

GYARAKI RÉKA ESZTER

Az IoT-eszközök használatának a veszélyei, különös tekintettel a rendőrség bűnügyi feladatainak ellátása során

Absztrakt

A tanulmány az Internet of Things (IoT) eszközök alkalmazásából eredő biztonsági és adatvédelmi kockázatokat vizsgálja, különös tekintettel a közszolgálati és rendvédelmi felhasználásra. Bemutatja az IoT-technológia főbb sérülékenységeit és a szabályozás hiányából fakadó veszélyeket. A kutatás hangsúlyozza a tudatos alkalmazás és az intézményi szintű szabályozás szükségességét.

Kulcsszavak: IoT, rendőrség, adatbiztonság, kihívások

Abstract

This study examines the security and data protection risks related to the use of Internet of Things (IoT) devices, with a focus on public service and law enforcement applications. It outlines key vulnerabilities of IoT technologies and highlights the need for user awareness and institutional regulation.

Keywords: IoT, Law Enforcement, Datasecurity, Challenge

Bevezetés

Az Ipar 4.0 egyik tagadhatatlan vívmánya, hogy a már több évtizede ismert és terjedő informatikai eszközök sokkal több területen jelenjenek meg az emberek életében, ezzel segítve és kényelmesebbé téve a munkájukat és más tevékenységeiket. Szükségessé váltak olyan eszközök, berendezések,

amelyek időt és pénzt spórolnak meg. 2017-re megjelentek az IoT-eszközök a kapcsolódó technológiákkal, amelyek egyszerűbbé tették a gép-gép közötti kommunikációt¹.

Az IoT (Internet of Things) eszközök elterjedése pedig egyre bővül, hiszen számos területen alkalmazzák már az ember fizikai jelenlétének kiváltására vagy helyettesítésére (távoli felügyelet), illetve egyes nagyobb összpontosítást igénylő területeken is az emberi jelenlét mellett. Mindemellett a hétköznapi életünkben is élvezzük a kényelmi funkcióit, mint amilyenek például a kamera- vagy riasztórendszereknek vagy az okosotthonok energiatakarékos eszközeinek vannak.

A tanulmány egy későbbi kutatás alapját képezi, mivel a Magyar Rendőrség nem rendelkezik az IoT-eszközök szabályozásával foglalkozó normával vagy utasítással, és azok alkalmazásával kapcsolatban kockázatfelmérést sem végzett, így az IKT eszközök terjedésének és felhasználásának veszélyeivel sem foglalkozott még az egyes szakterületeken.

Kutatásmódszertan

A kutatást, annak érzékeny témája miatt – a fókuszban a rendvédelmi szervezetek és az Internet of Things eszközök használatának lehetőségei és veszélyei vannak – leginkább az elérhető tanulmányokból, dokumentumkutatás módszerével végeztem el.

A kutatási kérdések

A 4. ipari forradalomban megjelenő új informatikai eszközök lassan, de beszivárogtak a rendvédelem munkájába. A szakemberek nemcsak az állandó kihívásokkal szembesülnek, mint egy bűnygy során az informatikai eszközön tárolt adat bizonyítékként történő felhasználása vagy egy közle-

¹ Kollár Csaba: IoT a gyakorlatban, az információbiztonság fókuszában I. Bolyai Szemle 2017/1. szám. 50. o.

kedési balesetnél a jármű informatikai rendszerének vagy a helyszíni kamerák ellenőrzésének nehézségei, hanem akár a munkahelyi feladataik során alkalmazott IoT-eszközök biztonsági kérdéseivel, illetve a saját maguk által használt IoT-eszközök biztonsági kihívásaival is.

A Magyar Rendőrség jelenleg még nem vezetett be az IoT-eszközökkel kapcsolatban semmilyen korlátozást, így azok alkalmazásának megfontolása sokszor a felhasználók biztonságtudatosságán múlik (H1).

Az IoT-eszközök mindennapi használatát a rendőrség állományának körében szigorításokkal lehetne csak alkalmazni, hiszen azok tartalmazhatnak olyan sérülékenységeket, amelyek veszélyeztethetik egy eljárás sikerét (H2).

Az IoT-eszköz fogalma

Mielőtt a jogszabályi fogalmat meghatároznánk – ami egyébként nem klasszikus definíció, csak egy szabályozás bevezetéséhez szükséges értelmező definíció –, egy érthetőbb leírásból indulunk ki.

„A hazai szabályozás szerint az IoT-eszközök olyan IKT-terméknek minősülnek, amelyek jelátalakítás révén a környezettel képesek kölcsönhatásba lépni. „A kölcsönhatás formája lehet:

- a) érzékelés, amelynek során az IoT-eszköz a környezetről adatot gyűjt, illetve*
- b) beavatkozás, amely által a környezetben változás következik be.*

Az említett kölcsönhatás megvalósulhat:

- a) alkalmazásprogramozási felület (a továbbiakban: API) által, amely biztosítja, hogy más számítástechnikai eszközök kommunikáljanak egy IoT-eszközzel az IoT-eszköz által biztosított alkalmazáson keresztül,*

- b) *felhasználói felület által, amely biztosítja az IoT-eszköz és a felhasználó közötti közvetlen kommunikáció lehetőségét, vagy*
- c) *hálózati kapcsolat által, amely biztosítja az IoT-eszköz elektronikus hírközlő hálózattal való kommunikációját adatok IoT-eszköze vagy IoT-eszközeről történő közlése céljából vagy a hálózati felhasználói felület elérését.*²

Az IoT-eszközöknél tehát kockázatot jelent az, hogy ezek az eszközök egymással kommunikálnak, amihez ugyanazt a hálózatot használják. Ezek a hálózatok sokszor nem titkosítottak és biztonságosak. A frissítéseket nem végzik el, hiszen nem mindig egyértelmű, hogy mikor ad ki a gyártó frissítést, ezért sebezhetőségük nincs vagy nem időben van kiküszöbölve. Ugyanakkor az is előfordul, hogy ismeretlen gyártótól származó eszközhez egyáltalán nem adnak ki frissítést.

A gyári beállítások, amelyek a jelszavak vagy a felhasználók adatvédelmével vannak összefüggésben, nincsenek a felhasználók igényeire szabva. Egyszerűen az eszközök minél gyorsabb beüzemelése a cél, így a jelszavaknál, a felhasználási feltételeknél és az adatvédelmi beállításoknál nem történik meg a felhasználók személyre szabása.

Az IoT vagyis az Internet of Things (dolgok internete) olyan internetre csatlakoztatott eszközök összessége, amelyek képesek kommunikálni más eszközökkel és hálózatokkal, de funkcionalitásuktól függően sokféle feladatra alkalmasak.³

Arról, hogy mit lehet IoT-eszköznek tekinteni, a szakemberek eltérő álláspontokat képviselnek. Egyesek szerint minden eszköz annak tekinthető, amelyik kapcsolódik az internetre – így az okostelefonok, tabletek –, míg mások szerint csak azok, amelyek nem rendelkeznek Windows, Linux, IOS

² Az IoT-eszközök nemzeti kiberbiztonsági tanúsítási rendszeréről szóló 10/2024. (VIII.8) SzTFH rendelet.

³ Nemzeti Kibervédelmi Intézet. 2022.

Forrás: https://nki.gov.hu/wp-content/uploads/2022/09/IoT-eszkozok-biztonsagi-kerdesei_II_CTI_jelentes.pdf

Letöltés ideje: 2026.08.08.

stb. operációs rendszerrel, ugyanakkor képesek a felhasználó felé adatok továbbítására. Egy dologban azonban a fellelt tanulmányok megegyeznek. Mégpedig abban, hogy ezek az eszközök gyengébb biztonsági rendszerrel rendelkeznek, hiszen a gyártók elsősorban úgy tervezték azokat, hogy olcsók és könnyen használhatók legyenek.⁴

Azért, hogy a felhasználók felé a kényelmi funkciók maradéktalanul be-tartassanak, nemcsak a környezetére vonatkozóan, maga a végfelhasználó számára küldi az adatokat, hanem valamennyi, a működése során össze-gyűjtött adatot akár a gyártó felé, akár egy másik IoT-eszköz felé is tovább-bíthatja.

Az utóbbi időben már egyre több oldalról közelítik meg az IoT-eszkö-zök szerepét a mindennapi életben, hiszen a kényelem és a praktikusság mellett felismerték annak kockázatait is, olyannyira, hogy a 2025-ben meg-jelent Magyarország Kiberbiztonsági Stratégiája a mesterséges intelligen-cia mellett szintén veszélyként azonosítja, és a kiberbiztonság legnagyobb kihívásai közt említi az adatbiztonsági kihívások pont alatt:

„...külső és egyéb fenyegetések mellett további kockázatot jelent, hogy a kibertér alkotóelemeiként szolgáló elektronikus információs rendszerek szabályozása nem elég széles körű, túlságosan decentralizált. A dinamiku-san megjelenő és terjedő technológiák – mint például a mesterséges intel-ligencia alapú technológiák, az Internet of Things (a továbbiakban: IoT) eszközök, az 5G-vel megjelenő új technológiák és eszközök – újabb bizton-sági kockázatok folyamatos kialakulásához vezetnek, a felhasználók tech-nológiai kitettsége folyamatosan növekszik, így elengedhetetlen annak el-várása, hogy az új technológiák bevezetésének elsődleges feltétele a biz-tonságos környezet kialakítása.”⁵

⁴ Oláh Levente: Az IoT eszközök veszélyei.

Forrás: <https://pecsimernok.hu/az-iot-eszkozok-veszelyei/>

Letöltés ideje: 2026.08.08

⁵ Magyarország Kiberbiztonsági Stratégiájáról szóló 1089/2025. (III. 31.) Korm. határo-zat

Az egyes statisztikai adatok szerint közel 15 milliárd IoT-eszköz csatlakozik világszerte, amelyeknek száma 2025-re eléri a 25 milliárdot is (G, 2024), amit már az újabb statisztikai adatok meg is cáfoltak, hiszen az internethez csatlakozó eszközök száma a 2025-ös év végére meghaladhatta a 35,2 milliárdot. Ugyanakkor egyes becslések szerint 2030-ban akár 100 milliárd IoT-eszköz lesz használatban. A számok pedig azért riasztók is egyben, mert a kiberbűnözők nagy hatékonysággal képesek kihasználni ezt a hatalmas és nagyon sebezhető támadási felületet.

Krasznay az IoT-eszközök kiberbiztonsági kockázatainál (Krasznay, 2022) a Mirai botnet példáján keresztül – amelyet 2016-ban fedeztek fel, és amely 2014 óta fertőzte meg az IoT-eszközöket, így az okoskamerákat, okos ajtócsengőket stb., bothálózatként használva őket –említi, leginkább azok a hálózatba kapcsolt és gyenge eszközök voltak ennek a támadásnak kitéve, amelyiken a gyári jelszót nem változtatták meg. Kezdetben a Linux operációs rendszert használó eszközök voltak kitéve ennek a támadásnak, majd az Android rendszerű eszközöket is képes volt a malware megfertőzni.⁶

Természetesen az IoT vagy sokszor okoseszközök szinonimájaként használt informatikai eszközök egyre nagyobb népszerűsége tettek és tesznek szert az otthonokban, valamint a mindennapjainkban is, hiszen képesek rengeteg emberi energiát megspórolni, irányításuk távolról elérhető, meghatározott időpontban elindíthatók, leállíthatók és a felhasználó által is kontrolálhatók.

Az okoseszközök közé tartoznak például a különböző mozgásokhoz, sportoláshoz használt órák, aktivitásmérők, pántok, tárgyakra és állatokra tehető helyzetjelző eszközök, berendezések, vagy az okosotthonokban is alkalmazott, sokszor az otthon biztonságának megőrzésén túl a felhasználók kényelmét is szolgáló okos kávéfőző, okostermosztát, porszívó, mérő-

⁶ Zieniüté, Ugné: What is the Mirai botnet, and how does it spread?

Forrás: <https://nordvpn.com/blog/mirai-botnet/>

Letöltés ideje: 2024.04.16

órák stb. Ezek az eszközök már önmagukban is rejthetnek veszélyeket, egyrészt a népszerűség miatt (ezt már fentebb is említettük) és azért, hogy minél többet tudjanak értékesíteni és a kereskedelmi áruk is elfogadhatóbb legyen, mint a vetélytársuké, azok biztonságára, az információk gyűjtésével kapcsolatos felhasználói magatartásra a lehető legkevesebb figyelmet fordítanak. Márpedig így a felhasználók sokkal sérülékenyebbek lehetnek, hiszen folyamatosan adatot gyűjtenek és továbbítanak róluk, illetve arról az eszközről is, amelyhez csatlakoztatva vannak.

Az Adatvédelmi Munkacsoport 2014-ben adta ki a tárgyak internetével foglalkozó véleményét⁷, amely szerint:

*„A tárgyak internete (Internet of Things) olyan infrastruktúrára utal, amelyben a mindennapi eszközökbe (önálló „dolgokba” vagy egyéb tárgyakhoz vagy személyekhez kapcsolódó dolgokba) beépített érzékelők milliárdjait arra tervezik, hogy adatokat rögzítsenek, kezeljenek, tároljanak és továbbítsanak, és – mivel egyedi azonosítóval rendelkeznek – a hálózati szolgáltatások segítségével együttműködjenek más eszközökkel vagy rendszerekkel.”*⁸

Az említett Stratégia az adatbiztonsági kihívások mellett adatvédelmi kihívásokkal is foglalkozik:

*„az IoT szenzorok folyamatosan adatokat gyűjtenek a környezetükről és a betegekről. Az eszközök által generált adatokat megfelelően szükséges védeni. Az adatok titkosítása, hitelesítése és biztonságos tárolása elengedhetetlenül fontos.”*⁹

⁷ 29. cikk szerinti Adatvédelmi Munkacsoport: 8/2014. számú vélemény a tárgyak internetének legújabb fejleményeiről, WP223, elfogadás: 2014. szeptember 16. (továbbiakban: WP223)

⁸ ua.

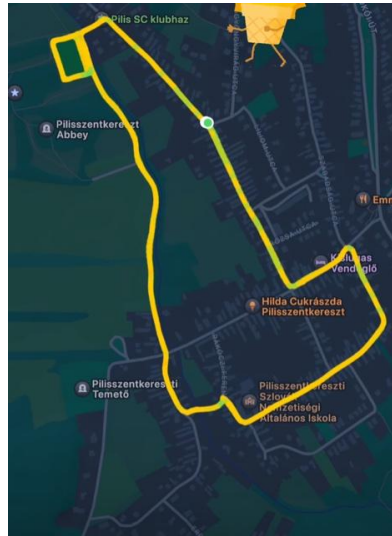
⁹ Magyarország Kiberbiztonsági Stratégiájáról szóló 1089/2025. (III. 31.) Korm. határozat

Az egyik jelentős eset egyébként 2018-ban történt, amikor az Amerikai Egyesült Államok hadserege állományának megtiltották a különböző okoseszközök, így az okosórák (beleértve a fitneszórákat), okostelefonok és egyéb olyan aktivitásmérők alkalmazását, amelyek helymeghatározó funkcióval is rendelkeznek, hiszen ezek a használók napi futásteljesítményének mérése során jól ábrázolható területen felfedték az amerikai hadsereg katonai bázisait, és megjelentették egy térképen, ezáltal veszélyeztetve azok biztonságát, titkosságát, vagy épp megismerhetővé téve az egyes alakulatok mozgását.¹⁰

Ezek az okosórák nagyon népszerűek a mindennapokban is, mivel segítségével a sporttevékenység, a mozgás ellenőrzése mellett egészségügyi adatokat (például többek között pulzusszám, véroxigénszint, EKG) tárolnak, valamint hozzáférést engedhetnek egyéb informatikai eszközökhöz is.

Az 1. képen egy közösségi médiában is szívesen posztolt futási tevékenység látszik, amiből egy egyszerű OSINT (Open Source Intelligence) technika segítségével a felhasználóról rengeteg információ kikövetkeztethető.

¹⁰ Forrás: <https://napidroid.hu/az-amerikai-hadsereg-megtiltotta-katonainak-az-okosorak-hasznalatat-mert-azok-titkos-bazisokat-lepleztek-le/>
Letöltés ideje: 2018.08.09.



1. számú kép
IoT-eszközzel készített fitnesztevékenység

Az IoT-eszközök sérülékenysége

A folyamatosan növekvő, mind a magán-, mind az ipari szférában alkalmazott IoT-eszközpark új és összetett kihívások elé állítja a biztonsági szakembereket. Az eszközök sajátos működési logikája és heterogén felépítése miatt a hagyományos kiberbiztonsági megközelítések nem elegendőek; új szemléletmódra és fejlesztési irányokra van szükség annak érdekében, hogy csökkenjen a felhasználók bűncselekményeknek való kitettsége, valamint a potenciális terrortámadások esélye is minimalizálható legyen.

Bár az IoT-eszközök elsődleges célja a hálózatba kapcsolt működés biztosítása, ez a funkció egyben az egyik legnagyobb biztonsági kockázat forrása is. Fontos hangsúlyozni, hogy az általános kiberbiztonsági protokollok nem egyenlők az IoT-rendszerek védelmével. Míg a klasszikus kiberbiztonsági szakértelem elsősorban a számítógépek és hálózati rendszerek védelmére koncentrált, az IoT-eszközök – mint az elektronika és számítástechnika határterületén mozgó eszközök – sajátos biztonsági kockázatokat hoz-

doznak. Bár rendelkeznek számítógépszerű komponensekkel, nem tekint-hetők teljes értékű számítógépeknek, így biztonsági kezelésük külön meg-közelítést igényel.

Az IoT-rendszerek működése során számos sérülékenység azonosítható. E sérülékenységek lehetnek egyszerűek vagy komplexek, és bár önmaguk-ban nem feltétlenül jelentenek közvetlen terrorfenyegetést, megismerésük elengedhetetlen a rendszerszintű kockázatelemzéshez.

Egyes tanulmányok megállapításai szerint az IoT-eszközök gyakran rendelkeznek gyenge hitelesítő mechanizmusokkal, elégtelen adatkezelési eljárásokkal, valamint a felhasználói tudatosság is alacsony szinten áll. To-vábbi problémák a hiányos biztonsági szabályozás, a tervezési hibák, a nyi-tott portok, a kritikus komponensek elválasztásának hiánya, az elégtelen fizikai védelem, a nem biztonságos interfészek és hálózati szolgáltatások, valamint az általános adatvédelmi aggályok.¹¹

A gyenge hitelesítő adatok alkalmazása az egyik legjelentősebb kocká-zati tényező. Az autentikáció – például felhasználónév és jelszó – alapvető biztonsági követelmény, azonban sok IoT-eszköz alapértelmezett, könnyen kitalálható hitelesítő adatokat használ, amelyeket gyakran nem lehet mó-dosítani. Például a fitnessórák egyáltalán nem vagy maximum 4–6 számje-gyet kérnek a rendszer hozzáféréséhez. Az ilyen gyenge védelemmel a tá-madók számára megkönnyítik, hogy a rendszerhez minimális erőfeszítéssel hozzá tudjanak férni, ami által akár más eszközökhöz is szabad bejárásuk lesz. Ez a gyártók oldaláról gyakran költségcsökkentési szempontokkal vagy a rendszerhasználat egyszerűsítésének igényével magyarázható.

A nem biztonságos adatkezelés szintén súlyos kockázatot jelent. Az IoT-eszközök működésük során érzékeny adatokat (például hitelesítő ada-tok, parancs adatok, személyes információk) generálnak, amelyek védelmét titkosítással és hozzáférés-szabályozással szükséges biztosítani. Ezen ada-tok védelmének elmulasztása súlyos következményekkel járhat, beleértve a rosszindulatú manipuláció lehetőségét is.

¹¹ Adaros Boye, Carolina A.: Understanding Cyberrisks in IoT: When Smart Things Turn Against You. Business Expert Press. 2019.

További problémát jelent a hitelesítési mechanizmusok hiánya. Ellenében a számítógépes rendszerekkel, ahol többszöri sikertelen bejelentkezés esetén automatikus zárolás lép életbe, sok IoT-eszköz nem rendelkezik ilyen védelmi mechanizmussal, még a legmodernebbek sem. Ezt a támadók kihasználhatják például a „brute force” támadások¹² során, vagy épp ellenkezőleg, egy üzemi környezetben a felhasználók kizárásával működési zavarokat okozhatnak.

Az emberi tényező, mint sérülékenységi komponens szintén kritikus jelentőségű. A felhasználók számára biztosított jogosultságoknak arányban kell állniuk a feladataikkal; minden jogosultság általános megadása a rendszer kompromittálásának kockázatát jelentősen növelheti, ezért a felhasználók rendszeres képzése, biztonságtudatosságuk növelése elengedhetetlen a kockázatok csökkentéséhez. Fontos továbbá az is, hogy ezek az eszközök kizárólag olyan funkciókat lássanak el, amelyek ténylegesen szükségesek, és például felesleges internet-hozzáféréssel ne rendelkezzenek, de ezekről a későbbiekben lesz még szó.

Számos gyártó nem rendelkezik megfelelő protokollal vagy supporttal sem a biztonsági hibák bejelentésére vagy kezelésére, továbbá hiányzik a kötelező biztonsági követelményekre vonatkozó szabályozás is. A gyenge biztonsági szabályozás a gyártói oldalon jelentkező strukturális problémára is utal, ami az átláthatóság és a felelősségvállalás hiányát is eredményezheti.

Az IoT-eszközöknél a megjelenő tervezési hibák gyakran lehetőséget biztosítanak rosszindulatú kódok integrálására, a kommunikációs csatornák kompromittálására vagy a jelszóváltoztatás korlátozására, és nem utolsósorban sokszor az ár-érték arány miatt nem fordítanak erre elég nagy figyelmet. Ezek nem kizárólag hardveres, hanem sokszor szoftveres eredetű problémák, amelyek kezelése firmware-frissítéseken keresztül lehetséges, azonban ehhez előbb szükséges a hiba lokalizálása.

¹² A brute force támadás egy olyan hackelési technika, amelyben a hacker több felhasználónevet és jelszót próbál ki gyorsan egymás után, gyakran számítógéppel teszteli a kombinációk széles skáláját, amíg meg nem találja a megfelelő bejelentkezési adatokat. (Forrás: Fortinet)

A portok – legyenek azok fizikai (például USB) vagy logikai (például hálózati portok) – sebezhetősége kiemelt figyelmet érdemel. A nyitott, nem megfelelően konfigurált portok visszaélésre adnak lehetőséget, például kártékony kódok fizikai adathordozókon történő bejuttatásával. Ezért elengedhetetlen, hogy az eszközök csak a feltétlenül szükséges portokkal rendelkezzenek.

Kritikus komponensek elkülönítésének hiánya esetén a rendszerek sérülékennyé válhatnak. Például egy vonaton az utasok számára biztosított nyilvános Wi-Fi hálózatot szigorúan el kell különíteni a vasúti irányítási rendszertől. E követelmény megsértése súlyos biztonsági kockázatokat hordozhat.

Végül, az IoT-eszközök földrajzi elhelyezkedése és fizikai hozzáférhetősége is kockázati tényező. Kültéri vagy távoli környezetben telepített eszközök fizikailag is hozzáférhetővé válhatnak illetéktelen személyek számára, akik ezeket manipulálhatják, vagy akár ki is cserélhetik, anélkül, hogy azok manipulálásáról értesítést küldenének, vagy akár bármilyen fizikai behatás észrevehető lenne rajta.

Az IoT-eszközök kockázatainak humán oldala

Ezeknek az eszközöknek a kockázatai ugyanakkor nemcsak magukban az eszközökben, vagyis azok gyártóiban keresendők, hanem sokszor a felhasználók viselkedésében is, így nem feltétlenül az eszközt, mint biztonsági tényezőt említem, hanem annak felhasználóját.

Az IoT elterjedésével az egyik legnagyobb probléma az, hogy máig sok eszközből még az alapvető biztonsági funkciók is hiányoznak. Az alapértelmezett jelszavak gyakran változatlanok maradnak a készülék megvásárlása után is, hiszen a felhasználó vagy nem tudja vagy nem is akarja megváltoztatni azt, illetve sokszor egy-egy szolgáltató neve vagy az eszköz márkája bizalmat kelt a felhasználókban. Az eszközök működését biztosító szoftverek és a firmware rendszeres biztonsági frissítései hiányoznak, és a titkosítást nem hajtják végre következetesen.

Az okos otthoni eszközök használata, aktivitása akár egy applikáción keresztül előre beállított (ismétlődő) időpontokban vagy külső/belső körülmény bekövetkezésekor (többek között időjárás megváltázása, mozgás vagy annak hiánya, a használó elesése) hangvezérléssel, de akár egy egyszerű gombnyomással is történhet. Ezek a körülmények adatokat, információkat továbbítanak, amelyekből sokszor olyan tények vonhatók le, amelyek a felhasználót vagy a környezetét akarva-akaratlanul is jellemzik. Erre példaként hozható 2020-ban Simon Weckert művész egyik kísérlete Berlinben, amikor 99 darab mobiltelefonnal, amelyek helyadata be volt kapcsolva, átsétált egy berlini hídon. Ezzel bizonyítva azt, hogy azok a gépjárműben ülők, akik a Google Mapson (vagy más közlekedést segítő alkalmazáson) keresztül figyelemmel kísérik a közlekedési útvonaluk megválasztása során, hogy merre vannak forgalmi dugók a városban, elkerülték azt az útvonalat, hiszen az applikáció forgalmi torlódást jelzett nekik.¹³

További kockázati tényező az alkalmazásoknál az adatszivárgás, amelyet egyrészt az eszköz gyártója vagy forgalmazója önmaga is okozhat, valamint maga a felhasználó, amennyiben nem megfelelően állítja be az eszközt vagy az azzal összekötött más eszközöket, illetve hálózatot.

Az IoT-eszközök gyakran gyűjtenek és továbbítanak bizalmas adatokat. Ha ezek az adatok nincsenek megfelelően titkosítva, miközben az eszközök és a háttérkiszolgálók között haladnak, a hackerek elfoghatják őket. A támadások során az ügyfelek adatai, vagy akár a szellemi tulajdona, egy válalkozás üzleti titkai is sérülhetnek.

A tudatosság hiánya és oktatás szükségessége

A felhasználók biztonságtudatossága kulcsfontosságú tényező az IoT-eszközök hatékony és biztonságos használata során. A felhasználók gyakran nincsenek tisztában az IoT-eszközöket érintő potenciális fenyegetésekkel, például az eszközök nyitott portjaival, a nem titkosított kommunikációval

¹³ Forrás: <https://www.simonweckert.com/googlemaphacks.html>
Letöltés ideje: 2026.08.08.

vagy a frissítések hiányával. Nagyon sok szervezetnél, bár vannak biztonság tudatosító oktatások, azok túl általánosak, a jogszabályoknak és belső szabályzóknak való gyors megfelelés miatt formálisak, nem specifikusak, nem mindig az adott szervezetre szabják a képzéseket, írják az oktatási segédleteket.

Oser és szerzőtársai hangsúlyozzák, hogy az edukációs kezdeményezések kulcsfontosságúak az IoT-ökoszisztéma védelme szempontjából¹⁴. Ez különösen fontos az ipari és egészségügyi IoT-alkalmazások esetében, ahol az eszközök kompromittálása közvetlen hatással lehet emberi életre is.

Az IoT biztonságának másik kritikus szempontja az általa generált és feldolgozott adatok köre. Az IoT-eszközök folyamatosan hatalmas mennyiségű adatot gyűjtenek, amelyek nagy része érzékeny vagy magánjellegű.

Ezen adatok védelme az életciklusuk során – az összegyűjtéstől és továbbítástól a tárolásig és feldolgozásig – rendkívül fontos. Az adatok biztonságos kezelésének, integritásának és elérhetőségének biztosítása az IoT-rendszerekben azonban kihívást jelent az adattárolás decentralizált jellege és az adatfeldolgozáshoz szükséges harmadik fél felhőszolgáltatásokra való támaszkodása miatt. Ezen túlmenően az IoT-rendszerek gyakran több érdekelt felet is magukban foglalnak, amelyek mindegyike eltérő biztonsági követelményekkel és kockázat-toleranciával rendelkezik, ami bonyolítja az egységes biztonsági politikák kidolgozását.¹⁵

Gyenge hitelesítési gyakorlatok

Az alapértelmezett hitelesítő adatok használata és a gyenge jelszavak alkalmazása továbbra is az egyik legjelentősebb emberi hibaforrás az IoT-eszközök védelmében. Butun és szerzőtársai rámutatnak arra, hogy számos eszközön nem lehet megváltoztatni az alapértelmezett jelszavakat, illetve a

¹⁴ Oser, R. et al.: 'Cybersecurity Awareness in IoT: A User-Centric Perspective'. Journal of Cyber Policy 2021/2. szám. 198–214. o.

¹⁵ Dritsas, Elias; Trigka, Maria: A Survey on Cybersecurity in IoT. Future internet. 2025.

felhasználók gyakran nem élnek a lehetőséggel még akkor sem, ha ez technikailag lehetséges.¹⁶ A hitelesítési gyakorlatok megerősítése érdekében többlépcsős azonosítási mechanizmusokat és rendszeres jelszócserét lenne célszerű bevezetni, amelyeket egyértelmű és érthető felhasználói útmutató egészít ki.

Az eszközhitelesítés és az identitáskezelés az IoT-ökoszisztéma biztonsági architektúrájának kritikus elemei, amelyek az első védelmi vonalat jelentik a jogosulatlan hozzáférés és a rosszindulatú tevékenységek ellen.¹⁷ A hagyományos számítástechnikai környezetekkel ellentétben az IoT-hálózatokat hatalmas méretű, heterogén módon összekapcsolt eszközök jellemzik, amelyek mindegyike különböző szintű számítási teljesítménnyel és biztonsági képességekkel rendelkezik.¹⁸

Hasonlóképpen, az intelligens városok alkalmazásai gyakran skálázható identitáskezelést igényelnek a dinamikusan hozzáadott és eltávolított eszközök, például a csatlakoztatott közlekedési lámpák és környezeti érzéklők kezeléséhez. Az IoT-eszközök hitelesítésének egyik fő kihívása a bizalom megteremtése olyan környezetben, ahol az eszközöket gyakran megbízhatatlan vagy ellenséges környezetben telepítik. Az identitáskezelés az IoT-eszközöknél túlmutat a pusztán hitelesítésen, és magában foglalja az eszközidentitásuk teljes életciklusát.

Az IoT-identitáskezelés egyik legfőbb kihívása az IoT-környezetek dinamikus jellege, ahol az IoT-identitáskezelés egyik legfontosabb kihívása az IoT-környezetek dinamikus jellege, ahol az eszközök gyakran csatlakoznak a hálózathoz és távoznak onnan, gyakran minimális emberi beavatko-

¹⁶ Butun, Ismail; Österberg, Patrik; Song, Houbing Herbert: Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures. IEEE COMMUNICATIONS SURVEYS & TUTORIALS. 2019.

¹⁷ Mamdouh, Moustafa; Awad, Ali Ismail; Khalaf, Ashraf; Hamed, Hesham F.A.: Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions. Computers & Security. 2021.

¹⁸ Javed, Asad; Malhi, Avleen; Kinnunen, Tuomas; Framling, Kary: Scalable IoT Platform for Heterogeneous Devices in Smart Environments. 2020.

zással vagy anélkül. Ez a dinamikus jelleg olyan identitáskezelési rendszereket igényel, amelyek autonóm módon működnek, biztosítva, hogy az eszközök biztonságosan integrálódjanak a hálózatba, és identitásuk kezelhető legyen a biztonság veszélyeztetése nélkül.

Nem biztonságos adatkezelés

Az emberi hibák jelentős részét az okozza, hogy a felhasználók nem megfelelő módon kezelik az eszközök által generált vagy továbbított adatokat. Az érzékeny információk – például biometrikus adatok, lokációs információk vagy egészségügyi paraméterek – gyakran titkosítás nélkül kerülnek továbbításra vagy tárolásra. Borgohain és társai szerint az ilyen nem biztonságos adatkezelés súlyos sebezhetőségekhez vezethet, különösen, ha az eszközök több másik rendszerrel is kapcsolatban állnak.¹⁹ Ezen túlmenően, a hozzáférési jogosultságok megfelelő beállítása is elengedhetetlen, hogy elkerülhető legyen az illetéktelen hozzáférés.

Az IoT-eszközök hatalmas mennyiségű adatot gyűjtenek, ami számos adatvédelmi kockázatot jelenthet. A Szövetségi Kereskedelmi Bizottság jelentése szerint mindössze 10 000, okosotthon-technológiát használó háztartás naponta akár 150 millió különálló adatpontot is generálhat.²⁰ Ezek az adatok gyakran érzékeny információkat tartalmaznak. Minél több adat áll rendelkezésre, annál nagyobb az esélye annak, hogy az adatokból következtetéseket lehessen levonni és azokat összekapcsolni egy profil létrehozása érdekében. Az IoT-ban a magánélet védelmével kapcsolatos másik probléma az, hogy az ellenségek lehallgathatnak, azaz virtuálisan behatolhatnak egy személy otthonába, követhetik mozgását és cselekedeteit, vagy akár megjósolhatják, hová mehet.

¹⁹ Borgohain, Tuhin; Kumar, Uday; Sanyal, Sugata: Survey of Security and Privacy Issues of Internet of Things. Computer Science. 2015.

²⁰ Staff, F: Internet of Things : Privacy and Security in a Connected World. Technical report, Federal Trade Commission. 2015.

Felhasználói jogosultságok hibás kezelése

A túl széles jogosultságok biztosítása a felhasználók számára komoly kockázatot jelent. Egy kompromittált fiók esetén a támadó adminisztratív jogosultságokkal férhet hozzá az eszköz teljes funkcionalitásához. Ennek megelőzése érdekében a „*legkisebb jogosultság elve*” alkalmazandó, azaz minden felhasználónak csak azokat a jogokat kell megadni, amelyek feltétlenül szükségesek a feladatuk elvégzéséhez. West és társai hangsúlyozzák, hogy az IoT-környezetekben különösen fontos a jogosultságok rendszeres auditálása és naplózása.²¹

Frissítések elmulasztása

Az eszközök szoftverének és firmware-jének naprakészen tartása létfontosságú a biztonság fenntartása szempontjából. Azonban a felhasználók sok esetben nem hajtják végre a szükséges frissítéseket, vagy nem is tudnak azok elérhetőségéről, amely probléma különösen az alacsony erőforrásigényű, olcsó IoT-eszközöknél gyakrabban fordul elő, és amelyek esetében nem áll rendelkezésre automatikus frissítési mechanizmus.²² A felhasználók edukációja mellett a gyártóknak is felelősséget kell vállalniuk, és egyszerű, automatizált frissítési lehetőségeket kell biztosítaniuk.

A fizikai biztonság elhanyagolása

Az IoT-eszközök gyakran olyan helyeken kerülnek elhelyezésre, ahol könnyen hozzáférhetők illetéktelenek számára. Ez különösen igaz az ipari, mezőgazdasági vagy városi környezetekben alkalmazott IoT-megoldásokra. A felhasználók gyakran nincsenek tisztában azzal, hogy a fizikai manipuláció – például az eszköz eltávolítása, átalakítása vagy cseréje – szintén

²¹ West, J; Bhattacharya, M; Islam, R: Intelligent Access Control for Internet of Things. Future Generation Computer Systems. 2019. 520-535. o.

²² Alrawais, A; Alhothaily, A; Hu, C; Cheng, X: Fog Computing for the Internet of Things: Security and Privacy Issues. IEEE Internet Computing. 2017. 34-42. o.

biztonsági kockázatot jelent. Roman és kutatótársai szerint a fizikai biztonsági protokollok hiánya sok esetben lehetővé teszi a támadók számára, hogy közvetlenül hozzáférjenek az eszköz hardveréhez, és így kompromitálják annak működését.²³

Az ember jelentette kockázatok közé tartozik, hogy az IoT-eszközöket a felhasználók magukkal is vihetik a munkahelyükre, illetve az odajutáshoz segítségül vehetik azokat. Az alkalmazásukra a munkáltatók előírhatnak vagy előírhatnának szabályokat, de ezek a szabályok/szabályzók leginkább a munkáltató által biztosított eszközökre és rendszerekre vonatkoznak (pl. a munkáltató által biztosított eszközt nem csatlakoztathatják nyílt wifi hálózathoz, vagy egyes weboldalakat tilos megnyitni stb.). Ugyanakkor a felhasználók tudatossága és kultúrája még mindig nem terjed ki arra, hogy milyen veszélyeket rejt a informatikai eszközök munkahelyi használatára vonatkozó előírások be nem tartása egy cégre.²⁴

Amennyiben belegondolunk abba, hogy a már említett, ártalmatlannak tűnő sportóra, amelyet minden egyes nap a munkába menet a megtett távolság vagy lépésszámok rögzítésére használnak, már megmutatja azt, hogy a felhasználó mikor és honnan, esetleg milyen eszközzel (például kérekpár) hova tart a hét melyik napjain, hány órakor indul el, és meddig tartózkodik az adott helyen, már nagyon sok információ forrása lesz, különösen akkor, ha valakinek a mozgását és szokását meg szeretnék ismerni. Ezek az eszközök egy applikáción keresztül is megtekinthetők, amely információkat ad, sokszor térképen megjelölve a viselője helyzetét vagy aktivitását.

²³ Roman, R; Najera, P; Lopez, J: 'Securing the Internet of Things'. Computer 2011/9. szám. 51-58. o.

²⁴ A belső szabályzat be nem tartása a munkavállaló felelősségi körébe tartozik.

A legkockázatosabb IoT-eszközök

Ahogy az első két fejezetben is írtam, az IoT-eszközök nem rendelkeznek beépített biztonsággal. Erre azért lenne szükség, mert ezek az eszközök titkosítás nélkül továbbítják az általuk gyűjtött adatokat többek között egy központi rendszerbe vagy a felhőbe, ezért azok biztonsága, például az adat-szivárgások megakadályozása kiemelt feladat és szempont a használatuk során. Az eszközök által jelentett kockázatot erősíti, amikor egy szervezet tevékenységének elősegítéséhez, vagyis az alkalmazott információs rendszerek működéséhez elengedhetetlen az IoT-eszközök használata.^{25,26}

Míg az otthonok és a vállalkozások is alkalmazzák az IoT-eszközöket, ezek üzleti környezetben való felhasználása aggályokat vethet fel. A kiskereskedelem, a gyártás, az egészségügy és a kritikus infrastrukturális ágazatok, mint például az energiaszolgáltatás és a szállítás, nagymértékben támaszkodnak az IoT-érzékelőkre, a rendszervezérlőkre és a távfelügyeletre, ezért a kiberbűnözők célpontjaivá válhatnak.

A vállalkozások 43%-a azonban nem rendelkezik biztonsági védelemmel az IoT-infrastruktúra egyes részein. A rengeteg IoT-eszköz közül a legtöbb Linux alapú operációs rendszeren működik. Ezek a Linux alapú IoT-eszközök a támadók kedvenc célpontjává váltak. Kaspersky több mint 1,5 milliárd IoT-támadást észlelt 2021 első felében – az előző félévi 639 millióhoz képest, ami több mint kétszerese az azt megelőző időszaknak.²⁷

Amikor a rosszindulatú programok megfertőzik az IoT-eszközöket, a támadók könnyen manipulálhatják ezeket az eszközöket saját céljaik szerint, például adatokat szerezhetnek a fizikai világból, vagy ugródeszkaként használhatják azokat más eszközök megfertőzésére.

²⁵ Forrás: <https://nki.gov.hu/it-biztonsag/elemzesek/iot-eszkozok-biztonsagi-kerdesei-az-okosotthon/>

Letöltés ideje: 2026.08.08.

²⁶ Például Internet of Medical Things (IoMT) vagyis az orvosi dolgok internete.

²⁷ Forrás: <https://hu.kaspersky.com>

Letöltés ideje: 2022.

Az, hogy lehet-e a legkockázatosabb jelzővel illetni egy informatikai eszközt, szintén kérdés, főleg az, hogy mi alapján. A NISA és NIST dokumentumaiban található szempontrendszeres kockázatelemzési logika alapján, az OWASP IoT Project által javasolt a sebezhetőségek pontozása (lista).

Az ISO/IEC 27005 (Információbiztonsági kockázatkezelés) szabvány kockázatértékelésre épülő rendszereket (például az „esemény valószínűség × hatás súlyossága” logika) és a NIST SP 800-30 (Guide for Conducting Risk Assessments) által alkotott pontrendszerek alapján egy mátrix felállítása is lehetséges, amelyet az 1. táblázatban láthatunk.

Szempont	1 pont (alacsony)	5 pont (nagyon magas)
Funkciókritikusság	Nem létfontosságú	Életvédelmi/Kritikus infrastruktúra
Adatérzékenység	Minimális adatgyűjtés	Érzékeny személyes vagy pénzügyi adatok
Sebezhetőség	Keményített, auditált	Gyenge beállítások, ismert sérülékenységek
Hálózati kitettség	Zárt belső hálózat	Internetre nyitott, gyenge védelem
Frissíthetőség	Automatikus biztonsági frissítések	Nem frissíthető, elavult
Gyártó megbízhatósága	Tanúsított, auditált	Ismeretlen, problémás múltú

*1. számú táblázat
IoT-eszközök kockázati mátrixa – saját szerkesztés²⁸*

Az értékelés szempontjai: Minél szorosabban integrálódnak az IoT-eszközök az életünkbe, annál komolyabb kockázatokat hordoznak, különösen amennyiben a biztonsági szempontokat nem megfelelően kezelik. Az IoT-eszközök értékelésekor különösen fontos azonosítani azokat a jellemzőket,

²⁸ Készült a CoPilot segítségével.

amelyek a legmagasabb kockázati szintre utalnak. A következőkben bemutatom azokat a szempontokat, amelyek alapján egy IoT-eszköz a „legkockázatosabbnak” tekinthető. Ezek alapján egy keretrendszert is fel lehet állítani.

Az IoT-eszköz funkciója és kritikus szerepe

Az első és legfontosabb szempont az eszköz funkciója. Az olyan IoT-eszközök, amelyek közvetlenül befolyásolják az emberi élet védelmét vagy a kritikus infrastruktúrák működését, eleve magasabb kockázati kategóriába esnek. Ide tartoznak például az orvosi implantátumok (például pacemaker, inzulinpumpák), ipari vezérlőrendszerek (ICS, SCADA komponensek), elektromos hálózati eszközök vagy közlekedésirányító rendszerek. Az ilyen eszközök meghibásodása vagy kompromittálása súlyos fizikai károkat, emberéletek elvesztését vagy tömeges szolgáltatáskieséseket okozhat. Minél kritikusabb a funkció, annál inkább indokolt a „*nagyon magas kockázatú*” besorolás.

Hozzáférhető adatok érzékenysége

Az IoT-eszközök gyakran adatokat gyűjtenek, tárolnak és továbbítanak. Az adatérzékenység mértéke szintén meghatározó tényező a kockázati besorolásban. Ha az eszköz például egészségügyi adatokat, biometrikus információkat, pénzügyi tranzakciós adatokat vagy akár pontos tartózkodási helyet kezel, akkor az adatvédelmi incidensek következményei súlyosak lehetnek. A GDPR és más adatvédelmi rendeletek is kiemelten kezelik az ilyen típusú adatok védelmét. Egy okosotthon-kamera vagy egy egészségügyi megfigyelőrendszer kompromittálása nem csupán magánéleti jogsértést, hanem zsarolóvírus-támadások vagy célzott fizikai támadások alapját is képezheti.

Sebezhetőségi szint és technikai biztonság

A technikai biztonsági jellemzők alapvetően befolyásolják egy IoT-eszköz kockázati profilját. A nem megfelelő biztonsági gyakorlatok – mint a kéménykódolt alapértelmezett jelszavak, titkosítatlan adatátvitel vagy a sérülékeny firmware-ek – hatalmas támadási felületet nyitnak. Különösen veszélyesek azok az eszközök, amelyek nem támogatják a rendszeres és automatikus biztonsági frissítéseket, így a felfedezett sérülékenységeik hosszú távon kihasználhatóak maradnak. Emellett a gyenge hitelesítési mechanizmusok és a hiányzó biztonsági naplózás is súlyosbítja a helyzetet. A Common Vulnerabilities and Exposures (CVE) adatbázisban való megjelenés vagy gyakori sérülékenységi jelentések szintén erős indikátorai lehetnek a magas kockázatnak.

Hálózati kitettség

Az IoT-eszközök hálózati architektúrában betöltött szerepe, illetve az internetre való közvetlen kitettségük szintén kulcstényező. Egy olyan eszköz, amely nyitott portokon keresztül elérhető az internetről, sokkal nagyobb támadási felületet jelent, mint egy szigorúan belső hálózatra korlátozott rendszer. A portszkennelési eredmények, a nyilvános IP-címmel való rendelkezés vagy a nem megfelelő tűzfalbeállítások mind hozzájárulnak a kockázati szint emelkedéséhez. Az olyan protokollok, mint az MQTT, CoAP vagy a nyílt Bluetooth-kapcsolatok, különös figyelmet igényelnek.

Frissíthetőség és életciklus-kezelés

Egy eszköz biztonságának fenntartása szinte lehetetlen megfelelő életciklus-kezelés és frissítési mechanizmus nélkül. Az elavult, nem frissíthető firmware-rel rendelkező IoT-eszközök évekig sebezhetőek maradhatnak a feltárt hibákkal szemben. Ha az eszköz gyártója nem biztosít frissítéseket, vagy megszűnik az eszköz támogatása, az komoly hosszú távú fenyegetést

jelent. A „beágyazott” IoT-megoldások, mint a mezőgazdasági szenzorok vagy az olcsó fogyasztói termékek, gyakran ilyen helyzetbe kerülnek.

A gyártó megbízhatósága

Nem elhanyagolható tényező a gyártó és a beszállítói lánc megbízhatósága sem. Ismeretlen, nem tanúsított vagy korábban adatvédelmi vagy biztonsági botrányokba keveredett gyártók termékei nagyobb kockázatot jelentenek. Emellett figyelmeztető jel, ha a gyártó nem ad részletes tájékoztatást az eszköz biztonsági funkcióiról, nem rendelkezik tanúsítványokkal (pl. ISO/IEC 27001, UL 2900), vagy nem hajlandó biztonsági auditokat végezni.

A végső kockázati besorolás az egyes pontszámok összegéből adódhat:

- 6–12 pont: Alacsony kockázat
- 13–20 pont: Közepes kockázat
- 21–30 pont: Nagyon magas kockázat

A kockázati besorolások az IoT-eszközök beszerzése előtt vagy a beszerzés során már támpontot adhatnak arra, hogy a vállalat, szervezet számára, az általuk kezelt, tárolt adatok, információk érzékenysége, valamint további szempontokra tekintettel milyen jellegű eszközök beszerzése és milyen forrásból lehet támogatott, illetve engedélyezett.

Az IoT-eszközök használata a közszolgálatban

Az IoT forradalmasította a mindennapokat, így a közszolgálati szektor működését is²⁹. Intelligens városi rendszerek, közlekedésirányító eszközök, egészségügyi szenzorok, okosirodai megoldások, közbiztonsági kamera-rendszerek – ezek mind az IoT-technológia alkalmazására épülnek. Bár ezek az eszközök hatékonyságot, átláthatóságot és kényelmet ígérnek,

²⁹ The Internet of Things: A survey. 2020.

használatuk számos kockázatot hordoz magában a mindennapi szolgáltatásokban.

Az IoT-eszközök közszolgáltatásban történő alkalmazása nem csupán technológiai újítás, hanem a modern városok működésének alapvető újraértelmezését is jelenti, aminek a segítségével a valós idejű adatgyűjtés és automatizált rendszerek hatékonyabbá, fenntarthatóbbá és felhasználó-barátabbá tehetik a közszolgáltatásokat. A jövő városai azok lehetnek, amelyek képesek lesznek ezeket a technológiákat biztonságosan, adatvédelmi szempontból átlátható módon és társadalmilag elfogadhatóan alkalmazni.

Először mindenképp a használatuk előnyeit emelném ki. Az állampolgárok biztonsága és kényelme szempontjából lehet ezeket az eszközöket alkalmazni (pl. okoszebra). A közszolgálati (közigazgatási) szféra – beleértve az önkormányzatokat, közlekedési hálózatokat, egészségügyi szolgáltatásokat, közbiztonságot és környezetvédelmet – mind profitálhat az intelligens eszközök és rendszerek alkalmazásából, fokozva a munkavégzésük hatékonyságát. Az IoT-megoldások nem csupán az erőforrások hatékonyabb felhasználását segítik elő, hanem hozzájárulnak a gyorsabb döntéshozatalhoz, a költségek csökkentéséhez és az állampolgári elégedettség növeléséhez is.

A közlekedési rendszerek és intelligens forgalomirányítás az egyik gyakori alkalmazási terület a (városi) közlekedésben. Az IoT-eszközök révén forgalomfigyelő kamerák, szenzorok és GPS alapú rendszerek segítségével valós idejű adatokat lehet gyűjteni az úthasználatról, torlódásokról, parkolási szokásokról. Ezek az adatok lehetővé teszik a dinamikus forgalomirányítást, az útvonalak optimalizálását és a közlekedési lámpák intelligens vezérlését.

Például Barcelonában az „*Urban Mobility Plan*” keretében IoT alapú parkolóérzékelőket telepítettek, amelyek jelzik, hogy egy parkolóhely szabad vagy foglalt, és az adatokat valós időben továbbítják egy mobilalkalmazáson keresztül az autósoknak. Ezzel csökkent a keresgéeléssel eltöltött idő és a forgalom is, valamint a légszennyezés mértéke.

Az okosvárosok (smart cities) koncepciójának egyik alapköve az IoT-eszközök széleskörű alkalmazása³⁰. A közlekedési lámpákba, parkolóhelyekre, tömegközlekedési eszközökbe telepített szenzorok képesek optimalizálni a forgalomirányítást, csökkenteni a torlódásokat és a károsanyag-kibocsátást. A parkolóhely-érzékelők például valós idejű információkat közölnek a szabad helyekről, amely az autósokat közvetlenül az elérhető parkolókhoz irányítja.

Az energiamenedzsment területén az intelligens villanyoszlopok, okos mérőórák és automatizált hálózati rendszerek lehetővé teszik a közintézmények számára az energiafelhasználás pontos monitorozását és optimalizálását³¹. Az okos mérőórák adatai révén a közüzemi szolgáltatók gyorsan azonosíthatják a rendszerhibákat és a túlterhelt hálózati szakaszokat.

A közüzemi vízszolgáltatók számára az IoT-eszközök lehetővé teszik a hálózati veszteségek (pl. csőtörések, szivárgások) gyors észlelését, valamint a fogyasztási szokások részletes nyomon követését. Az intelligens vízórák folyamatos adatokat küldenek a szolgáltatóknak, így pontosabb számlázás és gyorsabb hibafelismerés valósulhat meg. Az angliai Thames Water vállalat intelligens szenzorhálózatot alkalmaz, amely valós időben észleli a nyomáscsökkenést és a szivárgást, így megelőzhető a súlyosabb károk kialakulása. Emellett a lakosság is hozzáfér az adatokhoz, így az emberek tudatosabban kezelhetik a vízfogyasztásukat.

Az egészségügyben az IoT-eszközök hozzájárulnak a betegellátás minőségének javításához. A távoli betegmonitorozó rendszerek, az okos karkötők és a hordható egészségügyi eszközök lehetővé teszik a páciensek állapotának folyamatos figyelemmel kísérését³². Az adatok valós idejű továbbítása az egészségügyi szolgáltatók felé gyorsabb diagnózist és hatékonyabb kezelést eredményezhet. Az egészségügy az IoT-technológia egyik legérzékenyebb és egyben legdinamikusabban fejlődő alkalmazási területe.

³⁰ Kitchen R.: Making sense of smart cities: Addressing present shortcomings (Cambridge Journal of Regions Economy and Society 2014/1. szám. 131-136. o.

³¹ OECD, 2021

³² World Economic Forum, 2018.

Az IoT-eszközök lehetővé teszik az egészségügyi szolgáltatások hatékonyságának javítását, a betegbiztonság növelését, valamint a megelőző és személyre szabott orvoslás fejlesztését is. Az egyik legismertebb alkalmazás a távoli betegmonitorozás. Intelligens eszközök – például okos vérnyomásmérők, pulzus- és EKG-érzékelők, vércukorszint-figyelők – képesek folyamatosan adatokat továbbítani a kezelőorvoshoz vagy a kórházi rendszerhez. Ez különösen fontos krónikus betegek (pl. szívbetegek, cukorbeteg) esetében, ahol a rendszeres kontroll életmentő lehet. Például a finnországi Espoo városában az önkormányzat által működtetett idősgondozási rendszerbe integráltak olyan karpereceket, amelyek figyelik az idősök napi aktivitását, testhőmérsékletét és alvásminőségét. Ezen adatok alapján az egészségügyi dolgozók előre jelezhetik az állapotromlást, és idejében beavatkozhatnak.

Az IoT megoldások a kórházak működésében is kulcsszerepet játszanak. Például az eszközök és gyógyszerek nyomon követésére RFID alapú rendszert használnak, amely segít megelőzni a hiányt vagy téves kiadást. Emellett a kórházi ágyak intelligens szenzorai figyelik a beteg mozgását, így csökkenthető a felfekvéses sérülések száma.

Egy másik fontos terület a járványkezelés és kontaktkutatás. Az IoT-eszközök – például okostelefonok, viselhető érzékelők – segítségével valós időben nyomon követhető a fertőzött személyek mozgása, és gyorsabban azonosíthatók azok, akik potenciálisan kapcsolatba kerültek velük. Az ilyen rendszerek alkalmazását a COVID-19 világjárvány idején számos ország bevezette, különféle adatvédelmi megoldásokkal együtt.

Az egészségügyi környezetek biztonságának növelése is fontos szerepet kap: az IoT-rendszerek képesek monitorozni a hőmérsékletet, páratartalmat és levegőminőséget a műtőkben, steril szobákban, gyógyszertárakban, ezzel hozzájárulva a fertőzések megelőzéséhez.

Ugyanakkor a mentőszolgálatok is profitálhatnak az IoT-ből. A mentőautók felszerelhetők olyan eszközökkel, amelyek előzetes információkat küldenek a fogadó kórháznak a beteg állapotáról, így az ellátás már az érkezés előtt előkészíthető.

Az egészségügyben történő IoT-alkalmazás egyik legnagyobb kihívása azonban az adatbiztonság és adatvédelem kérdése. Az érzékeny egészségügyi adatok védelme szigorú szabályozást és megbízható kiberbiztonsági rendszert igényel, különösen akkor, ha távoli kommunikációról vagy felhő alapú adattárolásról van szó.

Összességében az IoT-eszközök az egészségügyben nemcsak a szolgáltatások hatékonyságát növelik, hanem hozzájárulnak az emberéletek megóvásához is, különösen az idős, krónikus betegek vagy hátrányos helyzetű csoportok esetében.

A közbiztonság területén is egyre elterjedtebbek az IoT-megoldások. Az okos kamerarendszerek, mozgásérzékelők és környezeti szenzorok révén a rendészeti szervek valós idejű információkhoz juthatnak³³. A környezet-monitorozó rendszerek például képesek érzékelni a levegő minőségének romlását, a veszélyes vegyi anyagok jelenlétét vagy a zajszenyezést.

Az IoT-eszközök a környezetvédelemben is jelentős szerepet játszanak. Az időjárás-figyelő állomások, vízszintmérők és légszennyezettség-mérő szenzorok segítenek a katasztrófavédelmi intézkedések előkészítésében³⁴. Egy árvízi veszély esetén például a vízszintérzékelők automatikusan riasztást küldhetnek a közszolgálati szerveknek.

Az oktatás területén az IoT-eszközök lehetővé teszik az intelligens tantermi környezetek kialakítását. A tantermekbe telepített okoseszközök segítenek a környezeti feltételek optimalizálásában, és támogatják a személyre szabott tanulási élményt³⁵.

³³ A BIZOTTSÁG JELENTÉSE A TANÁCSNAK, AZ EURÓPAI PARLAMENTNEK ÉS AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK Jelentés a mesterséges intelligencia, a dolgok internete és a robotika biztonsági és felelősségi vonatkozásairól

Forrás: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0064>
Letöltés ideje: 2025.06.03.

³⁴ ITU, 2022.

³⁵ World Economic Forum, 2018.

Az IoT rendszerek alkalmazása ugyanakkor komoly kihívásokat is támaszt. Az eszközök nagy száma és az általuk gyűjtött adatok fokozott információbiztonsági kockázatot jelentenek az OECD 2021-es jelentése szerint³⁶. Az adatlopás, az eszközök feltörése vagy az adatok manipulációja súlyos következményekkel járhat.

Az interoperabilitás, azaz a különböző eszközök és rendszerek zökkenőmentes együttműködése is jelentős kihívás (ISO/IEC, 2023). A közszolgálati intézményeknek gyakran többféle gyártótól származó eszközöket kell egy rendszerbe integrálniuk, amely jogi és technikai kérdéseket is felvet.

Etikai szempontból is kiemelkedő az átláthatóság és az adatvédelem biztosítása. A közszolgáltatóknak részletesen tájékoztatniuk kell a lakosságot arról, hogy milyen adatokat gyűjtenek, hogyan használják fel, és meddig őrzik meg azokat³⁷.

A fenntarthatósági szempontok szintén fontosak. Bár az IoT-rendszerek energiahatékonyabb működést ígérnek, maguknak az eszközöknek a gyártása és cseréje környezeti terheket jelenthet a World Economic Forum 2018-as megállapítása szerint.

A jövőben a mesterséges intelligenciával kombinált IoT-rendszerek képesek lesznek nemcsak adatokat gyűjteni, hanem azokat automatikusan elemezni és döntéseket is hozni³⁸. Ehhez azonban elengedhetetlen a megfelelő jogszabályi háttér megalkotása és az állampolgári jogok védelme.

³⁶ OECD Measuring of Internet of Things.

Forrás: https://www.oecd.org/en/publications/measuring-the-internet-of-things_021333b7-en.html

Letöltés ideje: 2025.06.03.

³⁷ NAIH, 2022.

³⁸ OECD, 2021.

Az IoT-technológia sajátosságai a közszolgálatban

Az IoT-eszközök alapvető jellemzői közé tartozik a folyamatos hálózati kapcsolódás, az adatok gyűjtése, továbbítása és elemzése. A közszolgálatban különösen fontos területek közül álljon itt néhány:

- közlekedésirányítás (intelligens jelzőlámpák, forgalomszámláló szenzorok),
- közbiztonság (okos térfigyelő kamerák, drónok),
- egészségügy (távfelügyeleti egészségügyi eszközök),
- közüzemek (okosmérők, vízminőség-figyelő rendszerek),
- irodai környezet (okostermosztátok, RFID alapú beléptető rendszerek).

A közszolgálati szférákat érő veszélyek és kihívások azért is bírnak kiemelt jelentőséggel, mert ezek elkerülése az állampolgárok számára szinte lehetetlen. Az IoT-eszközök alkalmazásának veszélyei ugyanakkor nemcsak adatvédelmi, hanem nemzetbiztonsági problémákat is eredményezhetnek, ami érintheti magát a szolgáltatás nyújtóját, a szolgáltatásokat igénybe vevő felhasználókat és az esetleges partnereket is.

Az IoT-eszközök nemcsak az adatbiztonságot veszélyeztethetik, hanem közvetlenül is fenyegethetik a fizikai világot.

Kockázatok és kihívások az IoT közszolgálati alkalmazásában

Az IoT-eszközök közszolgáltatásokban történő alkalmazása számos innovatív lehetőséget kínál, ugyanakkor jelentős kockázatokkal is jár, különösen a biztonság, az adatvédelem és az üzemeltetési megbízhatóság terén. Ezen kockázatok megfelelő kezelése nélkül az előnyök gyorsan hátrányokká válhatnak, különösen kritikus közszolgáltatások esetében, mint például az egészségügy, a közlekedés vagy a közbiztonság.

Kiberbiztonsági kockázatok

Az IoT-eszközök egyik legnagyobb gyengesége a kiberbiztonság. Mivel sok eszköz gyenge titkosítással, alapértelmezett jelszavakkal vagy elavult firmware-rel működik, könnyen válhatnak hackertámadások célpontjává. Ezek a támadások zavarokat okozhatnak a közszolgáltatások működésében (például közlekedési lámpák meghackelése), adatlopáshoz vezethetnek, vagy zsarolóvírusokon keresztül megbéníthatják az egész rendszert. A biztonsági frissítések elmaradása vagy késedelme csak súlyosbítja ezeket a kockázatokat.

Adatvédelmi és jogi kihívások

A közszolgáltatásokban alkalmazott IoT-eszközök gyakran személyes adatokat is gyűjtenek, például mozgásmintákat, biometrikus adatokat vagy egészségügyi információkat. Ezen adatok kezelése során kiemelten fontos a GDPR és más adatvédelmi szabályozások betartása. A nem kellően átlátható adatkezelés, a felhasználói hozzájárulás hiánya vagy az adatgyűjtés céljának tisztázatlansága súlyos jogi és etikai problémákhoz vezethet. Különösen érzékeny terület az egészségügyi adatok kezelése, ahol az adatvédelmi incidens akár emberéletekbe is kerülhet.

Üzemeltetési és technológiai kockázatok

A közszolgáltatásokban alkalmazott IoT-eszközök komplex ökoszisztémában működnek, ahol számos eszköz és rendszer összehangolt működésére van szükség. Az interoperabilitás hiánya, az elavuló eszközök vagy a rosszul tervezett hálózati infrastruktúra működési zavarokat, kimaradásokat okozhat. Ezen kívül a rendszerek karbantartása, felügyelete és frissítése jelentős humán és anyagi erőforrást igényel, amelyet sok önkormányzat vagy állami intézmény nem tud biztosítani.

Gazdasági és fenntarthatósági kockázatok

Az IoT-rendszerek kiépítése és fenntartása jelentős beruházást igényel. Ha a beruházásokat nem előzi meg megalapozott költség-haszon elemzés, könnyen előfordulhat, hogy az eszközök gyorsan elavulnak, vagy nem hoznak megfelelő társadalmi hasznot. Emellett a közszolgáltatók kiszolgáltatottá válhatnak bizonyos technológiai beszállítóknak, ami hosszú távon függőséget és gazdasági kockázatot jelent.

Társadalmi és etikai aggályok

A közszolgáltatásokban alkalmazott intelligens megfigyelőrendszerek (pl. kamerák, viselhető eszközök) erősíthetik a lakosságban a megfigyeltség érzetét. Ez bizalomvesztéshez vezethet az állami szervek irányába, különösen, ha a rendszerek működése nem transzparens. Emellett fennáll a digitális kirekesztés veszélye is: az IoT-rendszerek hatékony használatához szükséges digitális kompetenciák vagy eszközök nem állnak minden társadalmi csoport rendelkezésére, ami tovább növelheti a szociális különbségeket.

Az IoT-eszközök közszolgáltatásokban történő alkalmazása során nemcsak a technológiai lehetőségeket, hanem a potenciális kockázatokat is figyelembe kell venni. A siker kulcsa az átfogó kockázatelemzés, az adatvédelmi megfelelés biztosítása, valamint a bizalomépítés a társadalommal. Enélkül a technológia nem erősíti, hanem gyengítheti a közszolgáltatások hitelességét és hatékonyságát.

Az ellátási lánc sérülékenységei

A közszolgálat gyakran közbeszerzési eljárásokkal szerez be eszközöket, ahol az olcsóbb, de kevésbé biztonságos megoldások is előfordulhatnak:

- rosszul dokumentált firmware,
- hátsó kapuk (backdoorok) a gyártói oldalon,
- alacsony szintű frissítési támogatás.

A kompromittált eszközök telepítése már a kezdetektől alááshatja a rendszer biztonságát.

Az IoT-eszközök alkalmazása számos veszélyt rejt magában, éppen azért, mert biztonságuk még nincs kellőképpen megoldva. A technikai biztonság mellett azonban az emberi tényezővel is számolni kell, mivel azok nem tudatos használata, a frissítés hiánya vagy az eszközök nem megfelelő védelme magában hordozza a kockázatokat, akár munka során, akár a magánéletben.

Az IoT-eszközök elterjedése életünk számos területét alakítja át, beleértve az otthoni környezeteket is. Az okos hangszórók, intelligens biztonsági kamerák, okoszárak és egyéb önálló kommunikációra képes eszközök olyan új fenyegetéseket és kihívásokat teremtenek, amelyek közvetlen hatással vannak a rendőrség bünygyi tevékenységére, különösen a (ház)kutatás és a lefoglalás során.

A rendőr(ség) és az IoT-eszközök

A rendőrség feladatainak ellátása során természetesen ugyanúgy jelen vannak az IoT-eszközök (erre utaltam az előző fejezetben is), hiszen használatuk akár személyes használatra, akár a szakemberek munkájának megkönnyítésére is szolgálhat. Ezen eszközök védelem nélküli használata ugyanolyan kockázatot jelent, mint az egyébként sokszor az egymás közötti információmegosztásra használt kommunikációs alkalmazások (Viber, WhatsApp stb.), amelyekkel szemben kiberbiztonsági és adatvédelmi kérdések is felmerülnek.

Az IoT-eszközök előnyei a rendőrség számára

Először arra kerestem a választ, hogy segítheti-e a rendőrség munkáját az elérhető IoT-eszközök alkalmazása. A válasz egyértelműen igen (most nem a veszélyeire koncentrálna), hiszen ahogy a gyártók is arra törekednek, hogy segítségükkel a felhasználóknak a tevékenységeiket megkönnyítsék,

úgy a rendőrség állományának is jelenthet egyes esetben segítséget ezeknek az eszközöknek a használata. Amennyiben a nyomozások vagy rendőrségi vizsgálatok során történő felhasználásokat nézzük, akkor a bizonyítékok rögzítése, azok helyének detektálása, azok mérete vagy a helye egy területen, az eszközökön lévő vagy más eszközre továbbított adatok hozzájárulhatnak a bizonyítékok gyűjtéséhez, azonosításához. Ahhoz is segítséget nyújthat egy-egy ilyen eszköz, hogy vészhelyzetben a szakemberek a lehető legrövidebb idő alatt eljussanak a megfelelő helyre.

A bűnüldözés a bizonyítékok beszerzése céljából az online csalástól az emberölésig évtizedek óta keresi az internetszolgáltatókat és a hagyományos távközlési cégeket azért, hogy akár az elkövetők, akár a sértettek utolsó online tevékenységét (digital footprint – digitális lábnyomok) megismerjék, hiszen azok a nyomozások során alátámasztják vagy épp megdöntik a vallomások valóságát vagy az időbeli történések megismerését. Ezeken felül a bűnüldöző szervek egyre gyakrabban keresik a hagyományos elektronikus adatforrásokon túl az ügy megoldásának vagy könnyebb realizálásának kreatívabb módjait. Ezeknek egyszerűbb megtalálási eszközei az okoseszközökben vagy azok által rögzített adatok, hiszen sokszor nem kell forenzikus szakértőnek lenni ahhoz, hogy az adatokat megismerjék és felhasználják (értelemszerűen az eljárásjogi jogszabályok szigorú betartása mellett, hiszen a kutatás szigorú szabályai nemcsak a magánlakásra vagy bekerített helyre terjednek ki, hanem az informatikai eszközökre, így az IoT-eszközökre is, még akkor is, ha azok megismeréséhez nem kell szakértőnek lenni).

Az IoT-eszközök használata nemcsak a valós idejű adatok ellenőrzését teszi lehetővé, például az otthoni termosztát kontrollját távoli hozzáféréssel, hanem rövidebb-hosszabb távon adatok gyűjtését és rögzítését, elemzését is. Ezek az eszköz által végzett elemzések elérhetők sokszor magukon az eszközökön vagy pedig a felhőben tárolva.

A következőkben a leghasznosabb és talán legfontosabb eszközöket vagy lehetőségeket gyűjtöttem össze, amelyeknek a magyar rendőrségnél

történő bevezetése jogszabályi változtatás vagy minimális változtatás mellett lenne lehetséges.

1. Az eszközök nyomon követése egyrészt létező dolog (a járőrök mozgását lehetőség van a központból figyelni), amit egyébként is kiválóan lehet használni az olyan ellenőrzésekre, mint az esetleges rendőri túlkapások (korrupció), pihenőidő saját szakállra történő kivétele vagy egyéb a rendőrségi szolgálattal összefüggésbe hozható, de azzal össze nem férő tevékenység. Ha a rendőrség tulajdonában vannak még IoT-eszközök, akkor azok (akár távoli) nyomon követésére és kezelésére is használhatók. De lehetséges lenne civil járművek, rendszeresített fegyverek és berendezések ellopásának, elvesztésének vagy az azokkal kapcsolatos visszaéléseknek a megelőzése is³⁹.
2. Bűncselekmények felderítése során szintén kiválóan felhasználhatóak az IoT-eszközök a bűncselekmények felderítésére és megelőzésére, a különböző forrásokból származó adatok nyomon követésére és elemzésére, mint például forgalmi minták, közösségi média és nyilvános érzékelők.
3. Vészhelyzeti reagálás: Az IoT-eszközök felhasználhatóak a vészhelyzeti reagálás javítására és irányítására azáltal, hogy valós idejű információkat nyújtanak a természeti katasztrófákról, balesetekről és egyéb kritikus eseményekről.
4. Viselhető eszközök: Az IoT-eszközök, például a hordható technológia, figyelemmel kísérik a bűnüldöző szervek szakembereinek egészségét és biztonságát, és vészhelyzet esetén riasztást adnak. Így intézkedés során nem lenne szükséges manuálisan riasztást kiadni veszélyhelyzetben, hanem a viselhető eszközök a lehetséges vagy valós veszélyről a megfelelő szervezetet tájékoztatnák.

³⁹ Nem tartozik ide, amikor a gépjárművet csaliként helyezik ki, hiszen ahhoz szükséges a bírói engedély.

5. A rendőrségi IoT-eszközök használata segíti a bűnüldözést a bűnözők azonosításában és tartózkodási helyük nyomon követésében is. Jelenleg Magyarországon vannak erre olyan alkalmazások, amelyek a kiadott okoseszközökre telepíthetők. Ezeken az alkalmazásokon keresztül a városi biztonsági rendszerek és riasztók valós idejű bűnügyi információkat nyújtanak a rendőrség számára, míg az interneten keresztül elérhető nyilvántartások lehetővé teszik a szakembereknek, hogy gyorsan gyűjtsenek releváns információkat.
6. Az IoT-lőfegyverek intelligens fegyverek, amelyek biometrikus adatokat használnak a felhasználónak a lőfegyver üzemeltetésére vonatkozó engedélyéről. Ezek a tűzfegyverek rögzítik a lövések pontos helyét és egyéb eseményeket. Ezenkívül az IoT-technológia lehetővé teszi az automatikus testkamerák aktiválását.

Az IoT-eszközök veszélyei a nyomozások, felderítések során

Az otthoni IoT-eszközök a környezetről információt gyűjtenek, kommunikálnak és automatizálást végeznek. Ezek az előnyök ugyanakkor veszélyeztethetik egy-egy nyomozás vagy felderítés sikerét.

Bűnügyi szempontból olyan veszélyek merülnek fel, mint egy-egy rendvédelmi vagy nemzetbiztonsági művelet és az azt végző személy valós idejű megfigyelése. Így például a helyszínre belépő rendőröket intelligens kamerarendszerek, riasztók és szenzorok automatikusan rögzíthetik, és távoli szerverekre továbbíthatják a felvételeket, így akár dekonspirálva a műveletet. Ugyanúgy problémát jelenthetnek a ma egyre népszerűbb Tesla gépjárművek, amelyek automatikus rögzítőkamerákkal vannak ellátva⁴⁰. Így egy utcán vagy garázsban történő rendőri jelenlétet rögzíthetnek, illetve valós időben információt és képet továbbíthatnak a gépjármű tulajdonosának. Ezzel nemcsak a gépjárművet feltörő személyt vagy a rongálás tényét

⁴⁰ Forrás: https://www.tesla.com/hu_hu/support/vehicle-safety-security-features
Forrás: 2026.08.08.

lehet rögzíteni vagy látni, hanem olyan információkat is, amelyeket fedésben kellene tartani. Az egyik legnagyobb kockázat tehát nemcsak a rendőrség állományába tartozó személyek személyiségi jogainak védelme, hanem egyes műveletek, eljárások megghiúsulása, vagy az eljárási cselekmény megfigyelése, a digitális bizonyítékok, nyomok manipulálása is.

Az adatvesztés és manipuláció is kockázataként és kihívásaként jelenhet meg, hiszen a (ház)kutatás vagy akár más kényszerintézkedés során a gyanúsított vagy társai (esetleg hozzátartozók) távolról törölhetik az eszközök által tárolt adatokat, de a helyszíni bizonyítékok (például időbélyegek, hangrögzítések) is megváltoztathatók vagy megghamisíthatók.

Adatvédelemmel összefüggő kihívás, hogy az IoT-eszközök adatokat gyűjtenek az emberek mozgásáról és tevékenységéről, és ezek az adatok felhasználhatók az emberek magánéletének megsértésére. Fontos biztosítani a magánélet védelmét, amikor IoT-eszközöket használnak a bűnüldözéshez.

És nem mellesleg az eszközök költsége is fontos, hiszen ezek az eszközök drágák lehetnek, és nehéz lehet finanszírozást szerezni a vásárlásukhoz és a használatukhoz.

(Ház)kutatás IoT-környezetben: technikai és jogi kihívások

A magyar bűnvádi eljárási törvény (Be., 2017. évi XC. törvény) szabályozza a (ház)kutatást és a lefoglalást. Azonban az IoT-eszközök sajátosságai miatt

- az eszközök folyamatosan online állapotban vannak, így adatmozgás történhet a házkutatás alatt is;
- a helyszínre érkezéskor az eszközt gyorsan azonosítani kell az adatáramlás megállítása érdekében;
- szükséges lehet azonnali hálózatmegszakítás vagy áramtalanítás.

Kollár Csaba tanulmányában említi a támadások passzív és aktív formáját.⁴¹ Bár nem kifejezetten a nyomozások és a rendőrség munkájának akadályait gyűjti össze, de ugyanazokkal a nehézségekkel szembesít. A passzív támadások közé sorolhatjuk a következőket:

- A lehallgatás, amikor a támadó elfogja a szenzorok által rögzített és továbbított adatokat, ennek alapján saját vagy megbízója elvárásai szerint tudja magukat az adatokat elemezni.
- A forgalomelemzés során a támadó elemezni tudja a hálózaton folyó adatmennyiség változását, így meg tudja határozni a bázisállomások helyét, illetve a használt protokollokat is.
- Az üzenetfecskenyezés (vagyis message injection) során a támadó hamis adatokat juttat a hálózatba, szofisztikáltabb támadás esetén az ellenőrző információkat módosítja.⁴²

A gyenge hitelesítési eljárások és a titkosítás hiánya a rendészeti, nyomozati és bünygyi adatkezelés szempontjából különösen kritikus problémát jelent. Az IoT-eszközök ugyanis a rendőrségi infrastruktúrákban, például testkamerákban, helymeghatározó egységekben, drónokban vagy okos járműrendszerekben érzékeny műveleti és személyes adatokat rögzítenek. Amennyiben egy ilyen eszköz kompromittálódik, a támadók hozzáférhetnek nyomozati dokumentumokhoz, bizonyítékokhoz, tanúk vagy gyanúsítottak azonosító adataihoz, illetve bevetési egységek valós idejű mozgásához.⁴³ Egy ilyen adatvesztés vagy illetéktelen hozzáférés nemcsak az adott bünygytőeljárás integritását veszélyezteteti, hanem szélesebb körű rendészeti hálózatok bizalmasságát és működési biztonságát is alááshatja.

Az ilyen típusú kockázatok különösen aggasztóak abban az esetben, ha az eszközök hálózatba kötött környezetben működnek, ahol a támadók

⁴¹ Kollár Csaba: oT a gyakorlatban, az információbiztonság fókuszában I. Bolyai Szemle 2017/1. szám. 50. o.

⁴² Kollár Csaba: i.m. 50. o.

⁴³ Servida, Francesco; Casey, Eoghan: IoT forensic challenges and opportunities for digital traces. Digital Investigation. 2019.

egyetlen gyenge pont kihasználásával oldalirányú (lateral) mozgást valósíthatnak meg, így akár teljes nyomozati rendszerek felett szerezhethetnek kontrollt.⁴⁴ Ez a jelenség jól illusztrálja az OWASP IoT Top 10 által azonosított első két kategóriát: „*Weak, Guessable, or Hardcoded Passwords*” (I1.) és „*Insecure Network Services*” (I2.), amelyek évek óta a legfőbb támadási vektorok közé tartoznak⁴⁵.

A fenyegetés azonban nem kizárólag kiberbűnözői oldalról értelmezhető. Az IoT-eszközök idegen államok vagy hírszerző szervezetek számára is potenciális megfigyelési csatornákat biztosíthatnak. Egy, a rendőrség által használt testkamera, okostelefon vagy drón kommunikációjának lehallgatása lehetővé teheti valós idejű bevetések nyomon követését vagy a taktikai információk megszerzését. Amennyiben az adatátvitel nincs végpontok közötti titkosítással (end-to-end encryption) védve, a támadók vagy hírszerző aktorok képesek lehetnek valós idejű megfigyelésre, ami nemzetbiztonsági kockázatot is felvet⁴⁶.

Ezen körülmények között az adatbiztonsági kockázatok nem pusztán technikai problémát jelentenek, hanem rendszerszintű, stratégiai fenyegetést a rendészeti műveletek és az igazságszolgáltatás integritása szempontjából. Az információbiztonsági incidensek súlyos következményei a műveleti biztonságon túl az állampolgárok bizalmát is megrendíthetik a hatóságok adatkezelési gyakorlatában⁴⁷. Ezért az IoT-eszközök rendészeti alkalmazása során a biztonságos fejlesztési életciklus (Secure Development Lifecycle), a többretegű hitelesítés (Multi-Factor Authentication), valamint az adatok kriptográfiai védelme elengedhetetlen a működési biztonság és az adatvédelmi megfelelés fenntartásához.

⁴⁴ Nozomi Networks Conference. 2025.

⁴⁵ OWASP: IoT Top 10 Project. Open Web Application Security Project, 2023.

⁴⁶ Melissa Hathaway and Alexander Klimburg, "Preliminary Considerations: On National Cyber Security" In *National Cyber Security Framework Manual* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2012), p. 8.

⁴⁷ Kosta, Eleni: The Right to an Effective Remedy in International Data Transfers of Electronic Evidence: Past Lessons and Future Outlook.

A biztonsági hiányosságok fennmaradása egyértelműen mutatja, hogy az IoT-eszközök gyártói és üzemeltetői szintjén továbbra sem valósul meg a „security by design” és a „privacy by design” elv, amelyet az Európai Unió Általános Adatvédelmi Rendelete (GDPR, 2016/679/EU) kötelező alapelvként rögzít. Az e követelmények figyelmen kívül hagyásával gyártott vagy üzemeltetett eszközök nem csupán technológiai, hanem jogállami kockázatokat is hordoznak, mivel sérthetik az adatbiztonságra, adatkezelésre és nemzetbiztonságra vonatkozó jogszabályokat.

Az IoT-eszközök és a kényszerintézkedések a nyomozások során (a lefoglalás, kutatás és bizonyítékgyűjtés problematikája)

Az az előző fejezetekből is egyértelműen látszik, hogy a digitális bizonyítékok és a hagyományos bizonyítékok lefoglalása, az eszközök kutatása tekintetében nem tehető konceptuális különbség, hiszen a bűncselekmény nyomait hordozó „tárgyak”, IoT-eszközök gyakran felhőszolgáltatásban tárolják az adatokat, nem kizárólag helyi tárolón. A Be. 313. § értelmében a digitális adatok lefoglalása közvetlen vagy közvetett módon történhet: a Be. információs rendszer titkos megfigyelése esetén az információs rendszer; titkos kutatás esetén a helyiség, jármű vagy tárgy; hely titkos megfigyelése esetén a helyiség vagy jármű; küldemény titkos megismerése esetén a feladás vagy az átvétel helye, illetve a feladó vagy a címzett; lehallgatás esetén az elektronikus hírközlési szolgáltatás vagy az eszköz, illetve az információs rendszer egyértelmű azonosítására szolgáló adatokat. A büntetőeljárásról szóló 2017. évi XC törvény elektronikus adatra vonatkozó szabályozása nem tesz különbséget az eszköz jellege között, az eszközök tekintetében nem tesz különbséget az adott eszköz és a rajta lévő adat között. „elektronikus adat a tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.”⁴⁸

⁴⁸ Be. 205.§

Vagyis egy „buta” (internet nélküli) telefonban tárolt telefonszám is elektronikus adatnak minősül, ugyanakkor annak, az ahhoz történő hozzáférés mind eljárásjogilag, mind technikailag különbözik például egy IoT-eszköz által gyűjtött helymeghatározási adat megismerésétől és lefoglalásától.

A Be. az elektronikus adat lefoglalásának módját a következőképpen határozza meg:

„a lefoglalást

- a) az elektronikus adatról másolat készítésével (hiteles másolat, ami a bíróságon történő bemutatás során, az elektronikus adat hitelességét nem kérdőjelezi meg),*
- b) az elektronikus adat áthelyezésével,*
- c) az azt tartalmazó információs rendszer vagy adathordozó teljes tartalmáról történő másolat készítésével,*
- d) az azt tartalmazó információs rendszer vagy adathordozó lefoglalásával, vagy*
- e) jogszabályban meghatározott más módon lehet végrehajtani.”⁴⁹*

Miért fontos az eljárás betartása? Mert a digitális adatok a legkönnyebben változtatható, megsemmisíthető és módosítható bizonyítékok közé tartoznak, amelyeket akár távoli hozzáféréssel meg lehet változtatni, úgy, hogy azok bíróság előtti hitelessége megkérdőjelezhetővé válik, és így nem használhatók fel.

Az alábbi lehetőségek vannak:

- A helyszínen rögzített adatok és az eszközök fizikai lefoglalása – a Be. által meghatározott eljárás szabályai szerint.
- Felhőszolgáltató közreműködésének igénybevétele (például Google, Amazon) adatkéréssel.

⁴⁹ Be. 315.§ (1) bekezdés

A hatóság eredményes munkáját olyan kockázatok nehezíthetik, mint a távoli adattörlés vagy adatmanipuláció, amelyek az eszközhez való hozzáférés megakadályozását vagy megnehezítését teszik lehetővé, hiszen a távoli eszközmenedzsment funkciók komoly veszélyt jelentenek, mint például hogy a távoli törlés során az eszköz tulajdonosa vagy bűntársa eltávolíthatja az adatokat, vagy az IoT-eszközök konfigurációja, naplózása megváltoztatható.

Nemzetközi tapasztalatok

A nemzetközi tapasztalatok bemutatása a fejezetben leginkább dokumentumok felsorolására koncentrálva történik, illetve egy amerikai interneten megjelent hírrel kapcsolatos, ami jól mutatja, hogy az IoT-eszközök rendőrség általi felhasználása igenis foglalkoztatja a jogalkotókat. Az ellenük elkövetett bűnözés potenciálja nem csak egy tanulmányt érdemelne, hiszen a közszolgáltatásokban már alkalmazott IoT-eszközök elleni támadások komoly zavart tudnak okozni nemcsak a rendszernek, hanem a társadalomnak is. Az egyik dokumentum az ENISA (Európai Hálózatbiztonsági Ügynökség) „Good Practices for the Security of IoT” (2017) jelentése⁵⁰, amely ismerteti, hogy az IoT-eszközök adatai a tervezéstől egészen a felhasználásig kulcsfontosságúak lehetnek.

Az Europol minden évben kiadja az Internet Organised Crime Threat Assessment (IOCTA) jelentéseit, amelyek közül már a 2016-os is az IoT-eszközök bűnüldözési potenciáljára hívja fel a figyelmet.

Esettanulmány

2017 januárjában, Donald Trump beiktatása előtt néhány nappal kiderült, hogy Washington D.C. rendőrségének több mint 70 darab térfigyelő kame-

⁵⁰ Bellman, Christopher; van Oorschot, Paul C.: Best Practices for IoT Security: What Does That Even Mean? 2020.

ráját kompromittálták hackerek. A támadók rosszindulatú szoftvert telepítettek a kamerarendszerek szervereire, amivel időlegesen teljesen bénították a város bizonyos részein a közbiztonsági kamerahálózatot⁵¹.

Hogyan történt az említett eset?

- A kamerákhoz csatlakozó IoT-alapú rendszerek gyenge jelszavakat használtak, és nem voltak megfelelően frissítve.
- A hackerek adathalász e-mailekkel szereztek meg a rendőrség informatikai személyzetének belépési adatait.
- Miután hozzáfértek, rosszindulatú programokat (ransomware) telepítettek a kamerarendszer szervereire.

Következmények:

- Több napon át nem tudtak működni egyes térfigyelő kamerák a város kulcsfontosságú pontjain.
- A rendőrség kénytelen volt offline újratelepíteni a rendszereket, hogy helyreállítsák a működést.
- Bár nem kértek váltságdíjat, az eset világosan megmutatta, hogy a közszolgálati IoT-eszközök milyen kritikus sebezhetőséget jelentenek.

Az ügy tanulsága, hogy egy egyszerű adathalász támadás és néhány elavult biztonsági beállítás óriási operatív kiesést okozhat egy városi rendőrség működésében, ami nem csak az adatbiztonságot, de a fizikai közbiztonságot is veszélyeztetheti.

Arra vonatkozóan, hogy van-e belső szabályozás az okoseszközök ilyen irányú használatával kapcsolatban, sajnos a válasz, hogy nincs. Az egyes

⁵¹ Forrás: https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html

Letöltés ideje: 2026.08.08.

szervezetek folyamatos belső oktatással, tudatosítással és ellenőrzéssel lépnek fel az állomány IoT-eszközök használatának veszélyeire való figyelemztetésével, de belső szabályozások eddig nem születtek.

Az elsődleges és szükséges oktatási anyagokat leginkább a Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézete (korábbi néven Nemzeti Kibervédelmi Intézet) készítette, amelyet e-learnig tananyag formájában ismertettek az állománnyal. Ennek hatása, illetve betartása meg lehetőségen kétes.

A legnagyobb kockázat tehát két területen látható. Egyrészt maga a rendszer hordozza, amelyhez ezek az eszközök csatlakoznak, másrészt pedig az emberek, akik használják azokat. Ezekben a közös nevező az adat, így kiemelt fontossággal bír az adatvédelem és az adatbiztonság.

Ezek a biztonsági hibák lehetővé teszik a kiberbűnözők számára, hogy kihasználják az IoT-eszközöket, és hozzáférjenek az üzleti hálózatokhoz és adatokhoz.

Többször találkozunk azzal a kérdéssel, hogy melyik a legbiztonságosabb okoseszköz vagy rendszer, melyet érdemes venni, ha biztonságban akarjuk magunkat tudni.

A nem biztonságos IoT-eszközök által okozott főbb kockázatok közé tartoznak a botnetek, amikor a hackerek rosszindulatú programokkal fertőzik meg a gyenge biztonságú IoT-eszközöket, és botok seregeinek felépítésére használják őket. Ezeket a botneteket „felfegyverezhetik” DDoS-támadások indítására, spam e-mailek küldésére vagy rosszindulatú programok terjesztésére az interneten.

A jogi szabályozás szükségességéhez nem férhet kétség, ugyanakkor az „csak” egy válasz a már felmerült problémára, hiszen önmagában a szabályok betartása a felhasználókra van bízva. A rendőrség felderítési és bűnmegelőzési feladatainak ellátása során – így az Rtv.-ben és a Be.-ben szabályozott külső engedélyhez kötött vagy nem kötött (akár a leplezett eszközök alkalmazásának) sikerességéhez vagy egy ügy felderítéséhez – elengedhetetlen, hogy a rendőrség munkája idejekorán ne dekonspiriálódjon.

Az adatvédelmi és állampolgári szabadságjogok tekintetében ugyanakkor az IoT-technológiájának széles körű elterjedése vagy annak lehetősége (ez Magyarországon még kialakulóban van) a bűnüldözésben aggályokat vethet fel a magánélet védelmével és a polgári szabadságjogokkal kapcsolatban. A nagy mennyiségű személyes adat gyűjtésének lehetősége és elemzése potenciálisan sértheti az egyének személyiségi jogait, ha nem szabályozzák és nem biztosítják megfelelően.

Összefoglalás, következtetések és javaslatok

Az IoT-technológia forradalmasíthatja a bűnüldözést. Az IoT-eszközök használatával a bűnüldöző szervek javíthatják a bűnmegelőzést, a közlekedésszabályozást, a bizonyítékgyűjtést és a közbiztonságot. Ez segít abban, hogy közösségeink biztonságosabbak legyenek. Az IoT-technológia bűnüldözési célú használatával azonban együtt járnak olyan kihívások is, mint például az adatbiztonság, az adatvédelem és a költségek, amelyeket fontos kezelni a hatékony és biztonságos használat érdekében.

Az IoT-ökoszisztéma egyik legjelentősebb kockázati tényezője a beépített biztonsági gyengeségek tartós fennmaradása, amely a technológiai fejlődés üteme ellenére sem mutatott lényegi javulást az elmúlt évtizedben⁵². Mivel a kereskedelmi forgalomban elérhető IoT-eszközök többsége nem rendelkezik megfelelő hitelesítési és titkosítási mechanizmusokkal, vagyis a gyártók gyakran figyelmen kívül hagyják az alapvető információbiztonsági követelményeket, és számtalan eszköz még ma is alapértelmezett (gyári) jelszavakat alkalmaz, illetve titkosítatlan csatornákon továbbítja a kommunikációt, ezért rendkívül sérülékennyé teszi őket a kibertámadásokkal szemben, Ahogy a Zscaler 2023-as jelentése is mutatja, a legsérülékenyebb eszköznek a routereket találták: 400%-os növekedést mutattak ki az IoT-eszközöket érő malware támadások esetében⁵³.

⁵² OWASP: IoT Top 10 Project. Open Web Application Security Project. 2023.

⁵³ Zscaler: Zscaler ThreatLabZ . IoT Threat Landscape Report. 2023.

Az otthoni IoT-eszközök megjelenése új kihívásokat állít a magyar rendőrség bünyügyi munkája elé is. A hatékony fellépés feltétele a technológia alapos ismerete, a jogszabályok tudatos értelmezése és a gyors, szak-szerű helyszíni fellépés biztosítása.

Az IoT-eszközök közszolgálati és rendészeti alkalmazása nemcsak új lehetőségeket teremt, hanem komplex kockázatokat is generál. A jelenlegi szabályozási és gyakorlati hiányosságok fényében sürgetővé vált egy olyan intézményi szintű, jövőbe mutató stratégia kidolgozása, amely egyszerre támogatja a technológia biztonságos bevezetését és használatát, valamint csökkenti a kitettséget a kibertérből érkező fenyegetésekkel szemben.

Az első lépés ebben az irányban egy kockázatalapú eszközbeszerzési protokoll kialakítása lenne, amely lehetővé teszi, hogy az intézmények már a beszerzés előtt értékeljék az adott eszköz biztonsági kockázatait. A döntéshozatalt egy objektív, pontrendszerű mátrix segíthetné, amely a funkció-kritikusság, az adatérzékenység, a technikai sebezhetőség, a hálózati kitettség, a frissíthetőség és a gyártói megbízhatóság alapján osztályozná az eszközöket. Egy ilyen rendszer révén kiszűrhetők lennének azok az eszközök, amelyek potenciálisan súlyos biztonsági réseket hordoznak magukban, és így már korai szakaszban megalapozott döntések születnének a technológiai beruházásokról.

Szintén alapvető szükséglet egy intézményi szintű IoT-használati szabályzat létrehozása, amely részletesen szabályozza az eszközök alkalmazhatóságát, hálózatra csatlakoztatásának körülményeit, az adatkezelés eljárásrendjét, valamint a magáncélú eszközök munkahelyi használatát. Ilyen szabályzat híján az eszközhasználat teljes mértékben a felhasználók egyéni döntéseire, biztonságtudatosságára van bízva, ami a gyakorlatban komoly sebezhetőséget eredményezhet – különösen rendvédelmi vagy közbiztonsági környezetben. A szabályzatnak nemcsak tiltó rendelkezéseket kell tartalmaznia, hanem edukatív és gyakorlati útmutatásokat is a biztonságos használatra vonatkozóan.

A tanulmányban igyekeztem rávilágítani arra, hogy az emberi tényező továbbra is az egyik legkritikusabb biztonsági rés az IoT-eszközök kezelésében. Ebből kiindulva indokolt lenne a közszolgálati szférában dolgozók számára rendszeres, kötelező biztonságtudatossági képzések bevezetése, amelyek a saját (privát) eszközük használatára is nagyobb hangsúlyt fektetnének. Ezek a képzések nemcsak elméleti ismeretek átadására szolgálnának, hanem gyakorlati példákön keresztül segítenék a dolgozókat abban, hogy felismerjék a fenyegetéseket, megfelelően beállítsák az eszközeiket, és helyesen járjanak el biztonsági incidensek esetén. A képzéseknek érdemes lenne digitális, interaktív formát is öltetniük – például szimulációkkal, gamifikált modulokkal – annak érdekében, hogy minél hatékonyabban éréjk el a különböző korosztályú és informatikai jártasságú felhasználókat.

A hazai jogalkotás ugyan fontos lépést tett a kibertanúsítás bevezetésével, de különösen az IoT-eszközök vonatkozásában szükség lenne egy célzott, nemzeti szintű tanúsítási rendszer kialakítására. Ez a rendszer olyan auditfolyamatot biztosítana, amely kötelezően vizsgálja az eszközök titkosítási gyakorlatát, frissíthetőségét, jelszókezelését és a kommunikációs csatornák biztonságát. A tanúsítvány megléte feltételként szolgálhatna állami vagy önkormányzati beszerzéseknél, ezzel is ösztönözve a gyártókat a biztonsági követelmények teljesítésére. Egy ilyen rendszer nemcsak a végfelhasználók védelmét szolgálná, hanem hozzájárulna a kiberbiztonsági ökoszisztéma megerősítéséhez is.

Végezetül, a technológia fejlődésével párhuzamosan célszerű lenne az IoT-eszközök felügyeletére mesterséges intelligenciával támogatott anomáliaérzékelő rendszerek bevezetése. Ezek a rendszerek képesek lennének folyamatosan monitorozni az eszközök működését, hálózati kommunikációját, és automatikusan detektálni a gyanús viselkedési mintákat, amelyek biztonsági incidensre utalhatnak. A gépi tanulásra épülő algoritmusok nemcsak felismerik, hanem előre is jelezhetik a fenyegetéseket, lehetőséget biztosítva a gyors és proaktív beavatkozásra. Egy ilyen intelligens biztonsági réteg kulcsfontosságú lehet a jövő állami infrastruktúrájában, különösen olyan környezetekben, ahol nagyszámú, heterogén IoT-eszköz működik.

A dolgozat elején felállított hipotézisekkel kapcsolatban az alábbiakat állapíthatjuk meg.

A Magyar Rendőrség jelenleg még nem vezetett be az IoT-eszközökkel kapcsolatban semmilyen korlátozást, így azok alkalmazásának megfontolása sokszor a felhasználók biztonságtudatosságán múlik (H1).

A rendvédelmi állomány körében kevésbé népszerűek a Belügyminisztérium Vezetőképzési és Továbbképzési Főosztály által üzemeltetett e-learning felületen elérhető képzések. Közülük az elmúlt években főleg kampány jellegűen elérhető vizsgamodulok száma is csekély, és népszerűségük a kötelező teljesítés miatt megosztó az állomány körében. Évente 2-3 olyan modult készítettek, illetve az NKI által készített modult tettek elérhetővé, amelyek inkább általános ismereteket, nem pedig specifikus tudást nyújtottak volna. Ezek a képzések nem kifejezetten az IoT-veszélyekre hívják fel a figyelmet, illetve az ismeretek tényleges elsajátítása, megértésének nyomon követése nem is történik meg.

Az IoT-eszközök mindennapi használatát a rendőrség állományának körében szigorításokkal lehetne csak alkalmazni, hiszen azok tartalmazhatnak olyan sérülékenységeket, amelyek veszélyeztethetik egy eljárás sikerét (H2). Jelenleg az ORFK-nak nincs semmilyen utasítása arra vonatkozóan, hogy az IoT-eszközöket mikor vagy milyen formában lehet vagy nem lehet használni, akár a megengedett típusok vagy felhasználásuk tekintetében sem.

Irodalomjegyzék

- Kollár Csaba: IoT a gyakorlatban, az információbiztonság fókuszában I. Bolyai Szemle 2017/1. szám. 50. o.
- Az IoT-eszközök nemzeti kiberbiztonsági tanúsítási rendszeréről szóló 10/2024. (VIII.8) SzTFH rendelet.
- Nemzeti Kibervédelmi Intézet. 2022.
Forrás: https://nki.gov.hu/wp-content/uploads/2022/09/IoT-eszkozok-biztonsagi-kerdesei_II_CTI_jelentes.pdf
Letöltés ideje: 2026.08.08.

- Oláh Levente: Az IoT eszközök veszélyei.
Forrás: <https://pecsimernok.hu/az-iot-eszkozok-veszelyei/>
Letöltés ideje: 2026.08.08
- Magyarország Kiberbiztonsági Stratégiájáról szóló 1089/2025.
(III. 31.) Korm. határozat
- Zieniüte, Ugné: What is the Mirai botnet, and how does it spread?
- Forrás: <https://nordvpn.com/blog/mirai-botnet/>
Letöltés ideje: 2024.04.16
- 29. cikk szerinti Adatvédelmi Munkacsoport: 8/2014. számú vélemény a tárgyak internetének legújabb fejleményeiről, WP223, elfogadás: 2014. szeptember 16. (továbbiakban: WP223)
- Magyarország Kiberbiztonsági Stratégiájáról szóló 1089/2025.
(III. 31.) Korm. határozat
- Forrás: <https://napidroid.hu/az-amerikai-hadsereg-megtiltotta-katonainak-az-okosorak-hasznalatat-mert-azok-titkos-bazisokat-lepleztek-le/>
Letöltés ideje: 2018.08.09.
- Adaros Boye, Carolina A.: Understanding Cyberrisks in IoT:, When Smart Things Turn Against You. Business Expert Press. 2019.
- Forrás: <https://www.simonweckert.com/googlemaphacks.html>
Letöltés ideje: 2026.08.08.
- Oser, R. et al.: 'Cybersecurity Awareness in IoT: A User-Centric Perspective'. Journal of Cyber Policy 2021/2. szám. 198–214. o.
- Draitsas, Elias; Trigka, Maria: A Survey on Cybersecurity in IoT. Future internet. 2025.
- Butun, Ismail; Österberg, Patrik; Song, Houbing Herbert: Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures. IEEE COMMUNICATIONS SURVEYS & TUTORIALS. 2019.
- Mamdouh, Moustafa; Awad, Ali Ismail; Khalaf, Ashraf; Hamed, Hesham F.A.: Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions. Computers & Security. 2021.

- Javed, Asad; Malhi, Avleen; Kinnuen, Tuomas; Framling, Kary: Scalable IoT Platform for Heterogeneous Devices in Smart Environments. 2020.
- Borgohain, Tuhin; Kumar, Uday; Sanyal, Sugata: Survey of Security and Privacy Issues of Internet of Things. Computer Science. 2015.
- Staff, F: Internet of Things : Privacy and Security in a Connected World. Technical report, Federal Trade Commission. 2015.
- West, J; Bhattacharya, M; Islam, R: Intelligent Access Control for Internet of Things. Future Generation Computer Systems. 2019. 520-535. o.
- Alrawais, A; Alhothaily , A; Hu, C; Cheng, X: Fog Computing for the Internet of Things: Security and Privacy Issues. IEEE Internet Computing. 2017. 34-42. o.
- Roman, R; Najera , P; Lopez, J: Securing the Internet of Things'. Computer 2011/9. szám. 51-58. o.
- Forrás: <https://nki.gov.hu/it-biztonsag/elemzesek/iot-eszkozok-biztonsagi-kerdesei-az-okosotthon/>
Letöltés ideje: 2026.08.08.
- Készült a CoPilot segítségével.
- The Internet of Things: A survey. 2020.
- Kitchen R.: Making sense of smart cities: Addressing present shortcomings (Cambridge Journal of Regions Economy and Society 2014/1. szám. 131-136. o.
- A BIZOTTSÁG JELENTÉSE A TANÁCSNAK, AZ EURÓPAI PARLAMENTNEK ÉS AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK Jelentés a mesterséges intelligencia, a dolgok internete és a robotika biztonsági és felelősségi vonatkozásairól
Forrás: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0064>
Letöltés ideje: 2025.06.03.
- OECD Measuring of Internet of Things.
Forrás: https://www.oecd.org/en/publications/measuring-the-internet-of-things_021333b7-en.html

- Letöltés ideje: 2025.06.03.
- NAIH, 2022.
 - Forrás: https://www.tesla.com/hu_hu/support/vehicle-safety-security-features
 - Letöltés ideje: 2026.08.08.
 - Kollár Csaba: oT a gyakorlatban, az információbiztonság fókuszában I. Bolyai Szemle 2017/1. szám. 50. o.
 - Servida, Francesco; Casey, Eoghan: IoT forensic challenges and opportunities for digital traces. Digital Investigation. 2019.
 - Nozomi Networks Conference. 2025.
 - OWASP: IoT Top 10 Project. Open Web Application Security Project, 2023.
 - Melissa Hathaway and Alexander Klimburg, "Preliminary Considerations: On National Cyber Security" In National Cyber Security Framework Manual (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2012), p. 8.
 - Kosta, Eleni: The Right to an Effective Remedy in International Data Transfers of Electronic Evidence: Past Lessons and Future Outlook.
 - Bellman, Christopher; van Oorschot, Paul C.: Best Practices for IoT Security: What Does That Even Mean? 2020.
 - Forrás: https://www.washingtonpost.com/local/public-safety/hackers-hit-dc-police-closed-circuit-camera-network-city-officials-disclose/2017/01/27/d285a4a4-e4f5-11e6-ba11-63c4b4fb5a63_story.html
 - Letöltés ideje: 2026.08.08.
 - OWASP: IoT Top 10 Project. Open Web Application Security Project. 2023.
 - 1Zscaler: Zscaler ThreatLabZ . IoT Threat Landscape Report. 2023.
 - 1994. évi XXXIV. törvény a Rendőrségről
 - 2012. évi C. törvény a büntető törvénykönyvről
 - 2017. évi XC. törvény a büntetőeljárásról szóló törvény
 - 2024. évi LXIX. törvény Magyarország Kiberbiztonságáról szóló törvény