International Journal of Engineering and Management Sciences (IJEMS) Vol. 4. (2019). No. 4
DOI: 10.21791/IJEMS.2019.4.8.

Intelligens ingatlanok integrált védelme, kockázatainak elemzése
Security and Risk management of Intelligent Integrated Institutes

B. KOVÁCS[1], J. TÓTH[2]

[1]Debreceni Egyetem, Műszaki Kar, Mechatronikai Tanszék, kovacs.bence0730@gmail.com
[2]Debreceni Egyetem, Műszaki Kar, Mechatronikai Tanszék, tothjanos@eng.unideb.hu

Absztrakt. Egyre nagyobb teret hódítanak az okos technológiákkal párhuzamosan elterjedő intelligens háztartások is. Ez minden előnyeivel együtt magával hordozza az információs technológia veszélyeit is. Ezekkel a veszélyekkel számolni kell. Meg kell határozni a hatásukat és megfelelő védelmi intézkedéseket kell alkalmazni azokkal szemben. A hatékony védelem eléréséhez nyújt iránymutatást ez a publikáció.

Abstract. The intelligent households are getting more and more popular beside the intelligent technologies. With all the advantages that this can provide, it brings the security risk of the information technology as well. We must deal with those dangers. We have to determine the risks so that we can make proper precautions. This article gives an effective guideline to achieve safety.

Bevezetés

A kiberbiztonság napjaink egyik leggyorsabban fejlődő területe, mely számtalan kihívást hordoz magával a technológiák fejlődésének, modernizálásának következtében. A közösségi hálók, felhő alapú szolgáltatások, mobil eszközök és a dolgok internete egyre jobban részesei mindennapi életünknek. Manapság nem csak a telefonunk, óránk és más elektronikai eszközeink lehetnek okosak, hanem komplex háztartásunk is. Ezen technológia előnye a tulajdonosok kényelmének fokozása, azonban az „intelligens" technológia nem megfelelő alkalmazása komoly veszélyeket hordoz magával a felhasználókra nézve. A kibertérhez történő kapcsolódással járó veszélyeket azonosítani szükséges, hogy megfelelő intézkedéseket hozhassunk ellenük, ezzel lehetőséget biztosítva azok minimalizálására vagy megszűntetésére.

Az ipari (és hadászati) információs technológiának már a legelső hálózatok kialakulása után rövidesen részese lett a kibervédelem, mely számtalan védelmi megoldást biztosít a jelentkező fenyegetésekre. Elterjedő félben lévő intelligens ingatlanjaink terén azonban hiány a teljes körű információs technológiai védelem biztosítása. A tulajdonosok nagy veszélynek lehetnek kitéve, annak ellenére is, hogy a védelem egy-egy részegysége megvalósul. Ez a publikáció számba veszi az Internet és a

DOI: 10.21791/IJEMS.2019.4.8.

széleskörűen összekapcsolt hálózatok által nyújtott veszélyforrásokat, amelyek érinthetik okos otthonainkat. Az iparban is jól bevált kibervédelmi irányelveknek az alkalmazására és annak szükségességére hívja fel a figyelmet.

Először meghatározásra kerül, hogy milyen feltételeknek kell teljesülnie az adatainknak a hálózatunkon belüli védelméhez, ezt követően szó lesz a tudatos felhasználói magatartás szükségességéről, valamit azokról a fenyegetésekről, amikor a rendszerünk titkosítása megvalósul, de mégis használhatatlanná válik egy-egy támadás esetén a felhasználók számára.

1. ábra - Intelligens otthon irányítási lehetőségei. [1]

1. Hogyan érhető el a biztonság intelligens ingatlanunkban?

Intelligens ingatlanunk egy kiépített belső informatikai hálózat segítségével valósulhat meg, amely egy központi vezérlőegység által biztosít lehetőséget az épület különböző okos funkcióinak létrejöveteléhez. Ezen hálózaton belül biztosítani kell egy védett folyamatot, amely során a gyűjtött számítógépes adatok, valamint a számítógép által megvalósított irányítási folyamatok megfelelnek az International Standards Organization (ISO) által definiált bizalmasság (confidentiality), sértetlenség (integrity) és rendelkezésre állás (availability) feltételeinek. Fontos, hogy a rendszerünk működése folyamán a felhasználni kívánt információ bizalmasan, titkosított formában legyen tárolva, sértetlenül, teljes egészében, azonban, ha szükségünk van rá, akkor hozzáférhető legyen, és korlátozás nélkül rendelkezésünkre álljon [2].

2. ábra - ISO által definiált védett folyamat elemei. [3]

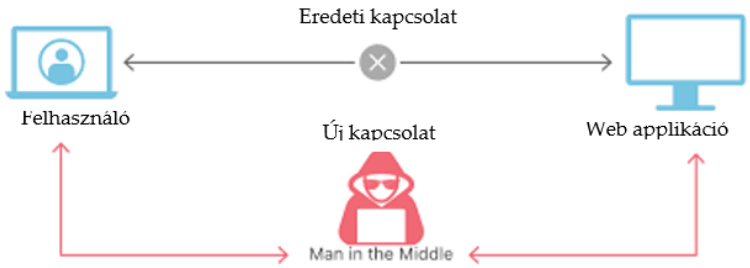
Napjainkra hálózataink határa elmosódik. Míg a 2000-es évekig helyi hálózatunk egyértelműen elválasztható volt a világhálótól vezetékes kiépítésének köszönhetően, addigra manapság egyre jobban elterjedő félben van a dolgok internete (Internet of Things – IoT) és a szenzorhálózatok vezeték nélküli adattovábbítása. Intelligens eszközeink kommunikációs technológiájában háttérbe szorulni látszik a

DOI: 10.21791/IJEMS.2019.4.8.

csavart érpár vagy optikai kábel, helyette a rádiófrekvencia használata dominál. Ebben az esetben a rádióhullámok által történik értékes adataink és irányítási folyamataink továbbítása, így bárki számára észlelhetők vagy befoghatók. Ennek következtében szükséges megfelelő szintű titkosítási protokollok alkalmazása, melyek gondoskodnak az információ biztonságos közléséről nyilvánosan elérhető adatátviteli csatornákon keresztül.

Ahhoz, hogy egy intelligens ingatlan informatikai rendszere védett legyen, nem csak a hálózatot alkotó számítógépeket, laptopokat, mobil eszközöket és hálózati forgalomirányítókat, kapcsolókat kell fizikailag védenünk attól, hogy ellenséges szándékú személyek tulajdonába kerüljenek. Gondoskodnunk kell az eszközeinken futó beágyazott-, és operációs rendszerek, valamint firmwarek korszerű védelméről, biztonságáról is. Ezt tűzfalak, vírusírtók, megfelelő szintű titkosítási protokollok, hozzáférhetőség korlátozás (access control), hálózati biztonságtechnológia (network security) és rendszermonitorozás alkalmazásával érhetjük el. Ha biztosítjuk, hogy a fizikai eszközeink, hardverjeink ne kerülhessenek illetéktelen kezekbe és a korábban említett elvek és metódusok alkalmazásra kerülnek, akkor a kibertéren keresztül is kellő mértékű védelemmel rendelkezhet hálózatunk [4].

A támadási módszerek fejlődése folyamán újabb kihívásokkal kellett felvenni a harcot. Ezen támadások esetén gyakran megfigyelés és lehallgatás útján sikeresen álcázzák magukat a támadók jogosultságokkal rendelkező klienseknek, így a szolgáltatásokat nyújtó fél nem feltétlen tapasztal rendellenességet a rendszerében, ami ellen fel kellene lépnie, hiszen nem minden esetben a sértettek ellehetetlenítése és működésképtelenné tétele a támadó célja, hanem inkább bizalmas információk megszerzése vagy hamis információk közlése. Ilyen esetekben nem a szolgáltatás megtagadás elleni védelem, hanem a szolgáltatáson belüli, kliens oldali támadás feltárása a hatékony védekezési eljárás. Ennek érdekében ki kell egészíteni az ISO szabvány által definiált bizalmasság, sértetlenség és hozzáférhetőség biztonsági elveit hitelesítési (authentikáció), felelősségre vonhatósági, visszajátszhatóság nélküliségi és megbízhatósági irányelvekkel is, hogy a lehallgatások és megfigyelések ellen is kellőképpen védett legyen otthonunk.



3. ábra - Megfigyelésen és lehallgatáson alapuló támadási forma. [5]

2. Emberi tényező szerepe intelligens rendszerünk biztonságában

Abban az esetben, ha az előző fejezetben felsorolt védelmet biztosítjuk rendszerünk számára, a hálózatunk továbbra is sebezhető maradhat, ugyanis intelligens rendszereink nem csak szoftveres hibák vagy operációs rendszerek frissítéseinek elmaradása miatt lehetnek sebezhetők, hanem az

DOI: 10.21791/IJEMS.2019.4.8.

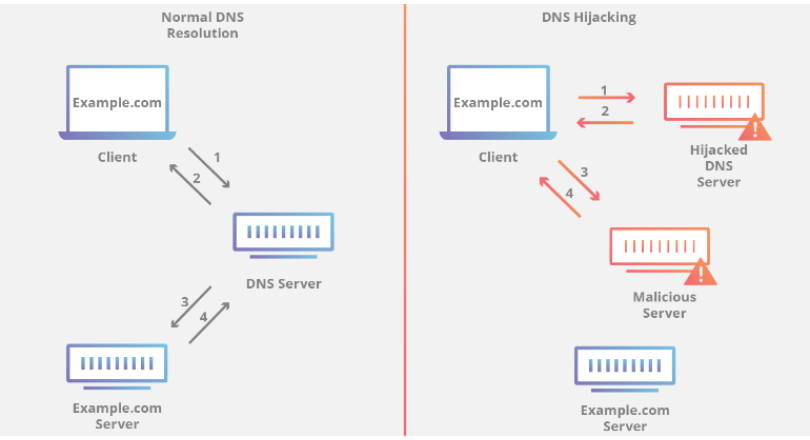
emberi tényezők következtében is. Az információs technológia biztonságát nem lehet egyszerűen csak technikai megoldásokkal megvalósítani, szükséges hozzá a tudatos felhasználói magatartás is.

A Verizon adatelemző cég által készített 2018-as riport alapján adott évben a biztonsági rendszerek feltöréséért 81%-ban eltulajdonított vagy gyenge felhasználói jelszavak felelősek. Továbbá, ha megfelelő jelszót választ magának egy-egy felhasználó, így is több, mint 70%-uk egy jelszót használ több felületen is, míg 59%-uk mindenütt ugyan azt használja. Ilyen esetben elegendő egy rendszer gyengeségéből eredően megszerezni egy jelszót, onnantól kezdve a hozzáférés biztosított a megfelelő kibervédelemmel ellátott hálózatokhoz is [6].

4. ábra - A sikeres kibertámadások 95%-ának okozója emberi mulasztás. [7]

Egy rendszer emberi gyengeségeiből adódó sebezhetőségeit kihasználó támadások a megtévesztésen alapuló támadások is. Tipikus példa, amikor a felhasználók email elérhetőségét megszerezve, hitelesnek tűnő üzenetet küldenek a támadók az elektronikus postafiók tulajdonosának egy-egy igénybe vett szolgáltatás nyújtójának nevében (például áram-, vagy hőszolgáltató), melyben egy „fontos ügy" elintézése érdekében kérik őket, hogy adják meg érzékeny adataikat, mint például a felhasználói nevüket vagy jelszavukat. Ezt ki lehet védeni tudatos internetes magatartással, ugyanis bevett gyakorlat, hogy a szolgáltatók tájékoztatják vásárlóikat, hogy sosem kérnek jelszavakat emailen keresztül, így a felhasználó gyanút foghat minden olyan kérésre, amely erre irányul. Ennél nehezebb kivédeni azokat a támadásokat, amelyeknél a támadók létrehoznak egy, a szolgáltatás nyújtójának weboldalával megtévesztésig hasonló weboldalt. Erre irányítva a felhasználókat, tudtukon és hozzájárulásukon kívül adják meg gyanútlanul a bizalmas adataikat. Ilyenkor nincs szükség a felhasználók közreműködésére, elegendő egy eltérített tartománynévrendszer (Domain Name System – DNS), amely átirányítja a felhasználókat a támadók weboldalára, ott megadja felhasználói nevét és jelszavát a támadóknak, majd ők visszatérítik az eredeti weboldalra, ahol tovább tudja intézni a felhasználó az ügyeit, anélkül, hogy az adatszivárgásról tudomása lenne [8].

DOI: 10.21791/IJEMS.2019.4.8.



5. ábra - Eltérített DNS szerver általi támadás. [9]

Ezek ellen a leghatékonyabb védekezési eljárás az adminisztrációs folyamatok, korlátozó szabályozások és más, technikai megoldásokon alapuló metódusok alkalmazása.

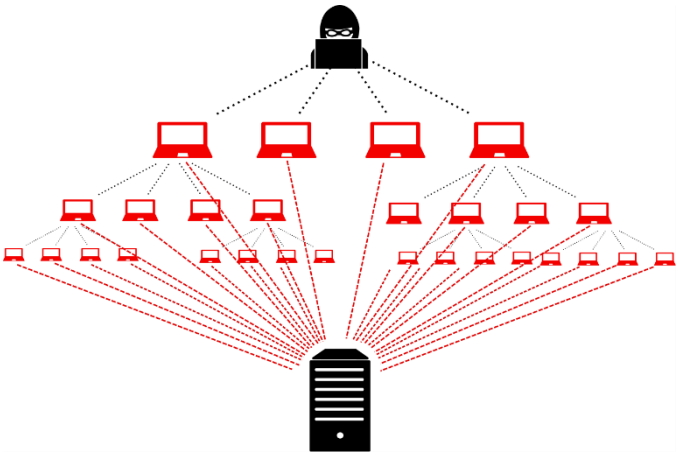
3. Informatikai rendszerek feltörés nélküli károsítása

Ahogy a technológia folyamatosan fejlődik, ezzel együtt fejlődnek a támadási eljárások is.

Az internetes támadások legrégibb, és ezzel együtt legkezdetlegesebb formája a vírus és féregprogramok általi megfertőződés, valamint a hálózatok nem megfelelő konfigurációjából eredő hibák és nyílt hozzáférhetőségek. Ezek ellen a kezdetek óta tűzfalakkal, antivírus programokkal, rendszeres frissítésekkel, valamint a hálózatok kiépítésénél alkalmazott megfelelő biztonsági protokollok alkalmazásával lehet védekezni. Amíg csak ezek a veszélyforrások fenyegették a felhasználókat, elegendő volt a hálózatuk sebezhetőségének monitorozása és védekezés a rendellenes működés ellen.

Napjainkra egyre több szolgáltatás és irányítási folyamat elérhető az interneten keresztül. Ez a támadások egy újabb formáját hozta létre, melynél nem az értékes adatok és információ megszerzése a cél, hanem a támadás a szolgáltatás megtagadások elérésére irányul. Ilyen esetben nem szükséges a megtámadni kívánt hálózat biztonsági protokolljainak feltörése, sőt, sok esetben ez nem is igazán kivitelezhető. Ehelyett a rendszer erőforrásai, számítási kapacitásai ellen történik a támadás. A támadó lekérdezést indít a célpont szerverei felé. Mivel nincs jogosultsága, így a szerver elutasítja kérését. Amennyiben a támadási folyamat ennyiből állna, a támadást sikertelennek lehetne nevezni, azonban ez a szolgáltatás kérés a szerverek felé másodpercenként több százszor történik meg. Annak ellenére, hogy a támadó nem jut át a védelmen, a hálózatunk erőforrásait lefoglalhatja. Ha csak egy számítógépről történik a lekérdezések indítása, akkor lehetőség van annak a letiltására, azonban egy profi rosszakaró „zombi hálózatot", azaz megfertőzött számítógépek sokaságát alkalmazza a támadásra (Distributer Denial of Service – DDoS), így nagyon nehéz kiszűrni, hogy mely szolgáltatás kérés érkezik valós ügyféltől, mely pedig nem. Az erőforrás lefoglalás pedig elérhetetlenné teszi a jogosultságokkal rendelkezők számára is a hálózat elérését.

DOI: 10.21791/IJEMS.2019.4.8.



6. ábra – „zombi hálózat" általi támadás illusztrációja. [9]

Erre a legnagyobb vállalatok is nehezen tudnak reagálni. Jó példa 2014. karácsonya, amikor hackerek egy csoportja DDoS támadással ellehetetlenítette a Microsoft és a Sony konzol szolgáltatását, ezzel közel 160 millió játékost fosztva meg az online játszás lehetőségétől, jelentős károkat okozva a cégeknek és a felhasználóknak egyaránt [10].

4. Sikeres támadás következményeinek hatása

A biztonsággal kapcsolatos veszélyforrások jobban fejlődnek, mintsem az ellenük fejlesztett védelmi technológiák. Ennek következtében elkerülhetetlen informatikai rendszereink sebezhetősége. Bármilyen nagy erőfeszítést is teszünk, sosem lehet azt kimondani, hogy rendszereink tökéletesek és sebezhetetlenek. Az adatvesztéssel vagy adatlopással mindig is számolnunk kell. Ahhoz, hogy minimalizálni tudjuk veszteségeinket és fenyegetettségünket ilyen esetek bekövetkeztekor, az alábbi kettő védelmi megoldás is számításba vehető kiegészítésként, a publikációban felsorolt további követelmény mellett:

- Helyreállíthatóság: Ahhoz, hogy rugalmasan tudjunk kezelni egy sikeres kibertámadást, szükséges adataink helyreállíthatósága. Bármilyen sérelem esetén, amennyiben rendelkezünk biztonsági mentéssel, úgy visszaállíthatjuk rendszerünk állapotát a sérülést megelőző állapotra. Erre lehetőség van lokális vagy felhő alapú biztonsági mentés alkalmazásával is.

7. ábra - Lokális és felhő alapú biztonsági mentés illusztrációja. [11]

DOI: 10.21791/IJEMS.2019.4.8.

- Gyors fejlődés: Megfelelő erőforrást (időt, energiát és pénzt) kell fordítani a technológia fejlődésével járó újítások megismerésére és alkalmazására, melyek fel tudják venni a gyorsuló ütemben fejlődő támadási lehetőségekkel a versenyt. Ilyen technológia például a blockchain, mesterséges intelligencia, gépi tanulás és deep learning is.

5. Intelligens ingatlanok veszélyforrásainak azonosítása

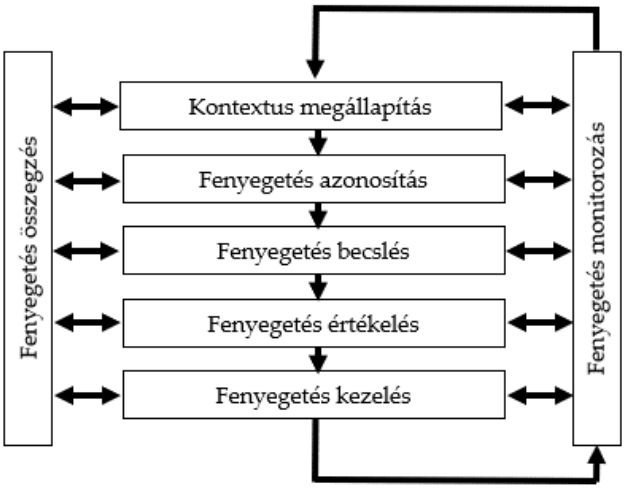
Ahogyan azt a korábbi fejezetekben is olvashattuk, számos veszély fenyegeti informatikai hálózatunkat. Ezek ellen lehet alkalmazni különböző védelmi megoldásokat, de ettől függetlenül lehetetlen elérni egy sebezhetetlen állapotot.

Intelligens ingatlanjaink esetében számos fenyegetés megegyezik egy általános hálózatban tapasztalható fenyegetéssel, azonban bizonyos területeken lényeges eltérések is tapasztalhatók. Ahhoz, hogy képesek legyünk teljeskörűen felmérni az értékeinket fenyegető veszélyeket, és megfelelő intézkedéseket tehessünk ellenük, segítségünkre szolgál az amerikai National Institute of Standards and Technology (NIST) rizikó menedzsment keretrendszere (Risk Management Framework – RMF) által 9 lépésben meghatározott eljárás:

1. Rendszer jellemzés.
2. Fenyegetés azonosítás.
3. Sebezhetőség azonosítás.
4. Irányítási analízis.
5. Valószínűség meghatározás.
6. Hatás vizsgálat.
7. Fenyegetés meghatározása.
8. Irányítási javaslatok.
9. Eredmények dokumentálása.

A Nemzetközi Szabványügyi Szervezet (ISO) és a Nemzetközi Elektronikai Bizottság (International Electrotechnical Commission – IEC) közösen megalkotott információbiztonság-irányítás szabványai, az ISO 17799 és az ISO 27000 is hasonló elveket határoz meg a veszélyekre való felkészülésre.

DOI: 10.21791/IJEMS.2019.4.8.



8. ábra - ISO 27005:2008 fenyegetettség felmérés és kezelés.

Habár az iparban már meghatározásra került a legtöbb fenyegetést jelentő kockázat, ez a most kialakuló intelligens háztartásokról nem mondható el. Igaz, hogy a fenyegetések számottevő része megegyezik, ugyanis a háztartásokban is kiépített informatikai hálózatban végzett irányítási folyamatokkal dolgozunk, azonban a háztartások sajátossága egyedi támadási lehetőségeket rejt. Jelenleg hiába áll rendelkezésünkre a NIST, valamint az ISO által nyújtott fenyegetettség meghatározására alkalmazható irányelvei, ez nem került még alkalmazásra a háztartási szektorral kapcsolatosan. Az alapvető meghatározás nélkül nehéz azonosítani a tényleges fenyegetéseket és teljeskörű intézkedéseket hozni ellenük. Nem elfogadható, hogyha a nem megfelelő veszélyek elhárítására pazaroljuk energiánkat, erőforrásainkat.

A legfontosabb kérdés az, hogy mi a valószínűsége annak, hogy egy támadás sikeresen megvalósul, valamint az, hogy mennyi minden és mi az, ami fenyegetve lenne ebben az esetben. Ugyanis előfordulhatnak olyan esetek, amikor a fenyegetettség igen nagy, azonban a veszély, amit magával hordoz a támadás, jelentéktelen. Ha az, ami irányában a támadás megvalósul, értéktelen, akkor a jelentős sebezhetőség fennállása mellett sem lehet veszélynek nevezni a kialakuló helyzetet. Nem mindegy, hogy egy feltört intelligens otthon esetén a támadó a világítás felett tudja átvenni az irányítást, vagy pedig egy intelligens sütő felett. Pár évvel ezelőtt egy intelligens otthon vezérelt világítással, légkondicionálóssal és okos zárakkal rendelkezett. A piacon nagy kereslet volt a termékek iránt, így minden háztartási eszköz gyártója elkezdte kifejleszteni a saját intelligens eszközét. Manapság már a redőnyvezérléstől kezdve, a robotporszívókon át, egészen az intelligens mosógépekig, sütőkig és egyéb nagyobb háztartási berendezésekig terjed az intelligens eszközök sora. A biztonságtechnika terén is megjelentek az intelligens kamerák is, mely aggodalomra adhat okot, ha még csak azonosításra sem kerültek a kockázatok, melyek fenyegethetik a lakók életét.

Meg kell határozni a kockázatot. A kockázat a fenyegetés, sebezhetőség, és magából az megszerzendő, megtámadandó érték hármas alkotóeleméből áll. Mindhárom tényezőnek jelen kell lennie, hogy egy kockázat előálljon. Szükséges léteznie annak az értéknek (legyen az fizikai, vagy eszmei), amelyre egy esetleges támadás irányulhat. Szükséges fenyegető személy vagy szervezet, amelynek érdekében áll megszerezni vagy megkárosítani a szóban forgó értéket. Továbbá annak az értéknek lennie kell

DOI: 10.21791/IJEMS.2019.4.8.

sebezhető pontjának, gyengeségének, melyet kihasználva megtörténhet az eltulajdonítás, károsítás. Ha ezen hármasság közül bármelyik nem áll fenn, akkor az nem jelent kockázatot háztartásunk számára.

Kockázat = Fenyegetés + Sebezhetőség + Érték

Miután meghatároztuk a kockázat tényét, fontos, hogy az összes létezőt számba vegyük és rangsoroljuk azokat. A rangsor felállításához először is meg kell vizsgálni a sikeres támadás előfordulási esélyét, majd annak károsító hatását. Egy-egy fenyegetés nem ugyan olyan valószínűséggel következhet be. Egy betörés folyamán egy rosszakarónak kevésbé célpontja a légkondicionáló rendszer felett átvenni az irányítást, mintsem az intelligens zárak felett. A két eszközzel kapcsolatosan más a támadás valószínűsége. Ugyanakkor a támadás elért hatása is különböző. Ezen tényezők megállapítása után rangsorolni lehet a kockázatokat és a fenyegetésük jelentőségét [12].

		Hatás		
		alacsony	közepes	magas
Előfordulás	magas	közepes	magas	magas
	közepes	alacsony	közepes	magas
	alacsony	alacsony	alacsony	közepes

1. táblázat - Kockázatok rangsorolása hatás-előfordulás szempontok alapján

Azokkal a fenyegetésekkel szemben, melyek megengedhetetlen kockázatot vonnak maguk után, fel kell lépni és intézkedéseket kell hozni.

Az 1. táblázat szempontrendszere alapján érdemes az okos otthonokban előfordulható legtöbb eszköz rangsorolása. Ezt a rangsort folyamatosan frissíteni szükséges, ugyanis újabb és újabb termékek jelennek meg a piacon, melyeket a felhasználók megvásárolhatnak és háztartásukban alkalmazhatnak. A kockázatok felmérése és óvintézkedések nélkül komoly veszélyt jelenthet a kényelem és a felhasználói élmény fokozása érdekében létrehozott ingatlan saját a felhasználóira. Például egy nem megfelelő eljárás során kiépített intelligens kamerarendszer könnyedén szivárogtathat érzékeny információkat a lakókról, akaratukon kívül. Az intelligens zárak alkalmazása is számos előnnyel járhat, de a nem megfelelő eszközök kiválasztása nagyobb veszélyt hordoz magával, mintsem amilyen előnyt nyújt. Kényelmes lehet telefonos applikáción keresztül vezérelni zárjainkat, vagy ellenőrizni állapotukat. Amennyiben elfelejtjük, hogy bezártuk-e ajtónkat távozásunk során, elég csak telefonos alkalmazásunkkal leellenőrizni azok állapotát, hogy meggyőződjünk helyzetükről, nem kell visszatérnünk ingatlanunkhoz. Azonban az Interneten keresztül elérhetők eszközeink, nem megfelelő védelmi módszerek alkalmazásából eredő feltörés esetén teljes fizikai hozzáférhetőséget biztosítanak értékeinkhez a rablók számára. Egy-egy zár nem megfelelő kivitelezése is további gondot jelenthet. Számos olyan intelligens zár érhető el, melynek tápellátása elemről biztosított. Ezek lemerülésük esetén, a teljes lemerülés előtt hangjelzéssel jeleznek a felhasználónak, hogy elemcsere szükséges. Amennyiben ez nem következik be, a zárak végső lemerülésük előtt kinyílnak, hogy ne ejtsék csapdába a lakókat, azonban ezzel szabad bejárást is biztosítanak!

DOI: 10.21791/IJEMS.2019.4.8.

9. ábra - Elem tápellátású intelligens zár. [13]

6. Konklúzió

Az intelligens háztartások elterjedésével a hétköznapi emberek életére is jelentősen hatással lehet az információs technológia használatával együtt járó veszélyek. Bár számos kockázatra létezik védelmi megoldás, az intelligens ingatlanok egyedi jellegzetességéből adódóan egy teljes kockázatelemzést szükséges végezni. Erre több módszer és metódus is létezik, melyeket már hatásosan alkalmazott az ipar, azonban a háztartásra való alkalmazása hiányzik. A kockázatok meghatározása, valamint azok rangsorolása is hiányzik. Ezáltal kifejezetten nehéz kellő színvonalú védelmet biztosítani a tulajdonosok számára, miközben értékeik, vagyonuk és érzékeny információik vannak veszélyben. Legszélsőségesebb esetekben egy hanyag információs védelemmel ellátott intelligens ingatlan képes olyan kényelmi funkciókat nyújtani a tulajdonosok számára, amelyet egy hétköznapi otthon nem, azonban ez a kényelem akár az életük veszélyeztetésével is járhat. Ahhoz, hogy kellő mértékben fel lehessen készülni a megfelelő fenyegetések ellen, fenyegetettség elemzését és a kockázatok rangsorolását pótolni szükséges. A védelem nem csak az informatikai rendszerünkbe történő behatolások, lehallgatások és megfigyelések elleni védelmet jelenti, hanem magába foglalja a tudatos felhasználói magatartást is. Ugyanakkor, mint minden informatikai hálózat esetén, a teljes védelem sosem lesz biztosított. A publikációban említett módszerek alkalmazása mellett, melyek a védelem maximalizálását szolgálják, szükséges felkészülni azokra az esetekre, amikor egy-egy jogosulatlan hozzáférés megkárosítja a rendszerünket. Ha felkészülten ér bennünket az eset, akkor egy-egy biztonsági mentés visszatöltésével könnyedén és gyorsan elháríthatjuk a fenyegetettséget és minimalizálhatjuk a károkat. Csak megfelelő elemzések megvalósulása és alkalmazása után tudjuk csak garantálni okos otthonaink maximális biztonságát.

DOI: 10.21791/IJEMS.2019.4.8.

Hivatkozások

[1] https://makeradvisor.com/smart-home-on-a-budget/
letöltve: 2018.11.15.

[2] ISO/IEC 27032 Information Technology – Security Techniques – Guidelines for Cybersecurity, letöltve: 2018.11.15. https://www.iso27001security.com/html/27032.html

[3] https://sealog.hu/hirek/53-mi-az-igazi-segitseg-audit-tobb-kell-ez-meg-nem-eleg
letöltve: 2018.11.15.

[4] R. Ottis, P. Lorents, Cyberspace: Definition and implications, ICIW, 267-270. 2010.

[5] https://www.cloudflare.com/learning/security/threats/man-in-the-middle-attack/
letöltve: 2018.11.16.

[6] Verizon – 2018 Data Breach Investigations Report, 11th edition. 2018.

[7] https://www.netpresenter.com/blog/cybersecurity-human-firewall/
letöltve: 2018.11.16.

[8] Guide for Conducting Risk Assessments, National Institute of Standards and Technology, NIST Special Publication 800-30, 2012.

[9] https://www.cloudflare.com/learning/security/threats/man-in-the-middle-attack/
letöltve: 2018.11.16.

[10] Internetes forrás: https://www.theguardian.com/technology/2014/dec/26/xbox-live-and-psn-attack-christmas-ruined-for-millions-of-gamers

[11] https://www.integranets.com/data-backup-recovery/
letöltve: 2018.11.20.

[12] J. Freaund, J. Jones, Measuring and Managing Information Risk: A FAIR Approach, ISBN-13:978-0124202313, 2014.

[13] https://www.amazon.com/August-Smart-Connect-Satin-Nickel/dp/B07H43TNNF
letöltve: 2018.11.20.