AZ OKOS OTTHONOK VEZETÉK NÉLKÜLI ALKOTÓELEMEINEK BIZTONSÁGA

SAFETY OF SMART HOME WIRELESS COMPONENTS

VARGA PÉTER JÁNOS egyetemi adjunktus
Óbudai Egyetem Kandó Kálmán Villamosmérnöki Kar

Abstract

Smart home has become more and more popular. The best definition of technology is: the integration of technology and services through home networking for a better quality of living. It involves the control and automation of lighting, heating, ventilation, air conditioning , and security. Smart homes consist of three main parts of the communication technology perspective:

– communication channel,
– peripheral devices,
– central control unit.

All three areas have wired and wireless components. Modern systems generally consist of switches and sensors connected to central control unit witch have a network connection. All system can be interacted either with a wall-mounted terminal, mobile phone, tablet or PC using a program or a web interface. WLAN is often used for remote monitoring and control the system. The safety of ingredients determines the security of the entire building.

1. Bevezetés

Napjainkra az okos otthonok különböző berendezések és rendszerek felügyelt és szabályozott egységes működésével üzemelnek. Minden ilyen komplex rendszer kialakításának fő célja az épület energiafogyasztásának optimalizálása, az épületben élők és értékeik biztonsága és kényelmük maximalizálása.

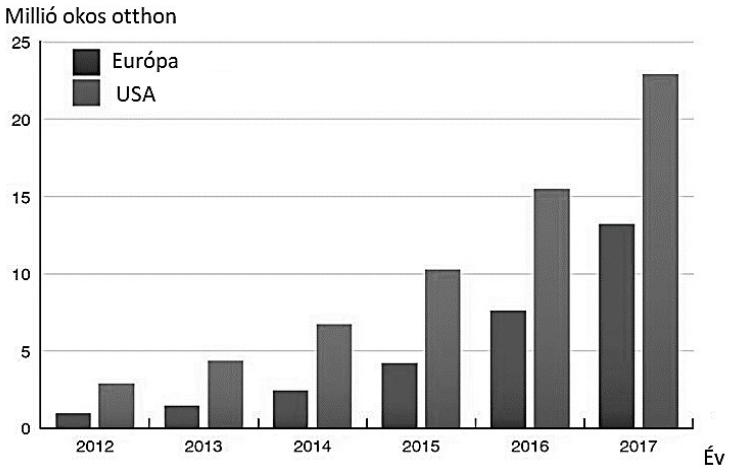
Az okos otthonok a kommunikációs technológiai szempontjából három fő részből állnak:

– kommunikációs csatorna,
– perifériás eszközök,
– központi vezérlő egység.

Mind a három terület rendelkezik vezetékes és vezeték nélküli összetevőkkel. Ezen összetevők biztonsága határozza meg a teljes épület biztonságát.

A rendszerek kialakítását figyelembe véve beszélhetünk az építéskor megtervezett és telepített intelligens rendszerekről és olyan megoldásokról, melyek csak a kivitelezés után, vagy egy régi építésű ingatlan esetében utólag kerültek beszerelésre. A következő diagram az okos otthonok számát mutatja 2012. és 2017. között Európában és USA-ban.

1. diagram: Okos otthonok száma Európában és USA-ban 2012 és 2017 között



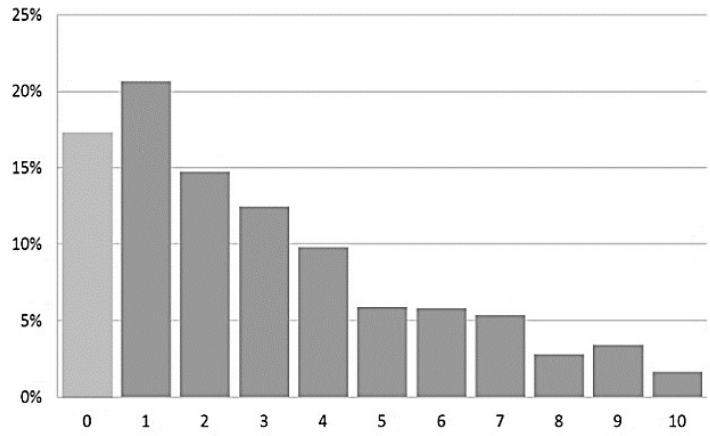
Forrás: https://mysmahome.com

A diagramon jól látszik, hogy az okos otthonok elterjedése Európában és az USA-ban is emelkedő tendenciát mutat. Ez azt jelenti, hogy az ilyen eszközök gyártási és eladási trendjei is emelkedtek.

2. Okos otthonok vezeték nélküli eszközeinek biztonsága

A PRPL alapítvány 2016-ban kutatást végzett az okos otthonok és eszközeinek biztonságáról. A kutatásban több mint 1000 fogyasztó vett részt három kontinensről és hat országból. A kutatás több tématerülettel foglalkozott. Az egyik tématerület, a vezeték nélküli intelligens eszközök penetrációját vizsgálta. A válaszadók 83%-a nyilatkozta azt, hogy rendelkezik olyan eszközzel, mely az otthoni vezeték nélküli hálózathoz csatlakozik. Ez az adat figyelemreméltó, ha azt vesszük alapul, hogy az olyan eszközök, mint a laptopok, okostelefonok és táblagépek nincsenek az intelligens otthoni eszközök listáján a kutatásban. A válaszadók 47%-a úgy nyilatkozott, hogy otthonában három vagy több intelligens eszköz van. A következő diagram az eszközök darabszámát mutatja otthononként.

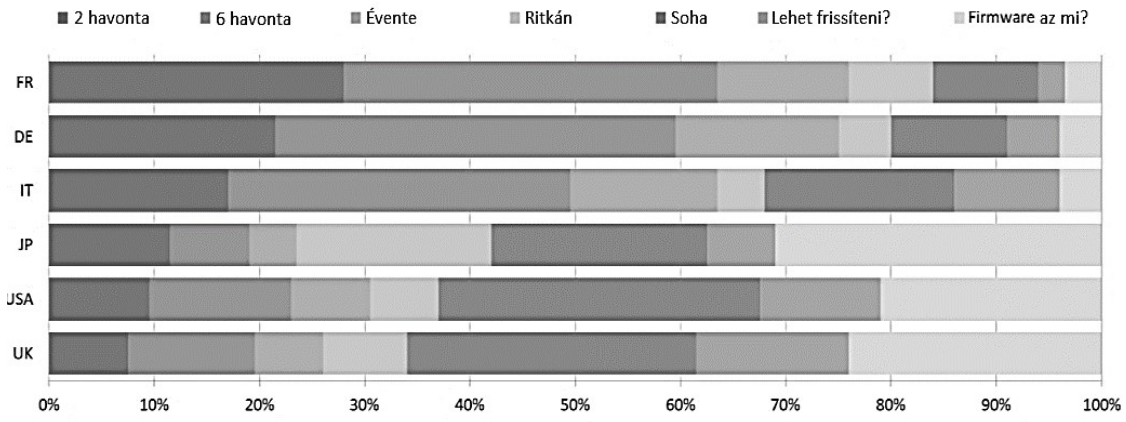
2. diagram: Eszközök darabszáma otthononként



Forrás: https://prplfoundation.org/

A legnépszerűbbek a multimédia centerek, a vezeték nélküli kamerarendszerek és az intelligens televíziók. Biztonsági aggályok az utóbbi években mindhárom eszközterületen felmerültek. Ilyenkor elgondolkodunk, hogy biztonságosak-e okos otthoni eszközeink. Sajnos nem jelenthető ki egyértelműen, hogy igen. A legnagyobb problémát az eszközök hálózati sebezhetősége jelenti. Maga a rendszer alapeleme a hálózat, mely sokszor kiegészül vezetékes vagy vezeték nélküli internet kapcsolattal is. Igy érhető el, hogy az eszközök ne csak saját ingatlanunkból, hanem bárhonnan elérhetők legyenek. Ezzel a megoldással azonban sok esetben biztonsági rés keletkezik okos otthonunk eszközeihez. A vezeték nélküli hálózati végpontokat működtető belső program – firmware – frissítéseinek figyelmen kívül hagyása kritikus sérülékenységet okozhat. A PRPL alapítvány kutatása ezt a kérdést is vizsgálta. A *3. diagram* ennek eredményét mutatja.

3. diagram: Firmware frissítési gyakoriság



Forrás: https://prplfoundation.org/

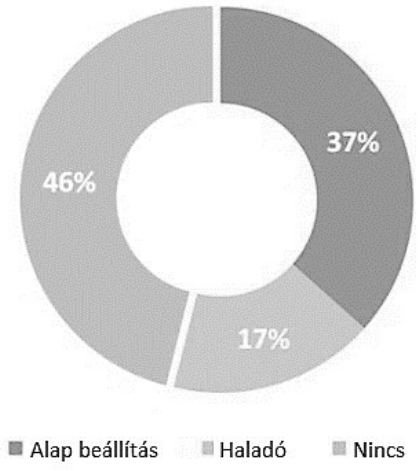
A megkérdezettek több mint fele (57%) azt mondta, hogy legalább évente egyszer frissítette a vezeték nélküli végpontja firmware-jét, de 20% soha nem tett így, és 23% nem is tudta, hogy lehetséges-e.

Az okos otthon vezeték nélküli hálózatában elengedhetetlen a végponti eszköz megfelelő hitelesítési és titkosítási beállításainak elvégzése. E nélkül a teljes hálózat védtelen az illetéktelen behatolóktól. Az eszközgyártók 2005 óta alapbeállítással ellátják eszközeiket, melynek adatai bárki számára hozzáférhetők az interneten. A kutatásból az is kiderül, hogy a válaszadók 37%-a csak ezt az alapbeállítást használja. A megkérdezetteknek 17%-a nyilatkozott arról, hogy a megfelelő beállításokat, jelszócseréket elvégezte eszközein. Sajnos 47%-uk nem tartja fontosnak ezt a lépést. Ez mutatja a *4. diagram*.

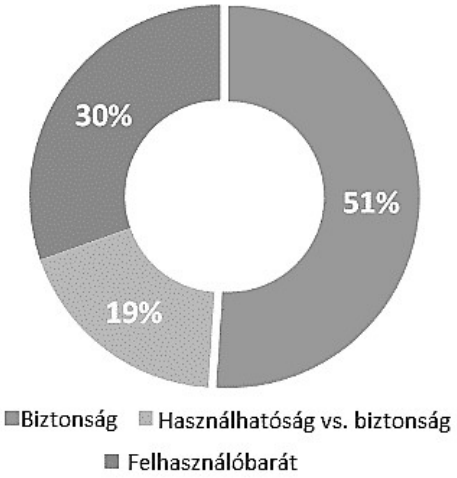
A kutatás másik kérdésköre arra irányul, hogy a felhasználók mit tartanak fontosabbnak az okos otthonuk biztonságát, meghatározott kötöttségekkel, vagy a felhasználóbarát esetleg bárki számára hozzáférhető rendszert. Az eredmények meglepték a kutatókat. A válaszadók 51%-a a teljes biztonságot választotta kötöttségekkel, 19%-uk nem akar kompromisszumokat, míg 30%-uk nyilatkozta, hogy a felhasználóbarát rendszert választja. Ez persze azzal jár, hogy Ő mint felhasználó teljes mértékben elfogadja a rendszerének alapbeállításait és paramétereit. Ezt mutatja az *5. diagram*.

A kérdések utolsó sorozata a fogyasztók biztonságára és az okos otthon eszközei árának viszonyára kérdezett rá. A válaszokból az derült ki, hogy a fogyasztók 42%-a fizetne a biztonságosabb eszközökért, 32%-át elgondolkodtatta a kérdés, míg 26%-a nem aggódik az eszközök, berendezések biztonsága miatt.

4. diagram: A vezeték nélküli eszközök biztonsági beállítása



5. diagram: Biztonság vs. felhasználóbarát



Forrás: https://prplfoundation.org/

A kutatás azt is megmutatta, hogy a felhasználók nagyobb számban vásárolnának intelligens eszközöket otthonaikban, ha a gyártók biztosítani tudják őket az eszközök megfelelő biztonságáról.

3. Okos otthonok eszközei Magyarországon

Napjainkra az okos városok és okos otthonok a kényelmünket szolgálják. Magyarországon is számos nagyvárosi fejlesztés indult el abba az irányba, hogy városainkat élhetőbbé tegyük. Ezek a fejlesztések mind annak a tükrében zajlanak, hogy statisztikai adatokkal bizonyítható, hogy a városok lakossága az elmúlt évtizedekben egyre emelkedett. Az okos városok koncepciójából itthon sem hiányozhatnak az okos otthonok, melyek száma rohamosan nő. Ez azért van, mert a városlakók életkora is változik. Fiatalodnak a városok. A fiatalok pedig egyre jobban függenek a digitalizációtól, mely begyűrűzik egészen az otthonukig. Szakértők arra figyelmeztetnek, hogy a digitalizációval sajnos együtt ját a kiberbűnözés elterjedése is. Az már ismert, hogy egyes gyártók okos otthon eszközei rejtenek magukban kockázatot. Ez elsősorban érinti a bluetooth és a WLAN kapcsolattal rendelkező eszközök egy részét. Ezen eszközök sebezhetőségét a gyártók egy része javította és publikálta. Sajnos még előfordulhat, hogy egyes gyártók eszközei biztonsági hibákat rejtenek magukban. Egy hazai biztonsági kutató szerint jelenleg a legnagyobb problémát az jelenti, hogy a felhasználók a legolcsóbb termékeket vásárolják meg, amelyek nem rendelkeznek megfelelő biztonsági megoldásokkal. Ezekhez az eszközökhöz legtöbbször nem biztosított a folyamatos frissítés, és még az is lehetséges, hogy az internetre felcsatlakoztatott eszköz felhasználói kontroll nélkül frissíti saját belső programját. Ezzel általában az a céljuk a gyártóknak, hogy a felhasználókról minél több információt tudjanak meg.

4. Konklúzió

Az okos otthonok eszközeinek elterjedése megállíthatatlan. Ezt kihasználják a fejlesztők és a gyártók is. A PRPL kutatásából kiderül, hogy az eszközök darabszáma növekszik. Sajnos a felhasználók egy része nincs tisztában a megfelelő biztonsági beállításokkal, de kész fizetni egy biztonságosabb termékért.

Az okoseszközök kényelmesebbé teszik a mindennapjainkat, de felhasználói szinten is tudatosabban kell kiválasztani és használni azokat, hogy ne érjenek bennünket kellemetlen meglepetések. Ezt szükséges megtenni otthonunk biztonsága, privát szféránk és adataink érdekében.

Felhasznált irodalom

5 steps to keep your smart home from being hacked, Online: https://www.pcworld.com/article/2925056/5-steps-to-keep-your-smart-home-from-being-hacked.html, Adatok letöltve: 2017. 10. 10.

A tévéjelen keresztül is feltörhetők az okostévék, Online: https://sg.hu/cikkek/it-tech/124602/a-tevejelen-keresztul-is-feltorhetok-az-okostevek, Adatok letöltve: 2017. 10. 10.

Funkstandards im Smart Home, Online: http://www.smart-home.one/funkstandards-im-smart-home-warum-nicht-wlan-und-bluetooth-20162, Adatok letöltve: 2017. 10. 10.

Haig Zsolt: „Információ-társadalom-biztonság", NKE Szolgáltató Kft, Budapest, 2015.

Lazányi Kornélia: Innovation – the role of trust, SERBIAN JOURNAL OF MANAGEMENT, 2017.

Market size of the global smart home market from 2013 to 2025, Online: https://www.statista.com/statistics/562298/smart-home-market-by-region/, Adatok letöltve: 2017. 10. 10.

Mert nem lehetünk mindig jelen… Online: http://vezerlemahazam.blog.hu/2017/10/17/mert_nem_lehetunk_mindig_jelen, Adatok letöltve: 2017. 10. 10.

Minden, amit az okosotthonról tudni kell, Online: http://www.intelligensotthon-tudastar.hu/ Adatok letöltve: 2017. 10. 10., Smart Home Security Report 2016, Online: https://prplfoundation.org/, Adatok letöltve: 2017. 10. 10.

Okos otthon, Intelligens otthon, épületautomatizálás, Online: https://www.smarthomecenter.hu/, Adatok letöltve: 2017. 10. 10.

Okosváros, okosotthon, Online: http://uni-nke.hu/hirek/2017/10/17/okosvaros_-okosotthon, Adatok letöltve: 2017. 10. 10.

Smart City Infographic, Online: https://www.postscapes.com/anatomy-of-a-smart-city/, Adatok letöltve: 2017. 10. 10.

Smart Home Market by Product, Online: http://www.marketsandmarkets.com/Market-Reports/smart-homes-and-assisted-living-advanced-technologie-and-global-market-121.html Adatok letöltve: 2017. 10. 10.

Smart home market size – Trends and projections, Online: http://www.ironpaper.com/webintel/articles/smart-home-market-size-trends-projections/, Adatok letöltve: 2017. 10. 10.

Smart Home, Online: https://www.itead.cc/smart-home.html, Adatok letöltve: 2017. 10. 10.