

37. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2025. április 22–24.
Nemzeti Közsolgálati Egyetem
Hadtudományi és Honvédtisztképző Kar

IoT eszközök kiberbiztonsági kihívásai az okos otthonok világában

Jelige: *Okos háztartás*

Pályamunka lezárásának időpontja: 2023. november

2025.

TARTALOMJEGYZÉK

Bevezető	4
A kutatást alátámasztó probléma	4
Téma aktualitása	4
Kutatási célkitűzések	5
Kutatási hipotézisek.....	5
1. Az IoT általános bemutatása	7
2. Az IoT technológiai felépítése az okos otthonok világában	12
2.1 Az okos otthonok rendszere.....	14
2.2 Kommunikációs protokollok	17
2.3 Következtetések	21
3. IoT-val kapcsolatos szabályozások és szabványok nemzetközi környezetben	22
3.1 Az USA szabályozása az IoT-ra.....	24
3.2 Az Európai Unió szabályozása az IoT-ra	27
3.3 Nemzetközi szabványok.....	31
3.4 Következtetések	35
4. IoT eszközök sérülékenységei és ezek kihasználását csökkentő védelmi intézkedések	36
4.1 IoT eszközök sérülékenységei és kihasználásuk típusai az okos otthonok tükrében	39
4.2 Védelmi opciók, kockázatcsökkentő intézkedések	42
4.3 Következtetések	46
5. Hazai felhasználók bizalma és elhivatottsága az otthoni IoT eszközök iránt	47
5.1 Kérdőív bemutatása	47
5.2 Eredmények kiértékelése	50
5.3 Következtetések	56
Összefoglaló	57
Irodalomjegyzék.....	59
Mellékletek	65
1. számú melléklet: Ábrajegyzék	65
2. számú melléklet: Táblázat jegyzék	65

3.	számú melléklet: Rövidítés jegyzék	67
4.	számú melléklet: Kérdőív.....	68
5.	számú melléklet: Kérdőív kielemezés	72

BEVEZETŐ

Kutatásom során az IoT eszközök kiberbiztonsági kihívásait fogom vizsgálni az okos otthonok világában. Az IoT (Internet of Things, magyarul a „dolgok internete”), olyan eszközök hálózatát foglalja magába, amelyek különböző szenzorokkal, szoftverekkel vannak ellátva, tudnak csatlakozni az Internetre, adatokat rögzítenek és fogadnak, valamint tudnak egymással kommunikálni, tehát adatátvitel megy végbe a különböző eszközök között, még hozzá rapid gyorsasággal. A mai modern világunkban szinte bármit fel tudunk okosítani az otthonunkban is, legyen szó többek között televízióról, klímáról, hűtőről, vagy akár a termosztátunkról.

A KUTATÁST ALÁTÁMASZTÓ PROBLÉMA

A témaválasztásom mögött főleg az az indok húzódik, hogy napjainkban az IoT világa egyre jelentősebb szerepet tölt be az életünkben és folyamatosan bővül azon szegmensek köre, ahova beférkőzik. Ez alól már az otthonunk sem kivétel. A felhasználók részéről érzékelhető az egyre fokozottabb érdeklődés, valamint igény, hogy körbevegyék magukat ezen eszközökkel és az általuk nyújtott kényelemmel. Nagy hangsúly helyeződik arra, hogy milyen külsővel rendelkeznek és persze a vásárlás során az ár is fontos szempont tud lenni. Ezzel szemben már kevésbé mozgatja a felhasználók fantáziáját, hogy biztonsági oldalról milyen nehézségekbe, problémákba ütközhetnek, amikre valószínűleg korábban nem is gondoltak volna. Az IoT eszközök használata felelősségteljes és tudatos vásárlókat kíván meg, hiszen nagyon gyorsan és egyszerűen a célkeresztbe kerülhetünk kiberbiztonsági szempontból. Természetesen a probléma nemcsak a felhasználókkal függ össze, hanem vissza kell mennünk egészen az IoT eszközök gyártásáig.

TÉMAAKTUALITÁSA

Ezen téma nagyfokú aktualitást élvez és mindenki számára hasznos tud lenni, ha kap egy átfogó képet az IoT világról és annak veszélyeiről. Az otthon a legtöbb ember számára a kényelmet, a biztonságot és a nyugalmat jelenti. Viszont a figyelmetlenség több szempontból is kárt tud okozni a felhasználóknak, sértheti a biztonságérzetet, ezért fontosnak tartom, hogy kiemeljem az okosotthonokban előfordulható incidenseket, mert valamilyen szinten mindannyian érintettek lehetünk benne. Számos olyan támadást lehetett megtapasztalni, ami alá tudja támasztani, hogy miért fontos beszélni erről a témáról. Ilyen többek között a Mirai és Satori Botnet támadás, vagy a Ring Camera Hacks, amelyeket kicsit bővebben ki fogok fejteni a következőkben.

KUTATÁSI CÉLKITŰZÉSEK

Kutatásom során bemutatom, hogy mit érdemes tudni az IoT-ról általában véve, illetve azt is, hogy hogyan épül fel a technológia az okos otthonok rendszerében és milyen kommunikációs protokollokat érdemes ismerni. Ezen felül a dolgozatban ismertetni fogom az IoT-val kapcsolatos szabályozásokat és szabványokat nemzetközi környezetben, kitérve külön az Amerikai Egyesült Államokra és az Európai Unióra. Szó lesz arról is, hogy mik azok a sérülékenységek, és támadástípusok, amelyekkel találkozhatunk, illetve milyen kockázatcsökkentő intézkedések vannak. A dolgozat végén bemutatom a felmérésem eredményét, amely középpontjában a magyarországi felhasználók fognak állni és azt fogom vizsgálni, hogy mennyire fordulnak bizalommal az IoT eszközök felé, egyáltalán milyen mértékben ismerik az IoT-t, illetve mennyire van igényük ezen technológiára és milyen félelmekkel küzdenek.

KUTATÁSI HIPOTÉZISEK

A kutatásom elején az alábbi hipotéziseket fogalmaztam meg:

- H1: Az IoT szabályozása erősebb az Amerikai Egyesült Államokban, mint az Európai Unióban.

- H2: Új sérülékenységeket és az azokat kihasználó támadási típusokat ismerhetünk meg az IoT világában.
- H3: Az IoT definíciójának ismerete befolyásolja az ezen technológiával kapcsolatos fenyegetések értékelését.
- H4: A nők kevésbé gondolják magabiztosnak magukat információbiztonsági tudatosság tekintetében és az IoT fogalmát illetően.
- H5: Az IoT eszközök száma befolyásolja az igényt az otthon egyes területeinek felokosítására.

1. AZ IOT ÁLTALÁNOS BEMUTATÁSA

Az IoT (Internet of Things) kifejezést először Kevin Ashton, a brit technológia úttörője, az MIT Auto-ID Laboratory társalapítója alkotta meg 1999-ben. Az IoT fogalma az "okosság" szó körül forog és a tudás önálló megszerzésére, alkalmazására való képességet jelöli. Vagyis az IoT azokra a dolgokra vagy eszközökre és érzékelőkre utal, amelyek intelligensek, kommunikációs protokolljaik alapján egyedileg címezhetőek, alkalmazkodóképesek és autonómok. Az IoT-t három vízióval lehetne jellemezni. Az első az Internet-orientáltság, vagyis a vízió az objektumok közötti összekapcsolhatóságra összpontosít. A második a „dolog” -orientáltság, amikor a vízió az általános objektumokra összpontosít. A harmadik pedig a tudás-orientáltság, amikor a vízió az információ ábrázolására, tárolására és szervezésére összpontosít. Ezek a víziók a Nemzetközi Távközlési Unió (International Telecommunication Union-ITU) IoT-víziója felé haladnak, amelynek lényege, hogy „bármikor, bárhol, bárki számára elérhető kapcsolat” legyen.¹

Ezek alapján elmondható, hogy az IoT az érzékelőkkel, processzorokkal és kommunikációs komponensekkel felszerelt fizikai eszközök integrációját jelenti az Internettel, amelyek érzékelési, számítástechnikai és kommunikációs képességekkel rendelkeznek az Interneten keresztül történő érzékelés, feldolgozás és információcsere érdekében. Mindez korlátozott emberi beavatkozással, vagy akár anélkül történik. Ezek az eszközök lehetnek biztonsági rendszerek, járművek, háztartási gépek, elektronikus eszközök és így tovább. A felhasználói interfész biztosítja a telepítésüket és a vezérlésre szolgáló parancsok megadását ezeknek az eszközöknek. Megosztják egymással az adatokat, vagy azokat a helyi feldolgozóegységeknek vagy távoli felhőszervereknek küldik el feldolgozásra. A tárgyak internetének ötlete már a kezdetektől fogva átalakította a mindennapi életünk különböző aspektusait, és forradalmi technológiai és hálózati paradigmának bizonyult. Az IoT nagyszerű piaci lehetőséget kínál többek között a készülékgyártóknak, az internetszolgáltatóknak, vagy például az alkalmazásfejlesztőknek. Lényegében különböző iparágak alkalmazzák az IoT koncepcióját annak érdekében, hogy zökkenőmentesen és hatékonyabban működjenek, jobban megértsék, hogyan nyújtsanak jobb szolgáltatásokat az ügyfeleknek. Az IoT-hálózatokban használt hálózati

¹ Kinza Shafique és mtsai., „Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios”, *IEEE Access* 8 (2020): 23022–40, <https://doi.org/10.1109/ACCESS.2020.2970118>.

és kommunikációs protokollok nagymértékben függenek a mögöttes alkalmazások jellegétől. Ezek a valós alkalmazások a fogyasztó-orientált alkalmazásokról, mint például az okos otthonok, a viselhető eszközök és az egészségügy, a vállalati alkalmazásokig, mint például az intelligens városok, a mezőgazdaság, az intelligens iparágak és a forgalomirányítás, terjednek. Nem helytelen azt állítani, hogy az IoT körül megjelent felhajtás óriási, és napról napra újabb IoT-képes termékek jelennek meg a piacon.² Számos vezető vállalat, csakúgy, mint a Google és az Amazon, folyamatosan kutat és dolgozik az IoT különböző területeinek feltárásán és megpróbálják integrálni a mindennapi életünkbe.³

Az egyre több okos tárgyak és alkalmazások egyben folyamatosan növekvő biztonsági kihívást is jelentenek. Az IoT-ban a biztonság kulcsfontosságú, de nehezen elérhető el. A hagyományos vezetékes hálózatok viszonylag biztonságosabbak, mint a vezeték nélküli IoT-hálózatok. A hagyományos hálózatok lehetővé teszik, hogy a forgalom különböző útválasztó eszközökön, például switcheken keresztül haladjon, amelyek gyakran magas konfigurált tűzfalakkal és számos más biztonsági kezelési technikával vannak ellátva. Ebből adódóan ezek a hálózatok jól felszereltnek tekinthetők bármilyen típusú behatolással vagy túlterheléses támadással (Distributed Denial of Service-DDoS) szemben. Ellenben az IoT hálózatai vezeték nélküliek és természetüknél fogva sebezhetőek a különböző típusú támadásokkal szemben.⁴

Elmondható, hogy az IoT eszközök sokszor nem rendelkeznek megfelelő védelemmel, ebből adódóan kijelenthető, hogy az IoT a kibertámadások népszerű célpontjává vált. Fontos figyelembe venni, hogy nem minden gyártónak az elsődleges célja, hogy minél biztonságosabb eszközt hozzon létre, hanem inkább más szempontok kerülnek előtérbe, mint például a profit vagy az olcsóbb és gyorsabb megjelenítés.⁵ A Statista riportja alapján is meglehetősen aggasztóak a számok. Az IoT-t ért kibertámadások száma 2022-ben világszerte meghaladta a 112 milliót. Az elmúlt évek során ez a szám a 2018-as mintegy 32 millió észlelt esetről jelentősen megnőtt. A legutóbbi mért évben az IoT-t érintő rosszindulatú szoftveres incidensek

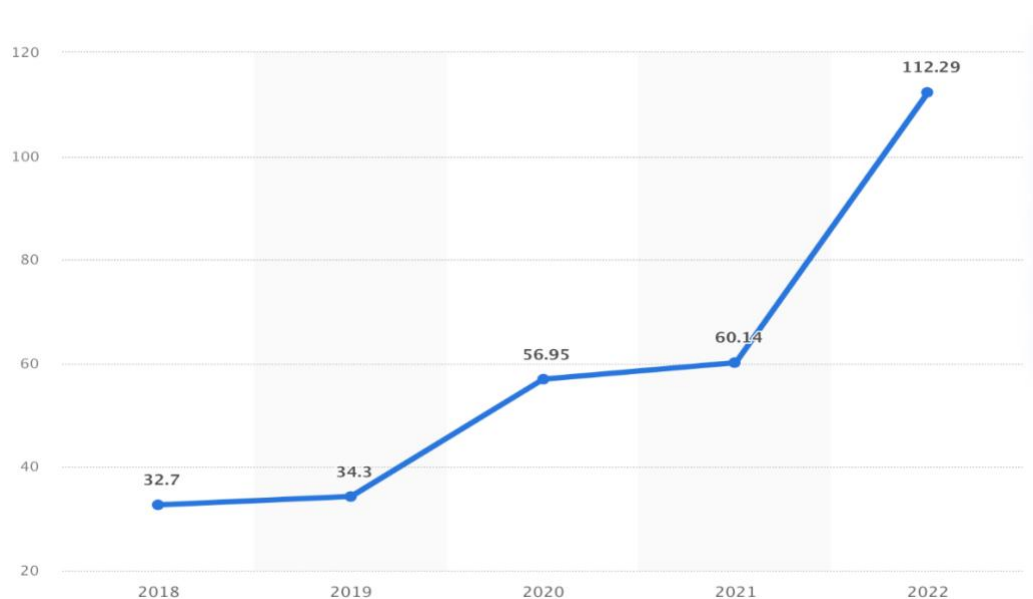
² Brij B Gupta és Megha Quamara, *Internet of Things Security: Principles, Applications, Attacks, and Countermeasures* (CRC Press, 2020), <https://doi.org/10.1201/9780429353529>.

³ Prangshu Dweep Baruah, Saru Dhir, és Madhurima Hooda, „Impact of IOT in Current Era”, in *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)* (2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India: IEEE, 2019), 334–39, <https://doi.org/10.1109/COMITCon.2019.8862187>.

⁴ Ala Al-Fuqaha és mtsai., „Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications”, *IEEE Communications Surveys & Tutorials* 17, sz. 4 (2015): 2347–76, <https://doi.org/10.1109/COMST.2015.2444095>.

⁵ Mandić Dorottya és Simon János, „Biztonságosak-e az okosotthonokban használt okoseszközök?”, *Biztonságtudományi Szemle* 4, sz. 4. (2022. december 7.): 59–67.

számának éves növekedése 87 százalékos volt. Pontosan ez miatt az IoT-val foglalkozó szakemberek nagy kihívások elé néznek, hogy biztosítsák a hálózatoknak, az adatoknak, és az eszközöknek a védelmét.⁶



1. ábra: IoT támadások száma 2018-2022 között globálisan. Forrás:

<https://www.statista.com/statistics/1377569/worldwide-annual-internet-of-things-attacks/>

Az egyik nagy kihívás a szoftverfrissítés. Sajnos az IoT eszközök szoftverfrissítéséről könnyebb beszélni, mint megvalósítani. Egyes eszközök nem rendelkeznek szoftverfrissítési képességekkel, míg másoknál előfordulhat, hogy a frissítésekre vonatkozó időszak lejár. Például a vélhetően hosszú évekig működő hűtőszekrények csak néhány évig kaphatnak szoftverfrissítéseket. Még ha rendelkezésre is állnának frissítések, azok alkalmazása kihívást jelenthet. Egyes eszközök esetében a felhasználóknak aktívan telepíteniük kell a frissítéseket, míg az automatikusan települő eszközök esetében előfordulhat, hogy újra kell indítani a firmware frissítését, ami hiányosságokat okozhat a rendelkezésre állásban. További nemkívánatos következményekkel járhat, ha a gyártók akkor frissítenek például egy villanykapcsolót, amikor a felhasználó éppen használja a lámpát vagy egy vízmelegítőt, amikor valaki éppen zuhanyzik. Az IoT eszközök tehát elkerülhetetlenül ki vannak és ki is lesznek téve biztonsági réseknek. Ezen rések gyors foltozása nem mindig lesz egyszerű, tekintettel arra, hogy a felhasználó kényelme és elégedettsége az egyik legfontosabb szempont, még akkor is,

⁶ „Annual Number of IoT Attacks Global 2022”, Statista, elérés 2023. szeptember 8., <https://www.statista.com/statistics/1377569/worldwide-annual-internet-of-things-attacks/>.

ha ez a biztonság rovására mehet.⁷ Fontosnak tartom, hogy a bevezetőben említett IoT támadásokat egy kicsit részletezzem, ezzel is szemléltetve a téma aktuálitását. Ha IoT-ról beszélünk talán az egyik, ha nem a legjelentősebb esemény volt a 2016-ban megtörtént Mirai Botnet támadás. 2016. szeptember 20-án Brian Krebs, kiberbiztonsági témákat feldolgozó újságíró weboldalát az egyik legnagyobb, eddig látott túlterheléses támadás (DDoS) offline állapotba hozta. Ezt a támadást a később Mirai botnet néven kiderült támadás eredményezte. Pár nap leforgását követően egy "Anna-Senpai" nevű felhasználó fórumbejegyzésében kiszivárogtatta a Mirai botnet forráskódját és utasításait a nyilvánosság számára. Ennek a támadásnak az eredményeképpen Brian Krebs végül sikeresen felfedte legalább egy olyan társszerző személyazonosságát, aki segített a Mirai létrehozásában. Majd közel három hónappal később a legnagyobb DDoS-támadás célpontjává egy népszerű dinamikus DNS-szolgáltató, a Dyn vált. Ez a támadás nemcsak a legnagyobb volt a maga nemében, hanem rendkívül hatékony is, nagy figyelmet és sajtóvisszhangot hozott a Mirai számára, és számtalan hírmédium foglalkozott vele.⁸ A Mirai Botnet mellett a 2017-es Satori Botnet is jelentős volt. 12 óra alatt 280 000 IoT eszközt térített el.⁹ 2019-ben volt egy másik eset, ami szintén figyelmet érdemel és jelentős az okos otthonok világában, ez pedig az Amazon Ring kameráinak feltörése. Több olyan esetet is jelentettek, amikor hackerek jogosulatlan hozzáférést szereztek a Ring okos otthoni biztonsági kamerákhoz. Kompromittált bejelentkezési adatokat használtak a kamerákhoz való hozzáféréshez, majd zaklatták a háztulajdonosokat, illetve online streamelték is a felvételeket.¹⁰

Mindezekről függetlenül az IoT eszközök mára olyan fejlődésen mentek keresztül, amely következtében előre meghatározott minták szerint, vagy a felhasználó igényei szerint képesek irányítani akár az otthonunkat is távolról. Az előrejelzések szerint az IoT eszközök száma világszerte majdnem megháromszorozódik. A 2020-as 9,7 milliárdról, 2030-ra több, mint 29

⁷ Stanislav Mamonov és Marios Koufaris, „Fulfillment of Higher-Order Psychological Needs through Technology: The Case of Smart Thermostats”, *International Journal of Information Management* 52 (2020. június 1.): 102091, <https://doi.org/10.1016/j.ijinfomgt.2020.102091>.

⁸ Joel Margolis és mtsai., „An In-Depth Analysis of the Mirai Botnet”, in *2017 International Conference on Software Security and Assurance (ICSSA)* (2017 International Conference on Software Security and Assurance (ICSSA), Altoona, PA: IEEE, 2017), 6–12, <https://doi.org/10.1109/ICSSA.2017.12>.

⁹ Tolijan Trajanovski és Ning Zhang, „An Automated and Comprehensive Framework for IoT Botnet Detection and Analysis (IoT-BDA)”, *IEEE Access* 9 (2021): 124360–83, <https://doi.org/10.1109/ACCESS.2021.3110188>.

¹⁰ August E. Grant és Jennifer H. Meadows, *Communication Technology Update and Fundamentals*, 17. kiad. (Routledge, 2020).

milliárd IoT eszközre lehet számítani. 2030-ra várhatóan Kínában lesz a legtöbb, mintegy 5 milliárd fogyasztói eszközzel.¹¹

¹¹ Lionel Sujay Vailshery, „IoT Connected Devices Worldwide 2019-2030”, Statista, 2022. november 22., <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/>.

2. AZ IOT TECHNOLÓGIAI FELÉPÍTÉSE AZ OKOS OTTHONOK VILÁGÁBAN

Dolgozatom fókuszában az okos otthonok állnak, így fontos megérteni azt is, hogy hogyan épülnek fel és hogy hogyan működik a mindezek mögött álló IoT. Az okos otthon valójában az az otthon vagy az a lakókörnyezet, amely olyan technológiával rendelkezik, ami lehetővé teszi a háztartási eszközök automatikus és távolról történő vezérlését. Hálózati szempontból vezetékes és vezeték nélküli rendszerekbe sorolható. Az okos otthonokban a felhasználó az Interneten keresztül könnyen nyomon követheti és vezérelheti az összes otthoni eszközt, vagy háztartási készüléket. Ezen készülékek hálózati architektúrában és protokollok használatával csatlakoznak.¹² Azonban fontos tudni, hogy ahhoz, hogy egy rendszer intelligens legyen, testreszabhatónak, kontextustudatosnak, adaptívnek és előrelátónak kell lennie. Az okos lakóteret az jellemzi, hogy a környezet képes reagálni a lakók igényeire. Ezért különbséget kell tenni az okos otthonok intelligenciája és az automatizálás között. Az automatizálás csak egy részhalmaza az intelligens környezetnek, és az emberek már korábban is használtak automatizálási technikákat (pl.: termosztátok, mosógép). Az automatizálás azonban nem látja a nagyobb képet, mivel csak korlátozott számú dolog kezelésével foglalkozik. Az intelligenciát viszont az határozza meg, hogy az összes összekapcsolt eszközön és érzékelőn keresztül nagyobb képet kap a teljes környezetről, és ezért jobban tud alkalmazkodni, valamint előrejelzéseket készíteni a rendszer aktuális állapota és a lakókról szerzett korábbi ismeretek alapján.¹³

Az IoT alapköveit áttekintve, egy átfogóbb képet tudunk kapni a valódi funkcionalitásáról és arról, hogy az okos otthonokba ez hogyan is épül be. Öt főbb elemet fogok bemutatni a dolgozatomban. Az első az azonosítás, amely kulcsfontosságú az IoT számára, hogy a szolgáltatásokat megnevezze és a keresletükhöz igazítsa. A tárgyak internetéhez számos azonosítási módszer áll rendelkezésre, mint például többek között az elektronikus termékkódok

¹² Pranay P. Gaikwad, Jyotsna P. Gabhane, és Snehal S. Golait, „A survey based on Smart Homes system using Internet-of-Things”, in *2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC)* (2015 International Conference on Computation of Power, Energy Information and Communication (ICCPEIC), Melmaruvathur, Chennai, India: IEEE, 2015), 0330–35, <https://doi.org/10.1109/ICCPEIC.2015.7259486>.

¹³ Dragos Mocrii, Yuxiang Chen, és Petr Musilek, „IoT-Based Smart Homes: A Review of System Architecture, Software, Communications, Privacy and Security”, *Internet of Things* 1–2 (2018. szeptember): 81–98, <https://doi.org/10.1016/j.iot.2018.08.009>.

(EPC). Ezenkívül a tárgyak címezése is kritikus fontosságú, annak érdekében, hogy különbséget tudjunk tenni az objektum azonosítója és a címe között. Az objektum azonosítója a nevére utal, az objektum címe pedig a kommunikációs hálózaton belüli címe. Az objektum azonosítása és a cím megkülönböztetése elengedhetetlen, mivel az azonosítási módszerek nem globálisan egyediek, így a címezés segíti az objektumok egyedi azonosítását. Az azonosítási módszerek arra szolgálnak, hogy a hálózaton belül minden egyes objektumnak egyértelmű azonosítást biztosítsanak. Második fontos szempont az érzékelés, ami valójában a kapcsolódó tárgyakról történő adatgyűjtést jelenti a hálózaton belül. Ezen adatok visszaküldésre kerülnek egy adattárházba, adatbázisba vagy felhőbe. Az összegyűjtött adatok kielemezésre kerülnek, hogy a szükséges szolgáltatások alapján konkrét intézkedések születhessenek.¹⁴

Harmadik nagyon lényeges pont a kommunikáció. Ez a téma a későbbiekben bővebben kifejtésre kerül, viszont, amit fontos megemlíteni, hogy a kommunikációs rendszerek segítenek a kommunikációs csatornák biztosításában, és lehetővé teszik a protokollok alkalmazását a tárgyak vagy dolgok, illetve a tárgyak internetének egyes elemei között.¹⁵

Az mellett a tény mellett sem szabad elmennünk, hogy az IoT eszközök korlátozott feldolgozási és energiaforrásokkal rendelkeznek, amelyek nem teszik lehetővé a komplex, helyszíni adatfeldolgozást. Pontosan ezért, az összegyűjtött adatokat általában nagyobb teljesítményű csomópontokra továbbítják, ahol a feldolgozás ténylegesen lehetségessé válik. A mai, modern technológiákat illetően a korábban is említett felhő technológia gyakorlatilag korlátlan feldolgozási lehetőségeket kínál.¹⁶ Végezetül, de nem utolsó sorban fontosnak tartom megemlíteni a szemantika fogalmát, ami nagyon szignifikáns pozíciót foglal el az IoT világában. A szemantika az IoT-ban tulajdonképpen arra a képességre utal, hogy a különböző gépek intelligensen tudják kinyerni a tudást a szükséges szolgáltatások nyújtása érdekében. A tudás kinyerése magában foglalja az erőforrások felfedezését és használatát, valamint az információk modellezését. Emellett magában foglalja az adatok felismerését és elemzését is. Így a szemantika lényegében az IoT agyát képviseli azáltal, hogy az igényeket a megfelelő erőforráshoz küldi.¹⁷

¹⁴ Al-Fuqaha és mtsai., „Internet of Things”.

¹⁵ Nallapaneni Manoj Kumar és Pradeep Kumar Mallick, „The Internet of Things: Insights into the Building Blocks, Component Interactions, and Architecture Layers”, *Procedia Computer Science* 132 (2018): 109–17, <https://doi.org/10.1016/j.procs.2018.05.170>.

¹⁶ Alessio Botta és mtsai., „Integration of Cloud Computing and Internet of Things: A Survey”, *Future Generation Computer Systems* 56 (2016. március): 684–700, <https://doi.org/10.1016/j.future.2015.09.021>.

¹⁷ Al-Fuqaha és mtsai., „Internet of Things”.

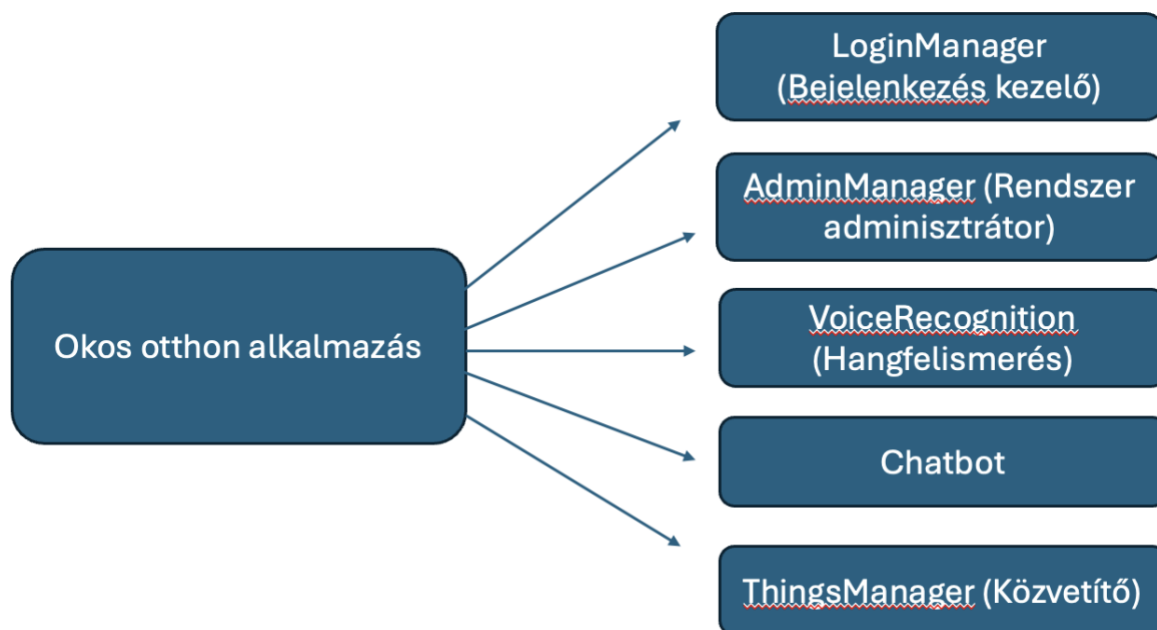
2.1 Az okos otthonok rendszere

Az okos otthonok architektúráját illetően alapvetően négy rétegre tudjuk osztani: Fizikai réteg, megjelenési réteg, hálózati réteg és alkalmazási réteg. A megjelenési réteg a fizikai eszközökkel gyűjtött adatok gyűjtéséért felelős. Az összegyűjtött adatok ezután továbbításra kerülnek a feldolgozó egységhez vagy alkalmazáshoz, és ez már a hálózati réteg feladata. Végül az alkalmazási rétegnek köszönhetően az adatok a végfelhasználótól függő interfészen keresztül jutnak el az alkalmazáshoz. A leggyakoribb példa erre az interfészre az okostelefon, vagy a táblagép. Az okoseszközök használatának növekedése a felhőbe feltöltött személyes adatok mennyiségének a növekedéséhez is vezetett. A probléma az, hogy az okos otthoni eszközök fejlődési üteme sokkal gyorsabbnak bizonyul, mint az olyan védelmi technikák fejlődése, amelyek megvédhetik ezeket az eszközöket és az általuk gyűjtött adatokat. Tekintettel az eszközök nagy kockázataira és a mindennapi élethez való kapcsolódásukra, rendkívül fontos megérteni az ezen eszközök által jelentett veszélyeket és kihívásokat, valamint azt, hogy ez egyáltalán hogyan kapcsolódik a magánéletünkhöz.¹⁸

Egy kutatás szerint az okos otthoni rendszer javasolt rendszerarchitektúrája öt részből tevődik össze, ez látható a kettes számú ábrán. Fontos, hogy webszolgáltatáson alapul, ebből adódóan a felhasználó, amikor nem tartózkodik a házban, akkor is tudja vezérelni az otthonát, csak éppen távolról. A rendszer telepíthető számítógépekre, táblagépekre és mobiltelefonokra is. Az első modul a Login Manager, ami gyakorlatilag a bejelentkezésekért felelős. A felhasználói engedélyezési és hitelesítési műveleteket kezeli. Ha megnézzük az ábrát, láthatunk egy újabb biztonsági komponenset, vagyis az Admin Managert, amelyet a rendszer adminisztrátora használ a felhasználók rendszerhez való hozzáféréseinek kezelésére. A ház készülékeinek vezérléséhez megadott jogosultságok között (azaz a hozzáférés típusa) lehet olvasás, írás vagy mindkettő. Az olvasási jogosultság lehetővé teszi az érzékelőadatok lekérdezését, míg az írási jogosultság lehetővé teszi a felhasználó számára, hogy kérést adjon le egy működtető eszközre. A harmadik modul a hangfelismerés, de ez akár opcionálisnak is tekinthető, hiszen nem feltétlenül biztos, hogy verbálisan szeretne kommunikálni a felhasználó a rendszerrel. Ezen felül láthatunk egy chatbot szolgáltatást is, amely két részre bomlik le. Egyrészt van olyan funkciója, ami a különböző célokkal foglalkozik, mert a bemeneti szöveget kanonikus

¹⁸ Lili Nemec Zlatolas, Nataša Feher, és Marko Hölbl, „Security Perception of IoT Devices in Smart Homes”, *Journal of Cybersecurity and Privacy*, 2022, <https://doi.org/10.3390/jcp2010005>.

kifejezéssé alakítja át, illetve tartalmaz egy olyan felismerő funkciót is, amely értelmezi a felhasználói kérést és megszerzi a chatbot választát. Az utolsó modul pedig a ThingsManager névre hallgat. Ez a webszolgáltatás felelős az utasítás továbbításáért az MQTT (Message Queue Telemetry Transport) brókerhez, amely az intelligens otthoni készülékeket felügyeli és vezérli. Az MQTT-ről a későbbiekben még további betekintést fog nyújtani a dolgozat.¹⁹



2. ábra: Az okos otthoni rendszer javasolt rendszerarchitektúrája, saját szerkesztés

Forrás: Rihab Fahd Al-Mutawa és Fathy Albourae Eassa, „A Smart Home System based on Internet of Things”, *arXiv e-prints*, 2020. szeptember 1., <https://doi.org/10.48550/arXiv.2009.05328>.

Az okos otthonok hálózata számos olyan alkalmazást tartalmaz, amelyek együttműködnek, hogy megfelelő szolgáltatásban legyen része a felhasználónak. Többek között megemlíthető a LED-vezérlés, amelynek segítségével a lámpákat fel és le lehet kapcsolni, valamint az izzó fényerejét is lehet szabályozni. Az elektromos készülékek is vezérelhetők, mint például az okos mosógépek, hűtőszekrények. A biztonsági vezérlés szintén kivitelezhető. Itt beszélhetünk többek között az ajtók nyitásáról, zárásáról, vagy akár a füstjelzőről és a mozgásérzékelőkről.

¹⁹ Rihab Fahd Al-Mutawa és Fathy Albourae Eassa, „A Smart Home System based on Internet of Things”, *arXiv e-prints*, 2020. szeptember 1., <https://doi.org/10.48550/arXiv.2009.05328>.

Bár ez nagyon kényelmes a felhasználók számára, ugyanakkor sebezhetőséget is jelenthet. Aggodalomra adhatnak okot többek között a hackerek, akik behatolhatnak az okoseszközökbe, és ezáltal kárt okozhatnak, például engedély nélkül kinyithatják az ajtókat, vagy kamerákon keresztül betekintést nyerhetnek a magánéletünkbe is. Sajnos ezek a szituációk nagy mértékben és negatívan befolyásolják a biztonságérzetünket, ami nem túl szerencsés, hiszen, ha otthon nem érezzük magunkat biztonságban, akkor felmerül a kérdés, hogy mégis hol tudnánk. ²⁰

²⁰ Yaser Al Mtawa és mtsai., „Smart Home Networks: Security Perspective and ML-based DDoS Detection”, in *2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)* (2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), London, ON, Canada: IEEE, 2020), 1–8, <https://doi.org/10.1109/CCECE47787.2020.9255756>.

2.2 Kommunikációs protokollok

Az IoT információ-kommunikációs technológiája (IKT) forradalmat hoz az ember-tárgy és tárgy-tárgy között történő információátvitelben. Az okos eszközök képesek összekapcsolódni, információt továbbítani és döntéseket hozni az emberek nevében. Ezen a ponton az interdependencia fogalmát is érdemesnek tartom megemlíteni, hiszen a végtelen kapcsolódásból adódóan megpróbáltatás elé kerülhetnek a felhasználók.

Az IoT-környezet hatalmas számú okos eszközből áll, de számos korlátozással. A feldolgozási képesség, a tárolási kapacitás, a rövid energiaellátás és a rádiótávolság is a korlátok közé tartozik, ezért az IoT megvalósításához olyan kommunikációs protokollokra van szükség, amelyek hatékonyan képesek kezelni ezeket a feltételeket. Az IoT-berendezés egyedi követelményeitől függően ugyanazon a hálózaton belül több kommunikációs protokollt is lehet használni a különböző interakciók megkönnyítésére. Az IoT-kommunikációs protokoll kiválasztása számos tényezőtől függ, például a használt eszközök típusától, a kívánt biztonsági szinttől és a hálózati korlátoktól. A megfelelő kommunikációs protokoll kiválasztásakor fontos figyelembe venni az IoT-projekt egyedi követelményeit és korlátait.²¹

Mivel az IoT-hálózatok tervezésekor az energiafogyasztás fontos tényező, az alacsony fogyasztású vezeték nélküli hálózati technológiák előnyösek. Ezeket a technológiákat két csoportba tudjuk sorolni:

- Alacsony energiaigényű nagy kiterjedésű hálózatok (Low Power Wide Area Networking- LPWAN), amelyek akár több kilométeres hatótávolságot biztosítanak, de a legtöbb esetben korlátozott adatátviteli sebességgel (többek között 6LoWPAN, LoRaWAN, Sigfox);
- Vezeték nélküli személyi hálózatok (Wireless Personal Area Networking- WPAN), akár 100 m-es hatótávolsággal (többek között Zigbee, RFID)²²

²¹ Shadi Al-Sarawi és mtsai., „Internet of Things (IoT) communication protocols: Review”, in *2017 8th International Conference on Information Technology (ICIT)* (2017 8th International Conference on Information Technology (ICIT), Amman, Jordan: IEEE, 2017), 685–90, <https://doi.org/10.1109/ICITECH.2017.8079928>.

²² Apostolos Gerodimos és mtsai., „IoT: Communication Protocols and Security Threats”, *Internet of Things and Cyber-Physical Systems* 3 (2023. január 1.): 1–13, <https://doi.org/10.1016/j.iotcps.2022.12.003>.

A 6LoWPAN, az IPv6 over Low-Power Wireless Personal Area Network rövidítése, amely egy olyan kommunikációs protokoll, ami lehetővé teszi az IPv6 csomagok átvitelét alacsony fogyasztású vezeték nélküli hálózatokon, amelyeket jellemzően az IoT alkalmazásaiban használnak. Célja, hogy lehetővé tegye az alacsony fogyasztású, erőforrás-korlátozott eszközök integrálását az Internetbe.²³

Miközben számos előnyt kínál az erőforrás-korlátozott IoT eszközök számára, biztonsági megfontolásokat is felvet. Többek között problémát okozhatnak a routing támadások. A 6LoWPAN-hálózatok útválasztási mechanizmusokra támaszkodnak az eszközök közötti csomagok továbbításában. Az útválasztási protokollok biztonsági sebezhetőségei különböző támadásokhoz vezethetnek, például útvonal-manipulációhoz, vagy feketelyuk-támadásokhoz, továbbá adatvédelmi aggályokról is beszélhetünk. A 6LoWPAN-hálózatok gyakran számos összekapcsolt eszközt tartalmaznak, amelyek érzékeny adatokat gyűjthetnek. Az adatvédelmi aggályok akkor merülnek fel, amikor ezeket az adatokat a hálózaton belül továbbítják, tárolják vagy feldolgozzák, és így azok a jogosulatlan hozzáférés vagy visszaélés potenciális célpontjává válnak.²⁴

A LoRaWAN (Low Range Wide Area Network) mellett sem mehetünk el, hiszen egy világszerte elterjedt IoT protokollról van szó, ami a Semtech Corporation által szabadalmaztatott LoRa technológián alapszik, amely lehetővé teszi az adatátvitelt nagy távolságokon keresztül, kevesebb energia felhasználásával. A LoRa csillag topológiájú hálózatot használ, amelyben az alkalmazáskiszolgáló nagyszámú átjáróhoz kapcsolódik. Ezek az átjárók pedig nagyszámú végberendezéshez kapcsolódnak. A LoRa architektúrája két fő részből áll. Az első rész a back-end és ez tartalmazza a hálózati szervert, amely az adatok tárolásáért felelős. A második a front-end, amely az átjárókat és a végberendezéseket tartalmazza. Ezek az átjárók a hálózati szerver és a végberendezések közötti híd szerepét töltik be. Az átjáró és a hálózati szerver között továbbított adatokat IP-kapcsolaton keresztül

²³ „IETF RFC 4919-2007 - IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals | Joinup”, elérés 2023. augusztus 17., <https://joinup.ec.europa.eu/collection/ict-standards-procurement/solution/ietf-rfc-4919-2007-ipv6-over-low-power-wireless-personal-area-networks-6lowpans-overview-assumptions>.

²⁴ Christine Hennebert és Jessye Dos Santos, „Security Protocols and Privacy Issues into 6LoWPAN Stack: A Synthesis”, *IEEE Internet of Things Journal* 1, sz. 5 (2014. október): 384–98, <https://doi.org/10.1109/JIOT.2014.2359538>.

továbbítják, az üzenetküldésben pedig a LoRaWAN jön segítségül. Tehát összességében elmondható, hogy a LoRa, maga a jel, amely az adatokat szállítja, a LoRaWAN pedig a kommunikációs protokoll, amely szabályozza és meghatározza, hogy az adatok hogyan kommunikálódnak a hálózaton keresztül.²⁵ A LoRaWAN előnyre törekvése mellett megjelennek azonban problémák is. Az adatátviteli sebesség növelése a magas biztonsági szint fenntartása mellett komoly kihívást jelent, és a megfelelő kompromisszum elérése egyáltalán nem egyszerű.

A SigFox technológia az LPWAN technológiacsalád része, amelyet elsősorban az IoT-hálózatok fejlesztésére használnak, amikor a küldött adatok mennyisége alacsony, a működési tartomány nagy, és az áramfogyasztás nagyon alacsony. A SigFox technológia által generált jelet nagy terület lefedésére is lehet használni, és a föld alatt található tárgyakra is lehet hatolni. A SigFox kommunikációs technológiát nagy kiterjedésű területek összekapcsolására hozták létre, vidéken több tíz kilométeres, városi területen pedig néhány kilométeres nagyságrendben.²⁶

Az IoT világában meglehetősen ismerősen csengő név a ZigBee, amely egy rádiófrekvenciás (RF) kommunikációs szabvány, amely az IEEE 802.15.4 szabványon alapul. A Zigbee-koordinátor felelős a hálózat létrehozásáért és fenntartásáért. Minden egyes elektronikus eszköz (pl. mosógép, TV, lámpa stb.) a rendszerben egy Zigbee-eszköz, amelyet a koordinátor kezel. Az eszközök közötti összes kommunikáció a koordinátoron keresztül jut el a célkészülékhez. A ZigBee vezeték nélküli jellege segít megoldani a meglévő otthoni automatizálási rendszerek korábban azonosított telepítési problémáját. A ZigBee szabvány elméletileg 250 kbit/s adatátviteli sebességet biztosít, és mivel a 40 kbit/s megfelel a legtöbb vezérlőrendszer követelményeinek, ez elegendő a legtöbb otthoni automatizálási eszköz vezérléséhez.²⁷ Mindenekelőtt a Zigbee sem kivétel, ugyanúgy találkozhatunk gyenge pontokkal biztonsági oldalról. A támadók a Zigbee-hálózatok sebezhetőségének kihasználásakor különböző célokat

²⁵ Jihen Souifi és mtsai., „Smart Home Architecture based on LoRa Wireless Connectivity and LoRaWAN® Networking Protocol”, in *020 1st International Conference on Communications, Control Systems and Signal Processing (CCSSP)* (2020 1st International Conference on Communications, Control Systems and Signal Processing (CCSSP), EL OUED, Algeria: IEEE, 2020), 95–99, <https://doi.org/10.1109/CCSSP49278.2020.9151815>.

²⁶ Alexandru Lavric, Adrian I. Petrariu, és Valentin Popa, „Long Range SigFox Communication Protocol Scalability Analysis Under Large-Scale, High-Density Conditions”, *IEEE Access* 7 (2019): 35816–25, <https://doi.org/10.1109/ACCESS.2019.2903157>.

²⁷ Khusvinder Gill és mtsai., „A zigbee-based home automation system”, *IEEE Transactions on Consumer Electronics* 55, sz. 2 (2009. május): 422–30, <https://doi.org/10.1109/TCE.2009.5174403>.

tűznek ki. A támadások fő típusai a felderítés, az eszközmanipuláció, a szolgáltatásmegtagadás (Denial of Service-DoS) és talán a legfontosabb, a hálózatrányítás.²⁸

A ZigBee-t követően az RFID-t is fontos megemlíteni. Az RFID (Radio Frequency Identification System) a rádiófrekvenciás azonosító rendszer rövidítése. Ez egy automatizált technológia, amely segít a különböző gépeknek azonosítani a tárgyakat, és rádióhullámok segítségével több más célgépet is vezérel. Az RFID olyan vezeték nélküli kommunikációs technológia, mint a WiFi és a Zigbee. Okos otthonokban például az ajtók nyitására és/vagy zárására is használható. Egy RFID-rendszer "címkéknek" (tag) nevezett adókból/válaszadókból és "olvasóknak" nevezett egyéb adókból/vevőkből áll. A nem védett címkék számos biztonsági tényezővel szemben sebezhetőek. Többféle kockázatnak vannak kitéve, például lehallgatásnak, hamisításnak, szolgáltatásmegtagadásnak, forgalomelemzésnek és még sok másnak. Bizonyos esetekben a hackerek le is másolhatják az RFID-eszköz hozzáférési vezérlését.²⁹

Kommunikációs protokollok esetében fontos kiemelni a korábban már szóba került átjárót. Az átjáró általában olyan eszköz, amely több kommunikációs protokollt támogat a végberendezésekkel való átjárhatóság érdekében. Elég nagy teljesítményű ahhoz, hogy a hálózat szélén elvégezzen néhány feldolgozási műveletet, mielőtt az adatokat a felhőbe küldené. Az átjáró egy biztonsági réteget is hozzáad az intelligens otthoni hálózathoz, mivel hidat képez a végberendezések és a külvilág közötti kommunikációban, és ezért minden kommunikáció szűrhető, mielőtt a parancsok eljutnak a végberendezésekhez (amelyek erőforrás-korlátozottak, alacsony energiaellátásúak, alacsonyabb biztonsági réteggel rendelkeznek, és ezért sebezhetőbbek a támadásokkal szemben). Ez lényegében a rendelkezésre állás, a megbízhatóság és a biztonság növelését teszi lehetővé. A felhő számos harmadik féltől származó szolgáltatással integrálható, mint például az adatmegjelenítés, az intelligens otthoni eszközközelés vagy a felhasználói hozzáférés és szerepkörök kezelése.³⁰

A korábban említett MQTT (Message Queue Telemetry Transport) protokoll is fontos szerepet tölt be az IoT világában. Lehetővé teszi az üzenetek küldését és fogadását anélkül, hogy a feladó vagy a címzett tudná, hogy ki küldi vagy fogadja az adatokat. Az MQTT-ben a kiszolgálónak

²⁸ Alireza Zohourian és mtsai., „IoT Zigbee Device Security: A Comprehensive Review”, *Internet of Things* 22 (2023. július 1.): 100791, <https://doi.org/10.1016/j.iot.2023.100791>.

²⁹ Al Mtawa és mtsai., „Smart Home Networks”.

³⁰ Mocrii, Chen, és Musilek, „IoT-Based Smart Homes”.

és a klienseknek (kommunikációra használt eszközök) nem kell tisztában lenniük egymás személyazonosságával. A kliens üzenetet kér a kiszolgálótól, hogy információt kapjon. Ezután az ügyfél (pl. valamilyen érzékelő, mobileszköz stb.) a bróker segítségével csatlakozhat a megadott kiszolgálóhoz. A bróker irányítja az információáramlást, és elsősorban az összes kiszolgálói üzenet összegyűjtéséért, rendezéséért, a kliensek kiválasztásáért és az üzenetek elküldéséért felelős az összes ügyfélnek. Az egészségügyi alkalmazások gyakran használják az MQTT-t.³¹

Ha megnézzük a biztonsági oldalát az MQTT-nek, a konfiguráció kihívást jelenthet. Az alapértelmezett hibás konfigurációval hagyott MQTT-kiszolgáló olyan, mint egy katasztrófa, amely csak arra vár, hogy bekövetkezhessen. Megdöbbentően sok, közel 67000 rosszul konfigurált MQTT-kiszolgáló érhető el nyilvánosan az interneten hitelesítés nélkül.³²

2.3 Következtetések

Összességében elmondható, hogy az okos otthonok komplex rendszerek, amelyek különböző kommunikációs protokollokat és eszközöket használnak. A kommunikációs protokollok valójában szabványosított módot biztosítanak az IoT eszközök számára az egymással, valamint a felhővel vagy más rendszerekkel történő kommunikációra, adatcserére.

Az okos otthonok IoT technológiára építése lehetővé teszi a háztartási eszközök automatizálását és távoli vezérlését. A rendszer négy fő rétegből áll: fizikai réteg, megjelenési réteg, hálózati réteg és alkalmazási réteg. Ezek mindegyike különböző funkciókat lát el a rendszerben. Azonban az IoT-rendszerek biztonságával kapcsolatban számos kihívásba ütközhetünk, mint például az adatvédelem, a hálózati sebezhetőség és az eszközök közötti biztonság kérdése.

³¹ Mohammad Mansour és mtsai., „Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions”, *Energies* 16, sz. 8 (2023. január): 3465, <https://doi.org/10.3390/en16083465>.

³² Joseph Anthraper és Jaidip Kotak, „Security, Privacy and Forensic Concern of MQTT Protocol”, *SSRN Electronic Journal*, 2019. január 1., <https://doi.org/10.2139/ssrn.3355193>.

3. IOT-VAL KAPCSOLATOS SZABÁLYOZÁSOK ÉS SZABVÁNYOK NEMZETKÖZI KÖRNYEZETBEN

Ahogy nőnek az IoT-val kapcsolatos biztonsági aggályok, úgy nő a vita a kormányzati szabályozás szükségességéről, hogy valóban fontosnak bizonyul-e. A korábbiakra hivatkozva, a ma forgalomban lévő IoT eszközöknél problémás a beépített biztonsági rendszer kérdése és ahogyan már említettem, ez veszélyeztetheti a fogyasztók magánéletét. Ettől függetlenül fogyasztói oldalról nem feltétlenül hallunk minden nap panaszról és igényről, hogy szabályozottabb keretek között működjön az IoT. Valójában a probléma gyökere abban lelhető fel, hogy mivel a fogyasztók többsége nem feltétlenül van tisztában ezen technológia veszélyeivel, érthető módon nem is vágnak nagyobb biztonságra és kontrolláltabb működésre. Ettől függetlenül a jelenlegi világunkban egyértelművé vált, hogy valamit tenni kell és pozitív hatása is tud lenni egy kormány általi szabályozásnak, hiszen az alkalmazott szabványok és törvények, elő tudják segíteni a fogyasztók védelmét, illetve a hiányosságok javítására vonatkozó követelmények kiterjesztése lehetőséget tud biztosítani a további incidensek megelőzésére. A másik oldalon viszont a kormány általi szabályozás nem feltétlenül az innováció barátja és mellette költséges is lehet, amely a kisebb cégeket ki tudja szorítani a piacról.³³ Egy dolog azonban biztos, fontos határokat húzni és szabályokat felállítani. Kutatásom alapján sajnos Magyarországon az IoT eszközökre egyelőre nem vonatkozik olyan kötelező jogi követelményrendszer, amely meghatározná legalább egy olyan alap védelmi szintet, amit kötelező biztosítani. Az tény, hogy vannak nemzetközi szabványok és ajánlások, amelyek tudnak iránymutatást adni, de valójában komolyabb szabályozásokig itthon egyelőre még nem jutottunk el.

Azáltal, hogy az IoT veszélyes oldalával is szembe kerülhetnek a fogyasztók, kritikusan fontos a különféle szabályozások és szabványok áttekintése, amelyek jelenleg érvényben vannak és próbálják a technológiát kordában tartani. Ezért ebben a fejezetben bemutatom az IoT-ra vonatkozó szabályozásokat és szabványokat nemzetközi környezetben a teljesség igénye nélkül. Külön ki fogok térni az Amerikai Egyesült Államokra, valamint az Európai Unióra, amelyek talán a legnagyobb vezetői szerepet töltik be a területen és a legnagyobb lépéseket teszik meg az élhetőbb IoT orientált jövő felé. Ezen felül a H1 hipotézisemre fogom keresni a

³³ Jennifer Fong, „Should the Government Regulate IoT Devices?”, *IEEE Innovation at Work* (blog), 2017. október 19., <https://innovationatwork.ieee.org/should-government-regulate-iot/>.

választ, miszerint az IoT biztonságának szabályozása erősebb az Amerikai Egyesült Államokban, mint az Európai Unióban.

3.1 Az USA szabályozása az IoT-ra

Ahogy az IoT technológiája fejlődött és hatékonyabb működést tudott elérni, egyre több és több fogyasztót szólított meg és kezdett el a mindennapok szerves részévé válni. Az IoT világához szorosan kapcsolódik a felhő technológia, amibe szintén egyre nagyobb mennyiségű adat kezdett el áramlani és tárolódni is. A felhőben tárolt jelentős mennyiségű adat egy igazán nagy motiváló erő tud lenni a támadók számára, ami az adatok ellopásához, valamint a magánélet és a tulajdonjogok megsértéséhez is vezethet. Pontosan ebből adódóan fellépett az igény arra, hogy valamilyen módon szabályozásra kerüljön az IoT, de valójában a szabályozás teljes mértékig országtól függ. Az Amerikai Egyesült Államokban nagy hangsúly helyeződik a magánélet és az adatok védelmére az IoT világában.³⁴

Az elnök által 2020. december 4-én aláírt, IoT Cybersecurity Improvement Act of 2020 (IoT CIA) az első olyan szövetségi törvény, amely az IoT eszközök biztonságát szabályozza. A célja az volt, hogy biztonságosabbá tegye az IoT használatát és megváltoztassa az eszközök gyártóinak, valamint a kormány számára azokat szállító vállalatoknak a helyzetét. Az új törvénytől azt várták, hogy a fogyasztói IoT-piacon is éreztesse majd a hatását, ami azt jelenti, hogy az IoT-alkatrészek és -termékek tervezésében, gyártásában és szállításában részt vevő valamennyi vállalatnak célszerű erősen gondolkodnia a biztonság beépítéséről az IoT-terméktervezésbe. Erre a törvényre az NIST (National Institute of Standards and Technology- Nemzeti Szabványügyi és Technológiai Intézet) nagy hatással volt.³⁵

A törvény olyan IoT eszközökre vonatkozik, amelyek egy ügynökség tulajdonában vagy ellenőrzése alatt állnak, és amelyek szövetségi információs rendszerhez kapcsolódnak, az NIST meghatározása szerint "egy végrehajtó ügynökség, egy végrehajtó ügynökség vállalkozója vagy egy másik szervezet által használt vagy működtetett információs rendszer". A törvény tiltja, hogy 2022. december 4. után IoT eszközöket szerezzenek be vagy használjanak, ha az adott

³⁴ Irjet Journal, „IRJET- Legal Regulations to Protect the Privacy and Data of IoT Technologies Users”, *IRJET*, 2020. január 1., https://www.academia.edu/44392468/IRJET_Legal_Regulations_to_Protect_the_Privacy_and_Data_of_IoT_Technologies_Users.

³⁵ Robin L. [D-IL-2 Rep. Kelly, „Text - H.R.1668 - 116th Congress (2019-2020): IoT Cybersecurity Improvement Act of 2020”, legislation, 2020. december 4., 2019-03-11, <https://www.congress.gov/bill/116th-congress/house-bill/1668/text>.

eszköz "nem felel meg" a Nemzeti Szabványügyi és Technológiai Intézet (NIST) által kidolgozott szabványoknak.³⁶

Ezen felül szintén fontos a Kalifornia állambeli California Consumer Privacy Act (CCPA). 2018. június végén Kalifornia elfogadott, egy olyan új adatvédelmi törvényt, amely nagyobb hatással lehet az amerikai vállalatokra, mint a 2018 májusában hatályba lépett Európai Unió Általános Adatvédelmi Rendelet (General Data Protection-GDPR). A kaliforniai törvény nem rendelkezik a GDPR néhány legterheesebb követelményével, például a szűk 72 órás ablakkal, amelyen belül a vállalatnak jelentenie kell a jogsértést, viszont más tekintetben még ennél is tovább megy.

A CCPA a GDPR-nál tágabban értelmezi a személyes adatok fogalmát. Tehát a biztonság számára a kihívást az jelenti, hogy felkutassa és biztosítsa ezeket a személyes adatokat. A California Consumer Privacy Act egy olyan törvény, amely lehetővé teszi bármely kaliforniai fogyasztó számára, hogy követelhesse, az összes olyan információ láthatását, amelyet egy vállalat róluk tárolt, valamint az összes olyan harmadik fél teljes listáját, akikkel az adatokat megosztották. Ezenkívül a kaliforniai törvény lehetővé teszi a fogyasztók számára, hogy bepereljék a vállalatokat, ha megsértik az adatvédelmi irányelveket, még akkor is, ha nem történt jogsértés.

Kiegészítés képpen a California Privacy Rights Act (CPRA) egy 2020. november 3-án elfogadott, az egész államra kiterjedő adatvédelmi törvényjavaslat. A CPRA kihangsúlyozza, hogy Kalifornia az Egyesült Államokban az adatvédelmi jogszabályok élvonalába tartozik, mivel jelentősen kibővíti a CCPA-t és megerősíti a kaliforniai lakosok jogait. Ez azt jelenti, hogy szigorítja a személyes adatok felhasználására vonatkozó üzleti szabályokat, és létrehoz egy új, az egész államra kiterjedő adatvédelmi jogérvényesítéssel foglalkozó kormányzati ügynökséget, a California Privacy Protection Agency-t (CPPA). A kaliforniai adatvédelmi törvény (CPRA) 2023. január 1-jén lépett teljeskörűen hatályba, 2023. július 1-jén kezdődő végrehajtással, amelynek keretein belül egészen 2022. január 1-jéig visszatekintve nézik át az összegyűjtött adatokat, hogy megfelelnek-e a felállított követelményeknek.³⁷

³⁶ PricewaterhouseCoopers, „Three Actions IoT Device Manufacturers Can Take Now to Get Ahead of the New Federal Law”, PwC, elérés 2023. augusztus 30., <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/iot-cyber-improvement-act.html>.

³⁷ „California Consumer Privacy Act (CCPA)”, State of California - Department of Justice - Office of the Attorney General, 2018. október 15., <https://oag.ca.gov/privacy/ccpa>.

Fontosnak tartom megemlíteni, hogy bár az Amerikai Egyesült Államok konzekvensen próbál előrelépést eredményezni az IoT biztonsága terén, az IoT eszközök gyors fejlődése és elterjedése miatt továbbra is egy folyamatos kihívást jelentő problémáról beszélünk.

3.2 Az Európai Unió szabályozása az IoT-ra

Nemcsak az Egyesült Államokban, hanem Európában is feltörekvőben van az IoT témaköre és több megmozdulás is zajlik annak érdekében, hogy egy biztonságosabb környezetet lehessen megteremteni.

A 2021-től hatályos EU Cybersecurity Act megerősíti az EU kiberbiztonsági ügynökségét (ENISA - European Union Agency for Cybersecurity), és létrehozza az IKT termékek és szolgáltatások kiberbiztonsági tanúsítási keretrendszerét.³⁸

Az Unió kiberbiztonsági intézkedéscsomag megkönnyíti a kockázatalapú tanúsítási rendszerek létrehozását, amelyek a szabályok, a kiberbiztonsági szabványok, a műszaki követelmények és eljárások átfogó rendszerét alkotják. Mindez lehetővé teszi az eladók számára az Unió határain átnyúló kereskedelmet, és támogatja a felhasználókat abban, hogy megértsék a termék biztonsági jellemzőit. Jelenleg, amikor megbízunk a termékekben, egyben a gyártó jóindulatában bízunk, ami az igazat megvallva nem biztos, hogy a legokosabb döntés és nem is célravezető. Az ENISA tanúsítással kapcsolatos erőfeszítéseit tekintve, az a végső cél vezérli, hogy növelje az eszközökbe vetett bizalmat és biztonságosabbá tegye a termékeket azáltal, hogy a bizalmi horgonyt az EU által elismert tanúsító testületekre helyezi át. Az EU kiberbiztonsági törvénye a termékek és szolgáltatások felhasználási módja alapján történő kategorizálására helyezi a hangsúlyt. Ez a kategorizálás viszonylag érthetővé teszi a kiberbiztonsági követelmények, a vonatkozó szabványok, a műszaki előírások, az értékelési módszerek és a megbízhatósági szint meghatározásának feladatát. Az EU kiberbiztonsági törvénye szerint az alapvető megbízhatósági szintre vonatkozó önértékelési folyamat csökkenti a triviális termékek tanúsításával járó többletköltségeket. Az EU által elismert tanúsítvány ideális esetben három olyan megbízhatósági szintre esik, amelyek megfelelnek az IoT eszköz rendeltetésszerű használatához kapcsolódó kockázati szintnek, és tükrözik a piaci igényeket (idő, költség és teljesítmény). Az ENISA azt ajánlja, hogy a meglévő (európai és nemzetközi) műszaki előírásokat és szabványokat használják vezérelvként a megbízhatósági szintek, az

³⁸ „Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA Relevance)”, elérés 2023. szeptember 1., <https://eur-lex.europa.eu/eli/reg/2019/881/oj>.

uniós megfelelőségi nyilatkozat és a tanúsítás alapszintjének meghatározásához. Ez lehetővé teszi a megkülönböztetésmentes, közös normákkal rendelkező, a nemzetközi együttműködést elősegítő tanúsítási rendszer kialakítását.³⁹

Az Európai Unió esetében nagyon lényeges szempont megemlíteni a Cyber Resilience Act (CRA) törvényjavaslatot. A Bizottság új, a kiberbiztonságról szóló jogszabályra irányuló javaslata a digitális komponensű termékeket és szoftvereket vásárló vagy használó fogyasztók és vállalkozások védelmét célozza. A törvényjavaslat értelmében az ilyen termékek gyártóira és kiskereskedőire vonatkozó kötelező kiberbiztonsági követelmények bevezetésével a nem megfelelő biztonsági jellemzők a múlté válnának, és ez a védelem a termék teljes életciklusára kiterjedne. A javasolt rendelet által kezelt probléma kettős. Az első a sok termékben rejlő nem megfelelő szintű kiberbiztonság, illetve az ilyen termékek és szoftverek korábban is említett nem megfelelő biztonsági frissítése. A második az, hogy a fogyasztók és a vállalkozások jelenleg nem tudják meghatározni, hogy mely termékek biztonságosak, illetve nem tudják azokat úgy beállítani, hogy kiberbiztonsági oldalról védve legyenek.⁴⁰

Az új EU Cyber Resilience Act (CRA) az alábbiakat garantálná többek között:

- Harmonizált szabályokat a digitális komponensű termékek vagy szoftverek forgalomba hozatalakor;
- A kiberbiztonsági követelmények keretrendszerét, amely az ilyen termékek tervezését, kialakítását, fejlesztését és karbantartását szabályozza, az értéklánc minden szakaszában teljesítendő kötelezettségekkel;
- Az ilyen termékek teljes életciklusára vonatkozó gondossági kötelezettség.
- A javasolt rendelet hatálybalépésekor az Internethez kapcsolódó szoftverek és termékek CE-jelöléssel látnák el azokat, amelyek megfelelnek az új szabványoknak.

A rendelet minden olyan termékre vonatkozna, amely közvetlenül vagy közvetve kapcsolódik egy másik eszközhöz vagy hálózathoz, kivéve a meghatározott kivételeket, például a nyílt forráskódú szoftvereket vagy szolgáltatásokat, amelyekre már a meglévő szabályok

³⁹ Anum Khurshid és mtsai., „EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme”, *IEEE Access* 10 (2022): 129932–48, <https://doi.org/10.1109/ACCESS.2022.3225973>.

⁴⁰ „European Cyber Resilience Act (CRA)”, elérés 2023. szeptember 7., <https://www.european-cyber-resilience-act.com/>.

vonatkoznak, mint például az orvostechnikai eszközökre, a légi közlekedésre vagy például a gépjárművekre.⁴¹

Ha tovább megyünk, akkor a GDPR is egy érdekes pont lehet. Bár a GDPR (General Data Protection Regulation - Általános Adatvédelmi Rendelet) az Európai Unió által az egyének magánéletének és személyes adatainak védelme érdekében hozott rendelet és nem kifejezetten az IoT biztonságára vonatkozik, mégis fontosnak tartom megemlíteni, hiszen a rendelet az IoT eszközökkel kapcsolatos biztonsági és adatvédelmi aggályokkal is foglalkozik azáltal, hogy előírja a szervezetek számára a megfelelő biztonsági intézkedések végrehajtását és az adatgyűjtéshez való kifejezett hozzájárulás megszerzését.

Valójában ez egy átfogó adatvédelmi törvény, amelyet az Európai Unió 2018-ban léptetett életbe és minden uniós tagállamra vonatkozik, valamint széles alkalmazási körrel rendelkezik. A GDPR extraterritoriális hatályú, ami azt jelenti, hogy az EU-n kívüli szervezetekre is vonatkozik, ha azok az Európai Unióban lakók személyes adatait dolgozzák fel, miközben árukat vagy szolgáltatásokat kínálnak nekik, vagy az EU-n belüli viselkedésüket figyelik. Ez biztosítja, hogy az uniós polgárok adatai védelmet élveznek, függetlenül attól, hogy hol történik a feldolgozásuk.⁴²

Az Európai Unió ösztönzi a tagállamokat és a szervezeteket az együttműködésre, továbbá az információcserére és az IoT-val kapcsolatos biztonsági kihívások hatékony kezelésére. Pontosan ezért, az EU-n belül szintén megemlítendő a NIS irányelv továbbfejlesztett változata a NIS2 direktíva, amely először foglalkozik az IKT-ellátási lánc kiberbiztonságával, ami az IoT esetében különösen fontos pont.⁴³

Összességében elmondható, hogy az Európai Unió olyan stratégiát alkalmaz, amely a jogalkotást, a tanúsítást, a különféle iránymutatásokat és az együttműködést ötvözi az IoT-ra

⁴¹ „EU Cyber Resilience Act | Shaping Europe’s Digital Future”, elérés 2023. szeptember 7., <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>.

⁴² „What Is GDPR, the EU’s New Data Protection Law?”, GDPR.eu, 2018. november 7., <https://gdpr.eu/what-is-gdpr/>.

⁴³ „EUR-Lex - 32022L2555 - EN - EUR-Lex”, elérés 2023. szeptember 8., <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>.

épülő intelligens eszközök biztonságának fokozása érdekében. Ezen felül a felhasználók magánéletének és adatainak védelme szintén nagyon fontos szerepet tölt be.

3.3 Nemzetközi szabványok

Több olyan szabvány is van, amiről fontos beszélni, hiszen nemzetközi szinten alkalmazható iránymutatásokat kaphatunk. Ilyen többek között a NISTIR 8259 szabvány. Célja, hogy a gyártóknak ajánlásokat adjon az általuk gyártott IoT eszközök biztonságosságának javítására. Ez azt jelenti, hogy az IoT eszközök olyan kiberbiztonsági képességeket, jellemzőket, vagy funkciókat kínálnak, amelyeket az eszközök hardverén és szoftverén keresztül biztosítanak, és amelyekre az ügyfeleknek, szervezeteknek és magánszemélyeknek egyaránt szükségük van az eszközök biztonsága érdekében, amikor azokat a rendszereikben és környezetükben használják. Az IoT eszközök gyártóinak gyakran olyan műveleteket is el kell végezniük, vagy olyan szolgáltatásokat kell nyújtaniuk, amelyeket ügyfeleik elvárnak és/vagy amelyekre szükségük van az eszköz kiberbiztonságának megtervezéséhez és fenntartásához a rendszereikben és környezetükben. A szabvány hat ajánlott alapvető kiberbiztonsági tevékenységet ismertet, amelyeket a gyártóknak érdemes megfontolniuk az általuk gyártott új IoT eszközök biztonságának javítása érdekében. Ezek közül négy elsősorban a gyártó által az eszköz forgalomba hozatala előtt, a fennmaradó két tevékenység pedig elsősorban az eszköz forgalomba hozatala után hozott döntésekre és intézkedésekre van hatással. Az alábbi hat pontot érdemes figyelembe venni:

- Biztonságos eszközkonfiguráció: A gyártóknak biztosítaniuk kell, hogy az alapértelmezett beállítások biztonságosak legyenek, és lehetővé tegyék a felhasználók számára az egyszerű, de biztonságos konfigurálást.
- Támadások elleni védelem: Az IoT-eszközöknek védekező mechanizmusokkal kell rendelkezniük, beleértve a tűzfalakat, az eszközazonosítást és az eseménynaplózást.
- Adatvédelem az eszközön: Az IoT-eszközök esetében alapvető fontosságú, hogy megfelelően védjék a rajtuk tárolt érzékeny adatokat, például titkosítás és hitelesítés révén.
- A biztonsági frissítések kezelése: Az IoT-eszközöknek képesnek kell lenniük a biztonsági frissítések fogadására és telepítésére, hogy reagálni tudjanak az új fenyegetésekre és sebezhetőségekre.
- A hálózati kapcsolatok biztonsága: Az IoT-eszközöknek biztonságosan kell kommunikálniuk a hálózaton keresztül, beleértve a titkosított kommunikációt és azonosítást.

- A támadások észlelése és az azokra való reagálás: Az IoT-eszközöknek képesnek kell lenniük a támadások korai észlelésére és a megfelelő válaszlépések elindítására, beleértve az eseménynaplózást és a jelentéstételt.

Mind a hat tevékenység elvégzése segíthet a gyártóknak olyan IoT eszközöket biztosítani, amelyek jobban támogatják az IoT eszköz vásárlóinak kiberbiztonsággal kapcsolatos erőfeszítéseit, ami viszont csökkentheti az IoT eszközök veszélyeztetettségének gyakoriságát és súlyosságát, valamint a veszélyeztetett IoT eszközökkel végrehajtott támadásokat. Ezen tevékenységek célja, hogy illeszkedjenek a gyártó meglévő fejlesztési folyamatába, és részben vagy egészben már megvalósulhatnak a meglévő folyamat során. ⁴⁴

Kiegészítésképpen érdemes néhány szót említeni a NISTIR (NIST Internal/Interagency Reports) 8259A-ról is. A NISTIR 8259 és 8259A bár kiegészíti és megerősíti a másikat, az NIST úgy döntött, hogy az iránymutatást két különálló kiadványban adja ki. Ez nagyrészt a gyártók visszajelzésein alapult, hogy növelje az egyértelműséget és megkönnyítse az egyszerű elfogadást. A NISTIR 8259A dokumentumban szereplő alapvető vonal a közös kiberbiztonsági ellenőrzések támogatásához általánosan szükséges eszközképességekből áll, amelyek célja a szervezet eszközeinek, adatainak, rendszereinek és ökoszisztémáinak védelme. Ez egy olyan létfontosságú alapot biztosít, amelyre iparág- és piacspecifikus irányvonalat lehet kialakítani. ⁴⁵

Európai viszonylatban talán az egyik leginkább kiemelkedő szabvány az ETSI EN 303 645. Az IoT-ra vonatkozó első globálisan alkalmazható szabványt a TC CYBER 2019 februárjában adta ki, és ez került továbbfejlesztésre a 2020 júniusában kiadott ETSI EN 303 645 tükrében. Az ETSI EN 303 645 célja, hogy megelőzze az okoseszközök elleni nagyszabású, elterjedt támadásokat, amelyekkel a kiberbiztonsági szakértők nap mint nap találkoznak, azáltal, hogy biztonsági alapszintet hoz létre az összekapcsolt fogyasztói termékek számára, és alapot biztosít a jövőbeli IoT-tanúsítási rendszerekhez. Ez a szabvány a biztonság beépítését írja le az IoT-termékek tervezésétől kezdve (security by design), ahelyett, hogy a biztonsági intézkedéseket csak a végén, kényelmetlenül rácsavaroznák. Az ETSI EN 303 645 támogatja a csatlakoztatott fogyasztói termékek megfelelő biztonsági alapszintjét. 13 ajánlást tartalmaz, amelyek közül a három legfontosabb az alábbiak: nincsenek alapértelmezett jelszavak, a sebezhetőségek

⁴⁴ Michael Fagan és mtsai., „Foundational Cybersecurity Activities for IoT Device Manufacturers” (National Institute of Standards and Technology, 2020), <https://doi.org/10.6028/NIST.IR.8259>.

⁴⁵ Michael Fagan és mtsai., „IoT Device Cybersecurity Capability Core Baseline” (National Institute of Standards and Technology, 2020. május 29.), <https://doi.org/10.6028/NIST.IR.8259A>.

nyilvánosságra hozatalára vonatkozó politika bevezetése és a szoftverek folyamatos frissítése. A fogyasztói IoT eszközökre vonatkozóan külön adatvédelmi rendelkezések is léteznek. A tárgykörbe tartozó IoT-termékek közé tartoznak a csatlakoztatott gyermekjátékok és bébiőrök, a biztonság szempontjából fontos csatlakoztatott termékek, például füstérzékelők és ajtózárok, intelligens kamerák, televíziók és hangszórók, viselhető egészségmegőrző eszközök, csatlakoztatott otthoni automatizálási és riasztórendszerek, csatlakoztatott készülékek (pl. mosógépek, hűtőszekrények) és intelligens otthoni asszisztensek.⁴⁶

Ezen szabványhoz kapcsolódóan érdemes megemlíteni kiegészítés gyanánt a TR 103 621-et és a TS 103 701-et. A TR 103 621 egy könnyen használható végrehajtási útmutatást ad a gyártók és más érdekelték számára, hogy segítse őket az ETSI EN 303 645 szabványban a fogyasztói IoT eszközökre vonatkozóan meghatározott rendelkezések teljesítésében. A TS 103 701 pedig egy megfelelőségi előírás, amelyet 2021 augusztusában tettek közzé. Az értékelési specifikáció meghatározza a fogyasztói IoT-termékek ETSI EN 303 645 szabvány rendelkezései alapján történő értékelésére szolgáló alapvető megfelelőségértékeléseket.⁴⁷

Az ISO (International Organization for Standardization, magyarul Nemzetközi Szabványügyi Szervezet) szabványosítási tevékenysége is folyik nemzetközileg az IoT biztonsága terén. Létezik egy szabvány, amely kiterjeszti a dolgok internetének biztonságára vonatkozó elveket, és útmutatást nyújt az elvekről, a kockázatokról, valamint a megfelelő információbiztonsági és adatvédelmi ellenőrzésekről, amelyekkel a dolgok internetének kockázatai csökkenthetők. Ez a szabvány az ISO/IEC 27400 Cybersecurity-IoT security and privacy-Guidelines, amely 2022-ben látott napvilágot. Ez az új szabvány tulajdonképpen az IoT-ra vonatkozó "kockázati források" és "kockázati forgatókönyvek" sorát határozza meg. Ezután ésszerű alapot javasol a kockázatok mérséklésére szolgáló biztonsági és adatvédelmi ellenőrzések kiválasztásához.⁴⁸

⁴⁶ „ETSI EN 303 645 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements” (ETSI, 2020. június), https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf.

⁴⁷ Sabine Dahmen-Lhuissier, „Consumer IoT Security”, ETSI, elérés 2023. szeptember 1., <https://www.etsi.org/technologies/consumer-iot-security>.

⁴⁸ Darine Ameyed és mtsai., „Quality and Security Frameworks for IoT-Architecture Models Evaluation”, *SN Computer Science* 4, sz. 4 (2023. május 15.): 394, <https://doi.org/10.1007/s42979-023-01815-z>.

A kutatásom során készítettem egy táblázatot dolgozatom harmadik fejezetéből, amely összefoglalja a legfontosabb tudnivalókat az említett jogszabályokról, szabványokról és törvényjavaslatról.

Törvény/szabvány/törvény javaslat	Cél	Földrajzi alkalmazhatóság	Célközönség
IoT Cybersecurity Improvement Act of 2020	Az USA kormánya által használt IoT eszközök kibiztonságának javítása	USA	IoT-eszközöket beszerző és használó szövetségi ügynökségek.
California Consumer Privacy Act (CCPA)	Kaliforniai lakosok adatvédelmi jogait biztosítja, és kötelezettségeket ró a személyes adatokat gyűjtő vállalkozásokra	Kalifornia Állam	Kaliforniai lakosok személyes adatait gyűjtő és feldolgozó vállalkozások.
California Privacy Rights Act (CPRA)	CCPA-ra épül, és a magánélethez fűződő jogokat további védelmek létrehozásával erősíti	Kalifornia Állam	Kaliforniai lakosok személyes adatait gyűjtő és feldolgozó vállalkozások.
EU Cybersecurity Act	Célja az uniós kibiztonsági keretrendszer megerősítése. Keretet hoz létre a közös kibiztonsági tanúsítási rendszerekhez, beleértve az IoT-hoz kapcsolódó eszközöket is	Európai Unió tagországok	EU-tagállamok, kibiztonsági tanúsító hatóságok és piaci szereplők
Cyber Resilience Act	EU-n belüli kritikus információs infrastruktúrák ellenálló képességének fokozására összpontosít. Alapvető szolgáltatások, beleértve az IoT-ra támaszkodó szolgáltatásokat is, biztonságosak és ellenállóak legyenek a kiberfenyegetésekkel szemben	EU	Gyártók
General Data Protection (GDPR)	Átfogó adatvédelmi rendelet, amely minden személyes adatra vonatkozik, beleértve az IoT-eszközök által gyűjtött adatokat is	EU tagállamaiban és az EU-n kívüli, az uniós polgárok személyes adatait kezelő szervezetek számára.	Az uniós polgárok személyes adatait kezelő szervezetek, köztük vállalkozások és hatóságok.
NIS2	Célja a hálózati és információs rendszerek biztonságának fokozása az egész EU-ban. A rendelet az IoT-val kapcsolatos szolgáltatásokra és üzemeltetőkre vonatkozó incidensjelentéssel, biztonsági követelményekkel és kockázatkezeléssel kapcsolatos rendelkezéseket is tartalmaz	Európai Unió tagországok	EU-tagállamok, az alapvető szolgáltatások üzemeltetői és a digitális szolgáltatók.
NISTIR 8259 és 8259A	Útmutatást nyújt az IoT-ra épülő eszközök kibiztonsági képességeiről. A 8259A a 8259-re épül,	Nemzetközi	IoT-eszkögyártók, -fejlesztők
ETSI EN 303 645	Meghatározza a fogyasztói IoT-ra vonatkozó alapvető biztonsági követelményeket	Nemzetközi	IoT-eszkögyártók, -fejlesztők
ISO/IEC 27400	IoT-eszközökkel, hálózatokkal és szolgáltatásokkal kapcsolatos biztonsági és adatvédelmi szempontokra összpontosít	Nemzetközi	Az IoT-val kapcsolatos tevékenységekben világszerte részt vevő szervezetek.

1. Táblázat: Összefoglaló az IoT biztonságának szabályozásáról (saját szerkesztés, forrás: TDK dolgozatom)

Összegezve, megállapítható, hogy a hatékony IoT biztonsági szabványok kialakításához nemzetközi együttműködésre van szükség. Bár a vélemények eltérnek, hiszen ahogyan említettem is, a szabályozások közbe tudnak szólni, ami a fejlődést és az innovációt érinti, de a másik oldalon pedig pontosan az bizonyosodik be, hogy szükség van a szabályozásokra és szabványokra, amit a sérülékenységek és ezeket kihasználó konstansan növekvő támadások száma tökéletesen alá is tud támasztani. Számos szakértő, a kormányok, az iparági érdekeltek és a szabványügyi szervezetek még nagyobb mértékű bevonása igazán fontos, annak érdekében, hogy olyan átfogó és világszerte elismert biztonsági keretrendszereket dolgozzanak ki, amelyek az IoT biztonságának meglehetősen sokrétű kihívásait kezelni tudják.

3.4 Következtetések

Az IoT eszközök biztonságával kapcsolatos aggályok és problémák egyre nőnek, és ezek valós veszélyeket jelenthetnek a fogyasztók magánéletére és a kiberbiztonságra. Itt lép életbe a kormányzati szabályozás szükségessége, viszont az IoT szabályozásának bevezetése mellett felmerül az innováció gátlásának veszélye, valamint a kisebb vállalatok piaci helyzetének megnehezítése. Ebből adódóan fontos az egyensúly megtalálása az innováció ösztönzése és a biztonság megteremtése között.

Szabályozás tekintetében az Amerikai Egyesült Államokban számos jogszabály és törvény van az IoT biztonságára vonatkozóan, ilyen többek között például az IoT Cybersecurity Improvement Act of 2020, vagy a California Consumer Privacy Act (CCPA). Ezek fő célja a biztonságosabb IoT-eszközök elősegítése. Emellett az Európai Unió is szigorúbbá teszi az IoT biztonságát, többek között az EU Cybersecurity Act és a Cyber Resilience Act révén.

Az IoT-biztonság területén nemzetközi szabványok is elérhetőek, például az ETSI EN 303 645, amely az IoT eszközök biztonsági alapszintjét határozza meg.

Ezek a következtetések azt mutatják, hogy az IoT biztonsága egy fontos és aktuális probléma, amelyre kormányok és nemzetközi szervezetek is egyre inkább reagálnak a jogszabályok és iránymutatások kifejlesztésével, hogy megvédjék a fogyasztókat és az adatokat az IoT-kapcsolatú eszközökkel szembeni kiberfenyegetésektől.

Tehát az eddigiek alapján elmondható, hogy a H1 hipotézisem, miszerint az IoT biztonságának szabályozása erősebb az Amerikai Egyesült Államokban, mint az Európai Unióban nem igazolódott be, hiszen összességében elmondható, hogy a szigorúság mértéke a megfelelő jogszabályok és azok végrehajtása alapján változik mind az USA-ban, mind az EU-ban. Az IoT szabályozása folyamatosan alakul és fejlődik, mindkét régió igyekszik lépést tartani a technológiai változásokkal, valamint a biztonsági kihívásokkal. Különbségek voltak, vannak és valószínűleg lesznek is a jövőben, de mivel egy folyamatosan változó területről és két erős befolyású régióról beszélünk, nem lehet egy egyértelmű nyertest kihozni.

4. IOT ESZKÖZÖK SÉRÜLEKENYSÉGEI ÉS EZEK KIHASZNÁLÁSÁT CSÖKKENTŐ VÉDELMI INTÉZKEDÉSEK

Korábban is szó esett arról, hogy az IoT eszközök az okos otthonok keretében számos kényelmi funkciót látnak el, de sajnos mindemelett rengeteg sebezhetőséggel is járhatnak. Ezen sebezhetőségek kihasználása a magánélet védelmének megsértéséhez, biztonsági fenyegetésekhez, sőt egyes esetekben akár fizikai sérülésekhez is vezethetnek. Folyamatosan növekszik az okos otthonokban található eszközök száma és így a lehetséges sebezhetőségeket kihasználó támadások száma is növekvő tendenciát mutat. Ezért ebben a fejezetben keresni fogom a választ H2 hipotézisemre, miszerint új sérülékenységeket és az azokat kihasználó támadási típusokat ismerhetünk meg az IoT világában.

A biztonság fontosságának szellemében hat kulcsfontosságú biztonsági célkitűzést is meg lehet fogalmazni. Nem meglepő módon a CIA (Confidentiality-Integrity-Availability, bizalmasság-sértetlenség-rendelkezésre állás) háromszög az alapja ezen területnek is, viszont fontos kiemelni a továbbiakban a hitelességet, az engedélyezést, valamint a letagadhatatlanságot is.

A hitelesség az okos eszközök személyazonosságának ellenőrzését takarja a rosszindulatú használat és a backdoor-ok megakadályozása érdekében, míg az engedélyezés a hozzáférési jogokat határozza meg a rendszeren belüli entitások számára a hozzáférés ellenőrzése érdekében. Végül a letagadhatatlanság biztosítja a tagadhatatlan bizonyítékokat bármely entitás állításainak valóságának ellenőrzésére.

Amikor meg szeretnénk vizsgálni a sérülékenységeket és az azok kihasználásra irányuló kibertámadásokat, érdemes két nagy kategóriába sorolni őket: Megkülönböztethetünk passzív és aktív támadásokat. A passzív támadások során a rendszer erőforrásainak befolyásolása nélkül próbálnak információt szerezni a támadók. Ez azt jelenti, hogy nem az adatok módosítása a cél, hanem az, hogy tanuljon belőle valamit a támadó. Passzív támadásra lehet példa többek között a lehallgatás, vagy a forgalomelemzés is. Az aktív támadások célja viszont az, hogy a rendszer erőforrásai megváltoztatásra kerüljenek, vagy a rendszer működését megzavarják. Ezen

támadástípusra jó példa lehet az üzenetmódosítás, a szolgáltatásmegtagadás és a rosszindulatú szoftveres támadások indítása is.⁴⁹

Technológiai oldalról sok sérülékenységet meg lehet nevezni, amely az okos otthonokban található IoT eszközöknél elő tud fordulni, de összefoglalva talán elmondható az ENISA riportja alapján, hogy a gyenge jelszavak magasan az elsődleges problémák között szerepelnek és ez egy tökéletes alapja tud lenni például a bruteforce támadások megkísérlésének. Szintén hatalmas kihívást jelentenek a hibás, vagy elmaradó frissítések, amelyek a malwareket támogatják. Továbbá fontosnak tartom megemlíteni a felsorolásban az IoT eszközök nem megfelelő módon történő konfigurálását, ami lehetővé teszi a man-in-the-middle támadásokat és nem mellesleg az adatvédelem is kihívást tud okozni.⁵⁰

A technológia sok megpróbáltatás elé tudja állítani a felhasználókat, de végső soron az IoT világában is az ember a leggyengébb láncszem és tulajdonképpen ez már önmagában is sérülékenységet tud jelenteni. A legnagyobb fejtörést a hiányzó tudatosság okozza, aminek köszönhetően olyan fontos dolgok sem kapnak kellő figyelmet, mint az erős jelszavak beállítása. Természetesen a social engineering jelentős mértékben kiveszi a részét az ember okozta problémákból, de ebben nem egyedülálló az IoT, hiszen mindenfajta célú kibertámadás esetén kihívást okoz az emberek manipulálhatósága.

Az emberi naivitásra sajnos nincs tökéletes ellenszer. A viselkedésünk soha nem lesz 100%-ban biztonságos, ami a technológiáról ugyanúgy elmondható. A technológia elképesztő sebességgel halad előre, a kiberbűnözők azonban pont ekkora lendülettel próbálják felvenni a versenyt. Ebből adódóan mind a szervezeteknek és mind a magánszemélyeknek képzettnek és felkészültnek kell lenniük saját biztonságuk fenntartására. A technológiai kultúra valójában lassabb, mint a fejlődése és erre komoly figyelmet kell fordítani. A social engineeringet alkalmazó bűnözők potenciális fenyegetést jelentenek a technológiai világra, mivel a biztonsági rendszerek jelentős előrelépést tettek az adatok védelmében. A hackeléshez elengedhetetlen a technikai tudás, míg a social engineering nem feltétlenül igényli, és jobb megtérüléssel jár. A social engineerek ahelyett, hogy a biztonsági rendszereket támadnák, e rendszerek felhasználóihoz, tulajdonosaihoz fordulnak, és rajtuk keresztül szereznek meg fontos

⁴⁹ Zaid Shouran, Ahmad Ashari, és Tri Priyambodo, „Internet of Things (IoT) of Smart Home: Privacy and Security”, *International Journal of Computer Applications* 182 (2019. február 15.): 3–8, <https://doi.org/10.5120/ijca2019918450>.

⁵⁰ „ENISA Threat Landscape 2022”, Report/Study, ENISA, elérés 2023. október 15., <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>.

információkat. Az IoT nagyszerű lehetőség lehet a social engineerek számára, mert bekapcsolódnak az emberi interakciókba. A megelőzéshez és a kockázatok mérsékléséhez szükség van tudatosságra, ami egy folyamatos cselekvés kell, hogy legyen, mivel a támadások típusai állandóan változnak, a felhasználók pedig sajnos feledékenyek tudnak lenni.⁵¹

⁵¹ Mohsen Ghasemi, Mohammad Saadaat, és Omid Ghollasi, „Threats of Social Engineering Attacks Against Security of Internet of Things (IoT)”, in *Fundamental Research in Electrical Engineering*, szerk. Shahram Montaser Kouhsari, köt. 480, Lecture Notes in Electrical Engineering (Singapore: Springer Singapore, 2019), 957–68, https://doi.org/10.1007/978-981-10-8672-4_73.

4.1 IoT eszközök sérülékenységei és kihasználásuk típusai az okos otthonok tükrében

Az eddigi információk alapján már kiderült, hogy rendkívül sok mindennel tudunk találkozni, ha IoT eszközök sérülékenységeiről van szó. Azonban egységesítve azt lehet elmondani, hogy az IoT eszközök biztonságának egyik legnagyobb kihívása a sokféleségük. Az IoT eszközök mindenféle formában és méretben léteznek, és a legkülönbözőbb célokra használják őket. Ez megnehezíti az egységes biztonsági megoldás kidolgozását. Sok IoT eszközt ráadásul nem a biztonság, hanem a költség és a kényelem szem előtt tartásával terveznek. Ennek eredményeképpen pedig hiányozhatnak az alapvető biztonsági funkciók, például a szoftver frissítésének vagy az alapértelmezett jelszavak megváltoztatásának lehetősége.⁵²

Ahhoz, hogy kapjunk egy átláthatóbb képet, érdemesnek tartom összegezni, hogy milyen szempontokat célszerű figyelembe venni az IoT eszközök sérülékenységei és azok kihasználásának típusai tekintetében.

A sebezhetőségeket vizsgálva, az IoT eszközök különböző típusú sebezhetőségekkel rendelkezhetnek, mint például a kommunikációs protokollok sebezhetőségei, gyenge jelszavak, szoftverhibák vagy fizikai biztonsági hiányosságok. Volt néhány kutatási erőfeszítés az okos otthoni környezetben lévő IoT eszközök sebezhetőségének vizsgálatára, ahol a biztonsági kihívások kielemezésre kerültek és támadási osztályozások kerültek bemutatásra. A támadások négy különböző kategóriába kerültek: fizikai, hálózati, szoftveres és titkosítási.

A fizikai támadások kategóriájában egy IoT eszköz hardvere esik áldozatul a támadásnak. A támadók ilyenkor fizikai hozzáférést szereznek az eszközhöz. Fizikai támadás lehet többek között a csomópontok manipulálása, rádiófrekvenciás (RF) interferencia a rádiófrekvenciás azonosítókön (RFID), csomópontok zavarása vezeték nélküli érzékelőhálózatokban, rosszindulatú csomópontok befecskendezése, fizikai sérülés, social engineering és rosszindulatú kód befecskendezése.

A hálózati támadásoknál nem feltétlenül szükséges, hogy a támadó a támadás végrehajtásához az IoT rendszer közvetlen közelében legyen. Hálózati támadás lehet például a forgalomelemzés, RFID spoofing, klónozás, jogosulatlan hozzáférés, sinkhole, man-in-the-middle és

⁵² „The challenges and problems of securing IoT devices | LinkedIn”, elérés 2023. október 19., <https://www.linkedin.com/pulse/challenges-problems-securing-iot-devices-isidoro-da-silva/>.

szolgáltatásmegtagadás.⁵³ A hálózati támadásra jó példa lehet a már korábban is említett Mirai Botnet támadás 2016-ból.

A szoftveres támadások, amelyeket néha firmware-támadásoknak is neveznek, az IoT rendszerek szoftverében meglévő sebezhetőségeket használják ki rosszindulatú szoftverek, például férgek, vírusok révén. A szoftveres támadások közül az adathalászat, a rosszindulatú szkriptek, a trójai, a kémprogramok, a reklámprogramok és a szolgáltatásmegtagadás, amelyek a puffer túlcsordulásokat, az SQL-injekciókat és más típusú sebezhetőségeket használják ki. Ezek a szoftveres sebezhetőségek az okos otthoni architektúrák különböző rétegeiben létezhetnek, például az egyes eszközök, a vezérlőközpont és a felhőszolgáltatások szintjén. Az eszköz szintjén a szoftveres sebezhetőség csak egy adott eszközre vonatkozik. A vezérlőközpont szintjén egy szoftveres sebezhetőség egy vezérlőközpontot érint, mint például a Samsung SmartThings, amely potenciálisan az összes, a központhoz csatlakoztatott eszközt érinti. A felhőszolgáltatás szoftverének sebezhetősége nem csak a felhőszolgáltatáshoz csatlakoztatott intelligens eszközöket érinti, hanem az összes, a felhőszolgáltatáshoz csatlakoztatott eszközt is.⁵⁴ A szoftveres támadások esetében érdekes lehet megnézni a háztartási gépek helyzetét, különösen például az okos kávéfőzők esetét, ugyanis meglehetősen könnyen hackelhetők. 2020-ban született is ezzel kapcsolatban egy tartalom az Ars Technica oldalán, ahol egy programozó bemutatta, hogy mennyire engedelmetlenné tudta tenni az eszközt egy zsarolóprogramnak köszönhetően, illetve utasítást is ki tudott írni a felhasználónak, amiben váltságdíjra kötelezte.⁵⁵

Az utolsó támadáskategória a titkosítás. A titkosítási támadásokra akkor kerül sor, amikor a támadó feltöri az IoT rendszerben használt titkosítási mechanizmust. Mivel az IoT eszközök korlátozott számítási kapacitással rendelkeznek az erős kriptográfiai protollok támogatásához, sebezhetőek az oldalcsatornás, kriptanalízis és man-in-the-middle támadásokkal szemben.⁵⁶

⁵³ Brittany D. Davis, Janelle C. Mason, és Mohd Anwar, „Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study”, *IEEE Internet of Things Journal* 7, sz. 10 (2020. október): 10102–10, <https://doi.org/10.1109/JIOT.2020.2983983>.

⁵⁴ Davis, Mason, és Anwar.

⁵⁵ Dan Goodin, „When Coffee Makers Are Demanding a Ransom, You Know IoT Is Screwed”, *Ars Technica*, 2020. szeptember 26., <https://arstechnica.com/information-technology/2020/09/how-a-hacker-turned-a-250-coffee-maker-into-ransom-machine/>.

⁵⁶ Davis, Mason, és Anwar, „Vulnerability Studies and Security Postures of IoT Devices”.

Kutatásom során készítettem egy táblázatot, amelyben összegyűjtöttem a teljesség igénye nélkül, hogy az egyes rétegek tekintetében milyen fenyegetésekkel lehet számolni az okos otthoni IoT rendszerekben.

Alkalmazási réteg	Megjelenési réteg	Hálózati réteg	Fizikai réteg
Sebezhető szoftverek	Lehallgatás	DoS támadás	Fizikai károsodás
Adathalász támadás	Leskelődés	Jogosulatlan hozzáférés	Környezeti támadások
Instabil konfigurálás	Oldalcsatornás támadás	Man-in-the-middle támadás	Áramkimaradás
Social Engineering	Adatok megzavarása	Hamis információk bejuttatása	Hardverhiba
Rosszindulató kódok		Adattovábbítás	Rosszindulató kódok
Hozzáférés-szabályozás elleni támadás		Feketelyuk támadás	RFID túlterhelése
Biztonsági javítások elmaradása		Átjárók támadása	Címkék megkettőzése

2. táblázat: Összefoglaló azon fenyegetésekről, amelyek az okos otthoni IoT rendszereknél megjelenhetnek (saját szerkesztés, forrás: Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F., & Bilal, M. (2021). Smart

Ahogy a táblázat is mutatja, számos támadást meg lehet említeni, az adathalásztól kezdve a DoS, vagy DDoS támadásokig, de összességében elmondható, hogy az IoT eszközök tekintetében is ugyanazon alap problémák és támadás típusok állapíthatóak meg, mint a technológia egyéb területein belül. A rétegek tekintetében pedig amit fontos tudni, hogy az alkalmazási réteg biztonságának megsértése gyakorlatilag egy olyan helyzetet vagy eseményt takar, amikor egy szoftveralkalmazás vagy program biztonsági védelme sérül. Ez a szituáció azt eredményezheti, hogy az alkalmazás működése zavarttá válik, vagy pedig a működése egyáltalán nem lesz megfelelő. Biztonsági problémák a megjelenési rétegben is előjöhethetnek.

A hackerek a csomóponti szintet veszik célba, mivel ezek érzékelőkből állnak és arra használják fel, hogy az eszköz szoftverét a sajátjukra cseréljék. Az észlelésnél a fenyegetések többnyire külső entitásoktól származnak, és az érzékelőkkel ellátott eszközök kulcsszerepet játszanak ennek megvalósításában. Elérkezve a hálózati réteghez, érdemes tudni, hogy ez a réteg felelős az eszközök közötti információcseréért. Ennek következtében az adatok torlódása is ezen a rétegen történik. Ennek a rétegnek a fő biztonsági kérdései az érintett eszközökhöz eljuttatandó adatok integritása és hitelesítése. A fizikai réteg biztonságának megsértése is tud okozni fejfájást. A tápegységek képezik az intelligens otthoni eszközök gerincét. Kell lennie egy olyan

mechanizmusnak, amelyen keresztül ezek az eszközök túlélhetik az áramellátás megszakadását. Ezen a rétegen az eszközöket az időjárástól és az egyéntől is meg kell védeni.⁵⁷

4.2 Védelmi opciók, kockázatcsökkentő intézkedések

A kockázatcsökkentő intézkedések tekintetében ki kell emelni mind a gyártókat, mind a felhasználókat, hiszen ebben a folyamatban mindkét fél döntő szerepet játszik. A Fortinet meglátása szerint a gyártók számítanak a kiinduló pontnak. Az IoT biztonsága azzal kezdődik, hogy a gyártók kezelik a termékeik ismert sebezhetőségeit, javításokat adnak ki a meglévő sebezhetőségekre, valamint jelentik, ha a támogatás megszűnik. A gyártók számára az is alapvető fontosságú kell, hogy legyen, hogy a biztonságot az IoT terméktervezés középpontjába helyezzék, és teszteket, például behatolásteszteket végezzenek. Emellett folyamatokat kell bevezetniük a termékeikkel kapcsolatos sebezhetőségi jelentések elfogadására. Ezen pontok pedig mind visszavezethetőek a korábban bemutatásra került szabályozásokra és szabványokra, amelyek szeretnék a gyártókat is támogatni. Ha megvizsgáljuk a felhasználók oldaláról is, akkor pedig elmondhatjuk, hogy a felhasználóknak meg kell érteniük az IoT-hoz csatlakoztatott eszközöket övező biztonsági kockázatokat, amit számtalanszor hangoztatnak is a szakemberek, de a tudatosság kialakítása és az ismeretek elsajátítása egy hosszú út, aminek csak az elején tartunk. Prioritásként kell kezelni az IoT eszközök biztonságát, és védeni kell a hozzájuk csatlakozó laptopokat, mobiltelefonokat és routereket. Tudniuk kell a felhasználóknak, hogyan kell biztosítaniuk az otthoni hálózatokon lévő IoT eszközöket, hogyan kell megváltoztatniuk az alapértelmezett jelszavakat, frissíteni a szoftvereket, és mindezek mellett biztosítaniuk kell a biztonságos beállításokat az IoT sebezhetőségének megelőzése érdekében.⁵⁸

Az előző alfejezetben bemutattam azt, hogy az egyes rétegeknek milyen gyenge pontjaik vannak, ebben az alfejezetben pedig szeretnék visszacsatolni rájuk.

⁵⁷ Haseeb Touqeer és mtsai., „Smart Home Security: Challenges, Issues and Solutions at Different IoT Layers”, *The Journal of Supercomputing* 77, sz. 12 (2021. december): 14053–89, <https://doi.org/10.1007/s11227-021-03825-1>.

⁵⁸ „Top IoT Device Vulnerabilities: How To Secure IoT Devices”, Fortinet, elérés 2023. október 19., <https://www.fortinet.com/resources/cyberglossary/iot-device-vulnerabilities>.

A megjelenési réteg esetében a biztonság megvalósítása bonyolult, mert alacsony tárolókapacitással és alacsony energiával rendelkezik. Annak érdekében, hogy a biztonság megvalósítása megtörténhessen, van egy sor követelmény, amelyet teljesítenie kell: hitelesítés az érzékelők és minden olyan eszköz számára, amely hozzáfér ehhez a réteghez. A titkosítás is jelentős az adatok bizalmassága szempontjából, valamint szükség van olyan technikákra az IoT eszközök kihívásainak való megfelelés érdekében, amelyek az alacsony tárolókapacitást és alacsony energiát jelentik. A hálózati biztonság javítása érdekében ebben a hálózati rétegben egy sor kommunikációs biztonsági mechanizmust érdemes használni, mint például az IP sec és az anti-DDoS. A biztonság fogalma olyan technikák halmazával érhető el, mint a hitelesítési és titkosítási mechanizmusok. Az alkalmazási réteg biztonsági megoldásait tekintve, a különböző környezeti alkalmazások miatt különböző biztonsági követelmények vannak, ezért az adatmegosztás fontos jellemzője ennek a rétegnek. Az adatvédelemmel, az adatok kiszivárgásával és a hozzáférés ellenőrzésével kapcsolatos néhány kérdéssel kell foglalkoznia. Így a követelményeket akár két részre is fel lehet osztani. Elsőként, hogy hogyan védjük és tartjuk fenn az adatvédelmet, majd pedig, hogy hogyan ellenőrizhető az adatok hitelesítése.⁵⁹

Kutatások alapján van több biztonsági követelmény, amelyet célszerű érvényesíteni az IoT-val felszerelt okos otthonokban. Többek között kulcsfontosságú a felhasználói hitelesítés. Az okos otthonokban több száz internetkapcsolattal rendelkező, szoftverfrissítéseket, biztonsági javításokat és adatcserét igénylő eszköz kerül telepítésre. Mindezeket a folyamatokat csak jogosult felhasználóknak lenne szabad elvégezniük, tehát kimondható, hogy erős felhasználói hitelesítés nélkül egy okos otthon nem lesz biztonságos a támadókkal szemben.

Hitelesítés tekintetében az eszközhitelesítés mellett sem szabad elmenni, ugyanis az intelligens otthoni hálózatot így van lehetőség megvédeni a kompromittált csomópontok támadásaitól. Az eszközhitelesítésnek lehetővé kell tennie a legitim eszközök azonosítását a jogosulatlan eszközöktől.

Ha pedig a hálózatról van szó, akkor ezen a ponton érdemes kiemelni a hálózati felügyeletet. Mivel a DDoS-támadások az intelligens otthoni hálózaton futó hálózati réteg protokolljait is

⁵⁹ Muneer Bani Yassein és mtsai., „Smart Home Is Not Smart Enough to Protect You - Protocols, Challenges and Open Issues”, *Procedia Computer Science*, The 10th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2019) / The 9th International Conference on Current and Future Trends of Information and Communication Technologies in Healthcare (ICTH-2019) / Affiliated Workshops, 160 (2019. január 1.): 134–41, <https://doi.org/10.1016/j.procs.2019.09.453>.

célba vehetik, alapvető fontosságú, hogy legyen egy behatolásérzékelő rendszer és felügyeleti eszköz a hálózati behatolások észlelésére és a forgalmi anomáliák jelentésére.

Szintén fontos a biztonságos kulcskezelési rendszer, ugyanis ez teszi lehetővé, hogy ezek a hálózati kulcsok védettek legyenek és ne legyenek kiszolgáltatva a kompromittáló támadóknak, még akkor sem, ha más eszközök a hálózaton belül kompromittálódnak. Ez fontos, mert ha egy támadó hozzáférést szerez egy kompromittált eszközhöz, megpróbálhatja kinyerni vagy manipulálni a hálózati kulcsokat, hogy jogosulatlan hozzáférést szerezzen más eszközökhöz vagy érzékeny adatokhoz az intelligens otthoni hálózaton belül. Az IoT eszközök, ideértve az érzékelőeszközöket is, gyakran előre telepített hálózati kulcsokat használnak a biztonságos kommunikáció kialakításához a hálózaton belül.

Végül a fizikai védelemről sem szabad megfeledkezni. Ismert tény, hogy az elektronikus eszközök gyakran felügyelet nélkül maradnak, így sebezhetővé válnak a manipulációs támadásokkal szemben. Ebből adódik, hogy a fizikai védelem az egyik fontos pontja a biztonsági követelményeknek. A hamisításálló eszközök vagy a visszafordítás-gátló rendszerek jelenthetnek megoldást a manipulációs támadások ellen.⁶⁰

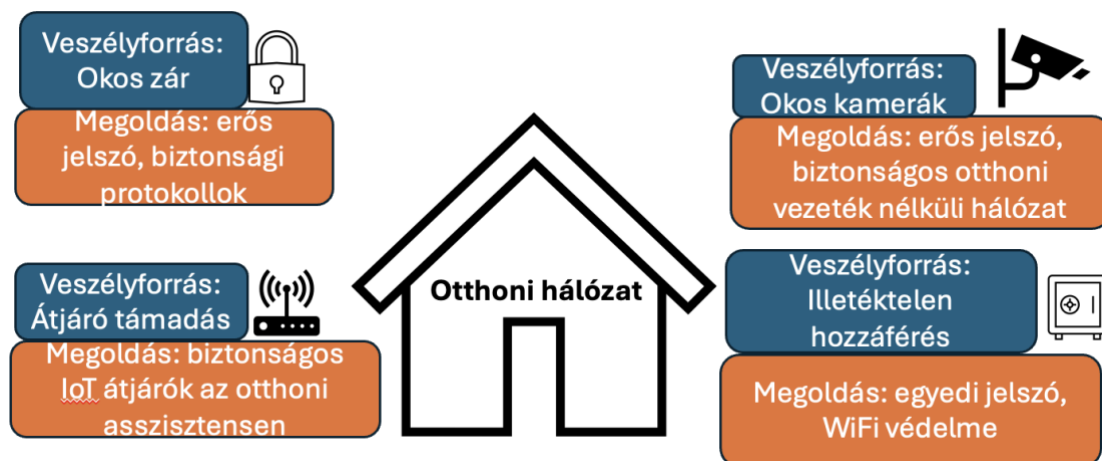
Nagyon fontosak a kockázatsökkentő intézkedések, azonban ez nagy mértékben összefügg a biztonság tudatossággal és ahogyan azt már tudjuk, nem feltétlenül a kiberbiztonsági tudatosság áll a felhasználók prioritásainak élén és talán sokszor a gyártók esetében sem más a helyzet. Azonban lényegesnek tartom arra is felhívni a figyelmet, hogy észrevegyük, amikor valami nem megfelelően működik, illetve, ami még fontosabb, hogy foglalkozzunk is vele és ne hagyjuk annyiban, ha pedig úgy érezzük, hogy egyedül nem tudjuk kezelni a fentálló problémát, kérjünk segítséget. Az IoT eszközök megtámadásának, kompromittálódásának számos jelei vannak és ahogyan nagyon sok szakember mondani szokta, ami gyanús, az nem véletlenül gyanús.

Az első jel, amire érdemes figyelni, az eszközök rendellenesen viselkedése. Ha szokatlan tevékenységet észlelünk az eszközünkön, például azt, hogy a mi beavatkozásunk nélkül be- és kikapcsol, az annak a jele lehet, hogy az eszköz valaki más irányítása alatt áll.

⁶⁰ Changmin Lee és mtsai., „Securing smart home: Technologies, security challenges, and security requirements”, in *2014 IEEE Conference on Communications and Network Security* (2014 IEEE Conference on Communications and Network Security (CNS), San Francisco, CA, USA: IEEE, 2014), 67–72, <https://doi.org/10.1109/CNS.2014.6997467>.

A hálózati forgalom megugrása egy másik jellegzetes probléma. Az adatforgalom megmagyarázhatatlan növekedése arra utalhat, hogy az eszköz nagy mennyiségű adatot küld egy támadónak. Emellett sokszor lehet tapasztalni, hogy a készülék vagy a hálózat lassúvá válik. Ha a készülék nem reagál, vagy a hálózati kapcsolat elhúzódik, az rosszindulatú fertőzés következménye lehet. Természetesen nem minden esetben ezen indok húzódik meg a háttérben, de számításba kell venni, mint lehetséges problémát. Továbbá az ismeretlen e-mailek vagy üzenetek hatalmas piros zászlóként jeleznek. Ha jelszó-visszaállítási kérelmet vagy más nem kívánt üzeneteket tartalmazó e-mailt kapunk, az annak a jele lehet, hogy egy hacker megpróbálja megszerezni az irányítást a felhasználói fiók felett. Ha már a felhasználói fiókokról van szó, nem mehetünk el a szokatlan fióktevékenységek mellett sem, ugyanis, ha egy IoT eszközhöz kapcsolódó fiókunk ismeretlen eszközöket vagy láthatatlan bejelentkezési helyeket mutat, az sajnos egy támadás következménye lehet.⁶¹

Az alábbi ábrán láthatunk eszközöket, hogy milyen fenyegetettséggel rendelkeznek és hogy milyen védelmi megoldásokat tudunk alkalmazni. Ezek fényében elmondható, hogy amelyek döntő szerepet játszanak a biztonságban, azok a jelszavak, a titkosítás és az autentikáció. Továbbá az is világossá válik, hogy hiába szolgálják a kényelmet az IoT eszközök, könnyen teherre is tudnak válni.



3. ábra: IoT fenyegetések és védelmi megoldások (saját szerkesztés, forrás: Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F., & Bilal, M. (2021). Smart home security: challenges, issues and solutions at different IoT layers. *The Journal of Supercom*

⁶¹ „IoT Attacks: How to Protect Your Devices | NordVPN”, 2023. július 20., <https://nordvpn.com/blog/iot-attacks/>.

4.3 Következtetések

Összességében az IoT eszközök sérülékenységei és azok védelmi intézkedései komplex kérdéseket vetnek fel, amelyek megfelelő tudatosságot és óvatosságot igényelnek mind a gyártóktól, mind a felhasználóktól a biztonságos használat érdekében. A gyártóknak javítaniuk kell termékeik biztonságát és kezelniük kell ismert sebezhetőségeiket. A felhasználóknak tudatosnak kell lenniük a kockázatokkal és megfelelő intézkedéseket kell tenniük az IoT eszközeik védelme érdekében.

Az IoT eszközök sérülékenységei tekintetében elmondható, hogy jelentős aggodalomra adnak okot, mivel azok kihasználása a felhasználók magánéletének megsértéséhez és egyéb biztonsági fenyegetésekhez vezethet. Az IoT eszközök biztonságát nagyban befolyásolja a sokféleségük és a különböző típusú sebezhetőségek, többek között például a kommunikációs protokollok sebezhetőségei, a gyenge jelszavak, a szoftverhibák és a fizikai biztonsági hiányosságok. A sérülékenységek kihasználására irányuló támadásokat pedig két nagy kategóriába sorolhatjuk: passzív és aktív támadások. Az IoT eszközök kompromittálódásának jelei lehetnek rendellenes viselkedések, szokatlan aktivitások vagy más gyanús tevékenységek, amelyeket a felhasználók észrevehetnek.

Az eddigi információk alapján elmondható, hogy ugyan nagyon sok sebezhetősége van az IoT technológiájának és sokféle képpen támadják az eszközöket, de maguk a sérülékenységek és a támadás típusok nem mutatnak jelentős megújulást, amivel máshol nem találkozhatnánk. Ezért a H2 hipotézisem, miszerint új sérülékenységeket és az azokat kihasználó támadási típusokat ismerhetünk meg az IoT világában, cáfolható. Viszont amellett nem szabad elmenni, hogy az emberi felhasználók a leggyengébb láncszemek az IoT rendszerek biztonságában is, és a social engineering technikáját használva a támadók vissza is élnek az emberek manipulálhatóságával a kibertámadások során, így jövőbeli célként mindenképpen, az eddiginél is nagyobb szerepet kell kapnia a tudatosság növelésének, hiszen az elsődleges tűzfal szerepét az ember tölti be a technológia világában is.

5. HAZAI FELHASZNÁLÓK BIZALMA ÉS ELHIVATOTTSÁGA AZ OTTHONI IOT ESZKÖZÖK IRÁNT

A kutatásom során fontosnak tartottam, hogy megvizsgáljam, hogy a hazai felhasználók milyen véleményt alkotnak az otthoni IoT eszközökről és egyáltalán mekkora bizalmat vetnek az IoT-t felépítő technológiába. Fontos szerepet kapott a biztonságtudatosság és a felhasználók félelme is. Erre a kérdésre azért is voltam kíváncsi, mert a biztonságtudatosság nagy kihívást okoz és érdekesnek tartottam megvizsgálni, hogy vajon az IoT eszközök használata és a felhasználók biztonságtudatossága mennyire van egyensúlyban egymással.

5.1 Kérdőív bemutatása

A kérdőívemet néhány alapvető demográfiai adat bekérésével kezdtem, mint például a nem, az életkor, a lakhely és az iskolázottság. Ezt követően kíváncsi voltam, hogy még mielőtt bármilyen választ adnak a felhasználók a konkrét témával kapcsolatban, mennyire érzik biztosnak az ismereteiket az IoT fogalmát illetően. Ezután szerettem volna megtudni, hogy megközelítőleg hány IoT eszközzel rendelkeznek és hogy mennyire tartják magukat információbiztonsági szempontból tudatosnak.

A következő kérdéskörben az volt a célom, hogy kiderítsem, hogy egyes okoseszközök használata mennyire számít fontosnak a felhasználók otthonában. Számos opciót felsoroltam, többek között a háztartási eszközöket, a biztonságtechnikát, a szórakoztatásra alkalmas eszközöket és néhány alapfunkciót ellátó eszközt, mint a fűtés és a világítás. Tekintve, hogy az IoT eszközök fel tudják borítani az életünket, érdekelt, hogy mennyire tartanak olyan kihívásoktól, amelyeket ezen eszközök nem megfelelő módon történő alkalmazása idézhet elő. Ilyen volt például az adatok ellopása, a magánélet megsértése, a biztonságérzet sérülése és az anyagi kár elszenvedése. Utána azt is szerettem volna kideríteni, hogy miután nyilatkoznak a félelmeikről, hogyan vélekednek azzal kapcsolatban, hogy az egyes területeken mennyire okosítanak fel a saját otthonukat. Ezen kérdésnél a biztonságtechnika, a fűtés, a világítás, a

szórakoztató elektronika, az intelligens nyílászárók és az okos háztartási eszközök kaptak szerepet.

Végezetül pedig megvizsgáltam, hogy egyes állításokkal mennyire értenek egyet a felhasználók. Az állítások arról szóltak, hogy fenntartás nélkül csatlakoztatják-e az eszközeiket az Internethez, félnek-e az Interneten történő adatszivárgástól, 100%-ig megbíznak-e az okos otthoni eszközeikben, szeretnék-e az otthoni berendezéseket távolról vezérelni és mobiltelefonon hozzáférni az összes otthonukkal kapcsolatos adathoz, valamint valós idejű adatokat kapni.

A kérdőív kitöltése természetesen anonim módon történt, olyan adatot nem kértem, amivel fellelhető lenne a kitöltők személyazonossága.

A kérdőívem kiértékelésre az IBM SPSS Statistics 25 programot használtam, amiben az eredményeim egyes részét Kruskal-Wallis-próba alá vetettem. A Kruskal-Wallis próba kettőnél több csoportot hasonlít össze ugyanazon változó alapján és célja, hogy segítse eldönteni, hogy a csoportok közötti különbség statisztikailag szignifikáns-e vagy sem. A Kruskal-Wallis próba során egy tesztváltozót kell vizsgálni egy csoportosító változóval. Ezt követően betöltjük a vizsgálni kívánt adatokat és lefuttatunk egy próbát. A próba eredményeként kapunk egy statisztikai értéket, amelyet az "Asymp. Sig." (Asymptotic Significance), vagy p értéként lehet ismerni. Ez jelöli a szignifikanciát. Amennyiben nem haladja meg a 0,005-t ($p < 0,005$) akkor ki lehet jelenteni, hogy a csoportok között jelentős különbség van a csoportosító változó függvényében. Ezt követi a rangátlag vizsgálata, amely azt mutatja meg, hogy a csoportosító változó értékeinek rangsorát hogyan befolyásolják a tesztváltozó értékei.

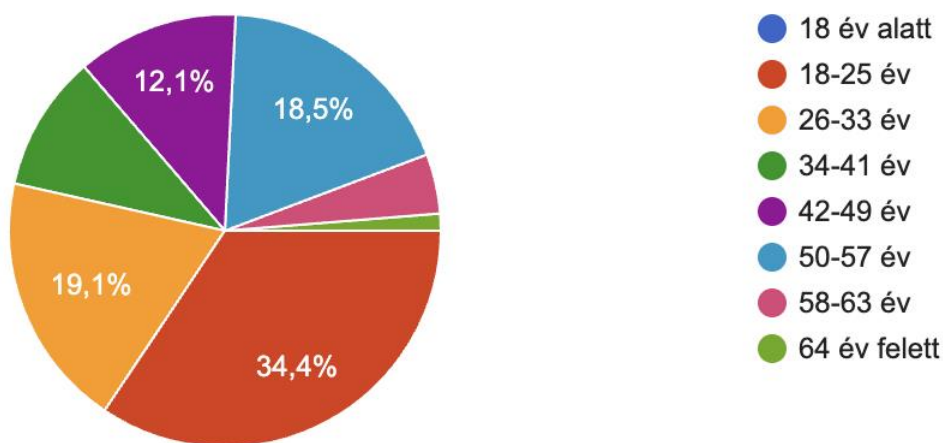
A kérdőívben az alábbi hipotézisekre kerestem a választ:

- H3: Az IoT definíciójának ismerete befolyásolja az ezen technológiával kapcsolatos fenyegetések értékelését.
- H4: A nők kevésbé gondolják magabiztosnak magukat információbiztonsági tudatosság tekintetében és az IoT fogalmát illetően.

- H5: Az IoT eszközök száma befolyásolja az igényt az otthon egyes területeinek felokosítására

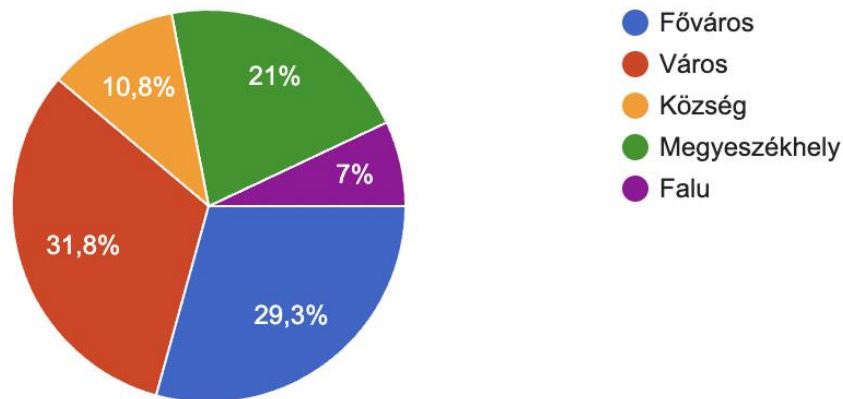
5.2 Eredmények kiértékelése

A kérdőívet 157 személy töltötte ki, jellegét tekintve nem reprezentatív a felmérés. A nemek megoszlásában látható, hogy 66,9%-ban nők töltötték ki és 33,1%-ban jelentek meg a férfiak. Korosztály tekintetében legnagyobb részben a 18-25 éves korosztály töltötte ki, számszerűsítve 34,4%-kal majd ahogyan emelkedtek a korcsoportok, csökkent a kitöltők száma. A megoszlás részletes adatait a 6. ábrán szemléltetem.



4. ábra: Kormegoszlás a kitöltők között (saját szerkesztés, forrás: kérdőív)

Az látható, hogy a kérdőívet főleg a városokból töltötték ki (31,8%), majd ezután következett a főváros (29,3%), a megyeszékhely (21%), a község (10,8%), végezetül a legkevebb kitöltés a falvakból érkezett (7%). Ezen információk szintén megtalálhatóak a 7. számú ábrán.

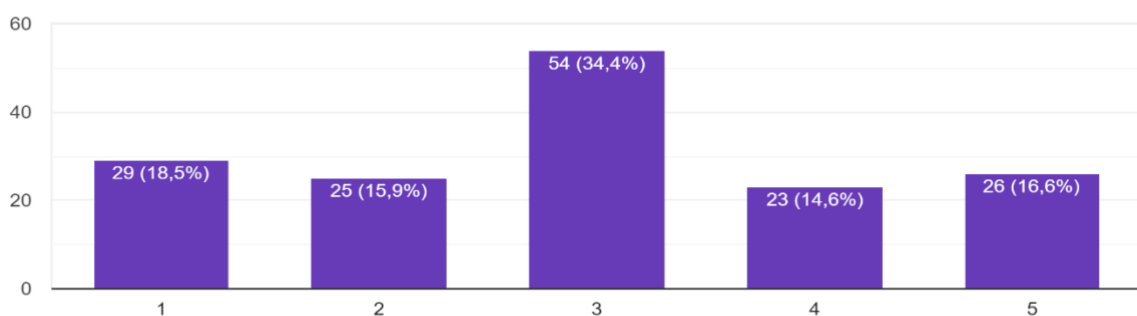


5. ábra: A kitöltők megoszlása az általuk lakott település típusa szerint (saját szerkesztés, forrás: kérdőív)

Megvizsgáltam, hogy a kitöltők körében mennyire érzik magukat biztosnak a felhasználók az IoT fogalmát illetően és itt lehetőség volt 1-5-ig tartó Likert skálán értékelni a saját ismereteiket. A kitöltők között az aranyközép utat választották a legtöbben (34,4%), viszont a második helyre az egyest jelölték meg többségében, tehát ez az jelenti, hogy a kitöltők 18.5% egyáltalán nincs tisztában az IoT fogalmával. Korábban is szó esett a biztonságtudatosságról, ez az eredmény pedig gyakorlatilag alá is támasztja, hogy nem alaptalan az a félelem, hogy a felhasználók úgy birtokolnak eszközöket, hogy valójában nem tudják pontosan, mire is képesek és milyen technológiával vannak ellátva.

Mennyire érzi biztosnak ismereteit az IoT (Internet of Things) fogalmát illetően?

157 válasz



6. ábra: A kitöltők megoszlása az IoT fogalmának ismereti szintje szerint (forrás: kérdőív)

Ezen információ kapcsán szerettem volna megtudni, hogy a kitöltők ismerete az IoT fogalmát tekintve mennyire befolyásolja a félelmet az egyes kihívásoktól, ugyanis az ismeretek jelentős mértékben befolyásolhatják a félelmet az egyes kiberbiztonsági kihívásoktól. Az ismeretek és az IoT technológiával kapcsolatos tudatosság segíthetnek a felhasználóknak jobban megérteni a kiberbiztonsági kockázatokat és a védekezés lehetőségeit, ami csökkentheti az általuk érzett félelmet. A kihívások tekintetében több opció is volt, mint az adatok ellopása, a magánélet megsértése, a biztonságérzet sérülése, illetve az anyagi kár elszenvedése. A kiértékelés során azt az eredményt kaptam, hogy az anyagi káron kívül, máshol nem tapasztalható szignifikancia, tehát ezáltal kimondható, hogy az eredmény megcáfolta a H3 hipotézisemet, amely azt állította, hogy az IoT definíciójának ismerete befolyásolja az ezen technológiával kapcsolatos fenyegetések értékelését.

	Mennyire tart az alábbi kihívásoktól? (Adatok ellopása)	Mennyire tart az alábbi kihívásoktól? (Magánélet megsértése)	Mennyire tart az alábbi kihívásoktól? (Biztonságérzet sérülése)	Mennyire tart az alábbi kihívásoktól? (Anyagi kár elszenvedése)
Kruskal-Wallis	4,539	4,491	6,972	9,899
df	4	4	4	4
Asymp.Sig.	0,338	0,344	0,137	0,042

3. táblázat: Kruskal-Wallis teszt szignifikancia eredmény (saját szerkesztés, forrás: SPSS)

Tovább haladva, de még mindig az IoT fogalmának ismeretét megragadva, kíváncsi voltam, hogy a nemek közötti különbség mennyire befolyásolja a magabiztosságot az IoT fogalmát, illetve az információbiztonsági tudatosságot tekintve a kitöltők körében. H4 hipotézisemben azt állítottam, hogy a nők kevésbé gondolják magabiztosnak magukat információbiztonsági tudatosság tekintetében és az IoT fogalmát illetően. Ezen állításnak azért szerettem volna utána járni, mert a nők aránya az IT szektorban eleve nem túl magas, összehasonlítva a férfiakéval. (Ezen aránnyal kapcsolatban további részleteket az alábbi oldalon lehet találni: https://explodingtopics.com/blog/women-in-tech?fbclid=IwAR2pSt8mkahKuQZa_LmoR_iDMNgkPliid_chLleI5530hkwj-MZFR4L69RY). A H4 hipotézisem végül helytállónak bizonyult, ugyanis erős szignifikanciát

mutatott mind az információbiztonsági tudatosság, mind az IoT fogalmának ismerete tekintetében.

	Mennyire tartja magát információbiztonsági szempontból tudatosnak?
Kruskal-Wallis H	6,038
df	1
Asymp.Sig.	0,014

4. táblázat: Kruskal-Wallis teszt szignifikancia eredmény (saját szerkesztés, forrás: SPSS)

	Mennyire érzi biztosnak ismereteit az IoT (Internet of Things) fogalmát illetően?
Kruskal-Wallis H	6,733
df	1
Asymp.Sig.	0,009

5. táblázat: Kruskal-Wallis teszt szignifikancia eredmény (saját szerkesztés, forrás: SPSS)

Annak ellenére, hogy majdnem kétszer annyi hölgy töltötte ki a kérdőívet, mint férfi, a rangátlag 73,01 volt a nők körében, míg a férfiak esetében 91,09.

Az IoT fogalmának ismeretét tekintve, a rangátlag szintén elég hasonlóan alakult. A nők esetében 72,57, míg a férfiaknál 91,98 volt.

Szerettem volna megtudni, hogy az IoT eszközök száma, amelyekkel a kitöltők rendelkeznek, befolyásolják-e a kitöltők igényeit arra, hogy egyes területeken okossá tegyék otthonukat. Az IoT eszközök számának növekedése és a sokféle okos otthoni eszköz elérhetővé válása

növelheti többek között a kényelmet és a szórakozást, valamint ösztönözheti a felhasználókat, hogy kipróbálják és használják ezt a technológiát. Ennek ellenére az eredmények megcáfolták a H5 hipotézisemet, miszerint az IoT eszközök száma befolyásolja az igényt az otthon egyes területeinek felokosítására. Mindössze egyetlen pontnál, a világításnál mutatott a program szignifikanciát, a többinél nem.

	Az alábbi területeken milyen mértékben tenné okossá az Ön otthonát? Biztonságtechnika (mozgásérzékelők, kamerák, ajtó- és ablakérzékelők stb.)	Az alábbi területeken milyen mértékben tenné okossá az Ön otthonát? Fűtés (hőmérséklet-, páratartalom szabályozás)	Az alábbi területeken milyen mértékben tenné okossá az Ön otthonát? Világítás (fényérzékelők, okoslámpák)	Az alábbi területeken milyen mértékben tenné okossá az Ön otthonát? Szórakoztató elektronika (pl.: okos TV, hálózati médialejátszó stb.)	Az alábbi területeken milyen mértékben tenné okossá az Ön otthonát? Intelligens nyílászárók (pl.: okos garázskapu)	Az alábbi területeken milyen mértékben tenné okossá az Ön otthonát? Okos háztartási eszközök (pl.: okosklíma, okoshűtő, okosmosógép, okostűzhely, okosporszívó stb.)
Kruskal-Wallis	5,479	2,291	8,768	7,595	5,229	5,453
df	3	3	3	3	3	3
Asymp.Sig.	0,14	0,514	0,033	0,055	0,156	0,141

6. táblázat: Kruskal-Wallis teszt szignifikancia eredmény (saját szerkesztés, forrás: SPSS)

A kérdőívem kiértékelése során találtam még olyan eredményeket, amelyekre ugyan hipotézist nem állítottam fel, viszont kutatásom szempontjából érdekesnek és fontosnak tartom bemutatni.

Megnéztem, hogy az egyes kihívásoktól való félelem mennyire befolyásolja a kitöltők bizalmát, hogy fenntartás nélkül csatlakoztassák az eszközeiket az Internethez, hiszen manapság egyre több személyt ér atrocitás a világhálón. Ezen felvetésnél az adatok ellopása, a magánélet megsértése, valamint a biztonságérzet sérülése esetében is erős szignifikanciát tapasztaltam, ellenben az anyagi kár elszenvedésével.

	Mennyire tart az alábbi kihívásoktól? Adatok ellopása	Mennyire tart az alábbi kihívásoktól? Magánélet megsértése	Mennyire tart az alábbi kihívásoktól? Biztonságérzet sérülése	Mennyire tart az alábbi kihívásoktól? Anyagi kár elszenvedése
Kruskal-Wallis H				
df	4	4	4	4
Asymp.Sig	0,003	0,001	0,015	0,455

7. táblázat: Kruskal-Wallis teszt szignifikancia eredmény (saját szerkesztés, forrás: SPSS)

Továbbá az is érdekelt, hogy az IoT fogalmának ismerete összefügghet-e az iskolázottság mértékével. Erre azért voltam kíváncsi, mert az IoT világa komplex és összetett technológiai terület, aminek megértése többek között sok technikai fogalmat, digitális jártasságot és műszaki ismeretet igényel viszont az is igaz, hogy ma már nagyon széles közönség számára és rengeteg formában, különböző célokkal elérhetőek az IoT eszközök. A vizsgálatot követően az eredmények megcáfolták ezen gondolatot, nem mutattak szignifikanciát.

	Mennyire érzi biztosnak ismereteit az IoT (Internet of Things) fogalmát illetően?
Kruskal-Wallis H	9,78
df	5
Asymp.Sig.	0,082

8. táblázat Kruskal-Wallis teszt szignifikancia eredmény (saját szerkesztés, forrás: SPSS)

5.3 Következtetések

Az általam bemutatott kutatás során az IoT otthoni eszközökkel kapcsolatos hazai felhasználók véleményét és bizalmát vizsgáltam. Az alábbiakban levonható néhány következtetés az eredmények alapján:

Az IoT fogalmának ismeretét és az információbiztonsági tudatosság kérdését tekintve a kutatásban részt vevők nagy része nem rendelkezett alapos ismerettel az IoT fogalmáról, és ez nagyban kihat az információbiztonsági tudatosságra is.

A nők az információbiztonsági tudatosság és az IoT fogalmának ismerete terén kevésbé biztosak magukban, összhangban az IT szektorban tapasztalható egyenlőtlen megoszlással a nemek tekintetében.

Az IoT eszközök otthoni jelenlétét megnézve elmondható, hogy az IoT eszközök száma nem mutatott szignifikáns kapcsolatot a felhasználók igényével az otthonuk egyes területeinek "okosítására", kivéve a világítást, ahol volt némi összefüggés.

Félelem és bizalom kérdésében megállapítható, hogy az adatok ellopásával, a magánélet megsértésével és a biztonságérzet sérülésével kapcsolatos félelem szignifikánsan befolyásolta a felhasználók hajlandóságát az eszközeik internethez való csatlakoztatásában. Az anyagi kár elszenvedésével kapcsolatban nem volt ilyen hatás.

ÖSSZEFOGLALÓ

A kutatásom egy részletesebb, átfogóbb képet ad arról, hogy az IoT világa milyen mértékben és milyen gyorsasággal növekszik globális szinten. A jövőben várhatóan még inkább nőni fog az IoT eszközök száma, lehetővé téve az otthonok távolról történő irányítását és fókuszba helyezve a nagyobb szintű kényelmet. Az IoT ígéretes technológia, de a biztonság kiemelten fontos és hogy megelőzzük a sérülékenységek kihasználását, ezzel együtt a kibertámadásokat. Kutatásom középpontjába az IoT-n belül az okos otthonokat helyeztem. Az IoT az okos otthonok alapját képezi, ahol az eszközök és érzékelők összekapcsolódnak, és Interneten keresztül elérhetők és vezérelhetők.

A növekvő aggodalmak azt eredményezték, hogy az IoT szabályozásának fontossága mára már nagyon vitatott téma lett és fontos szerepet tölt be, különösen az USA-ban és az EU-ban, ahol folyamatosan zajlanak a törekvések a biztonságosabb IoT használatra és eszközgyártásra. Az IoT eszközök jelenleg gyakran hiányos biztonsági rendszerekkel rendelkeznek, ami veszélyeztetheti a felhasználók magánéletét. Azonban sok fogyasztó nincs tisztában az IoT veszélyeivel, ezért nem igénylik erősebb szabályozást. A védelmi intézkedések terén mind a gyártók, mind a felhasználók szerepet játszanak. A gyártóknak kiemelten kell foglalkozniuk a termékeik biztonságával, ismert sérülékenységeik kezelésével és a biztonságos tervezéssel. A felhasználóknak pedig tisztában kell lenniük a biztonsági kockázatokkal, és megfelelően védeniük kell az eszközeiket, például az alapértelmezett jelszavak megváltoztatásával és a rendszeres frissítések végrehajtásával, hiszen a social engineering óriási kihívást jelent. Az IoT rendszerek sérülékenységei a különböző rétegeken megjelennek, és különböző támadási típusokat eredményezhetnek. A megjelenési réteg biztonságának megvalósítása összetett, a hálózati rétegben a kommunikációs biztonságot kell javítani, az alkalmazási rétegben az adatvédelmet és az adatbiztonságot kell figyelembe venni, a fizikai réteg védelme pedig a manipulációs támadások elleni intézkedéseket foglalja magában.

Az otthoni IoT eszközökkel kapcsolatos kutatás azt mutatja, hogy sokan nem ismerik az IoT technológiát, különösen a nők kevésbé magabiztosak ezen területen. Az IoT eszközök mennyisége kevés hatással van az otthoni okosítás iránti igényre, kivéve a világítás technikát. A félelem, különösen az adatvesztés és magánélet megsértése miatt, jelentősen befolyásolja az eszközök Internethez való csatlakoztatását, tehát az ismeretterjesztés és a bizalom növelése kulcsfontosságú az IoT elfogadásához.

Összegezve a hipotéziseimet, az alábbi megállapításokat tettem:

- H1 hipotézisem, miszerint az IoT szabályozása erősebb az Amerikai Egyesült Államokban, mint az Európai Unióban, megcáfolásra került.
- H2 hipotézisem, amely szerint új sérülékenységeket és az azokat kihasználó támadási típusokat ismerhetünk meg az IoT világában, megcáfolásra került.
- H3 hipotézisem, miszerint az IoT definíciójának ismerete befolyásolja az ezen technológiával kapcsolatos fenyegetések értékelését, megcáfolásra került.
- H4 hipotézisem, miszerint a nők kevésbé gondolják magabiztosnak magukat információbiztonsági tudatosság tekintetében és az IoT fogalmát illetően, beigazolódott.
- H5: Az IoT eszközök száma befolyásolja az igényt az otthon egyes területeinek felokosítására, megcáfolásra került.

Ezenkívül fontos megemlíteni, hogy a jelen kutatásban igyekeztem átfogó képet nyújtani, és több olyan területet is érinteni, amelyek segítségül szolgálhatnak jövőbeli kutatási irányok meghatározásában.

IRODALOMJEGYZÉK

Al Mtawa, Yaser, Harsimranjit Singh, Anwar Haque, és Ahmed Refaey. „Smart Home Networks: Security Perspective and ML-based DDoS Detection”. In *2020 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, 1–8. London, ON, Canada: IEEE, 2020. <https://doi.org/10.1109/CCECE47787.2020.9255756>.

Al-Fuqaha, Ala, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, és Moussa Ayyash. „Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications”. *IEEE Communications Surveys & Tutorials* 17, sz. 4 (2015): 2347–76. <https://doi.org/10.1109/COMST.2015.2444095>.

Al-Sarawi, Shadi, Mohammed Anbar, Kamal Alieyan, és Mahmood Alzubaidi. „Internet of Things (IoT) communication protocols: Review”. In *2017 8th International Conference on Information Technology (ICIT)*, 685–90. Amman, Jordan: IEEE, 2017. <https://doi.org/10.1109/ICITECH.2017.8079928>.

Ameyed, Darine, Fehmi Jaafar, Fabio Petrillo, és Mohamed Cheriet. „Quality and Security Frameworks for IoT-Architecture Models Evaluation”. *SN Computer Science* 4, sz. 4 (2023. május 15.): 394. <https://doi.org/10.1007/s42979-023-01815-z>.

Anthraper, Joseph, és Jaidip Kotak. „Security, Privacy and Forensic Concern of MQTT Protocol”. *SSRN Electronic Journal*, 2019. január 1. <https://doi.org/10.2139/ssrn.3355193>.

August E. Grant és Jennifer H. Meadows. *Communication Technology Update and Fundamentals*. 17. kiad. Routledge, 2020.

Baruah, Prangshu Dweep, Saru Dhir, és Madhurima Hooda. „Impact of IOT in Current Era”. In *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, 334–39. Faridabad, India: IEEE, 2019. <https://doi.org/10.1109/COMITCon.2019.8862187>.

Botta, Alessio, Walter De Donato, Valerio Persico, és Antonio Pescapé. „Integration of Cloud Computing and Internet of Things: A Survey”. *Future Generation Computer Systems* 56 (2016. március): 684–700. <https://doi.org/10.1016/j.future.2015.09.021>.

Dahmen-Lhuissier, Sabine. „Consumer IoT Security”. ETSI. Elérés 2023. szeptember 1. <https://www.etsi.org/technologies/consumer-iot-security>.

Davis, Brittany D., Janelle C. Mason, és Mohd Anwar. „Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study”. *IEEE Internet of Things Journal* 7, sz.

10 (2020. október): 10102–10. <https://doi.org/10.1109/JIOT.2020.2983983>.

ENISA. „ENISA Threat Landscape 2022”. Report/Study. Elérés 2023. október 15. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>.

„ETSI EN 303 645 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements”. ETSI, 2020. június. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf.

„EU Cyber Resilience Act | Shaping Europe’s Digital Future”. Elérés 2023. szeptember 7. <https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act>.

„EUR-Lex - 32022L2555 - EN - EUR-Lex”. Elérés 2023. szeptember 8. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>.

„European Cyber Resilience Act (CRA)”. Elérés 2023. szeptember 7. <https://www.european-cyber-resilience-act.com/>.

Fagan, Michael, Katerina Megas, Karen Scarfone, és Matthew Smith. „IoT Device Cybersecurity Capability Core Baseline”. National Institute of Standards and Technology, 2020. május 29. <https://doi.org/10.6028/NIST.IR.8259A>.

Fahd Al-Mutawa, Rihab, és Fathy Albourae Eassa. „A Smart Home System based on Internet of Things”. *arXiv e-prints*, 2020. szeptember 1. <https://doi.org/10.48550/arXiv.2009.05328>.

Fong, Jennifer. „Should the Government Regulate IoT Devices?” *IEEE Innovation at Work* (blog), 2017. október 19. <https://innovationatwork.ieee.org/should-government-regulate-iot/>.

Fortinet. „Top IoT Device Vulnerabilities: How To Secure IoT Devices”. Elérés 2023. október 19. <https://www.fortinet.com/resources/cyberglossary/iot-device-vulnerabilities>.

Gaikwad, Pranay P., Jyotsna P. Gabhane, és Snehal S. Golait. „A survey based on Smart Homes system using Internet-of-Things”. In *2015 International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC)*, 0330–35. Melmaruvathur, Chennai, India: IEEE, 2015. <https://doi.org/10.1109/ICCPEIC.2015.7259486>.

GDPR.eu. „What Is GDPR, the EU’s New Data Protection Law?”, 2018. november 7. <https://gdpr.eu/what-is-gdpr/>.

Gerodimos, Apostolos, Leandros Maglaras, Mohamed Amine Ferrag, Nick Ayres, és Ioanna Kantzavelou. „IoT: Communication Protocols and Security Threats”. *Internet of Things and Cyber-Physical Systems* 3 (2023. január 1.): 1–13. <https://doi.org/10.1016/j.iotcps.2022.12.003>.

Ghasemi, Mohsen, Mohammad Saadaat, és Omid Ghollasi. „Threats of Social Engineering Attacks Against Security of Internet of Things (IoT)”. In *Fundamental Research in Electrical Engineering*, szerkesztette Shahram Montaser Kouhsari, 480:957–68. Lecture Notes in

Electrical Engineering. Singapore: Springer Singapore, 2019. https://doi.org/10.1007/978-981-10-8672-4_73.

Gill, Khusvinder, Shuang-Hua Yang, Fang Yao, és Xin Lu. „A zigbee-based home automation system”. *IEEE Transactions on Consumer Electronics* 55, sz. 2 (2009. május): 422–30. <https://doi.org/10.1109/TCE.2009.5174403>.

Goodin, Dan. „When Coffee Makers Are Demanding a Ransom, You Know IoT Is Screwed”. *Ars Technica*, 2020. szeptember 26. <https://arstechnica.com/information-technology/2020/09/how-a-hacker-turned-a-250-coffee-maker-into-ransom-machine/>.

Gupta, Brij B, és Megha Quamara. *Internet of Things Security: Principles, Applications, Attacks, and Countermeasures*. CRC Press, 2020. <https://doi.org/10.1201/9780429353529>.

Hennebert, Christine, és Jessye Dos Santos. „Security Protocols and Privacy Issues into 6LoWPAN Stack: A Synthesis”. *IEEE Internet of Things Journal* 1, sz. 5 (2014. október): 384–98. <https://doi.org/10.1109/JIOT.2014.2359538>.

„IETF RFC 4919-2007 - IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals | Joinup”. Elérés 2023. augusztus 17. <https://joinup.ec.europa.eu/collection/ict-standards-procurement/solution/ietf-rfc-4919-2007-ipv6-over-low-power-wireless-personal-area-networks-6lowpans-overview-assumptions>.

„IoT Attacks: How to Protect Your Devices | NordVPN”, 2023. július 20. <https://nordvpn.com/blog/iot-attacks/>.

Journal, Irjet. „IRJET- Legal Regulations to Protect the Privacy and Data of IoT Technologies Users”. *IRJET*, 2020. január 1. https://www.academia.edu/44392468/IRJET_Legal_Regulations_to_Protect_the_Privacy_and_Data_of_IoT_Technologies_Users.

Khurshid, Anum, Reem Alsaaidi, Mudassar Aslam, és Shahid Raza. „EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme”. *IEEE Access* 10 (2022): 129932–48. <https://doi.org/10.1109/ACCESS.2022.3225973>.

Kumar, Nallapaneni Manoj, és Pradeep Kumar Mallick. „The Internet of Things: Insights into the Building Blocks, Component Interactions, and Architecture Layers”. *Procedia Computer Science* 132 (2018): 109–17. <https://doi.org/10.1016/j.procs.2018.05.170>.

Lavric, Alexandru, Adrian I. Petrariu, és Valentin Popa. „Long Range SigFox Communication Protocol Scalability Analysis Under Large-Scale, High-Density Conditions”. *IEEE Access* 7 (2019): 35816–25. <https://doi.org/10.1109/ACCESS.2019.2903157>.

Lee, Changmin, Luca Zappaterra, Kwanghee Choi, és Hyeong-Ah Choi. „Securing smart home:

Technologies, security challenges, and security requirements”. In *2014 IEEE Conference on Communications and Network Security*, 67–72. San Francisco, CA, USA: IEEE, 2014. <https://doi.org/10.1109/CNS.2014.6997467>.

Lili Nemec Zlatolas, Nataša Feher, és Marko Hölbl. „Security Perception of IoT Devices in Smart Homes”. *Journal of Cybersecurity and Privacy*, 2022. <https://doi.org/10.3390/jcp2010005>.

Lionel Sujay Vailshery. „IoT Connected Devices Worldwide 2019-2030”. Statista, 2022. november 22. <https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/>.

Mamonov, Stanislav, és Marios Koufaris. „Fulfillment of Higher-Order Psychological Needs through Technology: The Case of Smart Thermostats”. *International Journal of Information Management* 52 (2020. június 1.): 102091. <https://doi.org/10.1016/j.ijinfomgt.2020.102091>.

Mandić Dorottya, és Simon János. „Biztonságosak-e az okosotthonokban használt okoseszközök?” *Biztonságtudományi Szemle* 4, sz. 4. (2022. december 7.): 59–67.

Mansour, Mohammad, Amal Gamal, Ahmed I. Ahmed, Lobna A. Said, Abdelmoniem Elbaz, Norbert Herencsar, és Ahmed Soltan. „Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions”. *Energies* 16, sz. 8 (2023. január): 3465. <https://doi.org/10.3390/en16083465>.

Margolis, Joel, Tae Tom Oh, Suyash Jadhav, Young Ho Kim, és Jeong Noyo Kim. „An In-Depth Analysis of the Mirai Botnet”. In *2017 International Conference on Software Security and Assurance (ICSSA)*, 6–12. Altoona, PA: IEEE, 2017. <https://doi.org/10.1109/ICSSA.2017.12>.

Michael Fagan, Katerina N. Megas, Karen Scarfone, és Matthew Smith. „Foundational Cybersecurity Activities for IoT Device Manufacturers”. National Institute of Standards and Technology, 2020. <https://doi.org/10.6028/NIST.IR.8259>.

Mocrii, Dragos, Yuxiang Chen, és Petr Musilek. „IoT-Based Smart Homes: A Review of System Architecture, Software, Communications, Privacy and Security”. *Internet of Things* 1–2 (2018. szeptember): 81–98. <https://doi.org/10.1016/j.iot.2018.08.009>.

PricewaterhouseCoopers. „Three Actions IoT Device Manufacturers Can Take Now to Get Ahead of the New Federal Law”. PwC. Elérés 2023. augusztus 30. <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/iot-cyber-improvement-act.html>.

„Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No

526/2013 (Cybersecurity Act) (Text with EEA Relevance)". Elérés 2023. szeptember 1. <https://eur-lex.europa.eu/eli/reg/2019/881/oj>.

Rep. Kelly, Robin L. [D-IL-2. „Text - H.R.1668 - 116th Congress (2019-2020): IoT Cybersecurity Improvement Act of 2020". Legislation, 2020. december 4. 2019-03-11. <https://www.congress.gov/bill/116th-congress/house-bill/1668/text>.

Shafique, Kinza, Bilal A. Khawaja, Farah Sabir, Sameer Qazi, és Muhammad Mustaqim. „Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios". *IEEE Access* 8 (2020): 23022–40. <https://doi.org/10.1109/ACCESS.2020.2970118>.

Shouran, Zaid, Ahmad Ashari, és Tri Priyambodo. „Internet of Things (IoT) of Smart Home: Privacy and Security". *International Journal of Computer Applications* 182 (2019. február 15.): 3–8. <https://doi.org/10.5120/ijca2019918450>.

Souifi, Jihen, Yassine Bouslimani, Mohsen Ghribi, Azeddine Kaddouri, Tobie Boutot, és Hsan Hadj Abdallah. „Smart Home Architecture based on LoRa Wireless Connectivity and LoRaWAN® Networking Protocol". In *020 1st International Conference on Communications, Control Systems and Signal Processing (CCSSP)*, 95–99. EL OUED, Algeria: IEEE, 2020. <https://doi.org/10.1109/CCSSP49278.2020.9151815>.

State of California - Department of Justice - Office of the Attorney General. „California Consumer Privacy Act (CCPA)", 2018. október 15. <https://oag.ca.gov/privacy/ccpa>.

Statista. „Annual Number of IoT Attacks Global 2022". Elérés 2023. szeptember 8. <https://www.statista.com/statistics/1377569/worldwide-annual-internet-of-things-attacks/>.

„The challenges and problems of securing IoT devices | LinkedIn". Elérés 2023. október 19. <https://www.linkedin.com/pulse/challenges-problems-securing-iot-devices-isidoro-da-silva/>.

Touqeer, Haseeb, Shakir Zaman, Rashid Amin, Mudassar Hussain, Fadi Al-Turjman, és Muhammad Bilal. „Smart Home Security: Challenges, Issues and Solutions at Different IoT Layers". *The Journal of Supercomputing* 77, sz. 12 (2021. december): 14053–89. <https://doi.org/10.1007/s11227-021-03825-1>.

Trajanovski, Tolijan, és Ning Zhang. „An Automated and Comprehensive Framework for IoT Botnet Detection and Analysis (IoT-BDA)". *IEEE Access* 9 (2021): 124360–83. <https://doi.org/10.1109/ACCESS.2021.3110188>.

Yassein, Muneer Bani, Ismail Hmeidi, Farah Shatnawi, Wail Mardini, és Yaser Khamayseh. „Smart Home Is Not Smart Enough to Protect You - Protocols, Challenges and Open Issues". *Procedia Computer Science*, The 10th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2019) / The 9th International Conference on Current

and Future Trends of Information and Communication Technologies in Healthcare (ICTH-2019) / Affiliated Workshops, 160 (2019. január 1.): 134–41.
<https://doi.org/10.1016/j.procs.2019.09.453>.

Zohourian, Alireza, Sajjad Dadkhah, Euclides Carlos Pinto Neto, Hassan Mahdikhani, Priscilla Kyei Danso, Heather Molyneaux, és Ali A. Ghorbani. „IoT Zigbee Device Security: A Comprehensive Review”. *Internet of Things* 22 (2023. július 1.): 100791.
<https://doi.org/10.1016/j.iot.2023.100791>.

MELLÉKLETEK

1. számú melléklet: Ábrajegyzék

1. ábra: IoT támadások száma 2018-2022 között globálisan. Forrás: https://www.statista.com/statistics/1377569/worldwide-annual-internet-of-things-attacks/	9
2. ábra: Az okos otthoni rendszer javasolt rendszerarchitektúrája, saját szerkesztés	15
3. ábra: IoT fenyegetések és védelmi megoldások (saját szerkesztés, forrás: Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F., & Bilal, M. (2021). Smart home security: challenges, issues and solutions at different IoT layers. The Journal of Supercom	45
4. ábra: Kormegoszlás a kitöltők között (saját szerkesztés, forrás: kérdőív)	50
5. ábra: A kitöltők megoszlása az általuk lakott település típusa szerint (saját szerkesztés, forrás: kérdőív)	51
6. ábra: A kitöltők megoszlása az IoT fogalmának ismereti szintje szerint (forrás: kérdőív) ..	51

2. számú melléklet: Táblázat jegyzék

1. Táblázat: Összefoglaló az IoT biztonságának szabályozásáról (saját szerkesztés, forrás: TDK dolgozatom)	34
2. táblázat: Összefoglaló azon fenyegetésekről, amelyek az okos otthoni IoT rendszereknél megjelenhetnek (saját szerkesztés, forrás: Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F., & Bilal, M. (2021). Smart home security: challenges, issues and solutions at different IoT layers. The Journal of Supercomputing. doi:10.1007/s11227-	41
3. táblázat: Kruskal-Wallis teszt szignifikancia eredmény (saját szerkesztés, forrás: SPSS) ..	52
4. táblázat: Kruskal-Wallis teszt szignifikancia eredmény (saját szerkesztés, forrás: SPSS) ..	53
5. táblázat: Kruskal-Wallis teszt szignifikancia eredmény (saját szerkesztés, forrás: SPSS) ..	53

6. táblázat: Kruskal-Wallis teszt szignifikancia eredmény (saját szerkesztés, forrás: SPSS) ..	54
7. táblázat: Kruskal-Wallis teszt szignifikancia eredmény (saját szerkesztés, forrás: SPSS) ..	55
8. táblázat Kruskal-Wallis teszt szignifikancia eredmény (saját szerkesztés, forrás: SPSS) ...	55

3. számú melléklet: Rövidítés jegyzék

Rövidítés	Rövidítés jelentése
IoT	Internet of Things
ITU	International Telecommunication Union
DDoS	Distributed Denial of Service
IEEE	Institute of Electrical and Electronics Engineers
IKT	Információ-kommunikációs Technológia
LPWAN	Low Power Wide Area Networking
WPAN	Wireless Personal Area Networking
DoS	Denial of Service
RFID	Radio Frequency Identification System
IoT CIA	IoT Cybersecurity Improvement Act
NIST	National Institute of Standards and Technology
CCPA	California Consumer Privacy Act
CPRA	California Privacy Rights Act
NISTIR	NIST Internal/Interagency Reports
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
ISO	International Organization for Standardization
MQTT	Message Queue Telemetry Transport
CIA	Confidentiality – Integrity - Availability
LoRaWAN	Low Range Wide Area Network
CRA	Cyber Resilience Act
GDPR	General Data Protection Regulation
NIS	Network and Information Systems

4. számú melléklet: Kérdőív

1. Neme:

- Nő
- Férfi

2. Életkora:

- 18 év alatt
- 18-25 év
- 26-33 év
- 34-41 év
- 42-49 év
- 50-57 év
- 58-63 év
- 64 év felett

3. Lakhelye:

- Főváros
- Város
- Község
- Megyeszékhely
- Falu

4. Legmagasabb iskolai végzettsége:

- Általános iskolai végzettség
- Szakmunkás bizonyítvány
- Érettségi
- Alapszakos diploma
- Mesterszakos diploma
- Felsőoktatási szakképzés

- Posztgraduális képzés

5. Mennyire érzi biztosnak ismereteit az IoT (Internet of Things) fogalmát illetően?

- 1 = Egyáltalán nem
- 5 = Teljesen

IoT fogalma: Az IoT (Internet of Things, magyarra fordítva: a "dolgok internete") olyan internetre csatlakoztatott eszközök összessége, amelyek képesek kommunikálni más okos eszközökkel és hálózatokkal.

6. Megközelítőleg hány IoT eszköze van?

- 0
- 1-5
- 6-10
- 11-15
- 16+

7. Mennyire tartja magát információbiztonsági szempontból tudatosnak?

- 1 = Egyáltalán nem
- 5 = Teljesen

8. Mennyi tartja fontosnak az alábbi okos eszközök használatát az Ön otthonában?

- 1 = Egyáltalán nem
 - 5 = Teljesen
-
- Szórakoztató elektronika (pl. okostelefon, okos TV, okosóra, tablet, stb.)
 - Háztartási eszközök (pl. okosklíma, okos porszívó, okos kávéfőző, okos mosógép, bébiőr stb.)
 - Biztonságtechnika (mozgásérzékelők, kamerák, ajtó- és ablakérzékelők stb.)
 - Fűtés (hőmérséklet-, páratartalom szabályozás)
 - Világítás (fényérzékelők, okoslámpák)

9. Mennyire tart az alábbi kihívásoktól?

- 1 = Egyáltalán nem
 - 5 = Teljesen
-
- Adatok ellopása
 - Magánélet megsértése
 - Biztonságérzet sérülése
 - Anyagi kár elszenvedése

10. Az alábbi területeken milyen mértékben tenné okossá az Ön otthonát?

- 1 = Egyáltalán nem
 - 5 = Teljesen
-
- Biztonságtechnika (mozgásérzékelők, kamerák, ajtó- és ablakérzékelők stb.)
 - Fűtés (hőmérséklet-, páratartalom szabályozás)
 - Világítás (fényérzékelők, okoslámpák)
 - Szórakoztató elektronika (pl.: okos TV, hálózati médialejátszó stb.)
 - Intelligens nyílászárók (pl.: okos garázkapu)
 - Okos háztartási eszközök (pl.: okosklíma, okoshűtő, okosmosógép, okostűzhely, okosporszívó stb.)

11. Mennyire ért egyet az alábbi állításokkal?

- 1 = Egyáltalán nem
 - 5 = Teljesen
-
- Fenntartás nélkül csatlakoztatom az eszközeimet az Internethez.
 - Félek az Interneten történő adatszivárgástól
 - Az otthoni okos eszközeimben 100%-ig megbízhatok.
 - Szeretném az otthonomban lévő berendezéseket (klíma, mosógép, hőszabályzó, porszívó stb.) mobil eszközömről vezérelni.

- Szeretnék a mobilkészülékemen keresztül hozzáférni az otthonommal kapcsolatos összes adathoz.
- Szeretnék valós idejű adatokat kapni az otthoni okos eszközeim tevékenységi állapotáról.

5. számú melléklet: Kérdőív kielemezés

Descriptive Statistics

	N	Mean	Std. Deviation	Minimum	Maximum
Mennyire tart az alábbi kihívásoktól?	157	3,97	1,100	1	5
1: Egyáltalán nem					
5: Teljesen [Adattok ellopása]					
Mennyire tart az alábbi kihívásoktól?	157	3,90	1,145	1	5
1: Egyáltalán nem					
5: Teljesen [Magánélet megsértése]					
Mennyire tart az alábbi kihívásoktól?	157	3,68	1,246	1	5
1: Egyáltalán nem					
5: Teljesen [Biztonságérzet sérülése]					
Mennyire tart az alábbi kihívásoktól?	157	3,95	1,148	1	5
1: Egyáltalán nem					
5: Teljesen [Anyagi kár elszenvedése]					
Mennyire érzi biztosnak ismereteit az IoT (Internet of Things) fogalmát illetően?	157	2,95	1,310	1	5

Kruskal-Wallis Test

Ranks

	Mennyire érzi biztosnak ismereteit az IoT (Internet of Things) fogalmát illetően?	N	Mean Rank
Mennyire tart az alábbi kihívásoktól? 1: Egyáltalán nem 5: Teljesen [Adattok ellopása]	Egyáltalán nem	29	84,50
	Inkább nem	25	85,40
	Inkább igen	54	82,83
	Igen	23	66,98
	Teljesen	26	69,38
	Total	157	
Mennyire tart az alábbi kihívásoktól? 1: Egyáltalán nem 5: Teljesen [Magánélet megsértése]	Egyáltalán nem	29	84,52
	Inkább nem	25	86,92
	Inkább igen	54	81,44
	Igen	23	64,85
	Teljesen	26	72,67
	Total	157	
Mennyire tart az alábbi kihívásoktól? 1: Egyáltalán nem 5: Teljesen [Biztonságérzet sérülése]	Egyáltalán nem	29	80,33
	Inkább nem	25	91,12
	Inkább igen	54	84,33
	Igen	23	64,96
	Teljesen	26	67,21
	Total	157	
Mennyire tart az alábbi kihívásoktól? 1: Egyáltalán nem 5: Teljesen [Anyagi kár elszenvedése]	Egyáltalán nem	29	81,97
	Inkább nem	25	83,62
	Inkább igen	54	89,21
	Igen	23	66,63
	Teljesen	26	60,98
	Total	157	

Test Statistics^{a,b}

	Mennyire tart az alábbi kihívásoktól?	Mennyire tart az alábbi kihívásoktól?	Mennyire tart az alábbi kihívásoktól?	Mennyire tart az alábbi kihívásoktól?
	1: Egyáltalán nem	1: Egyáltalán nem	1: Egyáltalán nem	1: Egyáltalán nem
	5: Teljesen [Adatok ellopása]	5: Teljesen [Magánélet megsértése]	5: Teljesen [Biztonságérzet sérülése]	5: Teljesen [Anyagi kár elszenvedése]
Kruskal-Wallis H	4,539	4,491	6,972	9,899
df	4	4	4	4
Asymp. Sig.	,338	,344	,137	,042

a. Kruskal Wallis Test

b. Grouping Variable: Mennyire érzi biztonság ismereteit az IoT (Internet of Things) fogalmát illetően?

Descriptive Statistics

	N	Mean	Std. Deviation	Minimum	Maximum
Mennyire érzi biztonság ismereteit az IoT (Internet of Things) fogalmát illetően?	157	2,95	1,310	1	5
Neme:	157	1,33	,472	1	2

Kruskal-Wallis Test

Ranks

	Neme:	N	Mean Rank
Mennyire érzi biztosnak ismereteit az IoT (Internet of Things) fogalmát illetően?	Nő	105	72,57
	Férfi	52	91,98
	Total	157	

Test Statistics^{a,b}

Mennyire érzi
biztosnak
ismereteit az IoT
(Internet of
Things) fogalmát
illetően?

Kruskal-Wallis H	6,733
df	1
Asymp. Sig.	,009

a. Kruskal Wallis Test

b. Grouping Variable: Neme:

Descriptive Statistics

	N	Mean	Std. Deviation	Minimum	Maximum
Mennyire tartja magát információbiztonsági szempontból tudatosnak?	157	3,50	1,023	1	5
Neme:	157	1,33	,472	1	2

Kruskal-Wallis Test

Ranks

	Neme:	N	Mean Rank
Mennyire tartja magát információbiztonsági szempontból tudatosnak?	Nő	105	73,01
	Férfi	52	91,09
	Total	157	

Test Statistics^{a,b}

Mennyire tartja
magát
információbizton
sági
szempontból
tudatosnak?

Kruskal-Wallis H	6,038
df	1
Asymp. Sig.	,014

a. Kruskal Wallis Test

b. Grouping Variable: Neme:

Descriptive Statistics

N	Mean	Std. Deviation	Minimum	Maximum
---	------	----------------	---------	---------

Az alábbi területeken milyen mértékben tenné okossá az Ön otthonát? 1: Egyáltalán nem 5: Teljesen [Biztonságtechnika (mozgásérzékelők, kamerák, ajtó- és ablakérzékelők stb.)]	157	3,73	1,299	1	5
Az alábbi területeken milyen mértékben tenné okossá az Ön otthonát? 1: Egyáltalán nem 5: Teljesen [Fűtés (hőmérséklet-, páratartalom szabályozás)]	157	3,43	1,262	1	5
Az alábbi területeken milyen mértékben tenné okossá az Ön otthonát? 1: Egyáltalán nem 5: Teljesen [Világítás (fényérzékelők, okoslámpák)]	157	3,13	1,399	1	5
Az alábbi területeken milyen mértékben tenné okossá az Ön otthonát? 1: Egyáltalán nem 5: Teljesen [Szórakoztató elektronika (pl.: okos TV, hálózati médialejátszó stb.)]	157	3,87	1,191	1	5

Az alábbi területeken milyen mértékben tenné okossá az Ön otthonát? 1: Egyáltalán nem 5: Teljesen [Intelligens nyílászárók (pl.: okos garázskapu)]	157	3,15	1,446	1	5
Az alábbi területeken milyen mértékben tenné okossá az Ön otthonát? 1: Egyáltalán nem 5: Teljesen [Okos háztartási eszközök (pl.: okosklíma, okoshűtő, okosmosógép, okostűzhely, okosporszívó stb.)]	157	3,08	1,352	1	5
Megközelítőleg hány IoT eszköze van?	157	2,25	,713	0	5

Kruskal-Wallis Test

Ranks

	Megközelítőleg hány IoT eszköze van?	N	Mean Rank
Az alábbi területeken milyen mértékben tenné okossá az Őn otthonát? 1: Egyáltalán nem 5: Teljesen [Biztonságtechnika (mozgásérzékelők, kamerák, ajtó- és ablakérzékelők stb.)]	Kismértékű IoT eszközhasználat (1-5)	122	74,80
	Közepes mértékű IoT eszközhasználat (6-10)	22	80,39
	Magas mértékű IoT eszközhasználat (11-15)	7	95,14
	Kimagasló mértékű IoT eszközhasználat (16+)	3	125,00
	Total	154	
Az alábbi területeken milyen mértékben tenné okossá az Őn otthonát? 1: Egyáltalán nem 5: Teljesen [Fűtés (hőmérséklet-, páratartalom szabályozás)]	Kismértékű IoT eszközhasználat (1-5)	122	76,02
	Közepes mértékű IoT eszközhasználat (6-10)	22	77,50
	Magas mértékű IoT eszközhasználat (11-15)	7	89,86
	Kimagasló mértékű IoT eszközhasználat (16+)	3	109,00
	Total	154	
Az alábbi területeken milyen mértékben tenné okossá az Őn otthonát? 1: Egyáltalán nem	Kismértékű IoT eszközhasználat (1-5)	122	73,76
	Közepes mértékű IoT eszközhasználat (6-10)	22	83,07
	Magas mértékű IoT eszközhasználat (11-15)	7	99,50

	milyen mértékben tenné okossá az Ön otthonát?	milyen mértékben tenné okossá az Ön otthonát?	milyen mértékben tenné okossá az Ön otthonát?	milyen mértékben tenné okossá az Ön otthonát?	milyen mértékben tenné okossá az Ön otthonát?	milyen mértékben tenné okossá az Ön otthonát?
	1: Egyáltalán nem	1: Egyáltalán nem	1: Egyáltalán nem	1: Egyáltalán nem	1: Egyáltalán nem	1: Egyáltalán nem
	5: Teljesen [Biztonságtechni ka (mozgásérzékelő k, kamerák, ajtó- és ablakérzékelők stb.)]	5: Teljesen [Fűtés (hőmérséklet-, páratartalom szabályozás)]	5: Teljesen [Világítás (fényérzékelők, okoslámpák)]	5: Teljesen [Szórakoztató elektronika (pl.: okos TV, hálózati médialejátszó stb.)]	5: Teljesen [Intelligens nyílászárók (pl.: okos garázskapu)]	5: Teljesen [Okos háztartási eszközök (pl.: okosklíma,okosh űtő, okosmosógép, okostűzhely, okosporszívó stb.)]
Kruskal-Wallis H	5,479	2,291	8,768	7,595	5,229	5,453
df	3	3	3	3	3	3
Asymp. Sig.	,140	,514	,033	,055	,156	,141

- a. Kruskal Wallis Test
- b. Grouping Variable: Megközelítőleg hány IoT eszköze van?

Descriptive Statistics

	N	Mean	Std. Deviation	Minimum	Maximum
Mennyire tart az alábbi kihívásoktól?	157	3,97	1,100	1	5
1: Egyáltalán nem					
5: Teljesen [Adatok ellopása]					

Mennyire tart az alábbi kihívásoktól? 1: Egyáltalán nem 5: Teljesen [Magánélet megsértése]	157	3,90	1,145	1	5
Mennyire tart az alábbi kihívásoktól? 1: Egyáltalán nem 5: Teljesen [Biztonságérzet sérülése]	157	3,68	1,246	1	5
Mennyire tart az alábbi kihívásoktól? 1: Egyáltalán nem 5: Teljesen [Anyagi kár elszenvedése]	157	3,95	1,148	1	5
Fenntartás nélkül csatlakoztatom az eszközeimet az Internethez.	157	3,18	1,356	1	5

Kruskal-Wallis Test

Ranks

	Fenntartás nélkül csatlakoztatom az eszközeimet az Internethez.	N	Mean Rank
Mennyire tart az alábbi kihívásoktól? 1: Egyáltalán nem 5: Teljesen [Adattok ellopása]	Egyáltalán nem	29	98,93
	Inkább nem	15	85,93
	Inkább igen	42	87,30
	Igen	41	65,68
	Teljesen	30	62,85
	Total	157	
Mennyire tart az alábbi kihívásoktól? 1: Egyáltalán nem 5: Teljesen [Magánélet megsértése]	Egyáltalán nem	29	99,98
	Inkább nem	15	66,03
	Inkább igen	42	91,05
	Igen	41	67,37
	Teljesen	30	64,23
	Total	157	
Mennyire tart az alábbi kihívásoktól? 1: Egyáltalán nem 5: Teljesen [Biztonságérzet sérülése]	Egyáltalán nem	29	98,67
	Inkább nem	15	66,47
	Inkább igen	42	85,82
	Igen	41	73,91
	Teljesen	30	63,65
	Total	157	
Mennyire tart az alábbi kihívásoktól?	Egyáltalán nem	29	90,67
	Inkább nem	15	77,20

1: Egyáltalán nem	Inkább igen	42	79,69
	Igen	41	77,62
5: Teljesen [Anyagi kár elszenvedése]	Teljesen	30	69,53
	Total	157	

Test Statistics^{a,b}

	Mennyire tart az alábbi kihívásoktól?	Mennyire tart az alábbi kihívásoktól?	Mennyire tart az alábbi kihívásoktól?	Mennyire tart az alábbi kihívásoktól?
	1: Egyáltalán nem	1: Egyáltalán nem	1: Egyáltalán nem	1: Egyáltalán nem
	5: Teljesen [Adatok ellopása]	5: Teljesen [Magánélet megsértése]	5: Teljesen [Biztonságérzet sérülése]	5: Teljesen [Anyagi kár elszenvedése]
Kruskal-Wallis H	16,292	17,855	12,304	3,654
df	4	4	4	4
Asymp. Sig.	,003	,001	,015	,455

a. Kruskal Wallis Test

b. Grouping Variable: Fenntartás nélkül csatlakoztatom az eszközeimet az Internethez.

Descriptive Statistics

	N	Mean	Std. Deviation	Minimum	Maximum
Mennyire érzi biztosnak ismereteit az IoT (Internet of Things) fogalmát illetően?	157	2,95	1,310	1	5
Legmagasabb iskolai végzettsége:	157	4,12	1,216	2	7

Kruskal-Wallis Test

Ranks

	Legmagasabb iskolai végzettsége:	N	Mean Rank
Mennyire érzi biztosnak ismereteit az IoT (Internet of Things) fogalmát illetően?	Szakmunkás bizonyítvány	2	100,75
	Érettségi	59	72,41
	Alapszakos diploma	48	81,07
	Mesterszakos diploma	22	101,73
	Felsőoktatási szakképzés	18	64,22
	Posztgraduális képzés	8	80,50
	Total	157	

Test Statistics^{a,b}

Mennyire érzi
biztosnak
ismereteit az IoT
(Internet of
Things) fogalmát
illetően?

Kruskal-Wallis H	9,780
df	5
Asymp. Sig.	,082

a. Kruskal Wallis Test

b. Grouping Variable: Legmagasabb
iskolai végzettsége: