthonok és a közterületek, közintézmények, társasházak vagyonvédelmi rendszereiben fontos megemlítenünk a szerepét, hiszen olyan érzékelők működnek az IOT technológiával, mint például a hő, - füst, - szénmonoxid eszközök, valamint a behatolás jelző rendszerek (üvegtörés-érzékelő, beléptető rendszer, nyitás érzékelők).

2.2 Alkalmazása a kereskedelemben

Az IOT-eszközöket a kereskedelemben a készletek és a logisztikai folyamatok nyomon követésére használják, illetve a vásárlói szokások megfigyelésére, segítségével például személyre szabott termékjavaslatokat kaphatnak az ügyfelek.

2.3 Alkalmazása az egészségügyben

Egészségügyi alkalmazása is egyre sokrétűbb, már nem csak az okos órák, állapotfigyelők vannak, hanem különböző testbe épített orvosi eszközök is (pacemaker). Az egészségügyi adatok elérése megoldott interneten keresztül, ezáltal a távolról történő asszisztencia, a nyomonkövetés, a receptek felírása, és a gyógyszeradag meghatározása is megoldható lehet távolról is. Az IOT-eszközök segítségével a páciens egészségügyi kórképe sokkal részletesebben monitorozható, és az eredményeket kontextusban lehet vizsgálni.

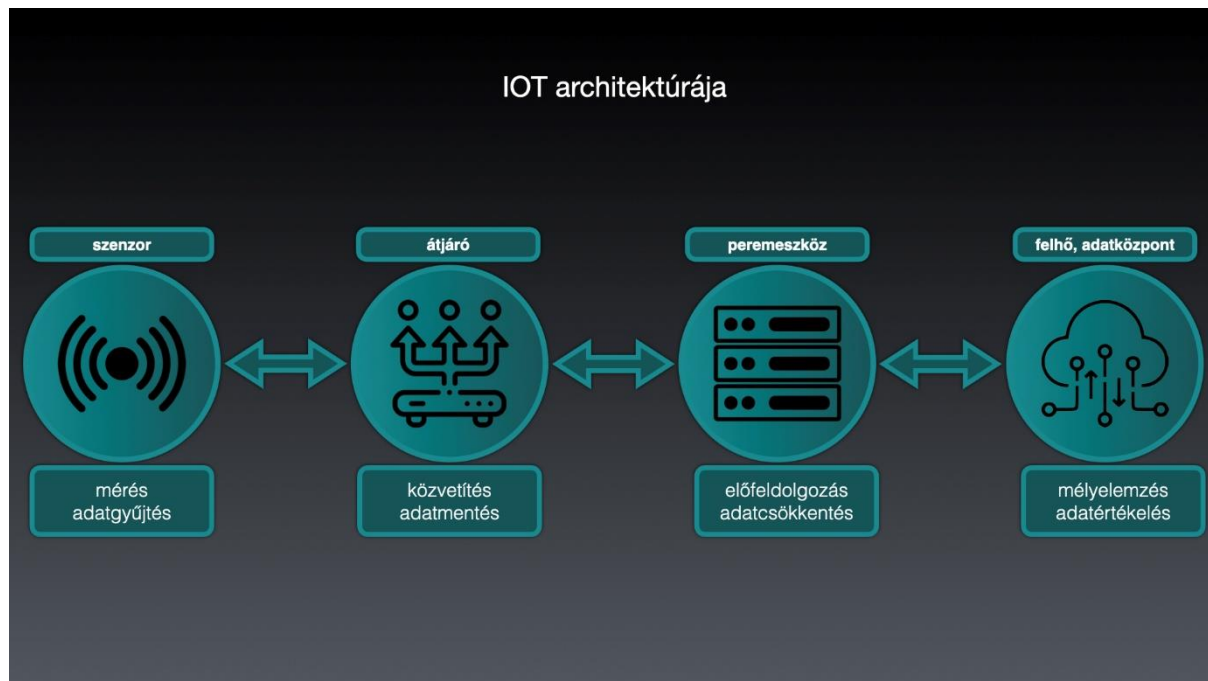
2.4 Alkalmazása a közlekedésben

Az IOT-eszközöket a közlekedésben is használják, segítségével a közlekedési infrastruktúra szintén digitalizálhatóvá vált. A hálózatba kötött járművek vezeték nélküli kommunikációs csatornán keresztül kapcsolódnak a hálózathoz, ezáltal egymással és más forgalomban részt vevő járművekkel, valamint a közlekedés részét képező eszközökkel (pl. lámpák) is képesek kommunikálni. Ma már léteznek a piacon önvezető autók is, amelyek a környezetük hatásainak változására reagálva önállóan képesek a közlekedésre, nem szükséges a vezető beavatkozása. Ebben a szektorban fontos megemlíteni az intelligens autókön kívül az intelligens forgalomirányítást, a forgalmi torlódási rendszereket, az intelligens parkolást, az elektronikus díjszedést vagy az utastájékoztató rendszereket, amelyek nagyrészt szintén IOT technológiával működnek.

2.5 Alkalmazása az épületautomatizálásban

Az épületautomatizálás célja az épületet használók (bérlők, lakók) komfortérzetének, biztonságérzetének növelése, az épület hatékony és gazdaságos működése, valamint a távoli vezérlés elérésének lehetősége. Intelligens energiatakarékos berendezések, kazánok, kapcsolók, csapok, fogyasztásmérők, szenzorok, háztartási eszközök közreműködésével működtethető egy lakás vagy épület, társasház, irodaház vízellátása, villamos energia ellátása, távfűtése, csapadékvíz vagy szennyvíz elvezetése. Ezáltal az épület működtetése gazdaságossá, komfortossá, költség- és energiatakarékossá tehető.

3. AZ IOT-ESZKÖZÖK MŰKÖDÉSE



3. ábra: IOT architektúrája

Forrás: a szerző saját szerkesztése

Az IOT-eszközök működése egy többrétű, összetett feladat, amelyben

- szenzorok,
- átjárók
- peremeszközök,
- vezérlők,
- kommunikációs csatornák
- és adatközpontok (pl. felhők, lokális szerverek) a főszereplők.

A szenzorok sokfélék lehetnek. Vannak:

- *“mechanikai,*
- *termikus,*
- *elektromos,*
- *optikai,*
- *kémiai*
- *és más fizikai paraméterek...”* érzékelésére alkalmas detektorok is.

Szenzorok például a hőmérséklet érzékelők, a nyomás érzékelők, a szintérzékelők. (Sallai, Budapest) A szenzorok folyamatosan mérnek, ebből adat keletkezik.

Ezeket az adatokat az adatösszegzők összegzik, a digitális átalakítók pedig digitalizálják. Az adatok ezután az átjárón és a kommunikációs csatornán keresztül eljutnak a hálózati peremeszközhöz, illetve a felhőalapú tárhelyhez.

Az átjárók feladata a közvetítés, képesek a kétirányú kommunikációra, valamint adatok mentésére és tárolására. Ez azért fontos, mert ez teszi lehetővé az adatok feltöltését, majd parancsok visszaküldését a felhőből az IOT-eszközre. Ugyanakkor nem minden esetben van biztonságosan elég idő arra, hogy a megvárjuk, amíg a felhőben megtörténik az adatok feldolgozása, ebben az esetben a peremeszközök segítségére támaszkodhatunk, ahol korábban van lehetőség az adatok kezelésére. A peremeszközben megtörténik az adatok csökkentése, előfeldolgozása és elemzése.

Ez három tényező miatt lényeges:

- egyrészt, mert ha valós idejű reagálásra van szükség – egy veszélyhelyzet esetén például -, akkor nincs idő arra, hogy az eszköz megvárja a felhőben történő adatfeldolgozást és válaszadást,
- másrészt, ezáltal csökkentik a hálózat terheltségét is,
- harmadrészt pedig a felhőszolgáltatás nem minden esetben érhető el, így viszont biztosan nem marad el a reakció.

Az adatok kiértékelése után a központi vezérlés küldi a parancsokat az eszköznek, amelyeket az eszköz végrehajt: leengedi a redőnyt, ha nagyon süt a nap, kinyitja a garázsajtót, ha érzékeli, hogy mi parkoltunk be az autónkkal, elzárja a csapot, ha vízszivárgást észlel. A felhőben az adatok mélyreható feldolgozása, kezelése, tárolása, elemzése, fejlesztése történik. A mélyelemzés és a részletes kiértékelés után a rendszer további visszacsatolásokat vagy parancsokat adhat, amely után a központi vezérlés ismét működésbe léphet. A részletes kiértékelésből kinyert információt a felhasználó (vagy épp a mesterséges intelligencia) a későbbiekben fejlesztheti, és a gyakorlatban is hasznosítható tudássá alakíthatja. (Haig, 2018) (Molnár, 2020)

A működést legegyszerűbben egy példán keresztül érthetjük meg. Vegyünk egy olyan esetet, amikor otthonunkban tűz keletkezik. Itt a személy és vagyonvédelem miatt is gyors reagálásra van szükség.

Amennyiben rendelkezünk IOT-alapú hőmaximum/hősebesség érzékelővel, illetve szintén IOT-alapú füstérzékelővel, akkor tűz esetén:

- az eszközökben lévő szenzorok a hőmérséklet-emelkedésre, és a füstre reagálva aktívvá válnak, mérni kezdenek, információkat gyűjtenek.
- az összegzett és digitalizált adatok a routeren és a WiFin keresztül eljutnak a peremeszközhöz, amely detektálja, hogy jelentősen megemelkedett a hőmérséklet - amely így már nem a megadott tartományban mozog -, illetve, hogy füst keletkezett a szobában.
- a peremeszköz ezután azonnal információt küld a vezérlőnek, amely pedig működésre készíteti a füstjelző berendezést, illetve értesítést küld a felhasználónak a veszélyről.
- ezzel együtt megtörténik az adatok továbbítása a felhőbe, ahol egy szoftver segítségével megtörténik az adatok mélyelemzése, értékelése.
- ezután a vezérlő további parancsokat is végrehajtathat, például más eszközt is működésbe hozhat: aktiválhatja a tűzvédelmi berendezéseket vagy a nyitásérzékelőket a menekülési útvonalakon.

4. A KOMMUNIKÁCIÓS CSATORNÁK ÉS A FELHŐSZOLGÁLTATÁSOK

A kommunikációs csatornát és a felhőszolgáltatást külön fejezetben is tárgyalom. Ennek oka, hogy a kommunikációs csatornák az IOT-rendszerek alapkövei, azok nélkül az eszközök nem működnek. A felhőszolgáltatást pedig azért említem külön fejezetben, mert az - a szenzorokkal és a peremeszközökkel ellentétben - egy fontos támadási terület.

4.1 Felhőszolgáltatások

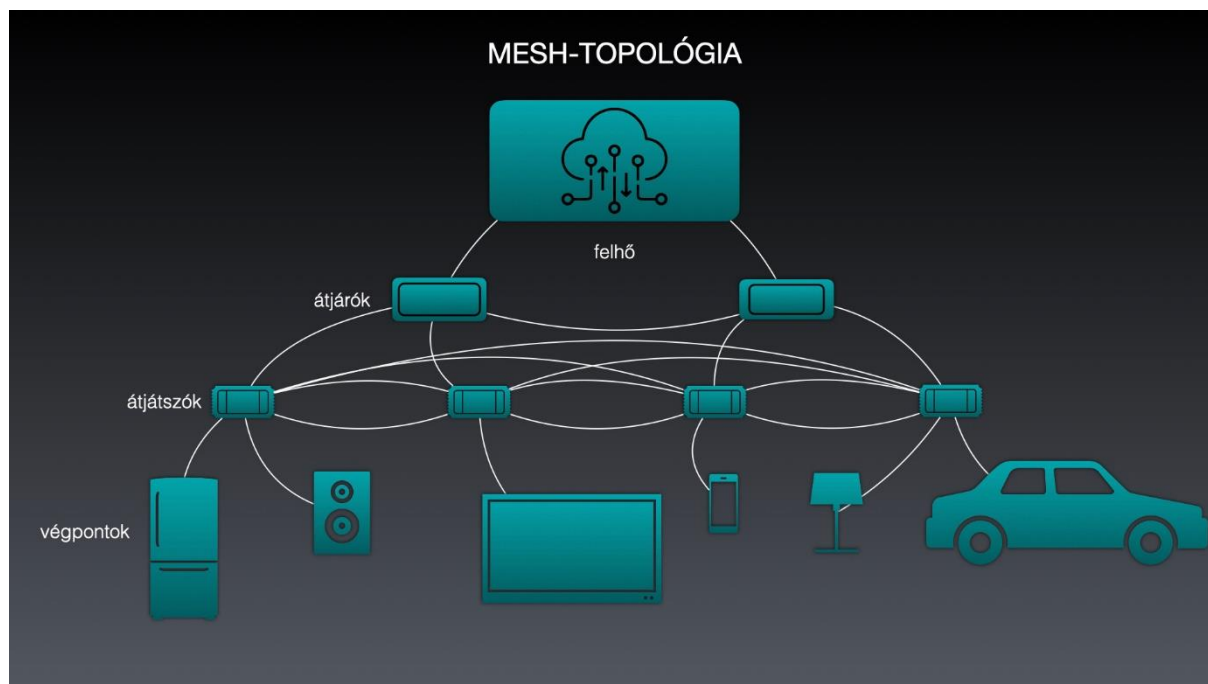
A felhőszolgáltatás lehetővé teszi az adatok egy helyen történő, komplex kezelését és tárolását. A Rendészettudományi Szaklexikon megfogalmazása szerint a felhőszolgáltatás *“adatok tárolására kialakított szolgáltatás. A szerverek a világ különböző pontjain működnek, amelyek folyamatosan kommunikálnak és adatcserét folytatnak egymással azért, hogy a felhasználók elérhessék az oda feltöltött adatállományait.”* (Boda, 2019) A felhő alapú szolgáltatás lényege tehát, hogy a felhasználók interneten keresztül érhetik el adataikat és eszközeiket, ezáltal azokat bárholonnan, bármikor kezelhetik, vezérelhetik. Nincs szükség fizikai szerverre, ezáltal a fizikai sérülés kockázata - legalábbis a felhasználónál - nem áll fenn. Hátránya azonban, hogy az adataink éppen ebből kifolyólag nem kézzel fogható helyen, hanem valahol a virtuális térben vannak.

Az amerikai Nemzeti Szabványügyi és Technológiai Intézet (NIST) négy fajta felhőszolgáltatás-módot különböztet meg:

- Nyilvános felhő: ez a leggyakrabban használt felhőszolgáltatás, bárki számára elérhető, a felhasználóknak azonban nincs rálátásuk az üzemeltetésre.
- Magánfelhő: kizárólag egy felhasználója van, a felhasználó nem osztja meg mással, interneten vagy saját magánhálózaton keresztül érhető el.
- Közösségi felhő: több szervezet egyszerre használja, egymás között megosztva.
- Hibrid felhő: az előző modellek keveréke, amikor az adatok megoszthatóvá válnak a nyilvános vagy magánfelhő között. (Kókay, 2017)

4.2 Kommunikációs csatornák

Az IOT-eszközök alkalmazása során gyakorlatilag mindegyik kommunikációs csatorna a mesh hálózati topológiát alkalmazza. A mesh hálózat azt jelenti, hogy az átjátszók közvetlenül egymáshoz kapcsolódnak, egymástól veszik és továbbítják a jelet, ezáltal sokkal nagyobb lefedettséget és stabilabb kapcsolatot biztosítanak. További előnye, hogy kevesebb hibalehetőséggel lehet számolni, mivel működése nem a központi vezérlőtől függ. (Putnóczki, 2019)



4. ábra: Mesh-hálózat

Forrás: a szerző saját szerkesztése

A kommunikációs csatorna háromféle lehet:

- mobilhálózat,
- vezetékes
- vezeték nélküli.

A mobilhálózat cellákon keresztül teszi lehetővé az adatáramlást. Minden cella tartalmaz egy bázist, egy rögzített adó-vevőt, amely biztosítja a kommunikációt a hálózat és a felhasználó között. Ezek a bázisok egymással vezetékes hálózati összekapcsolásban vannak. Azoknak az eszközöknek, amelyek használni akarják a rádiófrekvenciás kapcsolatot, mindig ahhoz a bázishoz kell kapcsolódniuk, amelyek a legközelebb vannak hozzájuk. (Kelényi, 2008)

Annak ellenére, hogy folyamatosan fejlesztik a mobilhálózatok adatátviteli sebességét, a mobilhálózat jelenlegi formájában nem feltétlenül ideális választás az IOT-eszközök kommunikációs csatornájaként. (Szemerey & Kis, 2020) Ugyanakkor az 5 G hálózat kiépítésével és bevezetésével – ami jelenleg is zajlik – a jövőben az IOT-eszközök mobilitása, és ennek köszönhetően akár több milliárd eszköz összekapcsolása is megoldható lesz ezzel a technológiával. Bevezetése azonban nem teljesen elfogadott, mert az 5 G elektromágneses hullámaihoz kapcsolódó bizalmatlanság, az egészségkárosító hatásaitól való félelem megosztja mind a lakosság, mind pedig a tudományos és politikai közösségeket.

A vezetékes hálózatok esetében a kommunikáció fizikai kábeleken keresztül zajlik, réz alapú vagy optikai kábelek teszik lehetővé a kommunikációt. Előnye, hogy stabil kapcsolatot biztosít, hátránya, hogy a felhasználás helyhez kötött, és a későbbiekben nehezen bővíthető. A vezetékes kommunikációs rendszerek közé tartozik a BUS topológia. (Szemerey & Kis, 2020) A BUS topológia egy egész épületen átfutó hálózat, amelyre a készülékeket sorban lehet rácsatlakoztatni. Az eszközök mindegyike külön címezést kap. Így minden egyes eszköz külön-külön kapcsolódik a központi vezérléshez, ezáltal viszont gondos tervezést és rengeteg vezetékelést igényel. (Kovács, 2018)³

A vezeték nélküli hálózatok úgy teszik lehetővé a hálózati eszközök, számítógépek, okos eszközök közötti adatáramlást, kommunikációt, hogy nincs szükséges fizikai kábelezésre, fizikai összeköttetésre a gépek között. Az eszközök ebben az esetben rádióhullámok igénybevételével képesek biztosítani az adatátvitelt, ezáltal biztosítva a felhasználók számára a mobilitást. A vezeték nélküli hálózatok közül a legismertebb a WLAN és WiFi hálózatok.

Ezek tehát a kommunikációs csatornák, maga a kommunikáció pedig kétféle lehet:

- kis hatótávolságú: maximum néhány 100 méter, ami leginkább a hálózatra kapcsolt eszközök és az átalakítók körében jellemző,
- nagy hatótávolságú, ami több tíz kilométer is lehet

Az IOT-eszközök esetében a kis hatótávolságú csatornáknak van relevanciája, hiszen az információt nem szükséges kilométerekről beszerezni.

Az alacsony adattovábbításra alkalmas protokollok közül a legismertebbek:

- WiFi: a legelterjedtebb és legismertebb kommunikációs interfész. Ha ezt a technológiát használjuk, akkor nagy hatótávolságon belül nagy adatforgalmat tudunk továbbítani, egyszerre több eszköz részére. A jel erősségét nagyban befolyásolja, hogy milyen vastagságú falakon, akadályokon kell átmennie, illetve minél több eszköz csatlakozik rá egyidejűleg, annál lassabb a hálózati kapcsolat. Mivel az okos otthonokban egyidejűleg számos eszközt kell működtetni, ott önmagában a WiFi nem biztosítja a megbízható működést.
- BLE: a Bluetooth technológia továbbfejlesztett változata, amely alacsony hatótávolságon belül működik. A Bluetooth Low Energy legfontosabb technológiai ismérve az, hogy környezettudatos, alacsony adatmennyiségeket továbbít, és közvetlen kapcsolatot biztosít a két összekapcsolt eszköz között. Főként szenzorokban használják.
- NFC: néhány centiméteres kommunikációs távolságának köszönhetően ez a legalacsonyabb hatótávolságú protokoll. A kis távolság miatt gyors az adatátvitel sebessége. Alkalmazható például beléptető rendszereknél vagy telefonnal történő bankkártyás fizetés esetén. Az adatátvitelhez a mágneses teret használja.
- RFID: ez egy olyan rendszer, amely a rádióhullámokat használja fel az adatok továbbítására. Alapvető eleme a korábban már tárgyalt RFID címke, az antenna és az RFID olvasó. Termékek vagy élőlények azonosítására szolgálhat.
- Thread: kifejezetten okos otthon megoldásokhoz fejlesztett kommunikációs csatorna, amely magas titkosítási lehetőséggel, és alacsony energiafelhasználással működik. Fő előnye a környezettudatosság és energiahatékonyság, alacsony fogyasztásának köszönhetően az elemes eszközök hosszú ideig képesek működni.
- z-Wave: energiatakarékos, a WiFihez képest kis hatótávolságú, kisméretű adatok továbbítására fejlesztették. Rádiófrekvenciás kommunikációs technológiával működik, leggyakrabban érzékelőkhöz használják. Jellemzően az eszközök mindegyike összekapcsolódik egymással. Vannak olyan eszközök, amelyek fogadják és továbbítják is a jelet, vannak, amelyek pedig csak fogadják, de nem továbbítják. Legfeljebb 232 csatlakozott eszközt tud kezelni. Ez egy biztonságos protokoll, épület-automatikához tervezték.⁴ Ideális ajtózárahhoz, háztartási gépekhez, világítástechnikához.

⁴ NKI Kibertámadás! Podcast: Okos az otthon, de biztonságos? <https://nki.gov.hu/en/podcast/> 09.24 perc letöltés 2022. 09. 01.

- ZigBee: egy széles körben használt vezeték nélküli kommunikációs csatorna, alacsony fogyasztással rendelkezik, ebből kifolyólag az elemről működő eszközök akár több éves üzemidővel rendelkeznek. Alacsony adatforgalom továbbítására tervezték. Több, mint 65 ezer eszközt képes kezelni. (Varga A. K., 2014) Jellemzően mesh hálózaton működik, az eszköz átjátszóként is funkcionál, tehát más eszközök adatait is képes venni és továbbítani. Leginkább háztartási készülékek, fűtés-és világítási rendszer vezérlésére használják. (Haig, 2018) (Lopez, Pasaoa, Morales, & Parado, 2016)

1. táblázat: Adatkommunikációs csatornák összehasonlítása

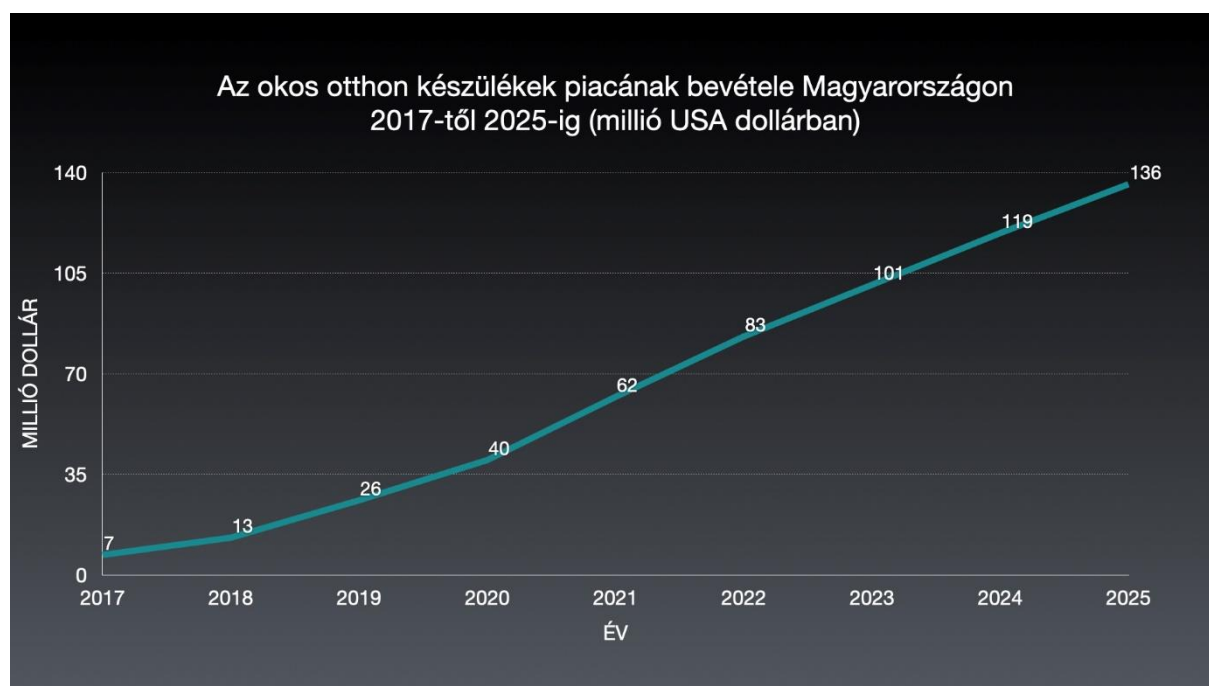
Kommunikációs csatornák összehasonlítása		
Kommunikációs csatorna	Adatátviteli sebesség	Hatótávolság
BLE	1-3 Mbit/s	35 m
NFC	100-420 kbit/s	10 cm
RFID	423 kbit/s	1 m
Thread	250 kbit/s	160 m
Z-Wave	100 kbit/s	30 m
ZigBee	250 kbit/s	160 m
WiFi	500 Mbit/s	100 m

Forrás: a szerző saját szerkesztése (Haig, 2018) alapján

5. IOT-ESZKÖZÖK AZ OTTHONUNKBAN

Az IOT fogyasztói és magáncélú alkalmazási területe leginkább az intelligens otthonokban mutatkozik meg, az IOT-eszközök alkalmazása az okos otthonokban pedig évről évre növekszik Magyarországon.

2. diagram: Okos otthon eszközök piacának bevétele Magyarországon 2017-2025



Forrás: a szerző saját szerkesztése (Statista, statista.com, 2021) alapján

Okos otthonokban IOT-eszközök többek között a kerítésvédelmi eszközök, a kaputelefon és csengő, a kül- és beltéri mozgásérzékelők, a falbontás-érzékelő, az üvegtörés-érzékelő, a kül- és beltéri kamerarendszer, az ajtó- és ablaknyitás érzékelő, a tűzjelző rendszer, a szén-monoxid jelző rendszer, a fénytechnikai rendszerek, a hűtés-fűtéstechnikai rendszerek, a szórakoztató elektronikai rendszerek és a háztartási berendezések. Ezt a technológiát használják továbbá a garázkapuk vezérlésére, az öntözőrendszerek automatizálására, a napelemek felügyeletére, a kerti világítások kezelésére és az árnyékolástechnikára is.

Fontos megjegyezni, hogy egy otthon nem attól lesz okos, hogy távolról vezérelhető eszközöket alkalmazunk. Attól, hogy távolról fel tudjuk kapcsolni a lámpát, el tudjuk indítani a mosógépet vagy rá tudunk nézni a kamerarendszerre, még nem beszélhetünk okos otthonról, de az, hogy eszközeink távolról vezérelhetők legyenek, kétségkívül egy kihagyhatatlan lépés.

Okos azonban akkor lesz egy otthon, ha az eszközök adatokat is gyűjtenek és elemeznek, összefüggéseket alkotnak és ez alapján képesek döntéseket hozni, és összehangoltan, összekapcsolva cselekedni a teendőkkel kapcsolatban. 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 egy egységes, organizált rendszerként tudjanak működni. Egy okos otthon vezérlése többféle módon történhet. Kézi vezérlés során a felhasználó kapcsolja ki vagy be az adott funkciót. Nincs szükség kézi vezérlésre, ha a tevékenység időponthoz van kötve. Ebben az esetben a kérdéses időpontban az eszköz elvégzi a feladatát.

Kezelhetjük a rendszerünket applikáció segítségével is valamely okos eszközünkről (telefon, tablet, számítógép). Ennek előnye, hogy mivel ezek az applikációk jórészt felhő alapon működnek, ezért interneten keresztül akár távolról is irányíthatóak az eszközök. Ilyen platform például a Google Home, a HomeKit, a Tuya Smart, az eWeLink, stb. (Putnóczki, 2019) A rádiófrekvenciás irányítás is egy vezérlési forma, amely egyirányú kommunikációt tesz lehetővé. Ebben az esetben megmaradnak azok a direkt vezérlési lehetőségek, amelyek akár a LAN hálózat ki-maradása esetén kézzel működtethetővé teszik az eszközt. Ilyen eszköz lehet például egy kapu nyitó távirányító. (OkosOtthonBolt, 2022)

A vezérlést megoldhatjuk úgy is, hogy eszközeinket előre megadott egyszeri vagy ismétlődő be és/vagy kikapcsolásra állítjuk be. Nem csak időpontot, de időintervallumot is programozhatunk. Az automatizálás lényege a szabályrendszer felállítása, tehát feltételeket állítunk be a működéshez. A parancsokat egy, vagy egyszerre több eszköz részére is leadhatjuk, így funkciójukat egymással összhangban vagy egymástól függetlenül is képesek ellátni. Az automatizálás felhő alapú. A felhő-alapú mellett létezik azonban helyi, lokális vezérlés is. Ebben az esetben a központ működése, illetve a programozott parancsok és szabályok lokális szerveren tárolódnak, nem pedig a felhőben. Elérésük, mivel helyhez kötött, bármikor hozzáférhetővé válik. További előnye, hogy ha nincs internet, az eszköz akkor is irányítható marad. Ilyen platform - ami képes kezelni a lokális okos eszközöket - például a Home Assistant.

Az okos eszközök hangvezérléssel is működtethetőek, amely a mesterséges intelligencián alapul. A virtuális asszisztensek csupán néhány éve vannak jelen a piacon, de mind az Apple, mind az Amazon, mind a Google folyamatosan fejleszti őket. A virtuális asszisztensek tulajdonképpen olyan okos hangszórókba épített virtuális segédek, amelyek nem csak zene lejátszására képesek, hanem értik a felhasználó utasításait, és azokat végre is hajtadják. A felhasználók ezáltal szóbeli parancsokat adva vezérelhetik az okos otthon eszközeit.

A virtuális asszisztensek ezen túl képesek válaszolni a felhasználó kérdéseire. Ilyen például az Amazon Echo és intelligens asszisztense, aki Alexa névre hallgat, a Google Home, ami szintén rendelkezik intelligens asszisztenssel és a HomePod, ami az Apple terméke, intelligens asszisztense pedig Siri. Magyarul még egyik sem képes kommunikálni. (OkosOtthonBolt, 2021)



1. kép: Amazon Echo, Google Home, HomePod

Forrás: (notebook.hu, 2022) (tutiplaza.hu, 2022) (apple.com, 2022)

6. IOT-ESZKÖZÖK ELŐNYEI AZ OKOS OTTHONOKBAN

6.1 Kényelem, szórakoztatás, megtakarítás

Az IOT-eszközök előnyei közé sorolható a kényelem és szórakozás, hiszen adott esetben a felhasználó helyett végez el feladatot, mindez pedig időmegtakarítással jár. Számos napi rutinfeladatot kivált, mint például az égve maradt lámpák lekapcsolása, a háztartási munka egy részének elvégzése, bevásárlólista készítése, de az sem lesz kérdés, hogy égve maradt-e a sütő, bedugva maradt-e a vasaló, nyitva maradt-e a garázskapu. Akár az ágyból fekvé elindíthatjuk az öntözőrendszerünket vagy hangüzenettel kérhetjük kedvenc dalunk lejátszását az okosvezérelt audio-technikánktól. A technológia emellett az otthon működését energiatakarékosabbá, környezetbaráttá, és biztonságosabbá is teheti. Az eszközök - érzékelve a környezeti hatásokat, az időjárás változását - biztosítják azt, hogy a fűtő vagy hűtő berendezések akkor kapcsoljanak be és ki, amikor azokra ténylegesen szükség van, a lámpák pedig csak akkor világítsanak, ha valaki valóban tartózkodik a helyiségben. Ezáltal a felesleges energiafelhasználás csökken vagy teljesen megszüntethető, így nem csak kevesebb rezsiköltséggel lehet számolni, hanem a gazdaságos üzemeltetésnek köszönhetően kialakítható a környezettudatos és környezetbarát felhasználás is. A Nest Labs tanulmánya szerint egy átlagos háztartás akár 12%-ot spórolhat a fűtési költségen, míg 15 %-ot a hűtési költségen abban az esetben, ha okos termosztátot használ. (Nest Labs, 2015) A rendszer a felhasználói szokásokhoz igazítható, tanítható és ennek megfelelően vezérelhető.

6.2 Biztonságtechnika

Az okos otthonok biztonságtechnikai eszközei komplex működésüknek köszönhetően jelentősen több biztonsági funkciót képesek ellátni az általános felügyeleti rendszerekhez képest. Gyánús mozgás esetén például nemcsak a riasztó szólal meg, a világítás is felkapcsolódik. Az eszközöknek köszönhetően bezárhatnak a biztonsági zárok, és rögtön jelzést adhatnak a telefonunkra. Biztonság tekintetében egyébként nem kizárólag bűncselekményre kell gondolnunk, hanem akár egy tüzesetre, ázásra, szénmonoxid veszélyre - ezekről szintén értesíteni tudják a felhasználót. Ázás vagy vízszivárgás esetén el tudják zárni a vizet, szénmonoxid szivárgás esetén azonnali szellőzést tudnak biztosítani.

6.3 Egészség

Egészségmegőrzés tekintetében szintén számos okos eszköz áll rendelkezésünkre otthonunkban. A legjelentősebbek a párásító vagy páramentesítő, levegőtisztító berendezések, valamint az okos vérnyomásmérő, különböző alvásfigyelő eszközök, illetve a testünkön viselhető okos karkötők, okos órák, amelyek a pulzust, véroxigénszintet, aktivitásunkat mérik és jeleznek, ha rendellenességet tapasztalnak, figyelmeztetnek, ha nem ittunk megfelelő mennyiségű folyadékot, figyelemmel kísérik fizikai állapotunkat.

7. AZ IOT-ESZKÖZÖK VESZÉLYEI - HOGYAN LESZ LÁTHATÓ BARÁTBÓL LÁTHATATLAN ELLENSÉG?

Az internethez kapcsolódó IOT-eszközök komoly biztonsági kockázatot jelentenek, ami egyéni és globális szinten is problémákat okozhat. *“Minden, ami felkapcsolódik az Internetre, meghekkkelhető. Az okosotthonnal a meghekkkelhető otthon is létrejön, (...)”* (Bálint, 2018.) Az adatok és információk biztonságos tárolása és kezelése tehát napjaink kihívása, a hálózatba kapcsolt eszközök biztonságossága megkérdőjelezhető. 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. A támadási lehetőségek feltérképezéséhez fontos megismernünk, hogy milyen biztonsági réseket használhatnak ki a bűnözők.

- mobilalkalmazás: ez teszi lehetővé az intelligens eszközök kezelését és irányítását. A legtöbb IOT-eszköz szerves részét képezi. A mobilalkalmazások feltörése egy belépési pontként is szolgálhat a felhőben tárolt adatok megtámadására. Amikor le-töltünk egy alkalmazást, akkor az alkalmazás használatához engedélyeket kell meg-adnunk arra vonatkozóan, hogy az alkalmazás mely adatainkhoz és egyéb alkalma-zásainkhoz férhessen hozzá. Nem mellesleg a mobilalkalmazások – amennyiben nem megbízható forrásból származnak – rosszindulatú programokat is tartalmazhat-nak. (Erdősi & Solymos, 2017) Nem egy esetben bizonyosságot nyert, hogy néhány kínai okos készülék már a forgalomba kerülésekor olyan alapértelmezett alkalma-zásokat tartalmaz, amelyek kémsoftvereket rejtenek magukban. 2015-ben például a Lenovo laptopok esetében találtak olyan felületet, amely a felhasználó monitoro-zását is lehetővé teszi, alkalmas volt továbbá támadások szervezésére is. (Bányász, 2022)
- webes felület: a legfontosabb sebezhetőségi pont ebben az esetben a felhasználói adatok tárolása a sütikben (cookie-kban), a felhasználói azonosítás, az információk továbbítása nem titkosított csatornán keresztül. A sütik eltárolják a korábbi böngé-szés során keletkezett adatokat, nem csak a böngészőben, de a webszerveren is. Egy esetleges támadás során a támadó megszerezheti a tárolt jelszavakat vagy akár hoz-záférhet a géphez is, amiről a böngészés történt. (Erdősi & Solymos, 2017)
- hálózati interfészek: ezek azok az elemek, amelyek hálózaton keresztül hozzáférhe-tőek. Az igénybe vett szolgáltatások során a kommunikáció nem feltétlenül titkosí-tottan folyik, így a kommunikáció védelem nélkül marad.

Ha a kommunikáció nem titkosítottan vagy megfelelően védetten zajlik, akkor könnyen lehallgathatóvá válik. A nem biztonságos hálózati kapcsolaton keresztül egyszerűbbé válik nem csak az adatszerzés, de a támadó egyszerűbben tud rosszindulatú vírusokat is elhelyezni az eszközre. (Gupta, 2019)

- firmware: felelős az eszközön végzett műveletekért, az elektronikai eszközök vezérlését végzi. Enélkül az eszköz működésképtelen lenne. Biztonsági szempontból az IOT-eszközök legkritikusabb összetevője. Számos biztonsági rést tartalmazhat, így például a nyitva hagyott hátsó bejáratokat, ez egy olyan kiegészítés a szoftverben, amely meghatározott személyek részére hozzáférést enged bizonyos programokhoz vagy eszközökhöz. A nyitva hagyott backdoor bejáratként szolgál a teljes irányítás és ellenőrzés átvételére és arra, hogy más hálózatba kapcsolt eszközök kezelése is elérhetővé váljon. De a szoftverekben a gyenge titkosítási megoldások is kihívást jelentenek. Az emberi tényező is szerepet játszhat a biztonsági kérdésekben, mert ha van is firmware frissítésre lehetőség, nem feltétlenül teszik meg ezt a biztonsági intézkedést. (Gupta, 2019)

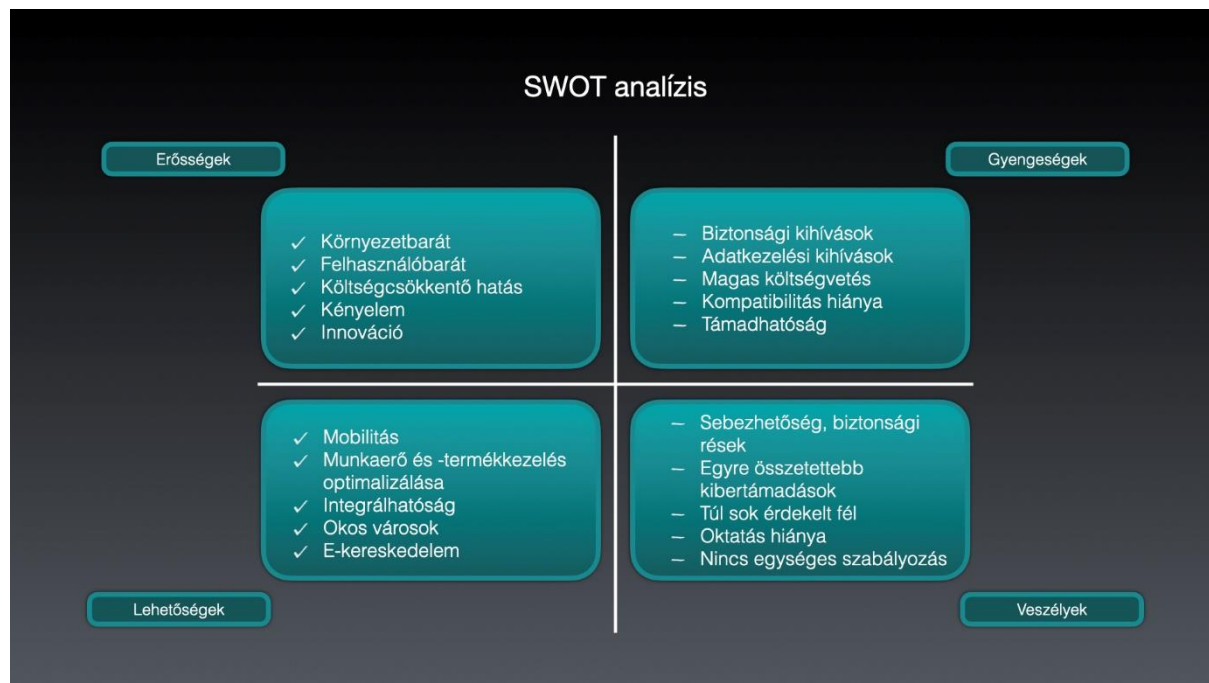
Bár számtalan felhasználó veszi ezeket az eszközöket, egyre több mindent okosít és automatizál, még sincs megfelelő képe a veszélyekről. Nincs oktatás adatvédelmi és egyéb biztonsági szempontok tekintetében, a felhasználónak alapvető ismeretei sincsenek azzal kapcsolatban, hogyan védheti meg magát a kibertámadásoktól, vagy egyáltalán milyen veszélyeknek van kitéve. Pedig a veszély adott. Dan Demeter, a Kaspersky biztonsági szakértője elmondta: „*We see that once users' interest in smart devices rose, attacks also intensified.*” Azaz „*Azt látjuk, hogy amint a felhasználók érdeklődése megnőtt az okoseszközök iránt, a támadások is felerősödtek.*” (Cyrus, 2021)

7.1 Az IOT-eszközök erősségei, gyengeségei, lehetőségei, veszélyei, SWOT analízis

A SWOT analízis egy mozaikszó, ami az alábbiakból tevődik össze:

- Strengths – erősségek
- Weaknesses – gyengeségek
- Opportunities – lehetőségek
- Threats – veszélyek

A SWOT analízis szerint a belső tényezők (erősségek és gyengeségek) azok, amelyekre van ráhatásunk, a külső tényezők (lehetőségek és veszélyek) pedig azok, amelyek hatáskörünkön kívül esnek.



5. ábra: SWOT analízis

forrás: a szerző saját szerkesztése

7.2 Esettanulmányok

7.2.1. Az okos akvárium és a kaszinó

A Darktrace nevű kiberbiztonsági vállalat vezérigazgatója, Nicole Eagan 2018-ban beszélt egy konferencián arról az esetről, amikor bűnözők egy akváriumban elhelyezett okos hőmérséklet-szabályozón keresztül hatoltak be egy kaszinó rendszerébe, majd lopták el a sokat költő játékosok személyes adatait. (Williams-Grut, 2018) Akik így potenciális áldozattá váltak.

Egy kiberbűnöző több milliárd emberből válogathat. Anyagi haszonszerzés esetén ugyanakkor csak azokat érdemes megcélozni, akik jelentős anyagi forrásokkal rendelkeznek. Azt viszont, hogy ki, mennyi pénzből él, nem könnyű kideríteni - ám aki milliókat költ el egy kaszinóban, az kétségkívül kiváló áldozatnak tűnik. Sokkal nagyobb esély van tőle pénzhez jutni, mint egy véletlenszerűen választott embertől az interneten. A pénzszerzés egyik módja a zsarolás. A kiberbűnözők ehhez úgynevezett zsarolóvírusokat, másnéven ransomware-eket használnak.

Ez egy olyan rosszindulatú szoftver, amely segítségével a támadó a felhasználó eszközén tárolt adatokat és információkat titkosítja, azokat pedig csak váltságdíj ellenében oldja fel, és teszi újra elérhetővé a tulajdonos részére. A zsarolóvírusok sok esetben e-mail-ben, egy csatolmány-nal jutnak 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
- 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 (Cisco, 2016) (Nemzeti Kibervédelmi Intézet, NKI, 2022)



6. ábra: Zsarolóvírus

Forrás: (eset.com, 2020)

A zsarolóvírusok a következő években várhatóan gyakoribbá válnak, mert az emberek 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 - adataihoz mindenki ragaszkodik, elvesztése hatalmas károkkal jár.

Elgondolkodtató kérdés ugyanakkor, hogy érdemes-e ilyen esetben fizetni vagy sem. A holland rendőrség Számítástechnikai Bűncselekmények Elleni Egysége, az Europol Európai Számítástechnikai Bűnügyi Központja, valamint a Kaspersky Lab és egy másik, információbiztonsággal foglalkozó vállalat segítségével létrejött a No More Ransom, azaz a Ne legyen több zsarolóvírus nevű honlap. Az oldal iránymutatása: „*Don't pay the ransom*”, azaz „*Ne fizess a zsarolónak*”.

A magyar Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztálya is csatlakozott a kezdeményezéshez. (Kovács, 2018) A „*ne fizess a zsarolónak*” elv melletti egyik érv, hogy semmilyen garancia nincs arra, hogy a pénz kifizetése után 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. (Nemzeti Kibervédelmi Intézet, NKI, 2020)

7.2.2. A 2016-os Mirai Botnet támadás

“Ha nem éri el kedvenc oldalait ne dühöngjön, ugyanis több kibertámadás miatt jelenleg az internet jó része sokak számára elérhetetlenné vált. A probléma eleinte főleg az USA keleti részét érinti, de mivel a weboldalak betöltéséhez szükséges eszközöket támadnak, így világszerte problémát jelent” – írta az index.hu 2016. 10. 21-én, amikor a Mirai botnet több százezer IOT-eszközt fertőzött meg és ennek köszönhetően több tucat nagyobb weboldal vált elérhetetlenné az USA-ban és Európában egyaránt. (Flachner & Klág, 2016) A robóhálózat (botnet) gyakorlatilag zombi eszközök 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. (Nemzeti Kibervédelmi Intézet, NKI, 2020)

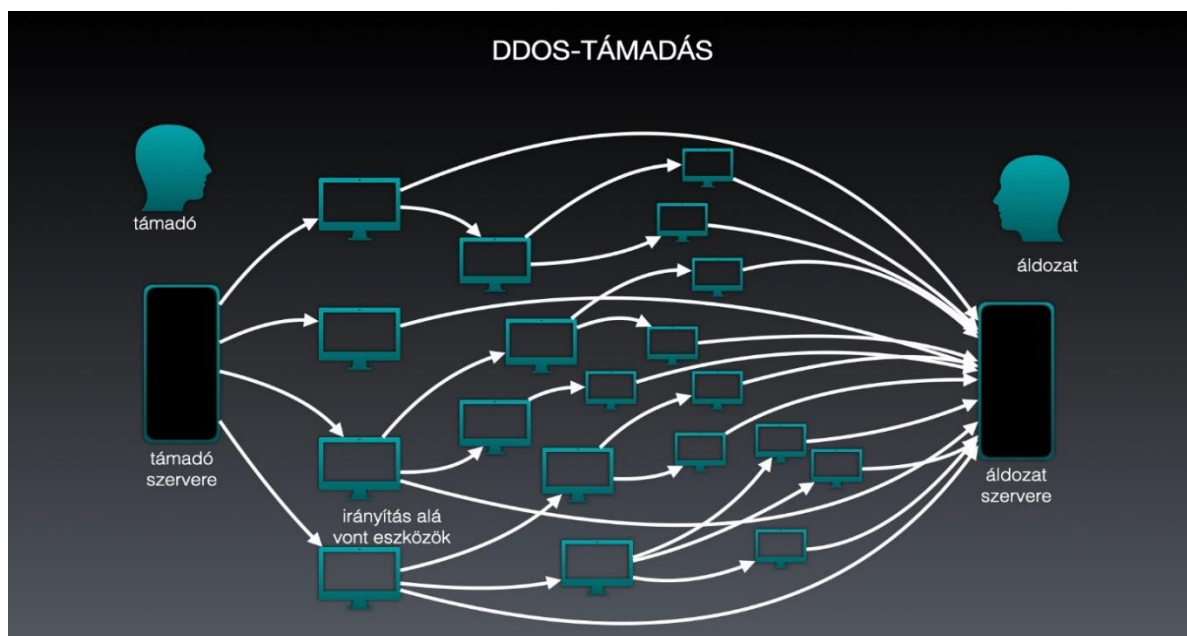
A Mirai botneteket a kiberbűnözők arra használják, hogy DDoS támadásokat indítsanak vele. A szolgáltatásmegtagadásos (DoS) vagy túlterheléses támadások lényege, hogy a támadók - kihasználva a hálózat gyengeségeit vagy az eszközök biztonsági réseit -, megtámadják az eszközöket vagy hálózatot úgy, hogy 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 elosztott szolgáltatásmegtagadásos (DDoS) támadásnak nevezzük. (Nemzeti Kibervédelmi Intézet, NKI, 2018)

A támadások lényege tehát az, hogy annyi kérést küldenek egy adott weboldalra, amit az oldal terhelhetősége már nem bír el, nem tud kiszolgálni. Ezáltal, ha új látogató érkezik az oldalra, akkor szolgáltatás-megtagadással fog találkozni. Egyszerűbben megfogalmazva, a botnet támadásokkal a támadó – kihasználva a biztonsági réseket – minél több eszközt céloz meg és átveszi felettük az irányítást - zombi hálózatot hoz létre-, majd az irányításuk alá került, külső utasításra cselekvő gépek egyszerre megkezdik a támadást a választott célpont ellen.

Ez történhet egy gépről, vagy több gépről. A több tízezer, több százezer eszköz, bár önmagában csekély adatmennyiséggel dolgozik, összehangolt támadás esetén hatalmas adatmennyiséggel támadja a kiszemelt célpontot. A 2016-os botnet támadás következtében leállt a Spotify, a Twitter, a PayPal, a Reddit, az Amazon és az egyik legnagyobb streaming szolgáltató, a Netflix is.

A Mirai gyenge biztonsági védelemmel ellátott IOT-eszközöket (kamerákat és otthoni okos eszközöket) támadott meg és vett az irányítása alá, majd egy összetett DDoS támadáshoz használták fel azokat. Már önmagában egy 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 tovább fertőzik a többi hálózatba kapcsolt IOT-eszközt, ahogy történt ebben az esetben is.

Az IOT-eszközök alkalmazási körének és számának növekedésével a DDoS-támadások is megnövekedtek. (ResearchGate, 2017)



7. ábra: DDoS-támadás

Forrás: a szerző saját szerkesztése

A biztonsági résekkel rendelkező, illetve a nem megfelelő védelemmel ellátott eszközök pedig használhatóak egy DoS támadás során. *"Mirai will be seen in future as the first major botnet that used the growing army of the internet of things [IoT],"* azaz *"A Mirai a jövőben az első olyan nagy botnetként fog megjelenni, amely a dolgok internetének (IoT) növekvő seregét használta,"* - kommentálta Alan Woodward professzor, a Surrey Egyetem kiberbiztonsági szakértője, *"It demonstrated just how vulnerable many of the cheap, internet-connected devices were to hackers who wanted to co-opt them to conduct massive attacks."*, *Bebizonyította, hogy sok olcsó, internetre csatlakozó eszköz mennyire sebezhető a hackerekkel szemben, akik tömeges támadások végrehajtására akarták bevonni őket."* (BBC News, 2017)

A Mirai botnet 2016-os támadása óta a botnet több új variánsa jelent már meg. 2019-ben az Echobot, (Nemzeti Kibervédelmi Intézet, NKI, 2019) a 2020-2021-es években a Dark Nexus, (Nemzeti Kibervédelmi Intézet, NKI, 2020) a Kaiji (Nemzeti Kibervédelmi Intézet, NKI, 2020), a Mukashi, ami leginkább sérülékeny routereket támadott meg. (Nemzeti Kibervédelmi Intézet, NKI, 2020)

7.2.3. A Nest bébiőr és az alapértelmezett jelszavak

A magánélet védelméről szóló 2018. évi LIII. törvény is megfogalmazza, hogy az embereknek joguk van ahhoz, hogy magánéletüket, családi életüket, otthonaikat, kapcsolataikat tiszteletben tartsák. A privát szféra, a magánélet az emberek egyik legnagyobb értéke, éppen ezért ennek megsértése fokozott sérelmet jelent az érintettnek. Különösen akkor, ha a sérelem az otthonában történik, ráadásul egy gyermek épségét és egészségét veszélyezteti.

A gyermekek testi épségének védelme érdekében sok szülő szívesen használ bébiőrt, aminek az a feladata, hogy ellenőrizni lehessen a kisbabát, ha másik helyiségben van, illetve, hogy az eszköz azonnal jelezzen, ha baj van. Ha egy támadó megszerzi az irányítást felette, az nem csak amiatt gond, mert valaki behatolt a magánszférájába, hanem azért is, mert ez akár a baba életébe is kerülhet: mivel az eszköz nem jelez, a felhasználó nem értesül arról, ha a gyermekkel probléma van. Több olyan eset is előfordult, amikor valaki átvette az irányítást a bébiőr felett.

Az NBC News oldalán olvashattuk azt az esetet, amely arról szólt, hogy egy hacker feltörte otthonukban a Nest bébiőrt, 2018-ban pedig egy texasi szülőpár ébredt arra, hogy 4 hónapos gyermekük szobájában lévő Nest kamerából szokatlan hangokat hallottak. Azonnal felkapcsolták a hálósobában a villanyt, ám erre egy másik, az ő szobájukban lévő Nest kamera is bekapcsolt, és egy férfihang mondta nekik, hogy kapcsolják le a villanyt.

Amikor a pár ennek nem tett eleget, akkor a hang azzal fenyegetőzött, hogy a baba szobájában van és el fogja rabolni a gyermeket. Az apa azonnal felszaladt a gyerekszobába, ahol sértetlenül találta a babát. Rájöttek, hogy valaki feltörte a bébiőrt, ezért lekapcsolták a WiFi-t és hívták a rendőrséget. A család értesítette a gyártó céget is. A Nest szerint a vállalat már találkozott hasonló esetekkel, miszerint a Nest ügyfelei újra felhasználták azokat a jelszavakat, amiket korábban más webhelyen történt incidensek során tettek közzé. Egyben figyelmeztették az ügyfeleket, éljenek a kétfaktoros hitelesítés lehetőségével. (Fieldstadt, 2018)

A kétfaktoros hitelesítés lényege a biztonság növelése. A jelszó beírását követően a bejelentkezés megerősítésekként minden alkalommal érkezik a felhasználó számára vagy SMS-ben vagy e-mailben egy egyszer használatos kód, vagy a felhasználó telefonján futó kódgeneráló szoftver generál egy szintén egyszer használatos kódot. Ezek érvényességi ideje csak néhány másodpercig vagy percig tart. A funkció legfőbb előnye, hogy ha a támadó a jelszó feltöréséig el is jut, a kétfaktoros hitelesítés esetében szüksége lesz a bejelentkezést megerősítő kódra, és a kód korlátozott érvényességi idejének köszönhetően nem lesz értelme azok feltörésén dolgozni.

Ebben az esetben a babának nem esett bántódása, de a bébiőr alapvető feladatát - hogy biztonságban tudja a felhasználó a gyermekét, és jelezzen a bébiőr probléma esetén - nem töltötte be, éppen ezért - a magánszféra megsértésén kívül - a gyermek testi épsége is veszélybe került. A jelszavak ellopása a legegyszerűbb támadási módszer, a leggyorsabban célravezető, ezért a hackerek körében a legnépszerűbbek is. Több fajtája van, ilyen például a brute force támadás, ami leginkább rövid és egyszerűbb jelszavak esetén működik, 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 felhasználó nevekhez keresik hozzá a korábban párosított vagy már használt jelszavakat. (Nemzeti Kibervédelmi Intézet, NKI, 2018) A gyenge jelszavak alkalmazása igen gyakori az IOT-eszközök körében. Az IoT-eszközök alapértelmezett felhasználó nevekkkel és jelszavakkal rendelkeznek, amelyek könnyedén megtalálhatóak az interneten.

Az okos otthonokban a vezetékek nélküli hálózatok elengedhetetlen eleme lenne a titkosított csatorna, valamint az erős jelszavak, a kétfaktoros hitelesítés használata. Az eszközgyártók a kétfaktoros évek eleje óta alapbeállításokkal ruházzák fel az eszközöket, az alapértelmezett jelszavak pedig minden nehézség nélkül bárki számára fellelhetőek az interneten. (Varga P. J., 2017)

Sok felhasználó 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, és onnantól már csak egy lépcsőfok, hogy az irányításuk alá vont IOT-eszközöket egy komplex DDoS támadáshoz használják, vagy ezek által ransomware fertőzés áldozatává válhatnak.

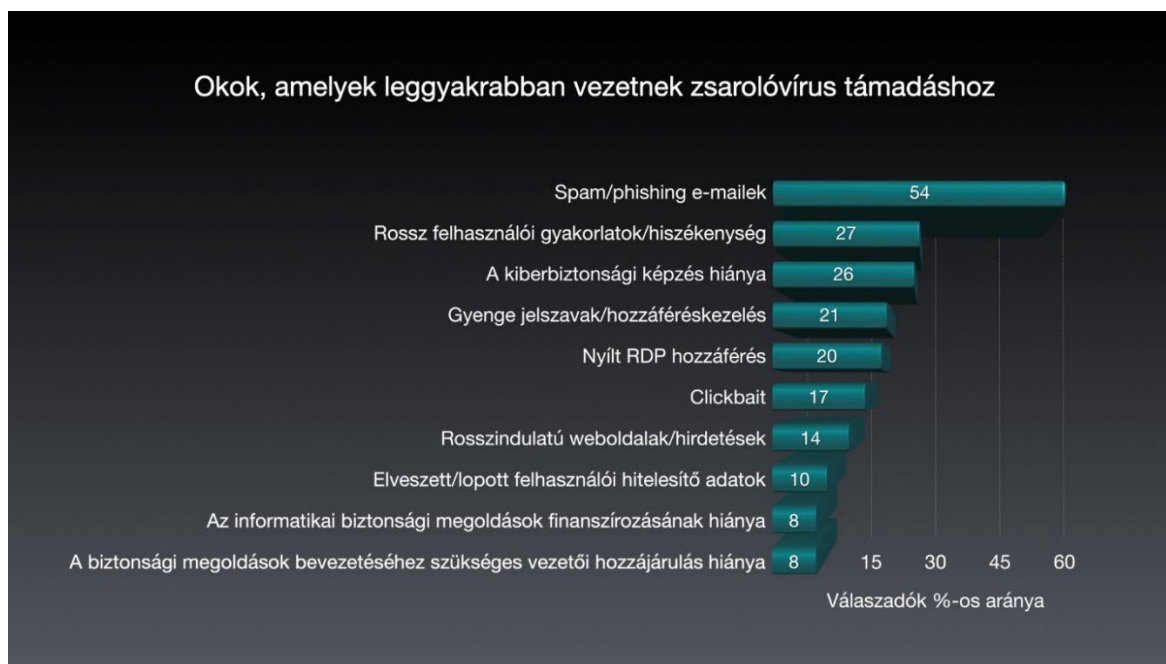
2. táblázat: Alapértelmezett jelszavak és leggyakrabban használt jelszavak

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 szerző saját szerkesztése (Nordpass, 2020) (Learnctv, 2020) (Woodham, 2020) (Buchholz, 2021) alapján

A gyenge jelszó egyébként a negyedik azon a listán, amely azokat az okokat összegzi, amelyek a leggyakrabban vezetnek zsarolóvírusos támadáshoz - a rossz felhasználói gyakorlatok, a kibbiztonsági képzés hiánya és a hozzáférés-kezelés mellett.

3. diagram: Zsarolóvírus támadás leggyakoribb okai



Forrás: a szerző saját szerkesztése (Statista, statista.com, 2022.) alapján

7.2.4. Lehallgatás

Az okos asszisztensek 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, hogy az asszisztens félrehallott egy parancsot - az elhangzottakat úgy értelmezte, hogy rögzítenie kell a beszélgetést, és azt el is kell küldenie. (Crist, 2018)

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 egy elektromágneses kisugárzása, megfelelő erősségű antenna segítségével a kisugárzás foghatóvá válik, így a támadó képes a küldött adatok lehallgatására. (Frész, Kálovics, & Puha, 2014) Mivel a szenzorok és átjárók közötti kommunikáció általában rövid hatótávolságú, így inkább a peremeszközök és a tárhely közötti, nagyobb hatótávolságú kapcsolat a kritikus.

A kommunikációs csatornán keresztül van lehetősége a támadónak az adatok lehallgatására úgy, hogy a bűnöző elfogja a két fél közötti forgalmat. Ezért is fontos titkosított kapcsolatot használni.

Néhány évvel ezelőtt az amerikai Szövetségi Nyomozó Iroda (FBI) hatósági közleményt adott ki az okos televíziókkal kapcsolatban. Szerintük az egyik gond az, 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 nem csak képes, de az adatvédelmi tájékoztatóban foglaltak szerint meg is teszi, hogy rögzíti 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. (Balogh, 2019)

7.2.5. További támadási módok

A fenti példákon kívül még számos okos eszköz használható „kémkedésre”. Ilyen például az okos porszívó, ami lézeres letapogatóval rendelkezik, rögzíti a lakás alaprajzát a megfelelő tisztítás céljából, vagy akár egy egyszerű okos termosztát, ami a hőmérsékletet szabályozza. Ezek feltörésével megszerezhetik az irányítást a vagyonvédelmi berendezések felett, és olyan információkat deríthetnek ki a támadók a fogyasztóról, ami akár egy precíz profilozást is lehetővé tesz. A social engineer egy olyan támadás, amely során a támadók az emberi természetet használják ki.

A támadók első körben információt gyűjtenek célpontjukról, ez történhet félrevezetéssel, (Deák, 2019) a bűnöző egy olyan személynek adja ki magát, akitől a célpont nem tagadja meg a válaszadást. Rendőrnek, rovarirtónak vagy mérőóra leolvasó személynek álcázza magát. Így feltérképezi az okos eszközöket, majd pedig, miután megtudta, milyen okos eszközeink vannak, feltöri azokat. Előfordul olyan is, hogy a bűnöző egy internetszolgáltató munkatársának adja ki magát, és egy adathordozó eszköz segítségével rosszindulatú szoftvert helyez el valamelyik kommunikációs eszközön.

A malware vagy rosszindulatú szoftver egy 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, amik számukra értéket képviselnek. (Erdősi & Solymos, 2017) Egy malware-fertőzés következtében az otthon támadhatóvá válik, a célszemély akár adatlopás, akár zsarolóvírus áldozatává válhat.

A social engineer egy fizikai támadás előkészítése is lehet. Amennyiben sikerül behatolni az okos eszközeinkbe – akár a fent említett malware segítségével –, akkor ezeken keresztül a támadó átveheti az irányítást, például azért, hogy kikapcsolja a riasztót, kinyissa az intelligens zárat, de betekinthet a lakásba a kamerán keresztül, vagy megszüntetheti a kameraképeket. Noha az intelligens zárok és biztonsági kamerák használata gyakran vonzó lehetőség, ha ezek nem megfelelően vannak beállítva, nagyobb bajt okozhatnak, mint amennyi hasznot hajtanak.

Ezek biztonsági réseit kihasználva ugyanis a behatolók a valóságban is bejuthatnak otthonunkba. A BLE technológiát (Bluetooth Low Energy) alapvetően nem zárrendszerekhez találták ki, mégis számos gyártó alkalmazza okos zároknál. A zár ebben az esetben felismer egy eszközt (telefon, tablet, adott esetben okos óra), és lehetővé teszi, hogy azzal kinyissa a zárat. Egy biztonsági cég Tesla autókra tesztelte ezt a fajta működést, és egy jelfogó segítségével lemásolta a zár és az okostelefon közötti jelet, majd gond nélkül kinyitotta az autót a zárral. (Rodríguez, 2022) 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 rá az áldozatot a szellőztetésre.

A nyitott ablakon a támadó könnyedén bejut az épületbe, ezzel megalapozva egy személy vagy vagyon elleni bűncselekmény elkövetését.⁵ Fontos szerepük van ebben az esetben a biztonsági kameráknak, amelyek célja a személy- és vagyonvédelem megerősítése lenne, ugyanakkor, ha egy támadó kihasználja a biztonsági réseket és hozzáfér a kameraképekhez, akkor a betekintés során megállapíthatja, hogy a terület mennyire őrzött, érdemes-e az épületbe behatolni, ha igen, akkor hány fő szükséges, hol lehet a legkönnyebben bejutni és milyen értékeket tudnak eltulajdonítani, tehát egy komplett betörési művelet 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 beavatkozásokat hamis adatok alapján hozzák meg. Tekintettel arra, hogy az IOT-eszközök rendkívül összetettek, nagy valószínűséggel a legtöbb eszköz biztonsági problémákkal rendelkezik. (Bocsok, Boldizs, Loós, & Major, 2015)

Az az eszköz, ami kifelé kommunikál, az befelé is nyitottá válik, ezáltal több ponton is számos lehetőség nyílik a bűnözőknek rákapcsolódni a hálózatra.

⁵ NKI Kibertámadás! Podcast: Okos az otthon, de biztonságos? <https://nki.gov.hu/en/podcast/10.15>.

Ha egy eszköz elérhető az internet felől, akkor az eszközök sérülékenységei kihasználhatóvá válnak, ezzel biztonsági rést teremtve a külső támadásokhoz. (Christián, Major, & Szabó, 2019) Az eszközök közötti, illetve az eszköz és az átjátszó, vagy az eszköz és a felhő közötti kommunikációs vonalak mindegyike fenyegetettségnek van kitéve. Az összekapcsolás és a különböző technológiák vegyítése során szintén biztonsági problémák merülhetnek fel. A fejlesztők biztonságtudatosság hiányában nincsenek tisztában az IOT-eszközökben rejlő sebezhetőségi lehetőségekkel. A SANS nevű információbiztonsággal foglalkozó szervezet és a Nemzeti Kibervédelmi Intézet közös kiadványfolyamának megfogalmazása szerint a probléma az, hogy

- a hackerek a felhasználó saját eszközét mások ellen tudják fordítani,
- a gyártók széles körű információkat gyűjtenek a felhasználókról,
- és ha az eszközök megfertőződnek, akkor akár ki is zárhatják a felhasználót magából az eszközből.

További probléma, hogy a legtöbb gyártónak nincs kiberbiztonsági tapasztalata, és mivel a biztonsági tényezők csak plusz költséget generálnának, ezért a forgalomban lévő eszközöket nem, vagy csak igen csekély védelemmel látják el. (Lee, 2018) Az IOT-eszközök piacán számos érdekelt fél van. Más a gyártó, más a kivitelező, más a forgalmazó érdeke. Az eszközök millió számra kerülnek piacra, és a tömeges gyártás során az idő hiánya miatt nem feltétlenül a biztonsági rések vizsgálata a legfontosabb tényező.

8. A TÁMADÓK MOTIVÁCIÓI ÉS TÍPUSAI

Bár sokan úgy vélekednek, hogy ők nem potenciális áldozatok a kibertérben, hiszen az ő adataik nem annyira érdekesek, hogy a hackerek azokkal foglalkozzanak, mégis tény, hogy az IOT-eszközöket használók egyre inkább a hackerek áldozataivá válnak. A Kaspersky vírusírtó és számítógép-biztonsági szolgáltató szerint az IOT-eszközök támadásának száma a 2021-es év első felében több, mint kétszeresére emelkedett az előző félévhez képest: 639 millióhoz képest 1,5 milliárd észlelt támadás volt. (Seals, 2021)

Az információszerzés irányulhat személyes adatok, bizalmas adatok, üzleti titkok megszerzésére, a megszerzett információk felhasználhatók saját célra, egy következő, nagyobb támadáshoz, illetve továbbértékesítés vagy nyilvánosságra hozás céljából is. Motiváció lehet továbbá egy informatikai vagy biztonsági rendszer gyenge pontjainak felfedése. Az információ ebben az esetben lehet rendszerszintű, mint például egy vállalat vagy egy okos otthon működése, de lehet személyre szóló is, ami alkalmas lehet egy social engineer vagy fizikai támadás előkészítésére is.

A hátráltatás is egy 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.

Motivációs cél a befolyásolás is, ebben az esetben az emberek bizonytalanságát vagy problémáját próbálják felhasználni hatásgyakorlással, megfélemlítéssel, zsarolással. Így a kiszemelt áldozat nem csak áldozattá válik, hanem adott esetben a támadó eszközévé is egy következő támadás elkövetéséhez.

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 kihívás, tudásvágy is egy motivációs cél, hiszen a technológia fejlődésével a hackerek támadási technikáját is fejleszteni kell.

Szükséges kipróbálni a legújabb módszereket, mert egy későbbi támadásra úgy lehet hatékonyan felkészülni, ha minél több tudás van a hacker birtokában. A fő motivációk között pedig az egyik legjelentősebb az anyagi haszonszerzés, ami többféleképpen is elérhető: zsarolással, amikor a támadó az eltulajdonított értékekért váltságdíjat követel, vagy értékesítéssel, amikor az illegálisan eltulajdonított információkat továbbértékesíti a dark weben. Illetve teljesen közvetlen módon is anyagi haszonra tehet szert, például személyes adatok, bankkártya adatok eltulajdonításával. Ebben az esetben nincsen szükség zsarolásra és megfélemlítésre, nincsen szükség értékesítésre, egyszerűen a támadás mások banki adatainak megszerzésére irányul.

A támadók lehetnek hackerek, hacktivisták, ipari kémek, kiberterroristák, belső vagy külső alkalmazottak és szakértők, és számítógépes bűnözők. A hackerek olyan számítástechnikai szakemberek, akinek az informatikai ismeretei az átlaghoz képest magasabbak és széleskörűbbek, az internet használatával képesek védett vagy belső információkhoz hozzájutni számítógépeken és más kommunikációs eszközökön keresztül.

Korábban mindössze két típust különítettünk el, az úgynevezett fehérkalapos (white hat) és feketekalapos (black hat) támadókat. A fehérkalapos hackerek az etikus hackerek, akik bizonyos információs rendszerek gyengeségeit és biztonsági réseit tárják fel. Mindezt úgy, hogy programokat, weboldalakat, rendszereket törnek fel annak érdekében, hogy a hibákat javítani tudják és a feketekalapos bűnözők betörési kísérleteit megelőzzék. Ők alapvetően biztonsági szakemberek, és az üzemeltetőtől minden esetben írásos megbízással rendelkeznek. A támadás minden egyes lépését és jellemzőjét dokumentálják, és minden esetben tiszteletben tartják a megbízó érdekeit. A fekete kalapos hackerek azok, akik visszaélnek a tudásukkal, jogosulatlanul szereznek meg információkat vagy törnek be rendszerekbe, céljukat minden esetben önös érdek, valamilyen haszonszerzés, rosszindulat vezérli.

Kevésbé ismert, de létező szereplő a szürke kalapos hacker (gray hat), a kékkalapos hacker (blue hat) és a script kiddies. A gray hat hacker a white hat hacker és black hat hacker közötti átmenet, annyiban különbözik a fehérkalapostól, hogy nincsen megbízása, nem legálisan végzi ezt a tevékenységet, de általában a megtalált biztonsági réseket nem használja saját célokra, hanem értesíti a rendszer üzemeltetőit. A blue hat hackerek feladata a különböző rendszerek tesztelése még azok megjelenése előtt. A script kiddies-ek pedig azok, akik kizárólag mások eszközeivel hackelnek, gyakran nem is ismerik az általuk használt eszközöket és nem mérik fel azt, hogy mekkora károkat tudnak okozni.



2. kép: Hacker

forrás: (itechwares.com, 2022)

A hacktivisták pedig olyan aktivisták, akik számítógépes tudásukat használják fel nézeteik és állásfoglalásaik terjesztésére. Céljuk lehet a szólásszabadság vagy politikai, vallási ideológiák hirdetése, valamilyen politikai állásfoglalás. Általában internetes oldalakat törnek fel, illegálisan adatokat szereznek róluk, vagy átalakítják, módosítják azokat, adott esetben működésüket korlátozzák vagy ellehetetlenítik.

Az ipari kémek konkurens cégek alkalmazottai, vagy olyan bűnözők, akik az illegálisan megszerzett ipari, vállalati adatokat tovább értékesítik a piacon vagy felhasználják saját fejlesztéseik során. Minden esetben figyelniük kell arra, hogy ne derüljön fény az elkövetett támadásra, mert ezzel a megszerzett adat értéktelenné válhat. Eszközük lehet egyébként a kémprogramok elhelyezése is, melyek a felhasználó tudtán kívül működnek és gyűjtenek adatokat a támadó részére.

A kiberterroristák terrrorszervezetek, akik vagy toborzás, támogatás céljából gyűjtenek adatokat, vagy kihasználva a sérülékenységeket, terrorakciókat hajtanak végre akár egyes országos kritikus infrastruktúrájával szemben. Céljuk valamilyen politikai, vallási meggyőződésük miatt a félelemkeltés és káosz okozása.

A számítógépes bűnözők magas szintű informatikai ismeretekkel rendelkeznek, elsődleges céljuk a pénzszerzés. Tevékenységük nem merül ki a támadásokban, hanem árulják a saját maguk által fejlesztett kódokat, valamint az illegálisan megszerzett adatokat. A belső – vagy adott esetben külső – alkalmazottak, szakértők a belső hálózaton való hozzáférési jogaikat használják

fel és ezzel élnek vissza. Értékes adatokat tulajdonítanak el, amelyekkel visszaéléseket követhetnek el, zsarolásra használhatják őket. Ebben a típusban szerepet játszhat a sértettség, irigység, bosszúvágy is. (Nemzeti Kibervédelmi Intézet, Az információbiztonság lélektana, 2019) (Sági, 2018)

9. A KOCKÁZATOK CSÖKKENTÉSE, LEHETSÉGES VÉDELMI MEGOLDÁSOK ÉS JAVASLATOK

Az IOT-eszközök elleni támadások igen komplexek, ezért a támadókkal szembeni védekezést is több oldalról szükséges megközelíteni. Az egyik legfontosabb intézkedésnek véleményem szerint egy egységes, nemzetközi szinten elfogadott törvényi szabályozás kialakításának kell lenni, mind a biztonsági intézkedéseket, mind a büntetőjogi felelősségeket és eljárásokat érintve. Az optimális védelem kialakítása a gyártó és a fogyasztó feladata is, ugyanakkor fontos meghatározni, hogy mi a gyártó, és mi a fogyasztó felelőssége. A kockázatok csökkentése érdekében a fogyasztóknak az alábbi intézkedéseket kellene megtenniük:

- vásárlás előtt ellenőrizze a sérülékenységgel és a gyártói támogatással kapcsolatos információkat, illetve maga a gyártó ellenőrzése is fontos feladat
- kerülje el a feltűnően olcsó, vagy ismeretlen gyártótól származó eszközök vásárlását
- tartsa naprakészen az eszközt, azaz rendszeresen frissítse azok szoftvereit, különös tekintettel a biztonsági frissítésekre
- kövesse a sérülékenységi információkat
- az eszközöket elkülönített VLAN hálózatokon kezelje
- folyamatosan készítsen biztonsági mentéseket
- amennyiben egy alkalmazást már nem használ, vagy az alkalmazás elavult, azokat távolítsa el
- az alkalmazások telepítése során figyelmesen olvassa el az adatkezelési tájékoztatót, és csak azoknak az engedélykéréseknek tegyen eleget, amelyek valóban szükségesek az eszköz megfelelő működéséhez
- minden esetben más, erős jelszót használjon, az alapértelmezett jelszavakat változtassa meg, éljen 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 alkalmazzon VPN-t

A gyártó részéről szintén csökkenthetőek 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, csere lehetőséget 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 kötelezően vonatkozó 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 minimum követelményeknek kell megfelelni egy okos eszköz 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. Például az adatvédelmi tájékoztató megismerése napjainkban a weboldalak látogatása-, illetve az alkalmazások letöltése során kötelező. A telepítés folytatása több esetben nem is lehetséges, ha a felhasználó nem görgeti végig az adatvédelmi tájékoztatót. Ebben az esetben véleményem szerint két út van: a felhasználó legörget, majd a tájékoztató tényleges megismerése nélkül elfogadja azt.

A másik, hogy a felhasználó ténylegesen végig olvassa a dokumentumot. Itt egyértelmű a felelősségi kör, hiszen az alkalmazás kötelezővé tette a tájékoztató megismerését, és innentől kezdve a felhasználó felelőssége, hogy elfogadás előtt ténylegesen milyen mértékben ismeri meg azt.

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 gondolom, 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 nem csak 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 átlag fogyasztó számára is érthető módon - a felhasználót, hogy neki milyen beállításokat és milyen módon szükséges elvégezni a minimális biztonsági követelményeknek való megfeleléshez. Ezen felül a fogyasztók biztonságtudatossága sem növekszik exponenciálisan a technikai eszközök fejlődésével, pedig az ember az egyik legfontosabb tényező ezekben az új kihívásokban.

Véleményem szerint a prevenciónak éppen olyan jelentősége van, mint a szankcionálásnak és büntetésnek, 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. (Ambrus, 2020)

Ugyanakkor véleményem szerint a kerettantervben meghatározott éves szintű 68 tanóra - míg például az ének zene 132 óra (Oktatási Hivatal, 2020) -igen alacsony. Az idei évben is még azt erősítették a felmérések, hogy az iskolákból hiányoznak az alapvető digitális eszközök, és a pedagógusok képzése, képzettségi szintjük is hátrányt jelent a megfelelő színvonalú oktatáshoz. Pedig maga a Nemzeti Kibervédelmi Intézet is megfogalmazza, hogy az egyik legfontosabb feladatuk a biztonságtudatosság növelése mind a fogyasztó, 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 kihívásokra. 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.

Következő legfontosabb intézkedésnek azt tartom, hogy az oktatásban, a jogalkotásban, jogértékesítésben és büntetőügyekben érintett szervek kössenek együttműködési megállapodásokat annak érdekében, hogy a biztonságot megteremtsék. A védelem megteremtése mindannyiunk érdeke nem csak a fizikai, de a kibertérben is. A biztonság megalkotásában ugyanakkor számos szervnek és szervezetnek részt kell venni, a feladatot nem delegálhatjuk sem egyetlen állami, sem egyetlen civil szervre, szervezetre, és sem az egyén, sem a szervezetek nem engedhetik meg maguknak, hogy áthárítsák a teendőket másra.

A komplementer rendszet célja a biztonság megteremtése úgy, hogy abban kiveszik a részüket és kollektíven együttműködnek mind az önkormányzatok, mind a magánbiztonsági vállalkozások, mind a civil önvédelmi szervezetek a rendvédelmi szervekkel és a rendvédelmi feladatokat ellátó szervekkel. (Dr. habil. Christián & dr. Rottler, 2019)⁶

A fokozott együttműködés a magánszektor és a hatóságok között mind a preventív feladatokat, mind pedig a büntetőügyeket képes elősegíteni. A magánbiztonságban tevékenykedő biztonságtechnikai, informatikai szakemberek nem csak az oktatási tevékenységben tudnak részt venni, de képesek feltárni azokat a biztonsági réseket és hiányosságokat, amelyek javításával és kiküszöbölésével a biztonsági kockázatok csökkenthetők. Ezek a magasan képzett szakemberek a tervezési szakaszban felmerülő hibáktól kezdve az üzemeltetési, működtetési és felhasználói tevékenység során keletkező kockázatokra is tudnak reagálni, támogatva ezzel a rendvédelmi szervek munkáját.

⁶ “A rendszet küldetésének teljesítése, a biztonság megteremtése társadalmi kooperáció és kollektív munka eredményeként teljesíthető, amelyben a rendvédelmi szervek, a rendvédelmi feladatokat ellátó szervek mellett fontos szerepet kapnak az önkormányzatok, a magánbiztonsági vállalkozások, a civil önvédelmi szervezetek is. Ezt nevezhetjük komplementer rendszeti rendszernek, amelyben az állami szervek tevékenységét piaci és civil szerveződések egészítik ki, támogatják, segítik”

10. A KÉRDŐÍV KIÉRTÉKELÉSE: AZ IOT-ESZKÖZÖK A MINDENNAPJAINKBAN

A primer kutatásom online kérdőív formában zajlott, a Google Form platformon keresztül.

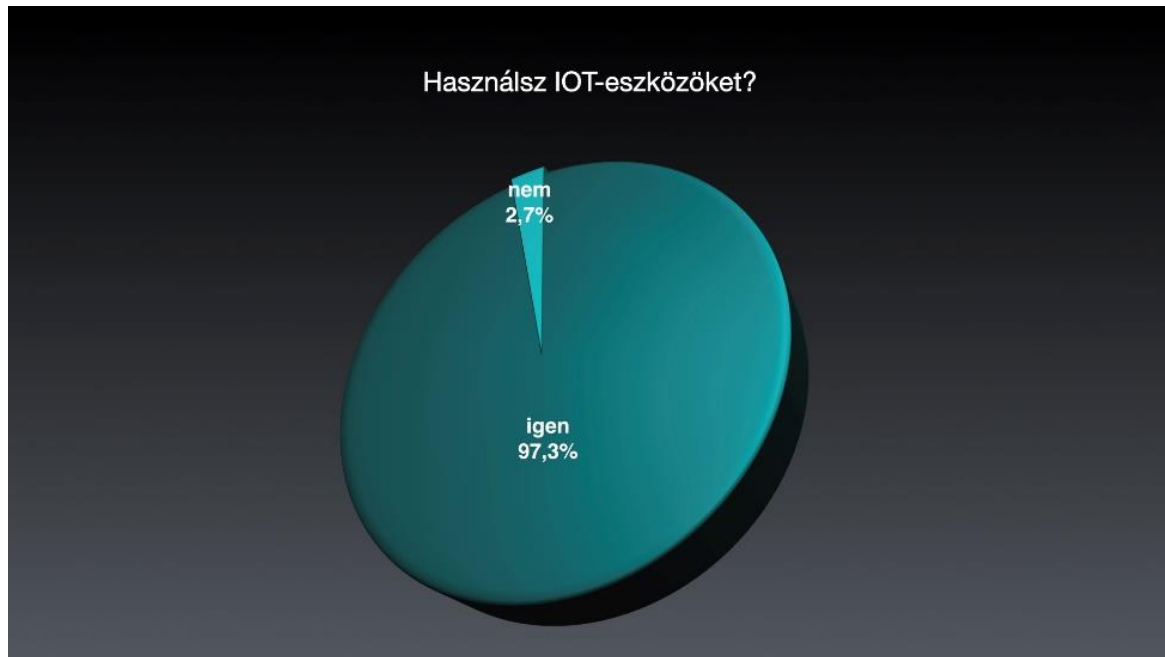
A vizsgálat célja az volt, hogy kiderüljön, hogy a hipotéziseim mennyire helytállóak, továbbá, hogy teljesebb képet kapjak a felhasználói szokásokról, arról, hogy mennyire figyelnek a fogyasztók a biztonsági kérdésekre. Valamint szerettem volna megtudni azt is, hogy a kitöltők közül hányan voltak már áldozatai kibertéri támadásnak, illetve, hogy a felhasználók tisztában vannak-e azzal, hogy egy esetleges támadás során hová fordulhatnak.

A kérdőívet 2022. 07. 18-án tettem közzé, és 2022. 09. 08-án zártam le. Ez idő alatt összesen 335 beküldés érkezett. A kitöltők 27,8 %-a nő, 71,9 %-a férfi, 0,3 %-a nembináris volt. A kérdőív kitöltése anonim volt, kortól, nemtől függetlenül bárki kitölthette, kitöltése nagyságrendileg 10 percet vett igénybe. Az összeállított kérdéssorozat összesen 26 kérdést tartalmazott, ebből 16 db-ra egy lehetséges válasz, míg 10 darabra több lehetséges válasz is megjelölhető volt. Természetesen lehetőség volt néhány kérdés esetében a válaszok szabad megfogalmazására is. A válaszadók nagy része (43,6 %) a 43-57 év közötti korcsoportba esett, míg a kitöltők összesen 46,9 %-a az Y, Z és Alfa generációból került ki. Iskolai végzettség tekintetében pedig jórészt a főiskolai/egyetemi, illetve a szakközépiskolai/gimnáziumi végzettséggel rendelkezők domináltak.

A kérdőívre adott válaszokból kiderült, a válaszadók 92,8 %-a hallott már az IOT-eszközökről, míg 7,2 %-a nem. Ez alapján tehát az IOT—eszközök igencsak ismertek.

A kitöltők 97,3 %-a azt állította, használ IOT-eszközöket (4. diagram) - ez tehát azt jelenti, hogy a válaszadók 4,5 %-a (15 fő) azt állította, hogy bár nem hallott az IOT-eszközökről, de használja azokat. Mindenesetre azt megállapíthatjuk, hogy az IOT-eszközök felhasználása igen gyakori a lakosság tekintetében.

4. diagram: IOT-eszközök alkalmazása

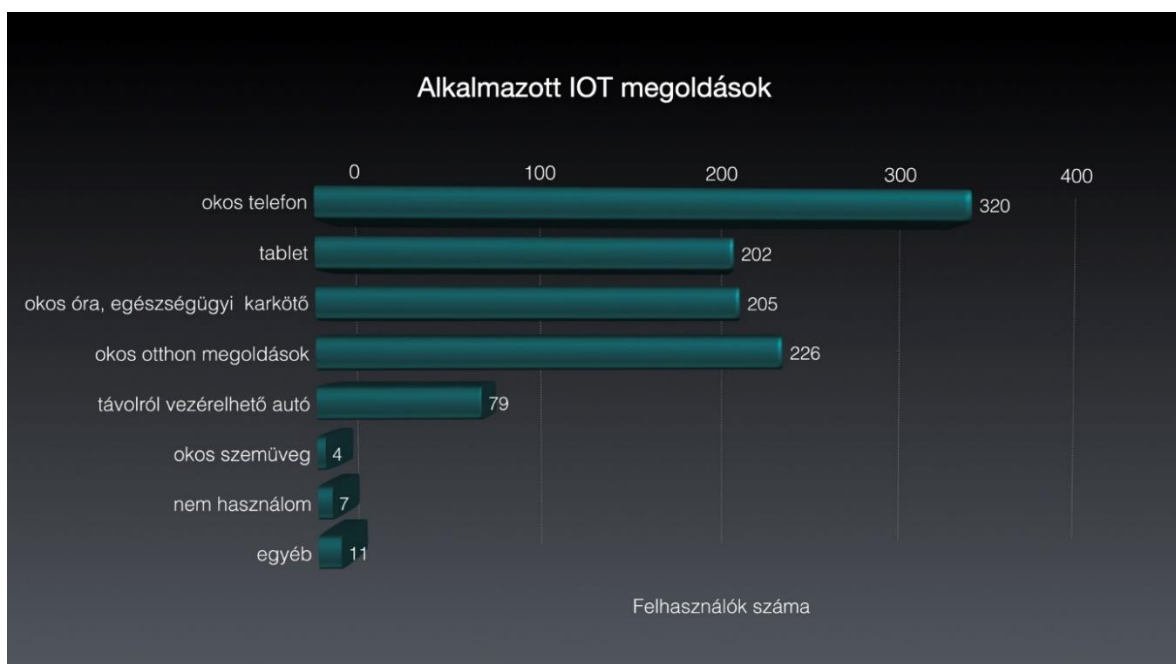


Forrás: a szerző saját szerkesztése

A válaszadók között a legnépszerűbb IOT-eszköz az okos telefon volt, a 335 válaszadó közül 320 fő használ okos telefont, emellett nagy számban használnak okos otthon megoldásokat (226 fő), tabletet (202 fő) és okos órát/egészségügyi karkötőt (205 fő) is. (5. diagram)

Az okos otthon megoldásokról egyébként a válaszadók 93,7 %-a hallott.

5. diagram: Alkalmazott IOT megoldások

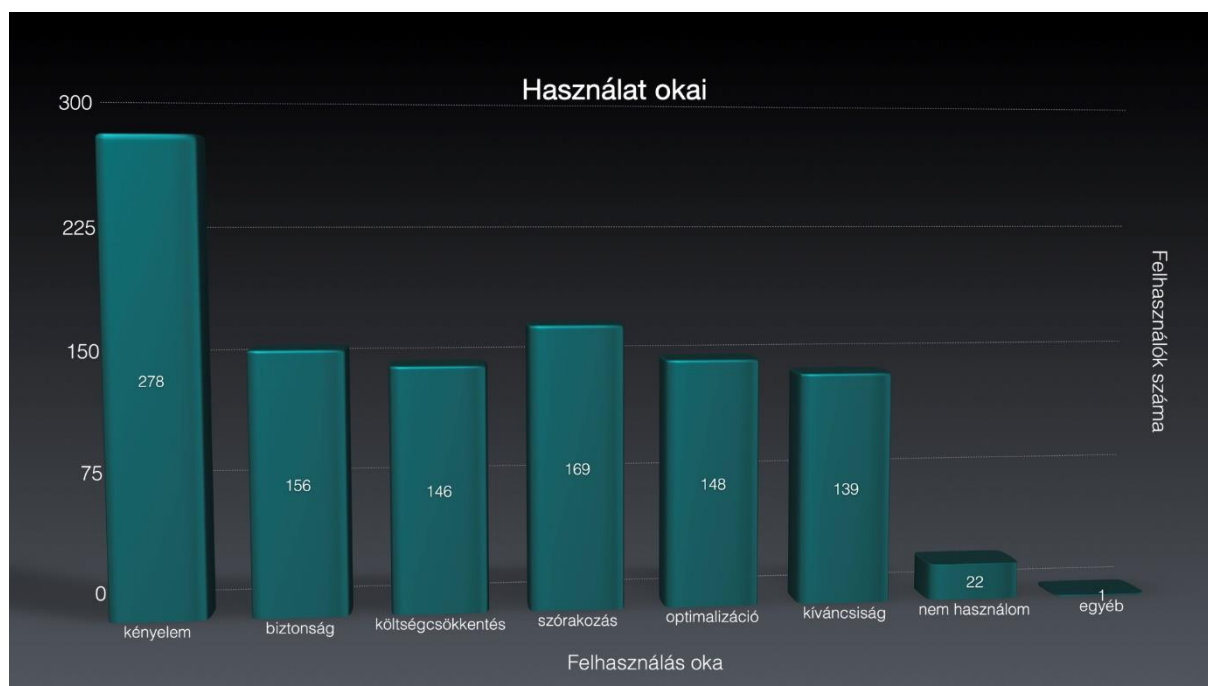


Forrás: a szerző saját szerkesztése

Az is kiderült, hogy a kitöltők szerint a legnépszerűbb okos otthon megoldás a szórakoztató elektronika (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 résztvevők közül a jövőben 215 fő biztonságtechnikát, 189 fő a hűtés-fűtést, 186 fő a világítástechnikát és 165 fő a robotporszívót szeretné alkalmazni legszívesebben otthonaikban. Mindössze a válaszadók 6 %-a az, aki egyik megoldást sem próbálná ki szívesen.

Szerettem volna azt is megtudni, hogy a válaszadók milyen okból használják ezeket az eszközöket, illetve mi alapján választanak, amikor okos otthon megoldásokat vásárolnak. Mint kiderült, a felhasználók legfontosabb motivációja a kényelem, ezt az opciót 278-an jelölték be, ami a válaszadók 83 %-át jelenti. A szórakozásra a válaszadók fele (50,4 %), a biztonságra a kitöltők 46,6 %-a tette le a voksát. (6. diagram)

6. diagram: IOT felhasználásnak okai

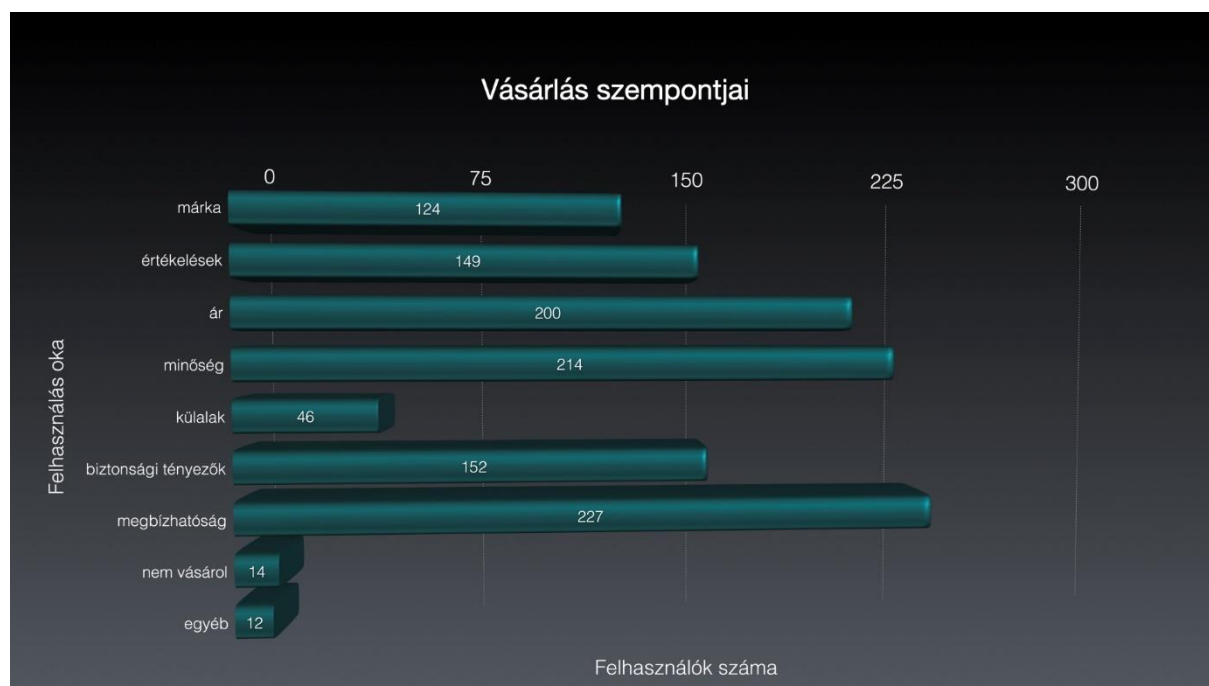


Forrás: a szerző saját szerkesztése

Ugyanakkor a következő kérdés rávilágít arra, hogy a válaszadók szerint a legfontosabb választási szempont a megbízhatóság (67,8 %), a második legfontosabb a minőség (63,9 %), a harmadik az ár (59,7 %).

Ezen két kérdés összefüggése a hipotézisem szempontjából igen lényeges, hiszen jól látható, (7. diagram) hogy a biztonság, mint vásárlási motiváció csak a 4. helyen végzett a fontossági sorrendben, a válaszadók kevesebb, mint felének (45,4 %) fontos vásárlási szempont, míg a fő motiváció az IOT-eszközök alkalmazásánál a kényelem.

7. diagram: Vásárlás szempontja



Forrás: a szerző saját szerkesztése

A kínai termékekről az embereknek leginkább a gyenge minőség és a termékhamisítás, utánzás jut eszébe. (Csizner, 2019) Nagyon fontos a biztonságtudatosságban az, hogy megbízható forrásból vásárolt eszközöket használjunk. Kínában számos nem ismert, kis gyártó cég tevékenykedik, és ezen eszközökhöz viszonylag alacsony áron hozzá lehet jutni a piacon. Ugyanakkor – éppen az alacsony ár és a tömeggyártás miatt – megkérdőjelezhető, hogy ezek az eszközök milyen biztonsági paraméterekkel rendelkeznek. Mégis a válaszadók mindössze 8,1 %-a tart a Kínában gyártott eszközöktől, míg a többség (48,1 %) választásában nem szempont az, hogy hol gyártották az eszközöket, 19,7 %-uk pedig szívesen is használja. (8. diagram)

A felmérésből már láthattuk, hogy a válaszadók vásárlási szempontjai közül az ár fontossága megelőzi a biztonsági tényezőket, sok esetben az ár dönt, viszont ami olcsó, azt általában vagy az adatainkkal, vagy a biztonságunk kockáztatásával fizetjük meg.

Példaképpen, a 2016-os Mirai botnet támadás során a Xiong Mai eszközei (amelyek kínai webáruházakban igencsak olcsón beszerezhetőek) nagy számban érintettek voltak. Ezen eszközök esetében nagyon bonyolult megváltoztatni az alapbeállításokat. Egy biztonsági szakértő pedig az iLink P2P szoftverében fedezett fel olyan sérülékenységeket, amelyek lehetővé teszik az eszközök könnyű támadhatóságát. Nincs lehetőség sem titkosításra, sem hitelesítésre. (GData, 2019)

8. diagram: Vélekedés a kínai gyártmányú eszközökről



Forrás: a szerző saját szerkesztése

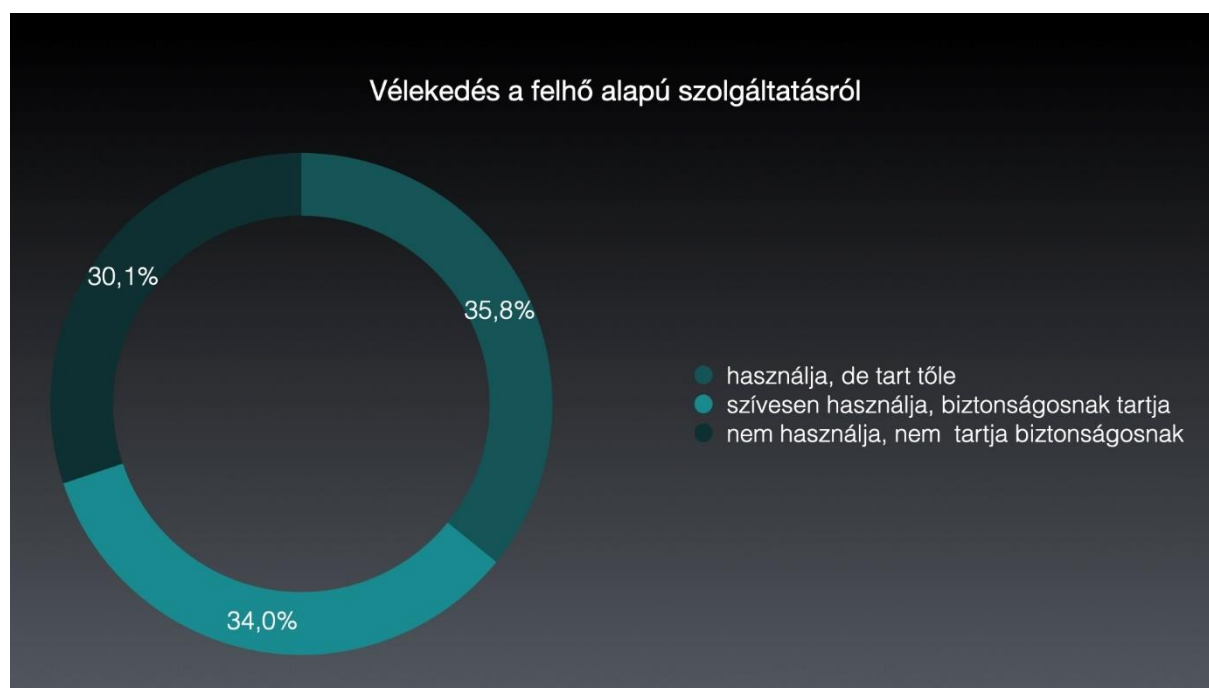
A következő három kérdés esetében a felhasználók felhasználásai szokásaira voltam kíváncsi. A válaszokból kiderült, hogy a fogyasztók közül 88,1 %-nak fontos az eszköz integrálhatósága, és rendszerintegrálás tekintetében a HomeAssistant, a Google Home és a Mi Home a legismertebbek. Ezek a platformok mobiltelefonos vagy webes applikációs felületek, amelyek belépési pontként szolgálhatnak egy támadás megindítására, vagy a támadók megszerezhetik a belépéshez szükséges adatokat, ezáltal átvehetik az irányítást az intelligens otthonok felett. A kommunikációs csatornák közül a WiFi, a BLE és a ZigBee a leggyakrabban használatos. A vezeték nélküli kommunikációs csatornák veszélyei közé sorolandó, hogy ha a kommunikáció nem titkosított csatornán zajlik, akkor könnyen támadhatóvá válik, illetve fennáll a jogosulatlan hozzáférés veszélye.

A következő kérdésben azt szerettem volna megismerni, hogy a válaszadók hogyan vélekednek a felhőszolgáltatásról?

A dolgozatban megismerkedtünk azokkal a veszélyekkel, amelyeket a felhőszolgáltatások rejtnek magukban. A válaszadók vélekedése nagyon megosztó a felhőszolgáltatással kapcsolatban, hiszen 34 %-uk szívesen használja, biztonságosnak és megbízhatónak tartja, 35,8 %-uk használja ugyan, de tart tőle, nem tartja biztonságosnak és megbízhatónak, és a válaszadók 30,1%-a pedig egyáltalán nem is használja, ők úgy vélik, hogy a felhőszolgáltatások nem biztonságosak és nem megbízhatóak, ők inkább a lokális szerveres megoldásokat preferálják. (9. diagram)

Az átlagfogyasztók körében a leginkább jellemző felhőszolgáltatási mód a nyilvános felhő. Aminek viszont igencsak nagy veszélyforrása az, hogy a felhasználóknak nincs rálátásuk az üzemeltetésre, a felhő szolgáltatások távoli szervereken futnak, a szolgáltatók tulajdonában vannak, így a felhasználók nem tudhatják biztosan, hogy a szolgáltató milyen szintű biztonsági intézkedéseket tesz meg az adataik védelme érdekében, ezáltal kiszolgáltatottá válnak.

9. diagram: Vélekedés a felhő alapú szolgáltatásokról

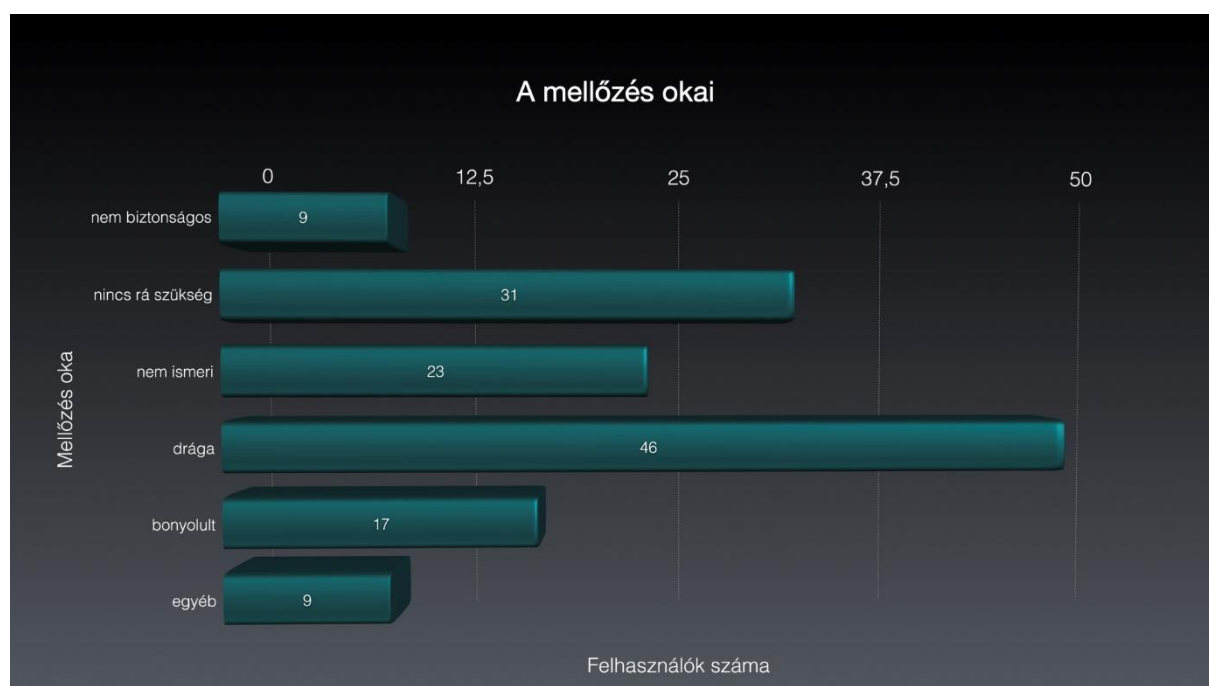


Forrás: a szerző saját szerkesztése

A következő kérdésem arra irányult, hogy aki nem használ okos otthon megoldást, az vajon miért nem? Szintén a hipotézisem alátámasztására adnak okot a válaszok, ugyanis a legkevesebb választ a nem tartom biztonságosnak lehetőség kapta – itt is több választ lehetett megjelölni, mégis ez a lehetőség igen csekély, mindösszesen 9 darab szavazatot kapott. (10. diagram)

Tehát akik nem használják az intelligens megoldásokat, azoknak a lehetséges válaszokból a biztonsági tényezők azok, amik legcsekélyebb mértékben szolgálnak elrettentő tényezőként. A nem használás okaként legtöbbször a drágának tartom opciót jelölték meg, ezt követően pedig azt, hogy nincs rá szükségük vagy pedig nem ismerik őket.

10. diagram: A mellőzés okai



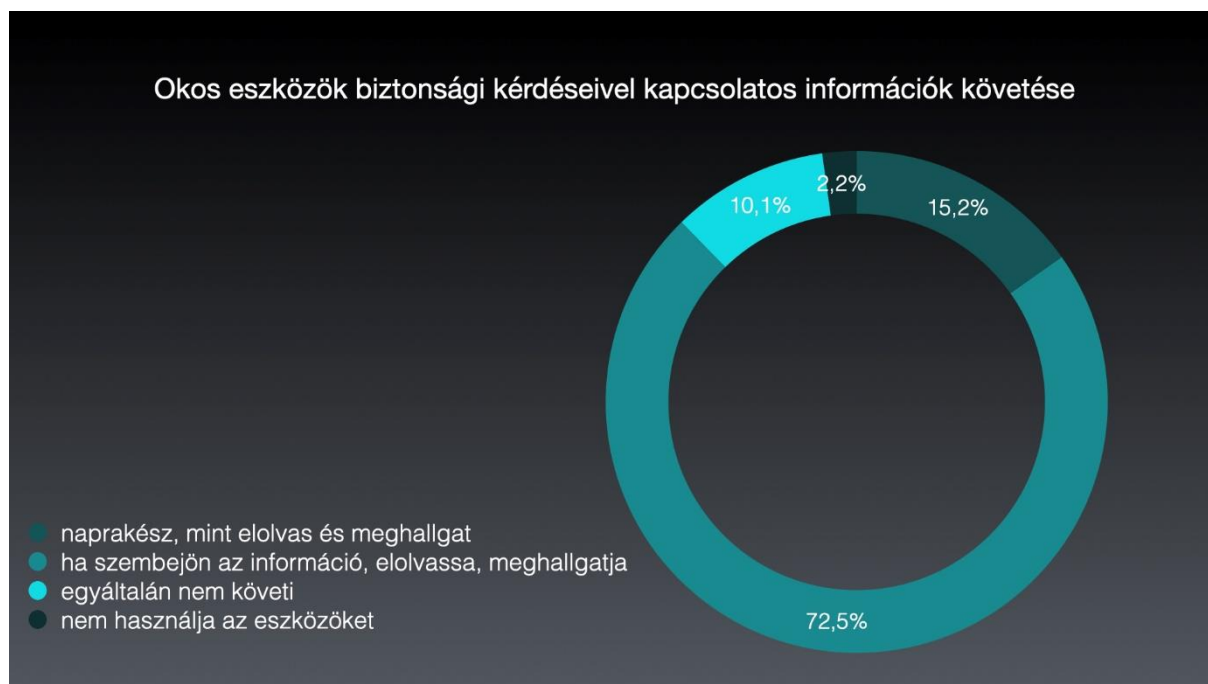
Forrás: a szerző saját szerkesztése

A további kérdésekkel az volt a célom, hogy megtudjam, a felhasználók mennyire biztonság-tudatosak: nyugodt szívvel használják az intelligens eszközöket, vagy minden lehetséges intézkedést megtesznek a védelmük érdekében?

A beérkezett válaszok összegzése nagyban erősítette a hipotézisemet.

A 18. kérdés így hangzott: Mennyire követed az okos eszközök biztonsági kérdéseivel kapcsolatos információkat? Mindösszesen a válaszadók 15,2 %-a az, aki elmondhatja magáról, hogy naprakész, és mindent elolvas és meghallgat a biztonsági kérdésekkel kapcsolatban. A válaszadók nagy többsége, 72,5 % csak abban az esetben foglalkozik ezekkel az információkkal, ha szembejönnek velük, illetve 10,1 % egyáltalán nem követi. (11. diagram)

11. diagram: Biztonsági kérdésekkel kapcsolatos információk követése

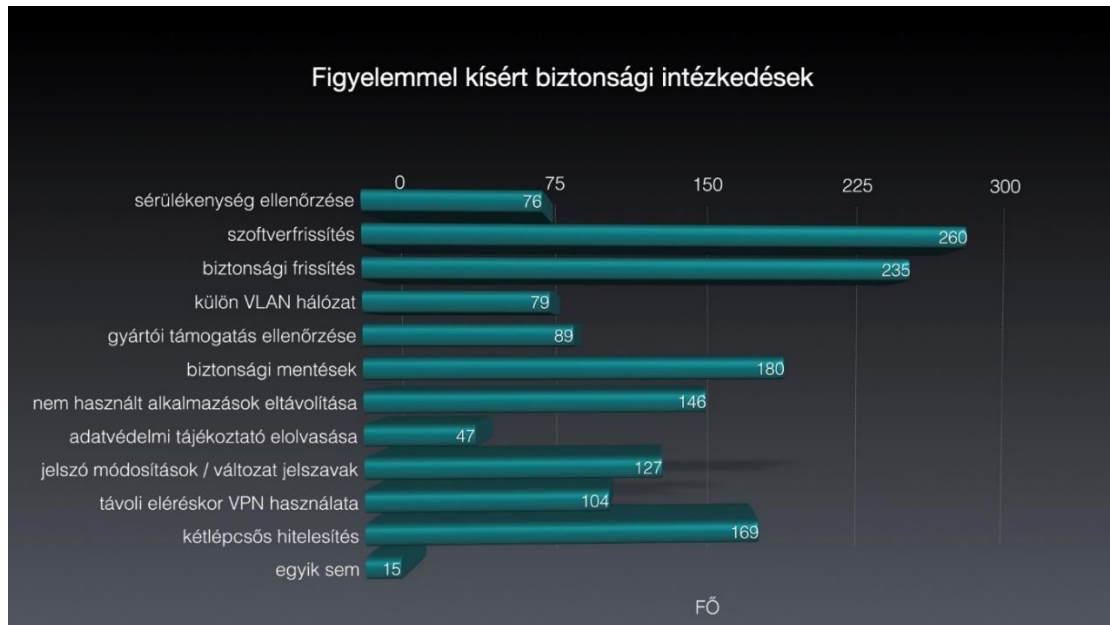


Forrás: a szerző saját szerkesztése

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. 15 fő egyébként azt az opciót jelölte meg, hogy egyik biztonsági intézkedésre sem figyel oda.

Bár első olvasatra akár úgy is tűnhet, hogy sokan odafigyelnek a biztonsági intézkedésekre, gyakorlatilag a felsorolt 11 biztonsági intézkedés közül négy intézkedést a kitöltők negyede végez el, két eset van, amit a kitöltők nagyjából egyharmad alkalmaz, mindössze kétfajta intézkedés van, amire a kitöltők nagyjából fele odafigyel, és két biztonsági intézkedés van, amit a kitöltők körülbelül hétharmada elvégez. Ezek igen csekély számok. (12. diagram)

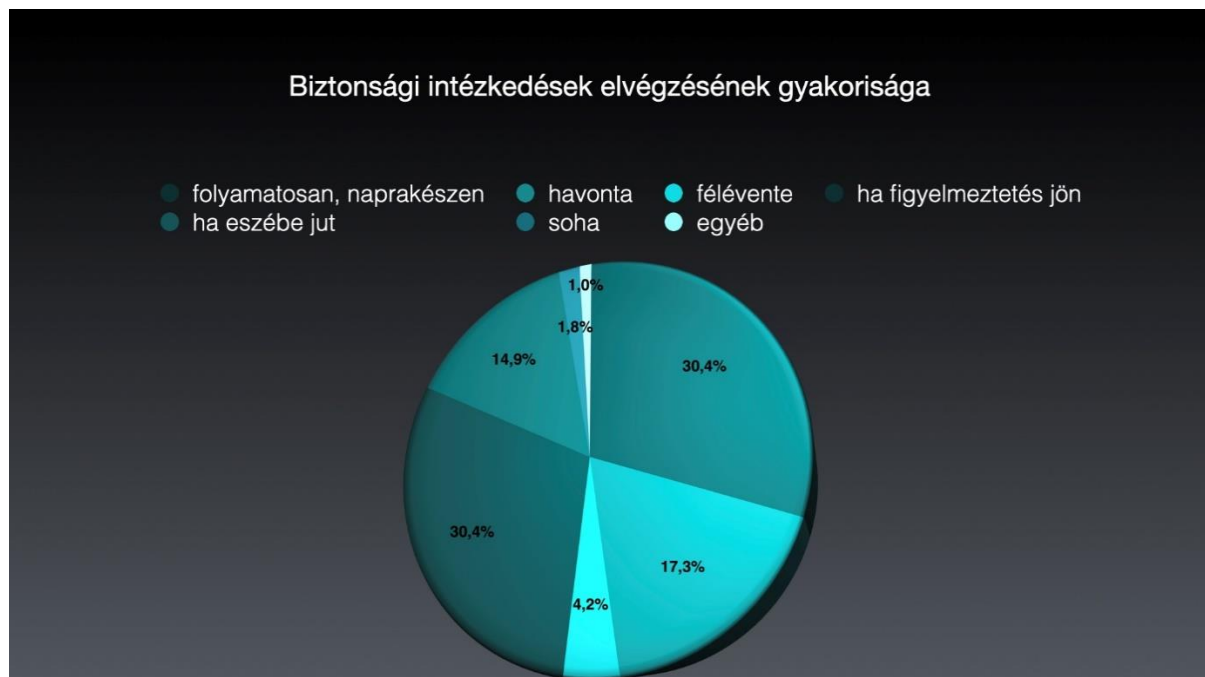
12. diagram: Figyelemmel kísért biztonsági intézkedések gyakorisága



Forrás: a szerző saját szerkesztése

A következő kérdésből megtudtuk, hogy a válaszadók mindössze 30,4%-a, tehát kevesebb, mint a harmada figyel folyamatosan arra, hogy biztonsági szempontból naprakészen tartsa eszközeit. (13. diagram) Viszont a kitöltők közel fele csak akkor végzi el a biztonsági intézkedéseket, ha figyelmeztetést kap a szükségességéről, ha éppen eszébe jut vagy soha nem is teszi meg.

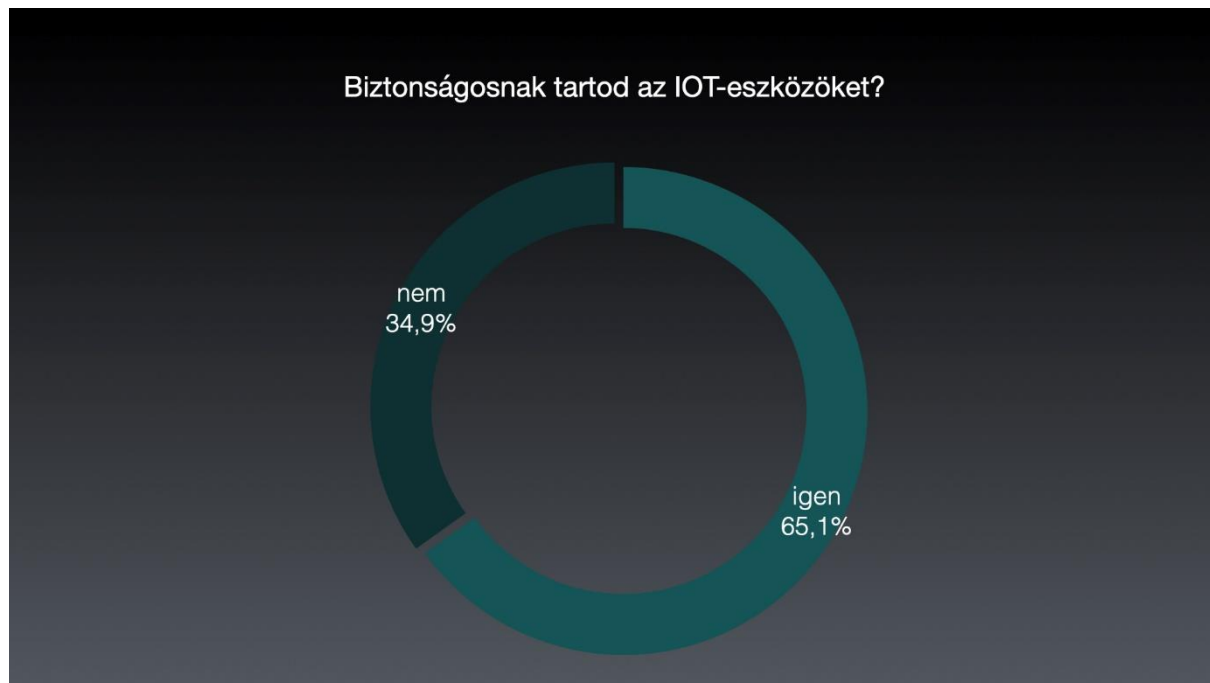
13. diagram: Biztonsági intézkedések elvégzésének gyakorisága



Forrás: a szerző saját szerkesztése

Megtudtuk azt is, hogy a válaszadók 65,1 % - 34,9 % arányban biztonságosnak ítélik az okos eszközöket. (14. diagram) Ez a válasz számomra azt tükrözi, hogy a felhasználók harmada nincs tisztában az IOT-eszközök sebezhetőségeivel.

14. diagram: Vélekedés az IOT-eszközök biztonságosságáról

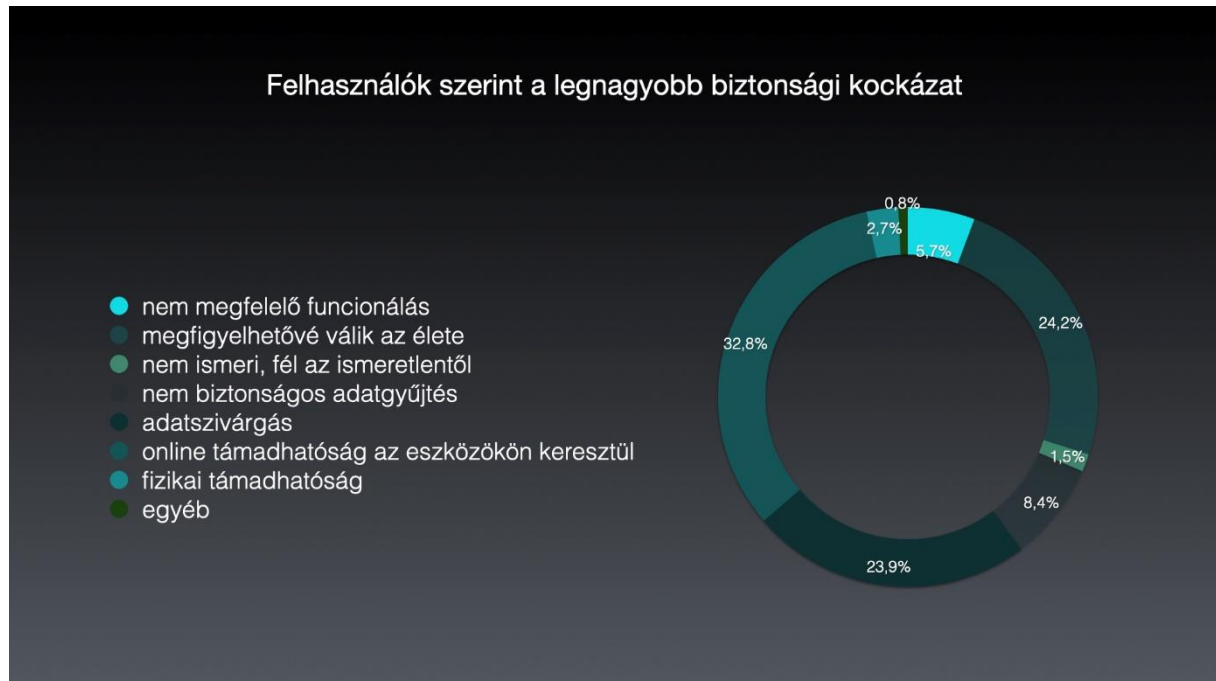


Forrás: a szerző saját szerkesztése

A kitöltők legnagyobb biztonsági kihívásnak (32,8 %) az online támadhatóságot látják az eszközeiken keresztül, a dobogó második fokán attól tartanak, hogy megfigyelhetővé válik az életük (24,2 %), a harmadik helyen pedig 23,9 %-kal az adatszivárgás áll. (15. diagram)

A válaszadók közül 111 fő jelölte meg legnagyobb biztonsági kockázatként az online támadhatóságot az eszközökön keresztül, mégis a 111 fő közül mindösszesen 16 fő tartja naprakésznek magát az okos eszközök biztonsági kérdéseivel kapcsolatban, a fennmaradó 95 fő vagy egyáltalán nem is követi az okos eszközök biztonsági kérdéseivel kapcsolatos információkat, vagy csak akkor követi, ha szembejön.

15. diagram: Legnagyobb biztonsági kockázatok

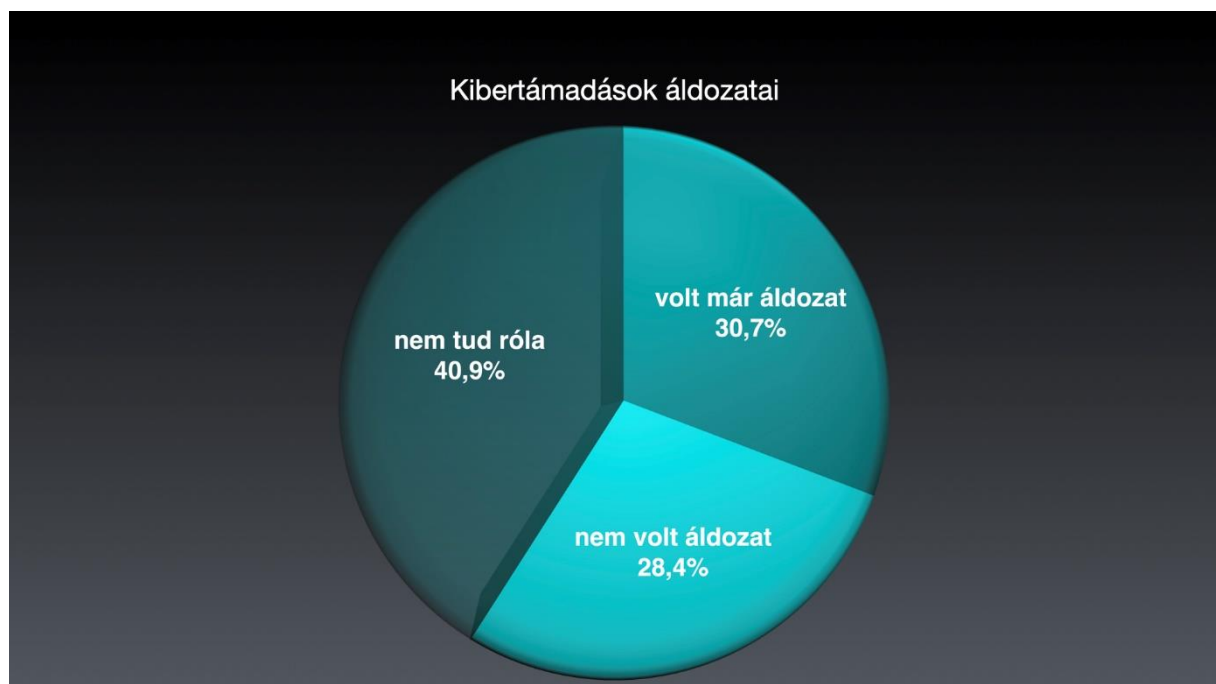


Forrás: a szerző saját szerkesztése

Szerettem volna megtudni, hogy hány válaszadó volt már áldozata valaha kibertámadásnak.

A válaszok szerint 28,4 % biztosan állítja, hogy nem volt, 30,7 % biztosan állítja, hogy volt, a többi válaszadó pedig nem tud róla. (16. diagram)

16. diagram: Kibertámadások áldozatai



Forrás: a szerző saját szerkesztése

A támadások típusai közül a leggyakoribb az adathalászat, a válaszadók 15,8 % -a esett már ennek áldozatul, zsarolóvírus áldozata a válaszadók 10,7 %-a volt már, míg rosszindulatú szoftver általi támadás 32 fő esetében történt. Érdekes információ, hogy a kitöltők közül 103 fő biztosan állítja, hogy volt már kibertámadás áldozata, ennek ellenére közülük 84 fő továbbra is csak akkor követi az okos eszközök biztonsági kérdéseivel kapcsolatos információkat, ha az szembejön, vagy egyáltalán nem is követik, és mindösszesen 17 fő az, aki naprakészen követi a biztonsági kérdéseket az okos eszközök kapcsán. 2 fő nem használja az IOT-eszközöket.

A biztonságtudatos felhasználás első lépcsőfokának azt tartom, ha a felhasználó tisztában van a rá leselkedő veszélyekkel, számol azzal az eshetőséggel, hogy ő is áldozattá válhat nem csak a fizikai, de a virtuális térben is. Emiatt kíváncsi voltam, hogy a kitöltők milyen arányban tartják magukat potenciális áldozatnak.

A válaszadók többsége, 57,9 % úgy vélekedik, hogy aki az online térben jelen van, az potenciális áldozat, 22,7 %-uk nem tartja magát potenciális áldozatnak azért, mert úgy gondolja, hogy mindent megtesz a biztonsága érdekében, 19,5 %-uk nem gondolja a saját adatait elég fontosnak ahhoz, hogy a bűnözők ezzel foglalkozzanak. (17. diagram)

17. diagram: : Potenciális áldozat vagy sem?



Forrás: a szerző saját szerkesztése

Ez a gondolkodás magyarázat lehet arra, hogy a válaszadók miért nem figyelnek az alkalmazások során az adatvédelmi tájékoztató elolvasására. Ugyanakkor dolgozatomban ismertettem, hogy a támadók célja nem feltétlenül a saját adataink megismerése, hanem az eszközök által egy nagyobb támadás indítása. Ennek fényében bár lehetséges, hogy a mi adataink nem válnak érdekessé az elkövető számára, de ha könnyen kihasználható biztonsági rések vannak az eszközeinken és könnyen támadhatóak vagyunk, akkor könnyedén egy nagyobb támadáshoz felhasznált fegyverré válhatunk.

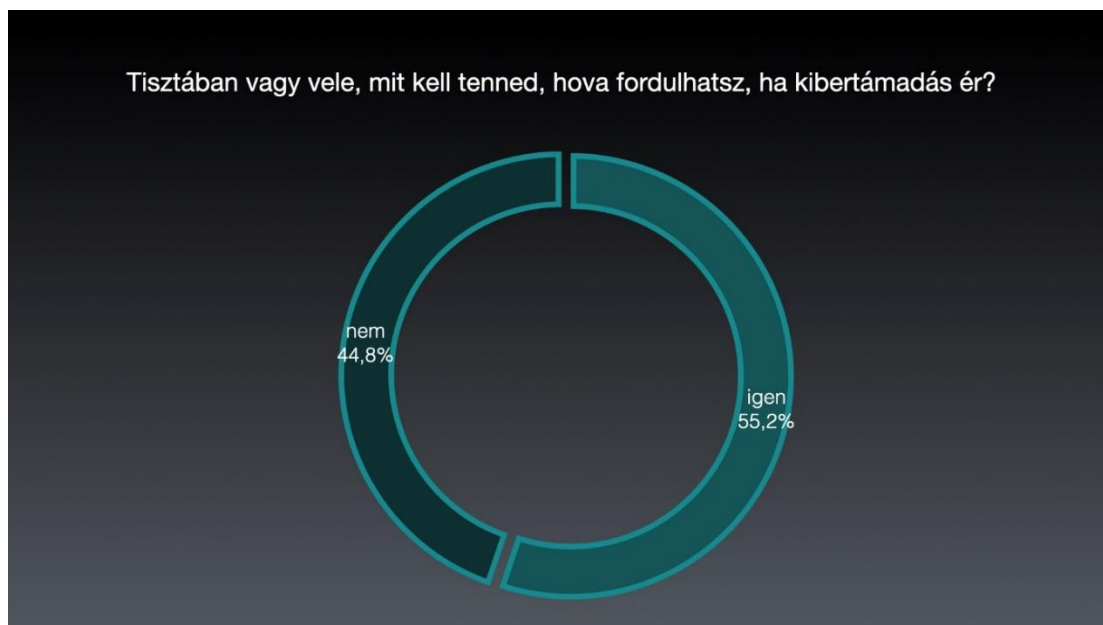
Érdekes tény az is, hogy azok közül, akik potenciális áldozatnak tartják magukat (194 fő), 28 fő követi naprakészen az okos eszközök biztonsági kérdéseivel kapcsolatos információkat és 101 fő az, ennek ellenére csak akkor végzi el a biztonságossághoz szükséges intézkedéseket, ha figyelmeztetést kap, ha éppen eszébe jut vagy egyáltalán nem is teszi meg. Továbbá közülük 89 fő az, akinek a vásárlási szempontok között egyáltalán megjelenik a biztonsági tényező, mint szempont is -több más egyéb mellett.

A válaszadók 22,7 %-a állítja, hogy nem tartja magát potenciális áldozatnak, mert mindent megtesz az adatai kellő védelméért. Ugyanakkor közülük, akik mindent megtesznek a biztonságuk érdekében (76 fő), kevesebb, mint fele (33 fő) az, aki folyamatosan figyel a biztonsági tevékenységek elvégzésére, és mindösszesen 18 fő az, aki naprakészen elolvas minden biztonsági kérdéssel kapcsolatos információt.

A 76 fő közül 58 fő csak abban az esetben tájékozódik, ha szembejön valamilyen információ, vagy egyáltalán nem. Számomra ez azt a tényt erősíti, hogy a felhasználók nincsenek tisztában azzal, hogy milyen biztonsági intézkedéseket kellene tenniük a védelmük érdekében, és ők ennek ellenére mégis azt gondolják, hogy mindent megtettek.

Az utolsó kérdés arra irányult, hogy a kitöltők milyen arányban tudják azt, hogy egy esetleges támadás során hova fordulhatnak?

18. diagram: Tisztában vagy vele, hova fordulhatsz, ha kibertámadás ér?



Forrás: a szerző saját szerkesztése

A válaszadók 44,8% nincs tisztában azzal, hogy hol kérhetnek segítséget. (18. diagram) Ez a kérdés számomra azért is volt fontos, mert a témaválasztásom oka az, hogy úgy gondolom, hogy a fogyasztók tájékoztatása és az IOT-eszközök biztonság tudatos használatával kapcsolatos tudása hiányos, pedig az első és legfontosabb lépés az lenne, hogy ha megtörténik a baj, akkor legalább tisztában legyenek vele, hogy honnan kérhetnek segítséget. A fogyasztók tájékozottsága tehát igencsak megkérdőjelezhető, ha sokan még azzal sincsenek tisztában, hogy mit kell tenniük, hova fordulhatnak egy esetleges támadás során.

ÖSSZEFOGLALÁS

A dolgozatban megismerkedtünk azzal, hogy milyen szerepet töltenek be mindennapi életünkben az IOT-eszközök. Megismertük ezen eszközök működését, előnyeit és veszélyeit, a támadhatósági réseket, illetve a támadók típusait és motivációit is.

Megtudtuk, hogy életünk számos területének szerves része az intelligens eszközök használata, ugyanakkor a kérdőív kiértékelése során megerősítést nyert az is, hogy 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 képeznék 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 és a támadási felületek egyre szélesebb körben és rohamos tempóban változnak és növekednek, és a virtuális térben keletkező, mérhetetlen adathalmaz értékéből fakadó kockázatok miatt elengedhetetlen, hogy ezzel egyidejűleg exponenciális növekedjen ezek biztonság tudatos használata és a biztonságos adatgenerálás is az egyén szintjén, döntéshozói és törvényhozói szinteken egyaránt.

Hipotézis 1: az IOT-eszközök működésükből fakadóan veszélyesek a felhasználóra nézve, viszont sok felhasználó nincs tisztában az IOT-eszközök veszélyeivel

Hipotézisemet a szekunder és a primer kutatásom is megerősíti. Mivel az IOT-eszközök összetett működésűek, számos támadási felületet rejtnek magukban, mind a mobilalkalmazások, mind a használt webes felületek, mind a kommunikációs csatorna, de a felhőszolgáltatás is számos lehetőséget biztosít a támadók részére.

A kérdőív válaszadóinak 65,1 %-a biztonságosnak tartja az IOT-eszközöket, illetve kiderült az is, hogy a fogyasztók nem feltétlenül és nem minden esetben tesznek meg mindent a védelmük érdekében. És bár sokan potenciális áldozatnak tartják magukat a kibertérben, mégis nagyon kevés felhasználó az, aki naprakészen biztosítja a megfelelő védelmet az eszközei, és ezáltal saját maga részére. A felhasználók 44,8 %-a azzal sincsen tisztában, hogy mit kell tenni egy esetleges támadás esetén vagy hogy hova fordulhat segítségért.

Hipotézis 2: a támadók az IOT-eszközök elterjedésének köszönhetően egyre inkább kihasználják azok biztonsági réseit

A felkutatott szakirodalom és a tudományos igényű publikációk megerősítették ezt a hipotézist, 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 támadás megindításához, ami történhet botnet-ek használatával, valamint részei lehetnek szolgáltatásmegtagadásos vagy elosztott szolgáltatásmegtagadásos támadásnak is.

Hipotézis 3: 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.

A kérdőívet kitöltő 335 fő közül 278 fő kényelmi és 169 fő a szórakoztatási funkciója miatt vásárolja az IOT-eszközöket, a vásárlások során a biztonsági szempontok a válaszadók kevesebb, mint felénél játszanak szerepet, és mindösszesen 5 fő az, aki kizárólag a biztonsági szempontokat tartja szem előtt a vásárlásnál. Annak ellenére, hogy az IOT-eszközök számos veszéllyel bírnak, a kitöltők a jelenleg használt eszközeik mellett a kényelmük, szórakoztatásuk érdekében szívesen próbálnának ki további intelligens eszközöket és okosítanák otthonaikat és környezetüket. Ugyanakkor a primer kutatásból kiderült, hogy igen alacsony arányban tartják naprakészen magukat, a biztonsági kérdésekkel kapcsolatos információk tekintetében mindösszesen a válaszadók 15,2 %-a. Illetve a felhasználók kevesebb, mint harmada, pontosan 30,4 %, akik naprakészen el is végzik a biztonságosságához szükséges tevékenységeket.

ÁBRAJEGYZÉK

Képek, ábrák, táblázatok, diagramok

1. kép: Amazon Echo, Google Home, HomePod.....	23
2. kép: Hacker	41
1. ábra: IOT-eszközök születése.....	10
2. ábra: IOT főbb alkalmazási területei.....	11
3. ábra: IOT architektúrája	13
4. ábra: Mesh-hálózat	17
5. ábra: SWOT analízis	28
6. ábra: Zsarolóvírus.....	29
7. ábra: DDoS-támadás	31
1. táblázat: Adatkommunikációs csatornák összehasonlítása	20
2. táblázat: Alapértelmezett jelszavak és leggyakrabban használt jelszavak	34
1. diagram: IOT-eszközök darabszámának növekedése.....	7
2. diagram: Okos otthon eszközök piacának bevétele Magyarországon 2017-2025	21
3. diagram: Zsarolóvírus támadás leggyakoribb okai	35
4. diagram: IOT-eszközök alkalmazása	48
5. diagram: Alkalmazott IOT megoldások	48
6. diagram: IOT felhasználásnak okai.....	49
7. diagram: Vásárlás szempontja.....	50
8. diagram: Vélekedés a kínai gyártmányú eszközökről.....	51
9. diagram: Vélekedés a felhő alapú szolgáltatásokról	52
10. diagram: A mellőzés okai.....	53
11. diagram: Biztonsági kérdésekkel kapcsolatos információk követése	54
12. diagram: Figyelemmel kísért biztonsági intézkedések gyakorisága	55
13. diagram: Biztonsági intézkedések elvégzésének gyakorisága	55
14. diagram: Vélekedés az IOT-eszközök biztonságosságáról	56
15. diagram: Legnyagobb biztonsági kockázatok	57
16. diagram: Kibertámadások áldozatai	57

17. diagram: : Potenciális áldozat vagy sem?	58
18. diagram: Tisztában vagy vele, hova fordulhatsz, ha kibertámadás ér?	60

IRODALOMJEGYZÉK

- Ambrus, B. (2020, július). *Pedagógiai Folyóiratok*. Retrieved from <https://folyoiratok.oh.gov.hu/uj-kozneveles/az-ervenyesules-kulcsa-a-digitalis-problema megoldas> letöltés: 2022.08.31.
- apple.com. (2022). Retrieved from <https://www.apple.com/homepod-mini/> letöltés 2022.09.01.
- Bálint, K. (2018.). Tanulmánykötet a Biztonságtudományi Doktori Iskola kutatásaiból Kiberbiztonság. Budapest: Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar. 359. oldal
- Balogh, C. (2019, december 03.). *hvg.hu*. Retrieved from https://hvg.hu/tudomany/20191203_okos_tevekeszulek_lehallgatas_megfigyeles_fbi letöltés 2022.09.01.
- Bányász, P. (2022). Az okos mobil eszközök jelentette kiberbiztonsági kihívások. Nemzeti Közszerológati Egyetem. 17. oldal
- BBC News. (2017, december 13.). *BBC News*. Retrieved from <https://www.bbc.com/news/technology-42342221> letöltés 2022.09.01.
- Beláz, A. (2020). Rendszerelmélet. Budapest: Dialóg Campus. 161-162. oldal
- Bocsok, V., Boldizs, P. F., Loós, C., & Major, T. (2015). *fornax.hu*. Retrieved from <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> letöltés 2022.09.01.
- Boda, J. (2019). *Rendészettudományi Szaklexikon*. Budapest: Dialóg Campus Kiadó. 104. és 285. oldal
- Buchholz, K. (2021, február 9). *statista.com*. Retrieved from <https://www.statista.com/chart/16922/most-popular-passwords-2017-and-2018/> letöltés: 2022.08.30.
- Christián, L., Major, L., & Szabó, C. (2019). *Biztonsági vezetői kézikönyv*. Budapest: Dialóg Campus Kiadó. 161-162. oldal
- Cisco. (2016). *Cisco*. Retrieved from https://www.cisco.com/c/dam/global/hu_hu/solutions/security/ransomware/pdf/ransomware-everything-you-need-to-know_hun.pdf letöltés: 2022.08.30.
- Columbus, L. (2016, november 27.). *Forbes*. Retrieved from <https://www.forbes.com/sites/louis columbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/> letöltés: 2022.08.30.

- Crist, R. (2018, május 24). *CNET*. Retrieved from <https://www.cnet.com/home/smart-home/alexa-sent-private-audio-to-a-random-contact-portland-family-says/> letöltés: 2022.08.30.
- Cyrus, C. (2021, szeptember 17.). *IOT World Today*. Retrieved from <https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/> letöltés: 2022.08.30.
- Csizner, Z. (2019). A tömeges adatgyűjtés kérdései. *Nemzetbiztonsági Szemle*, 31-41.
- Deák, V. (2019). Social engineering alapú információszerzés a kibertérben megvalósuló lélektani műveletek során. *Hadtudományi Szemle*, 3. szám 95-111.
- dr. Christián, L. r. (2018). *Magánbiztonság I. kötet középiskolások számára*. 5. oldal
- Dr. habil. Christián, L., & dr. Rottler, V. (2019). *A biztonság megteremtésének új megközelítése: komplementer rendszet*. 90. oldal
- Elder, J. (2019, 08 20). *Avast*. Retrieved from <https://blog.avast.com/kevin-ashton-named-the-internet-of-things> letöltés: 2022.08.30.
- Erdősi, P. M., & Solymos, Á. (2017). *IT biztonság közérthetően*. Budapest: Neumann János Számítógép-tudományi Társaság (NJSZT).
- eset.com. (2020). Retrieved from <https://www.eset.com/hu/hirek/harom-eves-minden-idok-legdurvabb-zsarolovirusa-2020/> letöltés: 2022.08.30.
- Evans, D. (2011, 04). *Cisco*. Retrieved from <https://blog.avast.com/kevin-ashton-named-the-internet-of-things> letöltés 2022.08.26.
- Fieldstadt, E. (2018, december 18.). *NBC News*. Retrieved from <https://www.nbcnews.com/news/us-news/nest-camera-hacker-threatens-kidnap-baby-spooks-parents-n949251> letöltés: 2022.08.26.
- Flachner, B., & Klág, D. (2016, november 21.). *Index*. Retrieved from https://index.hu/tech/2016/10/21/internet_hiba_kibertamadas/ letöltés: 2022.08.30.
- Frész, F., Kálovics, T., & Puha, G. (2014). *Hálózatok biztonsága*. Budapest: Nemzeti Közszerzői Egyetem. 12. oldal
- GData. (2019, május 08). *GData*. Retrieved from <https://virusirto.hu/blogbejegyzesek/2019/05/08/millionyi-kinai-iot-eszkoz-veszelyben/> letöltés: 2022.08.30.
- Gupta, A. (2019). *The IOT Hacker's Handbook A Pratical Guide to Hacking the Internet of Things*.
- Haig, Z. (2018). *Információs műveletek a kibertérben*. Budapest: Dialóg Campus Kiadó.
- itechwares.com. (2022). Retrieved from <https://itechwares.com/> letöltés: 2022.09.01.
- Kelényi, I. (2008). Bevezetés a mobilprogramozásba. Bicske: SZAK Kiadó. 5-6. oldal

- Kókey, P. (2017, március 3). *Kalauz*. Retrieved from <https://kalauz.lib.pte.hu/felholo-technologia/> letöltés: 2022.09.01.
- Kovács, L. (2018). *A kibertér védelme*. Dialóg Campus Kiadó.
- Learnctv. (2020). *Learnctv*. Retrieved from <https://learnctv.com/ip-camera-default-password/> letöltés: 2022.09.01.
- Lee, R. M. (2018, augusztus). *NKI*. Retrieved from <https://nki.gov.hu/wp-content/uploads/2019/03/201808-OUCH-August-Hungarian.pdf> letöltés: 2022.09.01.
- Lopez, N. A., Pasaoa, J. B., Morales, J. O., & Parado, J. A. (2016, november). A Comparative Study of Thread Against ZigBee, Z-Wave, Bluetooth, and Wi-Fi as a Home-Automation Networking Protocol.
- Lueth, K. L. (2020, július 8). *IOT analytics*. Retrieved from <https://iot-analytics.com/top-10-iot-applications-in-2020/> letöltés: 2022.08.22.
- Molnár, L. (2020). *Informatikai rendszerek a közszolgáltatásban II*. Budapest: Dialóg Campus Kiadó.
- Nemzeti Kibervédelmi Intézet. (2018, július 5.). *NKI*. Retrieved from <https://nki.gov.hu/it-biztonsag/tudastar/elosztott-szolgaltatasmegtagadasos-tamadas-ddos-2/> letöltés: 2022.08.22.
- Nemzeti Kibervédelmi Intézet. (2018, április 22). *NKI*. Retrieved from <https://nki.gov.hu/it-biztonsag/tanacsok/igy-vedekzhetsz-az-5-leggyakoribb-jelszo-elleni-tamadas-ellen/> letöltés: 2022.08.22.
- Nemzeti Kibervédelmi Intézet. (2019). *Az információbiztonság lélektana*.
- Nemzeti Kibervédelmi Intézet. (2019, június 19.). *NKI*. Retrieved from <https://nki.gov.hu/it-biztonsag/hirek/rengeteg-celpontja-van-egy-uj-botnetnek/> letöltés: 2022.08.22.
- Nemzeti Kibervédelmi Intézet. (2020, március 25.). *NKI*. Retrieved from <https://nki.gov.hu/it-biztonsag/hirek/zyxel-nas-ok-veszelyben-uj-kontosben-csap-le-a-mirai-botnet/> letöltés: 2022.08.22.
- Nemzeti Kibervédelmi Intézet. (2020, július). *NKI*. Retrieved from <https://nki.gov.hu/wp-content/uploads/2020/07/Zsarol%C3%B3v%C3%ADrusok-1.pdf> letöltés: 2022.08.22.
- Nemzeti Kibervédelmi Intézet. (2020, március 9.). *NKI*. Retrieved from <https://nki.gov.hu/it-biztonsag/tudastar/robothalozat-botnet-2/> letöltés: 2022.08.22.
- Nemzeti Kibervédelmi Intézet. (2020, május 5.). *NKI*. Retrieved from <https://nki.gov.hu/it-biztonsag/hirek/kaiji-uj-iot-malware-a-lathataron/> letöltés: 2022.08.22.
- Nemzeti Kibervédelmi Intézet. (2020, április 14.). *NKI*. Retrieved from <https://nki.gov.hu/it-biztonsag/hirek/egyszemelyes-iot-botnet-hadsereg-felemelkedoben/> letöltés: 2022.08.22.

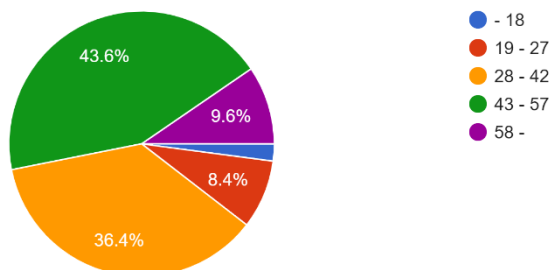
- Nemzeti Kibervédelmi Intézet. (2022). *NKI*. Retrieved from https://nki.gov.hu/wp-content/uploads/2022/03/ransomware_CTI_jelentes-1.pdf letöltés: 2022.09.02.
- Nest Labs. (2015, február). Retrieved from <https://storage.googleapis.com/nest-public-downloads/press/documents/energy-savings-white-paper.pdf> letöltés: 2022.09.02.
- Nordpass. (2020). *Nordpass*. Retrieved from <https://nordpass.com/most-common-passwords-list/> letöltés: 2022.09.02.
- notebook.hu. (2022). Retrieved from <https://www.notebook.hu/amazon-echo-dot-4-gen-okos-hangszoro-48203-fekete-294875> letöltés: 2022.09.02.
- OkosOtthonBolt*. (2021, július 21.). Retrieved from <https://okosotthon.bolt.hu/webaruhaz/okosotthon-kisokos/10-1-modszer-az-okosotthon-eszkozok-vezerlesere/> letöltés: 2022.09.02.
- OkosOtthonBolt*. (2022). *OkosOtthonBolt*. Retrieved from <https://okosotthon.bolt.hu/webaruhaz/okosvillamossagi-okosotthon-kisokos/> letöltés: 2022.09.02.
- Oktatási Hivatal. (2020). *Oktatási Hivatal*. Retrieved from https://www.oktatas.hu/koznevelis/kerettantervek/2020_nat/kerettanterv_alt_isk_1_4_evf letöltés: 2022.09.02.
- Perry, T. (2021, november 17.). *Smarthomepoint*. Retrieved from <https://www.smarthomepoint.com/history/> letöltés: 2022.08.24.
- Portfolio. (2014, január 14.). Retrieved from <https://www.portfolio.hu/uzlet/20140114/jon-az-okoshaztartas-mar-otthon-is-megfigyelhet-barkit-a-google-193906?amp> letöltés: 2022.08.24.
- Putnóczi, F. (2019). *Hangvezérelt okos otthon platform tervezése és elkészítése Raspberry PI miniszámítógépre*. Miskolc: Miskolci Egyetem.
- ResearchGate. (2017, december). *ResearchGate*. Retrieved from https://www.researchgate.net/figure/The-volume-sizes-of-DDoS-attacks-in-gigabits-per-second-2007-2016-2_fig1_321775189 letöltés: 2022.08.24.
- Rodríguez, J. (2022, május 17.). *Jalopnik*. Retrieved from <https://jalopnik.com/researchers-break-into-a-tesla-and-drive-away-using-blu-1848938417> letöltés: 2022.09.01.
- Sági, G. (2018). Célzott támadási modellek és műszaki védelem lehetőségek. Nemzeti Közszoigálati Egyetem.
- Sallai, G. (Budapest). *Az okosváros-koncepció és az internettechnológia*. 2019: Dialóg Campus Kiadó. 79. oldal
- Seals, T. (2021, szeptember 6). *threat post*. Retrieved from <https://threatpost.com/iot-attacks-doubling/169224/> letöltés: 2022.09.02.

- Statista. (2021, július 8.). *statista.com*. Retrieved from <https://www.statista.com/forecasts/1249200/revenue-smart-home-appliances-market-hungary> letöltés: 2022.09.02.
- Statista. (2022, 04 26). *Statista*. Retrieved from <https://www.statista.com/chart/27324/households-with-smart-devices-global-iot-mmo/> letöltés: 2022.09.02.
- Statista. (2022., július 7.). *statista.com*. Retrieved from <https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/> letöltés: 2022.09.02.
- Szemerey, S., & Kis, Z. (2020). A jó önkormányzás technológia háttere a digitális transzformáció korszakában. Budapest: Nemzeti közszolgálati Egyetem. 273-276. oldal
- Teicher, J. (2018, 02 07). *IBM*. Retrieved from IBM: <https://www.ibm.com/blogs/industries/little-known-story-first-iot-device/> letöltés: 2022.09.02.
- Tóth, A., & Tóth, L. (2014). *Biztonságtechnika*. Budapest: Nemzeti Közszolgálati Egyetem. 124. oldal
- tutiplaza.hu. (2022). Retrieved from <https://www.tutiplaza.hu/Google-Home-hangvezерelt-Multiroom-Google-Assistan> letöltés: 2022.09.02.
- Varga, A. K. (2014). *Oktatási segédlet a vezetékek nélküli kommunikációs szabványok oktatásához*.
- Varga, P. J. (2017). *Az okos otthonok vezetékek nélküli alkotóelemeinek biztonsága*. Óbudai Egyetem Kandó Kálmán Villamosmérnöki Kar.
- Williams-Grut, O. (2018, április 15.). *Privacy International*. Retrieved from <https://privacyinternational.org/examples/2559/aquarium-thermometer-enables-casino-hack> letöltés: 2022.08.25.
- Woodham, W. (2020). *howtofix.guide*. Retrieved from <https://howtofix.guide/default-password/> letöltés: 2022.09.02.
- Z. Karvalics, L. (2007). Az információs társadalom Az elmélettől a politikai gyakorlatig. Budapest: Gondolat - Új Mandátum. 34. oldal

MELLÉKLET: KÉRDŐÍV

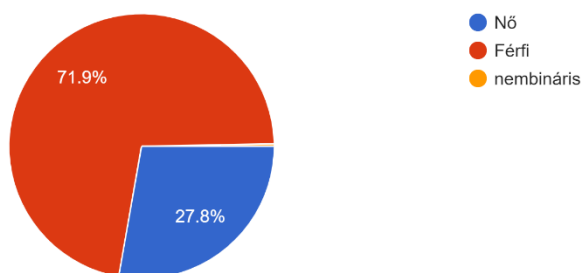
Melyik korkategóriába tartozol?

335 responses



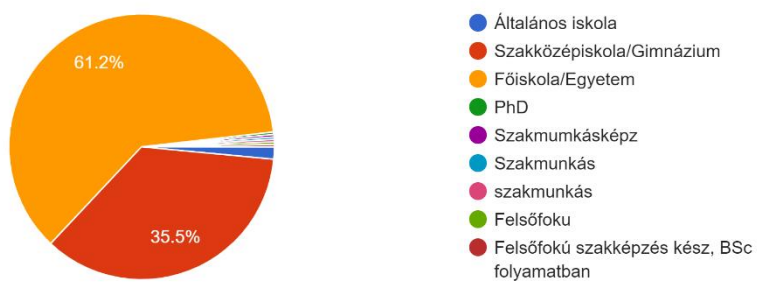
A nemed:

335 responses



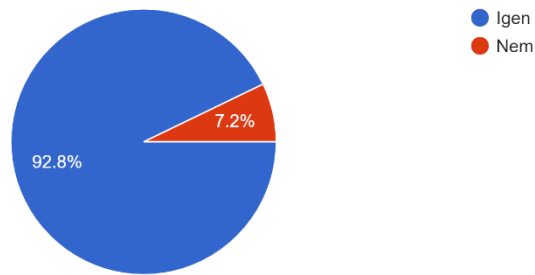
Mi a legmagasabb iskolai végzettséged?

335 responses



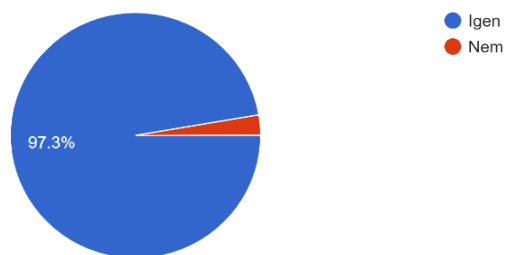
Hallottál már az IOT eszközökről?

335 responses



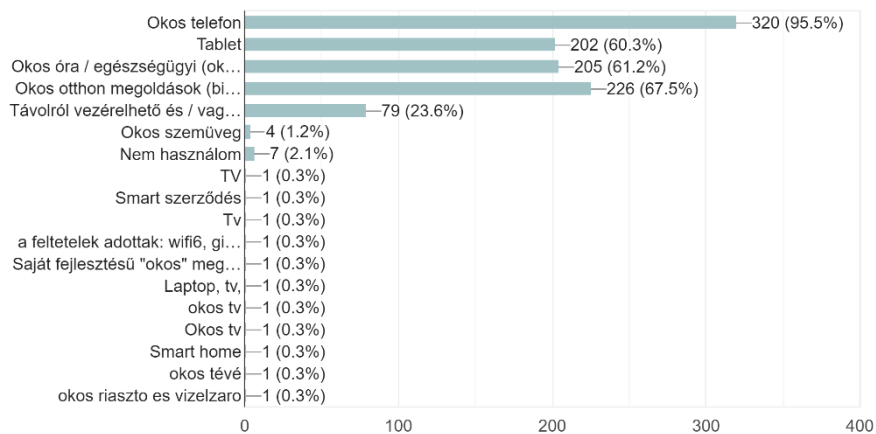
Használ sz IOT eszközöket? (Pl.: okos tv, okos óra, okos termosztát, okos mosógép, okos lámpa, okos zárok, okos konnektor...)

335 responses



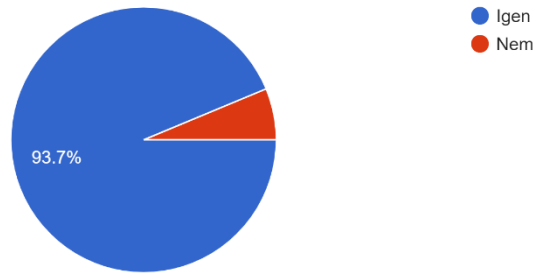
Milyen IOT megoldásokat használ sz? (több válasz is lehetséges)

335 responses



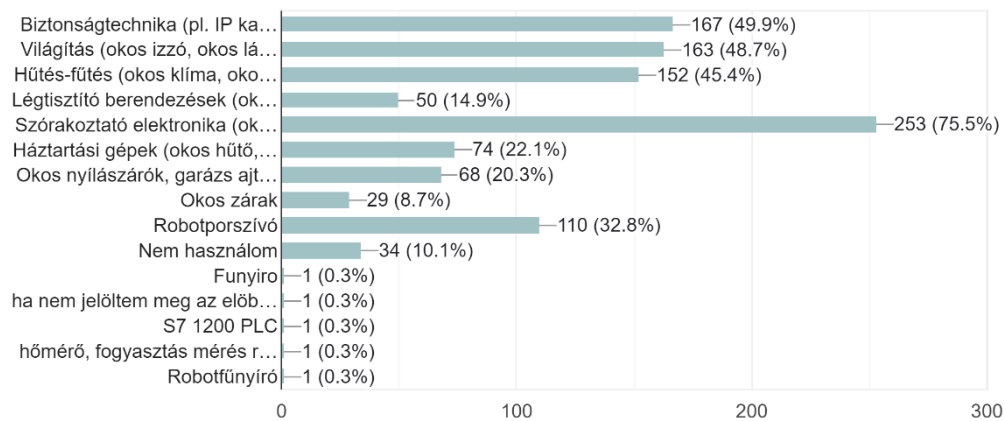
Hallottál már az okos otthon megoldásokról?

335 responses



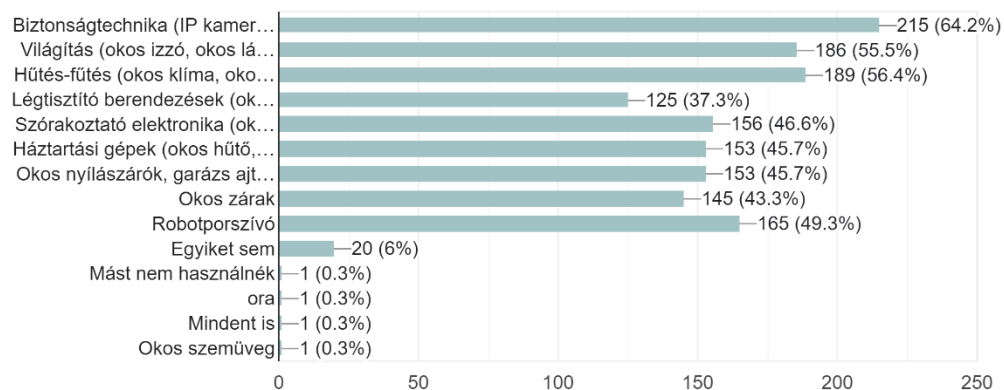
Melyik okos otthon eszközöket használsz? (több válasz is lehetséges)

335 responses



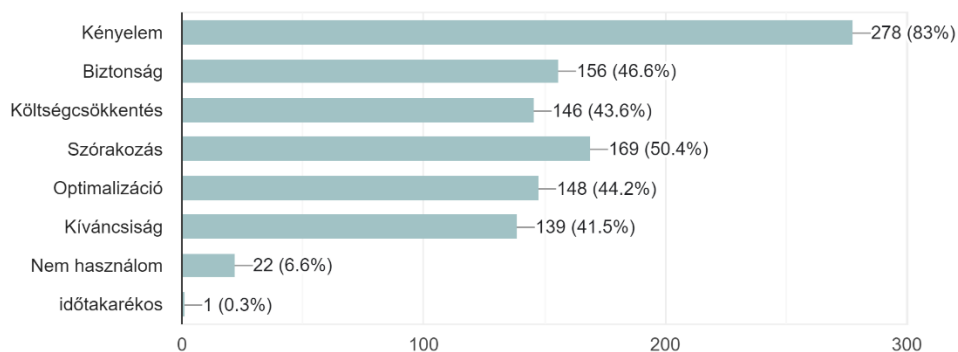
Melyik okos otthon eszközöket használnád továbbra is vagy próbálnád ki szívesen? (több válasz is lehetséges)

335 responses



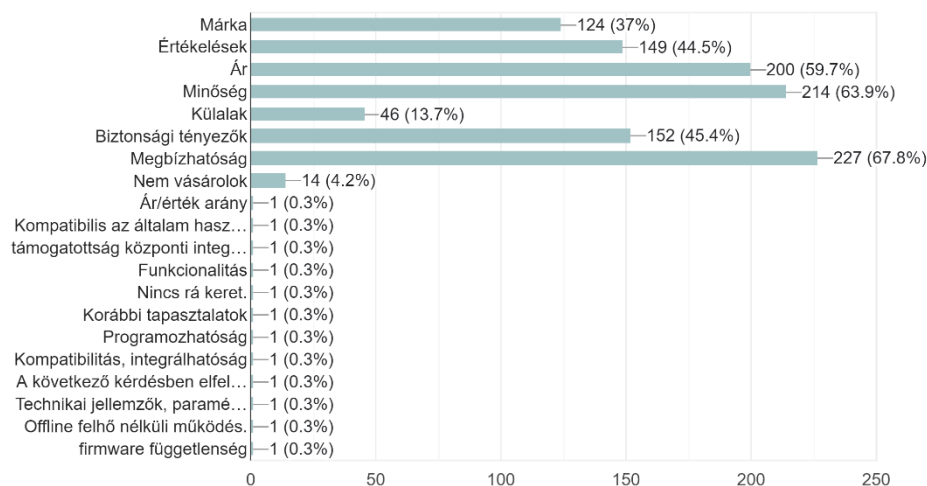
Milyen okból használsz ezeket az eszközöket? (több válasz is lehetséges)

335 responses



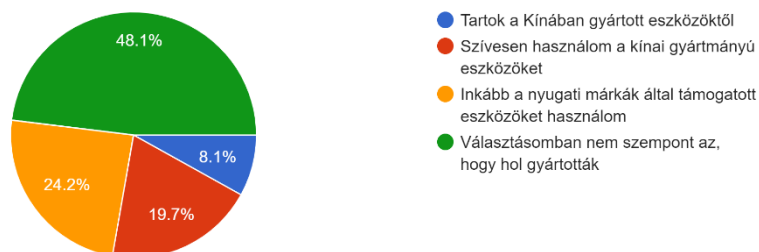
Mi alapján választasz, amikor okos otthon megoldásokat vásárolsz? (több válasz is lehetséges)

335 responses



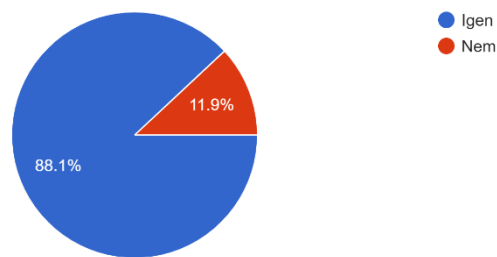
Szívesen használsz a kínai gyártmányú eszközöket, vagy inkább a nagy nyugati márkák által támogatott eszközöket használsz?

335 responses



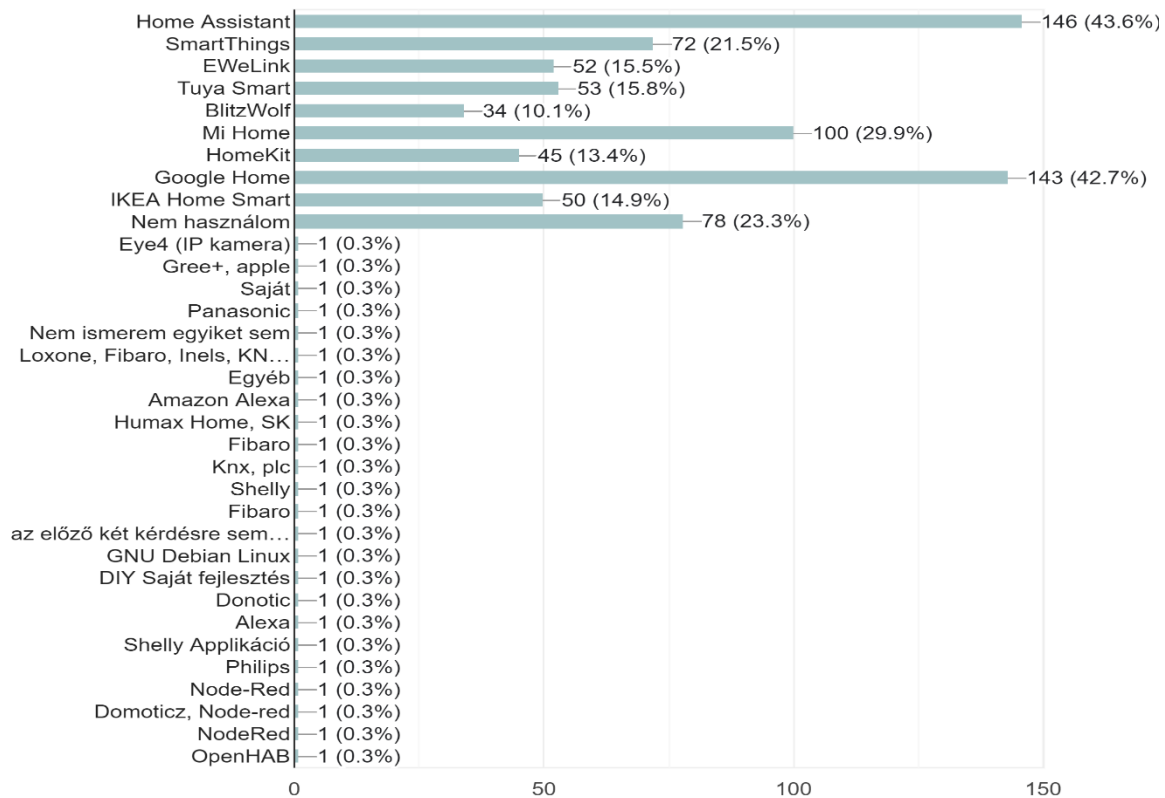
Amikor okos otthon eszközöket vásárolsz, akkor fontos szempont az eszköz integrálhatósága?
(Hogy ne kelljen külön megnyitni az összes eszkö...yben, egymással összehangolva lehessen kezelni)

335 responses



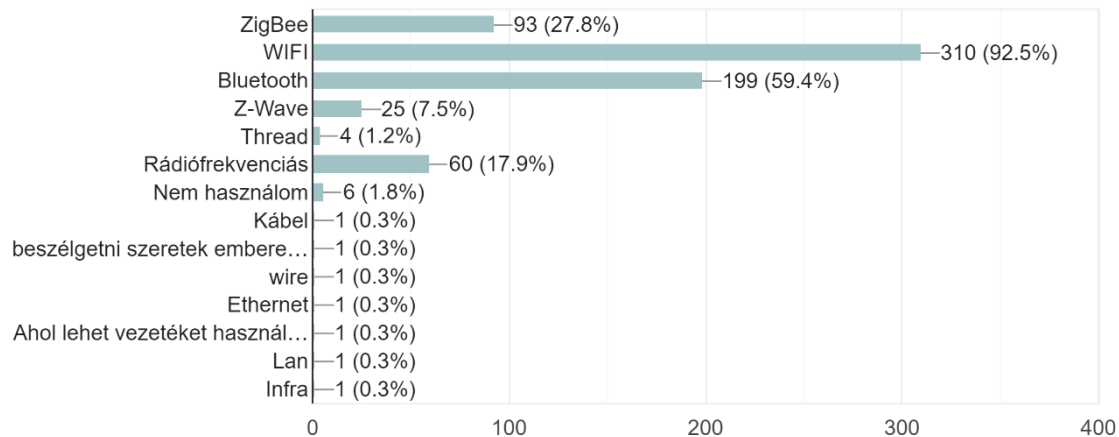
Rendszerintegrálás tekintetében melyik platformokat ismered / használod? (több válasz is lehetséges)

335 responses



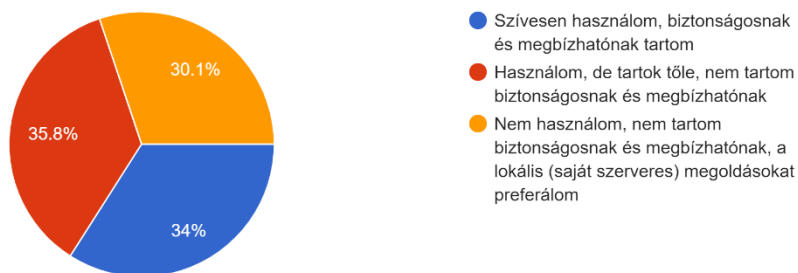
Melyik kommunikációs csatornát használsz szívesen? (több válasz is lehetséges)

335 responses



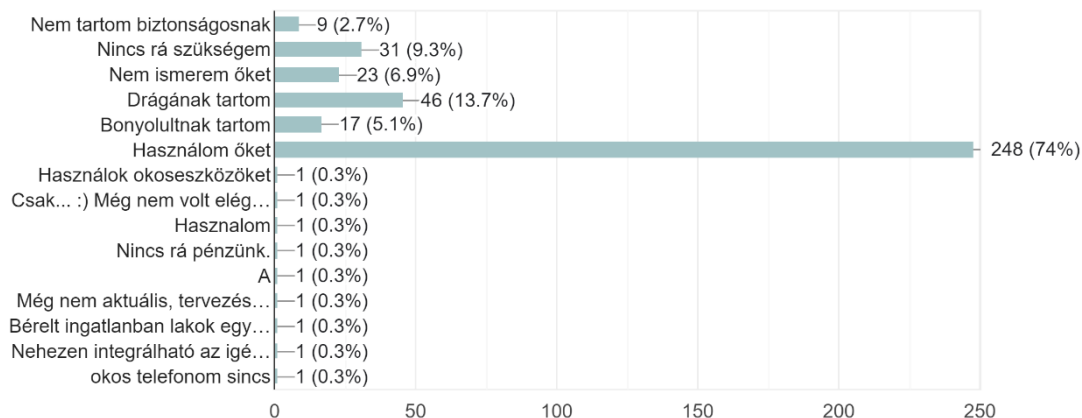
Szívesen veszel igénybe felhő alapú szolgáltatást vagy tartasz tőle?

335 responses



Ha nem használod okos otthon megoldásokat, akkor miért nem? (több válasz is lehetséges)

335 responses



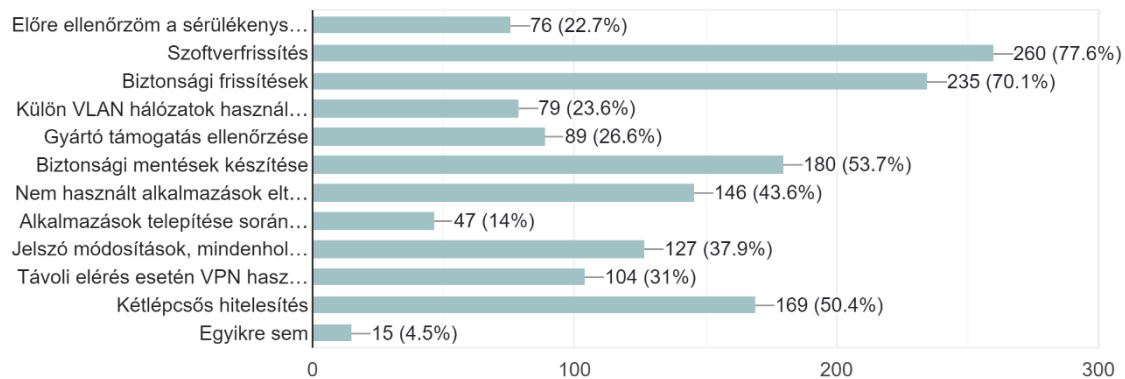
Mennyire követed az okos eszközök biztonsági kérdéseivel kapcsolatos információkat?

335 responses



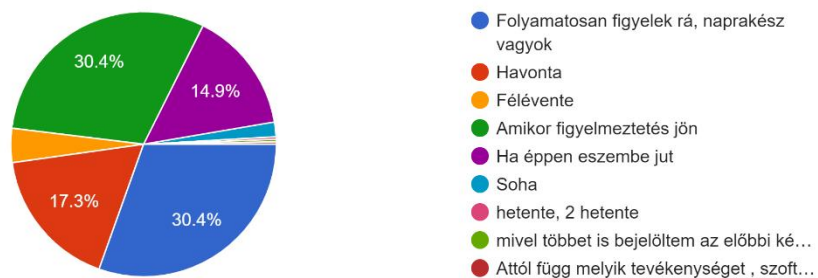
Az alábbiak közül melyikre figyelsz oda? (több válasz is lehetséges)

335 responses



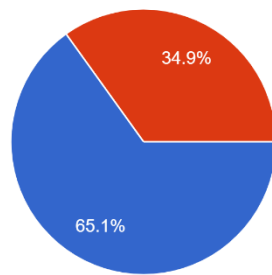
Milyen gyakran végzed el ezeket a biztonságossághoz szükséges tevékenységeket?

335 responses



Biztonságosnak tartod az okos eszközöket?

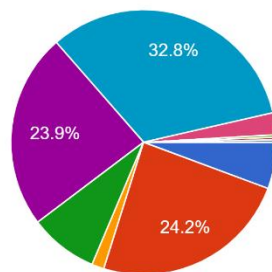
335 responses



- Igen
- Nem

Mit látsz a legnagyobb biztonsági kockázatnak?

335 responses

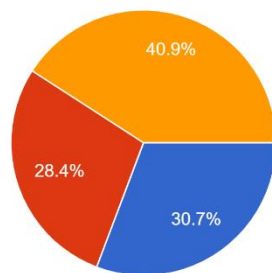


- Nem megfelelően látja el a funkcióját
- Megfigyelhetővé válik az életem miatt
- Nem ismerem, és félek az ismeretlentől
- Nem biztonságos adatgyűjtés
- Adatszivárgás (felhasználónevek, jelszavak)
- Online támadhatóság az eszközeimen...
- Fizikai támadhatóság
- Online támadhatóság az eszközeimen...

▲ 1/2 ▼

Voltál már valaha áldozata kibertámadásnak?

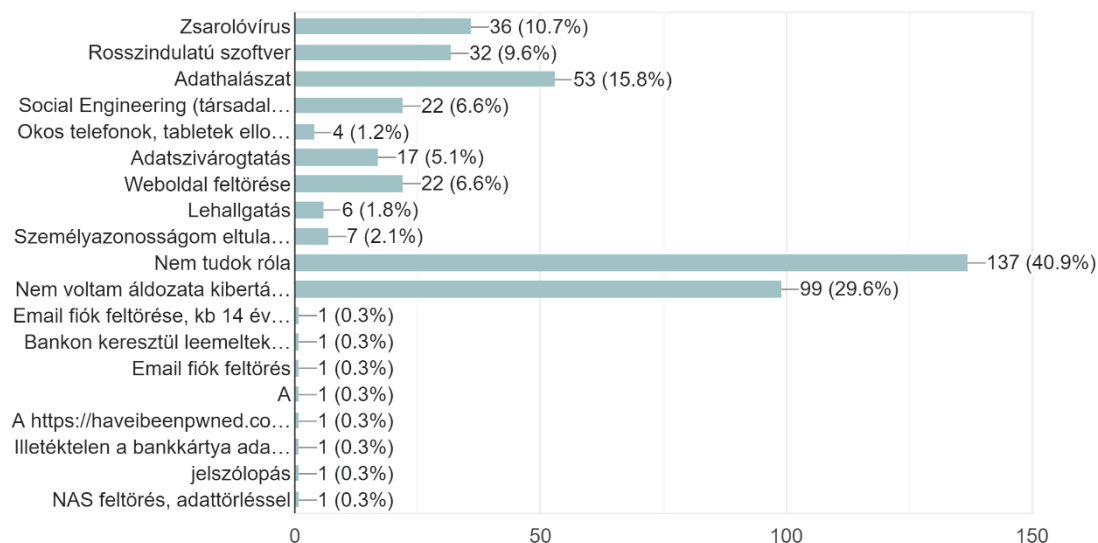
335 responses



- Igen
- Nem
- Nem tudok róla

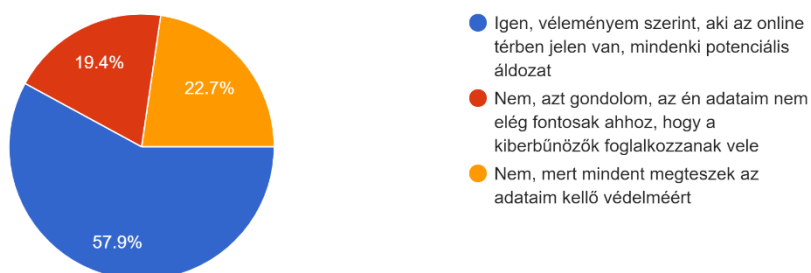
Milyen jellegű támadás volt? (több válasz is lehetséges)

335 responses



Potenciális áldozatnak tartod magad az online térben?

335 responses



Tisztában vagy vele, hogy mit kell tenned, illetve hova fordulhatsz, ha kibertámadás ér?

335 responses

