



Nemzeti Közszerológati Egyetem
Hadtudományi és Honvédtisztképző Kar
Intézményi Tudományos Diákköri Konferencia

Okosotthon rendszerek sérülékenysége a Mesterséges Intelligencia korában

JELIGE: HomEalone

2024.

Tartalomjegyzék

Bevezetés	3
A témaválasztás indokolása	3
Problémafelvezetés	3
1. Okosotthon rendszerek típusai, működése, használata	5
1.1. Mesterséges Intelligencia	7
1.2. Digitális kompetencia	9
2. IoT (Internet of Things)	11
2.1. Működése	11
2.2. Előnyei	11
2.3. Keretrendszere.....	12
3. SOHO (Small office home office)	14
3.1. SOHO rendszerek sérülékenysége	15
3.2. Otthoni Hálózati biztonsági modellek	16
3.3. Hálózati átjárók biztonsági tulajdonságai.....	17
4. Veszélyek	18
4.1. OSI modell.....	19
4.2. NAT támadási felületei.....	20
4.3. Kínai társadalmi kreditrendszer	23
4.3.1. Okosotthonnal való kapcsolat	24
5. Esettanulmány	26
6. Megelőzés és megoldások.....	28
Összegzés	30
Felhasznált irodalom.....	32
Ábrajegyzék	33

Bevezetés

Előző iskolámban volt szerencsém már okosotthon rendszerrel foglalkozni, mivel informatikát tanultam. Legfőbb oka ennek a „találkozásnak” egy megnyert GINOP-os projekt volt (ezt a szakképzési centrum hirdette), melynek keretében kellett egy többszörösen összetett projektet kifejleszteni, ahol a választásunk történetesen egy okosotthon rendszerre esett.

Legfőbb területünk maga az automatizálás volt, a szenzorok beállítása, illetve maga a telemetria kialakítása.

A témaválasztás indokolása

Témaválasztásom másik indoka a személyes kötődésen kívül az okosotthon rendszerek egyre nagyobb elterjedése. Manapság már minden modern építésű házban és ingatlanban egyaránt alapfelszereltségnek tekinthetők ezen rendszerek. Egyre gyakrabban kéri a lakástulajdonosok ezeknek a be- és kiépítését is.

A kényelem nagyon sokat ér, hiszen ténylegesen egy gombnyomással el lehet érni, hogy bekapcsoljon a fűtés, elinduljon akár a klímaberendezés, bekapcsoljon a borhűtő vagy a kapukat várakozás nélkül kinyissuk.

Mindezek miatt tartom különösen időszerűnek ezt a témát, hiszen egyre több vállalkozás foglalkozik okosotthon rendszereknek a kiépítésével. Ezzel egyidejűleg a téma újszerű is, mivel még csak most kezdi el kinőni magát ez az iparág is.

A Mesterséges intelligencia egyre inkább gyorsuló elterjedési tendenciát mutat, illetve intenzívebben fejlődik is. Egyre több rendszerbe kezdik el beépíteni az MI használatát, hiszen sokat könnyít az automatizáláson, az adatok feldolgozásán és azoknak felhő alapú tárolásában is tud segíteni.

Problémafelvezetés

Tekintettel a mai napokra, egyre több esetet olvasni, hallani, hogy az emberi meggondolatlanság, a tudatosság hiánya a forrása a legtöbb kibertámadásnak. Mindig ugyan az a jelszó, mert a gyári jelszavakat az ember nem akarja, vagy nem tudja módosítani. Mindent ugyanúgy hagy a lakásban és legfőképp, túl kiszámítható. Sajnos ezeket az egyszerű tulajdonságokat pedig könnyedén lehet kihasználni.

Továbbá ijesztőbbnél ijesztőbb híreket látni, miszerint akár elektromos fogkeféken keresztül indítanak terheléses támadást DDoS (Distributed Denial of Service - elosztott szolgáltatásmegtagadással járó támadás) technikát használva.¹

Ennek a folyamata úgy néz ki, hogy túlterhelik a hálózati csatornát a küldő és fogadó között, így megbénul a hálózat azon része, nem tudják már az adatokat fogadni. Mivel lebénul a hálózat és ezzel foglalkoznak, máris adott egy lehetőség, hogy egy másik ponton keresztül hozzá lehessen férni a hálózat többi részéhez.

Az információbiztonsági tudatosság az egyik legfontosabb eleme az elektronikus információs rendszerek védelmének, hiszen még mielőtt használnánk ezeket a rendszereket, ismerni kell a működésüket, és tapasztalatból tudom mondani, hogy ez különösképp nem szokta az embereket érdekelni, mert majd úgyis jön valaki, aki segít nekik. Csak az a szomorú helyzet, hogy nincs mindig valaki, és lehet pont az a valaki, akiben bízunk ő az, aki nyereszkedni akar rajtunk. Mindezt összefoglalva a digitális kompetencia nélkülözhetetlenségét kívánom vizsgálni a napjainkban.

Mivel gyűjtik az adatokat és ezek egy életképet adnak egy személyről, hogy pontosan mit használ mit nem. Ezekhez az adatokhoz, pedig könnyedén hozzá tudnak férni kívülről, mivel sokan nem tartják a személyiségi jogokat annyira fontosnak, mint mi itt Európában.

Köszönhetően a hálózatok használatának, de főként az IoT (Internet of Things; A dolgok Internete) rendszereknek már a személyes jelenlétre nincs is szükség ezekhez, vagy nagyon minimális emberi beavatkozás szükséges.

Tekintettel a fentiekre a kutatásom két fő hipotézise:

H1: Az okosokhonok elleni támadások kivédhetőek lennének, csak tudni kell kezelni az eszközöket és a hálózatokat.

H2: A kínai társadalmi kreditrendszert lehet ezzel is segíteni és éltetni.

Empirikus kutatásom során forrásokat kerestem, viszont ebben a témában nagyon kevés érhető el a tudományos adatbázisokban. Ezért tartom ezt egy friss és releváns témának és ezért fontos, hogy ne csak angol, hanem magyar nyelven készüljön erről egy tudományos mű.

¹ Nemzeti Kibervédelmi Intézet (2024.február 7.): [Malware-rel fertőztek meg okos fogkeféket](#)

1. Okosotthon rendszerek típusai, működése, használata

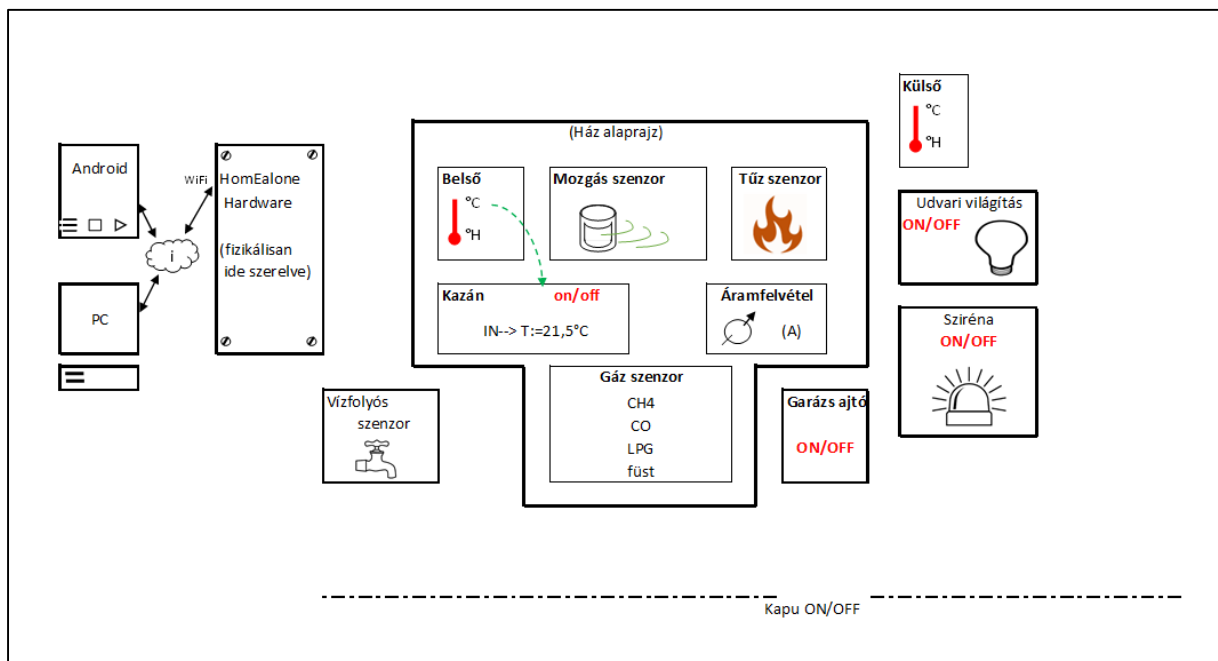
Mielőtt ismertetném kimondottan a rendszer „hibáit” és támadhatósági felületeit, szeretnék egy kis bemutatást is tenni előtte, hogy kimondottan mi mit készítettünk, csak hogy egy példán keresztül megismerhessük magát a rendszert és a gyenge pontokat.

Sorban haladva, először is a hardware-t mutatom be. Az alábbi képen látható, hogyan is épül fel a rendszer, és pontosan milyen alkalmazásokat is használ.

Balra a háztól maga a működési elv látható, valamint különböző színekkel feltüntetve, hogy az adott jelzés mennyire komoly értékű.²

Az értékek a következők lehetnek:

- Zöld villog: start (első RPI adat cseréig; jelzi, ha nincs RPI kommunikáció)
- Zöld: Normál állapot
- Kék villog: élesítés késleltetés | riasztás késleltetés
- Kék: élesítés
- Piros villog: szenzor jelzés, de nincs riasztás
- Piros: riasztás



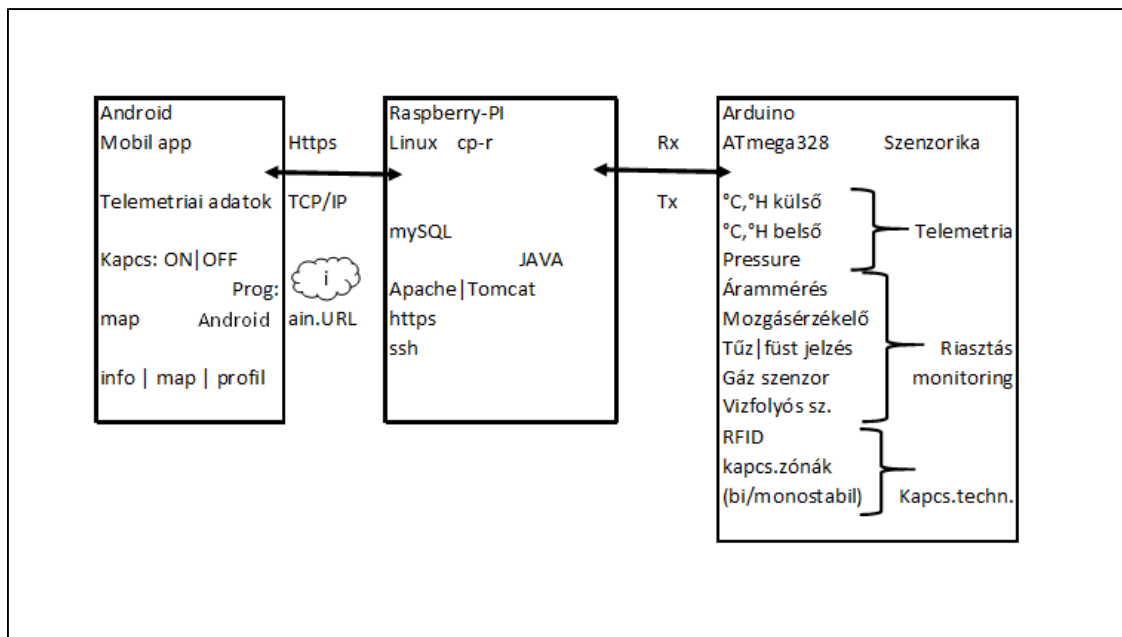
1. ábra: Egy okosotthon rendszer szenzor rendszere (saját szerkesztés, forrás: középiskolai projekt)

Láttuk azt is az előző rajzokon, hogy milyen mennyiségű eszköz, és ezzel együtt szenzor képes részt venni egy ilyen rendszerben. Fontos ezeket részletezni és ismerni, mivel így

² Kovács, V. (2021): HomEalone - avagy hogyan ne járjunk úgy, mint Kevin, ZSZC Csány László Technikum

láthatjuk át, hogy mekkora veszély is rejlik abban, ha sérülékeny a rendszer. Sokkal több adat is kiolvasható egy szenzor adataiból, mint gondolnánk. Vegyük is sorra ezeket:

- *Hőmérők:* Ezek lehetnek mind külső, mind belső hőmérők, melyek °C-ban mutatnak ki adatokat Európában. Ami mögöttes adatot tartalmaz magában, hogy kiszámítható, hogy az ember mikor van otthon. Jobbára a magasabb hőfok emberi jelenlétet következtet le maga után, így azt is meg lehet figyelni, illetve amennyiben az előzetesen be van kapcsolva, ki lehet számolni mikorra ér haza az adott illető.
- *Mozgásérzékelő:* Az itt letárolt adat true vagy false lehet. Azaz az adott helyiségben tartózkodik-e ember. Ha igen, és be van kapcsolva az érzékelő, akkor riasztás van. Mivel az érzékelő be van kapcsolva, az adott helyiségben ember nem lehetne. Tehát itt ez már egy jelzés lehet az otthon tulajdonosának, hogy hívja a hivatásos szervek segítségét, mert épp lehet betörnek hozzá.
- *Tűzjelző:* Szintén true vagy false adatot lehet letárolni. Ha aktív a szenzor és false az érték, az a jó. Szintén már ezzel is lehet játszani, hogyha feltörik a szenzor rendszerét, akkor egy false pozitív érték jöhet ki, mellyel megint egy figyelemelterelést lehet végrehajtani.
- *Kazán:* Itt, akárcsak a hőmérőnél, az az adat kérhető le, hogy van-e valaki az ingatlan területén.
- *Gázérzékelő:* Ebből többféle is lehet; helyiségnek megfelelő, előfordulható gázoknak megfelelő érzékelőkkel kihelyezve. Szintén erre is lehet false pozitív eredményt küldeni a készülékre, mely vezérelni az egész rendszert, ezzel egy kisebb pánikot okozva, az ingatlant kiürítve
- *Zárak:* Mint ahogy a legtöbb szenzor, ez is true vagy false adatot tud visszaküldeni. Ez alapján lehet tudni, hogy van-e valaki az adott helyiségben, vagy üres.
- *Okosporszívó:* Működését tekintve, szenzorok segítségével feltérképezi a helyiséget, hogy mi merre található, és meddig tud elmenni, és takarítani. Sokkal több és érzékenyebb adat kerülhet ki ez által.
- *Hűtő:* Ismételten az ember szokásai és élethelyzete, valamint életszínvonala is megfigyelhető ebből. Mit tárol benne, mire szokott szüksége lenni, esetleges allergiák megismerhetők az adatokból. De ezt egy későbbi fejezetben fejtem ki, mert már történt erről eset.



2. ábra: Egy okosotthon rendszer hálózata (saját szerkesztés, forrás: középiskolai projekt)

Egyszerű a képlet, szenzorokról van szó, amik, ha érzékelik a beállított adatokat jeleznek. Nézzük is ezt szoftveresen.

Mint látjuk itt már maga a folyamatban zajló kommunikáció is feljegyzésre került, és kimondottan nekünk ez azért fontos, mert innen látjuk magát a támadhatóságot. Ezeket a rendszereket sokkal könnyebben, és sokkal, nagyobb kárértékkel tudjuk tönkre tenni.

De ne is feltétlen akarjuk tönkre tenni a rendszert, hiszen az egy megbízónak fontos, hogy maga a szerkezet (jelen esetben az okos otthon rendszer) működésben maradjon. Erre azért is van szükség, mivel ezen keresztül van lehetőség csak információt szerezni.³

1.1.Mesterséges Intelligencia

Manapság egyre inkább kezd elterjedni a mesterséges intelligencia használata, hiszen ezekben a rohanó napokban, az segítség az embereknek, hogyha automatizált egy rendszer, és nem kell vele különösképp foglalkozni. Ám ez még mindig nem fedi a valóságot. Ma, amit legtöbbször mesterséges intelligenciának hívunk az egy egyszerű algoritmizálás, vagy gépi tanulás. Jobban megfigyeli az ember, ténylegesen csak ez történik. Az adott folyamatok le vannak kódolva egy egyszerű igen-nem válaszlehetőséggel, és egy szoftver eldönti, melyik legyen a válasz. Ezt rá lehet venni a szenzorok ki-be kapcsolásához is, illetve az adatok összegzésénél is, valamit a továbbításnál is.

³ Kovács, V. (2021): HomEalone - avagy hogyan ne járjunk úgy, mint Kevin, ZSZC Csány László Technikum

De visszavetítve, például a chatGPT-t is figyelve, az is csak egy generikus szöveggyártó. Hiszen semmi más nem történik, beírjuk azt, amire szükségünk van, ám csak az adatbázisában található anyagok közül keresi meg a megfelelő és általa a legfrissebbnek vélt választ. Ami nem is biztos, hogy jó, hiszen a mai chatGPT-k 2022-es adatokkal dolgoznak. Azóta rengeteg szabályozás változott. Vannak módszerek melyeket használva lehet tökéletesíteni ennek használatát, de ezek még mindig nem a nekünk szükséges információk.

Amire tökéletes manapság az MI (Mesterséges Intelligencia) az a döntéshozatal. Okosotthon rendszereknél ismert egy döntéstámogató keretrendszer, melynek angol megnevezése a CROSS (Cyber Risk Optimiser for Smart Homes). Ennek fő feladata tanácsot adni a felhasználónak, illetve az okosotthon rendszert szolgáltatónak a kiberbiztonsági ellenőrzések optimális kiválasztására.

A CROSS egy többcélú, kétszintű kétlépcsős optimalizáláson alapul. Az első szakaszban az optimalizálás a problémát több vezető-követő játékként modellezi, amely mind a biztonsági, mind a gazdasági célokat figyelembe veszi, ahol a szolgáltató biztonsági portfóliót választ ki, megvédi magát és felhasználóit, míg a racionális támadók a leggyengébb utat célozzák meg. Második szakasz optimalizálás egy Stackelberg biztonsági játék, amely további felhasználói biztonsági vezérlőkre összpontosít az intelligens hatáskörébe tartozik otthoni felhasználók.

Az IoT eszközök ellen újabb támadások keletkeznek, főleg a mesterséges intelligencia használatával. Ezek az újabbnál újabb támadások csak több és frissebb kiberfenyegetettséget jelentenek az otthonokban. ⁴

Nagyon fontos vizsgálni a sérülékenységet, hiszen sokaknak nincs pénzük megvenni milliókért ezeket az elkészített rendszereket, csak bevásárolnak hozzá a boltokban a polcokról kapható általános eszközöket, és ezeket próbálják használni. Ezzel sincs semmi gond, de mivel nincsenek összekötve, se ellenőrizve, csak nagyobb fenyegetettségnek van vele kitéve a tulajdonos.

⁴ Zhang, Yunxiao, Malacaria, Pasquale, Loukas, George and Panaousis, Emmanouil (2023) CROSS: a framework for cyber risk optimisation in smart homes. Computers and Security, 130:103250. pp. 1-15. ISSN 0167-4048

1.2. Digitális kompetencia

Napjainkban Magyarországon rengeteg projekt foglalkozik a digitális kompetenciával, így könnyű elemezni a helyzetet ám mégis a legfontosabb dokumentum a DigComp. Ez egy nyolc szintből álló tudást sorol fel, melyek a következők:

1. Alapszint (1): Az 1-es (alap) szintű jártassággal rendelkező személy (többféle formában elérhető) út-mutatásra támaszkodva egyszerű feladatokat, kisebb problémákat old meg, folyamatokat kezel, a lépéseket megjegyzi.
2. Alapszint (2): A 2-es (alap) szintű jártassággal rendelkező személy szükség esetén segítség igénybevételével egyszerű feladatokat old meg, kisebb problémákat kezel, a lépéseket megjegyzi.
3. Középszint (3): A 3-as (közép) szintű jártassággal rendelkező személy önállóan old meg jól meghatározott, rutinszerű feladatokat, problémákat, képes követni a lépéseket, érti a megoldásokat.
4. Középszint (4): A 4-es (közép) jártassági szinten az egyén önállóan, saját igényeinek megfelelően old meg feladatokat, konkrét, nem rutinszerű problémákat, értő módon alakítja a megoldáshoz vezető lépéseket.
5. Haladó szint (5): Az 5-ös (haladó) jártassági szinten az egyén sokféle feladatot és problémát képes meg-oldani úgy, hogy közben másoknak is segít és a segítségnyújtás kapcsán bővíti saját tudását is.
6. Haladó szint (6): A 6-os (haladó) jártassági szinten az egyén szinte minden feladatot, a célnak leginkább megfelelő módon képes megoldani úgy, hogy közben komplex helyzetekben másokhoz is tud alkalmazkodni, az ehhez szükséges lépéseket elemzi és értékeli.
7. Mester szint (7): A 7-es (mester) jártassági szinten az egyén olyan összetett problémákat kezel, amelyek meghatározott számú megoldással rendelkeznek, és ezeket a megoldásokat a szakmai gyakorlatba illeszti, másokat is segítve ezzel. A megoldáshoz vezető lépéseket képes maga is létrehozni.

8. Mester szint (8): A 8-as (mester) jártassági szinten az egyén rendkívül összetett, soktényezős problémákat, önállóan old meg. Az így kialakított új megközelítéseket és módszereket beilleszti az adott szakmai terület eljárásai közé. A megoldáshoz szükséges eljárásokat maga hozza létre.⁵

Ezekkel együtt pedig még öt fő kompetencia-fejlesztési területet figyeltek meg, ezek az alábbiak:

- Információ és adatmenedzsment.
- Kommunikáció és együttműködés.
- Digitális tartalmak létrehozása.
- Biztonság.
- Problémamegoldás.⁶

A digitális kompetencia, mint összefogó fogalom, és képesség mindig, mindenhol előjön napjainkban.

Fontos figyelembe venni ezt is, hiszen ez a tényező nélkül nem tudják az emberek megtanulni még a biztonságos internetezést sem nem, hogy azt, hogy hogyan kell használni bizonyos készülékeket vagy szenzorokat. Arról nem is beszélve, hogy egy egész komplex hálózati rendszert, hogyan tanulják meg. A hajlandóság is hiányzik nagyon sok emberből, de az is látszik, hogy ez a modernizálódó világ nem vesz figyelembe mindenkit. Inkább a fiatalabbakra vannak ráfókuszálva a marketing terén is már, nem csak a kivitelezésekben.

⁵ Vuorikari, R., Kluzer, S. és Punie, Y.,(2022) DigComp 2.2: Állampolgári Digitáliskompetencia-keret pg. 9, EUR 31006 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-48882-8, doi:10.2760/115376, JRC128415.

⁶ Vuorikari, R., Kluzer, S. és Punie, Y.,(2022) DigComp 2.2: Állampolgári Digitáliskompetencia-keret pg. 4, EUR 31006 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-48882-8, doi:10.2760/115376, JRC128415.

2. IoT (Internet of Things)

Egyértelműen látni, hogy egy ilyen rendszernél már egy IoT-ről (Internet of Things - Dolgok internete) van szó, mivel minden eszköz egy hálózatra csatlakozik fel, ott kommunikálnak egymással, adatot küldenek egymásnak, és ezeket le is tárolják egy adatbázisban. Fő haszna, hogy nincs szükség ember-ember vagy ember-gép kapcsolattartásra.

2.1.Működése

Ezek a rendszerek web-képes intelligens eszközökből állnak, melyek szenzorokkal és kommunikációs hardware-rel rendelkeznek. Ennek a rendszernek a begyűjtött adatok befogadására és kezelésére és azok kiértékelésére is képesnek kell lennie. Ez pedig úgy lehetséges, hogy minden eszköznek van egy IoT-eszköz szerinti portja, és ezen a porton keresztül történik a kommunikáció. Ám először a begyűjtött adatok egy szélső eszközre kerülnek, ott történik az elemzés és kiértékelés, erre pedig azért van szükség, hogy utána a felhőbe csak a tartalmilag releváns adatok kerülhessenek fel, minimalizálva a sávszélesség felhasználását. Ahogy korábban írtam, ez teszi lehetővé azt, hogy emberi beavatkozás nélkül működhessenek ezek a rendszerek. Ez még nem jelenti azt, hogy nem lehet beleavatkozni a folyamatba. természetesen erre mindig van lehetőség.

Ami viszont egyre elterjedtebb, az az, hogy az IoT- mesterséges intelligenciát használjon az adatok kezelésénél. Így sokkal könnyebb kezelni az adatokat, és szűrni is és ettől csak dinamikusabb lesz a folyamat. Ez napjainkban elengedhetetlen, hiszen mindenki rohan és soha semmire nincs ideje.⁷

2.2.Előnyei

Minden rendszernél, így ezeknél is meg kell kérdezni, hogy igazából mire is jók? Egy IoT rendszer csak segíti az ember életét. Könnyebbé teszi a mindennapokat, kicsit javítja az életszínvonalat. Könnyebb az élet, ha minden előre már be van készítve, és csak egy gombnyomásba kerül a jobb élet. Mind ezek mellett az IoT az üzleti életben is fontos, nem csak

⁷ Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. The internet society (ISOC), 80(15), 1-53.

a magánéletben. Betekintést nyújt a rendszerek működésébe, a logisztikai műveletekbe, egészen a gépek teljesítményétől az ellátási láncig a szervezetek számára.

Továbbá az automatizálással még a költségeket is lehet csökkenteni. Ez a technológia még folyamatosan fejlődik, de egyre több cég és vállalat veszi észre az ebben rejlő előnyöket.

2.3.Keretrendszer

Mivel egy összetett hálózati rendszerről van szó, így kihagyhatatlan a keretrendszerről beszélni, illetve, hogy melyszervezet felügyeli, vagy hozta létre az adott rendszert.

International Electrotechnical Commission (Nemzetközi Elektronikai Bizottság): egy nonprofit szervezet, amelynek munkája alátámasztja a minőségi infrastruktúrát és az elektromos és elektronikai cikkek nemzetközi kereskedelmét. Munkájuk elősegíti a műszaki innovációkat és a megfizethető infrastruktúra-fejlesztést is. 170 ország a tagja és 4 megfelelőségi értékelő rendszert vezet, melynek tagjainak tanúsítja, hogy a rendszerei, a telepítései és a szolgáltatásai az előírásoknak megfelelően működnek.⁸

Institute of Electrical and Electronics Engineers: egy nemzetközi szakmai szervezet, amely elektronikai, villamosmérnöki, valamint számítástechnikai tudományokhoz kapcsolódó szabványok kidolgozásával, oktatással, tudományos konferenciák szervezésével, illetve ezekhez kötődő tanulmányok publikálásával foglalkozik.⁹

Industrial Internet Consortium: technológiai vállalatokat, kutatókat, egyetemeket és kormányzati szervezeteket fog össze azzal a céllal, hogy azonosítsák, összegyűjtsék és előmozdítsák az ipari internet növekedésének felgyorsítását szolgáló legjobb gyakorlatokat.¹⁰

Open Connectivity Foundation: egy iparági szervezet, amely szabványokat dolgoz ki, egy sor interoperabilitási irányelvet hirdet, és tanúsítási programot biztosít a tárgyak internetéhez kapcsolódó eszközök számára.¹¹

Thread Group: egy IPv6-alapú, alacsony fogyasztású mesh hálózati technológia a dolgok internetes (IoT) termékekhez.¹²

⁸ International Electrotechnical Commission (2024): [What we do for safety, sustainability and global trade](#)

⁹ Institute of Electrical and Electronics Engineers (2024): [About: At a glance](#)

¹⁰ Industrial Internet Consortium (2024): [About us: Overview](#)

¹¹ Open Connectivity Foundation (2024): [About us](#)

¹² Thread Group (2024): [What is Thread?](#)

Connectivity Standard Alliance: egy olyan vállalatcsoport, amely számos más mellett karbantartja és kiadja a Zigbee and Matter szabványt.¹³

IPv6 (6LoWPAN): az internetprotokoll új verziója, melyet az Internet Protocol version 4 leváltására terveztek. Lefőbb eltérésük, hogy az IPv6 már hexadecimálisban van írva, és 8 csoportból áll, míg az IPv4 4 csoport decimális számrendszerben írt webcím.¹⁴

IEEE 802: nyílt és akkreditált eljárással hálózatépítési szabványokat és ajánlott gyakorlatokat dolgoz ki és tart fenn a helyi, nagyvárosi és egyéb területi hálózatok számára, és ezeket globális szinten támogatja. A legszélesebb körben használt szabványok az Ethernet, az áthidaló és virtuális hídhálózatok vezeték nélküli LAN, vezeték nélküli PAN, vezeték nélküli MAN, vezeték nélküli együttélés, médiafüggetlen átviteli szolgáltatások és vezeték nélküli RAN szabványok. Minden egyes területhez egyéni munkacsoport adja a fókusz.¹⁵

Data Distributed Service (DDS): Az OMG Data Distribution Service (DDS) egy köztes szoftver protokoll és API szabvány az Object Management Group (OMG) adatközpontú kapcsolatához. Egy rendszer összetevőit integrálja, alacsony késleltetésű adatkapcsolatot, rendkívüli megbízhatóságot és méretezhető architektúrát biztosítva, amelyre az üzleti és a kritikus dolgok internetes (IoT) alkalmazásainak szüksége van.¹⁶

Constrained Application Protocol (korlátozott alkalmazási protokoll): egy speciális webes átviteli protokoll a tárgyak internetének korlátozott csomópontjaihoz és korlátozott hálózataikhoz. A CoAP-ot úgy tervezték, hogy lehetővé tegye az egyszerű, korlátozott eszközök számára az IoT-hez való csatlakozást még alacsony sávszélességű és alacsony rendelkezésre állású, korlátozott hálózatokon keresztül is.¹⁷

Advanced Message Queuing Protocol: egy alkalmazási réteg protokoll, amely üzenet orientált middleware-ek működését határozza meg. Az AMQP meghatározó értékei: üzenet központúság, sorkezelés, üzenetirányítás, megbízhatóság, biztonság.¹⁸

Long-Range Wide Area Network (LoRaWAN): egy nyílt hálózati protokoll, amely lehetővé teszi az eszközök számára, hogy a hosszú hatótávolságú (LoRa – Long range) néven ismert szabadalmaztatott vezeték nélküli technológia segítségével kommunikáljanak. A nagyszabású

¹³ Connectivity Standard Alliance (2024): [About us](#)

¹⁴ Loshin, P. (2004). IPv6: Theory, protocol, and practice. pg. 156

¹⁵ John D'Ambrosia(2024): [IEEE 802](#):

¹⁶ DDS Foundation (2024): [What is DDS?](#), Object Management Group

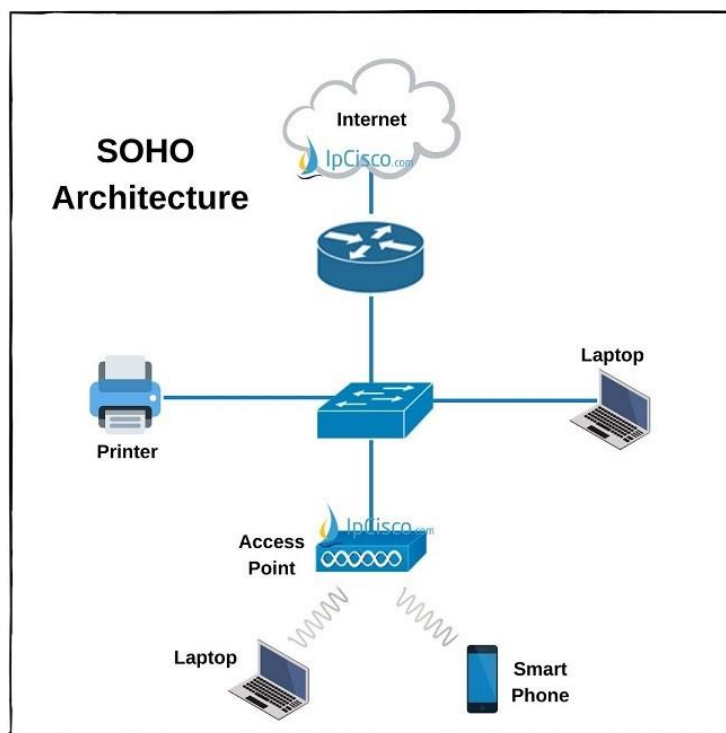
¹⁷Constrained Application Protocol (2024): [Technologies](#)

¹⁸ Advanced Message Queuing Protocol (2024): [About](#)

IoT-projektekhez tervezett LoRaWAN különösen hasznos az alacsony fogyasztású eszközökhöz, amelyek nagyon kis sávszélességet igényelnek.¹⁹

3. SOHO (Small office home office)

A small office home office egy hálózati kifejezés, amit leginkább LAN (Local Area Network) hálózatokra jellemző, mivel kis vállalatok használják. Hazánkban is egy viszonylagos újdonságként lépett be a közéletbe, amikor is a Covid miatt be kellett vezetni a távmunkát. Így mindenki, aki zárt és zsúfolt helyen dolgozott; azzal könnyített a dolgon – és főként a távolságtartás és egészségügyi szabályzások betartásával, hogy hazaküldte a munkavállalóit, és a saját hálózatokról, szervezeti eszközökkel kellett dolgozniuk. Ettől függetlenül a SOHO rendszerek maximum 10 emberig terjednek ki, tehát ténylegesen a kis vállalkozások képesek ezt a megoldást használni.²⁰



3. ábra: SOHO hálózat topológiája (forrás: [IPCisco.com](https://www.ipcisco.com))

Legtöbbször olyan vállalkozások választják ezt a munkatípust, akiknek nem feltétlen szükséges az irodai környezet, hogy az ügyfeleikkel találkozzanak, mivel ezt akár az otthonuk kényelméből is ki tudják alakítani, és innen ered a home office kifejezés. Ilyenek például a könyvelők, ügyvédek vagy a pénzügyi tanácsadók.

¹⁹ Long-Range Wide Area Network (2024): [About LoRaWAN](https://www.ipcisco.com)

²⁰ IPCisco (2024): [Network Topology Architectures](https://www.ipcisco.com)

Ezek a rendszerek lehetővé teszik, hogy egy virtuális irodából dolgozzanak a munkavállalók. Nem szükséges a személyes jelenlét, hiszen tudnak videóhíváson keresztül így egy megbeszélést tartani, illetve osztott naptárral még egymás teendőit is láthatják és akár szerkeszthetik is és ez mind a felhőalapú szolgáltatásoknak köszönhető. ²¹

3.1.SOHO rendszerek sérülékenysége

Mivel a SOHO rendszerek lényege és működése az, hogy otthoni hálózattal lehet használni, így a legnagyobb veszélyt a routerek és ezzel együtt a hálózat tudja adni.

Tudni illik jelenleg, ami internet protokollként használatban van az az IPv6. Ezt már korábban kifejtettem, hogy pontosan mi is. A fő probléma, hogy az IPv6-nál nem gyakran használt a NAT (Network Address Translation) jelenleg, mivel sokkal több cím található ebben, mint az IPv4-ben, illetve nincs is szüksége rá, mivel enélkül is biztonságosnak tartják, hiszen a tűzfal biztonsági beállításai ellátják ennek szerepét.

Ettől függetlenül a rendszerek viszont még tudják használni a NAT-olást, azaz a hálózati címfordítást, melyek a következők.

Erre minden csomagszűrő tűzfal képes és a hálózati eszközöknek is kiegészítő szolgáltatása. Ez teszi lehetővé a belső hálózatra kötött gépek közvetlen kommunikációját tetszőleges protokollokon keresztül a külső gépekkel anélkül, hogy azoknak a saját nyilvános IP címmel kellene rendelkezniük.

A NAT-nak három fajtáját különböztetjük meg. Statikus, dinamikus és a PAT, ami nem más, mint a port cím fordítása. A statikust inkább webek tárolására használják, mivel ezek előre bejegyzett IP címek. A dinamikusnak lényege, hogy több eszköz tudja ugyan azt a publikus IP címet használni, hogy el tudja érni az internetet. A PAT pedig hasonlít a dinamikushoz, azzal a különbséggel, hogy itt a portokat használják, hogy meg tudják különböztetni a forgalmat az IP címhez rendelve.

Ám amit még használni lehet, az a maszkolás. Tegyük fel, hogy egy hálózatban két A és B gazdagép kapcsolódik. Most mindkettő ugyanazt a célt kéri, ugyanazon a portszámon, mondjuk 1000-ben, a gazdagép oldalán, ugyanabban az időben. Ha a NAT csak az IP-címeket fordítja le, akkor amikor a csomagjaik megérkeznek a NAT-hoz, mindkét IP-címét elfedi a hálózat

²¹ IPCisco (2024): [Network Topology Architectures](#)

nyilvános IP-címe, és elküldi a célállomásra. A célállomás az útválasztó nyilvános IP-címére küldi el a válaszokat. Így a válasz érkezésekor a NAT számára nem lesz egyértelmű, hogy melyik válasz melyik gazdagéphez tartozik (mivel A és B forrás portszáma azonos). Ezért az ilyen problémák elkerülése érdekében a NAT maszkolja a forrás port számát is, és bejegyzést ad a NAT táblába.²²

3.2.Otthoni Hálózati biztonsági modellek

De mivel a jelenleg elterjedt protokoll az IPv6, lássuk így milyen megoldások lehetnek még:

Zárt modell: Peremvédelmi megközelítés, amely a biztonsági ellenőrzéseket a hálózatra összpontosítja, hogy megakadályozza a hozzáférést a hálózat belső vagy megbízható részéhez. Itt elsősorban a biztonság áll a középpontban a széles körű hálózati hozzáférés megakadályozására összpontosítva. A biztonsági határokon belüli eszközök általában szabadon kommunikálhatnak egymással finomabb biztonsági intézkedések, például virtuális LAN nélkül, külön SSID-k vagy gazdagép alapú szűrési stratégiák segítségével.

Nyílt modell: nyílt modell kommunikációja a végpontok közötti elérhetőségre törekszik anélkül, hogy címfordításra vagy tetszőleges határookra és korlátozásokra lenne szüksége. A biztonságért való felelősség az áthelyeződik itt a hálózat pereméről minden csatlakoztatott eszközre. Ez a megközelítés általában megtalálható a korai IP-hálózatoknál, amikor a mértéke és hatóköre az Internetnek sokkal kisebb volt, és az IPv6-hálózatok növekvő használatán belül a címterület lehetővé teszi minden csatlakoztatott eszköz egyedi címzését.

Hibrid modell: Egy többszintes megközelítése a biztonságnak, ami biztosítja mindkettő lehetőséget. Több formában is megtalálható, mint például egy hálózat széli tűzfal egyedi eszközházirendekkel, vagy a NAT-hoz hasonló címfordítási mechanizmusok újbóli bevezetése.

23

²² Wing D. (2010): Network Address Translation, Extending the Internet Address Space, IEEE Internet Computing, 14(4), 66–70. doi:10.1109/mic.2010.96

²³ Olson K. , Wampler J., Keller E. (2023) Doomed to Repeat with IPv6? Characterization of NAT-centric Security in SOHO Routers, pg.305:3

3.3.Hálózati átjárók biztonsági tulajdonságai

Fontos a tudatossághoz és a biztonsághoz is tudni azt, hogy milyen tulajdonságokkal is kell felruházni egy hálózati átjárót, csak azért is, hogy illetéktelen ne juthasson hozzá a hálózat többi részéhez.

Titkosítás: egy olyan tulajdonság, amely biztosítja, hogy az információk ne kerüljenek illetéktelen személyek tudomására. Egy biztonságos átjáróban soha nem szivároghat ki információ a hálózatról, rendszerekről, vagy az adatokról. Ez az előfeltevés azt feltételezi, hogy az átjárók biztonságosan jönnek létre az alapértelmezett konfigurációjukban, még akkor is, ha ez a gyakorlatban nem fordul elő.²⁴

Integritás: az a képesség, amely garantálja a rendszer működését vagy az adatátvitel hűségét eredeti megbízható formájukat vagy beállításait. Megkérdőjelezi ezen biztosíték hatékonyságát az a tény, hogy minden egyes a rendszert alkotó komponensnek követnie kell ezt az elvet, hogy elérje a bizonyossági szintet az egész készülék.²⁵

Rendelkezésre állás: ez biztosítja, hogy az összes ellenőrzési mechanizmus és biztonsági eljárás érvényben van, a felhatalmazott személyek igényelhetik ezeket a szolgáltatásokat. Ezen kívül a biztonságos működésben lévő rendszernek folytatnia kell a működést még akkor is, ha valamelyik eszköz meghibásodik vagy kompromittálják; mindaddig, amíg a hiba nem mutat új vektorokat, amelyek további kihatással lehetnek a hálózatokra.²⁶

Megbízhatóság, hitelesség és letagadhatatlanság: A CIA (Central Intelligence Agency – Központi Hírszerző Ügynökség) javasolt kiterjesztései hármas ISO 2700 szabvány szerint, amelyek a biztonsági célok elérésének további módját határozzák meg. A hitelesség garantálja, hogy a felhasználó vagy a rendszer az, akinek mondják magukat, gyakran egy igazolással ellenőrzik ezt, mely lehet bizonyos tudás, ujjenyomat, egy token. A letagadhatatlanság bizonyítékot szolgáltat olyan cselekedetekre, amelyek befolyásolhatják a rendszert vagy az adatokat. Ez általában rendszer- vagy eseménynaplózáson keresztül történik, ilyen például a biztonsági információ- és eseménykezelő (SIEM) rendszer. Végül a megbízhatóság érinti az eszköz ismételt és elvárt működését minden egyes művelethez vagy tranzakcióhoz és azt a képességet egy rendszernél, hogy az adott esemény elvárásainak megfelelően működjön.²⁷

²⁴ Olson K. , Wampler J. , Keller E. (2023) : i.m. pg.305:4

²⁵ Olson K. , Wampler J. , Keller E. (2023) : i.m. p.g.305.4

²⁶ Olson K. , Wampler J. , Keller E. (2023) : i.m. p.g.305.4

²⁷ Olson K. , Wampler J. , Keller E. (2023) : i.m. p.g.305.4

4. Veszélyek

Hosszas kutatások után néztem meg, hogy ezt a mai nappal melyik csoportjába is illesztenénk be a hírszerzés típusai közül, és amit személy szerint megfelelőnek találtam, ez a CYBINT²⁸ (cyber intelligence), a magyar megfelelője fordítást tekintve, a kiber hírszerzés. A SIGINT²⁹ (Signal Intelligence) ami rádióelektronikai felderítést jelent, ami pedig az emberek vagy elektronikus rendszerek közötti jelek elfogásával gyűjtött adatokat jelenti.

Pontosan ezeknél a rendszereknél ilyen területek képességeinek áttekintésére, átgondolására is van szükség főleg, ha mi vagyunk az a fél, akinek meg kell szereznie bizonyos ismereteket.³⁰

Hozzátenném ezek a rendszerek a HUMINT³¹-re (human intelligence) is épülhetnek.

Mindezekből látszik, hogy nagyon sok tényező van, amit figyelembe kell venni. Főleg mivel a „képletben” az ember is szerepel.

Dolgozatom fő kutatási területe maga a sérülékenysége egy ilyen okosotthon rendszernek, illetve a keletkezett veszélyek felfedezése, és esetleges elkerülése. Mivel már bemutattam egy ilyen rendszer telemetriáját és kimondott működését is, szeretnék áttérni a keletkeztethető veszélyekre is.

Legelső dolog, amit megtanultam az informatikában – a tanárain nagy hangsúlyt fektettek rá, hogy megtanuljuk – az az, hogy minél több az technológia (hardware és szoftver) található valamiben, annál több az esély a hibákra. Ezek a rendszerek pedig szinte 100%-osan hálózat szintű rendszer. Magyarán mondva, ha egy eszközhöz hozzá lehet férni, akkor mindenhez is hozzá lehet, és óriási károk okozhatóak.

Nemrégiben egy sikeres pályázatnak köszönhetően volt szerencsém az NMHH-nál (Nemzeti Média és Hírközlési Hatóság) egy intézménylátogatáson részt venni, ahol megmutatták nekem és még a sikeres pályázatot nyert társaimnak is, hogy hogyan ellenőrzik országos szinten a rádiófrekvenciás zavarokat. Bennem itt merült fel első kérdésként, hogy tudnak-e esetet amikor okosotthon rendszer okozott volna zavart. A válasz rövid volt és tömör, mivel nemleges volt,

²⁸ Yeboah-Ofori, Abel. (2018). Cyber Intelligence and OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media. *International Journal of Cyber-Security and Digital Forensics*. 7. 87-98. 10.17781/P002378.

²⁹ Frascà D., Venturi G., Ustenko M. and Zanasi A. (2023): Technologies for IMINT and SIGINT, 2023 IEEE International Workshop on Technologies for Defense and Security (TechDefense), Rome, Italy, 2023, pp. 165-169, doi: 10.1109/TechDefense59795.2023.10380827

³⁰ Izzat A. (2023): The NICE Cyber Security Framework; Cyber Security Intelligence and Analytics, Springer Cham, 978-3-031-21651-0, <https://doi.org/10.1007/978-3-031-21651-0>

³¹ Henrico S., Putter D. (2024): Intelligence Collection Disciplines—A Systematic Review. *Journal of Applied Security Research*. 1-25. 10.1080/19361610.2023.2296765.

de azt megjegyezték, hogy záruk és kapuk miatt már hívták ki őket. És most jönne a jogos kérdés, hogy mégis ez hogyan jön ide?

A válasz itt is egyszerű. A kapukulcsban lemerült az elem. Ez miatt a kapu szenzorja folyamatosan kereste a jelet, küldve közben a rádiófrekvenciás hullámokat, hogy csatlakozni tudjon a hálózathoz. Tapasztalatból mondták el az ott dolgozó kollégák, hogy ebből lesz még kellemetlenség, hiszen ez egy egyszerű dolog is viszonylag. Rosszul érezte magát az adott személy is, már szinte szégyellte magát, hogy ezért kellett a hatóság munkatársait kihívnia, de közben meg jól tette, hiszen sosem tudni, hogy nem más áll-e a háttérbe, amiért nem működik a rendszer.

Egyszerű egy ilyen rendszerbe is bejutni. Legfőbbként, ahogy írtam, az emberek egyszerűségén múlik minden. Ezt mi sem bizonyítja jobban, mint hogy az emberek nagy százaléka nem változtatja meg a router jelszavát sem. Vagy azért, mert nem tudja, vagy azért, mert nem akarja és nem tartja fontosnak.

4.1.OSI modell

Lehet úgy is figyelni ezeket a fenyegetettségeket, hogy az adott használt protokollnál, mely szinten, mivel történhetnek támadások. Ezt is a tudatosság előnyére lehet írni hiszen, ha valaki már ezekkel is tisztában van, akkor már egy lépéssel előre is van.

Ez a tudás sajnos bármikor bárkinek elérhető és könnyű is ezeket használni, hiszen ahogy korábban bemutattam egy generatív mesterséges intelligencia segítségével (chatGPT-vel kereséssel) meg lehet írni azokat a kódokat, vagy csak az alaplépéseket össze lehet szedni, amit ehhez szükségesek. Elegendő egy kódolni tudó személy, és máris a kapott generált lépések alapján, hozzá tud férni a hálózat bármely rétegéhez is. Nem szabályszerű, hogy ez történjen, de az emberi rosszindulat határtalan tud lenni.

Két nagy protokollt különböztetünk meg, az egyik az OSI a másik pedig a TCP/IP. Ezeket inkább sorolnám elvi modellek közé, hiszen ezek szabványosítják a távközlési és számítástechnikai rendszerek kommunikációit. Viszont a különböző rétegek közötti kommunikációban protokollokkal van lehetőség átjárni.³²

³² Nagy Tibor I. (2012): *SZENZORHÁLÓZATOK SZOFTVERFEJLESZTÉSI KÉRDÉSEI* (p.194-195), Military Engineer/Hadmérnök, 7(1).

7. Alkalmazási réteg – fenyegetettségvédelmi alkalmazás
6. Megjelenési réteg
5.Viszonyréteg
4.Szállítási réteg
3.Hálózati réteg – gazdagép tűzfala, hálózati tűzfal, NAT
2.Adatkapcsolati réteg – WPA, WiFi, MAC szűrés
1.Fizikai réteg – kapcsolódási döntés

4. ábra: OSI modell rétegei (saját szerkesztés, forrás: Nagy Tibor I. (2012): Szenzorhálózatok szoftverfejlesztési kérdései p194-195, Military Engineer/Hadmérnök, 7(1).)

4.Alkalmazási réteg (Protokoll)
3.Szállítási réteg (Protokoll)
2.Internet (Hálózat)
1.Hálózatelérési réteg (Hálózat)

5. ábra: TCP/IP modell rétegei (saját szerkesztés, forrás: Nagy Tibor I. (2012): Szenzorhálózatok szoftverfejlesztési kérdései p194-195, Military Engineer/Hadmérnök, 7(1).)

4.2.NAT támadási felületei

Port forwarding: A port továbbítás egy egyszerű módszer, amellyel a felhasználó statikusan hozzárendelheti a külső átjáró portját egy belső gazdagéphez, lehetővé téve a bejövő kommunikációt a NAT-on keresztül. Ez a leképezés mindaddig aktív marad, amíg a felhasználó el nem távolítja a konfigurációt, így a gazdagép ki van téve a nem kívánt kommunikációnak, különösen akkor, ha nem megfelelő a karbantartása. A felhasználók részvételével és annak folyamatosságával kapcsolatos kihívások kezelésére számos automatizált mechanizmust alkalmaznak a fogyasztói átjárókon belül, például az univerzális Plug-and-play (UPnP) és a portvezérlő protokollt (PCP). Az Univerzális Plug-and-play (UPnP)/Internet Gateway Daemon (IGD) olyan felderítési és koordinációs protokollcsomag, amely zökkenőmentes és automatizált átjárókonfigurációt tesz lehetővé. A konfigurációt kezdeményezők megengedő jellege, valamint az a tény, hogy a gyártók sok eszközön alapértelmezés szerint engedélyezik az UPnP-t, számos jól ismert biztonsági aggályhoz vezetett. Figyelemre méltó példák a „Unplug, Don’t Play”, „UPnPProxy” és „CallStranger” UPnP támadások, amelyek több milliárd fogyasztói eszközt tettek nyilvánosságra a nem megfelelő megvalósítás vagy hibás UPnP körüli

végrehajtás miatt. E hibák ellenére az UPnP továbbra is széles körben elterjedt jelenleg. Bár a fogyasztóknak azt tanácsolják, hogy kapcsolják ki ezt a funkciót a biztonsági kockázat korlátozása érdekében, de ehhez közvetlen beavatkozásra van szükség, és ez az, amit ez a protokoll elkerülni hivatott. A Port Control Protocol a NAT Port Mapping Protocol (NAT-PMP) utódja, az Apple rendszerek által széles körben használt fordítási mechanizmus. A PCP az UPnP-hez hasonlóan működik, egy NAT-átjárón található kiszolgálóra támaszkodva, amely a belső hálózathoz érkező portkonfigurációs kéréseket veszi át és hajtja végre. Ellentétben az UPnP-vel, melynek célja, hogy a felhasználók számára egyszerű interakciót lehetővé tevő kezelőfelületeket biztosítson, a PCP olyan programozási megoldásokat céloz meg, amelyeket jellemzően alkalmazások és számítógépes programok használnak.³³

Hole-punching method: A lyukasztás (vagy néha az átütés) egy olyan technika a számítógépes hálózatokban, amelyek közvetlen kapcsolatot hoznak létre két fél között, ahol az egyik vagy mindkettő tűzfal vagy hálózati címfordítást (NAT) használó útválasztók mögött található. A lyuk kilyukadásához minden kliens egy korlátlan, harmadik féltől származó kiszolgálóhoz csatlakozik, amely ideiglenesen tárolja az egyes kliensek külső és belső cím- és port információit. A szerver ezután továbbítja az egyes kliensek információit a másiknak, és ezen információk felhasználásával minden kliens megpróbál közvetlen kapcsolatot létesíteni; az érvényes port számokat használó kapcsolatok eredményeként a korlátozó tűzfal vagy útválasztók mindkét oldalon fogadják és továbbítják a bejövő csomagokat.

A lyukasztás működéséhez nem szükséges a hálózati topológia ismerete. Az ICMP lyukasztás, az UDP lyukasztás és a TCP lyukasztás Internet vezérlőüzenetet, felhasználói adatgrammot (User Datagram) és átvitelvezérlő protokollt (Transmission Control Protocol) használ.³⁴

Clients/ szerver vagy relay/ proxy módszer: A proxying módszerek egy külső, globálisan címzett kiszolgálót használnak arra, hogy koordinálja vagy segítse a végponti gazdagépeket a NAT átjárásában.

Ezeket a módszereket általában peer-to-peer (P2P) kommunikáció létrehozására használják, amikor mindkét fél NAT átjáró mögött található.³⁵

Increased security exposure for the consumer: (a fogyasztók fokozott biztonsági kitettsége) Noha ezen protokollok közül sok növeli a fogyasztói hálózatok biztonságát, az IETF (Internet

³³ Olson K. , Wampler J. , Keller E. (2023) : I.M. p.g.305.12

³⁴ Olson K. , Wampler J. , Keller E. (2023) : I.M. p.g.305.13

³⁵ Olson K. , Wampler J. , Keller E. (2023) : I.M. p.g.305.15

Engineering Task Force) széles körben támogatja ezt az célkitűzést. A NAT-PMP értékelése során megállapítják: A NAT-átjáró célja az, hogy több állomásnak lehetővé tegye egyazon cím megosztását, nem pedig az, hogy egyidejűleg akadályozza az adott állomás szabad kommunikációját. A biztonságot a legmegfelelőbbben a végponttól végpontig terjedő kriptográfiai biztonság és/vagy adott esetben explicit tűzfalfunkció biztosítja. Bizonyos kapcsolatok blokkolása csak kifejezett és szándékos tűzfalpolitika eredményeként történhet, nem pedig valamilyen más technológia véletlen mellékhatásaként. Ez a protokoll valamilyen módon részben visszafordítja ezt a kárt. Mivel azonban sok felhasználó elvárja, hogy a NAT-átjárója egyfajta tűzfalként működjön, minden, ezt a protokollt megvalósító NAT-átjárónak rendelkeznie KELL egy adminisztrációs mechanizmussal, amely letiltja azt, ezzel visszaállítva a NAT-PMP (Port Mapping Protocol) előtti viselkedést. Ez az álláspont számos aggályt vet fel a fogyasztói átjárók biztonságával kapcsolatban. Először is, az ilyen automatizált absztrakciók által lehetővé tett biztonsági kockázatok – finoman szólva – "funkciót jelentenek, nem pedig hibát". Másodszor, ez a pozíció feltételezi és megköveteli, hogy a felhasználók aktív résztvevői legyenek a saját biztonsági szabályzataik precíz kezelésében. Ez az álláspont szembe megy a gyártók azon törekvéseivel, hogy egyszerűsítsék annak kezelését, és levegyék a biztonsági protokollok kezelésének terhet a felhasználók válláról. Harmadszor, a záró álláspont tétován ajánl egy olyan adminisztratív mechanizmust, amely a NAT feltételezett előnyeit a felhasználó aktív érdekeltsége és részvétele révén, nem pedig alapértelmezett garanciaként állítja vissza. Bár az IETF elismerte, hogy a fogyasztói hálózatok biztonsága és a szélesebb körű internet-architektúra céljai közötti egyensúly megteremtése egyedülálló kihívást jelent, továbbra is a végponttól végpontig tartó összekapcsolhatóság mellett foglalnak állást, és vonakodnak az ezzel a tervvel ellentétes szabályozások meghatározásától és végrehajtásától. Az IPv6 fogyasztói átjárókon belüli működésének felmérésére során ugyanazokkal a kihívásokkal és buktatókkal szembesültek. Az eredmény a fogyasztói átjárókon belüli technológiák kétértelmű működési környezete, amely nem rendelkezik egyértelmű biztonsági vagy működési garanciával.³⁶

³⁶ Olson K. , Wampler J. , Keller E. (2023) : I.M. p.g.305.15

4.3.Kínai társadalmi kreditrendszer

Ahogy a bevezetőben megfogalmaztam az egyik hipotézisem ehhez a témához köthető, miszerint a kínai társadalmi kreditrendszert ezekkel a rendszerekkel lehet segíteni is. Hogy ez alatt mit is érteni, az a következő. Azt még tisztáznám, hogy ez nem egész Kínában található meg, csak néhány megyében, és azokon belül is csak pár városban.

Jelenleg Kínában pár megyében használják a kreditrendszert. Ezzel értékelik az embert, hogy milyen minőségű életet él. Vizsgálják továbbá a szokásait, a munkáját és azt is, hogy kikkel barátkozik. Nálunk Európában ez szokatlannak hangzik, viszont ez sajnos náluk nem teljesen furcsa. Utópisztikus gondolat, hogy valakit a cselekedetei alapján osztályozzanak, és ezek alapján élhesse tovább az életét. Ha jól teljesít és könnyedén összejön minden, akkor jobb az élete viszont, ha egyszer valami balul sül el, és még csak nem is feltétlenül tehet róla, akkor akár már a vonatjegyvásárlást is megtagadhatják az illető személytől.

Maga a rendszer már ismert, sok könyv és film vagy épp sorozat foglalkozik vele. Ilyen például az egyik epizód is a Black Mirror-ban (Fekete tükör) miszerint minél magasabb a kredited annál több mindenre vagy képes. Ezt tagadják, illetve ellenzik a kínaiak, hogy ez alapján menne a rendszerük, mivel ők csak a gazdasági szinten szeretnék ezt meghúzni, ezért is van az, hogy a kreditrendszert a Kínai Népi bank vezette be. itt a pontok 300 és 850 között kaphatók.

Két fő elemen alapszik a rendszer. az első, ahogy említettem a gazdasági vonal. A hitelminősítő intézetek jellemzően magánszemélyekre és cégekre vonatkozóan elemeznék kockázatokat és ésszerűsített számításokat igényelnek az értékelésükhöz. Így ezek az intézetek egy számosított értéket csatolnak az egyének vagy a cégek hírnevéhez, mint egy mutatót a megbízhatóság jegyében, hogy mennyire valószínű, hogy visszafizessék a hiteleiket. Azonban a kialakulóban lévő rendszerek köre, amelyek számszerűsítik és rangsorolják a státuszt, a hírnevet, az egyének és szervezetek bizalma pedig túlmutat a kreditpontokon. A második kar A big data-ban a szakértői értékelési rendszer. Magánszemélyek és vállalkozások rangsorolhatók és/vagy szakértői értékelési platformokon keresztüli értékelésekkel, amelyek tájékoztatják az embereket, hogy mennyire megbízhatóak a nyújtott szolgáltatások vagy termékek. Tehát, ha sok rossz értékelés érkezik, kreditet vonnak le tőlünk, pedig lehet nem is volt rossz az adott szolgáltatás, csak nem voltunk szimpatikusak a másik félnek. Sajnos ezért, mivel nem túl objektív a számítás, így nagyon sok rossz véleményt kapott ez a rendszer.³⁷

³⁷ Raghunath, N. (2024): Theorising quantified credibility in the age of big data: a case of China's Social Credit System. J. Chin. Sociol. 11, 12, <https://doi.org/10.1186/s40711-024-00212-0>

A Big Data-hoz kapcsolódó módszerek és megközelítések azért népszerűek, mert képesek megragadni az emberi viselkedés különféle nagy léptékű és mindenütt jelenlévő aspektusait, és olyan szintű betekintést nyújtanak, amelyet „intelligensnek” tartanak. Ennek ellenére komoly problémák vannak az ilyen rendszerekkel. Először is, a pontszámokat úgy alakították ki, hogy átláthatóságot teremtsenek az idegenek körében, ideális esetben hozzáférést biztosítva az erőforrásokhoz és növelve a társadalmi mobilitást. A számítások torzítása, vagy akár a pontszámok kiszámításához használt módszer és tényezők ismeretének hiánya megnehezíti a pontszámok kezelését. Ez az átlátszatlanság azt a nagyobb problémát mutatja, hogy a számszerűsített hitelességi számítások hogyan erősítik fel a torzulásokat és rejtik el a manipulációkat. Ehelyett normatív eszközként működnek, és ellentmondanak a kockázatok elkerülésének és az átláthatóság elősegítésének az idegenek közötti tranzakciókban. Ezen túlmenően az algoritmusok nagy adatelemzésben való használatát erős kritikák érték a tudósok részéről, mivel modelljeikben rejlő torzítások révén befolyásolhatják a státuszt, a hírnevet és a bizalmat, dacolhatnak a nyilvános ellenőrzéssel és csökkenthetik az átláthatóságot.³⁸

4.3.1. Okosotthonnal való kapcsolat

Ahogy írtam a kreditrendszer cégeket is értékel. Ez alá kell érteni azokat a gyárat is, amelyek az okosotthon rendszerhez gyártják az eszközöket. viszont az eszközök java részét itt adják el Európában. Náluk is ugyan úgy elterjedt a rendszer, hiszen technológiákat tekintve, hogy előttünk járnak, nem véletlenül a kínai gyártóktól vásároljuk ezeket a termékeket. Ez nekik is csak segítség, ha itt el tudják adni, mivel ez alapján is akár egy pozitív értékelést tudnak kapni, de még egyszer kiemelném, ez nem minden megyében és nem minden városban valósul meg, így nem feltétlen biztos, hogy ezekkel az eszközökkel ezt meg tudják valósítani. Ez sokkal inkább egy megfogalmazható előny lenne részükre.

Másik fő lehetőség már, és ez viszont a túlgondolás szintje, hogy amennyire előnyös, ugyan annyira hátrányos is. Semmi magánélete nem lenne az embereknek így, hiszen minden lépésük figyelve lenne. Ha nem is szó szerint a kamerákon keresztül, de például az alapján, hogy milyen gyakran mosnak, mikor takarítanak, és milyen alapanyagokból főznek, kiktől veszik ezeket meg, és milyen gyakorisággal teszik ezeket is.

Fontos megjegyezni, hogy ez valóban egy veszélyforrás lehet nekünk is, hiszen ha ezeket az adatokat be tudják gyűjteni és le is tudják képezni mesterséges intelligencia használatával,

³⁸ Raghunath, N. (2024): Theorising quantified credibility in the age of big data: a case of China's Social Credit System. J. Chin. Sociol. 11, 12, <https://doi.org/10.1186/s40711-024-00212-0>

akkor egy tényleges képet kaphatunk egy ember mindennapi életéről. Ezt természetesen igyekeznek jogi szabályozásokkal kivédeni, de kérdés, hogy ameddig nincs meg a tökéletes szabályzás, mi mindent lehet megtenni.³⁹

³⁹ Raghunath, N. (2024): Theorising quantified credibility in the age of big data: a case of China's Social Credit System. J. Chin. Sociol. 11, 12, <https://doi.org/10.1186/s40711-024-00212-0>

5. Esettanulmány

Hallottam egy esetről mely nem hazánkban, hanem történetesen Kínában történt. Ennek röviden a lényege a következő:

A kifigyelt és kiiktatni kívánt személy, egy ilyen lakásautomatizálási rendszerrel rendelkezett, amelybe beletartoztak a háztartási gépei, eszközei is. Minden eszköz hozzá volt csatlakoztatva okostelefonjához, és ezen a telefonon; az alkalmazáson belül pedig minden használati eszköz le volt profilozva adott személyünkre. Egyúttal itt jött be a hiba, mivel a betegségeire szedett gyógyszerei is fel voltak írva a rendszerbe. Ezt kifigyelték természetesen, majd egy hosszabb tervezést követően betörték az illető otthonába; könnyedén kijátszva a rendszert, és ezekkel az előbb említett gyógyszerekkel „játszottak”. Ennek okán az illető meg is halt.

Nem egy ilyen hírt olvasni a külföldi médiában, és nem is véletlenül tartanak az emberek ezektől a rendszerektől. A lehető legkisebb hanyagság miatt akár a saját sírunkat is megáshatjuk, pláne, ha fontos szerepet betöltő emberek vagyunk, ám hanyagok vagyunk a mindennapi életben.

Fontos megérteni azt is, hogy minden olyan rendszer, ahol egyre több a digitális elem, illetve egyre több a hálózatra illesztett eszköz, annál könnyebb hírt szerezni a többi eszközről is, illetve egy sokkal összetettebb képet tudunk magunkról, emberről alkotni, mivel ezeken keresztül megfigyelhetőek a szokásaink is.

Ezt is alátámasztva hoznék el egy 2016-os esetet is, amikor a Mirai nevű botnet (malware) rácsatlakozott több DVR-re (digitális videó rögzítő), kamerákra és útválasztók összekapcsolt eszközei közé és leállította a nagy webhelyeket DDoS (Distributed Denial of Service; elosztott szolgáltatásmegtagadással járó támadás) támadásokkal. Ezt a támadást és magát a Mirai malware-t egy csapat white hat hacker vette észre.⁴⁰

Device Hijacking (eszköz-eltérítés) egyébként a leggyakoribb hibái, támadási felületei egy ilyen rendszernek. Bár a fordítás nem a legjobb, ténylegesen a készülékek feletti uralom átvétel az elsődleges cél, illetve az eszköz is.

Erre hoznám is a következő kutatást⁴¹, amit olvastam. Ezt 2023-ban készítették, és leginkább a biztonsági kockázatokra világítottak rá ezeknél a rendszereknél.

⁴⁰ Young K. (2022): Cyber Case Study: [The Mirai DDoS Attack on Dyn](#), Coverlink Insurance

⁴¹ Aniketh Girish et. al. (2023): In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes, In Proceedings of the 2023 ACM on Internet Measurement Conference (IMC '23). Association for Computing Machinery, New York, NY, USA, 437–456.

„Amikor arra gondolunk, hogy mi történik otthonunk falai között, úgy gondoljuk, hogy ez egy megbízható, privát hely. A valóságban azt tapasztaljuk, hogy az otthonunkban lévő intelligens eszközök átütik a bizalom és a magánélet fátylát – oly módon, hogy szinte minden vállalat megtudja, milyen eszközök találhatók az Ön otthonában, megtudja, mikor van otthon, és megtudja, hol van az otthona...” – nyilatkozta David Choffnes, a Northeastern University Kiberbiztonsági és Adatvédelmi Intézetének ügyvezető igazgatója és a számítástechnikai docense egy sajtóközleményben.

Pontosan a kutatás ezt is tudja alátámasztani, hogy a fent említett adatok mennyire könnyen elérhetőek, és ez eléggé elgondolkodtató, hogy ér-e annyit a kényelmünk, hogy akár tudva vagy tudatlanul, bárki ránk törheti az ajtót.

A kutatást Montreálban, Kanadában az AMC Internet Measurement Conferene (AMC IMC), nevű konferencián hozták közönség elé, „In the room where it happens: Characterizing Local Communication and Threats in Smart Homes” címmel.

Ezekon kívül nap mint nap történnek ezek a támadások. Akár szándékosan, vagy csak tesztelési szándékkal. Ezen kívül felsorolnék még pár eshetőséget, amikben egy ilyen rendszer tulajdonosa sérülhet: ilyen például a személyazonosság-lopás, a célzott támadások, az adatvédelmi aggályok, a készülék vagy anyagi kár, maga a szoftver, és a jelszavak kihasználása. Valamint a behatolás, a hálózati problémák, a hangfelvétel és másítása, a hírszerzés továbbá az irányítás hiánya.

6. Megelőzés és megoldások

Több lépésen keresztül is van lehetőség megvédeni hálózatainkat. Szeretnék is egy pár lehetséges lépést bemutatni, amelyek hasznosak lehetnek akár a jövőre tekintve is.

Első fontos lépés, hogy a kiberhigiéné helyezzük előtérbe. Nagyon sok minden múlik ezen a lépésen, hiszen, ha nincs meg, a megelőzési fázis máris elbukott. Ide kell érteni alapvető lépésként a vírusirtó telepítését, a tűzfalak használatát, a rendszeres szoftverfrissítéseket, az erős jelszavaknak használatát, a több faktoros azonosítások használatát, az eszköztitkosítást, a rendszeres mentéseket és a merevlemezek tisztán tartását, illetve a router titkosítását is.⁴²

Ahogy korábban elemeztem, nagyon fontos eleme a rendszerek biztonságossá tételéhez, ha a wifi hálózat jelszava is meg van változtatva az eredetitől eltérőre, és sokkal bonyolultabbra. Ha az alapvető jelszó van beállítva, az csak egy sokkal könnyebb támadási felület egy kiberbűnözőnek. Ennél a lépésnél lehet már gondolkodni a jelszóbankok használatán is, hiszen könnyű ezeket is kezelni, illetve nekünk is egy segítség, hogy nem kell mindent fejben tartani.

Az IoT rendszerek sajátossága, hogy nem feltétlenül kell egy hálózaton lennie, mint a háztartásban többi használatos készülék (például okostelefonok, számítógépek). Ezért lehet célszerű egy vendég hálózatot kialakítani az IoT rendszer eszközeinek.

Érdemes ezeken felül többször, és gyakran ellenőrizni a felhasználók listáját, akik hozzáférhetnek ezekhez a rendszerekhez. Időközönként ezt még jó lehet frissíteni is, hiszen sosem lehet tudni, épp mikor ki szeretne adatainkhoz hozzáférni. Illetve az is megoldás lehet, ha csak egy vagy pár privilégiumokkal rendelkező felhasználó fér csak hozzá a rendszerhez.

Különösen fontos területként emelem ki a fizikai eszközöknek is az elérhetetlenséggé tételét, hiszen az is egy komoly megelőzési lépés, ha fizikailag nem lehet az eszközhez hozzáférni.

Fontos lépés akár a nem használt eszközök leválasztása is a rendszerről, mivel ezzel is ki lehet védeni egy támadási felületet. Nem kerülünk átverésbe sem, hogy pont egy olyan eszközről próbálnák meg megközelíteni a hálózatot, ami egyébként nincs is használatban.

A felesleges és nem használt tulajdonságait is ki lehet kapcsolni az eszközöknek, hiszen nem feltétlenül kell minden eszköznek minden háztartásban ugyan azokat a tevékenységeket

⁴² A. Vishwanath, L.S. Neo, P. Goh, et al., (2019) Cyber hygiene: The concept, its measure, and its initial tests, Decision Support Systems, <https://doi.org/10.1016/j.dss.2019.113160>

végeznie. Egy két gyerekes családnak és egy egyedül élő egyetemistának is mások az igényei. Így ezeket testre lehet szabni.

Illetve a frissítést már írtam, de itt is elengedhetetlen lépés, hogyha rendszerszinten érkezik egy frissítés az adott eszközre, akkor azt le is töltsük, hiszen lehet, hogy egy előzetes frissítési szoftverhibát javítottak ki.⁴³

⁴³ Trevino A. (2023) [How to Prevent Internet of Things \(Iot\) Attacks](#) Keeper Security, Inc.

Összegzés

A kutatásom megkezdésekor több feltevésem is volt a rendszerrel kapcsolatban. Az egyik felvetésem az volt, hogyha értenék és tudnák az emberek ezeket a rendszereket, akkor a keletkező hibák és támadhatósági részek leszűkülnek. Hiszen ha valami szokatlan dolog történik, akkor könnyebben és gyorsabban ki lehetne ezeket védeni. Eddigi kutatásom során megfogalmazódott bennem megoldási javaslatként az is, hogy több oktatást vagy képzést kell ezekkel kapcsolatban tartani. Mert még mindig, ha csak anyag található ezekkel kapcsolatban, azt nem fogják maguktól elolvasni az emberek. Illetve amikor implementálják a rendszert akkor biztosan elmondja a rendszer telepítője, hogy mit mikor hogyan kell használni, viszont ezt nem fogják megjegyezni. Sajnálatos tény, hogy még mindig, ha az ember nem akar valamit megtanulni, akkor nem is fogja.

Ezt viszont nagyapámtól tanultam el, hogy van egy szó: „akarom”, ha ez megvan, akkor már félig megoldottuk az akadályokat.

Második feltevésem pedig a kínai kreditrendszerrel volt kapcsolatos. Így, hogy megannyi forrást tanulmányoztam, és ez által rengeteget olvastam róla, én látom rá a lehetőséget, hogy az okosotthon rendszerekkel, könnyítsék a dolgukat a pontozásra. Megannyi szokása van az embernek, melyeket a zárt ajtó mögött nem látni, és inkább ezek azok, amelyek az igazi arcát mutatnák. Teljesen még ezt a kreditrendszert sem látom kiforrottnak, illetve ahogy mások fogalmazták, nem túl objektív. Ezeken is van még mit csiszolni, de látni a rendszer potenciálját.

Első példából adódóan, amit az esettanulmány bekezdésben fogalmaztam meg, lehet tapasztalni is, hogy még mindig saját magunk ellenségei tudunk lenni. Sok múlik azon, hogy mikor mit teszünk közzé, és ez miatt kell egy szintű tudatosságot is tanítani az eszközök mellé. Egy kis digitális kompetencia sem árt; tudni használni a rendszereket. Fontos tudni ám azt is, hogy mivel információs technológiáról van szó, így már eleve esélytelen a teljes biztonság.

Személy szerint mindig úgy állítottam, hogy minél több az elektronika ott egyre több a hiba lehetőség, vagy épp a támadási felület. Ahogyan ez a gépjárműveknél is így van, ez az okosotthon rendszerben is ugyan így megtalálható.

Tehát fontos azt leszögezni, hogy ez egy több tényezős rendszer, és ez által több a támadhatóság is. Márpedig mindig nem az eszköz, hanem a cél a legfontosabb. És ha valakinek az a fontos, hogy érzékeny adatokat tudjon meg rólunk, akkor ennek az érdekében mindent el is fog követni, hogy meg is szerezhesse az adatokat.

Sosem az a fontos, hogy mi kik vagyunk, csak az, amit tudunk, hiszen az információ hatalom, és van már az a szint, ahol veszélyes sokat tudni. A minősített adatok védelme pedig elengedhetetlen, az mindegy is, hogy milyen szervtől származnak.

Célom, hogy folytassam még részletesebben ezt a kutatást, amit elkezdtem, hiszen ez a téma napjainkban lassan kihagyhatatlan, valamint több példát is szeretnék a későbbiekben ehhez a kutatáshoz csatolni. Valamit kutatási területemnek szeretném kitűzni ezzel az írással az okos rendszerek és az emberi tudatosság kapcsolatát. Keveset kutatott téma ez véleményem szerint, ezért készítem szakdolgozatom is hasonló témában. Mivel emberek vagyunk fontos először a saját határainkat és „ellenfeleinket” megismerni.

Legyen ez a kis írás egy tanulság mindenki számára, hogy sokkal körültekintőbbnek, és sokkal tudatosabbnak kell lennünk saját magunkra, és környezetünkre való tekintettel.

Felhasznált irodalom

1. Advanced Message Queuing Protocol (2024) [About](#)
2. Constrained Application Protocol (2024) [Technologies](#)
3. DDS Foundation (2024): What is DDS?, Object Management Group
4. Frascà D., Venturi G., Ustenko M. and Zanasi A. (2023): Technologies for IMINT and SIGINT, 2023 IEEE International Workshop on Technologies for Defense and Security (TechDefense), Rome, Italy, 2023, pp. 165-169, doi: 10.1109/TechDefense59795.2023.10380827.
5. Girish A. et. al. (2023): In the Room Where It Happens: Characterizing Local Communication and Threats in Smart Homes, In Proceedings of the 2023 ACM on Internet Measurement Conference (IMC '23). Association for Computing Machinery, New York, NY, USA, 437–456.
6. Henrico S., Putter D. (2024): Intelligence Collection Disciplines—A Systematic Review. Journal of Applied Security Research. 1-25. 10.1080/19361610.2023.2296765.
7. Industrial Internet Consortium (2024): [About us: Overview](#)
8. Institute of Electrical and Electronics Engineers (2024): [About: At a glance](#)
9. International Electrotechnical Commission (2024): [What we do for safety, sustainability and global trade](#)
10. IPCisco (2024): Network Topology Architectures
11. Izzat A. (2023): The NICE Cyber Security Framework; Cyber Security Intelligence and Analytics, Springer Cham, 978-3-031-21651-0, <https://doi.org/10.1007/978-3-031-21651-0>
12. John D'Ambrosia (2024): [IEEE 802](#)
13. Kovács, V. (2021): HomEalone - avagy hogyan ne járjunk úgy, mint Kevin, ZSZC Csány László Technikum
14. Long-Range Wide Area Network (2024): [About LoRaWAN](#)
15. Loshin, P. (2004): IPv6: Theory, protocol, and practice.
16. Nagy Tibor I. (2012): *Szenzorhálózatok szoftverfejlesztési kérdései*, Military Engineer/Hadmérnök, 7(1).
17. Nemzeti Kibervédelmi Intézet (2024.február 7.): [Malware-rel fertőztek meg okos fogkeféket](#)
18. Olson K. , Wampler J. , Keller E. (2023): Doomed to Repeat with IPv6? Characterization of NAT-centric Security in SOHO Routers

19. Open Connectivity Foundation (2024): [About us](#)
20. Raghunath, N. (2024): Theorising quantified credibility in the age of big data: a case of China's Social Credit System. J. Chin. Sociol. 11, 12, <https://doi.org/10.1186/s40711-024-00212-0>
21. Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. The internet society (ISOC), 80(15), 1-53.
22. Thread Group (2024): [What is Thread?](#)
23. Trevino A. (2023): [How to Prevent Internet of Things \(Iot\) Attacks](#) Keeper Security, Inc.
24. Vishwanath, L.S. Neo, P. Goh, et al., (2019): Cyber hygiene: The concept, its measure, and its initial tests, Decision Support Systems, <https://doi.org/10.1016/j.dss.2019.113160>
25. Vuorikari, R., Kluzer, S. és Punie, Y.,(2022): DigComp 2.2: Állampolgári Digitáliskompetencia-keret, EUR 31006 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-76-48882-8, doi:10.2760/115376, JRC128415.
26. Wing D. (2010): Network Address Translation, Extending the Internet Address Space, IEEE Internet Computing, 14(4), 66–70. doi:10.1109/mic.2010.96
27. Yeboah-Ofori, Abel. (2018): Cyber Intelligence and OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media. International Journal of Cyber-Security and Digital Forensics. 7. 87-98. 10.17781/P002378.
28. Young K. (2022): Cyber Case Study: The Mirai DDoS Attack on Dyn, Coverlink Insurance
29. Zhang, Yunxiao, Malacaria, Pasquale, Loukas, George and Panaousis, Emmanouil (2023): CROSS: a framework for cyber risk optimisation in smart homes. Computers and Security, 130:103250. ISSN 0167-4048

Ábrajegyzék

1. ábra: Egy okosotthon rendszer szenzor rendszere (saját szerkesztés, forrás: középiskolai projekt)
2. ábra: Egy okosotthon rendszer hálózata (saját szerkesztés, forrás: középiskolai projekt)
3. ábra: SOHO hálózat topológiája (forrás: IPCisco.com)

4. ábra: OSI modell rétegei (saját szerkesztés, forrás: Nagy Tibor I. (2012): Szenzorhálózatok szoftverfejlesztési kérdései, Military Engineer/Hadmérnök, 7(1).) (utolsó elérés: 2024.április 13.)
5. ábra: TCP/IP modell rétegei (saját szerkesztés, forrás: Nagy Tibor I. (2012): Szenzorhálózatok szoftverfejlesztési kérdései, Military Engineer/Hadmérnök, 7(1).)(utolsó elérés: 2024.április 13.)