ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

SÁNDOR BARNABÁS

Okos épületek kiberbiztonsági intézkedéseinek vizsgálata

Témavezető: Prof. Dr. Rajnai Zoltán

**BIZTONSÁGTUDOMÁNYI
DOKTORI ISKOLA**

Budapest, 2024. március 11.

Szigorlati/komplex vizsga bizottság:

Elnök:

Prof. Dr. Rajnai Zoltán

Tagok:

Dr. Muha Lajos

Dr. Számadó Róza Zsuzsánna

Nyilvános védés teljes bizottsága:

Elnök:

Prof. Em. Dr. Berek Lajos

Titkár:

Bakosné Dr. Diószegi Mónika

Tagok:

Dr. Gogolák László

Prof. Dr. Michelberger Pál

Dr. habil. Szádeczky Tamás

Bírálók:

Dr. Jobbágy Szabolcs

Prof. Dr. Zlatko Čović

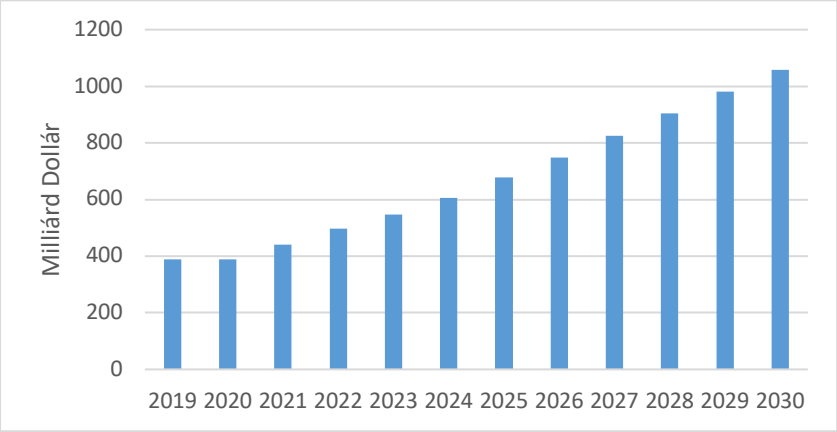
Nyilvános védés időpontja:

2024.

TARTALOMJEGYZÉK

BEVEZETÉS

A dolgok internetének (Internet of Things - IoT) elterjedése az elmúlt években megváltoztatta életmódunkat és a környezettel való interakciónkat. Az IoT iparban 2019 és 2023 között közel 41%-os növekedést volt mérhető a piacon, amely a termékekre és szolgáltatásokra érthető. (1. ábra)



1. ábra: IoT piac globális bevétele 2019 és 2030 között *[1]*

Az egyik ilyen átalakulás az épületek okos terekké alakítása és automatizálása volt, ahol az érzékelők és okos eszközök segítségével történő adatgyűjtés értékes információkkal szolgál az energiahatékonyság, a munkavállalók komfortérzetének, hatékonyságának és az épület általános teljesítményének javításhoz. Azonban ez a fokozott összekapcsolhatóság és információmegosztás kiberbiztonsági kockázatot hordoz magában, amelyet nem lehet figyelmen kívül hagyni. Más IoT-rendszerekhez hasonlóan az okos épületek is ki vannak téve olyan kiberfenyegetéseknek, amelyek veszélyeztethetik a munkavállalók magánszféráját vagy fizikai biztonságát, illetve károsíthatják a berendezéseket és ezáltal megzavarhatják a vállalat működését. Ezért egyre fontosabbá válik, hogy hatékony kiberbiztonsági intézkedéseket hozzunk az okos épületek biztonságos működésének biztosítása érdekében.

Értekezésem bevezetőjében áttekintést kívánok nyújtani arról, hogy az IoT hogyan alakította át az épületeket különböző célú adatgyűjtést alkalmazó okos terekké. Fontos kiemelnem, hogy ezek a fejlesztések tudományos aggályokat vetnek fel a biztonsági kérdésekkel kapcsolatban. Az okos eszközök és rendszerek potenciális sebezhetősége komoly veszélyt jelent a munkavállalók biztonságára és magánéletére, miközben a kibertámadások által okozott berendezések károsodása miatt működési zavarok felléphetnek. Ezért szükség van olyan mélyreható kutatásra, amely célja olyan átfogó

megoldások nyújtása, amelyek hatékonyan csökkentik az IoT-alapú okos épületekhez kapcsolódó biztonsági kockázatokat. Ugyanakkor kiemelném az okos épületekben a megnövekedett összekapcsolhatóság és adatmegosztás biztonsági kockázatait is. A bevezetőben végül hangsúlyt fogok fektetni arra, hogy az innovatív épületkörnyezetekben hatékony kiberbiztonsági intézkedésekre van szükség a munkavállalók bizonyos fokú magánszférájának és biztonságának védelme, valamint a zavartalan működés biztosítása érdekében.

A téma aktualitását alátámasztja, hogy a 2023. március 3-án megalakult Magyar Okosotthon és Épületautomatizálási Szövetség, rövid nevén Okosotthon Szövetség. A szövetség 14 tagvállalattal kezdte meg működését. A Szövetség célja, hogy egységes kommunikációval segítse a végfelhasználókat és a szakembereket a piac és a hozzá kapcsolódó megoldások megismerésében, valamint, hogy közelebb hozza a szakértőket és a döntéshozókat a hatékony és sikeres együttműködés érdekében. Továbbá céljai között szerepel az is, hogy egyfajta tájékozódási pontként, valamint szakmai fórumként szolgáljon az okosotthonok és az épületautomatika területén működő vállalkozások és szakemberek, a képző intézmények és egyéb szervezetek, valamint az állami döntéshozók számára. A szervezet számára kiemelten fontos a kiberbiztonság, így önálló Oktatási Szakosztállyal rendelkezik, melynek jelenleg én töltöm be az elnöki szerepét. Célunk, hogy a hazai szakmában iránymutatást adjunk a szakembereknek és a végfelhasználóknak. Ebbe beletartoznak a tervező és kivitelező mérnökök, akik akár egy komplex okos épületet is tervezhetnek. Ennek érdekében 2023-ban együttműködési megállapodást kötöttünk az Óbudai Egyetem - Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán indult Domotika szakmérnök/szaktanácsadó képzéssel, ahol kiemelt oktatási területek közé tartozik a kiberbiztonság.

A tudományos probléma megfogalmazás

A doktori értekezésemben tárgyalt tudományos probléma, hogy az okos épületek egyre inkább összekapcsolódnak és egyre több IoT-eszközre támaszkodnak, így nő a kibertámadásokkal szembeni sebezhetőségük. Jelenleg hiányzik a piacról egy olyan átfogó kiberbiztonsági keretrendszer, amely alkalmazkodóképes és rendelkezik valós idejű reagálóképességgel, így kezelni tudja a kiberfenyegetések változó és változatos természetét az okos épületek IoT rendszereiben. Így a meglévő kiberbiztonsági keretrendszerek elemzése és egy új ellenőrzőlista létrehozása a célom, amely segítségével

hatékonyan észlelhető, védhető és reagálható a kiberfenyegetésekre az okos épületek IoT környezetében. Ezt kívánom alátámasztani egy referenciamodell létrehozásával.

A tudományos probléma a következő fő szempontokra bontható:

Felismerés: A jelenleg legkorszerűbb okos épületek IoT kiberbiztonsága nem rendelkezik átfogó keretrendszerrel a kiberfenyegetések hatékony észlelésére és azonosítására. A meglévő észlelési rendszerek gyakran nem tudnak lépést tartani a támadók folyamatosan fejlődő taktikáival és technikáival szemben. Olyan fejlett észlelési mechanizmusokra van szükség, amelyek hatékonyan képesek az okos épületek IoT-rendszereiben található eszközök, protokollok és hálózati forgalom széles skáláját felügyelni, és valós időben, pontosan azonosítani a potenciális kiberfenyegetéseket.

Védelem: Az okos épületek IoT-rendszereinek kiberfenyegetésekkel szembeni védelme átfogó, több biztonsági ellenőrzési réteget magában foglaló keretrendszert igényel. A meglévő védelmi intézkedések nem elegendőek az okos épületek egyedi kihívásainak kezeléséhez. Olyan komplex védelmi mechanizmusokra van szükség, amelyek képesek az IoT-eszközök sebezhetőségének mérséklésére, valamint a jogosulatlan hozzáférés vagy az adatok megsértésének megakadályozására.

Ellenintézkedés: A kiberfenyegetésekre való gyors és hatékony reagálás kulcsfontosságú az okos épületek IoT-rendszereire gyakorolt hatásuk minimalizálásában. A meglévő válaszadási stratégiákból azonban hiányozhat az újonnan megjelenő fenyegetésekre való hatékony, valós idejű reagáláshoz szükséges agilitás és alkalmazkodóképesség. Olyan reagáló keretrendszerre van szükség, amely lehetővé teszi a gyors észlelést, a pontos fenyegetésértékelést és a hatékony incidensválaszadást az okos épületek IoT-környezeteiben. E szempontok alapján olyan új ellenőrzőlista és referenciamodell kidolgozása teszi szükségessé, amely a fejlett technológiákat, például a gépi tanulást, a mesterséges intelligenciát és az adatelemzést olyan személyre szabott módszerekkel kombinálja, amelyek az okos épületek IoT-rendszerei kiberfenyegetéseinek észlelésére, védelmére és az azokra való reagálásra szolgálnak. A keretrendszernek figyelembe kell vennie az okos épületek egyedi jellemzőit, beleértve a különböző eszközöket, protokollokat és adatfolyamokat, valamint a kiberfenyegetések változékonyságát.

Az okos épületek IoT-környezeteiben a kiberfenyegetések észlelésével, védelmével és az azokra való reagálással kapcsolatos kihívásokkal foglalkozó új ellenőrzőlista és

referenciamodell kidolgozásával a kutatásom célja, hogy hozzájáruljak az okos épületek IoT kiberbiztonságának javításához és hatékony eszközöket és stratégiákat biztosítsak az érdekelt felek számára rendszereikben a felmerülő kiberfenyegetések elleni védelméhez.

Célkitűzések

Az értekezésem célja az okos épületek IoT-rendszerei együttműködő védelmi stratégiájának vizsgálata és kidolgozása az érdekelt felek - köztük a gyártók, a szolgáltatók és a felhasználók - közötti fenyegetés-felderítési információmegosztás beépítésével. A cél az okos épületek kiberbiztonságának fokozása és a kiberfenyegetések mérséklése. Az alábbi konkrét kutatási célokat tűztem ki.

- Az okos épületek IoT-érintettjei - köztük a gyártók, szolgáltatók és felhasználók - jelenlegi helyzetének, valamint a fenyegetésekkel kapcsolatos információk megosztásával kapcsolatos meglévő gyakorlatuknak és képességeiknek a feltárása.
- Elemezni a fenyegetésinformációk megosztásának, mint közös védelmi stratégiának az okos épületek IoT-rendszereihez kapcsolódó előnyeit és kihívásait.
- A fenyegetésekkel kapcsolatos információk hatékony és biztonságos megosztása keretrendszerének kidolgozása az érdekelt felek között, figyelembe véve a magánélet védelmével kapcsolatos aggályokat, a jogi megfontolásokat és az okos épületrendszerek sokszínűségét.
- A különböző folyamatok és technológiák vizsgálata és elemzése a fenyegetésekkel kapcsolatos információk időben és hatékonyan történő gyűjtésére, elemzésére és terjesztésére.
- Kísérletek elvégzése annak felmérésére, hogy a fenyegetésekkel kapcsolatos információk megosztása milyen hatással van a rendszerbiztonság javítására, beleértve a kiberfenyegetések észlelését és mérséklését az okos épületek IoT-környezetében.
- Iránymutatás és ajánlás kidolgozása az érdekel felek számára a hatékony fenyegetettségi információk megosztására vonatkozó gyakorlatok megvalósítására és elfogadására vonatkozóan, beleértve az információmegosztás, a bizalomépítés és az együttműködésen alapuló védelmi stratégiák legjobb gyakorlatait.

E célok elérésével ez a kutatás hozzájárul az okos IoT-épületek kiberbiztonságának fejlesztéséhez azáltal, hogy az érdekelt felek közötti fenyegetés-felderítési információk megosztásának beépítésével együttműködő védelmi stratégiát hozna létre. Ez az együttműködésen alapuló megközelítés elősegíti az erősebb biztonsági helyzet kialakulását, lehetővé téve az érdekeltek számára, hogy proaktívan észleljék az okos épületek IoT-rendszereinek kiberfenyegetéseit, reagáljanak azokra, és enyhítsék azokat.

A téma kutatásának hipotézisei

H1: Egy átfogó kiberbiztonsági ellenőrzőlista kialakítása növelheti az okos épületekben lévő informatikai rendszerek átláthatóságát és megbízhatóságát, ezáltal csökkentve a kiberfenyegetések kockázatát.

H2: Feltételezem, hogy a kiberbiztonság növelése és a kibertámadások gyakoriságának csökkentése érdekében egy referenciamodell megvalósítása eredményre vezethet.

H3: Valószínű, hogy a meglévő kiberbiztonsági keretrendszerek hiányosságainak feltárása az okos épületekben javítja a kiber ellenállóképességet és a biztonság szintjét emeli.

Kutatási módszerek

Kutatásom alapját a primer kutatása adja, amely során versenyszférában szerzett saját tapasztalataimra építve vizsgáltam meg több aspektusból az okos épületeket kiberbiztonsági szempontból. Ebben az esetben a kutatási módszer egy összehasonlítóelemzés volt. Ezt továbbá segítette, hogy részt vettem Magyarország egyik legmodernebb és egyedülálló okos épületének a MOL Campus kiberbiztonsági szempontból fontos tényezőinek kezelésében is. Összehasonlító elemzést végeztem néhány kiemelt meglévő kiberbiztonsági keretrendszeren és szabványon. Továbbá a terület komplexitásának és újdonságtartalmának köszönhetően szakértői mélyinterjúkat készítetek hazai szakemberekkel, akiknek a kiberbiztonság és okos épületek a szakterülete. Használtam továbbá logikai kutatási módszerek is, mint az indukció, a dedukció, az analízis a szintézis és az absztrakció.

A kutatás lezárásának időpontja: **2024. március 11.**

1. OKOS ÉPÜLETEK ÉS AZ IOT KONVERGENCIÁJA

Az elmúlt években forradalmi technológiaként jelentek meg az IoT eszközök, amely alapvetően megváltoztatták a számítástechnikai, kommunikációs és vezérlőrendszerek világát. Paradigmaváltást jelentett a hagyományos, internetre csatlakoztatott eszközök, például számítógépek és okostelefonok helyett az egymással összekapcsolt tárgyak/eszközök hatalmas hálózata, amely valós időben képes adatokat gyűjteni, feldolgozni és megosztani. Ebben a fejezetben a dolgok internetének fejlődését mutatom be, nyomon követve annak eredetét, a legfontosabb mérföldköveket és a technológiai fejlesztéseket, amelyek hozzájárultak a jelenlegi állapothoz.

1.1. IoT-eszközök evolúciója

A dolgok internetének koncepciója az 1980-as évek elejére vezethető vissza, amikor a Carnegie Mellon Egyetemen kifejlesztették az első internetre csatlakoztatott eszközt, egy Coca-Cola-automatát. [2] Az internetre csatlakoztatott tárgynak ez a kezdetleges példája megalapozta az IoT fejlődését. A "dolgok internete" kifejezést azonban csak az 1990-es évek végén és a 2000-es évek elején alkotta meg Kevin Ashton brit vállalkozó, a Massachusetts Institute of Technology (MIT) Auto-ID Center társalapítója. [3] Ashton egy olyan világot képzelt el, ahol a mindennapi tárgyak csatlakoztathatók az internetre, kommunikálhatnak egymással és emberi beavatkozás nélkül hozzanak okos döntéseket. [3]

A 2000-es évek eleje kiemelt időszak volt a dolgok internetének fejlődésében, amikor olyan kulcsfontosságú alaptechnológiákat fejlesztettek ki, mint a vezeték nélküli érzékelőhálózatok (Wireless Sensor Networks - WSN), a rádiófrekvenciás azonosítás (Radio Frequency Identification - RFID) és a beágyazott rendszerek. A vezeték nélküli kommunikációra képes, kisméretű, kis teljesítményű érzékelőcsomópontokból álló WSN-ek döntő szerepet játszottak abban, hogy lehetővé vált az adatok gyűjtése és továbbítása a fizikai környezetből a digitális világba. [4] Az RFID-technológia, amely elektromágneses mezőket használ az eszközök azonosítására és nyomon követésére, megkönnyítette az okos dolgok kifejlesztését, amelyek egyedileg azonosíthatók és távolról ellenőrizhetők. [5] A mikrokontrollerekből vagy mikroprocesszorokból, memóriából és be- és kimeneti eszközökből álló beágyazott rendszerek lehetővé tették olyan okos gépek kifejlesztését, amelyek képesek adatok feldolgozására és meghatározott feladatok elvégzésére. [6]

Az okostelefonok elterjedése és a nagysebességű internet széles körű elterjedése a 2000-es évek végén és a 2010-es évek elején tovább gyorsította az IoT növekedését. A számos érzékelővel és kommunikációs interfésszel felszerelt okostelefonok átjáróként szolgálnak a különböző IoT-eszközök internethez való csatlakoztatásához. [7] A felhőalapú számítástechnika és a nagy adatelemzés fejlődése biztosította a szükséges infrastruktúrát az IoT-eszközök által generált hatalmas mennyiségű adat tárolásához, feldolgozásához és elemzéséhez. [8]

Az elmúlt években a mesterséges intelligencia (Artificial Intelligence - AI/MI) és a gépi tanulás (Machine Learning - ML) fejlődése tovább javította az IoT-eszközök képességeit. Az MI és az ML algoritmusok lehetővé teszik az IoT-eszközök számára az adatok elemzését, a minták felismerését és az önálló előrejelzések vagy döntések meghozatalát. [9] Ez az okos IoT-alkalmazások kifejlesztéséhez járult hozzá különböző területeken, többek között az egészségügyben, a közlekedésben, a mezőgazdaságban és az okos városokban. [10]

Összefoglalva, az IoT fejlődését számos kulcsfontosságú mérföldkő és technológiai előrelépés jellemezte, az első internetre csatlakoztatott eszköz kifejlesztésétől az MI és ML algoritmusok integrálásáig. Ezek az előrelépések hozzájárultak az IoT-eszközök és -alkalmazások elterjedéséhez, átalakítva mindennapi életünk különböző aspektusait és megnyitva az utat egy összekapcsolt és okos jövő előtt.

1.2. IoT-eszközök csoportosítása

Az IoT-eszközök széles skáláját foglalja magában, amelyek mindegyike meghatározott funkciók és alkalmazások ellátására szolgál. Ezen eszközök típusainak megismerése alapvető fontosságú ahhoz, hogy megértsük a különböző ágazatokra gyakorolt hatásának szélességét és mélységét. [11] Két fő kategóriába csoportosítjuk az eszközöket. Egyik az érzékelők az IoT-ökoszisztémák alapvető elemei. Az érzékelők adatokat gyűjtenek a környezetükből, amelyek közé tartozhat a hőmérséklet, a páratartalom, a fény, a mozgás, vagy a levegőminőség. Például egy okos termosztátban lévő hőmérséklet-érzékelő adatokat gyűjt az épület fűtési rendszerek szabályozásához, vagy egy jelenlét érzékelő a helyiségben tartózkodó személyek számát vizsgálja és méri a szén-dioxid mennyiséget. [12] Másik csoport az aktuátorok, olyan eszközök, amelyek a központi rendszerből kapott adatok vagy utasítások alapján hajtanak végre műveleteket. Ilyen például egy okos öntözőrendszer, amely a talajnedvesség-érzékelőktől kapott adatok

alapján öntözi a növényeket, vagy egy redőnyvezérlő, ami a napfény alapján szabályozza redőnyök lamelláinak nyitási szögét.

Megtalálhatók az ökoszisztémában még a viselhető IoT-eszközök, amelyek kiemelt népszerűségre tettek szert, különösen az egészségügyi és fitneszszektorban. Ezek közé tartoznak az okosórák és az egészségügyi monitorok. Ezek nyomon követik a különböző egészségügyi mérőszámokat, például a pulzusszámot, a lépéseket és az alvási szokásokat, betekintést nyújtva a felhasználó fizikai jólétébe. Erre példa az Apple Watch, amely figyeli a pulzusszámot és képes az esések észlelésére. [11][12]

Az okos épületek mellett az okos otthonok is egyre jobban elterjednek, így ebbe a kategóriába tartoznak az otthoni automatizálást és energiahatékonyságot javító eszközök. Az olyan okos termosztátok, mint a Nest vagy az Ecobee, idővel megtanulják a felhasználó preferenciáit, és az optimális kényelem és energiatakarékosság érdekében beállítják a fűtést és hűtést. Az okos világítási rendszerek, mint például a Philips Hue, lehetővé teszik a felhasználók számára a világítás távoli vezérlését és a különböző eseményekhez igazított beállítások testreszabását. Az okos biztonsági kamerák és ajtócsengők, mint például a Ring vagy az Arlo, valós idejű felügyeletet és riasztásokat biztosítanak a lakástulajdonosok számára. [15]

Az ipari szektorban is kritikus szerepet játszanak az IoT-eszközök, mint a gyártási folyamatok felügyeletében és optimalizálásában. Ezeket az úgynevezett (IIoT - Industrial IoT) eszközök. Ide tartoznak a gép teljesítményét, a környezeti feltételeket és a gyártási minőséget nyomon követő érzékelők. Egy gyárban például az érzékelők a karbantartási igények előrejelzése érdekében figyelemmel kísérhetik a berendezések rezgését. Az IIoT a logisztikához és az ellátási lánc irányításához szükséges eszközöket is magában foglalja, például a készletek nyomon követésére szolgáló RFID-címkéket. [16]

Az okos városokban is megjelennek az IoT-eszközök, mint a forgalomirányítás, a hulladékgazdálkodás és a környezetfelügyelet érzékelői és rendszerei. A közlekedési érzékelők optimalizálhatják a forgalomáramlást, míg az okos szemetesek jelzik, ha megteltek és ki kell üríteni őket. A környezetfigyelő szenzorok a levegőminőséget, a zajszintet és más tényezőket mérik a városi életkörülmények javítása érdekében. [17]

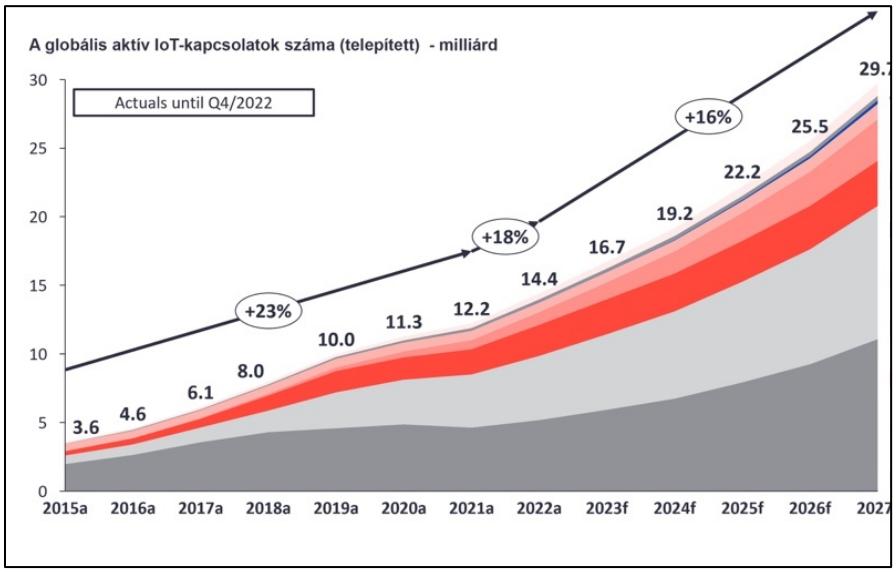
Az elmúlt években folyamatosan fejlődik az egészségügy, így ezen a területen a IoT-eszközök a viselhető egészségügyi monitoroktól a fejlett diagnosztikai és kezelési technológiákig terjednek. A krónikus betegségben szenvedő betegek viselhető eszközei adatokat továbbíthatnak az egészségügyi szolgáltatóknak a folyamatos nyomon követés érdekében. Az IoT-eszközök közé tartoznak a fejlett rendszerek is, mint például a

kórházakban az okos ágyak, amelyek képesek a betegek életfunkcióit nyomon követni és a személyzetet figyelmeztetni bármilyen problémára, vagy az okos vércukor mérő és adagoló. [16][17]

Végezetül pedig a mezőgazdaságban az IoT a talajminőséget, az időjárási körülményeket és a termés egészségét mérő érzékelőket foglalja magában. Ezek az eszközök lehetővé teszik a precíziós gazdálkodást, ahol az erőforrások, például a víz és a műtrágya optimális felhasználása valós idejű adatok alapján történik. Az IoT-technológiákkal felszerelt drónokat és autonóm járműveket is használják a termények megfigyelésére és kezelésére. [18][19]

1.3. IoT-eszközök jelenlegi helyzete

Az elmúlt közel 10 évben exponenciális növekedés figyelhető meg a piacon a telepített eszközök számát tekintve. Ezt jól mutatja az 2. ábra, ahol 2015 és 2027 közötti vizsgált időszakot láthatunk a csatlakozási típusok alapján és az összetett éves növekedési ráta (Compound annual growth rate - CAGR) egyes vizsgált időszakaiban. A vezetékes IoT eszközök 2021-22 között 5%-os növekedést értek el évente, míg az azt követő 2022-27 években a dupláját, 10%-ot várnak az elemzők. A vezeték nélküli személyi hálózatok (Wireless Personal Area Network - WPAN) esetében az elkövetkező 2022-27-es időszakban további 16%-os évenkénti növekedés várható, ami az otthoni IoT eszközöknek tudható be, hiszen egyre több készüléket használunk otthonvezeték nélkül.



2. ábra: Globális IoT piaci előrejelzés a csatlakoztatott eszközök számát tekintve *[22]*

1.4. IoT-keretrendszerek bemutatása

A Matter és a Thread kulcsfontosságú kommunikációs protokollok az IoT területén, amelyek növelik az okos eszközök összekapcsolhatóságát és interoperabilitását. A

Connectivity Standards Alliance (CSA) által kifejlesztett Matter egy nyílt forráskódú szabvány, amelyet az okos otthoni termékek egyetemes kompatibilitására terveztek, a hangsúlyt a biztonságra és az egyszerű használatra helyezve. A Thread egy alacsony fogyasztású vezeték nélküli hálós hálózati protokoll, amely az otthoni automatizálás megbízható, biztonságos kommunikációjára összpontosít, olyan nyílt szabványokat használva, mint az IPv6. Mindkét protokoll hozzájárul az okos otthoni ökoszisztémák növekedéséhez és funkcionalitásához.

1.4.1. Matter szabvány

A Matter egy univerzális kommunikációs protokoll, amelyet okos otthoni eszközökhöz terveztek. Meghatározza az eszközökön telepítendő alkalmazási réteget és a különböző kapcsolati rétegeket az interoperabilitás fenntartása érdekében. Az egyik legfontosabb biztonsági aggály, amelyet kiemeltek a szabványban az eszköz elleni támadás lehetősége volt. Ezt egy rosszindulatú eszköz vagy a személy hajthatja végre, offline „nyers erős" (bruteforce) támadást alkalmazva a kód visszafejtésére. A támadó jelen lehet a hálózaton helyben vagy távoli hozzáféréssel. Egy ilyen támadás lehetséges következményei súlyosak, beleértve az eszköz feletti kontroll megszerzését és az érzékeny adatokhoz, például az IP-kamera adatforgalmához való hozzáférést. Az ilyen típusú támadással kapcsolatos kockázati szint magas, ami jelzi a megelőzésére irányuló biztonsági intézkedések fontosságát. [23]

A szabvány részletezi a hálózati interfész működésével kapcsolatos különböző attribútumokat is. Ezek közé tartozik a TxErrCount attribútum, amely az vezetékes hálózati interfészen bekövetkezett átviteli hibák számát jelzi, valamint a CollisionCount attribútum, amely az vezetékes hálózati interfészen történő csomagátviteli kísérlet során bekövetkezett ütközések számát mutatja. Egy másik fontos attribútum az OverrunCount, amely a be- vagy kilépő csomagok számát jelzi, amelyek az vezetékes hálózati interfészen lévő összes csomag tárolására szolgáló puffer memória hiánya miatt estek ki.

Abban az esetben, ha egy eszköz áramkimaradás vagy újraindítás miatt elveszíti az időmérési állapotát, a szabvány javasolja, hogy az OTA (Over-the-air)-kérelmezők - ha képesek rá - naponta próbáljanak QueryImage parancsot adni, hogy időben hozzáférjenek a frissített szoftverhez, beleértve a biztonságkritikus frissítéseket is. Az OTA-szolgáltatónak egy, a megvalósítója által megfelelőnek ítélt algoritmust kell használnia a megfelelő eljárás meghatározásához.

A szabvány hangsúlyozza továbbá a firmware hitelességének és integritásának a telepítés előtti ellenőrzését. A csomópontoknak (node) a konfigurációt és a bemeneti adatokat is

validálniuk kell a hosszúság, valamint az elfogadható értékek és tartományok tekintetében, mielőtt azokat alkalmaznák. Ez az érvényesítés az alkalmazott konfigurációtól vagy bemenettől függ. Ebből következik, hogy a szabvány keretében kívánják beépíteni azt a biztonsági megoldást, hogy az eszköz folyamatosan naprakész legyen. Kiberbiztonsági szempontból az alábbi aspektusokat emelném ki, amivel a Matter foglalkozik.

Eszközbiztonsági intézkedések

- Hozzáférés-ellenőrzés: Ez olyan intézkedéseket foglal magában, mint az erős hitelesítési mechanizmusok, amelyek megakadályozzák az eszközökhöz való jogosulatlan hozzáférést.
- Rendszeres biztonsági frissítések: Annak biztosítása, hogy az eszközök időben frissítéseket kapjanak a sebezhetőségek kezelésére.
- Fizikai biztonsági intézkedések: Az eszközök védelme a manipulációtól vagy az illetéktelen fizikai hozzáféréstől.

Adatvédelem

- Az érzékeny adatok titkosítása: Erős titkosítási algoritmusok alkalmazása a felhasználói adatok nyugalmi és tranzitvédelmére, úgy, mint a 128 bites kulcs és SHA-256 hash funkció.
- Hozzáférés-szabályozás: Annak meghatározása és betartatása, hogy ki milyen körülmények között milyen adatokhoz férhet hozzá.
- Az adatok anonimizálása: Adott esetben a felhasználói adatok anonimizálásának biztosítása a magánélet védelme érdekében.

Firmware-biztonság

- Biztonságos indítási mechanizmusok: Annak biztosítása, hogy az eszközök csak ellenőrzött és megbízható firmware-rel bootoljanak.
- Firmware aláírása és validálása: A firmware aláírására és az aláírások telepítés előtti érvényesítésére szolgáló eljárások végrehajtása.
- Az alrendszerek biztonságos elkülönítése: A kritikus biztonsági funkciók elkülönítése a fő eszközszoftvertől a kompromittálódás kockázatának csökkentése érdekében.

Üzenetbiztonság

- Titkosítási kulcsok használata: Ezen kulcsok alkalmazása, min az R2IKey és I2RKey az üzenetek titkosítására és integritásvédelmére biztosítja, hogy az adatok bizalmasak és változatlanok maradnak az átvitel során.
- Biztonságos kulcskezelés: A titkosítási kulcsok biztonságos tárolása és kezelése a jogosulatlan hozzáférés megakadályozása érdekében.

Az adatok titkossága és sértetlensége

- Hitelesített titkosítás társított adatokkal: Ez a módszer egyesíti a titkosítást a titkosság és a hitelesítést az adatok integritása érdekében, biztosítva ezzel az adatok biztonságát és változatlanságát.
- Szimmetrikus blokkos kódolás használata: Hatékony titkosítás a csomópontok között kicserélt üzenetek titkosságának védelmére.

Fontos kiegészítés, hogy a Matter szabványt implementálóknak ajánlatos jelezniük, hogy megfelelnek-e a legjobb gyakorlatoknak vagy sem. Az Matter tanúsítás önmagában nem fogja ellenőrizni, hogy ezek a követelmények teljesülnek-e. A Matter 1.0 bejelentése óta, több, mint 1 év alatt 24.600 specifikáció letöltés, 1214 minősítés és 24%-os növekedés volt mérhető a CSA-hoz csatlakozott cégek számában. [24]

Végezetül a szabvány részletezi a különböző lehetséges hibákat, amelyek egy hálózatba kapcsolt eszköz működése során előfordulhatnak. Ezek közé tartozik a BoundsExceeded, amely azt jelzi, hogy egy hálózati konfiguráció hozzáadása meghaladná a MaxNetworks attribútum által meghatározott korlátot, és a NetworkIdNotFound, amely azt jelzi, hogy a hálózati azonosítót várhatóan megtalálták, de nem találták meg a Networks attribútumban a hozzáadott hálózati konfigurációk között. Az UnknownError azt jelzi, hogy a művelet során belső hiba történt. [23]

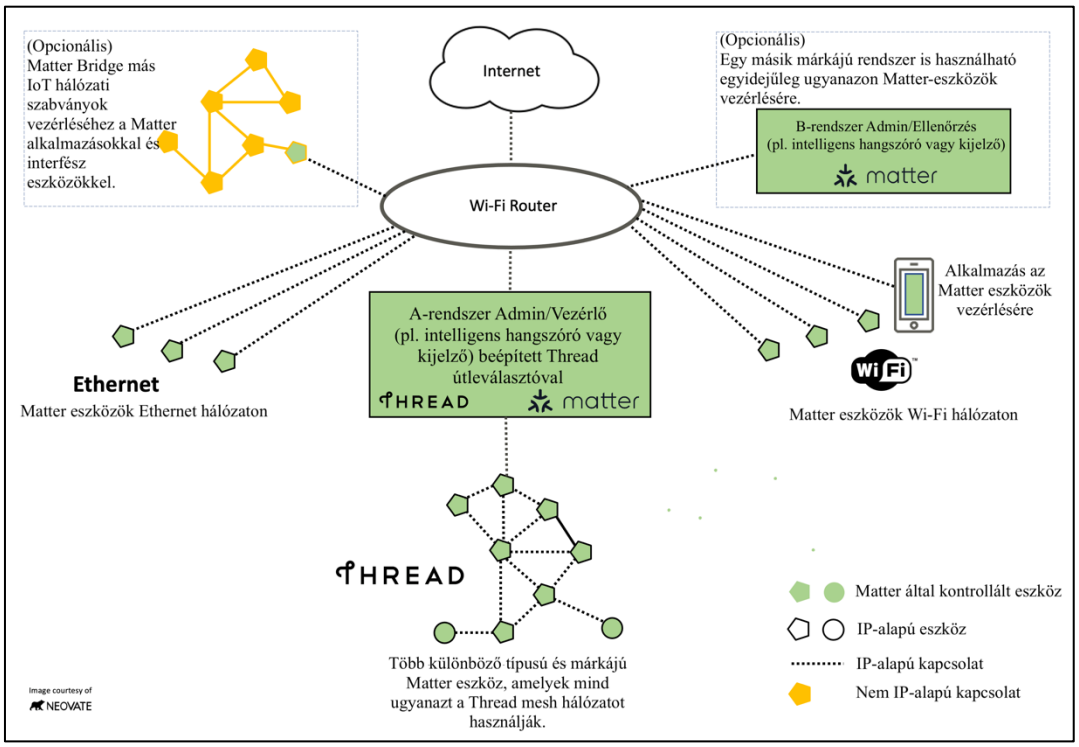
1.4.2. Thread protokoll

A Thread Group, Inc. által kiadott "Thread Commissioning White Paper" átfogó áttekintést nyújt a Thread üzembe helyezési folyamáról, amely az otthoni automatizáláshoz tervezett Thread a hálózati protokoll kulcsfontosságú eleme. Ez a protokoll a biztonságos, skálázható és komplex hálózatok létrehozására összpontosít az otthoni csatlakoztatott eszközök számára. A 2015 júliusában megjelent fehér könyv egy referenciának szánt technikai dokumentum, amely betekintést nyújt a Thread-hálózaton belüli eszközök üzembe helyezésének folyamatába.

Főbb összetevők és folyamatok

- Rendszertopológia és biztonsági alapok: A dokumentum a rendszer topológiájának és a Thread hálózaton belüli biztonság alapvető szempontjainak ismertetésével kezdődik. Kiemeli a biztonsági intézkedések fontosságát a csatlakoztatott eszközök biztonságos működésének biztosítása érdekében.
- Üzembe helyezési folyamat: Ez a folyamat alapvető fontosságú az eszközök (Joiners) biztonságos hozzáadásához a Thread hálózathoz.
- Hitelesítés és kulcsmegállapodás: Létfontosságúak a hálózaton belüli biztonságos kommunikáció létrehozásához. Ismerteti az egész hálózatra kiterjedő kulcsok használatát és e kulcsok karbantartását a folyamatos hálózati biztonság biztosítása érdekében.
- Üzembe helyezési protokoll: Bemutatja az üzembe helyezési protokollt, kiemelve az új eszközök hálózathoz való sikeres hozzáadásának lépéseit és követelményeit. Ez magában foglalja a kérelmezési folyamatot és a különböző típusú üzembe helyezők (külső és natív) szerepét.
- Biztonsági szekvenciák: A Joiner-Joiner Router-Border Router-Commissioner szekvencia. Ezek a szekvenciák vizuális és technikai ábrázolást nyújtanak arról, hogy az eszközök hogyan lépnek kapcsolatba egymással és hogyan hoznak létre biztonságos kapcsolatokat a hálózaton belül.
- Hivatkozások és műszaki szabványok: A Thread üzembe helyezésének folyamata szempontjából releváns műszaki szabványokra és protokollokra, például a TLS (Transport Layer Security) protokollra, a DTLS (Datagram Transport Layer Security) protokollra és a CoAP (Constrained Application Protocol) protokollra hivatkozik.

A Threadet és Mattert alapetően úgy tervezték, hogy szorosan együttműködve legyen ezen keresztül kontrollálható és monitorozható legyen egy okosotthon. Az alábbi ábrán szemléltetésre kerül a hálózati topológia, amely magában foglalja az otthoni vezeték nélküli router, a hozzákapcsolt vezetékes és vezeték nélküli IoT eszközök, a külső internet és a Matter kompatibilis, vagy inkompatibilis eszközök. Célja, hogy univerzális híd legyen a különböző gyártók eszközei között. A 3. számú ábrán látható egy okosotthon Thread hálózat Matter kompatibilis eszközökkel.



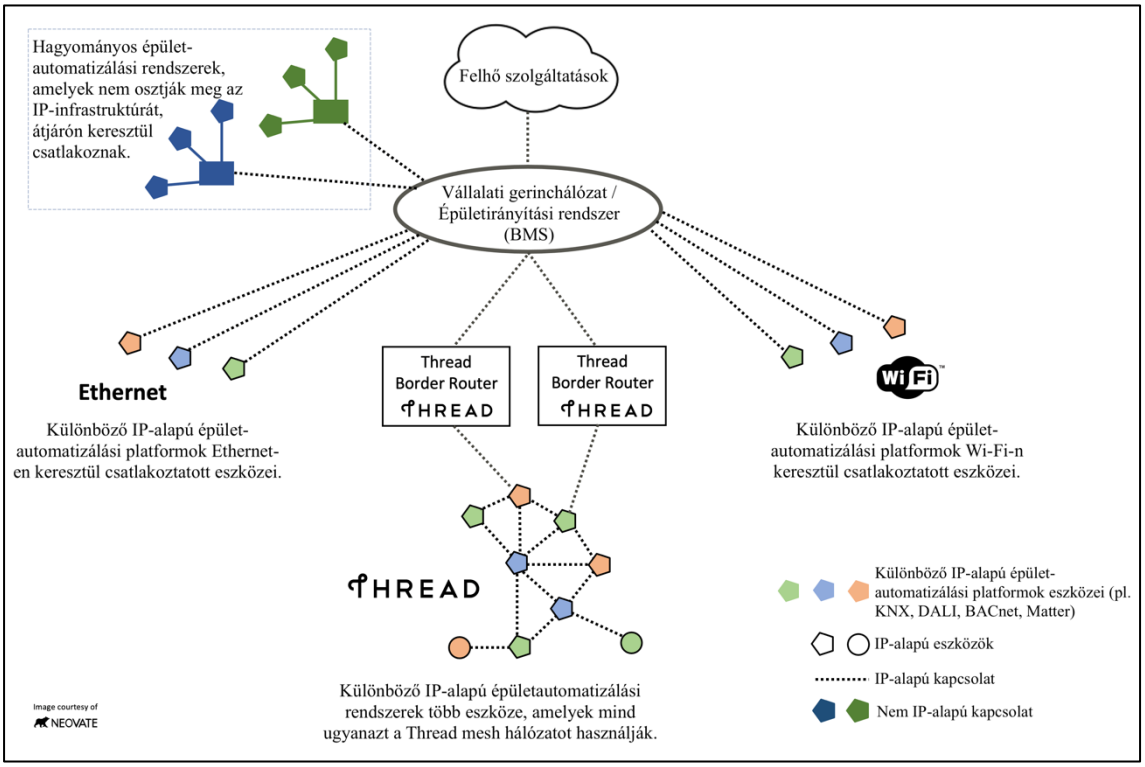
3. ábra: Thread kialakítása egy okosotthonban Matter eszközökkel *[25]*

Összefoglalva a technikai dokumentációt, részletes betekintést nyújt a Thread hálózaton belüli üzembe helyezési folyamatba. A rendszer topológiájának különböző aspektusait, a biztonsági alapokat, az üzembe helyezési protokollt és a hitelesítési folyamatokat tárgyalja.

Az okos épületek és a Tread kapcsolatát vizsgálva megvizsgáltam a Jorg Kennis, Klaus Waechter és Sujata Neidig által írt, 2022 szeptemberében megjelent "Thread 1.2 for Smart Buildings White Paper" című dokumentumát, amely a Thread hálózati protokoll mélyreható elemzését tartalmazza, különös tekintettel annak okos épületekben való alkalmazására Korábban ismertetésre került, hogy a Thread a vezeték nélküli kommunikáció nyílt szabványa, amely natív Internet Protocol (IP) megoldást kínál a megbízható, alacsony fogyasztású, biztonságos, eszköz-eszköz közötti kommunikációhoz. A széles körben támogatott IEEE 802.15.4 vezeték nélküli technológiai elv alapján működik, és IPv6-alapra épül, amely megkönnyíti a rugalmas beállítást, felügyeletet, adatelemzést, adatszolgáltatást és közvetlen felhőkapcsolatot a titkosítás és biztonság veszélyeztetése nélkül. [26]

A Thread fő jellemzői az okos épületekben

- IPv6-alapú hálózatépítés: Az IPv6 használata a Threadben kiküszöböli az IPv4 címzési tartományának korlátait, lehetővé téve a hatalmas számú eszköz csatlakoztatását. Ez kulcsfontosságú az IoT korszakában, ahol a csatlakoztatott eszközök száma gyorsan növekszik.
- Alacsony energiafogyasztás és Mesh hálózatépítés: A Thread tervezése az alacsony energiafogyasztásra és a hatékony működésre összpontosít, még az egyetlen AA elemmel működő eszközökön is. Egyszerűsített útválasztási protokollt és rövid üzenetméreteket alkalmaz a sávszélesség és az energia megtakarítása érdekében. Mesh topológia tekintetében pedig cél, hogy az eszközök egymással kommunikálva adják tovább az adatokat.
- Biztonság minden szinten: A Thread az IP-alapú alapjainak köszönhetően végponttól végpontig tartó biztonságot biztosít, így nincs szükség címfordításra vagy az adatcsomagok dekódolására és újbóli titkosítására. A hálózatot a MAC-rétegben használt, az egész hálózatra kiterjedő kulcs védi, amely alapvető biztonságot nyújt a lehallgatás és a megszakítás ellen.
- Rugalmasság és skálázhatóság: A Thread a Wi-Fihez hasonlóan több alkalmazási réteget támogat, lehetővé téve, hogy ugyanazon a hálózaton különböző szolgáltatások egyidejűleg fussanak. Ez a rugalmasság kulcsfontosságú a különböző technológiák integrálásához és a jövőbeli fejlesztésekhez való alkalmazkodáshoz.
- Okos épületalkalmazások: A Thread különösen előnyös az épületautomatizálási és világításvezérlő berendezések számára. Olyan előnyöket kínál, mint az egyéni vezérlés, a költségek csökkentése, a távoli és prediktív karbantartás, valamint az egész rendszerre kiterjedő egyszerűsített frissítések.
- Integráció nem IP-alapú rendszerekkel: A Thread képes áthidalni az épületekben található hagyományos nem IP-alapú rendszereket, és átjárókon keresztül integrálni azokat az újabb IP-alapú technológiákkal. Ez megkönnyíti a teljesen IP-alapú rendszerekre való fokozatos átállást.
- Interoperabilitás más szabványokkal: A Thread-et az épületautomatizálás különböző IoT-szabványai (pl. DALI+, KNX IoT, Matter, OCF és BACnet) jövőbiztos megoldásként ismerik el. Alkalmazás-agnosztikus jellege lehetővé teszi az egyedi igényeknek megfelelő egyedi alkalmazásréteg-fejlesztést.



4. ábra: Thread egy okos épületben többféle automatizálási szabvánnyal *[25]*

Összefoglalva a „Thread 1.2 Smart Building” protokoll rugalmas és biztonságos megoldásként jelenik meg az okos épületalkalmazások számára. IPv6-alapú, alacsony energiaigényű, öngyógyító hálós hálózati architektúrája a központosított üzembe helyezéssel és üzemeltetéssel együtt vezető technológiává teszi az okos épületek ágazatában. A fehér könyv kiemeli a Thread potenciálját az okos épületek működési hatékonyságának, kényelmének és karbantartásának fokozásában, és az IoT-térség egyik szereplőjeként jelöli meg. [27]

1.5. Az okos épületek fejlődése

Az okos épületek előrelépést jelentenek a technológia építészeti terekbe történő integrálásában, továbbá paradigmaváltást jelentenek az épületek tervezésében, kivitelezésében és üzemeltetésében. Az egymással összekapcsolt technológiák használata jellemzi az okos épületeket, amelyeket úgy terveztek, hogy olyan környezetet hozzanak létre, amely hatékony, fenntartható és a felhasználói igényekhez igazodik. [17]

Az okos épületek kialakulása az épületautomatizálási rendszerek 20. század végi megjelenéséig vezethető vissza. [28] Akkoriban ezek a rendszerek kezdetlegesek voltak, és elsősorban az alapvető vezérlésre és energiagazdálkodásra összpontosítottak. A technológiai fejlődéssel azonban, különösen a számítástechnika és a távközlés területén, elérhetővé vált az integráltabb és okosabb épületirányítási rendszerek lehetősége. [29] A

kezdeti szakaszban az okos épülettechnológia elsődlegesen az energiafogyasztás optimalizálására és a működési hatékonyság növelésére összpontosított. Ezt nagyrészt a környezeti fenntarthatósággal kapcsolatos növekvő tudatosság és az energiaköltségek csökkentésének szükségessége vezérelte. Az érzékelőtechnológia és a vezérlőrendszerek terén bevezetett innovációk lehetővé tették, hogy az épületek valós időben alkalmazkodjanak a változó körülményekhez, ami javulást eredményezett az energiahatékonyságban. [17] A 21. századba lépve az okos épületek köre kibővült, amit a dolgok internete is elősegített. Az IoT-eszközök integrációja az épületeket passzív szerkezetekből dinamikus ökoszisztémákká alakította át, amelyek képesek adatokat gyűjteni, elemezni és reagálni az adatokra. Ez a paradigmaváltás új korszakot jelentett az épületek irányításában, ahol a rendszerek képesek előre jelezni és alkalmazkodni a benne lévők igényeihez, ami a kényelem, a komfort és a biztonság eddig nem látott szintjéhez vezetett. [30] Ma az okos épületek fogalma a technológiák és alkalmazások széles spektrumát öleli fel. Az okos épületek képességei folyamatosan fejlődnek, kezdve a fejlett HVAC-rendszerektől kezdve, amelyek alkalmazkodnak a használati szokásokhoz, egészen az okos biztonsági rendszerekig, amelyek képesek azonosítani és csökkenteni a fenyegetéseket. A mesterséges intelligencia és a gépi tanulás integrálása tovább növelte az ezekben a struktúrákban rejlő lehetőségeket, lehetővé téve a prediktív elemzést és a kifinomultabb döntéshozatali folyamatokat. [31] Az okos épületek fejlődés ráadásul nem csupán egy technológiai fejlődés, hanem a változó társadalmi igények és értékek tükre is. A fenntarthatóság, az emberek jólétének és az erőforrás-hatékonyságnak a növekvő hangsúlyozása tükrözi a globális prioritások szélesebb körű változásait. Az okos épületek tehát nem pusztán fizikai struktúrák, hanem egy jobban összekapcsolt, hatékonyabb és fenntarthatóbb jövőre irányuló törekvéseink megtestesítői.

A továbbiakban megvizsgálom a legfontosabb technológiai fejlesztéseket és társadalmi trendeket, amelyek az okos épületek fejlődését alakították. Úgy, min az előttünk álló kihívásokat és lehetőségeket is, mivel a technológia épített környezetbe való integrációja továbbra is újra definiálja az épületekről alkotott elképzeléseinket.

1.6. Az okos épületek előnyei és kihívásai

Az okos épületek, amelyeket a fejlett technológiák integrálása jellemez, számos előnnyel járnak, de számos kihívással is szembe kell nézniük. Ebben az alfejezetben részletesen ismertetem ezeket a szempontokat, átfogó képet nyújtva az okos épülettechnológiák következményeiről. Egyik fő előny a fokozott energiahatékonyság, mely az optimalizált

erőforrás-felhasználásból áll, miszerint az okos épületek automatizált rendszereket alkalmaznak az erőforrások, például a villamos energia és a víz felhasználásának optimalizálására, ami az energiafogyasztás és a közüzemi költségek csökkenéséhez vezet. A megújuló energiaforrások, például a napelemek és a hatékony hulladékgazdálkodási rendszerek integrálása hozzájárul az okos épületek fenntarthatóságához. [15][25] A termelékenységhez hozzájárul a javított komfort, avagy adaptív környezetek, úgy, mint az automatizált klímavezérlés és világítási rendszerek révén az okos épületek olyan környezetet hoznak létre, amely alkalmazkodik a felhasználók preferenciáihoz, növelve a kényelmet és a termelékenységet. Ennek köszönhetően az egészség és jólét olyan funkciók, mint a levegőminőség-ellenőrzés és a természetes megvilágítás hozzájárulnak a felhasználók egészségéhez és jólétéhez. Biztonsági szempontból a fokozott felügyelet elve mellett az okos épületek fejlett biztonsági rendszerekkel vannak felszerelve, beleértve a megfigyelő kamerákat és a belépés-ellenőrzést, amelyek biztosítják a felhasználók biztonságát. Továbbá a vészhelyzeti reagálás is az előnyök között szerepel, mivel az automatizált rendszerek hatékonyabban észlelik és reagálnak a vészhelyzetekre, például a tűzesetekre vagy a biztonsági előírások megsértésére. Üzemeltetési és karbantartási hatékonyság szempontjából az előrejelző karbantartás során az IoT-eszközök és az adatelemzés lehetővé teszi a prediktív karbantartást, csökkentve az állásidőt és meghosszabbítva a berendezések élettartamát. Továbbá az épületrendszerek a valós idejű felügyelettel folyamatosan lehetővé teszik a problémák gyors felismerését és megoldását. [17]

A kihívásokat tekintve megjelennek a magas kezdeti költségek és megtérülési aggályok. Ezek között kiemelkedőek a beruházási követelmények, mivel az okos épülettechnológiák bevezetésének kezdeti költségei magasak lehetnek, ami kihívást jelent egyes fejlesztők és tulajdonosok számára. Így a beruházások megtérülésével (Return on Investment - ROI) kapcsolatban bizonytalanság állhat fenn, különösen az energiamegtakarítás és az üzemeltetési hatékonyság tekintetében. [32]

Megjelennek továbbá a kiberbiztonsági és adatvédelmi kockázatok, mint a kibertámadásokkal szembeni sebezhetőség az okos épületek összekapcsolt jellege sebezhetővé teszi őket a kiberfenyegetésekkel szemben, ami kiberbiztonsági intézkedéseket tesz szükségessé. Ahogy az adatvédelmi kérdések is aggályokat vethetnek fel, mivel az okos épületrendszerek által végzett adatgyűjtés és adatkezelés a szabályozásoknak való megfelelést igényelnek. [30]

Végezetül pedig a technológiai és interoperabilitási kérdések tekintetében az okos épülettechnológiák összetettsége kihívást jelenthet az irányítás és karbantartás szempontjából. A különböző gyártók különböző rendszerei és eszközei közötti kompatibilitás és integráció biztosítása kihívást jelent. [33] Így a szakképzett munkaerő és a felhasználók alkalmazkodása is nagy kihívást jelent, mivel az okos épületrendszerek üzemeltetése és karbantartása speciális készségekkel rendelkező munkaerőt igényel. Illetve a munkavállalók és a vezetők számára tanulási folyamatot jelenthet az okos épülettechnológiákhoz való alkalmazkodás és azok teljes körű kihasználása.

Az okos épületek előrelépést jelentenek az épülettechnológiában, és számos előnyt kínálnak a hatékonyság, a kényelem és a fenntarthatóság tekintetében. Ugyanakkor olyan kihívásokat is jelentenek, amelyekkel foglalkozni kell a bennük rejlő lehetőségek maximális kiaknázása érdekében. Az okos épületek sikeres megvalósítása és üzemeltetése szempontjából kulcsfontosságú ezen előnyök és kihívások egyensúlyban tartása.

1.7. Globális példák az okos épületekre

Az okos épületek fejlődése nem csupán elméleti koncepció, hanem kézzelfogható valóság, amit számos úttörő projekt bizonyít világszerte. Ezek a különböző célú és kialakítású épületek példázzák a technológia innovatív integrációját az épített környezetbe. Ebben az alfejezet a világ különböző részeiről származó, figyelemre méltó okos épületekből mutatok be egy válogatást, kiemelve a terület sokszínűségét és találékonyságát.

The Edge, Amszterdam, Hollandia

Az amszterdami The Edge-et gyakran emlegetik a világ egyik legokosabb irodaházaként. A PLP Architecture által tervezett épület IoT-érzékelők széles skáláját és fejlett épületirányítási rendszert használ. Az épület kifinomult energiagazdálkodási rendszerrel rendelkezik, beleértve a napelemeket és az esővízgyűjtést is, így az egyik legfenntarthatóbb irodaház a világon. A The Edge épületet gyakran a világ egyik leginnovatívabb és legfenntarthatóbb irodaházaként emlegetik. A PLP Architecture által tervezett és az OVG Real Estate által fejlesztett épület 2014-ben készült el. Az épület a Deloitte globális központjaként szolgál, és példaképe annak, hogy a technológia és a design hogyan találkozhat egymással, hogy élvonalbeli, fenntartható munkaterületet hozzon létre. [34] A The Edge építészeti kialakítása a modern esztétika és funkcionalitás bizonyítéka. Az épület feltűnő üveghomlokzata nemcsak elegáns, kortárs megjelenést

kölcsönöz az épületnek, hanem az energiagazdálkodási stratégiában is döntő szerepet játszik. A kialakítás optimalizálja a természetes fényt, csökkentve a mesterséges világítás szükségességét, és hozzájárul az épület energiahatékonyságához. A The Edge egyik legfigyelemreméltóbb aspektusa a fenntarthatósága. Az épület 98,36%-os BREEAM (Building Research Establishment Environmental Assessment Method) pontszámot ért el, ami a világ egyik legzöldebb épületévé teszi. Az elért eredményhez hozzájáruló legfontosabb jellemzők a következők:

- Napelemek: A tetőt és a déli fekvésű falat napelemek borítják, így az épület nagyrészt energiafüggetlen.
- Esővízgyűjtés: Az épületet esővízgyűjtő rendszerrel látták el, amelyet a WC-k öblítésére és a zöldterületek öntözésére használnak.
- Energiahatékonyság: Az Edge egy víztározó hőenergia-tároló rendszert használ a teljes fűtés és hűtés előállítására, ami csökkenti az energiafogyasztást.

Az Edge a kereskedelmi épületben történő IoT-integráció bemutatója. Több, mint 28.000 érzékelőt alkalmaz, amelyek a fényt, a hőmérsékletet, a mozgást, a páratartalmat és még a CO2-szintet is figyelik. Ezek az érzékelők szerves részét képezik az épület automatizált rendszereinek, amelyek valós időben állítják be a világítást, a fűtést és a hűtést a foglaltság és a környezeti feltételek alapján.

Az épület rendkívül rugalmas és okos munkakörnyezetet kínál. Az munkavállalóknak nincs állandó íróasztaluk, ehelyett a Deloitte által kifejlesztett "The Edge App" nevű alkalmazást használják, amely segít nekik megtalálni a napi igényeiknek megfelelő munkaterületet. Az alkalmazás emellett vezérli a személyes világítás és a klíma beállításait, tárgyalótermeket foglal, és a dolgozókat a rendelkezésre álló parkolóhelyekre irányítja. A The Edge egy adatvezérelt épület. Az érzékelői által gyűjtött hatalmas mennyiségű adatot elemzik az épület működésének optimalizálása és a munkakörnyezet javítása érdekében. Ez az adatvezérelt megközelítés lehetővé teszi a prediktív karbantartást, növeli az épület hatékonyságát, és betekintést nyújt a helykihasználásba.Az Edge nemzetközi elismerést szerzett az irodatervezés és a fenntarthatóság innovatív megközelítéséért. A jövő okos épületeinek mércéjévé vált, bemutatva, hogyan lehet a technológiát olyan munkaterületek létrehozására használni, amelyek nemcsak hatékonyak és fenntarthatóak, hanem a használók igényeire is reagálnak.

Összefoglalva, az amszterdami The Edge az okos épülettervezés innovációjának jelzőfénye. A fenntarthatóság, a technológia és a felhasználó-központú tervezés

integrációja új mércét állít fel az irodaházak számára világszerte, és értékes betekintést nyújt a munkahelyi környezetek jövőjébe.

Burj Khalifa, Dubai, Egyesült Arab Emírségek

A világ legmagasabb épületeként a Burj Khalifa nemcsak építészeti csoda, hanem az okos építési technológia bizonyítéka is. A legmodernebb biztonsági rendszereket, automatizált világítás- és klímavezérlést, valamint okos liftrendszereket tartalmaz, amelyek mind a hatékonyság és a látogatók élményének fokozását szolgálják. A Burj Khalifa az Egyesült Arab Emírségekben, Dubaiban található az elképesztő, 828 méteres magasságával. A 2010-ben elkészült Burj Khalifát a Skidmore, Owings & Merrill neves építésze, Adrian Smith tervezte. Nemcsak Dubai gyors fejlődésének és fényűzésének szimbóluma, hanem a csúcstechnológia és az okos épülettervezés megtestesítője is. [35]

- Tervezési inspiráció: A Burj Khalifa tervét a Hymenocallis virág ihlette, az épület szerkezete a virág sugárirányú szimmetriájára hasonlít.
- Szerkezeti tervezés: Az épület szerkezete vasbeton torony, nagy teljesítményű beton felhasználásával. Y-alakú alaprajza segít csökkenteni az épületre ható szélerőket.
- Torony: A Burj Khalifa tornya figyelemre méltó építészeti elem, amely nemcsak a teljes magasságához járul hozzá, hanem kommunikációs és műsorszóró toronyként is szolgál.

Okos építési technológiák:

- Felvonórendszer: A világ egyik legfejlettebb liftrendszerével van felszerelve. A liftek a leggyorsabbak közé tartoznak (64,8 km/h), és a leghosszabb utazási távolsággal rendelkeznek az épületben. okos funkciókkal vannak felszerelve a sebesség, a hatékonyság és a kényelem érdekében. [36]
- Klímavezérlés: Az épületben kifinomult klímavezérlő rendszer működik, amely kezeli Dubai szélsőséges hőmérsékletét. A rendszert a hatékonyság és a fenntarthatóság jegyében tervezték, a légkondicionáló rendszerből származó kondenzvíz összegyűjtését az épület kertészeti és kertészeti berendezéseinek öntözésére használja.
- Automatizált világítási és ablaktisztító rendszerek: Az épület automatizált világítási rendszerrel és egyedi ablaktisztító rendszerrel rendelkezik, amelyet a hatalmas magasság és az összetett homlokzat kezelésére terveztek.

Fenntarthatóság:

- Energiahatékonyság: Különböző funkciókat tartalmaz az energiahatékonyság növelése érdekében, beleértve a hőcsökkentő külső burkolatot és a nagy teljesítményű üvegeket a napenergia beáramlásának csökkentése érdekében.
- Vízhatékonyság: Az épület vízrendszerét a fenntarthatóság jegyében tervezték, a kondenzvíz összegyűjtésével és kezelésével az öntözéshez és egyéb felhasználásokhoz.

Biztonsági és védelmi funkciók:

- Tűzbiztonság: A legmodernebb tűzvédelmi rendszerekkel rendelkezik, beleértve a 25 emeletenként elhelyezett, nyomás alatt álló, légkondicionált menedékhelyeket.
- Biztonsági rendszerek: Az épületet fejlett biztonsági rendszerekkel szerelték fel, beleértve a megfigyelő-, beléptető- és kommunikációs hálózatokat, hogy biztosítsák a látogatók biztonságát.

A Burj Khalifa globális ikonná vált, amely Dubai technológiai képességeit és ambiciózus szellemét szimbolizálja. Új mércét állított fel a felhőkarcoló tervezésében, és katalizátora volt a környező terület további városfejlesztésének. Az épület nem csak egy turisztikai látványosság, hanem luxuslakások, vállalati irodák és az Armani Hotel központja is.

Apple Park, Cupertino, USA

Az Apple Park, az Apple Inc. vállalati központja a fenntartható tervezés és az okos technológia lenyűgöző példája. Az épületet teljes egészében megújuló energiával látják el, beleértve a világ egyik legnagyobb napelemes rendszerét. Szellőztető rendszerét úgy tervezték, hogy az év 75%-ában természetes légkondicionálást biztosítson, csökkentve ezzel a hagyományos HVAC-rendszerekre való támaszkodást. A komplexum 98,3%-os BREEAM és 87 pontos LEED platinum értékelést ért el. A kaliforniai Cupertinóban található Apple Park 2017-ben megnyitott és az épületet széles körben elismerik lenyűgöző építészetéről és innovatív dizájnjáról. A főépület szerkezetét, amelyet gyakran "űrhajónak" is neveznek, Steve Jobs álmodta meg, és a híres építész, Norman Foster (Foster + Partners) tervezte. [37]

- Tervezési koncepció: Az Apple Park tervezése a technológia és a természet ötvözésére összpontosít. A gyűrű alakú főépület az innovációt és az Apple előremutató gondolkodásmódját szimbolizálja.

- Tájkép: A campus egy 175 hektáros területen helyezkedik el, és kiterjedt zöldfelülettel rendelkezik, több mint 9000 szárazságtűrő fával és egy nagy központi parkkal. A tervezés célja, hogy elmosódjanak a határok az épület és a természet között.

Fenntarthatóság:

- Energiahatékonyság: Az Apple Park a világ egyik leginkább energiahatékony épülete. Teljesen megújuló energiával működik, beleértve egy 17 megawattos helyszíni napelemes létesítményt.
- Természetes szellőzés: Az épületet úgy tervezték, hogy természetes szellőztető rendszerének köszönhetően az év kilenc hónapjában ne legyen szükség fűtésre vagy légkondicionálásra.

Technológiai innovációk:

- Építőanyagok: A falak a világ legnagyobb ívelt üveglapjaiból készültek, ami átláthatóságot és zökkenőmentes beltéri-kültéri kapcsolatot biztosít.
- Okos épületrendszerek: Az épületet különböző okos világítási, klímavezérlési és biztonsági technológiákkal szerelték fel, amelyek mind az energiahatékonyság és az alkalmazottak kényelmének optimalizálását szolgálják.

Alkalmazotti létesítmények:

- Wellness központ: Egy 100.000 négyzetméteres wellness-központ áll a dolgozók rendelkezésére, beleértve egy edzőtermet és orvosi létesítményeket.
- Együttműködési terek: A tervezés nyitott és kollaboratív munkaterületeket tartalmaz, amelyek célja a kreativitás és a csapatmunka elősegítése.

Biztonság és magánélet:

- Campus biztonság: A kampuszt a biztonság szem előtt tartásával tervezték, ellenőrzött hozzáféréssel és az Apple alkalmazottainak és szellemi tulajdonának magas szintű védelmével.
- Adatbiztonság: Technológiai vállalatként az Apple gondoskodik arról, hogy központja a legkorszerűbb kiberbiztonsági intézkedésekkel legyen felszerelve.

Kulturális és közösségi hatás:

- Látogatóközpont: Az Apple Park látogatóközpontja egy Apple Store-t és egy nyilvános kávézót foglal magában, lehetővé téve a látogatók számára, hogy megismerjék a campus építészeti szépségét.

- Közösségi szerepvállalás: Az Apple Park gyakran ad otthont közösségi eseményeknek és oktatási kezdeményezéseknek, ami tükrözi az Apple elkötelezettségét a közösségi szerepvállalás iránt.

Az Apple Park nem csupán egy vállalati központ; az Apple márkaidentitásának szimbóluma - innováció, kiváló dizájn és fenntarthatóság. Széleskörű elismerést kapott építészeti tervezéséért, környezeti felelősségvállalásáért és a technológia és a természeti elemek integrálásáért. LEED BD+C: Új építés kategoriában, Platinum minősítés.

Összefoglalva, az Apple Park az Apple innováció, a fenntarthatóság és az alkalmazottak jóléte iránti elkötelezettségének bizonyítéka. Tervezése és funkcionalitása új mércét állít a vállalati kampuszok számára, és tükrözi a vállalat vezető szerepét a technológia és a design területén.

Siemens Crystal, London, Egyesült Királyság

A londoni Siemens Crystal a fenntartható városfejlesztés központja és az okos építési technológiák bemutatóhelye. Büszkélkedhet 100%-os elektromos energiaellátással, amelyet napelemekből és földhőszivattyúkból nyernek. Az épület okos infrastruktúrája valós idejű energia- és vízfelhasználás-felügyeleti rendszereket tartalmaz. A 2012-ben hivatalosan megnyitott, feltűnően futurisztikus épület nemcsak a Siemens operatív központjaként, hanem kiállítási központként és városi fenntarthatósági agytrösztként is szolgál. [38]

- Építészeti innováció: A Crystal egyedi, kristályos szerkezetre emlékeztető geometrikus kialakítása több mint látványos. Ez az épület környezetvédelmi stratégiájának funkcionális aspektusa, amely maximalizálja a természetes fényt, miközben minimalizálja a napfény okozta hőnyereséget.
- Fenntarthatósági fókusz: Az épületet úgy tervezték, hogy a világ egyik legfenntarthatóbb épülete legyen, amely mind a BREEAM, mind a LEED tanúsítási rendszerben kiemelkedő minősítést ért el. Napenergiát és földhőszivattyúkat használ, csökkentve ezzel a nem megújuló energiaforrásokra való támaszkodást.
- Víztakarékosság: A Crystal fejlett víztakarékossági technikákat mutat be. Esővízgyűjtő rendszerrel és helyszíni szennyvízkezeléssel rendelkezik, így a városi épületek vízhatékonyságának mintájává vált.

Okos építési technológiák:

- Integrált épületirányítási rendszer: A Crystal működési hatékonyságának középpontjában egy fejlett épületirányítási rendszer áll. Ez a rendszer integrálja a különböző funkciókat, beleértve a klímavezérlést, a világítást és a biztonságot, optimalizálva az energiafelhasználást és biztosítva a munkavállalók kényelmét.
- IoT megvalósítás: Az épületben számos IoT-technológiát alkalmaznak, a környezeti feltételeket figyelő szenzoroktól az energiafogyasztást kezelő okos rendszerekig. Ezek a technológiák nemcsak az épület hatékonyságát növelik, hanem valós idejű adatforrásként is szolgálnak a fenntarthatósági kutatásokhoz 3500 adatponttal.
- Energiahatékonyság: Crystal egy nulla szén-dioxid-kibocsátású épület, részben a technológia innovatív alkalmazásának köszönhetően. Az okos energiagazdálkodási rendszerek, a hatékony LED-es világítás és az automatizált épületvezérlés mind hozzájárulnak a minimális szénlábnyomhoz.

Oktatási és közösségi hatás:

- A nyilvánosság bevonása: A Crystal a városi fenntarthatósággal kapcsolatos oktatási forrásként szolgál, interaktív kiállításokat kínál és konferenciáknak ad otthont. Kulcsfontosságú szerepet játszik abban, hogy a nyilvánosságot és a szakembereket egyaránt bevonja a fenntartható városfejlesztésről szóló vitákba.
- Kutatási és innovációs központ: A kutatás és innováció központjaként a Crystal elősegíti a városi fenntarthatósági megoldásokra összpontosító tanulmányokat és együttműködéseket, élő laboratóriumként kihasználva saját tervezését és technológiáit.

A londoni Siemens Crystal az építészeti innováció, a környezeti fenntarthatóság és az okos épülettechnológia ötvözését példázza. Nemcsak a fenntartható tervezésben megvalósítható eredmények bizonyítéka, hanem a városi élet jövőjének aktív alakítója is.

MOL Campus, Budapest, Magyarország

Az új MOL székház egyedi formában fogja össze a 28 emeletes tornyot és a hozzá tartozó pódiumot, így alkotva egységes, függőleges campust. Az irodaház 28 emeletes, 120 méter magas, és 2500 munkavállalónak ad otthont, szintterülete pedig megközelítőleg 86 ezer négyzetméter.

- Belső terek: Az épület belső tereinek kialakításánál a modern, fenntartható és ideális, az együttműködést támogató munkahely megteremtésének koncepcióját vették alapul.
- Tevékenység-alapú munkahely: Az irodák kialakítása az ABW (Activity-Based Workplace) - tevékenység-alapú iroda modellt követi, azaz a munkavállalók adott feladatuktól függően maguk dönthetnek az épületen belüli változatosan kialakított és különféle hangulatú terek közül az aktuális munkahelyükről, és ezt bármikor rugalmasan változtathatják.

Innovatív műszaki és környezettudatos megoldások:

- Esővíz elvezetés: Az esővíz 100%-át helyben kezelik, egy részét a zöldfelületek szívják fel, a többit pedig az épület pincéjében gyűjtik össze, majd öntözésre és az épületben kiépített szürkevíz-hálózat segítségével WC-öblítésre használják – ezzel csökkentve a városi csatornarendszer terhelését és az öntözéshez, valamint öblítéshez felhasznált ivóvíz mennyiségét.
- Megújuló energiák hasznosítása: Az épület éves hűtés-fűtés energiafogyasztásának körülbelül 40%-át fedezi a talajszondás hőszivattyús rendszer. A tetőn elhelyezett napelemekkel az éves villamosenergia-fogyasztás 5-6%-a megtakarítható, a maradék villamosenergia igényt pedig 100%-ban zöldenergia forrásból vásárolják.
- Épített szerkezetek energiatudatos megoldásai: A tervezés során kiemelt szempont volt az anyaghatékonysági és a funkcionális adaptációs tervezési elvek érvényesítése. Az alkalmazott szerkezeti megoldások úgy teszik lehetővé a későbbi átépítések, karbantartások, javítások elvégzését, hogy ezekhez csupán minimális bontási munkálatokat kell elvégezni, ezáltal növelve a szerkezetek élettartamát és csökkentve a keletkező hulladékot.
- Hulladékenergia hasznosítása, hővisszanyerés és egyéb energia hasznosítás: Az épületben a központi légtechnikai rendszer által elhasznált irodai levegő, amely már előfűtötte a friss levegőt, a parkolószintek fűtésénél kerül hasznosításra. A konyhatechnológiai folyamatok során felszabaduló nagy mennyiségű és magas hőmérsékletű hulladékhő kidobás előtt, hőcserélőn keresztül hasznosításra kerül a beszívott kinti friss levegő felfűtésére.
- Napenergia: A pódium épületrész tetejére összesen több mint 700 db napelem került telepítésre, melyek összteljesítménye 270 kWp.

- Anyagfelhasználás: A toronyház építése során az építési hulladék 98%-át sikerült újrahasznosítani. A felhasznált építőanyagok több mint 23%-a újrahasznosított anyagból készült.

Épületautomatizálás:

- BMS: Az épület gépészeti rendszereit egy központi automatika rendszer szabályozza, folyamatosan a lehető legalacsonyabb energiafogyasztás mellett biztosítva az előírt beltéri komfortkövetelmények teljesülését.
- Légtechnika: Az irodákban, tárgyalókban és a nagy befogadó képességű termekben CO2-érzékelőkről szabályozott VAV-rendszerekkel, illetve a légkezelők frekvenciaváltós ventilátorainak fordulatszám csökkentésével biztosítják a szükséges frisslevegő-mennyiséget. Ezáltal az épület tényleges kiterheltségéhez igazítható a légkezelők energiafogyasztása.
- HVAC: A hűtési-fűtési rendszer fel van készítve free-colling működésre, azaz a kompresszor munkája nélküli hűtés-fűtésre is. A rendszer átmeneti időben a talajszondákból érkező víz keringtetésével, a frisslevegő minimális kezelésével, vagy a hűtőtornyok megfelelő szabályozásával a keringtetésen felüli plusz energiák nélkül temperálja az épületet.

Hazánkban egyedülállóan sikeresen megszerezte mind a LEED Platinum, mind a BREAM Excellent minősítést is az olyan innovatív megoldásoknak köszönhetően, mint a 900 m2 napelem, a geotermikus energiát használó hűtési és fűtési rendszer, valamint a szürkevíz újrahasznosítás.

Ezek a példák az okos épületfejlesztés élvonalát képviselik, és mindegyikük egyedülálló módon járul hozzá a területhez. Bemutattam, hogy a technológiát nemcsak a hatékonyság és a kényelem, hanem a fenntarthatóság és a munkavállalók jóléte érdekében is hasznosítani.

1.8. A mesterséges intelligencia szerepe az okos épületekben

A mesterséges intelligencia és a prediktív tanulás átalakító szerepét vizsgálom és mutatom be az okos épületek területén. A mesterséges intelligencia gyors fejlődése az épületek irányításának új korszakát nyitotta meg, ahol az adatvezérelt meglátásokat és a gépi tanulási algoritmusokat az épületek hatékonyságának, fenntarthatóságának és a munkavállalók kényelmének fokozására használják fel. A mesterséges intelligencia jelenlegi állapota a számítási teljesítmény, a fejlett algoritmusok és a hatalmas mennyiségű adat elérhetőségének figyelemre méltó konvergenciáját jelenti. Ez a

konvergencia az elméleti kutatásokból a gyakorlati alkalmazások felé mozdította el a mesterséges intelligenciát, ami hatással van a különböző iparágakra, köztük az okos épületek irányítására. A gépi tanulás (ML) során az algoritmusok komplex adathalmazok elemzésére fejlesztették ki, lehetővé téve az MI-rendszerek számára, hogy adatokból tanuljanak és az adatok alapján előrejelzéseket készítsenek. Az okos épületekben az ML-t elsősorban az energiafogyasztási minták elemzésére használják. A mély tanulás (deep learning - DL) az ML egy alcsoportja, a mély tanulás többrétegű neurális hálózatokat használ. A számítógépes látás és a természetes nyelvfeldolgozás fejlődésében játszott fontos szerepet, segítve a kifinomult épületautomatizálási rendszereket. A természetes nyelvi feldolgozás javította a felhasználók és az épületirányítási rendszerek közötti interakciót, lehetővé téve a hangvezérelt automatizálást és az okos asszisztenseket. A mesterséges intelligencia által vezérelt számítógépes látás forradalmasítja az épületbiztonsági rendszereket, lehetővé téve az arcfelismerést és az anomáliák felismerését. Az ML-nek és a DL-nek adatokra van szüksége a modellek képzéséhez. A kifejlesztett modellek pontossága és sokoldalúsága nagymértékben függ a jó adatkészlettől. A végponttól végpontig tartó ML/DL-modellek telepítése során az idő nagy részét az adatállományra kell fordítani, amely magában foglalja az adatgyűjtést, tisztítást, elemzést, vizualizálást és a jellemzőtervezést. [36][37][38][39]

Az okos épületek területén a mesterséges intelligencia integrálása átalakító változást jelent az adaptívabb és érzékenyebb környezetek felé. A mesterséges intelligencia képessége a különböző épületérzékelőkből származó hatalmas mennyiségű adat feldolgozására és elemzésére lehetővé teszi az energiagazdálkodás árnyaltabb megközelítését, a fogyasztás optimalizálását az épületben tartózkodók komfortérzetének fenntartása mellett. A mesterséges intelligencia által vezérelt prediktív karbantartási algoritmusok bevezetése előrelépést jelent az épületüzemeltetésben, előre látva a lehetséges rendszerhibákat és csökkentve a karbantartási igényt és esetleges üzemszüneteket. A mesterséges intelligencia a környezeti beállítások személyre szabásával is javítja az épületben tartózkodók élményét, a gépi tanulás segítségével alkalmazkodva az egyéni preferenciákhoz és használati szokásokhoz. Továbbá a mesterséges intelligencia integrálása az okos épületek biztonsági rendszereibe a fejlett felügyelet és az anomáliák észlelése révén erősíti az általános biztonsági és védelmi intézkedéseket. [41] A mesterséges intelligenciával támogatott, okos épületekben végzett prediktív karbantartás ugrást jelent az épületüzemeltetési gyakorlatban. Ez a megközelítés magában foglalja a korábban ismertetett mesterséges intelligencia algoritmusok

alkalmazását az épületrendszerek adatainak elemzésére és a lehetséges karbantartási problémák előrejelzésére, mielőtt azok bekövetkeznének. A hagyományos reaktív karbantartással ellentétben a prediktív karbantartás előre jelzi a problémákat, ezáltal csökkenti az állásidőt és meghosszabbítja a berendezések élettartamát. Az okos épületekben a prediktív karbantartás a mesterséges intelligenciát használja a különböző érzékelők és rendszerek adatainak feldolgozására és értelmezésére. Ezek az érzékelők olyan körülményeket ellenőriznek, mint a hőmérséklet, a páratartalom, a rezgés és az energiafogyasztás. Ezen adatok elemzésével az MI-algoritmusok olyan mintákat és anomáliákat azonosíthatnak, amelyek a berendezések közelgő meghibásodására vagy karbantartás szükségességére utalhatnak. [39][69]

MI-technológiák a prediktív karbantartásban

- Gépi tanulási algoritmusok: A gépi tanulási modellek, különösen azok, amelyek idősoros adatokkal dolgoznak, alkalmasak a berendezések meghibásodását megelőző minták felismerésére. Például a HVAC-rendszereknél a rezgés vagy a hőmérséklet növekedése jelezheti a karbantartás szükségességét.
- Mélytanulás és neurális hálózatok: A mélytanulás, a gépi tanulás egy részhalmaza, többrétegű neurális hálózatokat használ összetett adathalmazok elemzésére. Ez a megközelítés különösen hatékony a különböző épületérzékelőkből származó nagy mennyiségű adat feldolgozásában és értelmezésében.
- Természetes nyelvi feldolgozás: Az NLP-t a karbantartási naplók és jelentések elemzésére használják, és olyan értékes meglátásokat vonnak ki belőlük, amelyek javíthatják a prediktív karbantartási algoritmusokat.

A prediktív karbantartás alkalmazásai az okos épületekben

- HVAC-rendszerek: A mesterséges intelligencia algoritmusok elemzik a HVAC-rendszerek adatait, hogy előre jelezzék az olyan problémákat, mint a szűrő eltömődése, a hűtőközeg szivárgása vagy a mechanikai kopás. Ez a proaktív megközelítés optimális teljesítményt és energiahatékonyságot biztosít. [43], [44], [45]
- Liftkarbantartás: Az okos épületekben az érzékelőkkel felszerelt felvonók adatokat szolgáltatnak a használati szokásokról, az ajtók működéséről és a motor állapotáról. A mesterséges intelligencia elemzi ezeket az adatokat, hogy előre jelezze a karbantartási igényeket, ezáltal csökkentve az üzemzavarok kockázatát és növelve a biztonságot. [43], [44], [45]

- Elektromos rendszerek: A mesterséges intelligencia figyeli az elektromos rendszereket, és azonosítja az olyan potenciális problémákat, mint az áramkörök túlterhelése vagy az áramellátás ingadozása. E problémák korai felismerése megelőzheti a problémákat, és biztosíthatja az épület zavartalan működését. [43], [44], [45]

A megelőző karbantartás előnyei

- Költségmegtakarítás: A karbantartási problémák korai előrejelzésével és kezelésével az okos épületek elkerülhetik a költséges javításokat és a leállásokat. Ez a megközelítés idővel költségmegtakarítást eredményez. [46]
- Megnövelt élettartamú berendezések: A pontos előrejelzések által vezérelt rendszeres karbantartás meghosszabbítja az épületberendezések élettartamát, ami hosszú távú pénzügyi előnyökkel jár. [46]
- Javított biztonság és kényelem: A megelőző karbantartás biztosítja, hogy az épületrendszerek megbízhatóan és hatékonyan működjenek, növelve a munkavállalók biztonságát és kényelmét. [46]

Kihívások

- Az adatok minősége és mennyisége: A megelőző karbantartás hatékonysága az összegyűjtött adatok minőségétől és mennyiségétől függ. A nem megfelelő vagy pontatlan adatok téves előrejelzésekhez vezethetnek. [47]
- Integráció a meglévő rendszerekkel: A mesterséges intelligencia alapú előrejelző karbantartás integrálása a meglévő épületirányítási rendszerekbe kihívást jelenthet, mivel műszaki szakértelmet és befektetést igényel. [48]
- Szakképzett munkaerő: A mesterséges intelligencia alapú előrejelző karbantartási rendszerek bevezetéséhez és irányításához olyan munkaerőre van szükség, amely a mesterséges intelligencia és az épületrendszerek területén speciális készségekkel rendelkezik.

Az okos épületekben a mesterséges intelligencia által támogatott prediktív karbantartás forradalmasítja az épületek irányítását. Számos előnnyel jár, többek között költségmegtakarítással, a berendezések élettartamának növelésével és a kényelem javításával. A sikeres megvalósítás azonban az adatminőség, a rendszerintegráció és a munkaerő készségeinek gondos mérlegelését igényli.

Az okos épületek mesterséges intelligenciával kiegészített energiagazdálkodása kritikus fontosságú eleme a hatékonyságra, fenntarthatóságra és költséghatékonyságra való

törekvésnek. Az MI szerepe az energiagazdálkodásban az adatok okos elemzését jelenti az energiafelhasználás optimalizálása, a pazarlás csökkentése és az optimális környezeti feltételek fenntartása érdekében.

A mesterséges intelligencia átalakítja az okos épületek energiagazdálkodását azáltal, hogy lehetővé teszi az energiarendszerek dinamikus és előrejelző vezérlését. Ez nemcsak a feladatok automatizálását jelenti, hanem a valós idejű adatokon és előrejelző elemzéseken alapuló okos döntéshozatalt is.

- Gépi tanulás az előrejelző elemzéshez: A gépi tanulási algoritmusok múltbeli és valós idejű adatokat elemeznek a jövőbeli energiaszükségletek előrejelzése érdekében. Például a múltbeli energiafelhasználási minták és az időjárás-előrejelzések elemzésével a mesterséges intelligencia képes optimalizálni a HVAC-rendszereket az időjárás várható változásaihoz.
- Mélytanulás a komplex adatok értelmezéséhez: A mélytanulási modellek, különösen a konvolúciós neurális hálózatok, alkalmasak az összetett adathalmazok, például a különböző épületérzékelőkből származó adatok értelmezésére. Ez a képesség kulcsfontosságú az energiafelhasználási minták megértésében és előrejelzésében. [47]
- Megerősítő tanulás az optimalizáláshoz: A megerősítő tanulást, a mesterséges intelligencia egy olyan típusát, amelyben az algoritmusok próbálgatással és hibával tanulnak meg döntéseket hozni, az energiatakarékosság optimális stratégiáinak megtalálására használják. Például egy mesterséges intelligencia rendszer megtanulhatja a leghatékonyabb módját az energiafelhasználás kiegyensúlyozásának a különböző épületzónák között. [49]

A mesterséges intelligencia alkalmazásai az energiagazdálkodásban

- HVAC rendszer optimalizálása: A mesterséges intelligencia algoritmusok dinamikusan beállítják a HVAC-műveleteket a foglaltság, az időjárási viszonyok és más környezeti tényezők alapján csökkentve az energiafogyasztást, miközben fenntartják a komfortérzetet. [50]
- Világításvezérlés: A mesterséges intelligencia vezérelt világítási rendszerek elemzik a foglaltsági mintákat és a természetes fényszinteket a mesterséges világítás beállításához, ezáltal energiát takarítanak meg anélkül, hogy a dolgozók komfortérzetét veszélyeztetnék. [51]

- Energiaigény-előrejelzés: A mesterséges intelligencia modellek előre jelzik az energiaigény csúcs- és mélypontjait, lehetővé téve az okos épületek számára, hogy kiigazítsák energiafogyasztási szokásaikat, részt vegyenek a keresletre reagáló programokban, vagy energiát tároljanak a csúcsidőszakokon kívüli időszakokban. [51]

A mesterséges intelligencia előnyei az energiagazdálkodásban

- Fokozott energiahatékonyság: A mesterséges intelligencia által vezérelt rendszerek biztosítják, hogy az energiát csak akkor és ott használják fel, ahol és amikor arra szükség van, ami a pazarlás és a költségek csökkenéséhez vezet. [52]
- Csökkentett működési költségek: Az energiafelhasználás optimalizálásával az AI hozzájárul a közüzemi számlák és az üzemeltetési költségek csökkenéséhez pénzügyi előnyöket kínálva az épületek tulajdonosainak és használóinak. [52]
- Hozzájárulás a fenntarthatósághoz: A hatékony energiagazdálkodás összhangban van a fenntarthatósági célokkal, csökkenti az épületek szénlábnyomát és hozzájárul a környezetvédelemhez. [52]

Kihívások közé tartozik az adatvédelem és biztonság. A nagy mennyiségű adat gyűjtése és elemzése aggályokat vet fel a magánélet védelmével és biztonságával kapcsolatban. Ezen adatok védelmének biztosítása kiemelten fontos. [16][78] Az MI-alapú energiagazdálkodási rendszerek integrálása a meglévő épületinfrastruktúrába összetett lehet, és gondos tervezést és kivitelezést igényel. [48] Az energiagazdálkodási MI-technológiákba történő kezdeti beruházás lehet, bár a hosszú távú megtakarítások gyakran igazolják a kiadásokat. Az okos épületek mesterséges intelligenciával támogatott energiagazdálkodása az épületek üzemeltetésének előremutató megközelítését jelenti. Számos előnnyel jár, beleértve a hatékonyság növelését, a költségek csökkentését és a fenntarthatósághoz való hozzájárulást. A megvalósítás során azonban óvatosan kell eljárni, figyelembe véve olyan tényezőket, mint az adatbiztonság, az integrációs kihívások és a kezdeti költségek.

A mesterséges intelligenciával kiegészített okos épületek komfortja gyorsan fejlődő terület, amely az optimális élet- és munkakörnyezet megteremtésére összpontosít. A MI szerepe ezen a területen túlmutat a puszta hőmérsékletszabályozáson, és a környezetszabályozás, a személyre szabott beállítások és a jólét holisztikus megközelítését foglalja magában. Lehetővé téve az okos épületek számára, hogy tanuljanak a felhasználók preferenciáiból és viselkedéséből, és alkalmazkodjanak

azokhoz. Ez az adaptív megközelítés biztosítja, hogy az épületek belső környezete ne csak hatékony legyen, hanem az egyéni igényekhez is igazodjon. [17]

A kényelmet fokozó MI-technológiák

- Gépi tanulás a személyre szabásért: A gépi tanulási algoritmusok elemzik a bent tartózkodók viselkedését és preferenciáit, hogy személyre szabják a környezeti beállításokat, például a hőmérsékletet, a világítást és a levegő minőségét. Például egy mesterséges intelligencia rendszer megtanulhatja az egyén preferált hőmérsékleti beállításait, és ennek megfelelően állíthatja be a HVAC rendszert.
- Előrejelző analitika a környezetszabályozáshoz: A prediktív analitikát a külső körülmények, például az időjárás változásainak előrejelzésére és az azokra való reagálásra használják, hogy fenntartsák az állandó belső komfortfokozatot. Ez magában foglalja a fűtési vagy hűtési rendszerek megelőző beállítását a várható hőmérséklet-ingadozások ellensúlyozására.
- Érzékelők integrálása a valós idejű beállításhoz: Az MI integrálja a különböző érzékelők (pl. hőmérséklet, páratartalom, fény, mozgás) adatait, hogy valós idejű beállításokat végezzen az épület környezetében, biztosítva a folyamatos kényelmet.

A mesterséges intelligencia alkalmazásai a kényelem fokozásában

- HVAC rendszer optimalizálása: A mesterséges intelligencia által vezérelt HVAC-rendszerek dinamikusan alkalmazkodnak az optimális hőmérséklet és levegőminőség fenntartásához, figyelembe véve olyan tényezőket, mint a foglaltság, a napszak és a külső időjárási körülmények.
- Okos világítási rendszerek: A mesterséges intelligencia vezérelt világítási rendszerek a természetes fény elérhetősége, a napszak és a felhasználók preferenciái alapján állítják be a fényerőt és a színhőmérsékletet, hozzájárulva a kényelemhez és az energiahatékonysághoz.
- Akusztikai kényelem: Az MI-algoritmusok képesek az épületeken belüli hangszintek kezelésére, csökkentve a zajszennyezést és növelve a munkavállalók akusztikai kényelmét.

A mesterséges intelligencia előnyei a komfort terén

- Fokozott jólét: Az optimális környezeti feltételek fenntartásával az AI hozzájárul az épületben tartózkodók fizikai és pszichológiai jólétéhez.

- Fokozott termelékenység: A mesterséges intelligencia által elősegített kényelmes munkakörnyezet a felhasználók körében megnövekedett termelékenységet és csökkentett stresszt eredményezhet.
- Személyre szabott élmények: Az MI lehetővé teszi a környezeti beállítások egyéni preferenciákhoz való igazítását, személyre szabott élményt nyújtva minden egyes felhasználó számára.

Kihívások

- A személyre szabás és az adatvédelem egyensúlya: Miközben a személyre szabás növeli a kényelmet, adatgyűjtést igényel, ami adatvédelmi aggályokat vet fel, amelyeket kezelni kell.
- A rendszer összetettsége és megbízhatósága: A mesterséges intelligencia által vezérelt kényelmi rendszerek összetettsége megbízható üzemeltetést és karbantartást tesz szükségessé a folyamatos kényelem biztosítása érdekében.
- Inkluzivitás és hozzáférhetőség: Az MI-rendszereket úgy kell megtervezni, hogy minden személy különböző igényeit kielégítsék, biztosítva az inkluzivitást és a hozzáférhetőséget.

A mesterséges intelligencia által működtetett okos épületekben a komfort olyan terület, amely javítja az életminőséget az épített környezetben. Miközben számos előnnyel jár, beleértve a fokozott jólétet és a személyre szabhatóságot, olyan kihívásokat is jelent, amelyek gondos mérlegelést igényelnek, különösen a magánélet védelme és a rendszer összetettsége tekintetében.

Összefoglalva, ebben a fejezetben az okos épületek, az IoT-technológia és a mesterséges intelligencia közötti kapcsolatot vizsgáltam, kiemelve, hogy ezek a komponensek szinergiájukkal hogyan határoznak meg egy új, modern infrastruktúrát. Feltártam az IoT alapvető szerepét az okos épületek különböző elemeinek összekapcsolásában. Bemutattam, hogy a mesterséges intelligencia integrációjával tovább erősíthető ez az ökoszisztéma. Fejlett elemzési és tanulási képességekkel biztosítva az épületek optimalizált irányításához és üzemeltetéséhez. Kiemeltem továbbá e technológiáknak az épületek hatékonyságára, fenntarthatóságára és az élményére gyakorolt átalakító hatását. Kitértem az ilyen integrált rendszerek megvalósításával kapcsolatos kihívásokra is, hangsúlyozva a biztonság, az interoperabilitás és az etikai megfontolások fontosságát. Végül a fejezet átfogó képet ad a városi építészet jövőjéről az IoT és a mesterséges intelligencia intelligens épületekbe történő integrációjának szemszögéből.

2. KIBERBIZTONSÁGI KERETRENDSZEREK VIZSGÁLATA

Kiberbiztonsági szakemberként egyik fő célom, hogy a szakma legfőbb területeit átlássam és ismerjem. Ebben a fejezetben az okos épületek és a kiberbiztonság szoros kapcsolatát vizsgáltam az épületautomatizálási rendszerek, hálózati elemek és adatok védelme érdekében a különféle kibertámadások aspektusából. Ez számos olyan gyakorlatot, technológiát és folyamatot fed le, amelyek célja az információk integritásának, bizalmasságának és rendelkezésre állásának védelme az okos épületek ökoszisztémáin belül.

2.1. A kiberbiztonság alapjai

A kiberbiztonság alapja a CIA-modell - a bizalmasság, az integritás és a rendelkezésre állás – elveire épül a hálózati, alkalmazási és végponti biztonsági intézkedések mellett. Ebben az alfejezetben ezeket az alapvető fogalmakat ismertetem, és rávilágítok a jelentőségükre az okos épületek kiberbiztonságának összefüggésében.

A CIA-modell

- Bizalmasság (confidentiality): Az okos épületek bizalmassága magában foglalja annak biztosítását, hogy az érzékeny adatokhoz, például a dolgozók adataihoz és az üzemeltetési részletekhez csak az arra jogosult személyek férjenek hozzá. Ez alapvető fontosságú a jogosulatlan hozzáférés és az adatsértések megelőzésében. A titkosítási technológiák, a hozzáférés-szabályozás és a biztonságos hitelesítési protokollok a titkosság védelmét szolgálják. [31]
- Sértetlenség (integrity): Az sértetlenség az okos épületrendszereken belüli adatok pontosságára és megbízhatóságára utal. Létfontosságú annak biztosítása, hogy az összegyűjtött adatokat ne lehessen manipulálni vagy megváltoztatni. Az adatok integritásának fenntartására olyan technikákat használnak, mint az ellenőrző összegek (checksums), a digitális aláírások és az audit nyomvonalak, biztosítva, hogy az épület működését vezérlő információk pontosak és megbízhatóak legyenek. [31]
- Rendelkezésre állás (availability): A rendelkezésre állás biztosítja, hogy az épület rendszerei és adatai szükség esetén az arra jogosult felhasználók számára hozzáférhetőek legyenek. Ez a szempont kritikus fontosságú az épület alapvető funkcióinak folyamatos működése szempontjából. A redundancia, a failover

rendszerek és a rendszeres karbantartás olyan stratégiák, amelyeket az okos épületrendszerek magas rendelkezésre állásának biztosítására alkalmaznak. [31]

5. ábra: CIA-modell

Célkitűzés	Alacsony hatás	Mérsékelt hatás	Nagy hatás
Bizalmasság	Az információk jogosulatlan nyilvánosságra hozatala várhatóan korlátozott, hátrányos hatást gyakorol a szervezeti működésre, a szervezeti eszközökre vagy egyénekre.	Az információk jogosulatlan nyilvánosságra hozatala várhatóan súlyosan káros hatással lenne a szervezeti működésre, a szervezeti vagyonra vagy egyénekre.	Az információk jogosulatlan nyilvánosságra hozatala várhatóan súlyos vagy katasztrofális káros hatást gyakorolna a szervezeti működésre, a szervezeti eszközökre vagy egyénekre.
Sértetlenség	Az információk jogosulatlan módosítása vagy megsemmisítése várhatóan korlátozottan káros hatással lesz a	Az információk jogosulatlan módosítása vagy megsemmisítése várhatóan súlyos káros hatással lehet a szervezeti	Az információk jogosulatlan módosítása vagy megsemmisítése várhatóan súlyos vagy katasztrofális káros hatással lehet

	szervezeti működésre, a szervezeti eszközökre vagy az egyénekre.	működésre, a szervezeti eszközökre vagy az egyénekre.	a szervezeti működésre, a szervezeti eszközökre vagy egyénekre.
Rendelkezésre állás	Az információkhoz vagy információs rendszerekhez való hozzáférés vagy azok használatának megszakadása várhatóan korlátozottan káros hatással lesz a szervezeti működésre, a szervezeti eszközökre vagy az egyénekre.	Az információkhoz vagy egy információs rendszerhez való hozzáférés vagy azok használatának megszakadása várhatóan súlyos káros hatással lesz a szervezeti működésre, a szervezeti eszközökre vagy az egyénekre.	Az információkhoz vagy információs rendszerekhez való hozzáférés vagy azok használatának megszakadása várhatóan súlyos vagy katasztrofális káros hatással lesz a szervezeti működésre, a szervezet vagyonára vagy egyénekre.

1. táblázat: CIA-modell hatásszintjeinek magyarázata

A hálózat-, az alkalmazás- és a végpontbiztonság kritikus összetevői elengedhetetlenek az okos épületek összekapcsolt ökoszisztémáinak védelméhez. Továbbiakba a védelem különböző rétegeit vizsgálom, amelyek a kiberfenyegetések ellen más-más szinteken nyújtanak védelmet, a tágabb hálózati infrastruktúrától az egyes alkalmazásokig és az egyes végponti eszközökig. Hangsúlyozva e biztonsági rétegek összetettségét és kölcsönös függőségét, elemezve szerepüket az okos épületrendszereken belüli adatok integritásának, bizalmas jellegének és rendelkezésre állásának biztosításában.

Hálózat-, alkalmazás- és végpontbiztonság

- Hálózatbiztonság: Az okos épületek hálózati biztonsága magában foglalja az alapul szolgáló hálózati infrastruktúra védelmét az olyan fenyegetésekkel szemben, mint a behatolások, támadások és az illetéktelen hozzáférés. A hálózati biztonság gerincét tűzfalak, behatolásérzékelő és -megelőző rendszerek (IPS/IDS) és biztonságos hálózati protokollok alkotják. Például az erős titkosítási és

hitelesítési módszerekkel ellátott biztonságos Wi-Fi hálózat megvalósítása alapvető fontosságú a jogosulatlan hozzáférés megakadályozásában. [31]

- Hálózati hozzáférés-szabályozás (NAC): A NAC-rendszereket arra használják, hogy ellenőrizzék, mely eszközök csatlakozhatnak az épület hálózatához. A hálózati hozzáférés engedélyezése előtt értékelik az eszköz megfelelőségét, és így érvényesíthetik a biztonsági irányelveket. A NAC segítségével biztosítható, hogy csak engedélyezett és megfelelő IoT-eszközök, például okos világítási rendszerek csatlakozzanak az épület hálózatához, ami növeli az általános biztonságot.
- Fejlett tűzfal: Az alapvető tűzfalvédelmen túl az okos épületek olyan fejlett tűzfal-technológiákat igényelnek, amelyek képesek a rosszindulatú adatforgalom ellenőrzésére és kiszűrésére, nemcsak a periférián, hanem a belső hálózaton belül is. Ide tartoznak az új generációs tűzfalak (NGFW), amelyek képesek a mély csomagvizsgálatra és az alkalmazásszintű biztonságra.
- Behatolásfelderítő és -megelőző rendszerek (IDS/IPS): Az IDS/IPS kritikus szerepet játszik a potenciális fenyegetések valós idejű azonosításában és mérséklésében. Az okos épületekben ezeknek a rendszereknek képesnek kell lenniük a kifinomult támadások észlelésére, beleértve az IoT-eszközöket és az épületirányítási rendszereket célzó támadásokat is.
- Biztonságos hálózati protokollok: A biztonságos hálózati protokollok megvalósítása alapvető fontosságú. Az olyan protokollok, mint a TLS az adattitkosításhoz és a biztonságos MQTT (Message Queuing Telemetry Transport) az IoT-kommunikációhoz biztosítják, hogy a hálózaton keresztül továbbított adatok védve legyenek a lehallgatással és a manipulációval szemben.
- Hálózati szegmentálás: Az épület hálózatának különböző zónákra történő szegmentálása, amelyek mindegyike saját biztonsági ellenőrzéssel rendelkezik, kulcsfontosságú az esetleges betörések megfékezéséhez. Például a HVAC-rendszerek, a biztonsági rendszerek és a felhasználók adatai szegmentálhatók, hogy megakadályozzák, hogy az egyik rendszerben bekövetkező sérülés hatással legyen a többi rendszerre.

- Vezeték nélküli kommunikáció: A vezeték nélküli technológiák elterjedésével az okos épületekben a Wi-Fi hálózatok biztosítása kritikus fontosságú. Ez magában foglalja a WPA3 (Wi-Fi Protected Access 3) használatát a titkosításhoz, az erős hozzáférés-ellenőrzés megvalósítását és az illetéktelen hozzáférési pontok rendszeres ellenőrzését. Utóbbi kiemelten fontos, hiszen a 2018-ban megjelent WPA2 KRACK sérülékenység világszerte több millió eszközt érintett egészen addig amíg nem lettek frissítve, vagy lecserélve. [54] A Wi-Fi mellett a kis hatótávolságú kommunikációra általánosan használt Bluetooth-technológia szigorú biztonsági intézkedéseket tesz szükségessé. Ez magában foglalja a Bluetooth Low Energy (BLE) használatát fejlett titkosítási szabványokkal és biztonságos párosítási protokollokkal a lehallgatás és a "man-in-the-middle" támadások megelőzése érdekében. A Zigbee, egy alacsony fogyasztású vezeték nélküli kommunikációs protokoll, amelyet alacsony energiafogyasztása és hálós hálózati képességei miatt széles körben használnak az IoT-eszközökben. A Zigbee-hálózatok biztonsága AES-128 titkosítással, kulcskészítési protokollokkal és eszközhitelesítési mechanizmusokkal érhető el az illetéktelen hozzáférés és az adatok megsértése elleni védelem érdekében. A Z-Wave, egy másik, az automatizálásban használt vezeték nélküli protokoll, olyan biztonsági funkciókat tartalmaz, mint a Security 2 (S2) keretrendszer. Ez a keretrendszer javítja a titkosítást, biztonságos kulcscsere-mechanizmusokat tartalmaz, és jobb ellenőrzést biztosít az eszközök hálózatba való bevonása felett

- Alkalmazásbiztonság: Az alkalmazásbiztonság annak biztosítására összpontosít, hogy az okos épületekben használt szoftveralkalmazások biztonságosak és sebezhetőségektől mentesek legyenek. Ez magában foglalja a rendszeres biztonsági auditokat, a kód felülvizsgálatát és az alkalmazás tűzfalak használatát. A biztonságos kódolási gyakorlatok kulcsfontosságúak az épületautomatizálási rendszereket kezelő alkalmazások fejlesztése során, biztosítva, hogy azok ne legyenek fogékonyak az olyan támadásokra, mint az SQL-injekció vagy a cross-site scripting. [31][82]
    - DevSecOps integráció: DevSecOps, azaz a biztonsági gyakorlatok integrálása a DevOps-folyamatba, alapvető fontosságú az okos épületek

alkalmazásbiztonsága szempontjából. Ez a megközelítés biztosítja, hogy a biztonsági protokollok a szoftverfejlesztés teljes életciklusába beágyazódjanak, a kezdeti tervezéstől a telepítésig és a karbantartásig. A DevSecOps beépítése az okos épületrendszerekben, ahol a szoftverek olyan kritikus funkciókat vezérelnek, mint a HVAC, a világítás és a biztonság, folyamatos biztonsági felügyeletet és gyors reagálást jelent az ezekben az alkalmazásokban felfedezett sebezhetőségekre.

- Folyamatos integráció és folyamatos telepítés (CI/CD): A CI/CD a szoftverfejlesztésben lehetővé teszik a gyakori és megbízható kódfrissítéseket. A biztonság integrálása a CI/CD folyamatokba biztosítja, hogy minden egyes frissítés alapos biztonsági ellenőrzéseken menjen keresztül, beleértve az automatikus kódvizsgálatot és a sebezhetőségi értékelést. A CI/CD megkönnyítik a biztonsági frissítések és javítások gyors bevezetését, ami elengedhetetlen az épületautomatizálási rendszerek integritásának és biztonságának fenntartásához a fejlődő kiberfenyegetésekkel szemben.
- Harmadik féltől származó könyvtárak kezelése (3rd-party library): A harmadik féltől származó könyvtárak és keretrendszerek használata gyakori az alkalmazásfejlesztés során. Ezek a könyvtárak azonban sebezhetőségeket rejthetnek, így e kockázat csökkentéséhez elengedhetetlen a harmadik féltől származó komponensek szigorú biztonsági ellenőrzése, rendszeres frissítése és javítása. Az okos épületek alkalmazásainál, ahol harmadik féltől származó könyvtárakat használhatnak olyan funkciókhoz, mint az adatelemzés vagy a felhasználói felület kialakítása, ezen összetevők biztonságának biztosítása létfontosságú az esetleges jogsértések megelőzése érdekében.
- Proaktív sebezhetőség-megelőzés: A biztonságos kódolási gyakorlatok proaktív intézkedéseket foglalnak magukban a sebezhetőségek, például az SQL-injekció vagy a cross-site scripting megelőzésére. Ez magában foglalja a bemeneti érvényesítést, a kimeneti kódolást és a paraméterezett lekérdezések használatát. Az okos épületirányítási rendszerek esetében a biztonságos kódolás megakadályozza, hogy a támadók a sebezhetőségeket kihasználva jogosulatlan hozzáférést vagy irányítást szerezzenek az épületrendszerek felett.

- Végpontvédelem: A végpontvédelem az épület hálózatához csatlakozó egyes eszközök, például érzékelők, vezérlők és felhasználói kezelőpanelek védelmére vonatkozik. Ez magában foglalja a vírusirtó szoftverek használatát, a rendszeres javításokat és a biztonságos konfigurációt. A végpontbiztonság egyik legfontosabb szempontja például annak biztosítása, hogy az épületben lévő IoT-eszközök naprakész firmware-rel rendelkezzenek, és erős jelszavakkal legyenek konfigurálva. [31]
    - Átfogó végpontbiztonsági stratégia: Az okos épületekben a végpontok védelme túlmutat a hagyományos vírusirtó megoldásokon. Többrétegű biztonsági megközelítést foglal magában, amely fejlett fenyegetésérzékelést, viselkedéselemzést és gépi tanulási algoritmusokat tartalmaz az IoT-eszközöket és más végpontokat célzó kifinomult kiberfenyegetések azonosítása és mérséklése érdekében. Az épületek okos HVAC-rendszerei és beléptetőpaneljei például fejlett végpontvédelmi eszközökkel vannak felszerelve, amelyek képesek észlelni a működési mintákban mutatkozó anomáliákat, amelyek potenciális biztonsági réseket jeleznek.
    - Integráció az épületirányítási rendszerekkel (BMS): A végpontvédelmi megoldásokat a központosított felügyelet és kezelés érdekében integrálni kell a BMS-be. Ez az integráció lehetővé teszi a biztonsági eseményekre való összehangolt reagálást az összes végponton. A BMS-szel való integráció lehetővé teszi a végpontok, például az okos mérőórák valós idejű biztonsági felügyeletét, így az épület üzemeltetői átfogó képet kapnak az összes csatlakoztatott eszköz biztonsági állapotáról.

A kiberbiztonság alapjainak megértése, különösen a CIA-modell és a hálózati, az alkalmazási és a végponti biztonság szintjeinek megértése alapvető fontosságú az okos épületek kiberfenyegetésekkel szembeni védelmében. Ahogy az okos épületek tovább fejlődnek, és fejlett technológiákat építenek be, a kiberbiztonsági intézkedések egyre fontosabbá válnak.

2.2. Felhőbiztonság

A felhőbiztonság az okos épületekkel összefüggésben egy fejlődő terület, amely kulcsfontosságú e technológiailag fejlett szerkezetek biztonságos és hatékony működéséhez. Mivel az okos épületek egyre inkább felhőalapú megoldásokra

támaszkodnak az adatfeldolgozás, -tárolás és -kezelés terén, a felhőbiztonsági intézkedések fontossága kiemelkedővé válik. Célom, hogy ismertessem és elemezzem az okos épületekre jellemző felhőbiztonság egyedi aspektusait vizsgálom, kiemelve az ezzel kapcsolatos kihívásokat és stratégiákat.

Az okos épületek a felhőalapú számítástechnikát különböző funkciókhoz használják, beleértve az adatelemzést, a távfelügyeletet és az épületrendszerek vezérlését. Ez a felhőalapú architektúra skálázhatóságot, rugalmasságot és továbbfejlesztett adatfeldolgozási képességeket kínál. Ugyanakkor sajátos biztonsági kihívásokat is felvet, amelyeket kezelni kell az érzékeny adatok védelme és a zavartalan épületüzemeltetés biztosítása érdekében. A felhőszolgáltatók olyan szervezetek, amelyek felhőalapú számítástechnikai szolgáltatásokat kínálnak. Az olyan nagy szereplők, mint az Amazon Web Services (AWS), a Microsoft Azure és a Google Cloud Platform uralják a nyilvános felhőpiacot, és szolgáltatások széles skáláját kínálják, beleértve a tárolást, a számítási teljesítményt és a különböző felhőalapú alkalmazásokat. Ezek a szolgáltatók felelősek az infrastruktúra karbantartásáért és az alapvető biztonsági intézkedések biztosításáért.

Három féle felhő típust különböztetünk meg egymástól, nyilvános, privát és hibrid. A nyilvános felhők tulajdonosa és üzemeltetője a harmadik fél felhőszolgáltató. Számítási erőforrásokat, például szervereket és tárolóeszközöket biztosítanak az interneten keresztül, a szolgáltatásokat pedig fizetős alapon kínálják. A nyilvános felhők skálázhatóságukról, megbízhatóságukról és hatékonyságukról ismertek, de az adatbiztonsággal és a magánélet védelmével kapcsolatos aggályokat is felvetnek, mivel az erőforrásokat több felhasználó között osztják meg. A privát felhőket kizárólag egyetlen vállalkozás vagy szervezet használja. Fizikailag elhelyezkedhetnek a szervezet helyszíni adatközpontjában, vagy egy harmadik fél szolgáltató által üzemeltetve. A privát felhők nagyobb ellenőrzést és biztonságot nyújtanak, így alkalmasak olyan szervezetek számára, amelyek szigorú szabályozási megfelelési igényekkel vagy érzékeny adatokkal rendelkeznek. A hibrid felhők egyesítik a nyilvános és a privát felhőket, amelyeket olyan technológia köt össze, amely lehetővé teszi az adatok és alkalmazások megosztását közöttük. Ez a modell nagyobb rugalmasságot és több telepítési lehetőséget biztosít a vállalkozások számára, de robusztus biztonsági intézkedéseket igényel a különböző felhőkörnyezetek közötti adatátvitel és integráció kezeléséhez.

A szolgáltatási modellek tekintetében szintén három típus van, SaaS, PaaS, IaaS. Szoftver, mint szolgáltatás (SaaS) az interneten keresztül, előfizetéses alapon nyújt szoftveralkalmazásokat. Ebben a modellben a felhasználók a szolgáltató által üzemeltetett

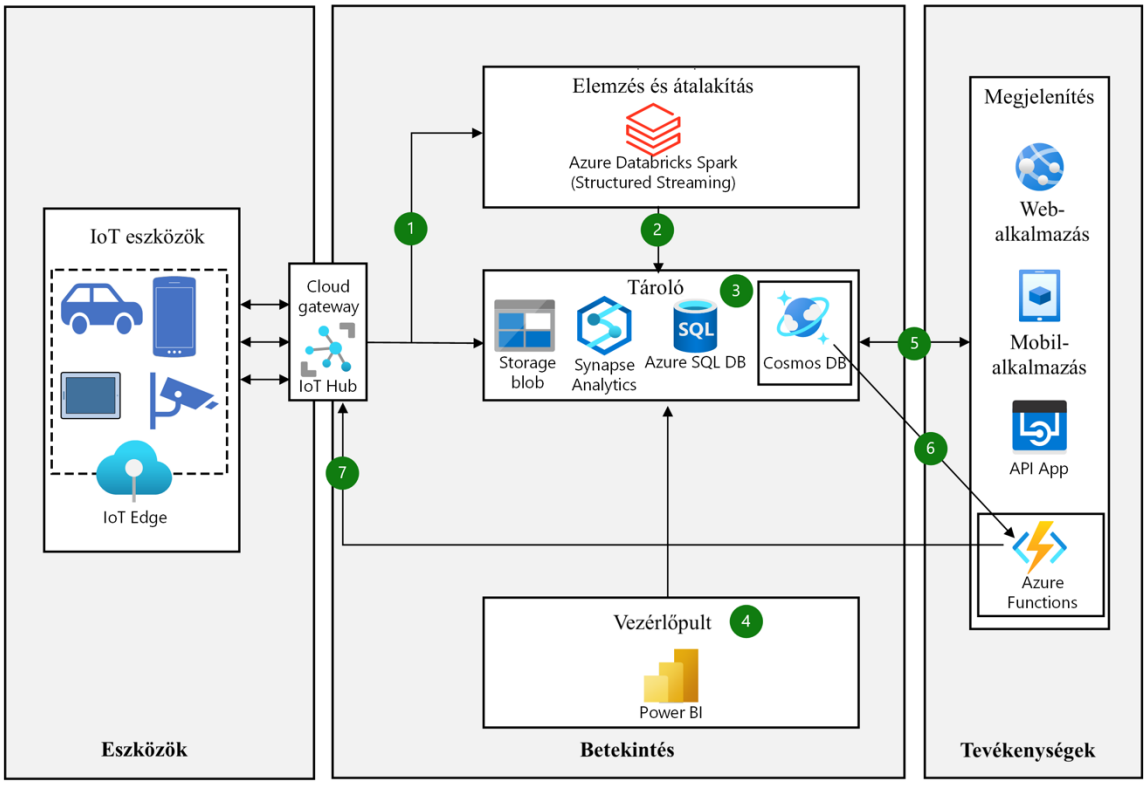
szoftveralkalmazásokhoz férnek hozzá. A szolgáltató kezeli az infrastruktúrát, a platformokat és a szoftvert, míg a felhasználók egyszerűen egy webböngészőn vagy alkalmazáson keresztül használják a szoftvert. Ilyen például a Google Workspace, a Salesforce és a Microsoft Office 365. Platform, mint szolgáltatás (PaaS) platformot biztosít az ügyfelek számára az alkalmazások fejlesztéséhez, futtatásához és kezeléséhez anélkül, hogy az alkalmazás fejlesztésével és elindításával jellemzően együtt járó infrastruktúra kiépítésének és karbantartásának bonyolultsága miatt az ügyfelek számára ez nem lenne szükséges. A PaaS a fejlesztéshez, teszteléshez, telepítéshez és tárhelyhez kínál környezetet, valamint különböző fejlesztői eszközöket. Ilyen például a Microsoft Azure, a Google App Engine és a Heroku. Infrastruktúra, mint szolgáltatás (IaaS) olyan alapvető számítástechnikai erőforrásokat kínál, mint a virtualizált hardver, a tárolás, a hálózatok és az operációs rendszerek, fizetős alapon. A felhasználók számára magas szintű ellenőrzést biztosít az infrastruktúra felett, miközben elkerüli a fizikai hardverek tőkeköltségeit. Ilyen például az Amazon Web Services (AWS), a Google Compute Engine (GCE) és az IBM Cloud.

Különféle biztonsági kihívások jelennek meg a felhőalapú környezetekben, mint az adatvédelem. A felhőben az adatok védelmének és a magánélet védelmének biztosítása elsődleges szempont. Az okos épületek hatalmas mennyiségű adatot generálnak, beleértve a munkavállalók személyes adatait és az üzemeltetési részleteket. A hatékony adatvédelmi stratégiák magukban foglalják a titkosítást, a biztonságos adatátviteli protokollokat és az adatvédelmi előírások betartását. A felhőalapú rendszerekhez való hozzáférés kezelése kulcsfontosságú, így a hozzáférés-szabályozás és hitelesítés magában foglalja a hitelesítési mechanizmusok és hozzáférés-szabályozási irányelvek bevezetését annak biztosítása érdekében, hogy csak az arra jogosult személyek férhessenek hozzá az érzékeny adatokhoz és rendszerekhez. A felhőkörnyezetek különféle sebezhetőségekre lehetnek érzékenyek. A rendszeres biztonsági értékelések, a sebezhetőségi vizsgálatok és az időben történő javításkezelés elengedhetetlen a biztonsági gyenge pontok azonosításához és kezeléséhez. Nem elhanyagolható továbbá a biztonság felelősségi köre Ennek érdekében egy megosztott felelősség modell működik a felhőszolgáltatóknál attól függ, hogy milyen szolgáltatási modellt választunk (SaaS, PaaS, IaaS) választunk. Míg az IaaS esetében a felhasználó, úgy a SaaS esetében a szolgáltató felel a biztonságért, a PaaS esetében pedig közös felelősség terheli a feleket.

Stratégiai szempontból szükséges egy biztonságos felhőarchitektúra kialakítása. A biztonságos felhőarchitektúra tervezése magában foglalja a biztonsági megfontolások

beépítését minden szinten. Ez magában foglalja a biztonságos API-k használatát, a hálózati szegmentáció megvalósítását és a többszintű biztonsági megközelítés elfogadását. A szabványoknak és szabályozásoknak való megfelelés: Az iparági szabványok és szabályozási követelmények betartása kritikus fontosságú. Az olyan keretrendszereknek való megfelelés, mint a NIST SP 800-53, ISO 27001 és a GDPR segít a szilárd biztonsági gyakorlatok kialakításában és a bizalom fenntartásában. Folyamatos felügyelet és incidensek kezelése: A felhőkörnyezetek folyamatos felügyeletének megvalósítása biztosítja a potenciális biztonsági incidensek korai észlelését. A hatékony incidensreagálási terv kulcsfontosságú az esetleges jogsértések vagy anomáliák gyors kezeléséhez és enyhítéséhez.

Az alábbiakban a Microsoft felhőalapú Azure IoT architektúráját mutatom be, mert ők az egyik olyan szolgáltató, amely komplex megoldást kínál egy okos épület kiberbiztonsági IoT-architektúrájának létrehozására. A referenciaarchitektúra három fő csoportot tartalmaz - eszközök, feldolgozás/elemzés (betekintés) és végrehajtás/cselekvés - ezek a csoportok olyan eszközöket és szolgáltatásokat tartalmaznak, amelyek egy okos épület komplex rendszerét alkothatják. Például felhőalapú aggregálás és vezérlés, adatfeldolgozás, adatátvitel, felhasználók kezelése és a biztonság ellenőrzése.



6. ábra: Microsoft Azure IoT referencia architektúra *[55]*

Az okos épületek felhőbiztonsága dinamikus és kritikus szempont a működésük és kezelésük során. A felhőkörnyezetek által támasztott egyedi kihívások kezelése átfogó megközelítést igényel, amely magában foglalja a biztonságos architektúra kialakítását, a szigorú hozzáférés-ellenőrzést, a folyamatos felügyeletet és a szabályozási előírások betartását.

2.3. Kiberbiztonság IoT-környezetekben

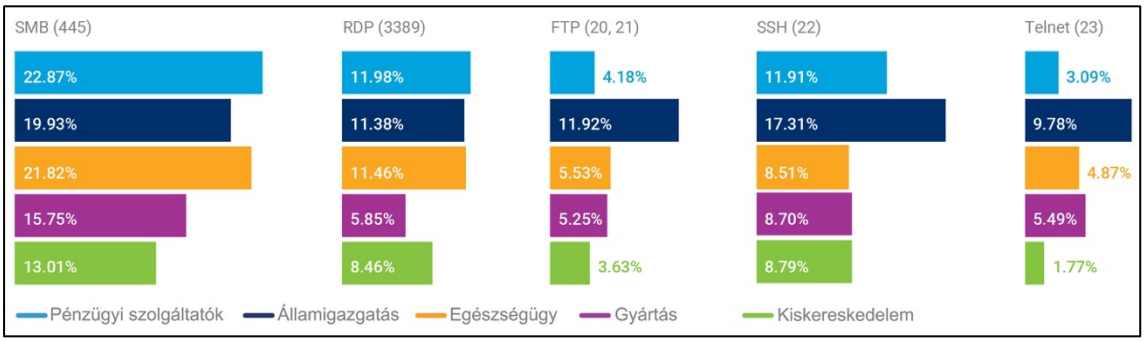
A dolgok internetének az okos épületekbe történő integrálása a hatékonyság és az automatizálás új korszakát hozta el. Ez az integráció azonban egyedi biztonsági kihívásokat is jelent, tekintettel arra, hogy az IoT-eszközök, miközben javítják az épületek funkcionalitását, az összekapcsolt jellegük és az általuk kezelt adatok érzékenysége miatt sebezhetőséget is jelenthetnek. Az okos épületekben található IoT-eszközök gyakran folyamatosan üzemelnek, és az épület működése szempontjából létfontosságú adatokat gyűjtenek és továbbítanak. Ez az állandó összekapcsolhatóság növeli a kibertámadások kockázatát. Az eszközök sokfélesége, amelyek mindegyike saját firmware-rel és szoftverrel rendelkezik, tovább bonyolítja a biztonsági helyzetet.

Az okos épületek összefüggésében vizsgálom meg az IoT-hoz kapcsolódó kiberbiztonsági kihívásokat, fenyegetéseket és sérülékenységeket. Az elemzésem középpontjában az IoT-eszközök integrálásából adódó különálló kihívások és fenyegetések állnak, kiemelve azok sajátos sebezhetőségét és az ebből következő, az épületek biztonságára és működési hatékonyságára gyakorolt hatásokat.

Az IoT-biztonság konkrét kihívásai

- Az eszközök sebezhetősége: Sok IoT-eszköz korlátozott feldolgozási teljesítményű és memóriájú, ami korlátozza a fejlett biztonsági protokollok futtatására való képességüket. Ezáltal fogékonnyá válnak a kibertámadások különböző formáira, például rosszindulatú szoftverekre vagy zsarolóprogramokra.
- Bizonytalan hálózati kapcsolatok: Az IoT-eszközök gyakran olyan hálózatokon keresztül kommunikálnak, amelyek nem feltétlenül biztonságosak. Az ezeken a hálózatokon továbbított adatok lehallgathatók egy közbeékelődéses támadással, ami a titkosság és az integritás lehetséges megsértéséhez vezethet. Problémát okoznak továbbá a nyitott, nem használt portok is, mint az FTP (File Transfer Protocol), vagy SSH (Secure Shell), melyeken keresztül hozzáférés vagy kontroll szerezhető az eszköz vagy hálózat felett. A 7. ábra szemlélteti, hogy az egyes

vertikális területeken hány százaléknyi olyan eszközzel rendelkeznek, amelyeken a fenyegető szereplők által gyakran kiaknázott szolgáltatások működnek. Az oszlopdiagram minden színe egy-egy hálózati szolgáltatást jelöl; az általuk használt alapértelmezett portok a következők zárójelben szerepelnek.



7. ábra: Az engedélyezett szolgáltatások megoszlása *[56]*

A kiszolgálói üzenetblokk (SMB) a Windows számítógépek fájlmegosztásra, nyomtatómegosztásra és távoli szolgáltatások elérésére használják. A WannaCry és NotPetya két példa az EternalBlue-t kihasználó zsarolóvírusokra, melyek az SMB sebezhetőségeit használták ki. [30] A távoli asztali protokoll (RDP) távoli hozzáférést biztosít az eszközök grafikus felületen keresztül történő kezeléséhez, éppen ezért gyakran használják ki a modern automatizált fenyegetések, beleértve a brute-force támadások és a közelmúltban megjelent Ryuk zsarolóprogram. [57] Az SSH távoli kezelési lehetőségeket, különösen Linux/UNIX szerverekhez, és bár kriptográfiailag biztonságos, vissza lehet élni vele, a brute-force támadások és más sebezhetőségek kihasználásával a gépek távoli bejelentkezésére. Nemrég frissítették a TrickBot adatszivárgási kártevőt, hogy gyűjtsön SSH-kulcsokat a fertőzött hálózatokban. Telnet és FTP gyakran kiaknázott vektorok. Ezek a protokollok nem biztonságosak és nem titkosítanak hálózati munkameneteket, lehetővé téve a hitelesítő adatok vagy érzékeny adatok kiszimatolását a hálózatban. A Mirai és a SYSCON botnetek például nagymértékben támaszkodtak a Telnet és az FTP kihasználására. [27]

- A szabványosítás hiánya: Az IoT-ökoszisztéma nem rendelkezik egységes biztonsági szabványokkal. A szabványosítás hiánya azt jelenti, hogy a különböző gyártók eszközei eltérő biztonsági szintekkel rendelkezhetnek, ami a rendszer potenciális gyenge pontjaihoz vezet. Kutatásom fő célja, hogy rámutassak ezen hiányosságokra és a megoldási javaslatot tegyek egy olyan keretrendszer kialakítására, amellyel szabályozható ezen eszközök használata egy okos épületben.

- Szoftver- és firmware-frissítések: Az IoT-eszközök frissítése a legújabb biztonsági javításokkal kihívást jelent. Egyes eszközök nem támogatják a távoli vagy automatikus frissítéseket, így manuális beavatkozást igényelnek, ami erőforrás-igényes lehet.
- Adatvédelmi aggályok: Az okos épületekben található IoT-eszközök hatalmas mennyiségű adatot gyűjtenek, amelyek egy része érzékeny lehet. Ezen adatok védelmének biztosítása kihívást jelent, különösen az adatvédelmi előírásoknak való megfelelés tekintetében.

Kockázatcsökkentési stratégiák

- Fokozott biztonsági protokollok: Az IoT-eszközök védelméhez elengedhetetlen a biztonsági protokollok implementálása az eszközök szintjén, beleértve az erős titkosítást és a biztonságos hitelesítési módszereket.
- Hálózati biztonsági intézkedések: A biztonságos hálózati architektúrák, például a virtuális magánhálózatok (VPN) és tűzfalak használata védelmet nyújthatnak az adatoknak az átvitel során. A hálózati szegmentálás szintén hatékony lehet az eszközök elszigetelésében és a potenciális jogsértések megfékezésében.
- Rendszeres szoftverkarbantartás: Az IoT-eszközök rendszeres frissítéseinek és javításainak biztosítása kulcsfontosságú a biztonság fenntartása szempontjából. Az automatizált frissítési mechanizmusok segíthetnek e folyamat hatékony kezelésében.
- Szabványok kidolgozása és betartása: Az IoT-eszközökre vonatkozó iparági szintű biztonsági szabványok kidolgozása és elfogadása javíthatja az okos épületek általános biztonsági helyzetét.

Kutatások alapján az alábbi 4 főkategóriába sorolhatóak a leginkább kockázatos eszközök, melyek a hálózatokra csatlakoznak. A táblázat végén helyet kap az IoMT (Internet of Medical Things), avagy az orvosi dolgok internete, mely eszközök az elmúlt években folyamatosan ki van téve támadásoknak. Megoszlási arányt tekintve, 4000 sebezhetőség található meg a Forescout Vedere Labs adatbázisában melynek megoszlása, IT: 78%, IoT: 14%, OT: 6% és IoMT: 2%. Ugyan a legtöbb sebezhetőség IT-eszközöket érint, közel 80%-uk, azonban ezek csak magas súlyosságúak. Ezzel szemben az IoMT-eszközökön kevesebb sebezhetőséggel bírnak, de 80%-uk kritikus, ami jellemzően lehetővé teszi az eszköz teljes kontrolljának átvételét. [58]

	IT	IoT	OT	IoMT
1	Számítógép	Hálózati tároló (NAS)	Szünetmentes tápegység (UPS)	Egészségügyi munkaállomás
2	Szerver	Nyomtató	Programozható logikai vezérlő (PLC)	Képalkotás
3	Router	IP kamera	Mérnöki munkaállomás	Nukleáris medicina rendszer
4	VPN átjáró	Sávon kívüli kezelés (OOBM)	Épületautomatizálás	Vércukorszint-monitor
5	Biztonsági eszköz	VoIP	Távoli terminálegység (RTU)	Betegmonitor

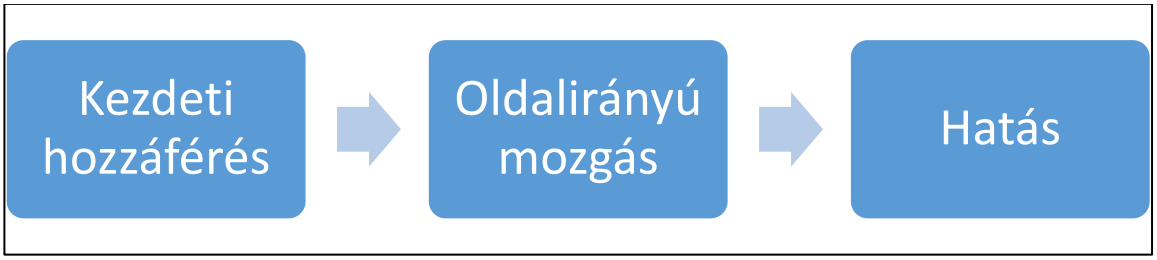
2. táblázat: A legkockázatosabb csatlakoztatott eszközök 2023-ban [58]

Kibertámadások közül az alábbiakban néhány ismertetésre kerül, melyek dokumentáltan bekövetkeztek, vagy laborkörnyezetben került végrehajtásra.

Ransomware for IoT (R4IoT)

Az "R4IoT: Next-Generation Ransomware" című, a Vedere Labs által készített kutatási jelentés a zsarolóvírus-támadások változó helyzetének mélyreható elemzését tartalmazza, különös tekintettel az IoT és az OT támadásokba való integrálására. A kutatás úgy épül fel, hogy átfogó képet nyújtson a zsarolóvírus-támadások jelenlegi helyzetéről, fejlődéséről és e kiberfenyegetések lehetséges jövőbeli pályájáról. A kutatócsapat a zsarolóvírusok új formájának, az R4IoT-nek a megjelenése mögött meghúzódó okokat vizsgálja. Fő fókuszterületük az IoT és OT eszközök növekvő összekapcsolódása az üzleti műveletekben, és az, hogy ez az integráció hogyan jelent új sebezhetőségeket és támadási vektorokat a kiberbűnözők számára. A kutatás részletes áttekintést nyújt a zsarolóvírusok jelenlegi helyzetéről, beleértve a fenyegető szereplők motivációit és a puszta adattitkosításról a sokrétű zsarolási taktikákra való áttérést. Miszerint ez a fajta támadási mód igen kifizetődő, hiszen a JBS 11 millió dollárt fizetett a REvil csoportnak. A jelentés felvázolja a zsarolóvírus-támadások anatómiáját, részletezve a lépéseket a kezdeti hozzáféréstől a végrehajtásig. Mely szerint a kezdeti lépésben a támadó jogosulatlan hozzáférést szerez a rendszerekhez helyben, vagy távolról egy sebezhetőség kihasználásával, például puffer túlcsordulás. Második lépésben, amikor oldalirányú mozgást végez a támadó megpróbál a hálózaton belül eljutni a célpontig, vagy minél több eszközt kompromittálni, megfertőzni és irányítása alá vonni. Ezeket különféle

eszközökkel érheti el, például CobaltStrike vagy Mimikatz. Amint átvette az adott rendszer felett az irányítást, vagy elhelyezte a kártékony kódot következik a harmadik lépés a hatás, ahol az összegyűjtött adatok és az elhelyezett zsarolóvíruskódok alapján a támadó távolról irányíthatja, így titkosíthatja az adatokat. Melyről az áldozatot értesíti a megfelelő váltságdíjat követelve, ami legtöbb esetben kriptovaluta. [59]

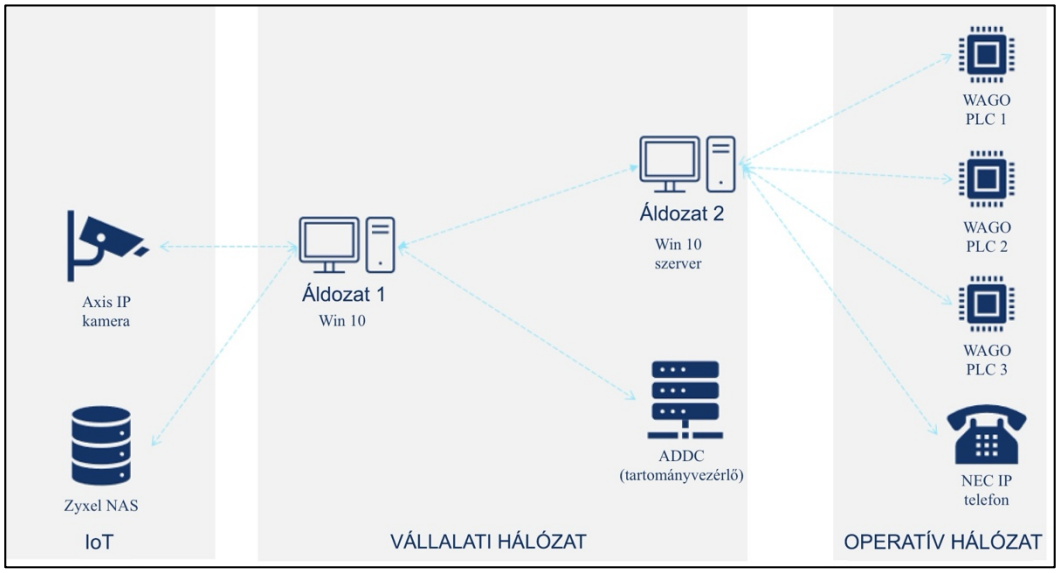


8. ábra: Zsarolóvírus-támadás anatómiája

Az előretekintő elemzés kapcsán képek kapunk arról, hogyan alakulhatnak a jövőbeni zsarolóvírus-támadások. Kiemelik az IoT és az OT eszközök lehetséges használatát a kezdeti hozzáféréshez, valamint a hagyományos titkosítási módszereken túlmutató hatásokat, beleértve az üzleti műveletek fizikai megzavarását is. Továbbá az egyik dolog, ami összeköti a beágyazott IoT- és OT-eszközök által nyújtott kezdeti hozzáférési és lehetséges hatásokat, az az ellátási láncban megjelenő egyre több olyan sebezhetőség, amely egyszerre több millió ilyen eszközt érint. Például az TCP/IP stackeket érintő Project Memoria, az Access:7 [60], amely egy népszerű IoT-kezelőt érint. platformot, valamint a busybox alkalmazásban található sebezhetőségek. [59] A Forescout elemezte a telepítések alkalmával begyűjtött és birtokában lévő ügyfelek anonimizált adatait. Hatalmas mennyiségű adat áll rendelkezésükre, melyekből kiemelném a 39 milliárd egyedi adatpontot, a 18,7 millió egyedi eszközprofilt, a 8132 egyedi gyártót és a 2014 egyedi operációsrendszer verziót. Az adatokból kiolvasható, hogy az IoT, IoMT és OT eszközök együttesen 44%-ot ölelnek fel a vállalati hálózatokban lévő összes eszközből. Ez azt jelenti, hogy a zsarolóvírus-fenyegető szereplők a csak az informatikai eszközökre irányuló fenyegetések csaknem felét hagyják figyelmen kívül a szervezeteket érő támadási felületet. [59] Ebből következik, hogy az elkövetkező években nagy kihívás elé állítja a szakembereket az IoT eszközök védelme, hiszen ez a „kiaknázatlan piac” hatalmas extra bevételi forrást jelenthet a bűnözőknek az egyre jobban elterjedő IoT eszközök piacán. [59]

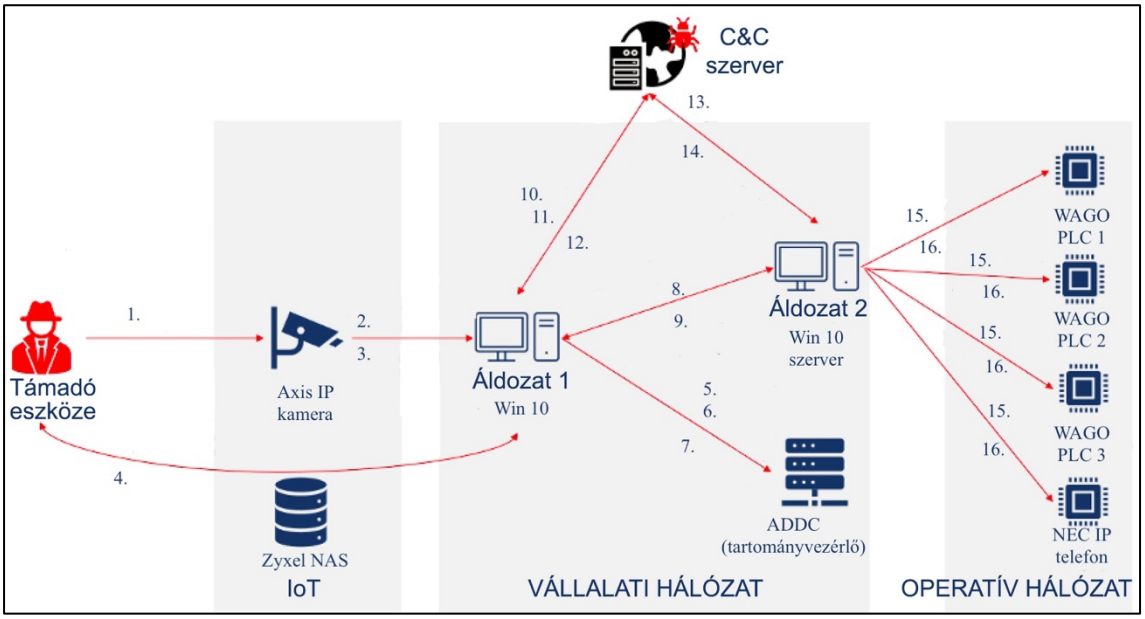
R4IoT laborkörnyezetben

A Vedere Labs kutatásában részletezi azt a kísérletet, amelynek során laboratóriumi körülmények között zsarolóvírust hoztak létre.



9. ábra: Laborhálózat [59]

Három fő szekcióra osztották hálózati szinten a rendszert**,** IoT, vállalati hálózat és operatív hálózat. A fő cél az volt, hogy az IoT rétegből eljussanak a támadók az operatív hálózat WAGO PLC vezérlőéig, így átvéve az épületirányításrendszer felett a kontrollt. A támadók a sérülékeny Axis IP kamerának és a Zyxel NAS-nak használták ki a (CVE-2018-10660, CVE-2018-10661, CVE-2020-10662, CVE-2020-9054) sérülékenységeit. Alábbiakban a támadás részletes lépésit ismertetem.



10. ábra: Támadás áttekintése [59]

A támadás 16 lépésből állt:

1. Az Axis kamera sérülékenységeit kihasználva privilegizált felhasználót adott hozzá és elhelyezte a fájljait, illetve az SSH hozzáférést bekapcsolta;

2. A hálózatra csatlakoztatott „áldozat 1” gép felfedezése;
3. RDP hitelesítő adatok brute force támadása;
4. SSH-csatorna kiépítése az Zyxel NAS és az „áldozat 1” gép között, kikapcsolva a védelmi megoldásokat és kártékony kód elhelyezése;
5. Domain Controller (DC) és domainbe léptetett gépek keresése;
6. DC (CVE-2020-1472, Zerologon) sebezhetőségének kihasználása;
7. Admin jelszó kinyerése;
8. Ransomware, crypto miner és OT malware programok elhelyezése az „áldozat 2” gépre;
9. További gépekre való oldalirányú mozgás és fertőzés;
10. Adatkinyerési parancs kiadása a C&C szerverről;
11. Adatkinyerés FTP-n keresztül;
12. Adattitkosítási parancs kiadása a C&C szerverről;
13. Crypto miner (Monero) indítási parancs kiadása a C&C szerverről;
14. IoT/OT malware indítási parancs kiadása a C&C szerverről;
15. Hálózati feltérképezés;
16. FTP alapú túlterheléses támadás (DoS) és a WAGO PLC-k távoli kontrollálása.

A támadás komplexitása jól szemlélteti, hogy az egymástól elválasztott rendszerek nem megfelelő konfigurálása és az eszközökön létező sebezhetőségek kihasználása milyen hatékonysággal bír. Éppen ezért kiemelten fontos, hogy egy olyan összetett rendszer esetében, mint egy okos épület megfelelő legyen a tervezés és kivitelezés informatikai és kiberbiztonsági szempontból. [59] A kísérleti jelentésben részletezik a kutatók, hogy a támadás során kihasznált sérülékenységek ellen hogyan lehetett volna védekezni. Melyek között megtalálható a megfelelő frissítések telepítése, hálózati szegmentáció, többfaktoros azonosítás bevezetése és az RDP kapcsolat korlátozása.

Colonial Pipeline

A Colonial Pipeline Company egy amerikai csővezetékrendszer, amely üzemanyagot szállít a keleti partvidéken, és döntő szerepet játszik az ország energetikai infrastruktúrájában. A támadás időpontja: 2021. május 7-én fedezték fel. Hatása a keleti part üzemanyagellátásának nagy részét szállító csővezeték leállításához vezetett, ami széles körű üzemanyaghiányt okozott. A támadást a DarkSide nevű, feltehetően kelet-európai székhelyű kiberbűnözői csoportnak tulajdonították. A DarkSide Ransomware-as-a-Service (RaaS) szolgáltatóként működik, és zsarolóvírus eszközöket kínál a

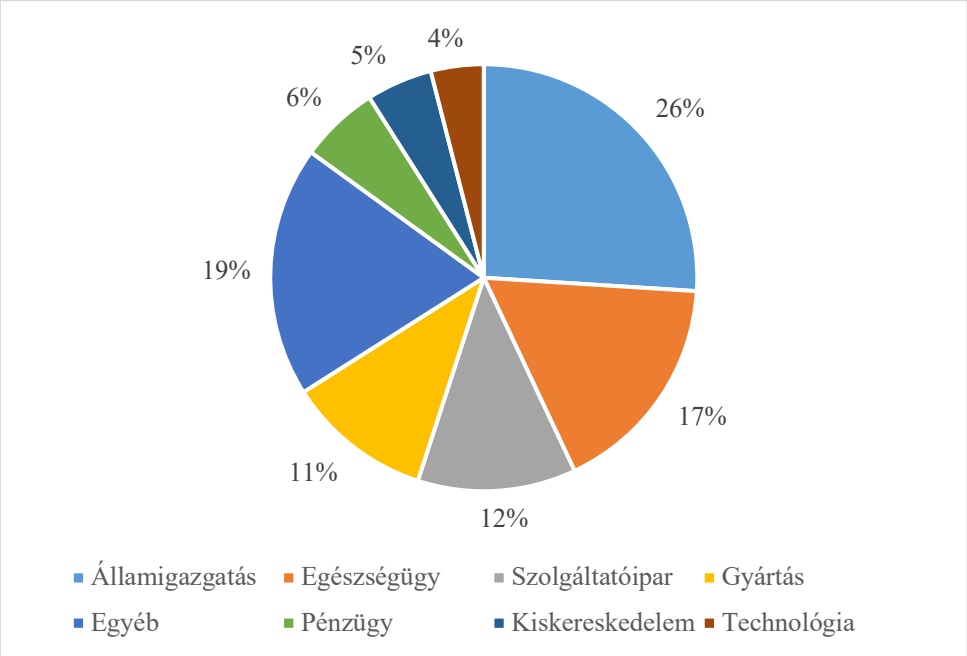
társszervezeteknek, akik aztán végrehajtják a támadásokat. A zsarolóprogram titkosította az adatokat a vállalat számítógépein, használhatatlanná téve azokat, és a támadók váltságdíjat követeltek a visszafejtő kulcsért. A Colonial Pipeline hálózatába való kezdeti behatolás pontos módját nem részletezték nyilvánosan, de a gyanú szerint adathalászat vagy egy ismert sebezhetőség kihasználása történt. A jelentések szerint a behatolt rendszerben nem volt MFA, egy kritikus biztonsági intézkedés. Az adatok titkosítása mellett a támadók a jelentések szerint közel 100 gigabájtnyi adatot is elloptak, azzal fenyegetőzve, hogy kiszivárogtatják azokat, hacsak nem fizetnek váltságdíjat. A Colonial Pipeline körülbelül 4,4 millió dollár váltságdíjat fizetett, bár az amerikai kormány általában nem tanácsolja a váltságdíj kifizetését. A csővezeték több napra leállt, ami üzemanyaghiányhoz és a gázárak emelkedéséhez vezetett. Az FBI-nak sikerült visszaszereznie a váltságdíj egy részét a kriptovaluta kifizetésének nyomon követésével. A támadás hatására a kritikus infrastruktúrák kiberbiztonsága fokozottan előtérbe került, és az amerikai kormány új biztonsági irányelveket adott ki a csővezetékeket üzemeltető vállalatok számára. Az incidens felhívta a közvélemény figyelmét a kritikus infrastruktúrák kibertámadásokkal szembeni sebezhetőségére. A Colonial Pipeline zsarolóvírus-támadás kiemelt esemény volt, amely kiemelte a kritikus infrastruktúrák kiberfenyegetésekkel szembeni sebezhetőségét. Rávilágított a szilárd kiberbiztonsági intézkedések szükségességére, beleértve az alkalmazottak képzését, a hálózat szegmentálását, a rendszeres frissítéseket és javításokat, valamint az MFA bevezetését. Az incidens esettanulmány lett a kiberbiztonsági felkészültség fontosságáról, valamint a zsarolóvírus-támadásokra való reagálás és az azokból való felépülés összetett kihívásairól.

Amnesia:33

A Forescout Research Labs által kiadott "AMNESIA:33 - How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT, and IT Devices" című kutatási jelentés átfogó elemzést nyújt a nyílt forráskódú TCP/IP stackek sebezhetőségéről.

A jelentés a nyílt forráskódú TCP/IP stackek biztonságára fókuszál, amelyek az IoT-, OT- és IT-környezetekben található eszközök széles körének működéséhez elengedhetetlenül szükségesek. A kutatók 33 új sebezhetőséget azonosítottak, rávilágítva az e stackek által jelentett potenciális kockázatokra. Az azonosított sebezhetőségek az információszivárgástól és a szolgáltatásmegtagadástól (DoS) a DNS-cache mérgezéséig terjednek. Minden egyes sebezhetőséget a lehetséges hatás és súlyosság szempontjából részletezünk, így világosan megérthetjük a kockázatokat. A kutatás tárgyalja az e stack-

ek fejlesztése során előforduló gyakori anti-mintákat, például az alapvető korlátozási ellenőrzések hiányát és az RFC-dokumentumok félreértelmezését vagy helytelen implementálását. Ezek az anti-minták hasonló sebezhetőségekhez vezetnek a különböző stackekben. A kutatók részletezik e sebezhetőségek kihasználhatóságát, felmérve az általuk jelentett tényleges veszélyt. Ez magában foglalja annak elemzését, hogy mely komponensek jellemzően hibásak, és melyek a leggyakoribb sebezhetőségi típusok. A jelentés megbecsüli e sebezhetőségek hatókörét, kitérve arra, hogy hol találhatók meg a modern ellátási láncban. Foglalkozik az érintett eszközök azonosításának és foltozásának kihívásával, és becsléseket ad az érintett gyártók, eszköztípusok és eszközegységek számáról. Körülbelül 11.000 online potenciálisan sebezhető eszközöt találtak, és több mint 35.000 példányt a Device Cloud-ban, mely az alábbi ábrán látható. [61]



11. ábra: Potenciálisan veszélyeztetett eszközök iparági vertikumonként [61]

A jelentés a hatékony IoT-kockázatcsökkentésre vonatkozó ajánlásokkal zárul. Hangsúlyozza a hálózati eszközök átfogó láthatóságának és ellenőrzésének fontosságát az említett sebezhetőségek elleni védelem érdekében.

Összefoglalva az "AMNESIA:33" egy kulcsfontosságú kutatás, amely rávilágít az IoT, OT és IT eszközök széles körében használt nyílt forráskódú TCP/IP stackekben található kritikus sebezhetőségekre. A jelentés a kiberbiztonsági szakemberek, az eszközgyártók és a politikai döntéshozók számára fontos segítséget nyújt az ilyen sebezhetőségekkel kapcsolatos kockázatok megértésében és mérséklésében. Emellett megalapozza a

TCP/IP-kötegek biztonságának javítására irányuló további kutatásokat és vitákat a gyorsan fejlődő IoT-térben.

Az okos épületek IoT-biztonsága sokrétű kihívás, amely átfogó megközelítést igényel. E kihívások kezelése nemcsak technikai megoldásokat, hanem a legjobb gyakorlatok és szabványok betartását is magában foglalja. Ahogy a dolgok internete folyamatosan fejlődik, úgy kell fejlődniük a biztonsági stratégiáknak is.

2.4. Zero Trust Architektúra az okos épületrendszerekben

A zéró bizalmi architektúra (Zero Trust Architecture - ZTA) kialakítása az okos épületrendszerekben kritikus követelmény a kiberbiztonsági intézkedések fokozásában. Ez a megközelítés összhangban van a NIST SP 800-207. sz. külön-kiadványában foglalt iránymutatásokkal, amely átfogó keretet kínál a ZTA megvalósításához az okos épületekben, ahol különböző IoT-eszközök és hálózati rendszerek kapcsolódnak egymáshoz, a ZTA megbízható és adaptálható biztonsági modellt biztosít.

A ZTA alapelvei a NIST SP 800-207 értelmezésében

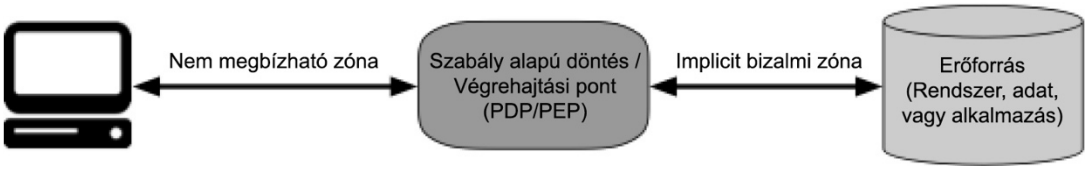
- Szigorú személyazonosság-ellenőrzés: A NIST SP 800-207 szabványnak megfelelően a ZTA az okos épületekben az összes felhasználó és eszköz szigorú személyazonosság-ellenőrzésére helyezi a hangsúlyt. Ez magában foglalja a többfaktoros hitelesítés és a dinamikus hozzáférés-ellenőrzés végrehajtását, biztosítva a hozzáférési jogok folyamatos ellenőrzését és kiigazítását.
- Legkisebb jogosultság elve és mikroszegmentáció: A legkisebb jogosultság elve, a ZTA egyik legfontosabb alapelve, összhangban van a NIST SP 800-207 ajánlásával. Ez az alapelv az egyes feladatokhoz szükséges minimális hozzáférés biztosítását jelenti. A mikroszegmentálás tovább fokozza a biztonságot azáltal, hogy a hálózatot kisebb, ellenőrzött szegmensekre osztja, ezáltal korlátozva a lehetséges jogsértések körét.
- Folyamatos felügyelet és biztonsági analitika: A NIST SP 800-207 szorgalmazza a hálózatok folyamatos felügyeletét, ami a ZTA szerves részét képezi. Az okos épületekben ez a hálózati tevékenységek valós idejű felügyeletét jelenti, a mesterséges intelligencia által vezérelt analitikát kihasználva az anomáliák azonnali észlelésére és az azokra való reagálásra.

A ZTA megvalósítása okos épületekben (NIST 800-207 megközelítés)

- Hálózati architektúra és szegmentálás: A NIST SP 800-207 szerinti ZTA megvalósítása a hálózati architektúra újragondolását jelenti. A hálózatok

különálló zónákra történő szegmentálása, amelyek mindegyike testre szabott biztonsági ellenőrzésekkel rendelkezik, alapvető fontosságú. Ez a megközelítés különösen hatékony az okos épületek különböző funkcióinak kezelésében, a HVAC-rendszerektől a biztonsági protokollokig.

- Szabályok érvényesítése és alkalmazkodóképesség: A NIST SP 800-207-ben vázolt dinamikus házirend-kényszerítés alapvető fontosságú a ZTA-ban. A hozzáférést és a biztonságot szabályozó irányelveket folyamatosan értékelik, és az okos épületeken belül a változó fenyegetésekhez és a működési változásokhoz igazítják.
- Integráció a meglévő infrastruktúrával: A ZTA megvalósításának összehangolása a meglévő épületirányítási rendszerekkel a NIST iránymutatásainak megfelelően gondos tervezést igényel. Ez biztosítja a kompatibilitást és az üzemeltetés folyamatosságát, elkerülve az épületfunkciók megszakítását.[30], [31], [62]



12. ábra: Zero Trust Access [62]

A fenti ábrán látható a hozzáférési modellben, hogy egy felhasználó hozzáférne a vállalati erőforráshoz. A hozzáférés biztosítása egy szabállyal kapcsolatos szabály alapú döntési ponton (PDP) és a megfelelő házirenden keresztül történik a végrehajtási pont (PEP). Amennyiben a szabályoknak megfelel a felhasználó, úgy férhet hozzá az adott erőforrásokhoz.

A NIST SP 800-207 szabvány betartása a ZTA okos épületekben történő megvalósítása során összetett feladat. Mind a ZTA-keretrendszer, mind az épületrendszerek sajátos működési dinamikájának alapos megértését igényli. A szigorú biztonsági intézkedések, a felhasználói élmény és az üzemeltetési hatékonyság közötti egyensúly megteremtése kulcsfontosságú. A ZTA-nak nem akadályoznia, hanem fokoznia kell az épületrendszerek funkcionalitását és használhatóságát. A NIST SP 800-207 szabványnak megfelelően a ZTA folyamatos irányítást és rendszeres frissítéseket igényel, hogy hatékony maradjon a fejlődő kiberbiztonsági fenyegetésekkel szemben. [63]

A NIST SP 800-207 által vezérelt Zero Trust Architecture okos épületrendszerekben történő alkalmazása strukturált és hatékony megközelítést kínál a kiberbiztonságra. Bár bizonyos kihívásokkal jár, a szigorú hozzáférés-ellenőrzésre, a folyamatos felügyeletre és az alkalmazkodóképességre helyezett hangsúlya miatt létfontosságú eleme a modern okos épületek védelmének. Így egy új épület esetén a tervezéskor mindenképp figyelembe kell venni a ZTA követelményeit és be kell építeni a kiberbiztonsági tervbe.

Összefoglalva a fejezetet, a kiberbiztonság sokrétű területei kerültek bemutatásra az okos épületek kontextusában, a kiberbiztonsági elvek feltárásával megalapozva az alapokat. A fejezetben bemutattam a felhőbiztonság kulcsfontosságú szerepét, kiemelve annak jelentőségét az okos épületek IoT-eszközei által generált adatok tárolásában és kezelésében. A zéró bizalmi architektúra koncepcióját kritikus keretként vizsgáltam, amely a "soha ne bízz, mindig ellenőrizd" megközelítést támogatja, amely elengedhetetlen az okos épülethálózatok jogosulatlan hozzáféréssel szembeni megerősítéséhez. A fejezetben emellett kiemeltem az IoT konkrét sebezhetőségeit, bemutatva, hogy ezek az eszközök milyen potenciális kockázatot jelentenek az okos épületek ökoszisztémáinak integritására nézve.

3. MINŐSÍTÉSI ÉS KIBERBIZTONSÁGI KERETRENDSZEREK

Ebben a fejezetben a kiberbiztonság és az épülettanúsítás területét alakító kulcsfontosságú keretrendszerek, szabványok és szabályozások átfogó bemutatását és a későbbi elemzésének készítettem elő. Úgy, mint a BREEAM, a LEED, az ISO/IEC 27001, az ISO/IEC 30141, a releváns IoT és kiberbiztonsági NIST keretrendszerek, az ENISA iránymutatásai, a kiberbiztonságról szóló törvény, a GDPR és a NIS2. Minden egyes keretrendszert megvizsgálok az IoT kiberbiztonságra gyakorolt hatásukat figyelembe véve és feltárom a hiányosságaikat az IoT és az okos épületek területén. Az elemzés célja annak feltárása, hogy ezek a keretrendszerek együttesen hogyan járulnak hozzá, illetve milyen hiányosságokkal rendelkeznek a biztonság, a fenntarthatóság és a megfelelés fokozásához a fejlődő digitális és építészeti, különösen az IoT kiberbiztonság területén.

3.1. Okos épületek tanúsítási keretrendszereinek áttekintése

A BREEAM (Building Research Establishment Environmental Assessment Method) és a LEED (Leadership in Energy and Environmental Design) a fenntartható épületek tanúsításának két vezető keretrendszerének tudományos ismertetését kívánom elvégezni. Ebben az elemzésben a kritériumok, módszertanok és a modern építészeti gyakorlatra gyakorolt hatásukra összpontosítok, különösen a környezeti fenntarthatóság és hatékonyság összefüggésében, illetve kitérek azon hiányosságokra, mint a kiberbiztonság és az IoT eszközök.

A BREEAM az épületek fenntarthatóságának értékelésére szolgáló vezető globális keretrendszer. Bár elsősorban a környezeti teljesítményre összpontosít, elvei és kritériumai hatással vannak az okos épületek fejlesztésére. A BREEAM átfogó megközelítése az épületek fenntarthatóságának értékelésére számos olyan szempontot foglal magában, amelyek összhangban vannak az okos épülettervezés alapvető célkitűzéseivel, mint például az energiahatékonyság, a munkavállalók jóléte és az erőforrás-gazdálkodás. Az okos épületek, amelyeket a fejlett automatizálási és hatékonysági technológiák integrálása jellemez, a BREEAM-ben kiegészítő keretrendszer található. Ez az értékelési módszer olyan kritériumok alapján értékeli az épületeket, amelyek az energiafelhasználást, az egészséget és a jólétet, a környezetszennyezést, a közlekedést, az anyagokat, a hulladékot, az ökológiát és a gazdálkodási folyamatokat foglalják magukban. Az okos épületek esetében a BREEAM kritériumai olyan technológiák és gyakorlatok beépítését ösztönzik, amelyek nemcsak az

épület intelligenciáját növelik, hanem a fenntarthatóságot és a környezeti felelősségvállalást is elősegítik. [64]

A BREEAM nagy hangsúlyt fektet az energiahatékonyságra, amely az okos épületek egyik kulcsfontosságú szempontja. Értékeli az épület energiafogyasztási szokásait, ösztönzi a megújuló energiaforrások használatát és az okos energiagazdálkodási rendszerek integrálását a felhasználás optimalizálása és a szén-dioxid-kibocsátás csökkentése érdekében. Az okos épületek fejlett környezetszabályozó rendszereik révén hozzájárulnak a munkavállalók egészségéhez és jólétéhez. A BREEAM olyan tényezőket értékel, mint a beltéri levegő minősége, a világítás minősége és a hőkomfort, amelyek az okos épületek tervezésének szerves részét képezik. A környezeti paraméterek megfigyelésére és beállítására szolgáló IoT-eszközök használata összhangban van a BREEAM egészséges és produktív beltéri környezet kialakítására vonatkozó kritériumaival. A BREEAM értékeli az épületek építése és üzemeltetése során felhasznált anyagok fenntarthatóságát. A hatékonyságra és fenntarthatóságra összpontosító okos épületek gyakran alkalmaznak olyan anyagokat és technológiákat, amelyek minimalizálják a környezeti hatásokat, és ezzel összhangban vannak a BREEAM célkitűzéseivel. A BREEAM elismeri és díjazza az innovatív gyakorlatokat az épületek tervezésében és üzemeltetésében. Az okos épületek, a fejlett felügyeleti, adatelemző és adaptív vezérlőrendszereikkel magas pontszámot érhetnek el ebben a kategóriában, ami tükrözi hozzájárulásukat a fenntartható építési gyakorlatok határainak kitolásához. [64]

Az okos épülettechnológiák integrálása a BREEAM fenntarthatósági kritériumainak megfelelő módon kihívást jelenthet. Ez a tervezés és üzemeltetés holisztikus megközelítését igényli, amely a technológiai innováció mellett a környezeti hatásokat is figyelembe veszi. A BREEAM tanúsítási folyamatban való eligazodás összetett lehet, különösen az IoT-t és más okos technológiákat nagymértékben alkalmazó épületek esetében. Annak biztosítása, hogy ezek a technológiák pozitívan járuljanak hozzá a BREEAM értékelési kritériumaihoz, gondos tervezést és kivitelezést igényel. [65]

A BREEAM keretrendszer átfogó megközelítést kínál az épületek fenntarthatóságának értékeléséhez és javításához, ami az okos épületek korában egyre fontosabbá válik. Az okos technológiák integrációjának a BREEAM kritériumaihoz való igazításával a fejlesztők és üzemeltetők biztosíthatják, hogy okos épületeik nemcsak technológiai szempontból fejlettek, hanem környezetvédelmi szempontból is felelősek és fenntarthatóak legyenek. Azonban az IoT biztonságával és implementálásával kapcsolatban nem tesz említést.

A LEED egy széles körben elismert zöld épületek tanúsítási rendszere, amelyet az Egyesült Államok Zöld Épületek Tanácsa (USGBC) fejlesztett ki. A rendszer keretet biztosít a nagy teljesítményű zöld épületek, köztük az okos épületek tervezéséhez, építéséhez és üzemeltetéséhez. A LEED tanúsítás világszerte keresett, és a fenntartható építési gyakorlatok kiválóságának mércéjeként tartják számon. Az okos épületek, amelyek a fejlett technológiákat a hatékonyság és a munkavállalók komfortérzetének növelése érdekében használják fel, szorosan illeszkednek a LEED fenntarthatósági céljaihoz. A LEED átfogó értékelési kritériumai az energiahatékonyságra, a víztakarékosságra, a CO2-kibocsátás csökkentésére, a beltéri környezetminőség javítására és az erőforrásokkal való gazdálkodásra terjednek ki. Ezek a kritériumok összhangban vannak az okos épülettervezés alapvető célkitűzéseivel, amelynek célja az okos, érzékeny és fenntartható élet- és munkakörnyezet kialakítása. [66]

A LEED központi alapelve az energiahatékonyság. Az okos épületek integrált energiagazdálkodási rendszereikkel gyakran alkalmaznak olyan technológiákat, mint az automatizált világítás, a HVAC-rendszerek és az energiafigyelő érzékelők. Ezek a technológiák az energiafelhasználás optimalizálásával és az általános környezeti hatás csökkentésével járulnak hozzá a LEED-tanúsítványhoz. A LEED hangsúlyozza a beltéri környezetminőség fontosságát, amely magában foglalja a levegőminőséget, a világítást, a hőviszonyokat és az akusztikát. Az okos épületek automatizált klímavezérlő rendszerek, levegőminőség-érzékelők és okos világítási megoldások révén javítják ezeket a szempontokat, igazodva a LEED egészséges beltéri környezetre vonatkozó kritériumaihoz. A LEED másik kulcsfontosságú szempontja a víztakarékosság. Az okos épületek olyan technológiákkal járulnak hozzá ehhez a célhoz, mint a vízszivárgás-érzékelő rendszerek, a hatékony vízkészülékek és az okos öntözőrendszerek. Ezek a technológiák segítenek a vízfelhasználás minimalizálásában és a vízkészletekkel való hatékonyabb gazdálkodásban. A LEED ösztönzi az innovációt a fenntartható építési gyakorlatok terén. Az okos épületek az IoT és más fejlett technológiák integrálásával pontokat szerezhetnek a LEED keretében az épületek tervezésének és üzemeltetésének olyan innovatív megközelítéseiért, amelyek túlmutatnak a szabványos gyakorlatokon. [66]

Az okos technológiáknak a LEED fenntarthatósági kritériumainak megfelelő módon történő integrálása holisztikus megközelítést igényel. Ez nemcsak a fejlett rendszerek telepítését jelenti, hanem annak biztosítását is, hogy azok pozitívan járuljanak hozzá az épület környezeti teljesítményéhez. Az okos épületek LEED tanúsítási folyamatában való

eligazodás összetett lehet. Alapos ismereteket igényel arról, hogy az okos technológiák hogyan hatnak a különböző LEED-kategóriákra, és hogyan lehet ezeket a hatásokat hatékonyan dokumentálni és bizonyítani.

A LEED tanúsítás átfogó keretet biztosít az épületek, köztük az okos épületek fenntarthatóságának értékeléséhez és elismeréséhez. Az okos technológiák integrációjának a LEED fenntarthatósági kritériumaihoz való igazításával a fejlesztők és üzemeltetők biztosíthatják, hogy épületeik nemcsak technológiailag fejlettek, hanem környezetvédelmi szempontból is felelősek, hozzájárulva a tágabb fenntarthatósági célokhoz. Azonban a LEED sem tesz mélyreható említést az IoT ezközök telepítése és kiberbiztonsága érdekében.

A korábban ismertetett két fenntarthatósági keretrendszert, a BREEAM-et és a LEED-et vizsgálom az okos épületek kiberbiztonságának aspektusából. Míg mindkét keretrendszer mércét állít az épületek tervezésében a környezeti fenntarthatóság tekintetében, a kiberbiztonság fejlődő területeivel való integrációjuk egyedi kihívásokat és hiányosságokat jelent. Az elemzésem célja, hogy rávilágítsak arra, hogy a BREEAM és a LEED hogyan foglalkozik, illetve hogyan nem foglalkozik az okos épülettechnológiák és az IoT-ökoszisztémák sajátos igényeivel és biztonsági problémáival.

BREEAM a fenntartható építési gyakorlatokra összpontosít, de nem foglalkozik kifejezetten az okos épülettechnológiák, köztük az IoT kiberbiztonsági vonatkozásaival. Okos épületekre összpontosít: Bár a BREEAM ösztönzi a fenntartható és hatékony technológiák alkalmazását az épületekben, beleértve az IoT-eszközöket is, hiányzik az e technológiák kiberbiztonsági helyzetének értékelésére szolgáló keretrendszer.

A LEED is a környezeti fenntarthatóságra összpontosít, és nem foglalkozik az okos épületekben található IoT kiberbiztonsági szempontjaival. A LEED tanúsítvánnyal rendelkező épületek gyakran tartalmaznak IoT-technológiákat az energiahatékonyság és a környezeti felügyelet érdekében, de nem rendelkeznek külön kerettel e rendszerek biztonságának értékelésére.

Így kijelenthetem, hogy sem a BREEAM sem a LEED keretrendszer nem tartalmaz iránymutatást az okos épületek kiberbiztonságára vonatkozóan.

3.2. Kiberbiztonsági keretrendszerek alkalmazása okos épületek tervezésekor

A legfontosabb kiberbiztonsági keretrendszerek, ajánlások közül megvizsgálom az ISO/IEC 27001-et, az ISO/IEC 30141-et, néhány IoT releváns NIST ajánlást, az ENISA-irányelveket, a NISTIR 8259 relevanciáját és alkalmazhatóságát az okos épületeken belül. Az "ISO/IEC 27001 - Information Security Management Systems - Requirements" (ISO/IEC 27001 - Információbiztonsági irányítási rendszerek - követelmények) az információbiztonság irányításának nemzetközileg elismert szabványa. A Nemzetközi Szabványügyi Szervezet (ISO) és a Nemzetközi Elektrotechnikai Bizottság (IEC) által kidolgozott szabvány szisztematikus megközelítést biztosít az érzékeny vállalati információk kezelésére, biztosítva azok bizalmas jellegét, sértetlenségét és rendelkezésre állását. Az ISO/IEC 27001 olyan keretrendszert hoz létre, amelyet a szervezetek követhetnek az információbiztonsági irányítási rendszer (ISMS) megvalósításakor. Ezt a keretrendszert úgy tervezték, hogy bármilyen méretű vagy iparágú szervezetre alkalmazható legyen, rugalmas, mégis átfogó megközelítést kínálva az információbiztonsághoz.

Az ISO/IEC 27001 fő összetevői

- Kockázatkezelés: A szabvány központi eleme a kockázatkezelés fogalma. A szervezeteknek rendszeres kockázatértékeléseket kell végezniük a potenciális biztonsági fenyegetések és sebezhetőségek azonosítása érdekében. Ezen értékelések alapján megfelelő biztonsági ellenőrzéseket kell végrehajtaniuk az azonosított kockázatok mérséklésére.
- Biztonsági ellenőrzések: A szabvány tartalmaz egy sor biztonsági ellenőrzési célt és legjobb gyakorlatot, amelyeket a szabvány melléklete ismertet. Ezek az ellenőrzések az információbiztonság különböző aspektusaira terjednek ki, beleértve a hozzáférés-ellenőrzést, a kriptográfiát, a fizikai biztonságot és az üzemeltetési biztonságot.
- Folyamatos fejlesztés: Hangsúlyozza az ISMS folyamatos fejlesztésének fontosságát. A szervezeteket arra ösztönzik, hogy rendszeresen vizsgálják felül és frissítsék biztonsági gyakorlataikat a fejlődő fenyegetésekre és üzleti változásokra reagálva. [67]

Tanúsítási folyamat

- Végrehajtás: Az szabvány tanúsítás megszerzéséhez a szervezetnek a szabvány követelményeinek megfelelően kell bevezetnie az ISMS-t. Ez magában foglalja a biztonsági irányelvek kialakítását, az ISMS hatályának meghatározását, kockázatértékelések elvégzését és a szükséges ellenőrzések végrehajtását.
- Auditálás és tanúsítás: Az ISMS bevezetése után a szervezetnek egy akkreditált tanúsító szervezet által végzett auditáláson kell részt vennie. Ha az audit sikeres, a szervezet megkapja az ISO/IEC 27001 tanúsítványt, ami bizonyítja az információbiztonság iránti elkötelezettségét. [67]

Előnyök és kihívások

- Fokozott biztonsági helyzet: Az MSZ ISO/IEC 27001 bevezetése segít a szervezeteknek megerősíteni a biztonsági helyzetüket, csökkentve a biztonság megsértésének és az adatvesztés kockázatát. Emellett növeli a bizalmat az ügyfelek és az érdekelt felek körében.
- Megfelelés és versenyelőny: Az MSZ ISO/IEC 27001 tanúsítás segíthet a jogi és szabályozási követelményeknek való megfelelésben. Emellett versenyelőnyt is nyújt, mivel bizonyítja az információbiztonság iránti elkötelezettséget.
- Erőforrásigény: Az MSZ ISO/IEC 27001 bevezetésének és a tanúsítás fenntartásának folyamata erőforrás-igényes lehet és időt és erőfeszítést igényel. [67]

Az szabvány átfogó megközelítést képvisel a szervezet információbiztonságának kezelésére. Elfogadása proaktív hozzáállást jelent az érzékeny adatok és rendszerek védelmére, ami a mai digitális környezetben létfontosságú. Bár a tanúsítási folyamat igényes lehet, a fokozott biztonság és az üzleti hitelesség szempontjából előnyökkel jár. Azonban ez a szabvány sem foglalkozik az okos épületek kiberbiztonságával.

ISO/IEC 30141

Az ISO/IEC 30141 "Internet of Things - Reference Architecture (IoT RA)" című nemzetközi szabvány magas szintű keretrendszert biztosít az IoT rendszerek tervezéséhez, telepítéséhez és irányításához. Az ISO és IEC által közösen kidolgozott szabvány célja a megbízható, biztonságos és hatékony IoT-rendszerek biztosítása a különböző iparágakban és alkalmazásokban. Az ISO/IEC 30141 átfogó referenciaarchitektúrát hoz létre az IoT számára, iránymutatást és legjobb gyakorlatokat kínálva az IoT-ökoszisztémák interoperabilitásának, skálázhatóságának és

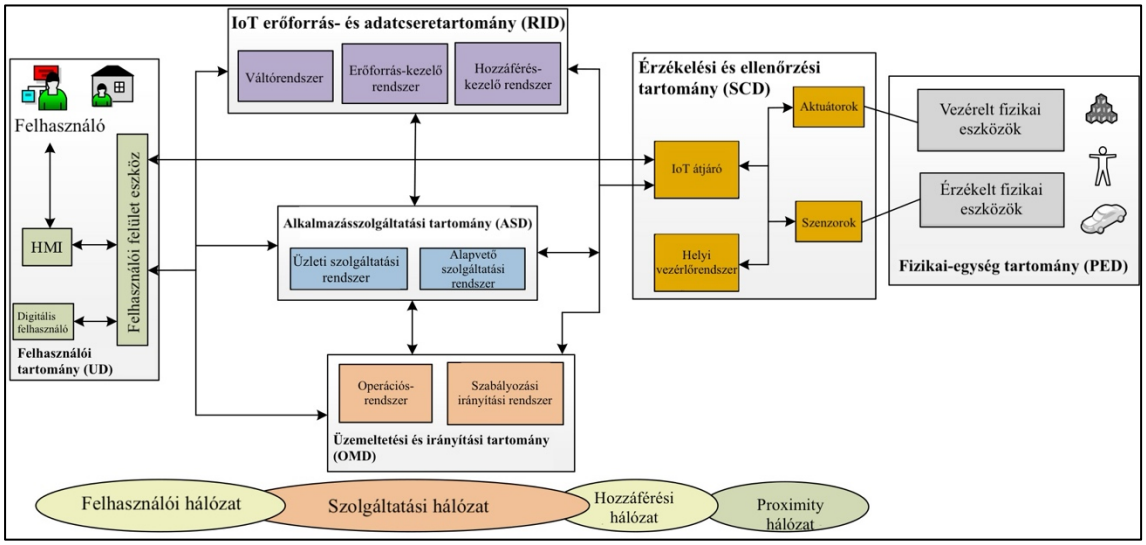
fenntarthatóságának elősegítésére. A szabványt úgy tervezték, hogy a legkülönbözőbb IoT területen alkalmazható legyen, az okos otthonoktól az ipari automatizálásig.

Az ISO/IEC 30141 fő összetevői

- Referenciamodell: A szabvány bevezet egy referenciamodellt, amely meghatározza az alapvető IoT-fogalmakat és azok kapcsolatait, például az eszközök, kiszolgálók, hálózati kommunikáció, ZPA és különféle hálózatinformatikai protokollok (UPnP, DHCP). Ez a modell szolgál alapul az IoT-rendszerek megértéséhez és megvitatásához, biztosítva az érdekeltek közös nyelvezetét és megközelítését.
- Referenciaarchitektúra: Az ISO/IEC 30141 részletes referenciaarchitektúrát biztosít, amely felvázolja az IoT-rendszerek alapvető összetevőit, beleértve az eszközöket, átjárókat, hálózatokat és platformokat. Leírja ezen összetevők funkcionalitását és kölcsönhatásait, iránymutatást adva az összetett IoT-megoldások tervezéséhez és integrálásához.
- Interoperabilitás és szabványok összehangolása: A szabvány egyik fő célja az IoT-eszközök és -rendszerek közötti átjárhatóság elősegítése. Hangsúlyozza a szabványok összehangolásának és a közös protokollok használatának fontosságát a zökkenőmentes kommunikáció és adatcsere elősegítése érdekében. [68]

Megvalósítás és alkalmazás

- Tervezési elvek: A szabvány az IoT-rendszerek alapvető tervezési elveit vázolja fel, mint például a modularitás, a hordozhatóság és a skálázhatóság. Ezek az elvek a fejlesztőket és a mérnököket rugalmas és adaptálható IoT-megoldások létrehozásában irányítják.
- Biztonság és adatvédelem: Az ISO/IEC 30141 nagy hangsúlyt fektet az IoT-rendszerek biztonságára és adatvédelmére. Az IoT-architektúra minden szintjén biztonsági intézkedéseket javasol, és kiemeli a felhasználói adatokat és a magánélet védelmét.
- Használati esetek és forgatókönyvek: A szabvány különböző felhasználási eseteket és forgatókönyveket tartalmaz, hogy szemléltesse az iránymutatások gyakorlati alkalmazását. Ezek a példák segítenek az érdekelteknek megérteni, hogy a referenciaarchitektúra hogyan alkalmazható a valós helyzetekben. [68]



13. ábra: IoT referencia architektúra [68]

Kihívások és megfontolások

- Az IoT-ökoszisztémák összetettsége: Az ISO/IEC 30141 iránymutatásainak végrehajtása kihívást jelenthet az IoT-ökoszisztémák eredendő összetettsége miatt, amelyek gyakran eszközök, technológiák és érdekelt felek sokaságát foglalják magukban.
- Fejlődő technológiai környezet: Az IoT-technológiák gyorsan fejlődő jellege megköveteli, hogy a szabvány alkalmazkodóképes és előretekintő legyen, és képes legyen a jövőbeni fejlesztésekhez és változásokhoz igazodni. [68]

Az ISO/IEC 30141 lépést jelent az IoT-rendszerek szabványosítása felé, strukturált keretet biztosítva azok fejlesztéséhez és kezeléséhez. Az interoperabilitásra, a biztonságra és a fenntarthatóságra helyezett hangsúlya kulcsfontosságú eszközzé teszi az IoT-technológiák érintettjei számára, a fejlesztőktől a politikai döntéshozókig. Kitér az okos épületekben található rendszerekre is, mint például a HVAC.

NIST keretrendszerek összehasonlítása

Az alábbi összehasonlító elemzésben a különböző NIST keretrendszereket vizsgálom meg, amelyek mindegyike kulcsfontosságú szerepet játszik a kiberbiztonsági gyakorlatok és szabályok kialakításában. A kockázatértékeléstől a IoT biztonságáig terjedő keretrendszerekre összpontosítva az összehasonlításban kiemelem a különböző célokat, alkalmazásokat és kulcsfontosságú területeket. A keretrendszerek egymás mellett történő vizsgálatával átfogó képet kapunk a kiberbiztonság és az információbiztonság tágabb környezetéhez való egyéni hozzájárulásukról.

Összehasonlító elemzés

- Kockázatértékelés és IoT: A NIST SP 800-30 kockázatértékelési keretrendszer, bár nem IoT-specifikus, kulcsfontosságú a kockázatok azonosításához és mérsékléséhez a dolgok internetének telepítésében, figyelembe véve az IoT ökoszisztémáiban rejlő egyedi sebezhetőségeket és fenyegetésvektorokat. [69]
- Biztonsági ellenőrzések az IoT számára: A NIST SP 800-53, bár szélesebb körű, de olyan alapvető ellenőrzéseket biztosít, amelyek hatékonyan alkalmazhatók és testre szabhatók az IoT-eszközök és -hálózatok biztonsága érdekében. [70]
- Naplókezelés az IoT-ben: A NIST SP 800-92 a naplókezelésre összpontosít, ami az IoT szempontjából is releváns, mivel az IoT-eszközök naplóinak nyomon követése kulcsfontosságú a biztonsági incidensek észleléséhez és az IoT-rendszerek integritásának biztosításához. [71]
- Biztonságos IoT-rendszerek tervezése: A NIST SP 800-160 rendszerbiztonsági tervezésre helyezett hangsúlya különösen fontos a biztonságos IoT-rendszerek tervezése és fejlesztése szempontjából. [72]
- IoT-alkalmazások biztonsága: Bár a NIST SP 800-163 a mobilalkalmazásokra fókuszál, az alkalmazások ellenőrzésére és biztosítására vonatkozó alapelvei kiterjeszthetők a tárgyak interneteire, amelyek gyakran hasonló biztonsági problémákkal küzdenek. [73]
- Dedikált IoT biztonsági útmutató: A NIST SP 800-213 kifejezetten az IoT-eszközök kiberbiztonságával foglalkozik, és átfogó iránymutatást kínál, amely a kormányzati és egyéb környezetben az IoT-eszközök teljes életciklusára kiterjed, a tervezéstől a leszerelésig. [74]

Az alábbi táblázatban összehasonlító áttekintést készítettem az egyes NIST keretrendszerek IoT relevanciája és a kiberbiztonsági fókusz alapján.

Keretrendszer	Cím	IoT relevancia	Kiberbiztonsági fókusz
NIST 800-30	Útmutató a kockázatértékeléshez	Közvetetten releváns; alkalmazható az IoT-vel kapcsolatos kockázatok értékelésére.	- Az IoT telepítésekre jellemző kockázatok azonosítása és értékelése. - A kockázatértékelési folyamatok IoT-

			ökoszisztémákra való szabása.
NIST 800-53	Információs rendszerek és szervezetek biztonsági és adatvédelmi ellenőrzései	Alkalmazható; olyan ellenőrzéseket biztosít, amelyek az IoT biztonságához igazíthatók.	- Az IoT-eszközök és -rendszerek biztonsági ellenőrzésének kiválasztása és végrehajtása. - Az IoT-adatgyűjtéssel és -feldolgozással kapcsolatos adatvédelmi aggályok kezelése.
NIST 800-92	Útmutató a számítógépes biztonsági naplókezeléshez	A naplókat generáló IoT-rendszerek esetében releváns.	- Az IoT-eszközök naplóadatainak kezelése a biztonsági felügyelethez. - Az IoT által generált naplófájlok elemzése anomáliák észleléséhez és incidensekre való reagáláshoz.
NIST 800-160	Rendszerbiztonsági mérnöki tevékenység	Rendkívül releváns; a biztonságos IoT-rendszerek tervezésénél alkalmazható elveket kínál.	- A biztonsági megfontolások beépítése az IoT rendszerek tervezésébe és fejlesztésébe. - A rendszertechnikai elvek alkalmazása az IoT kiber-biztonságának fokozására.
NIST 800-163	A mobilalkalmazások biztonságának ellenőrzése	Közvetve releváns; az elvek kiterjeszthetők a tárgyak internete alkalmazásokra.	- Az IoT-alkalmazások biztonságának értékelése. - Az IoT-alkalmazások telepítésével

			kapcsolatos kockázatok kezelése.
NIST 800-213	IoT-eszközök kiberbiztonsági útmutatója a szövetségi kormányzat számára	Közvetlenül releváns; kifejezetten az IoT-re összpontosít.	- Átfogó útmutatás az IoT-eszközök védelméről. - Életciklus-menedzsment és kockázatcsökkentési stratégiák az IoT számára kormányzati környezetben.

3. táblázat: NIST keretrendszerek összehasonlítása

Összefoglalva ez az összehasonlítás rávilágít arra, hogy az egyes NIST keretrendszerek hogyan alkalmazhatók vagy befolyásolhatják az IoT eszközök és rendszerek kiberbiztonságát, kiemelve a sokoldalú megközelítést, amely az IoT-technológiák összetett területének biztosításához szükséges.

NISTIR 8259 sorozat

A NISTIR 8259 „Alapvető kiberbiztonsági tevékenységek IoT-eszközgyártók számára" című kiadványt a NIST jelentette meg. Alapvető útmutatást és ajánlásokat tartalmaz, amelyek kifejezetten az IoT használó eszközök gyártói számára készültek. A dokumentum része a NIST szélesebb körű erőfeszítéseinek, amelyek célja az IoT-eszközök kiberbiztonságának javítása, amelyek egyre inkább szerves részét képezik a különböző ágazatoknak, többek között az egészségügynek, a közlekedésnek és az okos épületeknek. [75] A NISTIR 8259 elsődleges célja, hogy segítséget nyújtson az IoT-eszközök gyártóinak az IoT-eszközök fejlesztése során a kiberbiztonsági intézkedések megértésében és végrehajtásában. Célja továbbá az ezekben az eszközökben rejlő biztonsági kihívások kezelése, amelyeket gyakran különféle, olykor kritikus környezetekben alkalmaznak.

A NISTIR 8259 az IoT-eszközök gyártóinak ajánlott alapvető kiberbiztonsági tevékenységeket vázol fel:

- Eszközazonosítás: A gyártóknak azt tanácsolják, hogy biztosítsák, hogy minden egyes eszköz fizikai vagy logikai eszközökkel egyedileg azonosítható legyen. Ez az azonosítás kulcsfontosságú az eszközök életciklusuk során történő kezeléséhez, különösen a frissítések és a biztonsági kezelés szempontjából. [75]

- Eszközkonfiguráció: Az iránymutatás hangsúlyozza a biztonságos alapértelmezett konfigurációk fontosságát, valamint azt, hogy a felhasználók a saját biztonsági igényeiknek megfelelően módosíthassák a konfigurációkat. Ez magában foglalja a konfigurációs adatok biztonságos tárolását is. [75]
- Adatvédelem: A dokumentum intézkedéseket javasol az IoT-eszközökön tárolt és az IoT-eszközök által továbbított adatok védelmére. Ez magában foglalja az adattitkosítás végrehajtását, valamint az adatok titkosságának és sértetlenségének biztosítását. [75]
- Logikai hozzáférés az interfészekhez: A NISTIR 8259 az IoT-eszközök interfészeinek – beleértve a fizikai és a hálózati interfészeket is – védelmére vonatkozó tanácsokat ad a jogosulatlan hozzáférés és az adatok megsértésének megelőzése érdekében. [75]
- Szoftver- és firmware-frissítések: A kiadvány hangsúlyozza az eszközszoftver és a firmware frissítésére szolgáló biztonságos mechanizmus szükségességét, beleértve a frissítés integritásának ellenőrzését is. [75]
- Kiberbiztonsági eseménynaplózás: A kiadvány javasolja, hogy az IoT-eszközök vezessenek naplót a kiberbiztonsági eseményekről, amelyek kulcsfontosságúak a biztonsági incidensek megértéséhez és enyhítéséhez. [75]

Hatás

- Az IoT-eszközök biztonságának fokozása: A NISTIR 8259 ezen alapvető iránymutatások biztosításával szerepet játszik az IoT-eszközök általános biztonsági helyzetének javításában, ami egyre fontosabbá válik, mivel ezek az eszközök mindenütt jelen vannak a kritikus és mindennapi alkalmazásokban.
- Szabványosítási erőfeszítések: A dokumentum hozzájárul az IoT-biztonság szabványosítási erőfeszítéseihez, olyan alapvonalat biztosít, amelyre a gyártók, a szabályozó hatóságok és a kiberbiztonsági szakemberek építhetnek.
- A szakpolitika és a szabályozás tájékoztatása: A NISTIR 8259 az IoT-biztonsággal kapcsolatos politikai és szabályozási vitákat is segíti, mivel jól meghatározott gyakorlatokat kínál, amelyek referenciaként szolgálhatnak az iparági szintű szabványok és szabályozások kidolgozásához. [75]

A NISTIR 8259 fontos lépést jelent a dolgok internetének gyorsan terjedő területével kapcsolatos kiberbiztonsági kihívások kezelésében. Azáltal, hogy az eszközgyártók felelősségére összpontosít, megteremti a biztonságosabb IoT-ökoszisztémák alapjait, és

ezáltal hozzájárul a modern élet szerves részévé váló technológiák rugalmasságához és megbízhatóságához.

ENISA

Az Európai Unió Kiberbiztonsági Ügynöksége (ENISA) 2017 novemberében közzétett "Alapvető biztonsági ajánlások a dolgok internetére a kritikus információs infrastruktúrákban" című dokumentum átfogó keretet nyújt az IoT, a kritikus információs infrastruktúrákban használt eszközei biztonságának fokozásához.

A dokumentum legfontosabb elemei

- Az IoT biztonságának elemzése a kritikus infrastruktúrákban: A dokumentum a kritikus infrastruktúrákban található IoT-eszközökkel kapcsolatos egyedi kihívásokra és sebezhetőségekre összpontosít. Hangsúlyozza, hogy a potenciális kiberfenyegetések elleni védelem érdekében szilárd biztonsági intézkedésekre van szükség.
- Biztonsági ajánlások és bevált gyakorlatok: A dokumentum kiemelt részét a konkrét biztonsági intézkedések és bevált gyakorlatok felvázolásának szenteli. Ezek az ajánlások a kockázatok mérséklésére és az IoT-eszközök általános biztonsági helyzetének javítására irányulnak. A dokumentum különböző biztonsági területeket fed le, többek között az engedélyezést, a személyazonosság- és hozzáférés-kezelést, valamint az IT biztonsági architektúrát.
- Átfogó biztonsági intézkedések: Az ajánlások közé tartozik a finomabb engedélyezési mechanizmusok, például az attribútumalapú hozzáférés-szabályozás (ABAC) vagy a szerepköralapú hozzáférés-szabályozás (RBAC) bevezetése, a legkisebb jogosultság elvének (POLP) betartása, valamint annak biztosítása, hogy a firmware tervezése elkülönítse a kiváltságos kódot és folyamatokat.
- Hivatkozás szabványokra és keretrendszerekre: A dokumentum hivatkozik különböző nemzetközi szabványokra és keretrendszerekre, például az ISO27001-re, a NIST SP 800-30-ra, a NIST SP 800-53-ra, az OWASP IoT Top Ten-re, valamint olyan szervezetek iránymutatásaira, mint az IoT Security Foundation és az Industrial Internet Consortium.
- Eszközök és fenyegetések taxonómiája: Az IoT szempontjából releváns eszközök és fenyegetések részletes taxonómiáját nyújtja, segítve a szervezeteket az IoT-

ökoszisztémájuk különböző összetevőinek és potenciális kockázatainak kategorizálásában és megértésében.

- IoT támadási forgatókönyvek: A dokumentum különböző IoT-támadási forgatókönyveket vázol fel, betekintést nyújtva abba, hogy a kiberfenyegetések hogyan jelentkezhetnek valós helyzetekben. Ez olyan forgatókönyveket tartalmaz, mint az IoT-adminisztrációs rendszer kompromittálása, az IoT-eszközök értékmanipulációja és a botnet/parancsinjekciós támadások.
- Életciklus-kezelés és felelősség tisztázása: Hangsúlyozza a biztonságos IoT-termék/szolgáltatás életciklus-menedzsment kialakításának és a felelősség tisztázásának fontosságát az IoT-érintett felek között.
- Mellékletek a részletes elemzéshez: A dokumentum mellékleteket tartalmaz, amelyek részletes biztonsági intézkedéseket, a biztonsági intézkedések és a fenyegetések közötti megfeleltetést, a biztonsági szabványok áttekintését és a tárgyak internetével kapcsolatos indikatív biztonsági incidensek leírását tartalmazzák. [76]

Az "Alapvető biztonsági ajánlások a dolgok internetére" című dokumentum alapvető fontosságú útmutatóként szolgál a kritikus információs infrastruktúrákban működő szervezetek számára. Strukturált megközelítést nyújt az IoT-eszközökkel kapcsolatos kockázatok azonosításához és mérsékléséhez. Ezen ajánlások beépítésével a szervezetek növelhetik IoT-infrastruktúrájuk biztonságát és ellenálló képességét a fejlődő kiberfenyegetésekkel szemben. A dokumentum átfogó jellege - amely a konkrét biztonsági intézkedésektől a szélesebb körű stratégiai megfontolásokig mindent lefed - felbecsülhetetlen értékű forrássá teszi a kiberbiztonsági szakemberek és a tárgyak internetbiztonságával foglalkozó politikai döntéshozók számára.

3.3. A kiberbiztonsági keretrendszerek általános elemzése

A kezdeti hiányelemzésemben megállapítottam, hogy a különböző keretrendszerekben nincsenek konkrét kiberbiztonsági ellenőrzési módszertanok az okos épületek tekintetében. Ebben a kibővített elemzésbe mélyebben foglalkozom a kiberbiztonsági szempontokkal, kiemelve az okos épületek által támasztott egyedi biztonsági kihívásokhoz igazított, speciális ellenőrzési módszertanok kritikus szükségességét. Ezzel létrehozva egy önálló kiberbiztonsági ellenőrzőlistát az okos épületekhez.

A kiberbiztonsági hiányosságok részletes vizsgálata

- Az IoT-rendszerek összetettsége

- Kiberbiztonsági kihívások: Az IoT-rendszerek eszközök, protokollok és hálózati konfigurációk komplexek. Éppen ezért a hagyományos biztonsági ellenőrzési módszerek nem megfelelőek az ilyen összetett környezetek esetében, mivel nem foglalkoznak a dolgok internetéhez kapcsolódó sajátos sebezhetőségekkel és fenyegetésvektorokkal.

- Az IoT fenyegetések dinamikus jellege
  - Kiberbiztonsági kihívások: Az IoT-eszközök gyorsan fejlődő kiberbiztonsági fenyegetéseknek vannak kitéve. Így a hatékony IoT biztonsági ellenőrzési módszertannak alkalmazkodóképesnek kell lennie, és képesnek kell lennie az újonnan megjelenő fenyegetések és sebezhetőségek valós idejű azonosítására.
- Integráció a meglévő rendszerekkel
  - Kiberbiztonsági kihívások: Az IoT-eszközök gyakran integrálódnak a meglévő IT- és OT-rendszerekkel. Egy átfogó IoT biztonsági ellenőrzési módszertannak nem csak magukra az eszközökre, hanem a más rendszerekkel való kölcsönhatásukra is ki kell terjednie, felmérve a biztonság megsértése esetén fellépő kaszkádhatások lehetőségét.

Az IoT biztonsági ellenőrzési módszertan javasolt elemei

- Eszközszintű biztonság
  - Módszertani komponens: Az egyes IoT-eszközök biztonsági helyzetének értékelése, beleértve a firmware integritását, a hitelesítési mechanizmusokat és az adattitkosítási szabványokat. Ennek az értékelésnek figyelembe kell vennie az eszközök fizikai biztonsági szempontjait is.
- Hálózatbiztonság
  - Módszertani komponens: Azon hálózatok biztonságának elemzése, amelyekhez az IoT-eszközök csatlakoznak. Ez magában foglalja a hálózati szegmentáció, a kommunikációs protokollok és a tranzitadatok biztonságának értékelését.
- Az ökoszisztéma egészére kiterjedő kockázatelemzés
  - Módszertani komponens: A teljes IoT-ökoszisztéma holisztikus kockázatelemzésének elvégzése, a lehetséges sebezhetőségek

rendszerszintű azonosítása, beleértve a különböző eszközök és rendszerek közötti kölcsönhatásokat is.

- Megfelelőségi és szabályozási felülvizsgálat
    - Módszertani komponens: Annak biztosítása, hogy az IoT-ökoszisztéma megfeleljen a vonatkozó kiberbiztonsági előírásoknak és szabványoknak. Ezt a felülvizsgálatot a tárgyak internetének telepítésére vonatkozó konkrét jogi és szabályozási környezethez kell igazítani.
- Incidensreakció és helyreállítási tervezés
    - Módszertani komponens: A dolgok internetére jellemző incidensre adott válasz- és helyreállítási tervek hatékonyságának értékelése. Ez magában foglalja a veszélyeztetett eszközök gyors elszigetelésére és a normál működés helyreállítására való képesség értékelését.

A kiterjesztett hiányelemzésben hangsúlyozom, hogy átfogó IoT biztonsági ellenőrzési módszertanra van szükség, amely foglalkozik az IoT-ökoszisztémák egyedi kiberbiztonsági kihívásaival. Egy ilyen módszertannak dinamikusnak kell lennie, és magában kell foglalnia az eszközszintű biztonságot, a hálózatelemzést, az ökoszisztéma egészére kiterjedő kockázatértékelést, a megfelelőség felülvizsgálatát és az incidensekre való reagálás tervezését. E módszertan kidolgozása és bevezetése javítani fogja az IoT telepítések biztonsági helyzetét, különösen az olyan kritikus ágazatokban, mint az okos épületek.

3.4. A NIST SP 800-as sorozat elemzése IoT kiberbiztonsági szempontból

A NIST SP 800-as sorozata szilárd keretrendszert biztosít a kiberbiztonsághoz, a dolgok internetére való alkalmazása egyedi kihívásokat jelent. Ez a kiterjesztett hiányelemzésem a NIST SP 800-as sorozat IoT-specifikus aspektusaira összpontosít, különösen az IoT-biztonsági ellenőrzési módszertan hiányát vizsgálva.

A NIST SP 800-as sorozat, amely olyan dokumentumokat tartalmaz, mint a NIST SP 800-53 és a NIST SP 800-183, átfogó iránymutatásokat kínál a kiberbiztonsági gyakorlatokról. Ezek az iránymutatások azonban gyakran általánosak, és nem kifejezetten az IoT-ökoszisztémák árnyalt követelményeihez igazodnak. A sorozat, bár alapvető kiberbiztonsági keretrendszert biztosít, nem tartalmaz speciális módszertant az IoT-eszközök és -rendszerek biztonságának ellenőrzésére, különösen az olyan összetett környezetekben, mint az okos épületek.

A hiányosságok és kihívások azonosítása

- Az IoT-eszközök sokféleségének sajátosságai: Az IoT-eszközök funkcionalitásuk, összetettségük és biztonsági képességeik tekintetében széles skálán mozognak. A NIST SP 800-as sorozat nem ad konkrét útmutatást a dolgok internetének eszközei sokféleségének ellenőrzésére, az egyszerű érzékelőktől az összetettebb összekapcsolt rendszerekig.
- Valós idejű biztonsági értékelési igények: IoT-környezetek dinamikus jellegük miatt valós idejű biztonsági értékeléseket igényelnek. A NIST SP 800-as sorozatából hiányoznak a tárgyak internete eszközeinek és hálózatainak folyamatos nyomon követésére és valós idejű értékelésére vonatkozó konkrét módszerek.
- Integráció a meglévő architektúrákba: Az IoT-eszközöknek gyakran integrálódniuk kell a meglévő IT- és OT-rendszerekkel. A NIST 800 sorozat nem nyújt részletes útmutatást az ilyen integrációk biztonsági vonatkozásainak ellenőrzésére vonatkozóan, ami elengedhetetlen az átfogó IoT-biztonság szempontjából.

3.5. Szabályozási rendszerek

Ebben az alfejezetben kritikusan megvizsgáljuk a kulcsfontosságú szabályozással kapcsolatos rendszereket - a Kiberrezilienciáról szóló jogszabály, a GDPR és a NIS2 – az IoT egyre növekvő területének keretmetszetéből. Elemzésemben azt vizsgálom, hogy ezek a szabályozások hogyan alakítják és szabályozzák az IoT-implementációkat, különös tekintettel a megfelelésre, az adatvédelemre és a kiberbiztonsági ellenálló képességre. Megvizsgálom az egyes szabályozási rendszerek konkrét mandátumait és következményeit, értékelve azok hatását a dolgok internetére épülő eszközök telepítésére és kezelésére a különböző ágazatokban. Célom, hogy megvilágítsam a fejlődő szabályozási környezetet és annak szerepét a biztonságos és felelős IoT-gyakorlatok biztosításában.

Kiberrezilienciáról szóló jogszabály

A kiberrezilienciáról szóló jogszabály (EU Cyber Resilience Act) jogalkotási kezdeményezést jelent, amelynek célja a digitális termékek és szolgáltatások kiberbiztonsági helyzetének megerősítése. Kutatásom során a legfrissebb információk 2024. januárjában elérhető változatát dolgoztam itt fel. Ez a törvény egy szélesebb körű stratégia részét képezi, amelynek célja a digitális infrastruktúrák ellenálló képességének

növelése és a kibertérben jelentkező növekvő fenyegetések elleni védelem. A törvény tükrözi a kiberbiztonság kritikus fontosságának növekvő felismerését a digitális korban a köz- és magánszektor érdekeinek védelme szempontjából. A Kiberrezilienciáról szóló jogszabály elsődleges célja, hogy átfogó jogi keretet hozzon létre a digitális termékek és szolgáltatások magas szintű kiberbiztonságának biztosítására. Ez magában foglalja a gyártókra, fejlesztőkre és szolgáltatókra vonatkozó egyértelmű szabványok és követelmények meghatározását, amelynek célja a sebezhetőségek csökkentése és a digitális ökoszisztémák általános biztonságának fokozása.

A jogszabály előírja a biztonsági funkciók integrálását már a digitális termékek és szolgáltatások tervezési szakaszában. Ez a „tervezés általi biztonság" megközelítés biztosítja, hogy a kiberbiztonsági megfontolások beépülnek a fejlesztési folyamatba, és nem utólagos szempontok maradnak. A jogszabály előírja a jogalanyok számára, hogy megbízható kockázatkezelési folyamatokat hajtsanak végre, és jelenteniük kell a kiberbiztonsági incidenseket. E rendelkezés célja, hogy elősegítse a kiberkockázatok azonosításának és mérséklésének proaktív megközelítését. A jogszabály hangsúlyozza a kiberbiztonsági gyakorlatok átláthatóságát és a megállapított szabványoknak való megfelelést. Kötelezi a jogalanyokat, hogy hozzák nyilvánosságra a termékeik és szolgáltatásaik kiberbiztonsági jellemzőire vonatkozó releváns információkat. A jogszabály hangsúlyt fektet a fogyasztók kiberfenyegetésekkel szembeni védelmére. Olyan rendelkezéseket tartalmaz, amelyek biztosítják, hogy a fogyasztók tájékoztatást kapjanak a digitális termékekkel és szolgáltatásokkal kapcsolatos kiberbiztonsági jellemzőkről és kockázatokról.

A Kiberrezilienciáról szóló jogszabály döntő szerepet játszik a kiberbiztonsági szabványok emelésében a különböző ágazatokban. Azáltal, hogy egyértelmű jogi követelményeket állapít meg, a digitális termékek és szolgáltatások biztonságának javítását ösztönzi. A jogszabály hozzájárul a kiberbiztonsági kultúra előmozdításához, ahol a biztonsági megfontolások a digitális megoldások fejlesztésének és bevezetésének szerves részét képezik. A digitális infrastruktúrák biztonságának fokozásával a jogi aktusnak gazdasági és társadalmi hatásai vannak. Hozzájárul a kibernetikai incidensekből eredő pénzügyi veszteségek elleni védelemhez, és védi az egyének magánéletét és jogait a digitális térben.

A jogszabálynak való megfelelés biztosítása kihívást jelent, különösen a kisebb szervezetek számára, amelyeknek esetleg nincsenek meg a szigorú követelményeknek való megfeleléshez szükséges erőforrásaik és szakértelmük. Az innováció iránti igény és

a szilárd kiberbiztonság követelményeinek egyensúlyba hozása kritikus szempont. A jogszabálynak biztosítania kell, hogy a biztonsági követelmények ne fojtsák el az innovációt a digitális ágazatban. [77]

A Kiberrezilienciáról szóló jogszabály mérföldkőnek számító kezdeményezés a kiberbiztonsági jogszabályok terén. Hangsúlyozza a digitális világ szilárd biztonsági intézkedéseinek kritikus szükségességét, és precedenst teremt a jövőbeni jogalkotási erőfeszítésekhez ezen a területen. A jogszabály a tervezés általi biztonságra, a kockázatkezelésre, az átláthatóságra és a fogyasztóvédelemre helyezi a hangsúlyt, ami lépést jelent a biztonságosabb és ellenállóbb digitális jövő felé.

GDPR

Az Általános adatvédelmi rendelet (GDPR) az Európai Unió által elfogadott átfogó adatvédelmi törvény. Bár elsődlegesen a személyes adatok és a magánélet védelmére összpontosít, hatásai kiterjednek a kiberbiztonság, a dolgok internete és az okos épülettechnológiák területére is. A GDPR átformálta az adatbiztonság megközelítését ezeken a területeken, hangsúlyozva a személyes adatok védelmének fontosságát az egyre inkább összekapcsolt digitális környezetben. A kiberbiztonsággal összefüggésben a GDPR szigorú követelményeket vezet be az adatvédelemre és a jogsértések bejelentésére vonatkozóan. Kötelezi a szervezeteket, hogy megfelelő technikai és szervezeti intézkedéseket hajtsanak végre a magas szintű biztonság biztosítása érdekében, különösen a személyes adatok feldolgozása során. Ez magában foglalja a titkosítás, a hozzáférés-ellenőrzés és a rendszeres biztonsági értékelések alkalmazását. Adatvédelmi incidens esetén a GDPR előírja az illetékes hatóságok és bizonyos esetekben az érintett személyek azonnali értesítését, különösen, ha az adatvédelmi incidens magas kockázatot jelent a jogaikra és szabadságaikra nézve.

Az IoT-eszközök elterjedése aggodalmakat vetett fel az adatvédelemmel és az adatbiztonsággal kapcsolatban, különösen azért, mert ezek az eszközök gyakran nagy mennyiségű személyes adatot gyűjtenek. A GDPR értelmében az IoT-eszközök gyártóinak és szolgáltatóinak olyan elveket kell betartaniuk, mint az adatminimalizálás, a célhoz kötöttség és az érintettek hozzájárulása. Emellett olyan intézkedéseket kell végrehajtaniuk, amelyek biztosítják a beépített és alapértelmezett adatvédelmet. Ez azt jelenti, hogy az IoT-eszközöket és -alkalmazásokat az adatvédelmi szempontok figyelembevételével kell megtervezni, biztosítva a személyes adatok biztonságos és átlátható feldolgozását.

Az okos épületek, amelyek IoT-technológiákat használnak különböző funkciókhoz, például energiagazdálkodáshoz, biztonsághoz és környezetszabályozáshoz, a GDPR hatálya alá tartoznak, amikor az uniós polgárok személyes adatait dolgozzák fel. A GDPR-nak való megfelelés az okos épületekben annak biztosítását jelenti, hogy a lakosoktól vagy felhasználóktól gyűjtött adatokat a GDPR elveinek megfelelően kezeljék. Ez magában foglalja az adatgyűjtéshez való kifejezett hozzájárulás megszerzését, az adatok felhasználásának átláthatóságát, valamint a lakosok számára az adataik feletti ellenőrzés biztosítását. Az okos épületek üzemeltetőinek és a technológiai szolgáltatóknak azt is biztosítaniuk kell, hogy szilárd mechanizmusokkal rendelkezzenek az adatbiztonság megsértésének észlelésére, jelentésére és az arra való reagálásra.

A GDPR végrehajtása a kiberbiztonság, a tárgyak internete és az okos épületek összefüggésében számos kihívást jelent. Az egyik elsődleges kihívás a GDPR-nak megfelelő adatvédelmi és biztonsági intézkedések integrálása a meglévő rendszerekbe és technológiákba. Ez gyakran extra beruházásokat igényel a technológiai korszerűsítések és a személyzet képzése tekintetében. Emellett az IoT-ökoszisztémák és az okos épületek környezetének dinamikus és összetett jellege miatt a folyamatos megfelelőség-ellenőrzés és -irányítás igényes feladat. [78]

A GDPR hatással van a kiberbiztonságra, a IoT-re, így az okos épületek technológiáira, mivel magas szintű adatvédelmi és adatvédelmi normákat határoz meg. A személyes adatok védelmére, az adatfeldolgozás átláthatóságára és az adatbiztonság megsértéséért való felelősségre vonhatóságra helyezett hangsúlya szükségessé tette a szervezetek adatbiztonsághoz való hozzáállásának megváltoztatását ezeken a területeken. Így a GDPR nemcsak az egyéni adatvédelmi jogokat védi, hanem a kiberbiztonsági gyakorlatok terén is előrelépést eredményez.

NIS2 irányelv

A NIS2 irányelv, amely a hálózati és információs rendszerekről szóló uniós irányelv továbbfejlesztése jogalkotási fejleményt jelent a kiberbiztonság területén. Célja a hálózati és információs rendszerek biztonságának megerősítése az Európai Unióban, különös tekintettel a kritikus ágazatokra. Az irányelv kibővített hatálya és szigorú követelményei hatással vannak az IoT kiberbiztonságra. Kutatásom során a legfrissebb információk 2024. januárjában elérhető változatát dolgoztam itt fel.

A NIS2 irányelv a kiberbiztonsági kötelezettségeket az ágazatok és szervezetek szélesebb körére terjeszti ki, beleértve a digitális szolgáltatókat és a kritikus infrastruktúrán belüli

szervezeteket is. Kötelezi kockázatkezelési intézkedések és incidensjelentési protokollok végrehajtását. A kiberbiztonság tekintetében ez a fenyegetések azonosítására, a biztonsági ellenőrzésekre és az incidensekre reagáló mechanizmusokra vonatkozó fokozott kötelezettségeket jelent. Az irányelv hangsúlyozza a kiberbiztonság proaktív megközelítésének szükségességét, megkövetelve a szervezetektől, hogy megelőzzék az újonnan megjelenő fenyegetéseket és folyamatosan frissítsék biztonsági gyakorlataikat.

Az IoT-eszközök elterjedése kiberbiztonsági aggályokat vetett fel, különösen a kritikus ágazatokban. A NIS2 ezeket az aggályokat a szabályozási keretnek a dolgok internete eszközeire és szolgáltatásaira való kiterjesztésével kezeli. Ez magában foglalja az eszközök biztonságos fejlesztésére, gyártására és telepítésére vonatkozó követelményeket. A NIS2 értelmében az IoT-eszközök gyártóinak és szolgáltatóinak biztosítaniuk kell, hogy termékeik és szolgáltatásaik megfeleljenek a szigorú kiberbiztonsági előírásoknak, csökkentve ezzel a sebezhetőséget és fokozva az IoT-ökoszisztémák általános biztonságát.

Az okos épületek, amelyek különböző funkciók tekintetében nagymértékben támaszkodnak az IoT-technológiákra, a NIS2 hatálya alá tartoznak, amennyiben a kritikus infrastruktúra részét képezik vagy digitális szolgáltatásokat használnak. Az irányelv megköveteli, hogy az okos épületek technológiái ne csak a kiberbiztonsági szabványoknak feleljenek meg, hanem biztosítsák a hálózati és információs rendszereik ellenálló képességét is. Ez magában foglalja a kibertámadások elleni védelmet szolgáló szilárd biztonsági intézkedések végrehajtását, az épületüzemeltetés folyamatosságának biztosítását, valamint az okos épületrendszerek által gyűjtött és feldolgozott adatok védelmét. A NIS2-irányelv betartása számos kihívást jelent, különösen azon szervezetek számára, amelyek korábban nem tartoztak az eredeti NIS-irányelv hatálya alá. Az IoT-gyártók és az okos épületek üzemeltetői számára ez azt jelenti, hogy termékeiket és rendszereiket hozzá kell igazítaniuk az új biztonsági követelményekhez, ami technológiai és eljárási fejlesztéseket jelenthet. Emellett az irányelv kockázatkezelésre és incidensjelentésre való összpontosítása strukturált megközelítést igényel a kiberbiztonság tekintetében, ami a biztonsági gyakorlatok folyamatos nyomon követését, értékelését és kiigazítását teszi szükségessé. [79]

A NIS2-irányelv kritikus lépést jelent az EU kiberbiztonsági környezetének megerősítésében, különösen a kritikus ágazatok növekvő digitalizációjával szemben. A kibővített hatály és a szigorú követelmények hatással van az okos épületek IoT

kiberbiztonságára, ösztönzik a biztonsági gyakorlatok fejlesztését és fokozzák a kritikus hálózati és információs rendszerek ellenálló képességét.

3.6. A GDPR, a NIS2 és a kiberrezilienciáról szóló jogszabály elemzése IoT kiberbiztonsági szempontból

Ez a kiterjesztett hiányelemzés azt vizsgálja, hogy a GDPR, a NIS2-irányelv és a kiberrezilienciáról szóló jogszabály mennyire megfelelő az IoT kiberbiztonsága szempontjából, különös tekintettel a biztonsági ellenőrzésére vonatkozó konkrét módszertan hiányára. Bár ezek a keretrendszerek átfogó iránymutatásokat nyújtanak az adatvédelem és a kiberbiztonság tekintetében, a dolgok internetének egyedi kihívásaira való alkalmazhatóságuk alaposabb vizsgálatot igényel.

Az okos épület kiberbiztonsági fókusz

- GDPR: A GDPR elsősorban az adatvédelemmel és a magánélet védelmével foglalkozik, és hatással van a személyes adatokat feldolgozó IoT-eszközökre. Hiányoznak azonban az IoT-eszközök átfogó biztonsági ellenőrzésének elvégzésére vonatkozó kifejezett iránymutatások, ami elengedhetetlen az adatvédelem és a megfelelőség biztosításához.
- NIS2 irányelv: A NIS2 irányelv a kiberbiztonsági kötelezettségeket az ágazatok szélesebb körére terjeszti ki, potenciálisan a dolgok interneteinek eszközeire is kiterjedve. Mégsem nyújt részletes keretet az IoT-rendszerek biztonságának ellenőrzésére, különösen azokban az ágazatokban, ahol az IoT integrációja kritikus jelentőségű.
- Kiberrezilienciáról szóló jogszabály: Célja a digitális termékek, köztük az IoT-eszközök biztonságának megerősítése. A jogszabály azonban elsősorban a kiberfenyegetésekkel szembeni ellenálló képességre összpontosít, és nem határozza meg az IoT-ra vonatkozó biztonsági ellenőrzések elvégzésének módszertanát.

A hiányosságok azonosítása

- Az IoT kiberbiztonsági specifikussága a GDPR-nak: Mivel a GDPR nem tartalmaz konkrét IoT kiberbiztonsági iránymutatásokat az okos épületekkel kapcsolatban, a szervezetek gyakran küzdenek annak biztosításával, hogy IoT-eszközeik megfeleljenek az adatvédelmi követelményeknek. Ez a hiányosság következetlenségekhez vezethet a megfelelés és a biztonsági gyakorlatok terén.

- IoT-ellenőrzési keretrendszer hiánya a NIS2-ben: Bár a NIS2 fokozott kiberbiztonsági intézkedéseket ír elő, a részletes IoT biztonsági ellenőrzési keretrendszer hiánya nem megfelelő biztonsági gyakorlatokat eredményezhet, különösen az IoT-t használó kritikus infrastrukturális ágazatokban.
- Korlátozott IoT-ellenőrzési útmutatás a kiberrezilienciáról szóló jogszabályban: A digitális termékek biztonságára való összpontosítása ellenére nem biztosít átfogó ellenőrzési módszertant a dolgok internete eszközeire vonatkozóan. Ez a mulasztás sebezhetőségekhez vezethet a tárgyak interneteinek ökoszisztémáiban, ami kihat az általános kiberbiztonságra.

3.7. IoT Security Foundation

A londoni székhelyű IoT Security Foundation (IoTSF) egy együttműködő, nonprofit szervezet, amely a IoT biztonságának fokozására törekszik. Az IoTSF-et azért hozták létre, hogy reagáljon az IoT biztonsága körüli növekvő aggodalmakra, és a legjobb gyakorlatok népszerűsítésére, iránymutatás nyújtására és a biztonsági kultúra előmozdítására összpontosít az IoT ökoszisztéma valamennyi érdekeltje körében. Az IoTSF elsődleges küldetése az IoT biztonságosabbá és biztonságosabbá tétele. Ezt az IoT-eszközök és -rendszerek elterjedése által támasztott széles körű biztonsági kihívások kezelésével érjük el. A szervezet célkitűzései közé tartozik a tudatosság növelése, a szilárd biztonsági szabványok támogatása és a tudásmegosztás elősegítése az iparági szereplők között.

Főbb tevékenységek és kezdeményezések

- A legjobb gyakorlatok kidolgozása: Az IoTSF fontos szerepet játszik a dolgok internetének biztonságára vonatkozó legjobb gyakorlatokra vonatkozó iránymutatások kidolgozásában és terjesztésében. Ezek az iránymutatások különböző szempontokra terjednek ki, beleértve az eszközbiztonságot, a hálózati biztonságot és az adatvédelmet. Úgy tervezték, hogy az iparágak és IoT-alkalmazások széles körében alkalmazhatóak legyenek.
- Képzés és oktatás: Az IoTSF nagy hangsúlyt fektet az oktatásra és képzésre. A szervezet workshopokat, webináriumokat és konferenciákat szervez, hogy a gyártók, fejlesztők és felhasználók számára az IoT-biztonság fontosságáról és a legjobb módszerekről oktatást nyújtson.
- Együttműködés és érdekérvényesítés: Az IoTSF együttműködik az iparági csoportokkal, szabályozó testületekkel és kormányzati ügynökségekkel, hogy az

IoT erősebb biztonsági intézkedéseiért szálljon síkra. Kulcsszerepet játszik az IoT biztonságával kapcsolatos szakpolitikai és szabályozási fejlemények befolyásolásában.

Az IoTSF kutatásokat végez az IoT biztonságának különböző aspektusairól, valamint jelentéseket és fehér könyveket ad ki. Ezek a kiadványok értékes betekintést nyújtanak az aktuális biztonsági trendekbe, a felmerülő fenyegetésekbe és a lehetséges megoldásokba. Forrásként szolgálnak az iparági szakemberek, a tudományos szakemberek és a politikai döntéshozók számára.

Kihívások és hatás

- A különböző biztonsági igények kielégítése: Az IoTSF előtt álló egyik kihívás az IoT sokszínűsége, amely az eszközök és alkalmazások széles skáláját foglalja magában. Az átfogó és a különböző kontextusokra adaptálható biztonsági iránymutatások kidolgozása összetett feladat.
- Fejlődő fenyegetettségi környezet: A kiberfenyegetések gyorsan változó jellege folyamatos kihívást jelent. Az IoTSF-nek e fejlemények előtt kell járnia, hogy releváns és hatékony biztonsági iránymutatásokat nyújtson.
- Iparági elfogadás és megfelelés: További kihívást jelent a legjobb biztonsági gyakorlatok széles körű elfogadásának ösztönzése és a megfelelőség biztosítása a gyártók és fejlesztők körében. Az IoTSF a biztonsági kultúra kialakításán dolgozik az iparágon belül, ami elengedhetetlen ahhoz, hogy iránymutatásai hatékonyak legyenek.

Az IoT Security Foundation kulcsfontosságú szerepet játszik az IoT-ökoszisztéma biztonságának fokozásában. A legjobb gyakorlatok kidolgozására, az erősebb biztonsági intézkedések támogatására és az együttműködés előmozdítására irányuló erőfeszítései révén az IoTSF hozzájárul ahhoz, hogy az IoT-eszközök és -rendszerek biztonságosabbá váljanak a felhasználók számára, és ellenállóbbak legyenek a kiberfenyegetésekkel szemben.

3.8. A szakértői mélyinterjúk eredményeinek bemutatása

Kutatósmódszertani szempontból szakértői mélyinterjúkat készítettem hazai szakemberekkel, akik a témámhoz kapcsolódó fő területen tevékenykednek. Őket az elmúlt évek személyes és szakmai tapasztalata alapján választottam. Fontos szempont volt a kiválasztás során a szakmában szerzett releváns tapasztalat, minősítések megléte, illetve az esetleges referenciák. Az általam összeállított 12 kérdéses (1. függelék)

kérdéssoron mentünk végig, melyeket legjobb tudások és tapasztalatuk szerint válaszoltak meg. Célom az volt, hogy képet kapjak arról, hogy ők hogyan látják a hazai és nemzetközi helyzetét az okos épületek kiberbiztonságának. Az interjúkat személyesen és online készítettem a résztvevők írásos hozzájárulásával, melyek 30-60 perc hosszúságúak voltak. Annak érdekében, hogy jobban feldolgozható legyen felvételt készítettem a beszélgetésekről, melyeket a Cockatoo[1] AI alapú átiratkezelővel a hangfájlokat átkonvertáltam szöveges dokumentum formájába. Az eszköz 98%-osan volt pontos, így néhány helyen a tördelésbe és helyesírásba bele kellett javítani. Az alábbi táblázatban összesítve látható minden interjúalany a pozíciójuk, cégnév és szakmai területük alapján.

#	Név	Pozició, cég	Szakmai terület
1	Balázs Zoltán	Vezető sérülékenységi kutató – Cujo AI	Okos otthonok biztonsága
2	Dr. habil. Buttyán Levente	Laborvezető, egyetemi tanár - CrySyS Lab, BME	IoT biztonság, vezeték nélküli hálózatok kiberbiztonsága, szoftverbiztonság
3	Dr. Dombora Sándor	Óraadó - Óbudai Egyetem KVK	Információbiztonság, audit
4	Fehér Dávid János	Security Architect - Blackbelt Technology Kft.	Audit, incidenskezelés, infrastruktúra biztonság, felhő biztonság
5	Görgényi István	Enterprise Architect – MOL-csoport	Okos épületek informatikai architektúrális tervezése és auditálása, fejlesztői folyamatok vezetése
6	Rubóczki László	Solution Architect – Rubedi Kft.	Felhőtechnológiák, okos épületek hálózatinformatikai architektúrális tervezése
7	Varga Péter	GCISO és MOL Campus MD – MOL-csoport	Kiberbiztonsági vezető ás MOL Campus üzemeltetési igazgató

[1] Forrás: www.cockatoo.com

8	Zsák Péter	Elnök - Magyar Okosotthon és Épületautomatizálási Szövetség	Okosotthon és épületautomatizálási rendszerek tervezése

4. táblázat: Interjúalanyok

3.8.1. Kiberbiztonsághoz kapcsolódó szakértői interjúk összegzett elemzése

A szakértői interjú készítéséhez a mintavételem azon alapult, hogy olyan elismert személyekkel készítsek interjút, akik szakmai háttere, tapasztalata és képesítése garantálta, hogy hozzáértő és a kutatást előbbre vivő irányokat kapjak tőlük a kutatásomban szereplő hipotéziseimhez. Így ebben a részben a kiberbiztonsági szakemberek (#1, 2, 3, 8) által elmondott összegzett következtetések kerülnek bemutatásra.

A 1. függelékben található kérdések közül a kiemelten kiberbiztonsági relevanciával rendelkezőkre (1, 2, 6, 8, 10, 12. kérdés) a szakértők összegzett válasza alapján egyértelműen kijelenthető, hogy az IoT eszközök kiberfenyegetettsége növekszik évről-évre, melyet azzal indokoltak a szakértők, hogy egyre nagyobb az IoT eszközök piaca, így a jelenléte is folyamatosan nő az egyes ipari szektorokban. A zsarolóvírusok folyamatos elterjedése is nagy veszélyt jelent az IoT eszközökre nézve, mivel a kiberbűnözőknek egyre jövedelmezőbb az erről a területről származó bevétel. Védelmi szempontból az egyre jobban fejlődő MI segítséget jelent a szakemberek számára az egyes támadások detektálásában és esetleges megfékezésében, ami az IoT rendszerekre is átültethető, hiszen léteznek már olyan okos szűrő rendszerek, melyek az abnormális tevékenységet észlelve automatikusan elzárják a forgalom elől a fertőzött eszközt, vagy hálózatot. Nagyban nehezíti azonban az okos épületek esetében az IoT eszközök védelmét az a tény, hogy a folyamatosan fejlődő technológia miatt rengetek startup cég jelent meg a piacon, akik hatalmas ígéretekkel rendelkeznek, viszont a biztonság sok esetben nem szerepel az eszközeik, vagy szolgáltatásaik között. Továbbá, hogy ahány épület annyi igény, így több 10-100 különféle rendszernek az informatikai integrálása és azok védelme is nagy nehézségeket okoz a szakembereknek. Azonban abban bíznak, hogy az új szabványok (Matter és Thread) segítséget nyújtanak a konszolidációban. Hiányolják továbbá azokat a kézzelfogható javaslatokat, melyekkel megfelelően lehet megtervezni és üzemeltetni egy épületet. Éppen ezért előre mutatónak ítélik meg a kutatásom annak érdekében, hogy az okos épületek kiberbiztonságával foglalkozom. Ezen felül pedig a

legnagyobb kihívást az okos épületekben található IoT-eszközök sebezhetőségével kapcsolatban nyilatkozták a szakértők egyöntetűen, hogy egyes eszközök olyan alacsony kapacitással és funkcióval rendelkeznek, hogy védelmük nagy kihívás elő állítja őket hiszen sokszor még akár egy gyári jelszót sem lehet lecserélni, vagy éppen nem képes az eszköz tanúsítvány alapú azonosításra. Végezetül pedig a szakértők a jelenlegi helyzetet értékelve elmondták, hogy nincs olyan konkrét intézkedés, amit IoT eszközökre, vagy rendszerekre lehetne egységesen alkalmazni, így inkább a meglévő informatikai rendszerek szabványait és ajánlásait veszik alapiul.

3.8.2. IoT és okos épület technológiához kapcsolódó szakértői interjúk összegzett elemzése

IoT és okos épület szakemberek (#1, 2, 5, 6, 8, 9) által elmondott összegzett következtetések ismertetése a 7, 9, 11. kérdésekre adott válaszok alapján az alábbiakat támasztják alá.

Fontos kiemelni azt a szakértői tényt, hogy az okos épületekben elhelyezett szenzorok rengeteg adatot gyűjtenek, akár másodpercenként több gigabyte-ot. Ezeket az adatokat megfelelően le kell tárolni, hogy ne sérülhessen a CIA-elv. Az egyik szakértő véleménye, hogy a blokklánc technológia kiválóan alkalmas lehet naplófájlok tárolására is, hiszen az tárolt adatok meghamisíthatatlanok, így garantálható az integritása. Ezt alátámasztja egy közös kutatásom Fehér Dávid Jánossal is, amit *„Log File Authentication and Storage on Blockchain Network”* címen készítettünk [80], amiben azt vizsgáljuk, hogy hogyan lehet naplófájlokat szétdarabolni és biztonságosan letárolni blockchain hálózaton. „*Annak érdekében, hogy egy okos épületben teljesülhessen a felhasználói élmény, különféle kompromisszumokat kell kötni”*, emelte ki az 5. számú interjúalany, aki a MOL Campus IoT hálózatának tervezésében is részt vett. „*Tekintettel arra, hogy a felhasználók, munkavállalók nagy része nem rendelkezik informatikai ismeretekkel, így hátrány lehet egy olyan rendszer, ami bonyolult számukra és túl van biztosítva. Itt jön képbe az a kiberbiztonsági elv, hogy amennyiben egy rendszert túlbiztosítunk, úgy az a felhasználói élmény rovására megy. Felhasználói élmény szempontjából figyelembe kell vegyük”* – hangsúlyozta az Okosotthon Szövetség elnöke, Zsák Péter –, továbbá a „*felhasználók oktatása nagy szerepet kell játsszon ezen épületek átadását követően, illetve a tervezési folyamatok során érdemes fókuszcsoportokat kialakítani, akiken keresztül lemérhető és később implementálhatóak a belső szabályzatok és szokások. Egyik szakértő véleménye alapján azonban van olyan korosztály, akinél nehézségeket okozhat egy ilyen épület*

megértése és használata, hiszen olyan innovatív megoldásokat kell használniuk, amik hosszú évekkel ezelőtt még nem léteztek, így nehezen, vagy egyáltalán nem tudnak adaptálódni." Összetett következtetés pedig, hogy a szabványosítás egy örök kérdés, hiszen egy felől biztonságot ad, hiszen a tervező és kivitelező is ugyan azon a szabvány alapján tudja elvégezni a munkálatokat egy ilyen rendszer kialakításánál, üzemeltetésénél. Másrészt pedig egy nehézség is, hiszen folyamatosan jelennek meg új eszközök és technológiák, amik egy szabvány előtt járhatnak az innovációnak köszönhetően. Így esetlegesen hátráltató hatással lehet rá egy zárt-rendszerű, kötött szabvány.

Összefoglalva a fejezetet, összehasonlító elemzést végeztem az okos épületek tanúsítási rendszerein, nevezetesen a BREEAM és a LEED rendszereket, valamint elemzem az olyan kiberbiztonsági tanúsítási rendszereket, mint az ISO27001 és az ISO30141, megvilágítva azok jelentőségét és alkalmazását az okos épületek paradigmáján belül. Az értekezés középpontjában a különböző NIST-keretrendszerek részletes összehasonlítása és elemzése áll, betekintést nyújtva az okos épületek kiberbiztonságának fokozásához való konkrét javaslattételbe. A fejezetben továbbá a szabályozási környezetet is vizsgálom, elemezve a GDPR-t, a NIS2 irányelvet és a Kiberrezilienciáról szóló jogszabály tervezetet. Kiemelve a magánéletre, az adatvédelemre és a kiberbiztonság rugalmasságára gyakorolt hatásukat az IoT-alapú intelligens épületekkel összefüggésben. Továbbá elemzésre kerültek a mélyinterjúk is, melyek alátámasztották a hipotéziseim egy részét.

4. KIBERBIZTONSÁGI SZEMPONTOK INTEGRÁLÁSÁNAK VIZSGÁLATA

A korábban elemzett keretrendszerekre építve ismertetem az általam kialakított megbízható és átfogó értékelési keretrendszert, mely javíthatja az IoT eszközök, rendszerek és szolgáltatások kiberbiztonságának átláthatóságát, megbízhatóságát és megköveteli az okos épületrendszerek és a biztonsági fenyegetések összetettségének és sokféleségének kezelését. Ehhez a korábbiakban ismertetett keretrendszereket, köztük az ISO/IEC 27001, a SP NIST 800-as sorozatot, a BREEAM-et és a LEED-et vizsgáltam meg a kiberbiztonság és az okos épületekben összefüggésében.

4.1. Kiberbiztonsági referenciamodell bemutatása

Megalkottam egy referenciamodellt annak érdekében, hogy a ZTA hogyan valósítható meg egy okos épületben, a kiberbiztonsági szempontokra összpontosítva. A modell egy hipotetikus modern irodaház, a "TechTower", amely fejlett IoT-rendszerekkel van felszerelve különböző funkciókhoz, többek között a klímavezérléshez, a biztonsághoz és az energiagazdálkodáshoz. Az épület integrált épületirányítási rendszerrel (BMS), különböző funkciókat ellátó IoT-eszközökkel és felhőalapú adatkezelési rendszerrel rendelkezik. A TechTower kiberbiztonsági helyzetének javítása a ZTA bevezetésével, a NIST SP 800-207 iránymutatásokkal való összehangolással és az épület összetett IoT-ökoszisztémája által támasztott egyedi biztonsági kihívások kezelésével.

Végrehajtási stratégia

Személyazonosság-ellenőrzés és hozzáférés-szabályozás

- Privilegizált felhasználó: Minden felhasználónak egyedinek és megkülönböztethetőnek kell lennie, így auditálható módon végezhető a hozzáférés.
- Többfaktoros hitelesítés (MFA): Minden felhasználónak, beleértve az adminisztrátorokat és a karbantartó személyzetet is, a BMS-hez vagy bármely IoT-eszközhöz, rendszerhez való hozzáféréskor kétfaktoros azonosítást kell használnia. Ezt a rendszerek esetén alapértelmezett módon ki kell kényszeríteni.
- Dinamikus hozzáférési irányelvek: A hozzáférési jogok kiosztása szerepkör, hely és idő alapján történik, folyamatos értékelés és kiigazítás mellett.
    - Just in Time (JIT): Kizárólag abban az időintervallumban férjen hozzá a rendszerekhez a felhasználó, amikor szükséges.

    - Just Enough Access (JEA): Kizárólag ahhoz a rendszerhez férjen hozzá a felhasználó, amihez szükséges.
- Hálózati mikroszegmentáció: Az épület hálózata szegmentált zónákra van osztva, amelyek mindegyike saját biztonsági vezérléssel rendelkezik. Például a HVAC-rendszerek, a világításvezérlők és a biztonsági rendszerek egymástól elszigetelt, különálló hálózati szegmensekben működnek. Külön működik az irodai és vendég WiFi hálózat is.
- Folyamatos felügyelet és anomália-detekció: A mesterséges intelligencia által vezérelt biztonsági rendszer folyamatosan figyelik a hálózati forgalmat a szokatlan minták vagy potenciális fenyegetések szempontjából. Ez a rendszer integrálva van az épület incidenskezelési protokolljába. Ide tartoznak még az XDR és SIEM rendszerek, melyek gyűjtik és elemzik a beérkező naplófájlokat.

Kihívások és megoldások

- Integráció a meglévő rendszerekkel
    - Kihívás: A ZTA integrálása a TechTower meglévő BMS és IoT infrastruktúrájába.
    - Megoldás: Fokozatos bevezetési megközelítés, amely a kritikus rendszerekkel, például a HVAC- és biztonsági rendszerekkel kezdődik, majd fokozatosan integrálódik a többi rendszerrel.
- A biztonság és a használhatóság egyensúlyban tartása
    - Kihívás: Annak biztosítása, hogy a fokozott biztonsági intézkedések ne akadályozzák az épület működési hatékonyságát vagy felhasználói élményét.
    - Megoldás: A felhasználók visszajelzéseit beépítették a ZTA-rendszer tervezésébe, biztosítva, hogy a biztonsági intézkedések felhasználóbarátok legyenek, és ne akadályozzák a napi működést.
- A személyzet képzése és tudatosítása
    - Kihívás: Annak biztosítása, hogy a személyzet minden tagja tisztában legyen az új biztonsági protokollokkal és betartsa azokat.
    - Megoldás: Átfogó képzések, valamint rendszeres frissítések és felfrissítő tanfolyamok a legjobb kiberbiztonsági gyakorlatokról.

Eredmények és értékelés

- Fokozott biztonsági helyzet: A bevezetést követően a TechTower a biztonsági incidensek nagyfokú csökkenését tapasztalta. A dinamikus hozzáférés-szabályozás és a folyamatos felügyelet hatékonyan mérsékelte a potenciális fenyegetéseket.
- Működési hatékonyság: A kezdeti aggodalmak ellenére a ZTA bevezetése nem okozott fennakadást az épület működésében. A mikroszegmentációs megközelítés lehetővé tette a különböző rendszerek hatékony kezelését a biztonság veszélyeztetése nélkül.
- Felhasználói visszajelzések: Az épületben tartózkodók és a személyzet visszajelzései túlnyomórészt pozitívak voltak, sokan értékelték a fokozott biztonságérzetet és a ZTA-rendszer zökkenőmentes integrációját a napi rutinokba.

A Zéró bizalom architektúra megvalósítása a TechTowerben azt mutatja, hogy gondos tervezéssel és kivitelezéssel a ZTA növelheti az okos épületek kiberbiztonságát anélkül, hogy az üzemeltetési hatékonyság vagy a felhasználói élmény sérülne. Ez az esettanulmány modellként szolgál más okos épületekben történő hasonló megvalósításokhoz, bemutatva a ZTA hatékonyságát a komplex IoT-ökoszisztémák védelmében.

4.2. Keretrendszerekre vonatkozó fejlesztési javaslatok kiberbiztonsági szempontból

A korábbi fejezetben tett vizsgálatok alapján javaslatot teszek az egyes keretrendszerek módosítására kiberbiztonsági szempontból, így rámutatok azon hiányosságokra, melyek kiegészítése szükséges. Továbbá egy új kiberbiztonsági ellenőrzési listát (check list) hozok létre.

4.2.1. ISO/IEC ISO27001 – A-melléklet kiegészítése

Az ISO/IEC 27001 A-melléklete átfogó biztonsági ellenőrzési célkitűzéseket és ellenőrzéseket tartalmaz. A gyorsan fejlődő IoT összefüggésében azonban szükség van ezen ellenőrzések kiterjesztésére, hogy az eszközei és rendszerei által támasztott egyedi kihívásokat kezelni lehessen. Éppen ezért az alábbiakban kiegészítem az ISO/IEC 27001 A-mellékletét a saját kiberbiztonsági ajánlásaimmal az okos épületekre nézve.

Kiterjesztési javaslatok az A-melléklet pontjaiban:

- A.5 Adatbiztonsági szabályok: Kifejezetten az IoT-eszközökre vonatkozó biztonsági irányelvek kidolgozása és végrehajtása, amelyek olyan egyedi

szempontokkal foglalkoznak, mint az eszköz életciklusa, az adatgyűjtés és az interoperabilitás. A szabályzatoknak ki kell terjedniük a teljes IoT-ökoszisztémára, az érzékelőktől az átjárókig és a felhőszolgáltatásokig.

- A.6. Az adatbiztonság felépülése: Az IoT biztonságirányításhoz kapcsolódó szerepek és felelősségi körök megállapítása. Ez magában foglalja az IoT-biztonság felügyeletére és az eszközgyártók, a szoftverfejlesztők és a hálózati szolgáltatók közötti koordinációra kijelölt csapatokat.
- A.9: A hozzáférés ellenőrzés: Szigorú hozzáférés-ellenőrzési mechanizmusok bevezetése az IoT-eszközök számára, úgy, mint biztonságos hitelesítés és engedélyezés biztosítását az eszközökhöz való hozzáféréshez, különösen az érzékeny adatokat kezelő eszközök esetében.
- A.12: A beszerzés: Az üzemeltetési biztonsági ellenőrzések kiterjesztése az IoT-eszközök kezelésére, mint a biztonságos konfigurációt, a rendszeres frissítéseket és az IoT-eszközök nyomon követését bármilyen rendellenes tevékenységre vonatkozóan.
- A.13 Kommunikációbiztonság: A kommunikációs biztonság megerősítése az IoT-eszközök által továbbított adatok védelme érdekében. Alkalmazzon titkosítási szabványokat a nyugalmi és tranzit adatokra, valamint biztonságos kommunikációs csatornákat, különösen a vezeték nélküli IoT-hálózatokban.
- A.14 Rendszerbeszerzés, -fejlesztés és -karbantartás: A biztonság beépítése az IoT-eszközök és -alkalmazások fejlesztési életciklusába. A biztonságos kódolási gyakorlata, a sérülékenységvizsgálat és a biztonsági funkciók beépítése a tervezési fázisban.
- A.16 Információbiztonsági incidensek kezelése: Kifejezetten az IoT-vel kapcsolatos incidensekkel foglalkozó incidenskezelési tervek kidolgozása. Ez magában foglalja az IoT-eszközöket érintő biztonsági rések gyors észlelési, reagálási és helyreállítási mechanizmusait.
- A.17 Az üzletmenetfolytonosság kezelésének adatbiztonsági szempontjai: Az IoT-eszközök és -rendszerek bevonása az üzletmenet-folytonossági és katasztrófa-helyreállítási tervezésbe. Biztosítani kell, hogy az IoT-eszközök gyorsan helyreállíthatók vagy kicserélhetők legyenek nagyobb fennakadás esetén.

- A.18 Megfelelőség: Megfeleljen az IoT-re vonatkozó jogi és szabályozási követelményeknek. Ez magában foglalja az IoT-eszközök biztonságával és adatvédelmével kapcsolatos szabványok és előírások betartását.

Részkövetkeztetés

Az ISO/IEC 27001 A-mellékletének kiterjesztése az IoT biztonságára kulcsfontosságú a jelenlegi digitális környezetben, ahol az IoT-eszközök egyre inkább beépülnek a kritikus üzleti folyamatokba és infrastruktúrába. Ez a kibővített keretrendszer holisztikusabb megközelítést biztosít az információbiztonsághoz, és biztosítja, hogy az IoT-eszközökkel és -rendszerekkel kapcsolatos egyedi kockázatok megfelelő módon kezelhetők legyenek.

4.2.2. A NIST SP 800-as sorozat továbbfejlesztése

- A IoT-re szabott ellenőrzési keretrendszer: A NIST SP 800-as sorozaton belül egy speciális IoT biztonsági ellenőrzési és értékelési keretrendszer kidolgozása, mely tartalmaz egy kockázatértékelő mátrixot az IoT eszközökre és rendszerekre vonatkozóan.
- Folyamatos nyomon követési és értékelési iránymutatások: Irányelvek bevezetése az IoT-környezetek folyamatos nyomon követésére és valós idejű biztonsági értékelésére. Ez magában foglalná a dinamikus kockázatértékelés és a tárgyak internetére jellemző fenyegetések észlelésének módszereit.
- Iránymutatások az IoT integráció biztonságához: Részletes útmutatás nyújtása a meglévő IT- és OT-rendszerekkel való IoT-integrációk biztonságának ellenőrzésére vonatkozóan. Ez segítene az ilyen integrációkból eredő kockázatok azonosításában és mérséklésében.

Részkövetkeztetés

A NIST SP 800-as sorozatának kiterjesztett hiányelemzése rámutat arra, hogy szükség van egy IoT-specifikusabb biztonsági ellenőrzési módszertanra. Egy ilyen módszertannak foglalkoznia kell az IoT-eszközök sokféleségéből adódó egyedi kihívásokkal, a valós idejű biztonsági értékelés szükségességével és a meglévő architektúrákba történő IoT-integráció összetettségével. A NIST SP 800-as sorozat ezen szempontok figyelembevételével történő továbbfejlesztése megerősítené a tárgyak internetének kiberbiztonsági helyzetét.

4.2.3. A GDPR, a NIS2 és a kiberrezilienciáról szóló jogszabály javasolt fejlesztései

- IoT-ellenőrzési protokollok kidolgozása a GDPR-ban: A GDPR keretében speciális IoT biztonsági ellenőrzési protokollok bevezetése. Ez biztosítaná, hogy a személyes adatokat kezelő IoT-eszközöket következetesen és alaposan értékeljék a megfelelőség és a biztonság szempontjából.
- IoT biztonsági ellenőrzési keretrendszer a NIS2-ben: Részletes IoT biztonsági ellenőrzési keretrendszer kidolgozása a NIS2 keretében. Ennek a keretnek figyelembe kell vennie a tárgyak internete rendszerek változatos és összetett jellegét, különösen a kritikus ágazatokban.
- Az IoT-ellenőrzési módszertanok beépítése a kiberrezilienciáról szóló jogszabályban: Konkrét IoT-biztonsági ellenőrzési módszertanok beépítése. Ez megerősítené a IoT eszközök ellenálló képességét a felmerülő kiberfenyegetésekkel szemben.

Részkövetkeztetés

A kibővített hiányelemzés rámutat arra, hogy a GDPR, a NIS2 és a kiberrezilienciáról szóló jogszabály keretében szükség van a dolgok internetének biztonságának egyedi ellenőrzési módszereire. E hiányosságok kiküszöbölésére alkottam meg a saját keretrendszeremet, ami fokozná az IoT eszközeinek biztonságát és megfelelőségét az okos épületekben, biztosítva azok ellenálló képességét a fejlődő kiberfenyegetésekkel és adatvédelmi aggályokkal szemben.

4.3. Okos épületek kiberbiztonsági ellenőrzőlistája

Kutatásom során feltártam azon hiányosságokat, melyekkel az egyes keretrendszerek, szabványok rendelkeznek az okos épületek kiberbiztonságra vonatkozóan. Ennek következtében megalkottam egy ellenőrzőlistát, amely segítségével egy okos épület kiberbiztonsági szempontból vizsgálható, segítve az előkészítést és önellenőrzést. Így elkerülhetőek a hiányosságok és segítségével már a tervezési fázisban fel lehet készülni egy okos épület esetén az IoT-rendszereket érintő kockázatokra. Az ellenőrzőlistát területekre, azon belül témakörökre bontottam és olyan feladatokat írtam le, amelyek segíthetik megérteni és kialakítani a kulcsfontosságú kontrollokat egy ilyen rendszernél.

Az ellenőrzőlistában 14 területet és 16 témakört azonosítottam, melyekhez olyan feladatokat rendeltem, mint például *„Értékelje a harmadik féltől származó IoT-összetevők és -szolgáltatások biztonsági intézkedéseit.”* vagy *„Tekintse át az IoT-re*

vonatkozó adatvédelmi intézkedéseket, az adattitkosításra, az anonimizálásra és a biztonságos adattárolási gyakorlatokra összpontosítva."

Az **Okos épületek kiberbiztonsági ellenőrzőlistája** a 2. függelékben található.

Összefoglalva a fejezetet, javaslatot tettem az egyes kiberbiztonsági keret, - és tanúsító rendszerek kiegészítésére, melyekkel az okos épületek kiberbiztonsága növelhető. Kidolgoztam a kiberbiztonsági ellenőrzőlista egy alkalmazható változatát az okos épületekre. Összeállítottam egy olyan referenciamodell, amely az okos épületeket ért kibertámadásokat csökkentheti. Végezetül pedig hipotéziseimet alátámasztottam a szakértői mélyinterjúk elemzésével is.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Kutatásom célja a meglévő kiberbiztonsági keretrendszerek átfogó elemzése, egy új ellenőrzőlista létrehozás és egy referenciamodell kidolgozása volt annak érdekében, hogy az okos épületek tervezésekor vagy üzemeltetésekor kiemelt szerepet kapjon a kiberbiztonság. Ennek érdekében három hipotézist fogalmaztam meg.

Új tudományos eredmények

Értekezésemben a kiberbiztonság és az okos épületek kapcsolatát vizsgáltam. A primer kutatásom során összehasonlító elemzést végeztem néhány kiemelt kiberbiztonsági keretrendszeren és szabványon, ahol megvizsgáltam, hogy az okos épületeknél hogyan alkalmazható és milyen hiányosságokkal rendelkezik. Ezeket alátámasztottam szakmai interjúkkal, melyeket olyan hazai szakemberekkel készítettem, akik a kiberbiztonság és az okos épületek területén több éves tapasztalattal rendelkeznek. Tekintettel arra, hogy én is gyakorló szakember vagyok, így résztvevői megfigyelés keretében beépítettem a saját tapasztalataim, melyeket az elmúlt közel 15 év során szereztem. Elkészítettem egy kiberbiztonsági ellenőrzőlistát, melyet az okos épületek tervezésekor és üzemeltetésekor lehet használni a kiberbiztonság növelés érdekében. A szekunder kutatáshoz forrásokat dolgoztam fel dokumentumelemzés formájában. Kutatási eredményeimet értekezésem logikai felépítése mentén ismertettem, így voltak olyan kutatási eredményeim melyek nem az empirikus, hanem a teoretikus részeknél szerepeltek. Ezekben az esetekben a megfogalmazással, illetve a táblázatok forrásának feltüntetésével egyértelműen utaltam erre.

Három hipotézist vizsgáltam értekezésem során, melyekkel kapcsolatban az alábbi megállapításokat teszem:

T1: Bizonyítottam, hogy összeállítható egy kiberbiztonsági ellenőrzőlista, ami segíti az a kiberbiztonsági szempontoknak való megfelelést az okos épületekben. Erre kidolgoztam az ellenőrzőlista egy alkalmazható változatát. [33] [54] [82]

T2: Bizonyítottam, hogy összeállítható egy olyan referenciamodell, amely az okos épületeket ért kibertámadásokat csökkentheti. [17] [30] [54]

T3: Összehasonlítóelemzéssel igazoltam, hogy a meglévő kiberbiztonsági keretrendszerekből és szabványokból hiányzik az okos épületekre vonatkozó kiberbiztonsági ajánlás. Ennek érdekében javaslatokat tettem azok bővítésére. [31]

Új tudományos eredmények alkalmazhatósága

Értekezésem célja az volt, hogy azon kiberbiztonsági szakemberek és szervezetek számára segítsek, akik okos épületek IoT rendszereit tervezik és/vagy üzemeltetik. Olyan problémákra adtam javaslatot, melyek súlyos hiányosságok a különféle kiberbiztonsági keretrendszerekben és szabványokban az okos épületek kiberbiztonságát tekintve. Értekezésem ajánlom:

- Kiberbiztonsági tervezők számára, akik IoT rendszereket terveznek okos épületekbe.
- Kiberbiztonsági üzemeltetők számára, akik a meglévő rendszereket átveszik üzemeltetésre.
- IoT szakemberek számára, akik növelni szeretnék a kiberbiztonságot az IoT eszközeik, rendszereik területén.
- Vállalatok számára, akik okos épületet terveznek, vagy üzemeltetnek.
- Eredményeimet ajánlom széles körben felhasználni a kiberbiztonság területén műszaki ajánlás szintjén.

Új kutatási irányra tett javaslatok

A kutatást az alábbi irányokban folytatnám a jövőben, tekintettel arra, hogy az okos épületek és IoT eszközök és rendszerek folyamatosan terjednek el és így válnak a kibertámadások célpontjaivá.

- MI-vezérelt prediktív kiberbiztonság intelligens épületek számára

  Az intelligens épületek potenciális kiberbiztonsági fenyegetéseinek előrejelzésére alkalmas MI-algoritmusok kifejlesztésének és megvalósításának vizsgálata. Ebben a kutatásban olyan gépi tanulási modelleket vizsgálhat, amelyek a múltbeli adatokat elemzik a minták azonosítása és a jövőbeli sebezhetőségek vagy támadások előrejelzése érdekében.
- Blokklánc az intelligens épületek fokozott IoT-biztonságáért

  A blokklánc-technológia alkalmazásának vizsgálata az intelligens épületekben található IoT-eszközök biztonságának és integritásának javítása érdekében. Ez a kutatás olyan decentralizált biztonsági protokollokra összpontosíthat, amelyek a blokkláncot használják az adatintegritás és a biztonságos eszköz-eszköz kommunikáció biztosítására.

HIVATKOZOTT SZAKIRODALOM

[1] A. Jay, „Number of Internet of Things (IoT) Connected Devices Worldwide 2024: Breakdowns, Growth & Predictions”, Financesonline.com. Elérés: 2024. február 4. [Online]. Elérhető: https://financesonline.com/number-of-internet-of-things-connected-devices/

[2] F. Mattern és C. Floerkemeier, „From the Internet of Computers to the Internet of Things”, in *From Active Data Management to Event-Based Systems and More: Papers in Honor of Alejandro Buchmann on the Occasion of His 60th Birthday*, K. Sachs, I. Petrov, és P. Guerrero, Szerk., Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, o. 242–259. doi: 10.1007/978-3-642-17226-7_15.

[3] K. Ashton, „That “Internet of Things” Thing: In the Real World Things Matter More than Ideas”, *RFID J.*, köt. 22, sz. 7, o. 97–114, 2009.

[4] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, és E. Cayirci, „Wireless sensor networks: a survey”, *Comput. Netw.*, köt. 38, sz. 4, o. 393–422, 2002, doi: 10.1016/S1389-1286(01)00302-4.

[5] R. Want, „An introduction to RFID technology”, *IEEE Pervasive Comput.*, köt. 5, sz. 1, o. 25–33, 2006, doi: 10.1109/MPRV.2006.2.

[6] T. Givargis és F. Vahid, „Platune: A tuning framework for system-on-a-chip platforms”, *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, köt. 21, sz. 11, o. 1317–1327, 2002, doi: 10.1109/TCAD.2002.804107.

[7] C. Perera, A. Zaslavsky, P. Christen, és D. Georgakopoulos, „Sensing as a service model for smart cities supported by internet of things”, *Trans. Emerg. Telecommun. Technol.*, köt. 25, sz. 1, o. 81–93, 2014, doi: 10.1002/ett.2704.

[8] A. Botta, W. De Donato, V. Persico, és A. Pescapé, „Integration of cloud computing and internet of things: a survey”, *Future Gener. Comput. Syst.*, köt. 56, o. 684–700, 2016, doi: 10.1016/j.future.2015.09.021.

[9] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, és M. Ayyash, „Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications”, *IEEE Commun. Surv. Tutor.*, köt. 17, sz. 4, o. 2347–2376, 2015, doi: 10.1109/COMST.2015.2444095.

[10] J. Tisóczki, „A mesterséges intelligencia alkalmazása az egészségügyi ellátási folyamatokban”, *Biztonságtudományi Szle.*, köt. 4, sz. 2. Ksz., o. 137–153, 2022.

[11] M. A. Abid *és mtsai.*, „Evolution towards Smart and Software-Defined Internet of Things”, *AI*, köt. 3, sz. 1, o. 100–123, 2022, doi: 10.3390/ai3010007.

[12] K. Lalitha, D. R. Kumar, C. Poongodi, és J. Arumugam, „Healthcare Internet of Things–The Role of Communication Tools and Technologies”, in *Blockchain, Internet of Things, and Artificial Intelligence*, Chapman and Hall/CRC, 2021, o. 331–348.

[13] R. S. Bisht, S. Jain, és N. Tewari, „Study of wearable IoT devices in 2021: Analysis & future prospects”, in *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)*, IEEE, 2021, o. 577–581. doi: 10.1109/ICIEM51511.2021.9445334.

[14] M. Wu és J. Luo, „Wearable technology applications in healthcare: a literature review”, *Online J Nurs Inf.*, köt. 23, sz. 3, 2019, [Online]. Elérhető: https://www.proquest.com/openview/6c96964dfb83ca06895f330233831a50/1?pq-origsite=gscholar&cbl=2034896

[15] M. S. Aliero, K. N. Qureshi, M. F. Pasha, és G. Jeon, „Smart Home Energy Management Systems in Internet of Things networks for green cities demands and

services”, *Environ. Technol. Innov.*, köt. 22, o. 101443, 2021, doi: 10.1016/j.eti.2021.101443.
[16] S. Ahmetoglu, Z. Che Cob, és N. Ali, „Internet of Things Adoption in the Manufacturing Sector: A Conceptual Model from a Multi-Theoretical Perspective”, *Appl. Sci.*, köt. 13, sz. 6, Art. sz. 6, jan. 2023, doi: 10.3390/app13063856.
[17] B. Sándor és Z. Rajnai, „Okos épületek és az IoT: A globális gyakorlatok átfogó áttekintése”, *Biztonságtudományi Szle.*, köt. 5, sz. 2, o. 33–46, 2023.
[18] S. Selvaraj és S. Sundaravaradhan, „Challenges and opportunities in IoT healthcare systems: a systematic review”, *SN Appl. Sci.*, köt. 2, sz. 1, o. 139, dec. 2019, doi: 10.1007/s42452-019-1925-y.
[19] S. B. Junaid *és mtsai.*, „Recent Advances in Artificial Intelligence and Wearable Sensors in Healthcare Delivery”, *Appl. Sci.*, köt. 12, sz. 20, o. 10271, 2022, doi: 10.3390/app122010271.
[20] M. R. M. Kassim, „IoT Applications in Smart Agriculture: Issues and Challenges”, in *2020 IEEE conference on open systems (ICOS)*, IEEE, 2020, o. 19–24. doi: 10.1109/ICOS50156.2020.9293672.
[21] W.-S. Kim, W.-S. Lee, és Y.-J. Kim, „A review of the applications of the internet of things (IoT) for agricultural automation”, *J. Biosyst. Eng.*, köt. 45, o. 385–400, 2020, doi: 10.1007/s42853-020-00078-3.
[22] „State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally”, IoT Analytics. Elérés: 2024. február 4. [Online]. Elérhető: https://iot-analytics.com/number-connected-iot-devices/
[23] „Matter Specification, Version 1.0”. Connectivity Standards Alliance, Inc., 2022. szeptember 28. Elérés: 2023. december 19. [Online]. Elérhető: https://csa-iot.org/wp-content/uploads/2022/11/22-27349-001_Matter-1.0-Core-Specification.pdf
[24] Connectivity Standards Alliance, „Matter 1.2 Arrives with Nine New Device Types & Improvements Across the Board”. Elérés: 2024. január 8. [Online]. Elérhető: https://csa-iot.org/newsroom/matter-1-2-arrives-with-nine-new-device-types-improvements-across-the-board/
[25] „Typical Thread Network Topologies - Smart Homes with Matter & Commercial Buildings > Thread Group”. Elérés: 2024. február 4. [Online]. Elérhető: https://www.threadgroup.org/news-events/blog/ID/291/Typical-Thread-Network-Topologies--Smart-Homes-with-Matter-Commercial-Buildings
[26] D. Coppens, A. Shahid, S. Lemey, B. Van Herbruggen, C. Marshall, és E. De Poorter, „An overview of UWB standards and organizations (IEEE 802.15. 4, FiRa, Apple): Interoperability aspects and future research directions”, *IEEE Access*, köt. 10, o. 70219–70241, 2022, doi: 10.1109/ACCESS.2022.3187410.
[27] „Thread 1.2 for Smart Buildings White Paper”. Thread Group, Inc., 2022. Elérés: 2023. december 19. [Online]. Elérhető: https://portal.threadgroup.org/DesktopModules/Inventures_Document/FileDownload.aspx?ContentID=3065
[28] P. Domingues, P. Carreira, R. Vieira, és W. Kastner, „Building automation systems: Concepts and technology review”, *Comput. Stand. Interfaces*, köt. 45, o. 1–12, 2016, doi: 10.1016/j.csi.2015.11.005.
[29] F. Mofidi és H. Akbari, „Intelligent buildings: An overview”, *Energy Build.*, köt. 223, o. 110192, 2020, doi: 10.1016/j.enbuild.2020.110192.
[30] B. Sándor és Z. Rajnai, „Cyber Security Analysis of Smart Buildings from a Cyber Security Architecture Point of View”, *Interdiscip. Descr. Complex Syst. INDECS*, köt. 21, sz. 2, o. 141–147, 2023, doi: 10.7906/indecs.21.2.2.

[31] B. Sandor és Z. Rajnai, „Smart Building IoT Cybersecurity: A Review of Threats and Mitigation Technique”, előadás 2023 IEEE 21st International Symposium on Intelligent Systems and Informatics (SISY), IEEE, 2023, o. 321–326.
[32] M. M. Froufe, C. K. Chinelli, A. L. A. Guedes, A. N. Haddad, A. W. Hammad, és C. A. P. Soares, „Smart buildings: Systems and drivers”, *Buildings*, köt. 10, sz. 9, o. 153, 2020, doi: 10.3390/buildings10090153.
[33] B. Sándor és Z. Rajnai, „Az IoT-eszközök és a felhőkörnyezetek interoperabilitásának értékelése intelligens épületrendszerekben”, *Biztonságtudományi Szle.*, köt. 5, sz. 3, o. 47–61, 2023.
[34] J. Aftab, B. Ron, és R. Michael, „The Edge Amsterdam – showcasing an exemplary IoT building”. University of Cambridge, 2018. augusztus 20. Elérés: 2024. január 8. [Online]. Elérhető: https://www.cdbb.cam.ac.uk/news/2018CaseTheEdge
[35] K. Khurshid, A. Danish, M. U. Salim, M. Bayram, T. Ozbakkaloglu, és M. A. Mosaberpanah, „An in-depth survey demystifying the Internet of Things (IoT) in the construction industry: Unfolding new dimensions”, *Sustainability*, köt. 15, sz. 2, o. 1275, 2023, doi: 10.3390/su15021275.
[36] Construction Week, „Burj Khalifa has world’s third-fastest elevator”. Elérés: 2023. január 10. [Online]. Elérhető: https://www.constructionweekonline.com/projects-tenders/article-20616-burj-khalifa-has-worlds-third-fastest-elevator
[37] B. Deborah, „Apple Park”. Elérés: 2024. január 8. [Online]. Elérhető: https://arquitecturaviva.com/works/apple-park-1
[38] Green Building Magazine, „The Crystal - A Landmark Global Urban Sustainability Centre”. Elérés: 2024. január 8. [Online]. Elérhető: https://gbplusamag.com/the-crystal/
[39] S. K. Baduge *és mtsai.*, „Artificial intelligence and smart vision for building and construction 4.0: Machine and deep learning methods and applications”, *Autom. Constr.*, köt. 141, o. 104440, szept. 2022, doi: 10.1016/j.autcon.2022.104440.
[40] B. Pardamean, H. H. Muljo, T. W. Cenggoro, B. J. Chandra, és R. Rahutomo, „Using transfer learning for smart building management system”, *J. Big Data*, köt. 6, sz. 1, o. 110, dec. 2019, doi: 10.1186/s40537-019-0272-6.
[41] H. Farzaneh, L. Malehmirchegini, A. Bejan, T. Afolabi, A. Mulumba, és P. P. Daka, „Artificial intelligence evolution in smart buildings for energy efficiency”, *Appl. Sci.*, köt. 11, sz. 2, o. 763, 2021, doi: 10.3390/app11020763.
[42] T. A. Dovramadjiev, R. Dimova, D. Pavlova, és R. V. Filchev, „Applications of artificial intelligence in people & lifestyle based on education experience”, *Biztonságtudományi Szle.*, köt. 4, sz. 1. Ksz., o. 35–48, 2022.
[43] M. Klees és S. Evirgen, „Building a smart database for predictive maintenance in already implemented manufacturing systems”, *Int. Conf. Ind. Sci. Comput. Sci. Innov.*, köt. 204, o. 14–21, jan. 2022, doi: 10.1016/j.procs.2022.08.002.
[44] R. Panchalingam és K. C. Chan, „A state-of-the-art review on artificial intelligence for Smart Buildings”, *Intell. Build. Int.*, köt. 13, sz. 4, o. 203–226, okt. 2021, doi: 10.1080/17508975.2019.1613219.
[45] D. Sembroiz, D. Careglio, S. Ricciardi, és U. Fiore, „Planning and operational energy optimization solutions for smart buildings”, *Inf. Sci.*, köt. 476, o. 439–452, febr. 2019, doi: 10.1016/j.ins.2018.06.003.
[46] M. Tavakoli, F. Shokridehaki, M. Funsho Akorede, M. Marzband, I. Vechiu, és E. Pouresmaeil, „CVaR-based energy management scheme for optimal resilience and operational cost in commercial building microgrids”, *Int. J. Electr. Power Energy Syst.*, köt. 100, o. 1–9, szept. 2018, doi: 10.1016/j.ijepes.2018.02.022.

[47] A. Pejić és P. S. Molcer, „Predictive machine learning approach for complex problem solving process data mining”, *Acta Polytech. Hung.*, köt. 18, sz. 1, o. 45–63, 2021.
[48] Y. Xu, P. Ahokangas, M. Turunen, M. Mäntymäki, és J. Heikkilä, „Platform-Based Business Models: Insights from an Emerging AI-Enabled Smart Building Ecosystem”, *Electronics*, köt. 8, sz. 10, Art. sz. 10, okt. 2019, doi: 10.3390/electronics8101150.
[49] L. P. Kaelbling, M. L. Littman, és A. W. Moore, „Reinforcement learning: A survey”, *J. Artif. Intell. Res.*, köt. 4, o. 237–285, 1996, doi: 10.1613/jair.301.
[50] J. Reynolds, Y. Rezgui, A. Kwan, és S. Piriou, „A zone-level, building energy optimisation combining an artificial neural network, a genetic algorithm, and model predictive control”, *Energy*, köt. 151, o. 729–739, máj. 2018, doi: 10.1016/j.energy.2018.03.113.
[51] M. K. M. Shapi, N. A. Ramli, és L. J. Awalin, „Energy consumption prediction by using machine learning for smart building: Case study in Malaysia”, *Dev. Built Environ.*, köt. 5, o. 100037, márc. 2021, doi: 10.1016/j.dibe.2020.100037.
[52] Z. Liu, X. Zhang, Y. Sun, és Y. Zhou, „Advanced controls on energy reliability, flexibility and occupant-centric control for smart and energy-efficient buildings”, *Energy Build.*, köt. 297, o. 113436, okt. 2023, doi: 10.1016/j.enbuild.2023.113436.
[53] B. Qolomany *és mtsai.*, „Leveraging Machine Learning and Big Data for Smart Buildings: A Comprehensive Survey”, *IEEE Access*, köt. 7, o. 90316–90356, 2019, doi: 10.1109/ACCESS.2019.2926642.
[54] D. J. Fehér és B. Sándor, „Effects of the WPA2 KRACK Attack in Real Environment”, előadás 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), IEEE, 2018, o. 000239–000242.
[55] martinekuan, „Azure Cosmos DB in IoT workloads - Azure Solution Ideas”. Elérés: 2024. február 4. [Online]. Elérhető: https://learn.microsoft.com/en-us/azure/architecture/solution-ideas/articles/iot-using-cosmos-db
[56] Forescout Research Labs, „The Enterprise of Things Security Report”, Forescout Research Labs, Version 01_21, 2021. Elérés: 2024. január 9. [Online]. Elérhető: https://www.forescout.com/resources/the-annual-connected-enterprise-report/
[57] A. G. Masid, J. B. Higuera, J.-R. B. Higuera, és J. A. S. Montalvo, „Application of the SAMA methodology to Ryuk malware”, *J. Comput. Virol. Hacking Tech.*, köt. 19, sz. 2, o. 165–198, jún. 2023, doi: 10.1007/s11416-022-00434-1.
[58] Forescout Vedere Labs, „The 5 Riskiest Connected Devices in 2023: IT, IoT, OT, IoMT”. Elérés: 2023. december 9. [Online]. Elérhető: https://www.forescout.com/blog/riskiest-connected-devices-it-iot-ot-iomt/
[59] Forescout Vedere Labs, „R4IoT: Next-Generation Ransomware”, Version 01_03, jún. 2022. o. 13-14. Elérés: 2023. január 5. [Online]. Elérhető: https://www.forescout.com/resources/r4iot-next-generation-ransomware-report
[60] CyberMDX és Vedere Labs, „Access:7 - How Supply Chain Vulnerabilities Can Allow Unwelcomed Access to Your Medical and IoT Devices”, Version B, 2022. Elérés: 2024. január 9. [Online]. Elérhető: https://www.forescout.com/resources/access-7-supply-chain-vulnerabilities-can-allow-unwelcomed-access-to-your-medical-and-iot-devices/
[61] dos S. Daniel, D. Stanislav, W. Jos, és A. Amine, „Amnesia:33 - How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices”, Forescout Research Labs, Version 12_20, 2020. o. 4. Elérés: 2023. december 31. [Online]. Elérhető: https://www.forescout.com/resources/amnesia33-identify-and-mitigate-the-risk-from-vulnerabilities-lurking-in-millions-of-iot-ot-and-it-devices/

[62] S. Rose, O. Borchert, S. Mitchell, és S. Connelly, „Zero Trust Architecture”, National Institute of Standards and Technology, aug. 2020. doi: 10.6028/NIST.SP.800-207. o. 5.
[63] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, és R. Doss, „Zero Trust Architecture (ZTA): A Comprehensive Survey”, *IEEE Access*, köt. 10, o. 57143–57179, 2022, doi: 10.1109/ACCESS.2022.3174679.
[64] S. H. Li, „An overview of sustainable assessment tools of BREEAM, LEEDv4 and GB”, 7th International Conference on Energy and Environment of Residential …, nov. 2016. doi: 10.4225/50/581076f34a16a.
[65] A. Ferreira, M. D. Pinheiro, J. de Brito, és R. Mateus, „A critical analysis of LEED, BREEAM and DGNB as sustainability assessment methods for retail buildings”, *J. Build. Eng.*, köt. 66, o. 105825, máj. 2023, doi: 10.1016/j.jobe.2023.105825.
[66] P. Wu, Y. Song, X. Hu, és X. Wang, „A Preliminary Investigation of the Transition from Green Building to Green Community: Insights from LEED ND”, *Sustainability*, köt. 10, sz. 6, Art. sz. 6, jún. 2018, doi: 10.3390/su10061802.
[67] Dombora S. és Horváth G. K., „Információbiztonság integrált megvalósítása MSZ ISO/IEC 27001:2014, és IBTV. (NIST SP 800-53 rev 4) alapon”, előadás Kommunikáció 2015, Budapest: NKE Szolgáltató Kft., nov. 2015, o. 43–55. Elérés: 2024. január 10. [Online]. Elérhető: https://www.puskashirbaje.hu/pdf/Kommunikacio_2015-NSZTK.pdf
[68] ISO/IEC CD 30141:20160910 - "Information technology – Internet of Things Reference Architecture (IoT RA)". 2016, o. 44. Elérés: 2024.01.10. [Online] Elérhető: https://www.w3.org/WoT/IG/wiki/images/9/9a/10N0536_CD_text_of_ISO_IEC_30141.pdf
[69] J. T. F. T. Initiative, „Guide for Conducting Risk Assessments”, National Institute of Standards and Technology, NIST Special Publication (SP) 800-30 Rev. 1, szept. 2012. doi: 10.6028/NIST.SP.800-30r1.
[70] Joint Task Force Interagency Working Group, „Security and Privacy Controls for Information Systems and Organizations”, National Institute of Standards and Technology, szept. 2020. doi: 10.6028/NIST.SP.800-53r5.
[71] K. Kent és M. Souppaya, „Guide to Computer Security Log Management”, National Institute of Standards and Technology, NIST Special Publication (SP) 800-92, szept. 2006. doi: 10.6028/NIST.SP.800-92.
[72] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, és R. McQuaid, „Developing Cyber-Resilient Systems: A Systems Security Engineering Approach”, National Institute of Standards and Technology, NIST Special Publication (SP) 800-160 Vol. 2 Rev. 1, dec. 2021. doi: 10.6028/NIST.SP.800-160v2r1.
[73] M. Ogata, J. Franklin, J. Voas, V. Sritapan, és S. Quirolgico, „Vetting the Security of Mobile Applications”, National Institute of Standards and Technology, NIST Special Publication (SP) 800-163 Rev. 1, ápr. 2019. doi: 10.6028/NIST.SP.800-163r1.
[74] M. Fagan *és mtsai.*, „IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements”, National Institute of Standards and Technology, NIST Special Publication (SP) 800-213, nov. 2021. doi: 10.6028/NIST.SP.800-213.
[75] M. Fagan, K. Megas, K. Scarfone, és M. Smith, „Foundational Cybersecurity Activities for IoT Device Manufacturers”, National Institute of Standards and

Technology, NIST Internal or Interagency Report (NISTIR) 8259, máj. 2020. doi: 10.6028/NIST.IR.8259.
[76] European Union Agency for Cybersecurity, *Baseline security recommendations for IoT in the context of critical information infrastructures*. European Network and Information Security Agency, 2017. doi: 10.2824/03228.
[77] Európai Bizottság, *AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről és az (EU) 2019/1020 rendelet módosításáról (CRA)*. o. 93. Elérés: 2024. január 22. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52022PC0454
[78] Európai Unió, *AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (GDPR)*. 2016, o. 88. Elérés: 2023. október 10. [Online]. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32016R0679
[79] Európai Unió, *AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2555 IRÁNYELVE (NIS 2 irányelv)*. 2022, o. 73. Elérés: 2024. január 10. [Online]. Elérhető: https://eur-lex.europa.eu/eli/dir/2022/2555
[80] D. J. Fehér és B. Sándor, „Log File Authentication and Storage on Blockchain Network”, in *2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY)*, szept. 2018, o. 000243–000248. doi: 10.1109/SISY.2018.8524848.
[81] D. J. Fehér és B. Sándor, „Examining the Relationship between the Bitcoin and Cybercrime”, in *2019 IEEE 13th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, 2019, o. 121–126. doi: 10.1109/SACI46893.2019.9111568.
[82] B. Sándor, „ Vulnerability Analysis of a Smart Heating System”, Műszaki Tudományos Közlemények, 2019. vol. 9., 211-214., 4 p., doi: 10.33895/mtk-2018.09.48.

RÖVIDÍTÉSJEGYZÉK

Rövidítés	Angol	Magyar
AEAD	Authenticated Encryption with Associated Data	Hitelesített titkosítás társított adatokkal
AI	Artificial intelligence	Mesterséges intelligencia (MI)
BAS	Building Automation Systems	Épületautomatizálási rendszerek
CAGR	Compound Annual Growth Rate	Összetett éves növekedési ráta
CD	Continuous Delivery / Continuous Deployment	Folyamatos szállítás / telepítés
CI	Continuous Integration	Folyamatos integráció
CoAP	Constrained Application Protocol	Korlátozott alkalmazás protokoll
DevOps	Development and Operation	Fejlesztés és üzemeltetés
DevSecOps	Development, Security and Operation	Fejlesztés, biztonság és üzemeltetés
DTLS	Datagram Transport Layer Security	Datagram szállítási réteg biztonsága
FTP	File Transfer Protocol	Fájlátviteli protokoll
HVAC	Heating, ventilation, and air conditioning	Fűtés, szellőzés és légkondicionálás
IaaS	Infrastructure as a Service	Infrastruktúra, mint szolgáltatás
IDS	Intrusion Detection System	Behatolásfelderítő rendszer
IEC	International Electrotechnical Commission	Nemzetközi Elektrotechnikai Bizottság
IIoT	Industrial Internet of Things	Dolgok ipari internete
IoT	Internet of Things	Dolgok internete
IPS	Intrusion Prevention System	Behatolásmegelőző rendszer
ISMS	Information Security Management System	Információbiztonsági irányítási rendszer
ISO	International Organization for Standardization	Nemzetközi Szabványügyi Szervezet
JEA	Just Enough Access	Éppen elegendő hozzáférés

JIT	Just in Time	Éppen-időben
MFA	Multi-Factor Authentication	Többfaktoros hitelesítés
ML	Machine Learning	Gépi tanulás
MQTT	Message Queuing Telemetry Transport	Üzenetek sorbaállításán alapuló telemetriai adattovábbítás
NAC	Network Access Control	Hálózati hozzáférés-szabályozás
OT	Operational Technology	Operatív technológiák
OTA	Over-the-Air	Levegőn keresztül
PaaS	Platform as a Service	Platform, mint szolgáltatás
PDP	Policy Decision Point	Szabály alapú döntési pont
PEP	Policy Enforcement Point	Szabályzat végrehajtási pont
RDP	Remote Desktop Protocol	Távoli asztali protokoll
RFID	Radio Frequency Identification	Rádiófrekvenciás azonosítás
RL	Reinforcement learning	Erősítő tanulás
ROI	Return on Investment	Befektetés megtérülése
SMB	Server Message Block	Kiszolgálói üzenetblokk
SSH	Secure Shell	Fájl átviteli protokoll
WSN	Wireless sensor network	Vezeték nélküli érzékelőhálózat

TÁBLÁZATJEGYZÉK

ÁBRAJEGYZÉK

FÜGGELÉK

1. függelék – Szakmai interjú kérdések

1. Hogyan nehezíti az IoT-technológia integrálása a hagyományos kiberbiztonsági gyakorlatokat az okos épületek esetében?
2. A kibertámadások aspektusából nézve mennyire jelentős a mesterséges intelligencia és a gépi tanulás az okos épületek kiberbiztonságának fokozásában?
3. Az okos épületrendszerek összetettségére és sokfélesége szempontjából, milyen szempontokat javasol a kiberbiztonság fejlesztése érdekében?
4. Milyen kulcsfontosságú tényezőket kell figyelembe venni az IoT-alapú kiberbiztonsági megoldások kapcsán az átláthatóság és a megbízhatóság biztosítása érdekében?
5. Milyen kontrollokra és megfelelésékre van szüksége az IoT-eszközök gyártóinak ahhoz, hogy termékeik biztonságosak legyenek, és ne veszélyeztessék az okos épületek kiberbiztonságát?
6. Hogyan látja a kiberbiztonsági fenyegetések alakulását az egyre inkább IoT-alapú világban, és hogyan alkalmazkodhat ezekhez a változásokhoz kiberbiztonsági szempontból?
7. Milyen szerepet játszhat a blokklánc technológia az IoT kiberbiztonságában az okos épületeken belül?
8. Mi a véleménye az okos épületekben található IoT-eszközökkel kapcsolatos főbb kiberbiztonsági kockázatokról, és arról, hogy egy kiberbiztonsági ellenőrzőlista hogyan képes csökkenteni ezeket a kockázatokat?
9. Megosztaná tapasztalatát a felhasználóiélmény és a biztonság közötti egyensúlyról az IoT-eszközök okos épületekben történő használatával kapcsolatban?
10. Hogyan értékelné az okos épületek kiberbiztonsági intézkedéseinek jelenlegi helyzetét az IoT-technológia által jelentett fenyegetésekkel szemben?
11. Hogyan képzeli el az okos épületek kiberbiztonságára vonatkozó szabványosított megoldások bevezetésének akadályainak leküzdését?
12. Kifejtené, hogy a jelenlegi biztonsági intézkedések mire elegendőek az okos épületek védelmére a kifinomult kibertámadásokkal szemben, és hogy egy ellenőrzőlista hogyan csökkentené ezeket a kockázatokat és problémát?

2. függelék – Okos épületek kiberbiztonsági ellenőrzőlistája

#	Terület	Témakör	Feladat
1	Irányítás és szabályzat-kezelés	IoT biztonsági politika felülvizsgálata	- Ellenőrizze, hogy az IoT biztonsági szabályzat tartalmazza-e az eszközök biztonságára, a hálózati protokollokra és az adatkezelésre vonatkozó műszaki szabványokat. - Ellenőrizze az IoT-eszközök beszerzésére és telepítésére vonatkozó konkrét irányelveket.
2	Humánerőforrás-biztonság	A munkavállalók IoT-biztonsággal kapcsolatos képzése	- Értékelje az IoT-biztonsággal kapcsolatos képzési programok hatékonyságát, a technikai szempontokra, például az eszközkezelésre és az adatbiztonságra összpontosítva.
3	Eszköz-gazdálkodás	IoT-eszközök leltározása és osztályozása	- Ellenőrizze, hogy minden IoT-eszköz leltárba vételére és osztályozására sor került-e kockázatuk és funkciójuk alapján. - Biztosítsa, hogy az eszköznyilvántartások tartalmazzák a firmware-verziókat és a javítások állapotát.
4	Hozzáférés-ellenőrzés	IoT-eszközök hozzáférésének kezelése	- Tekintse át az IoT-eszközökre vonatkozó hozzáférés-ellenőrzési irányelveket, biztosítva, hogy azok olyan technikai intézkedéseket tartalmazzanak, mint a többfaktoros hitelesítés.
5	Kriptográfia	Titkosítási szabványok az IoT számára	- Értékelje a titkosítás végrehajtását az IoT-kommunikációban és az adattárolásban. - Ellenőrizze a naprakész és megbízható titkosítási algoritmusok használatát.
6	Fizikai és környezeti biztonság	Az IoT-eszközök fizikai biztonsága	- Ellenőrizze az IoT-eszközök fizikai biztonsági intézkedéseit, különösen a hozzáférhető helyeken lévő eszközök esetében.
7	Üzemeltetési biztonság	IoT-eszközök konfigurációja és kezelése:	- Értékelje az IoT-eszközök biztonsági konfigurációját, beleértve az alapértelmezett beállításokat és a hálózati interfészeket. - Ellenőrizze az IoT-eszközök biztonságos kezelési protokolljainak végrehajtását.
8	Kommunikációs biztonság	Wi-Fi biztonság	- Értékelje az IoT-eszközök által használt Wi-Fi hálózatok biztonságát,

			beleértve a WPA3 és a hálózati szegmentáció használatát. - Ellenőrizze a csaló hozzáférési pontok jelenlétét és a vezeték nélküli behatolásmegelőző rendszerek hatékonyságát.
9	Rendszerbeszerzés, fejlesztés és karbantartás	Biztonságos szoftverfejlesztési életciklus (SDLC) az IoT számára	- Tekintse át a biztonság integrálását az IoT-alkalmazások SDLC-jébe, beleértve a biztonságos kódolási gyakorlatokat és a sebezhetőségi tesztelést. - Értékelje az Io-ra épülő szoftverek frissítésének és javításának folyamatát.
10	Beszállítói kapcsolatok	IoT ellátási lánc biztonsága	- Értékelje a harmadik féltől származó IoT-összetevők és -szolgáltatások biztonsági intézkedéseit. - Tekintse át a szerződéseket a kiberbiztonsági felelősséggel és az incidensekre való reagálással kapcsolatos záradékok tekintetében.
11	Információbiztonsági incidenskezelés	IoT incidensek elhárításának tervezése	- Tekintse át az IoT-eszközöket és -rendszereket érintő forgatókönyvekre vonatkozó incidensreagálási terveket. - Értékelje az IoT-specifikus biztonsági incidensek észlelésére és az azokra való reagálásra való képességet.
12	Az üzletmenet-folytonossági menedzsment információbiztonsági szempontjai	Az IoT bevonása az üzletmenet-folytonosságba	- Ellenőrizze, hogy az IoT-eszközök és -rendszerek megfelelően szerepelnek-e az üzletmenet-folytonossági és katasztrófa-helyreállítási tervekben.
13	Megfelelés	A tárgyak internetére vonatkozó szabályozási megfelelés	- Ellenőrizze a vonatkozó IoT kiberbiztonsági szabályozásoknak és szabványoknak való megfelelést. - Győződjön meg arról, hogy az IoT-adatkezelési gyakorlatok megfelelnek az adatvédelmi jogszabályoknak, mint például a GDPR-nak.
14	IoT-specifikus technikai biztonsági ellenőrzési pontok	Firmware-biztonság	- Értékelje az IoT-eszközök firmware-ének biztonságát, beleértve a biztonságos frissítések folyamatát és a firmware meghamisítása elleni védelmet. - Ellenőrizze a biztonságos rendszerindítási mechanizmusok és a firmware integritásának ellenőrzését.

15		Hálózati biztonság a tárgyak internete számára	- Értékelje az IoT-ra jellemző hálózati biztonsági intézkedéseket, például a hálózati tűzfalakat, a behatolásjelző rendszereket és a biztonságos hálózati protokollokat. - Ellenőrizze az IoT-forgalom elkülönítését a kritikus hálózati szegmensektől.
16		IoT adatvédelem	- Tekintse át az IoT-re vonatkozó adatvédelmi intézkedéseket, az adattitkosításra, az anonimizálásra és a biztonságos adattárolási gyakorlatokra összpontosítva. - Értékelje az adatmegőrzési és adatvédelmi irányelveknek való megfelelést.

KÖSZÖNETNYILVÁNÍTÁS

Köszönettel tartozom a **családomnak** a türelmükért és támogatásukért a doktori tanulmányaim és kutatómunkám ideje alatt;

nagypapámnak, aki miatt folyamatosan motivált voltam az elmúlt években a tudományos munka iránt, hiszen ő is a Magyar Tudományos Akadémián tevékenykedett;

Prof. Dr. Rajnai Zoltán tanár úrnak a témavezetésért és sok éves támogatásáért;

Prof. Dr. Kovács Tibor tanár úrnak, akitől a BSc, MSc és PhD tanulmányim alatt sokat tanultam a tudományos és hétköznapi életről;

Fehér Dávid János barátomnak, akinek a közös cikkek megírása mellett az elmúlt 8 év során nagyon sokat köszönhetek emberileg és szakmailag;

Dr. habil. Velencei Jolánnak a disszertációm korrektúrázásában és nyelvi lektorálásban nyújtott segítségértért;

minden szakmai interjúalanyomnak, **Balázs Zoltán**nak, **Dr. habil. Buttyán Levente**nek, **Dr. Dombora Sándor**nak, **Fehér Dávid János**nak, **Görgényi István**nak, **Rubóczki László**nak, **Varga Péter**nek és **Zsák Péter**nek;

Dr. Tokody Dánielnek és **Ady László**nak az elmúlt évek során kapott szakmai és publikációs lehetőségért;

a Biztonságtudományi Doktori Iskola és az Óbudai Egyetem vezetésének és egyes dolgozóinak, hogy doktori tanulmányaim során szakmailag és tudományosan támogattak.

ELÉRHETŐSÉGEK ÉS AZONOSÍTÓK

- **MTMT azonosító:** 10064423
- **ODT:** 32485
- **ORCID:** 0000-0001-7133-8082
- **Google Scholar:** scholar.google.com/citations?user=pSqxGQUAAAAJ&hl
- **ResearchGate:** www.researchgate.net/profile/Barnabas-Sandor
- **Web of Science:** M-7380-2018
- **IEEE Xplore ID:** 37086507551
- **Academia:** independent.academia.edu/BarnabasSandor
- **Web:** www.sandorbarnabas.hu
- **LinkedIn:** www.linkedin.com/in/sandorbarnabas