INFORMATIKA TANSZÉK
DEPARTMENT OF COMPUTER SCIENCE

SZÉCHENYI EGYETEM
UNIVERSITY OF GYŐR

SZAKDOLGOZAT

Okosotthonok biztonsága és sérülékenységei

Tölgyesi Dániel

Mérnökinformatikus BSc

Mérnökinformatikus Szakirány

2022

Tartalomjegyzék

Ábrák jegyzéke

Nyilatkozat

Alulírott, **Tölgyesi Dániel (GHGO5W)**, Mérnökinformatikus BSc szakos hallgató kijelentem, hogy a *Okosotthonok biztonsága és sérülékenységei* című szakdolgozat feladat kidolgozása a saját munkám, abban csak a megjelölt forrásokat, és a megjelölt mértékben használtam fel, az idézés szabályainak megfelelően, a hivatkozások pontos megjelölésével.

Eredményeim saját munkán, számításokon, kutatáson, valós méréseken alapulnak, és a legjobb tudásom szerint hitelesek.

Győr, 2022-11-09

Tölgyesi Dániel
hallgató

1. fejezet

Bevezetés

A digitalizáció hatására ma, már minden háztartásban található vezetékes és vezeték nélküli eszköz is hozzáfér az internethez, melynek nemcsak előnye, de hátránya, hogy ezek ugyanolyan veszélynek vannak kitéve, mint bármely más, kisebb vagy nagyobb cégekhez tartozó üzleti hálózatok. Szeretném bemutatni a hálózatok működésének alapfogalmait és az okos otthoni hálózatban résztvevő eszköztípusokat, feltárom azokat a sérülékenységi lehetőségeket, melyek nagy szerepet játszanak abban, hogy eljussunk a teljesen biztonságos lakhatáshoz.

1.1. ábra. Smart home felépítése

Egy modern, intelligens, „okos” otthont különféle számítástechnikai és elektronikai eszközök, illetve vezeték nélküli érzékelők együttesen alkotják. Az automatizáció megjelenése során a felhasználók újabb és nagyobb elvárásokat követelnek, mely a felhasználókra szabott, fejlesztett automatizált rendszerek viselkedéséhez új utakat lehet törni. Az okosotthonok világa előtt, egy átlagos családnak közönséges betörőkkel, bűnözőkkel kellett szembe szállniuk, míg jelen pillanatban a fejlesztőknek és az okos otthonnal rendelkezőknek, számítástechnikában jártas, technikailag igencsak fejlett kiberbűnözőkkel kell felvenni a harcot, hogy megvédhessék otthonukat az esetleges külső támadásoktól. Ezek az emberek képesek megtalálni és kihasználni azokat a biztonsági réseket, amelyek alapján lehetőségük van manipulálni az adott hálózatot és az ahhoz csatlakoztatott eszközöket is, ezáltal könnyedén szabad utat nyerve a bejutáshoz. A lakatok és zárak fizikai feltörését felváltja például

egy riasztórendszer tűzfalának kiiktatása vagy az automata kapunyitórendszer meg hackelése. Azonban az okosotthonok biztonsági kérdése kritikusan foglalkoztatott és fokozott figyelmet kap, viszont a technika mai állása szerint kijelenthetjük, hogy teljesen tökéletes és 100Számos kutatás és kísérletezés valósult meg az okosotthonok koncepciójával kapcsolatban az 1970-es évek vége óta. Fontos tényező, hogy mivel megfizethetőbbek és népszerűbbek lettek az elektronikus eszközök és az internethez való hozzáférés is. Hatalmas szerepet játszik az automatizálás és a kényelem, ezért egyre jobban érdeklődnek az emberek az okosotthonok iránt. [4]

2. fejezet

Okosotthonok megítélése és elterjedése

2.1. Világszerte

2.2. Magyarországon

3. fejezet

Alapvető definíciók ismertetése

3.1. Internet of Things

Az IoT-ről, azaz a dolgok internetéről, akkor beszélhetünk, amikor az otthonunkban az az internethez csatlakoztatott eszközök meghaladják az ott élő emberek számát. Ezeknek az eszközöknek a célja, hogy megkönnyítse mindennapi életünket, úgy, hogy egy digitális világban intelligens környezetet biztosít számunkra. Autonóm eszközök segítségével adatgyűjtést végeznek a mindennapi tevékenységünkről, melyet továbbítják az úgynevezett felhőbe, hogy még precízebb képet tudjanak alkotni cselekvéseinkről. Az IoT eszközök nagyrészt vezeték nélkül csatlakoznak az internethez, mint például okos telefonok, okos otthonok és különböző az intelligens környezethez csatlakoztatható eszközök, plug-in modulok.
Az IoT 4 fő réteg szakaszból épül fel:[2]

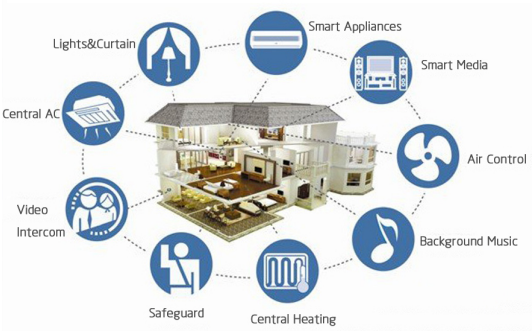
- Észlelési réteg
- Hálózati réteg
- Közvetítői réteg
- Alkalmazási réteg

3.1.1. Smart Home

Az intelligens otthon a technológia és a szolgáltatások integrálása az otthoni hálózatba. Automatizáció implementálása a jobb életminőség érdekében. Rengeteg különböző technológiákat használ az otthon egyes részeinek felszerelésére az intelligensebb felügyelet és távvezérlés érdekében. A mindennapi háztartási feladatok és tevékenységek automatizálása anélkül, hogy a felhasználó beavatkozna abba. Bizonyos esetekben az otthoni szolgáltatások integrációja lehetővé teszi, hogy azok kommunikáljanak egymással az otthoni vezérlőn keresztül, ezáltal lehetővé téve, hogy

egyetlen gomb segítségével különböző otthoni rendszereket vezéreljenek a mi fizikai beavatkozásunk nélkül.

Egy okosotthonban előre beprogramozott forgatókönyvek vagy működési módok, illetve tanulási minták alapján tervezett lépések vannak a rengeteg összegyűjtött szokási mintákból. Az intelligens otthonok javíthatják az otthoni kényelmet, komfortot, biztonságot és energiagazdálkodást. Ezen kívül az idősek és fogyatékkal élők számára is biztonságos és védett környezetet nyújthatnak.[6]



3.1. ábra. Okosotthon integrációs szolgáltatások

Rendkivűl pozitív előnye ennek a technológiának, hogy energiát és más erőforrásokat takarít meg. Az intelligens otthonok iránti fogyasztói lelkesedés ellenére azonban a biztonság és a védelem még mindig komoly aggodalomra ad okot. Ezek együttesen szabnak gátat a technológia elfogadásához.

3.2. Biztonság

Megállapíthatjuk, hogy a biztonság fogalma a civilizáció fejlődése során folyamatosan és exponenciálisan változik. Nehéz megfogalmazni, mivel nagyon komplex és számos területre ágaztathatjuk. Jogi biztonság, közlekedési, főként katonai és informatikai. A biztonságra való törekvés a történelem során mind az egyénben, mind a társadalomban jelen volt. Az élet számos területein szükség van biztonsági intézkedésekre és azok elhárítására. Ma a katasztrófák vagy fenyegető vészhelyzetek olyan kihívások elé állítják a szakembereket, amelyek jellegükben, nagyságrendjükben és összetettségükben gyökeresen eltérnek a korábban tapasztaltaktól.[1] Ebben a szakdolgozatban az okosotthonok technologiájához kapcsolódó biztonsági intézkedéseket és azok sérülékenységeit fogom részletesen kifejteni és ismertetni.

3.2.1. IT Security

Ahogy a hackerek okosabbak és találékonyabbak lesznek, így még nagyobb az szükség van a digitális eszközök védelmére. Nagyrészt egy biztonságos rendszer kivitelezé-

se költséges, de egy nem ismert biztonsági rés, jóval nagyobb pénzügyi kiesést tud okozni. A személyes adatok védelméhez informatikai biztonsági mechanizmusokra van szükség. Az IT security az információkat kezelő és tároló rendszereket, valamint az ezekbe történő feldolgozott adatokat védelmét fogalmazza meg. Az informatikai biztonságot gyakran a magánélet technikai oldalának tekintik. A biztonsági mechanizmusok belső mechanizmusok, amelyeket az informatikai rendszer valósít meg és külső mechanizmusok, amelyek a rendszeren kívül történnek. A témát öt fő részre taglalnák, amelyek közül kiemelném a hálózati biztonságot, ami lényegében megakadályozza, hogy illetéktelen felhasználók hozzáférhessenek egy hálózathoz. Ez a fajta biztonsági tényező biztosítja, hogy ne lehessen elérni az érzékeny és privát adatokat a hálózatokon keresztül.

Néhány szót ejtenék a végpontbiztonságról is, mely eszközszintű védelmet nyújt. A végpontbiztonság megakadályozza, hogy az eszközök hozzáférjenek a rosszindulatú hálózatokhoz, amelyek veszélyt jelenthetnek a felhasználók adataira. Naojain fejlett rosszindulatú programjaik elleni védelem és az eszközkezelő szoftverek példák a végpontbiztonságra. A végpontbiztonság által védett eszközök a táblagépek, mobiltelefonok, laptopok.

Tulajdonképpen minden olyan rendszerek, rendszerösszetevők, hálózati eszközök melyek alkalmasak adatok tárolására és továbbítására az IT Security fogalma alá tartoznak.[8]

3.2.2. Cyber Security

Alapesetben a kiberbiztonság a hálózatok és a rendszerek szoftveres biztonságát jelenti, számítógépekkel történő támadások ellen, viszont az elmúlt években a hálózatok a puszta kommunikációs eszközökből mindenütt jelenlévő számítástechnikai infrastrukturális hálózatokká alakultak át. A jelenlegi hálózatok nagyobbak, gyorsabbak és rendkívül dinamikusak. Ennek eredményeként a számítógépek és hálózati technológiák használata a kiberbiztonságot mára, már nemzetbiztonsági kérdéssé tette. Az internet a kormányok, vállalatok és a hétköznapi ember életének szerves része lett. A számítógépeket és a hálózatot például gyártási folyamatok kivitelezésére, tőzsdei rendszerek üzemeltetésére, légiforgalmi irányítási rendszerek kezelésére és a legújabb TikTok videó feltöltésére is használjuk. Az életünkbe való beépülés miatt a hálózati támadások elkezdték befolyásolni a valódi életünket is. Elsődleges célja egy kibertámadónak a pénzszerzés, melyet többféle módon is kivitelezhet. Célpont lehet közvetlenül egy kiszemelt bank, ami lássuk be nehezebben megvalósítható, viszont könnyebb préda egy ártatlan bankkártyafelhasználó. Különféle módok vannak a felhasználói adatok megszerzésére, amihez kizárólag a bankfiók tulajdonosát kell „meghackelni”, ezt nevezzük a Social Engineeringnek. Ebben az esetben az ember

a kulcs és a gyenge láncszem. A felhasználóknak meg kell érteniük és be kellene tartaniuk olyan alapvető szabályokat és biztonsági előírásokat, mellyel megelőzhető lenne a személyes adataiknak a kiszivárgása.

A digitális világban végrehajtott bűncselekményeket 3 fő csoportra oszthatjuk fel, ezek közül az elsőként említendő és a köztudatban a legelterjedtebb a kiberbűnözés, amely véghezvihető egyedül és csoportban is. Ezek a támadások legfőképpen pénzszerzés céljából alakulnak ki, a rendszer vagy hálózat sérülékenységeit kihasználva nyerészkednek, vagy kárt tesznek abban.

3.2. ábra. Anonymous hackercsoport szimbóluma

A kiberterror, az a jelenség, amikor a digitális világ adta előnyöket kihasználva információs infrastruktúrákat támadnak vagy ezen keresztül félemlítenek meg embereket, előre megfontolva ugyanúgy egyedül vagy csoportosan.

Az utolsó ismertetett fogalom a kiber támadás, amelynek általában a legfőbb célpontjai nagyobb csoportok, mint például egy ország vagy nemzet.[3]

4. fejezet

Okosotthon bemutatása és felépítése

Az intelligens otthon a számítógépes technológia, a vezérlési technológia, a képmegjelenítési technológia és a kommunikációs technológiát a különböző létesítmények hálózatán keresztül összekapcsolják, hogy megfeleljen a az egész rendszer automatizálási követelményeinek teljesítése érdekében, hogy kényelmesebb vezérlést és irányítást biztosítson. Az intelligens otthon nagyjából a következőképpen írható le egy ház, mely fel van szerlve intelligens tárgyakkal, egy otthoni hálózat lehetővé teszi az információk továbbítását az eszközök között, és egy, az okosotthonokat összekötő lakossági átjáró, ami összeköti az otthont és a külső internetes világot. Az intelligens tárgyak lehetővé teszik a lakókkal való interakciót vagy a lakók megfigyelését.

Az intelligens hálózatot alkotó egyik rendszer a következő a távközlés. A távközlési rendszerek lehetővé teszik a összekapcsolják a villamosenergia-ágazat különböző szereplőit a megbízhatóság, skálázhatóság, rendelkezésre állás, biztonság, alacsony energiafogyasztás, biztonság és alacsony késleltetést, a szolgáltatás minőségét, az interoperabilitást és a költségeket.
A távközlési rendszerek a következőképpen csoportosíthatók földrajzi terület szerint, ugyanazt a célt szolgálva:

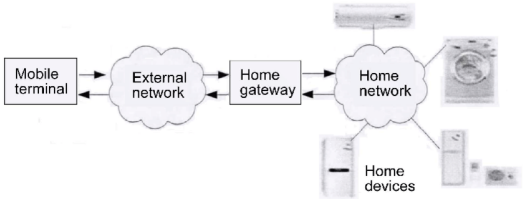
- Home area network (HAN)
- Neighborhood Area Network (NAN)
- Wide area network (WAN)

4.1. Intelligens otthoni rendszer modell

Az okosotthonba integrálható intelligens tárgyak lehetnek olyan egyszerűek, mint egy lámpa, amelyet vezérelhetünk vagy lekérdezhetjük a valós idejű az állapotáról,

egy hűtőszekrény, amely ismeri az állapotát és képes önkiszolgálni a azt változtatni vagy akár egy otthon hagyott telefon is. Biztonsági rendszerek...stb.

Az otthoni hálózat (HAN) 10%-os átviteli sebességet igényel. A hálózatnak 5 kbps és 1 Mbps közötti sebességet és 5 és 100 közötti távolságot kell lefednie. Legfeljebb 5 méteres távolságot kell lefednie. A felhasználók és az elektromos hálózat közötti kommunikáció a generátor között proaktív, és lehetővé teszi az energia valós időben a fogyasztás függvényében. Eszközök, televíziók, világítási rendszerek, intelligens fogyasztásmérők Mindezek a tárgyak csatlakoznak az otthoni hálózathoz,



4.1. ábra. Okosotthoni rendszer felépítése

hogy megadják az állapotukat, vagy utasításokat kapjanak és vezérelhetőek legyen távolról. Az otthoni hálózat lehetővé teszi, hogy az otthon teljes mértékben összekapcsolódjon, mind külsőleg, mind belsőleg vezérelve. Az otthoni hálózati átjáró (gateaway) biztosítja a külső hozzáférést Ethernet vagy az interneten keresztül. Ez az átjáró lehetővé teszi az otthoni csatlakozást és az új szolgáltatások letöltését. A szolgáltató felelős az új szolgáltatásokért és azok elérhetőségéért a lakók számára.[5]

4.2. IoT alapú intelligens otthon kialakítása

Annak elérése érdekében, hogy minden eszköz kapcsolatban álljon egymással az általunk tervezett intelligens otthoni rendszernek a ZIGBEE-t kell hogy használja a helyi otthoni hálózat kiépítéséhez, hogy érzékelje az otthonban lévő tárgyakat vagy eszközöket, és a helyi otthoni hálózatot 3G-n vagy Etherneten keresztül összekapcsolja az internettel. A rendszer három rétegre oszlik: érzékelő és működtető réteg, hálózati réteg és alkalmazási réteg.

4.2.1. Mi is az a Zigbee?

A Zigbee egy vezeték nélküli kommunikációs forma, amelynek az alapja az IEEE 802.15.4 hálózati szabvány, ami a személyi hálózatot használja. Ez technológia több mint egy évtizede jelen van a piacon és sokan a Wi-Fi és a Bluetooth technológia alternatívájaként tekintik az alacsony fogyasztású, nagy sávszélességet nem igénylő eszközök számára. Kiváló példa a működésének bemutatásához, hogy amikor van egy intelligens izzó és egy villanykapcsoló, amit szeretnénk összekapcsolni, hogy a

kapcsolóval tudjuk irányítani az izzót. A Zigbee kommunikáció segítségével a két eszközt össze tudjuk hangolni, hogy megértsék egymást, még akkor is, ha azok teljesen más gyártótól származnak.

A Zigbee-t erdetileg nem P2P kommunikációra tervezték, mint például a Bluetooth-t, használatához mindenképpen szükség van egy helyben felszerelt központi egységre, egy hubra vagy átjáróra, amellyel minden eszköz tud kommunikálni. A Zigbee további előnye, hogy egy tisztán Zigbee-alapú rendszerben csak a hub / gateway rendelkezik WiFi vagy vezetékes internetkapcsolattal, így a sok okoseszköz nem terheli túl a WiFi hálózatot, mivel minden eszköz egy dedikált rendszerben beszél egymással az okoseszközök számára, amelyek a WiFi-től eltérő frekvenciasávokat használnak, így még néhány hubdal is kiváló rendszer lehet egy nagy ingatlanban.

Be kell vallani, hogy a Zigbee igénytelen, egyszerű, viszont megbízható és kiválóan működik, ha intelligens rendszer kialakításához szeretnénk összekötni eszközöket.[7]

4.2.1.1.

5. fejezet

Okosotthon előnyei és hátrányai

6. fejezet

Az okosotthonok elleni kibertámadások

6.1. Bűnözők a monitor másikfelén

6.2. Script kiddies

6.3. Elterjedt ámadási technikák

6.3.1. Támadások egyik

6.3.1.1. Phising websites

6.3.2. Támadások másik

6.4. Biztonsági sérülékenységek a hálózaton

6.5. Kibertámádások elhárítása

6.5.1.

Irodalomjegyzék

[1] Dr. Csutorás Gábor, 2013. https://tudastar.mk.uni-pannon.hu/anyagok/29-Biztonsagtudomany.pdf.

[2] Li Jiang – Da-You Liu – Bo Yang: Smart home research. In *Proceedings of 2004 International Conference on Machine Learning and Cybernetics (IEEE Cat. No.04EX826)* (konferenciaanyag), 2. köt. 2004, 659–663 vol.2. p.

[3] R.A. Kemmerer: Cybersecurity. In *25th International Conference on Software Engineering, 2003. Proceedings.* (konferenciaanyag). 2003, 705–715. p.

[4] Nikos Komninos – Eleni Philippou – Andreas Pitsillides: Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys & Tutorials*, 16. évf. (2014) 4. sz., 1933–1954. p.

[5] Vincent Ricquebourg – David Menga – David Durand – Bruno Marhic – Laurent Delahoche – Christophe Loge: The smart home concept: our immediate future. In *2006 1st IEEE international conference on e-learning in industrial electronics* (konferenciaanyag). 2006, IEEE, 23–28. p.

[6] Rosslin John Robles – Tai-hoon Kim: Applications, systems and methods in smart home technology: A. *Int. Journal of Advanced Science And Technology*, 15. évf. (2010), 37–48. p.

[7] Stanislav Safaric – Kresimir Malaric: Zigbee wireless standard. In *Proceedings ELMAR 2006* (konferenciaanyag). 2006, 259–262. p.

[8] What is it security? - information technology security, 2022. May. https://www.cisco.com/c/en/us/products/security/what-is-it-security.html.