DANGERS OF SMART DEVICES | AZ OKOSESZKÖZÖK VESZÉLYEI

MANDIĆ Dorottya[1]

Abstract

Smart devices have become part of our everyday life. We can hardly imagine our daily lives without our smart devices. However, you can hear more and more that the use of smart devices can be dangerous. Many of the users buy the given smart device with only basic knowledge of how to use it safely these devices. In addition, manufacturers often prioritize profit over safety. This study shows, some of the dangers that smart devices can cause, and which are the most popular smart devices.

Keywords

smart devices, Internet of Things, dangers, security, IoT

Absztrakt

Az okoseszközök a mindennapi életünk részévé váltak. Szinte már el sem tudjuk képzelni a mindennapi életünket az okoseszközeink nélkül. Egyre többet lehet hallani arról, hogy az okoseszközök használata veszélyekkel járhat. Ezen kívül a felhasználók sokan úgy vásárolják meg az okoseszközöket, hogy még csak alapvető ismeretekkel sem rendelkeznek arról, hogy hogyan tudnák biztonságosan használni. A gyártók is sokszor előtérbe helyezik a haszon szerzést a biztonság helyett. A tanulmány bemutatja az egyes veszélyeket, melyeket az okoseszközök használata okozhat, valamint, hogy melyek a legnépszerűbb okoseszközök.

Kulcsszavak

okoseszközök, dolgok internete, veszélyek, biztonság, IoT

[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

BEVEZETŐ

A „dolgok internete vagy angolul az Internet of Things (IoT)" kifejezést egyre többet lehet hallani. [40] Az IoT eszközöknek a száma rohamosan nő világszerte, és jelenleg megközelítőleg 15 milliárd IoT eszköz van jelen, ami várhatóan 2030-ra elfogja érni a 29 milliárd IoT eszközt. Az IoT eszközöknek a száma évről évre növekedni fog, és 2030-ra várhatóan Kínában lesz a legtöbb IoT eszköz. [1] Az IoT eszközöket már számos területen használják, és egyre több hétköznapi eszköz és tárgy is csatlakozik az internetre. [2] A felhasználók körében az okoseszközök egyre népszerűbbek. A Huawei Technologies Hungary felmérése szerint a magyar felhasználók körében az okoseszközök rendkívül népszerűek, és egyre többen használják az okoseszközeiket például a sportoláshoz vagy az egészségügyi funkciók méréséhez. [3] A felmérés szerint az emberek 60%-a például az eszközök által mért értékek alapján orvoshoz fordulna. [5] Az eNet 2018-ban végzet kutatása szerint például minden tizedik felnőtt internetező Magyarországon használ már okosórát vagy okoskarkötőt. [6] Az INNObyte 2021-ben végzett kutatása szerint a felhasználók egyre többen használnak okoseszközöket az otthonaikban. [4] Egyre többet lehet hallani arról is, hogy mennyire sérülékenyek az IoT eszközök biztonsági szempontból, és hogy a gyártók sokszor előtérbe helyezik a haszon szerzést, és a gyors megjelenítést a biztonság helyett. A Gemalto biztonsági vállat 2017-es felmérése szerint, az IoT eszköz gyártók, és szolgáltatók a költségvetésükből csak a 11%-át költik az IoT eszközök biztonságára. Ezen kívül a felhasználók 90%-a nem bízik az okoseszközök biztonságában. Az egyik fő aggodalom, hogy a hackerek átvehetik az irányítást az eszközeik felett. A felmérésben résztvevők mindössze 14%-a válaszolta, hogy megfelelően tájékozódott az IoT eszközök biztonságát illetően. [7] Az okoseszközöknek a használata számos előnnyel jár a mindennapi életben, hiszen segítik a mindennapi tevékenységeink elvégzését, az egészségünket is figyelemmel tudjuk kísérni a használatuk által, otthonunkat is kényelmesebbé, jobbá és biztonságosabbá tehetjük, ez mellett még számos előnye van annak, ha okoseszközöket használunk. A gyártók felelőssége fontos szerepet játszik az IoT eszközök biztonságában, de sajnos a biztonság sokszor háttérbe kerül. A felhasználóknak is fontos szerepük van az okoseszközök biztonságos használatában, viszont sokan még csak alapvető ismeretekkel sem rendelkeznek, hogy biztonságosan tudják használni ezeket az eszközöket. [9] Az IoT eszközökkel kapcsolatban az egyik aggodalmat az internetre csatlakoztatott eszközöknek a száma jelenti, valamint a sebezhetőség, amit a bűnözök kihasználhatnak. Ezen kívül az IoT eszközök hatalmas mennyiségű adatokat generálnak, ez által fennáll annak a veszélye is, hogy illetéktelen személyek hozzáférhetnek ezekhez az adatokhoz. [8]

Okoseszközök népszerűsége

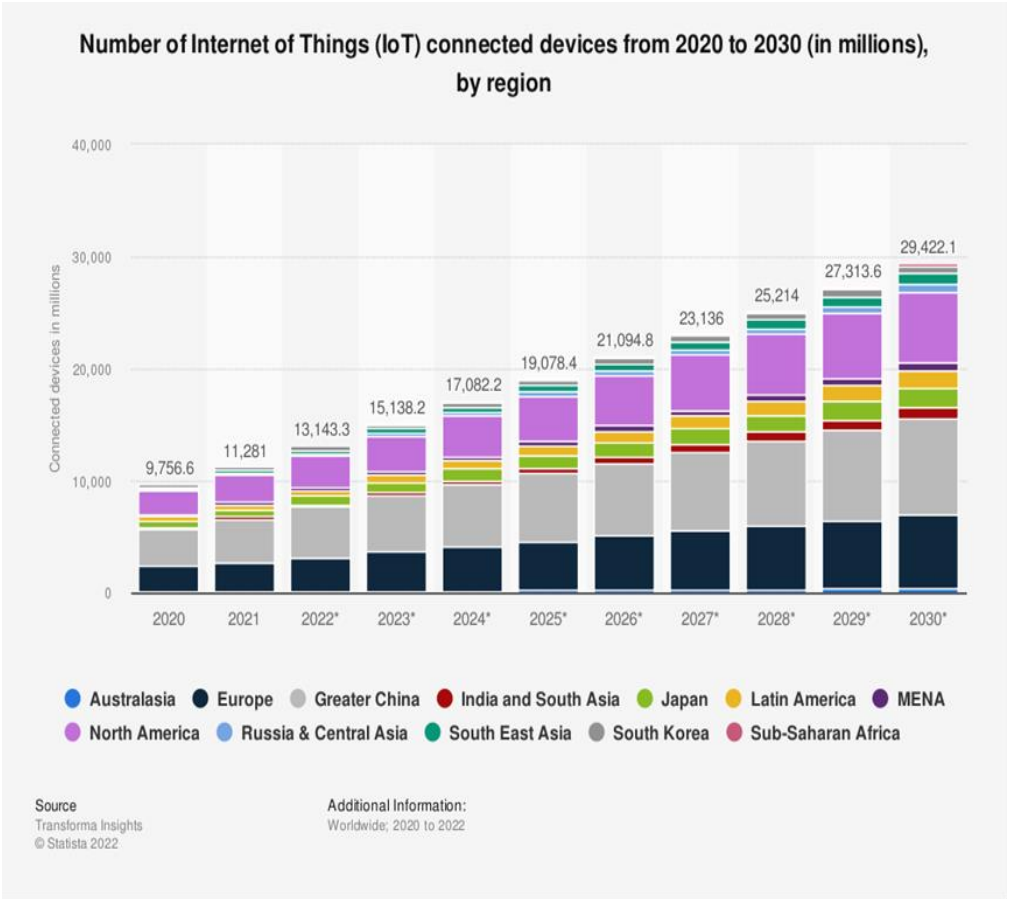
Manapság már szinte mindenki használ legalább egy okoseszközt például okostelefont. A Statista jelentése szerint 2019 és 2020 között jelentősen megnőt világszerte a csatlakoztatott hordozható eszközöknek a száma. [27] 2021-ben az eNet felmérése szerint Magyarországon 6,2 millióan használnak okostelefont. [10] Az okosóra is igen népszerű a felhasználók körében, hiszen lehetőség van az okosórán keresztül beszélni, üzeneteket küldeni és fogadni, a mozgást és a pulzust, valamint az alvás változásait is figyelemmel tudjuk kísérni. [11] A Huawei Technologies Hungary 2021-ben készített felmérést, melyben közel 8000 ezer válaszadó vett részt. A felmérésben azt vizsgálták, hogy mennyire népszerűek a különféle okoseszközök a magyarok körében, és hogy vásárláskor, melyek a legfontosabb

szempontok, amit figyelemmel vesznek, illetve, hogy milyen funkcióra használják az okoseszközöket. A válaszok alapján „63%-a visel okosórát vagy okoskarkötőt, 54%-a rendelkezik vezeték nélküli fülhallgatóval, 12%-a rendelkezik okosmérleggel vagy vérnyomásmérővel, és 15%-a válaszolta, hogy nem használ semmilyen okoseszközt.” A válaszok alapján, ami a vásárlást illeti a legfontosabb szempontok közé tartozik a hosszú üzemidő, ár, és a kényelem. [14]

1. Ábra: Okoseszközök. (forrás:https://www.jtsec.es/iot-cybersecurity)

A Samsung is végzett kutatást 2021-ben az Impetus Research által, melyben 815 válaszadó vett részt 18 és 64 év között. A felmérésben a magyar emberek otthonaikban használt okoseszközeik használatát vizsgálták. A felmérés szerint a járvány ideje alatt sokan vásároltak új okoseszközöket, és legtöbben a válaszadók közül okostelefont vásároltak. [15] Az INNObyte 2021-es felmérése szerint a válaszadók 83%-a rendelkezik otthonában okoseszközzel. A válaszadók 32%-a válaszolta azt, hogy azért vásárolt okoseszközt, mert fontos számára a kényelem, 17%-a szórakozás miatt vásárolt okoseszközt, és a 14%-a az energiamegtakarítás véget. A válaszadók 93%-a szerint előnyös, ha otthonában vannak okoseszközök, 82%-a szerint kényelmes a használatuk, és megkönnyítik a mindennapi életet az okoseszközök használata, 49%-a pedig azt válaszolta, hogy időmegtakarítást ért el az okoseszközök használata által. Azok a válaszadók, akik azt válaszolták, hogy nem rendelkeznek okoseszközökkel anyagi, valamint biztonsági okokkal indokolták. Egyes felhasználók például veszélyt látnak abban, hogy otthonaikban okoseszközöket használjanak. [4] 2022-ben a Deloitte végzett felmérést a digitális fogyasztói trendekről, melyben 36 ezer felhasználó vett részt világszerte, és 1000 Magyarországon. A 18 évestől az 54 éves kor-

osztály a legnagyobb érdeklődést az okostelefonok iránt mutatta. [12] A Reviews.org felmérése, mely szintén 2022-ben készült a 18 éves vagy ennél idősebb amerikaiak válaszai alapján a legnépszerűbb okoseszközök a személyes használatra az okostelefon, okosóra, és a tablet. Az otthonukban használt okoseszközök közül pedig a legnépszerűbbek például a hangszórók, tévék, hűtők, okoscsengők, biztonságkamerák és zárak. [13] A Digital Trends 2023-ban a legjobb otthoni okoseszközök közé sorolta a következőket ezekből néhányat megemlítenék például a hangasszisztens, biztonsági kamera, termosztát, robotporszívó. [17] A Statista szerint az IoT eszközöknek a száma várhatóan 2030-ban Kínában lesz a legnagyobb, majd ezt fogja követni Európa és Észak Amerika. [18]



2. Ábra: Az IoT eszközök száma területek szerint 2020-tól 2030-ig.
(forrás:https://www.statista.com/statistics/1194677/iot-connected-devices-regionally/)

Okoseszközök veszélyei

Az okoseszközök használatának számos előnye van, de ez még nem jelenti azt, hogy ezeknek az eszközöknek a használata biztonságos is. Az utóbbi időben egyre többet lehet hallani arról, hogy az okoseszközeinken keresztül például megfigyelhetik a szokásainkat, vagy ellophatják a személyes adatainkat. A tömeggyártásban alacsony költségvetés-

ből készült eszközök következménye lehet, hogy gyenge biztonsági megoldásokat tartalmaznak. [19] Az IoT eszközök az otthonokban adatokat gyűjthetnek arról, hogy például a felhasználók mikor tartózkodnak otthon, vagy hogy milyen fogyasztási szokásai vannak. [22] Az IoT eszközök sérülékenyek lehetnek, melyeket a támadók kihasználhatnak, és az utólagos javítást nem egyszerű elvégezni. [20] Az OWASP (Open Web Application Security Project) az IoT Sérülékenységek Projektje szerint a legfontosabb IoT sérülékenységek közül néhányat megemlítenék például gyenge jelszavak, gyenge titkosítás, hiányzó frissítési mechanizmus. [21] Az IoT eszközök esetében gyakori, hogy gyenge jelszavakat alkalmaznak, és nem mindegyik gyártó kötelezi például a felhasználót, hogy módosítsa a készülék alapértelmezett jelszavát. [30] Ezért fontos, hogy elvégezzük az alapvető biztonsági beállításokat, ami azt jelenti, hogy az alapértelmezett felhasználónevet, és jelszót meg kell változtatni. Ez azért fontos, mert a megvásárolt eszközök esetében ezek azonosak lehetnek. A felhasználónév, és a jelszó kiválasztásakor például fontos figyelembe venni, hogy olyat válasszunk, ami nem található ki könnyen. Ez mellett az is fontos, hogy tartalmazzon számokat, valamint speciális karaktereket, és a hosszúságra is fontos figyelni. [31] A NordVPN felmérést végzett hét országban az IoT eszközök biztonságát illetően. Az országok között szerepelt Németország, Egyesült Államok, Ausztrália, Kanada, Franciaország, Hollandia és Nagy Britannia. A legrosszabb helyre az országok közül az IoT biztonságát illetően Nagy Britannia került, mivel a felmérésből kiderült, hogy legkevesebb intézkedést az eszközeik biztonsága érdekében a vizsgált országok közül Nagy Britanniában teszik. A többi országhoz képest, Nagy Britanniában a válaszadók 95%-a válaszolta, hogy rendelkezik legalább egy okoseszközzel, és 24%-a azt válaszolta, hogy egyáltalán nem tesz semmilyen intézkedést az eszközök védelme érdekében. A hét ország közül a válaszok alapján a legkevesebb IoT eszközzel Franciaország rendelkezik. A felmérésben résztvevők 41.4%-a gondolja úgy, hogy a gyártóknak kellene felelőséget vállalnia a biztonságért, 55.9%-a szerint a felhasználók felelőssége lenne, még a válaszadók 45.3%-a úgy gondolja, hogy az internetszolgáltatók felelősége lenne. [35] [36] [37] 2013-ban egy LG okostévével rendelkező felhasználó fedezte fel, hogy az okostévéje adatokat gyűjt a nézési szokásairól, akkor is, ha ez a funkció ki van kapcsolva. A Samsung okostévénél történt már olyan esett, hogy az okostévé beszédfelismerő funkciója személyes beszélgetéseket rögzített. [26] Mivel az okostévé rendelkezhet beépített kamerával, mikrofonnal, valamint hangfelismeréssel, ez által megfigyelhetik a beszélgetéseinket, és felvétel is készülhet róla. [23] 2019-ben az FBI hatósági közleményt adott ki az okostévékkel kapcsolatban, melyben felhívták a figyelmet, hogy az okostévék gyártója vagy a telepített alkalmazások fejlesztői az okostévén keresztül megfigyelhetik a felhasználókat. A Samsung például jelezte a felhasználóknak, hogy kerüljék a személyes beszélgetéseket az okostévék előtt, ha nincs kikapcsolva a hangvezérlő funkció. A Northeastern University, valamint az Imperial College London szerint a gyártók, mint például a Samsung vagy az LG, illetve az Apple okostévéi a felhasználók bizonyos adatait kiadják harmadik félnek. A kiberbűnözők pedig a haszonszerzés céljából akár az okostévé kamerája és mikrofonja által felvételeket készíthet. [28] 2019-ben az Amazon Echo valamint a Google Home okosrendszerről derült ki, hogy adatvédelmi szempontból ezek az eszközök sokkal több adatot gyűjtenek össze, mint amire lett volna például engedélyük, hiszen olyan információkat is rögzítettek, melyeket a tulajdonos nem szeretett volna megosztani. A Philips Hue okosvillanykörtéről is kiderült, hogy könnyen feltörhető, és mivel Kínában készül-

nek, így nehéz elkerülni, hogy ne legyenek sérülékenyek. [23] Az Amazon Ring otthonokban használt biztonsági rendszerről például kiderült, hogy adatokat oszt meg a Google, valamint a Facebookkal. A Roomba robotporszívó igen népszerű a felhasználók körében, viszont a kutatók az feltételezik erről a robotporszívóról, hogy a Lidar technológiát használva térérzékeléshez kifejlesztett lézeres letapogatóval képes hangot érzékelni. [24] 2018-ban az ESET figyelmeztetést adott ki, hogy a Dongguan Diqee 360 robotporszívóban biztonsági hiányosságokat fedeztek fel a szakértők, és mivel rendelkezik 360 fokos kamerával, abban az esetben, ha a támadók feltörnék, teljes képet kapnának otthonunkról. [25] Egyes okoseszközök nem csak megkönnyítik a mindennapi életünket, de a biztonságunkról is gondoskodik, mint például a biztonsági kamera. A felhasználók körében igen népszerűek, hiszen a kamera segítségével megfigyelhetjük például az otthonunkat, akkor is, ha nem tartózkodunk otthon. Az olcsó IP kamerák, amik az otthonunk megfigyelésére szolgálnak sajnos az egyik legtöbbet feltört eszközök közé tartoznak. Volt már olyan esett, hogy egy nagyobb kínai gyártónak az eszköze képeket osztott meg idegen otthonokról a többi felhasználóval. [29] A Nemzeti Kibervédelmi Intézet 2023-ban közzétette, hogy sebezhetőségeket találtak az olasz, valamint a brit kutatók a népszerű TP-Link Tapo L530E okosizzóban. Ez az okosizzó igen népszerű, és megvásárolható például Amazonon is. [16]

ÖSSZEGZÉS

Az okoseszközök egyre népszerűbbek a felhasználók körében, és egyre többen vásárolnak már ilyen eszközöket. Legtöbben a kényelem, a szórakozás, az időmegtakarítás vagy az otthonuk biztonsága, illetve az egészségi állapotuk nyomon követese miatt vásárol okoseszközt. A felhasználók többsége rendelkezik okoseszközzel, és hasznosnak tartja ezeknek az eszközöknek a használatát. Viszont vannak olyan felhasználók, akik veszélyt látnak az okoseszközök használatában, és nem bíznak a biztonságukban. A felhasználók közül, akik okoseszközöket használnak sokan nem rendelkeznek alapvető ismeretekkel sem, hogy biztonságosan tudják használni az okoseszközeiket vagy egyáltalán nem tesznek semmilyen intézkedést az eszközök védelme érdekében. A gyártók pedig sokszor nem helyezik előtérbe a biztonságot. A jövőben várhatóan még több hétköznapi eszköz és tárgy fog csatlakozni az internetre. 2022-ben az Európai Bizottság nyilvánosságra hozta a kiberrezilienciáról szóló törvényjavaslatot (Cyber Resilience Act). A törvényjavaslat kiberbiztonsági szabályokat vezetne be a digitális elemeket tartalmazó termékek gyártói, és fejlesztői számára, és lehetővé tenné, hogy a termékek vásárlói megfelelő tájékoztatást kapjanak az általuk vásárolt, és használt termékek kiberbiztonságáról. A törvényjavaslat szerint „a gyártóknak felelőséget kell majd vállalniuk a termékeik sérülékenységeiért a teljes életciklus alatt.” [32] [33] [34] [39] A törvényjavaslat „minden olyan termékre alkalmazandó lesz, amely közvetlenül vagy közvetve csatlakozik egy másik eszközhöz vagy hálózathoz.” A tagállamok 2023-ban „megállapodtak a digitális termékekre vonatkozó biztonsági követelményekre irányuló közös álláspontról.” [38]

FELHASZNÁLT IRODALOM

[1] Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030 [Online]. Elérhető: https://www.statista.com/statistics/1183 457/iot-connected-devices-worldwide/ (Letöltve:2023.07.28)

[2] Haig Zsolt: Információs műveletek a kibertérben, Dialóg Campus Kiadó, Budapest, 2018.

[3] Kutatás: Már a magyarok kétharmada visel okoseszközt a csuklóján [Online]. Elérhető: https://consumer.huawei.com/hu/press/news/2021/news-210304/ (Letöltve:2023.07.28)

[4] Egyre többen használnak okoseszközöket otthonukban - INNObyte kutatás [Online]. Elérhető:https://innobyte.hu/egyre-tobben-hasznalnak-okoseszkozoket-otthonukban-innobyte-kutatas/ (Letöltve:2023.07.28)

[5] Az okoseszközök előnye a folyamatos egészségmonitoring [Online]. Elérhető: http://medicalonline.hu/informatika/cikk/az_okoseszkozok_elonye_a_folyamatos_egeszseg-monitoring (Letöltve:2023.07.30.)

[6] Egészségtudatosabbak az okosórák, és okoskarkötők hazai használói [Online]. Elérhető: https://enet.hu/egeszsegtudatosabbak-az-okosorak-es-okoskarkotok-hazai-hasznaloi/ (Letöltve:2023.07.30.)

[7] Gemalto survey confirms that consumers lack confidence in IoT device security [Online]. Elérhető: https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/press-release/gemalto-survey-confirms-that-consumers-lack-confidence-in-iot-device-security- (Letöltve:2023.08.01.)

[8] Az IoT eszközök veszélyei [Online]. Elérhető: https://mernoknok.hu/az-iot-eszkozok-veszelyei/(Letöltve:2023.08.01.)

[9] Mandic Dorottya, Simon János: Biztonságossak-e az okosotthonokban használt okoseszközök? Biztonságtudományi Szemle, 4. évf. 4. szám 59-67 (2022)

[10] A plafont súrolja a hazai okostelefon használat [Online]. Elérhető: https://enet.hu/a-plafont-surolja-a-hazai-okostelefon-hasznalat/ (Letöltve:2023.08.03.)

[11] Okoseszközök térhódítása [Online]. Elérhető: https://www.smartos.hu/blog/okoseszkozok-terhoditasa-64 (Letöltve:2023.08.05.)

[12] Digitális Fogyasztói Trendek 2022 [Online]. Elérhető: https://www2.deloitte.com/content /dam/Deloitte/hu/Documents/technology/Digitalis_Fogyasztoi_Trendek_Felmeres_Magyarorszag_2022.pdf (Letöltve:2023.08.08.)

[13] The most popular Smart Home Devices 2022 [Online]. Elérhető: https://www.reviews.org/home-security/most-popular-smart-home-device-statistics/ (Letöltve:2023.08.08.)

[14] Kutatás már a magyarok kétharmada visel okoseszközt a csuklóján [Online]. Elérhető: https://huawei.hu/2021/03/04/kutatas-mar-a-magyarok-ketharmada-visel-okoseszkozt-a-csuklojan/ (Letöltve:2023.08.11.)

[15] Sok az új okoseszköz a magyar háztartásokban, de a bevásárlólista még nem üres [Online]. Elérhető:https://www.samsung.com/hu/news/local/sok-az-uj-okoseszkoz-a-magyar-haztartasokban-de-a-bevasarlolista-meg-nem-ures/ (Letöltve:2023.08.13.)

[16] A támadók TP-LINK okosizzókon keresztül képesek megszerezni jelszavainkat [Online]. Elérhető: https://nki.gov.hu/it-biztonsag/hirek/a-tamadok-tp-link-okosizzokon-keresztul-kepesek-megszerezni-jelszavainkat/ (Letöltve:2023.08.25.)

[17] The best smart home devices for 2023 [Online]. Elérhető: https://www.dig italtrends.com/home/best-smart-home-devices/ (Letöltve:2023.08.26.)
[18] Number of Internet of Things (IoT) connected devices from 2020 to 2030 (in millions), by region, [Online]. Elérhető: https://www.statista.com/statistics/1194677/iot-connected-devices-regionally/ (Letöltve:2023.08.26.)
[19] Dr. Albert Ágota, Üveges András József: Az IoT eszközök biztonsága a személyes adatok tükrében [Online]. Elérhető: https://www.knbsz.gov.hu/hu/letoltes/szsz/2022_2_szam.pdf (Letöltve:2023.08.27.)
[20] Mit tudnak rólunk okoseszközeink? [Online]. Elérhető: https://ikron.hu/okoseszkozok-veszelye/ (Letöltve:2023.08.27.)
[21] Kovács László: A kibertér védelme, Dialóg Campus Kiadó, Budapest, 2018
[22] Eszteri Dániel: Az új technológiák megjelenésének hatása a személyes adatok védelmére: gépi tanulás, blokklánc, internet-of-things, agyhullám-olvasás [Online]. Elérhető: http://real.mtak.hu/133906/1/eszteri.daniel.uj.technologiak.adatvedelem.pdf (Letöltve:2023.08.27.)
[23] Kémkedő eszközök [Online]. Elérhető: https://itlawpro.com/hu/adatvedelem/kemkedo-eszkozok (Letöltve:2023.08.28.)
[24] Az okoseszközök veszélyei a porszívó is kémkedik? [Online]. Elérhető: https://zero itlab.com/hu/blog/az-okos-eszkozok-veszelyei-porszivo-kemkedik (Letöltve:2023.08.28.)
[25] Veszélyben vannak a hálózatba kapcsolt eszközeink? [Online]. Elérhető: https://www.eset.com/hu/hirek/milyen-veszelyek-leselkednek-a-halozatba-kapcsolt-eszkozeinkre/ (Letöltve:2023.08.28.)
[26] Az okos eszközök veszélyei – Lehet, hogy a TV néz téged [Online]. Elérhető: https://crosssec.com/az-okos-eszkozok-veszelyei-lehet-hogy-a-tv-nez-teged/ (Letöltve:2023.08. 28.)
[27] Number of connected wearable devices worldwide from 2019 to 2022 [Online]. Elérhető: https://www.statista.com/statistics/487291/global-connected-wearable-devices/ Letöltve:2023.08.28.)
[28] Milyen tévéje van otthon? Figyelmeztetést adott ki az FBI [Online]. Elérhető: https://hvg.hu/tudomany/20191203_okos_tevekeszulek_lehallgatas_megfigyeles_fbi (Letöltve:2023.08.29.)
[29] Kényelmesek az okoskütyük - de elég biztonságosak is? [Online]. Elérhető: https://www.eset.com/hu/hirek/az-okoseszkozok-kenyelmesek-de-vajon-biztonsagosak-is-2020/ (Letöltve:2023.08.29.)
[30] Kanizsai Viktor: Tárgyak Internete-tárgyak bizonytalansága [Online]. Elérhető: http://www.vmtt.org.rs/mtn2016/503_513_Kanizsai.pdf (Letöltve:2023.08.29.)
[31] Tóth András: Új típusú kihívások az infokommunikációban, Ludovika Egyetemi Kiadó, Budapest, 2023
[32] Kanyarban az uniós IoT-védelmi jogszabály [Online]. Elérhető: https://www .hwsw.hu/hirek/65139/europaiunio-bizottsag-kiberbiztonsag-kiberreziliencia-tervezet.ht ml (Letöltve:2023.08.30.)
[33] State of the Union: EU Cyber Resilience Act - Questions & Answers [Online]. Elérhető: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_5375(Letöltve:2023.0 5.29.)

[34] Új uniós szabályok teszik még biztonságosabbá a hardver- és szoftvertermékeket [Online]. Elérhető: https://infovilag.hu/uj-unios-szabalyok-teszik-meg-biztonsagosabba-a-hardver-es-szoftvertermekeket/ (Letöltve:2023.08.30.)
[35] A brit felhasználók negyede nem védi az okoseszközeit [Online]. Elérhető: https://iot-zona.hu/biztonsag/a-brit-felhasznalok-negyede-nem-vedi-az-okoseszkozeit (Letöltve:2023.08.30.)
[36] Research finds that 24% of Brits aren't securing their IoT devices [Online]. Elérhető: https://www.iottechnews.com/news/2021/jul/22/research-finds-that-24-of-brits-arent-securing-their-iot-devices/ (Letöltve:2023.08.30.)
[37] Almost 9/10 people have at least one IoT device [Online]. Elérhető: https://nordvpn.com/research-lab/iot-device-security/ (Letöltve:2023.08.30.)
[38] A kiberrezilienciáról szóló jogszabály: a tagállamok megállapodtak a digitális termékekre vonatkozó biztonsági követelményekre irányuló közös álláspontról [Online]. Elérhető: https://www.consilium.europa.eu/hu/press/press-releases/2023/07/19/cyber-resilience-act-member-states-agree-common-position-on-security-requirements-for-digital-products/ (Letöltve:2023.08.31.)
[39] A kiberrezilienciáról szóló jogszabály [Online]. Elérhető: https://digital-strategy.ec.europa.eu/hu/library/cyber-resilience-act (Letöltve:2023.08.31.)
[40] Tárgyak internete [Online]. Elérhető: https://sealog.hu/tudastar/fogalomtar/targyak-internete (Letöltve:2023.09.03.)