ARE SMART DEVICES USED IN SMART HOMES SAFE?

BIZTONSÁGOSAK-E AZ OKOSOTTHONOKBAN HASZNÁLT OKOSESZKÖZÖK?

MANDIĆ Dorottya[1] SIMON János[2]

Abstract

Nowadays, there is a growing demand for various smart devices and more users are choosing to buy them. Smart devices are now used in many areas since they have many benefits. Customers pay not only for convenience, fun, and cost savings for smart devices in their homes, but also to increase security. Many users are unaware that smart devices can pose a number of security challenges, even the most harmless devices, when connected to cyberspace, can expose users to a variety of threats. In this study, we learn about the benefits of smart devices and security challenges.

Keywords

smart devices, IoT, smart homes, cybersecurity

Absztrakt

Napjainkban egyre nagyobb a kereslet a különféle okoseszköz iránt, és egyre több felhasználó vásáról okoseszközt. Az okoseszközöket már nagyon sok területen használják, hiszen számos előnnyel jár a használatuk. A felhasználók nem csak a kényelem, a szórakozás és a költségmegtakarítás miatt vásárolják meg az okoseszközöket otthonaikban, hanem az otthonuk biztonsága növelése érdekében is. A felhasználók közül sokan nincsenek tudatában azzal, hogy az okoseszközök számos biztonsági kihívást rejthetnek, ha kapcsolódnak a kibertérhez, még azok az eszközök is veszélyt jelenthetnek, melyek a legártalmatlanabbnak tűnnek. A tanulmányban megismerkedünk az okoseszközök előnyeivel, és biztonsági kihívásaikkal.

Kulcsszavak

okoseszközök, IoT, okosotthonok, kiberbiztonság

[1] mandic.dorottya@uni-obuda.hu | ORCID: 0000-0002-3384-5590 | PhD student, Óbuda University Doctoral School on Safety and Security Science | PhD hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

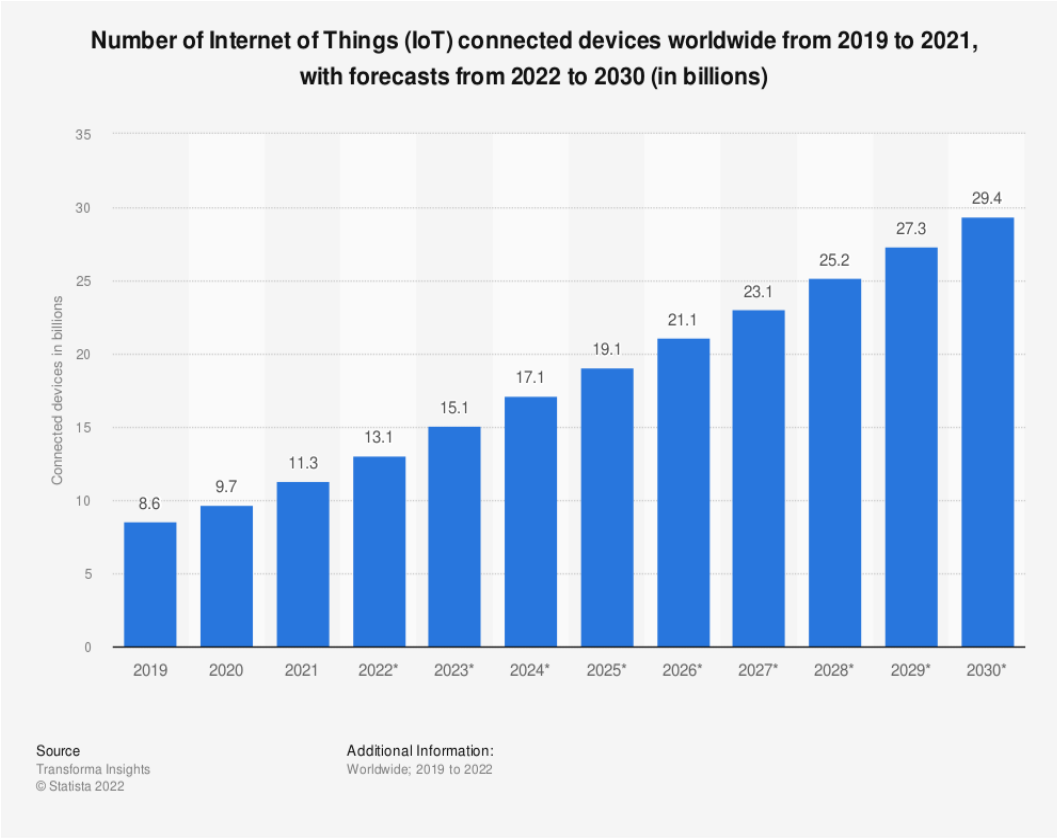
[2] simon@mk.u-szeged.hu |ORCID: 0000-0003-2870-5718 | associate professor, Department of Mechatronics and Automation, Faculty of Engineering, University of Szeged |egyetemi docens, Mechatronikai és Automatizálási Intézet, Mérnöki Kar, Szegedi Tudományegyetem

BEVEZETÉS

Az okoseszközök egyre elterjedtebbek napjainkban, és egyre több felhasználó vásáról otthonában különféle típusú okoseszközt. Az első dolgok internete eszköz az 1980-as évek elején jött létre a Carnegie Mellon Egyetemen, ami egy Coca-Cola automata volt. [1] Az Internet of Things magyarul azt jelenti, hogy dolgok internete. Az Internet of Things vagy csak rövidítve IoT alatt értünk, minden olyan dolgot és használati tárgyat, melyet egy hálózaton keresztül más gépekhez csatlakozva működnek. [5] Az eszközök egymás közötti kommunikációját Machine to Machine vagy magyarul gép-gép kommunikációnak hívunk, ami emberi beavatkozás nélkül történik. [43] Az IoT eszközök alkalmazását feloszthatjuk fogyasztói, kereskedelmi, ipari és infrastrukturális területekre. [3] Ezek a területek lehetnek például az okosvárosok, okosépületek, okosházak, okosjárművek, mezőgazdaság, egészségügy, viselhető eszközök, és egyéb területek. [2] A felhasználók közül sokan nincsenek tudatában azzal, hogy az okoseszközök használata komoly biztonsági kihívásokat okozhat, és sokszor azok az eszközök is veszélyforrássá válhatnak, ha az internetre vannak csatlakoztatva, melyekre talán nem is gondolnánk. [15] Az internetet világszerte 5 milliárd ember használja, ami a világ teljes népességének a 63%-át jelenti. [35] Az IoT Analitycs elemzése szerint az IoT eszközök száma el fogja érni a 30.9 millárd eszközt 2015-től 2025-ig. [4] A biztonság egyre fontosabbá vált a mindennapi életünkben. Napjainkban a kiberbűnözés jelenti az egyik legnagyobb kihívást. [9] Az IoT eszközök biztonságának a védelme az egyik legnagyobb kihívást jelenti, hiszen az IoT eszközök olyan információkat gyűjtenek, amelyek lehetnek személyes, vállalati vagy ipari információk. [22] Az elmúlt évek során megnőtt az érdeklődés az okosotthonokban használt okoseszközök iránt, amihez hozzá járult a COVID-19 járvány is.[7] Egyre elterjedtebbek az épületautomatizálási eszközök, okosszenzorok és egyéb megoldások, és a becslések szerint 175 millió okosotthon található meg a világon. [8] [18] Az okoseszközök számos előnyt nyújtanak az otthonokban, mint például az energia és költségmegtakarítás, kényelem, jobb életminőség vagy a biztonság növelése. [34] Európa szerte egyre gyakrabban fordulnak elő kibertámadások, és a kiberbűncselekmények, ami a jövőben várhatóan még nagyobb számban lesz jelen, hiszen még több eszköz fog az internethez csatlakozni. [28] Az Európai Unió tanácsa elfogadta a következtetéseket a csatlakoztatott eszközök kiberbiztonságáról, melyben elismerik, hogy az internetre csatlakoztatott fogyasztási cikkek, és ipari eszközöknek a használata megnőtt, és új kockázatok jöttek létre, valamint Európa digitális jövőjének az alakításában is fontos szerepet fognak kapni. [25]

Az okoseszközök előnyei az okosotthonokban

Az Internet of Things vagy csak rövidítve IoT alatt, olyan internetre csatlakoztatott eszközöket értünk, melyek kommunikálni tudnak más eszközökkel. Az internetkapcsolat segítségével lehetővé válik a felhasználók számára az, hogy az IoT eszközöket távolról is használni tudják. [43] Egyre többen vásárolnak okoseszközöket az otthonaikban, hiszen fontosnak tartsák a kényelmet, a költségmegtakarítást, a szórakozást vagy az otthonuk biztonságosabbá tételét. A Statista jelentése szerint az IoT eszközök száma egyre nő, és 2019-től 2030-ig az IoT eszközök száma elfogja érni a 29.4 milliárd eszközt. [11]



1. Ábra: Az IoT eszközök száma 2019-től 2030-ig. [11]

Az okoseszközök az otthonok különböző funkcióit vezérelhetik, automatizálhatják vagy optimalizálhatják. [13] Az okostermosztátok használata nagyban hozzá járul az energiatakarékossághoz. [41] A Google 2014-ben 3,2 milliárd dollárt fizetett a Nest okostermosztárok és okosfüstriasztókért. [33] Az okosotthon fűtéssel például átlagosan 30%-kal kevesebb fűtési energia használódik el. [36] Mivel az okoseszközökkel energiát takaríthatunk meg otthonunkban, ez által pénzt is spórolhatunk, hiszen kevesebbet kell majd fizetnünk a számlákra. A biztonságról sem szabad megfeledkeznünk, hiszen az okoseszközök segítségével az otthonunkat is biztonságosabbá tehetjük például egy kamera által, amely segítségével figyelemmel tudjuk kísérni az otthonunk történéseit, abban az esetben is, amikor nem tartózkodunk otthon. Az internethez különféle módon tudnak csatlakozni az IoT eszközök, ez leggyakrabban a Wifi által történik. [17] A Statista jelentése szerint az okosotthonok száma 2025-ig elérheti a 478.2 millió okosotthont világszerte. [16] A Deloitte felmérés szerint egy átlagos amerikai háztartásban 25 egymáshoz csatlakoztatott eszköz található meg. [12] A felhasználók körében a legnépszerűbb IoT eszközök közé tartoznak a termosztátok, biztonsági kamerák, zárak, hangszórók. [19] Ezen kívül még népszerűek az okosajtócsengők kamerával, okosvillanykapcsolók, okosfüstjelzők, okosizzók, okoskonnektorok is. [45]

2. Ábra: Az IoT használata az okosotthoni rendszerben. [14]

A hangasszisztensek igen népszerűek lettek, mint például az Amazon Alexa, Google Assistant vagy az Apple Siri. [17] Minél több eszközt csatlakoztatunk az internetre, annál nagyobb veszélynek leszünk kitéve. [44] Sokan úgy gondolják, hogy egy okosház kiépítése költséges viszont, ha jobban bele gondolunk az okosotthonok által számos előnyre tehetünk szert. Ez mellett pedig takarékoskodni is tudunk, ezért megéri választani az okosotthont még ha költségesebb is, mint egy átlagos ház kiépítése. Az okosotthon biztosítsa a tulajdonos, illetve az ott lakók kényelmét, költségmegtakarítását, és a biztonságát. A biztonság egyre fontosabbá vált, és mindenki azt szeretné, ha otthona biztonságban lenne, akkor is, amikor távol tartózkodik otthonától. Az okosotthon által ez is lehetséges, hiszen a távoli vezérlésnek köszönhetően bárhol is tartózkodunk a világon az internet által folyamatosan tudjuk például az okostelefonunk segítségével otthonunkat figyelni. [21] [38]

A biztonsági kihívások és ajánlások

Az IoT eszközök biztonsága aggodalomra adhatnak okot, hiszen ezek az eszközök gyenge vagy semmilyen védelemmel nem rendelkeznek. [43] Az IoT a kibertámadások, és egyéb veszélyek célpontjául vált. [10] Ha a biztonságot vesszük figyelembe tudnunk kell, hogy nem minden gyártónak az elsődleges célja, hogy minél biztonságosabb eszközt hozzon létre, inkább más szempontok kerülnek előtérben a biztonság helyett, mint például a profit szerzés, vagy az olcsóbb és gyorsabb megjelenítés. [23] Az IoT-vel foglalkozó szakemberek kihívásai, hogy biztosítsák, a hálózatok, az adatok, és az eszközöknek a védelmét. [37] Az

elmúlt évek során több olyan támadás is történt az IoT eszközöket iránt, amelyek esetében gyenge vagy rosszul védett IoT eszközök miatt történtek a támadások. A támadók az eszközöket próbálták támadni, és próbálták kihasználni a sebezhetőségeket, és a gyenge biztonsági megoldásokat. [42] Egyre többféle okoseszköz vásárolható meg, az egyik legnépszerűbb a felhasználók körében a biztonsági kamera. Az olcsó IP kamera az egyik leggyakrabban feltört eszközök közé tartozik. [20] Az IoT biztonsági kihívások, valamint a veszélyek egyik leglátványosabb példája 2016-ban történt meg, amikor az USA keleti partján DNS-szolgáltatásleállás következett be, valamint az Egyesült Államok más területein is. A támadás DDoS támadássorozat volt, és a támadás három hullámban történt. A következménye pedig az lett, hogy több tízmillió IP-cím vált elérhetetlenné. A támadásban IoT eszközökre épülő botnetek vettek részt, és nagy szerepe volt a Mirai néven ismert malwernek. [44] A Palo Alto Networks 42 kutatói 2020-as jelentése szerint az IoT eszközök több mint fele ki van szolgáltatva különböző típusú támadásoknak. A személyes és bizalmas adatokhoz a támadók könnyen hozzá tudnak jutni, ami kiberbiztonsági szempontból hatalmas kockázatot jelent. [24] Egyes szakértők szerint fontos lenne a gyártók támogatása a biztonság növelése érdekében. [26] Az NCC Group és a Global Cyber Alliance (GCA) végzett kutatásban az okosotthonban található IoT eszköz elleni irányuló támadásokat elemezték. A kutatásnak az eredménye szerint egy hét alatt 12.807 támadás érte ezeket az eszközöket. [29] Az ESET véleménye szerint fontos lenne, hogy a vásárlók az eszközök megvásárlása előtt néhány szabályra oda figyeljenek, mint például az eszközök megvásárlása előtt fontos lenne utána nézni az adott eszköz leírásának, valamint fontos lenne elkerülni azokat a márkákat, melyek kevésbé ismertek. [20] Az IoT eszközök gyártásában Kínának igen meghatározó szerepe van, és fen áll annak a veszélye is, hogy az adott eszköz nem rendelkezik megfelelő biztonsági védelemmel. A felhasználók sokan úgy használják az IoT eszközöket, hogy nincsenek még alapvető ismereteik sem arról, hogy hogyan kellene megvédeniük az IoT eszközöket a kibertámadásoktól. [40] Az Európai Távközlési Szabványosítási Intézet (ETSI) által elérhető az IoT eszközök kiberbiztonsági szabványa. [31] [32] A SANS és a Nemzeti Kibervédelmi Intézet (NKI) közös kiadványában olvashatunk az otthonokban található okoseszközökről, melyben arról írnak, hogy a legtöbb gyártónak nincs tapasztalata kiberbiztonsági téren, és a legtöbb eszköz nem rendelkezik védelemmel. Fontos lenne, hogy csak azokat az eszközöket csatlakoztassuk az internethez, melyekre tényleg szükségünk van. A frissítés is fontos, ezért minden eszköz fontos, hogy frissítve legyen. [27] A Nemzeti Kibervédelmi Intézet (NKI) és az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) közösen készített összefoglalásában írnak arról, hogy hogyan kellene használni biztonságosan az IoT eszközöket. Ezek közül néhány ajánlást megemlítenék, mint például azt, hogy az eszközöket biztonságosabbá tehetjük úgy, hogy például erős jelszavakat használunk, és amennyiben elérhető, akkor beállítjuk a kéttényezős hitelesítést (2FA). Az alkalmazások ellenőrzése is fontos, mivel a hivatalos áruházból letöltött alkalmazások a legbiztonságosabbak. Figyelembe kell venni azt is, hogy a telepítés előtt milyen információkat fogunk majd megadni, illetve, hogy milyen engedélyeket hagyunk majd jóvá. Abban az esetben, ha támadás érné az eszközöket csökkenthetjük a veszteségünket úgy, hogy elkülönítsük a munkára használt, és az otthonunkban használt eszközöket. [39] Fontos megemlíteni, hogy minden új eszköz, ami csatlakozik az internethez biztonsági kockázatot rejthet, ezért fontos lenne, hogy megfelelő figyelmet fordítsunk ezekre az eszközökre. A Nemzetbiztonsági Szakszolgálat Nem-

zeti Kibervédelmi Intézet odalán elérhető a CTI tájékoztató az otthoni hálózatok biztonságáról, melyben javaslatok találhatóak meg a felhasználók számára, melyek segítségével az otthoni hálózatukat biztonságosabbá tehetik. [44] A Nemzeti Kibervédelmi Intézet oldalán szintén megtalálható egy CTI tájékoztató az IoT eszközök biztonsági kérdéseivel az okosotthonokban. Ennek a dokumentumnak a célja, hogy bemutassa az IoT eszközöket, a biztonsági hiányosságokat, valamint megoldásokat adjanak a kockázatok elkerülésére. [45]

ÖSSZEGZÉS

A tanulmány célja az volt, hogy bemutassa, hogy az okoseszközök használata számos előnnyel jár az okosotthonokban, viszont ezeknek az eszközöknek a használata az előnyök mellett számos kihívást is rejthet. Az okoseszközök igen hasznosak a mindennapi életünkben, hiszen segítik a mindennapi tevékenységeink elvégzését, és számos más előnyt nyújtanak, viszont nem szabad megfeledkezni arról sem, hogy ezeknek az eszközöknek a használata veszélyeket is hordozhat. Nem szabad megfeledkezni arról sem, hogy a gyártók felelőssége is fontos szerepet játszik, viszont a piaci verseny, és a profit szerzése sokszor előtérbe kerül a biztonság helyett. A felhasználókat is meg kell említeni, hiszen a felhasználóknak is fontos szerepük van az IoT eszközök biztonságosabbá tételéhez, viszont a felhasználók közül sokan még az alapvető ismeretekkel sem rendelkeznek, hogy megvédjék az eszközöket a kibertámadásoktól. [6] A biztonság komoly kihívást jelent az IoT eszközök esetében, és akár a jövőben súlyos következményeket is vonhat maga után, ha nem foglalkozunk megfelelően az IoT eszközök biztonságával. Az IoT technológia várhatóan a jövőben még fontosabb szerepet fog kapni a társadalomban, és még több eszköz fog csatlakozni az internethez, ami biztonság szempontjából aggodalomra adhat okot. [30]

FELHASZNÁLT IRODALOM

[1] A Brief History of the Internet of Things [Online]. Elérhető: https://www.dataversity.net/brief-history-internet-things/ (Letöltve: 2022.03. 20.)
[2] Hol alkalmazható az IoT? [Online]. Elérhető: https://iotzona.hu/meg-tobb-iot/hol-alkalmazhato-az-iot (Letöltve: 2022. 03. 25.)
[3] Mesterséges intelligencia: A negyedik ipari forradalom, [Online]. Elérhető: https://books.google.rs/books?id=tx3NDwAAQBAJ&printsec=frontcover&rdir_esc=y#v =one page& q&f=false (Letöltve: 2022. 04. 07.)
[4] State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time, [Online]. Elérhető: https://iot-analytics.com/number-connected-iot-devices/ (Letöltve: 20 22. 04. 09.)
[5] A tárgyak internete-IoT, [Online]. Elérhető: https://hu.rs-online.com/web/gener alDisplay.html?id=i/iot-internet-of-things (Letöltve: 2022. 04. 09.)
[6] A 10 legjobb otthoni automatizálás az IoT (dolgok internete) használatával, [Online]. Elérhető: https://ciksiti.com/hu/chapters/6280-the-10-best-home-automation-using-iot-internet-of-things (Letöltve: 2022. 04. 09.)
[7] Mit jelent a COVID-19 az intelligens otthoni technológiához? [Online]. Elérhető: http s://hu.denizatm.com/pages/48116-what-covid-19-has-meant-for-smart-home-technology (Letöltve: 2022. 04. 09.)

[8] IT, OT, IoT - a biztonságosnak hitt környezet is potenciális veszélyforrása válhat, [Online]. Elérhető: https://www.itbusiness.hu/technology/aktualis_lapszam /kiadvanyok/clico-2021/it-ot-iot--a-biztonsagosnak-hitt-kornyezet-is-potencialis-veszelyforrassa-val hat (Letöltve: 2022. 04. 10.)
[9] Mezei Kitti: A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre, Állam és Jogtudomány, LXI. évfolyam, 4.szám 2020
[10] Samuel Greengard: The Internet of Things (MIT Press Essential Knowledge series), Massachusetts Institute of Technology, 2021, ISBN: 9780262542623
[11] Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030 [Online]. Elérhető: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (Letöltve: 2022. 04. 11.)
[12] Deloitte: How the Pandemic Stress-Tested the Increasingly Crowded Digital Home, [Online]. Elérhető: https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-pandemic-stress-tested-digital-home.html(Letöltve: 2022. 04. 11.)
[13] Hogyan fejleszthetjük otthonunkat okosotthonná? [Online]. Elérhető: https://okosotthon.bolt.hu/webaruhaz/okosotthon-diy-blog-termektesztek/hogyan-fejleszthetjuk-otthonunkat-okosotthonna/ (Letöltve: 2022. 04. 12.)
[14] Zia, Ahmad. (2020). A Research Paper on Internet of Things based upon Smart Homes with Security Risk Assessment using OCTAVE Allegro. International Journal of Engineering Research and. V9. 10.17577/IJERTV9IS060692. [Online]. Elérhető: https://www.researchgate.net/publication/342538259_A_Research_Paper_on_Internet_ o f _Things_based_upon_Smart_Homes_with_Security_Risk_Assessment_using_OCTAVE_Allegro (Letöltve: 2022. 04. 25.)
[15] Mi az IoT-biztonság? [Online]. Elérhető: https://azure.microsoft.com/hu-hu/overview/internet-of-things-iot/iot-security-cybersecurity/ (Letöltve: 2022. 04. 25.)
[16] Number of Smart Homes forecast in the World from 2017 to 2025, [Online]. Elérhető: https://www.statista.com/forecasts/887613/number-of-smart-homes-in-the-smart-home-market-in-the-world (Letöltve: 2022. 10. 14.)
[17] Minden amit az Okos Otthonról tudni kell, [Online]. Elérhető: https://bitthon.hu/2022/03/27/minden-amit-az-okos-otthonrol-tudni-kell/ (Letöltve: 2022. 04. 20.)
[18] 30 Smart Home Statistics for All High-Tech Enthusias, [Online]. Elérhető: https://comfyliving.net/smart-home-statistics/ (Letöltve: 2022. 04. 27.)
[19] Dinamikus növekedés előtt áll az okosotthon piac, [Online]. Elérhető: https://iotzona.hu/meg-tobb-iot/dinamikus-fejlodes-elott-all-az-okosotthon-piac (Letöltve: 2022. 05. 02.)
[20] Az okoseszközök valóban kényelmesek, de biztonságosak is? [Online]. Elérhető: https://www.eset.com/hu/hirek/az-okoseszkozok-kenyelmesek-de-vajon-biztonsagosak-is-2020/ (Letöltve: 2022. 05. 03.)
[21] Teljes körű távoli hozzáférés,[Online]. Elérhető: https://www.okosotthon.me/telj eskoru-tavoli-hozzaferes/ (Letöltve: 2022. 05. 07.)

[22] Sher Ali & Syed Babar Ali Rizvi & Yousaf Ali & Afia Zafar, 2020. "Survey Paper On Iot Attacks And Its Prevention Mechanisms," Information Management and Computer Science (IMCS), Zibeline International Publishing, vol. 3(2), pages 38-41, December.
[23] Simon János, "A tárgyak internete – Internet of Things (IoT)", Proceedings of the Conference: A Magyar Tudomány Napja a Délvidéken - 2014, pp. 1-9, Novi Sad, Serbia, 2014.
[24] 2020 Unit 42 IoT Threat Report, [Online]. Elérhető: https://iotbusinessnews.com /download /white-papers/UNIT42-IoT-Threat-Repo rt.pdf (Letöltve: 2022. 05. 08.)
[25] A Tanács következtetéseket fogadott el a csatlakoztatott eszközök kiberbiztonságáról, [Online]. Elérhető:https://www.consilium.europa.eu/hu/press/press-releases/2020/12/02/c ybersecurity-of-connected-devices-council-adopts-conclusions/ (Letöltve: 2022. 05. 09.)
[26] Óvatosságra intenek az okos eszközök kapcsán a szakértők, [Online]. Elérhető: https://www.ludovika.hu/magazin/eloado/2021/10/07/ovatossagra-intenek-az-okos-eszkoz ok-kapcsan-a-szakertok/ (Letöltve: 2022. 05. 10.)
[27] Az okos otthon eszközök – Sans Ouch! – Augusztus, [Online]. Elérhető: https://nki.gov.hu/en/it-biztonsag/kiadvanyok/sans-ouch/okos-otthoni-eszkozok-sans-ou ch-augusztus/ (Letöltve: 2022. 05. 11.)
[28] Kiberbiztonság: hogyan kezeli az EU a kiberfenyegetéseket? [Online]. Elérhető: https://www.consilium.europa.eu/hu/policies/cybersecurity/ (Letöltve: 2022. 10. 16.)
[29] Smart Home Experiences Over 12,000 Cyber-Attacks in a Week, [Online]. Elérhető: https://www.infosecurity-magazine.com/news/smart-home-experiences-cyber/ (Letöltve: 2022. 05. 13.)
[30] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in internet of things: Challenges, solutions and future directions," in Proc. 49th Hawaii International Conference on System Sciences (HICSS). IEEE, 2016, pp. 5772–5781
[31] Uniós szabvány készült a konzumer IoT eszközök biztonságossá tételéhez, [Online]. Elérhető:https://nki.gov.hu/it-biztonsag/hirek/unios-szabvany-keszult-a-konzumer-iot-esz ko zok-biztonsagossa-tetelehez/ (Letöltve: 2022. 05. 13.)
[32] Cyber Security for Consumer Internet of Things, [Online]. Elérhető: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v 010 101p.pdf (Letöltve: 2022. 05. 15.)
[33] 10 tudnivaló a Dolgok Internetéről, [Online]. Elérhető: https://iotzona.hu/big-data/10-tudnivalo-a-dolgok-interneterol (Letöltve: 2022. 05. 16.)
[34] Az okos otthon valódi előnye, [Online]. Elérhető: https://otthonautomatika.hu/blog/107-az-okos-otthon-valodi-elonyei/ (Letöltve: 2022. 05. 17.)
[35] Digital around the world, [Online]. Elérhető: https://datareportal.com/global-digital-overview (Letöltve: 2022. 05. 18.)
[36] Fűtés okos otthonnal: Akár 30%-kal kevesebb energia és teljes kényelem, [Online]. Elérhető:https://www.oott.hu/futes-okos-otthonnal-akar-30-kal-kevesebb-energia-es-

telj eskenyelem/?gclid=Cj0KCQjwm6KUBhC3ARIsACIwxBhroUHgu5OSjfgiu-qgWsCwsl 8k2XBziPitf0k1H8OfmVwdFz3_9lMYaAhXtEALwwcB (Letöltve: 2022. 05. 19.)
[37] Az IoT rendszerek biztonságának a növelése, [Online]. Elérhető: https://computerworld.hu/biztonsag/iot-rendszerek-biztonsaganak-novelese-266828.html (Letöltve: 2022. 05. 19.)
[38] Az okosotthon és az épületautomatika, [Online]. Elérhető: https://ezermester.hu/cikk-9030/Okosotthon_es_epuletautomatika (Letöltve: 2022. 05. 20.)
[39] Tippek az otthoni kiberbiztonság megteremtéséhez, [Online]. Elérhető: https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/tippek-az-otthoni-kiber-biztonsag-megteremtesehez/ (Letöltve: 2022. 05. 21.)
[40] „Kütyük támadása" – az IoT eszközök veszélyei, [Online]. Elérhető: https://ahrt.hu/hu/kutyuk-tamadasa-az-iot-eszkozok-veszelyei-2 (Letöltve: 2022. 10. 15.)
[41] Otthonunk okosítása, [Online]. Elérhető: https://ezermester.hu/cikk-8179/Ott honunk_okositasa (Letöltve: 2022. 05. 24.)
[42] Mi az IoT-biztonság? [Online]. Elérhető: https://azure.microsoft.com/hu-hu/overview/internet-of-things-iot/iot-security-cybersecurity/ (Letöltve: 2022. 05. 25.)
[43] Kovács László: A kibertér védelme, Dialóg Campus Kiadó, Budapest, 2018
[44] Otthoni hálózatok biztonsága, [Online]. Elérhető: https://nki.gov.hu/it-biztonsag/elemzesek/otthoni-halozatok-biztonsaga/ (Letöltve: 2022. 09. 13.)
[45] IOT eszközök biztonsági kérdései – Az okosotthon, [Online]. Elérhető: https://nki.gov.hu/it-biztonsag/elemzesek/iot-eszkozok-biztonsagi-kerdesei-az-okosotthon/ (Letöltve: 2022. 10. 14.)