# A NEGYEDIK IPARI FORRADALOM A KÖZMŰVEKNÉL – LEHETŐSÉGEK ÉS KIBERBIZTONSÁGI VESZÉLYEK

**KIVONAT** A 2020-as évek kezdetén a negyedik ipari forradalom zajlik éppen, talán úgy, hogy észre sem vesszük, hogyan alakítja át a digitális technológia a mindennapi életünket. A hétköznapi ember ezeket a változásokat leginkább úgy érzékelheti, hogy egyre több okostelefont, okosórát, okos villanykörtét használ, miközben a háttérben az ipar, a termelés, a közművek, általánosságban az egész gazdaság egyre jobban függ ezektől a hálózatba kötött eszközöktől, melyeket összefoglaló néven Internet of Things-nek (IoT), azaz a dolgok internetének nevezünk. Jelen tanulmány célja bemutatni, hogyan hat a negyedik ipari forradalom a közműszolgáltatásra, és ezen belül is milyen kibertérveszélyeket fog jelenteni a következő években ez az átalakulás.

**KULCSSZAVAK** kiberbiztonság, negyedik ipari forradalom, Internet of Things, okosváros, okosotthon

DR. KRASZNAY CSABA *Nemzeti Közszolgálati Egyetem Kiberbiztonsági Kutatóintézet*

## Bevezetés

A negyedik ipari forradalom egyik leglátványosabb jele az, hogy otthonaink okossá válnak, olyan informatikai eszközöket kezdünk használni, melyeknek 10 évvel ezelőtt még nyomuk sem volt. Az első iPhone-t mint az okoseszközök egyik legjellegzetesebb példáját 2007. január 9-én mutatták be, majd villámgyorsan elterjedt a fogyasztók között, de például az okos fitneszkarkötők, az okosizzók, az okosautók, az okos hűtőszekrények mind-mind a 2010-es évek termékei.

Ez az évtized kitermelt számos olyan okoseszközt is, melynek a létjogosultságát sem feltétlenül értik azok, akik nem ebben a világban nőttek fel. Példaként lehetne kiemelni az okos vizespalackot, melynek célja nem más, mint hogy ezt az eszközt összekötve az okostelefonnal és a fitneszkarkötővel jelezze, hogy nem ittunk eleget, és figyelmeztessen minket az ivás fontosságára. Mivel a vízfogyasztás alapvető biológiai szükséglete az embernek, felmerül a kérdés: vajon mi indokolja egy ilyen eszköz létrehozását? Különös tekintettel arra, hogy nem csak egy megoldás van jelen, hiszen számos gyártó dobott piacra olyan terméket, mely ezt az igényt fedi le, ami azt jelenti, hogy a fogyasztóknak feltehetőleg ténylegesen szüksége van ilyen eszközökre. (Bondor 2020)

A választ a generációs különbségekben kell keresni. Jelen pillanatban 6 különböző generáció él egymás mellett, és ez a hat különböző generáció különböző módon alkalmazkodott a technológiához, különböző módon fogadta az elmúlt 100 év technológiai vívmányait. (Howe, Strauss 2007)

- Az első generáció az építők generációja (az 1946 előtt születettek), ahogy az amerikai terminológiában hívják, akik a második világháború után újjáépítették a világot, és kialakították azt a fogyasztói társadalmat, melyet ma is ismerünk. A számítógépek ennek a generációnak köszönhetők.
- Utánuk következtek a baby boomerek (az 1946–1964 között születettek), akiket Magyarországon Ratkó-gyerekekként ismerünk. Az ő életükben vált komputerizálttá a gazdaság, az ipar, az ő idejük alatt jelent meg a hálózatba kötött első eszköz, a ma ismert internet elődje.
- Az X generáció (az 1965–1979 közöttiek), más néven a digitális bevándorlók világa hozta el az otthoni számítógépek korszakát, illetve az internetet olyan formában, ahogy azt ma ismerjük. Mivel fiatalkorukban érte őket a kétpólusú világrend összeomlása, a globalizáció megjelenése, egyrészt érdeklődésből, másrészt munkahelyi kényszerből is alkalmazni kezdték az informatikai eszközöket, melyeknek a használatát sokkal könnyebben tanulták meg, mint az előttük levő generációk.
- Az Y generáció, az 1980 és 1994 közöttiek generációja már ösztönszinten használta az informatikai vívmányokat. Az ő idejükben jelent meg például a Google vagy a Facebook, vált tömegessé a mobiltelefonok használata. Ők azok, akik fiatalkorukban tapasztalták meg először a kibertér árnyoldalait.
- Utánuk következett a Z generáció, az 1995 és 2009 között születetteké, akiket már digitális bennszülötteknek lehet nevezni. Életükben a kezdetektől jelen van az internet és a különböző digitális technológiák használata, így ők, a következő évtizedek dolgozói tudnak a legjobban alkalmazkodni a negyedik ipari forradalomhoz.
- Végül az alfa generáció tagjairól kell megemlékezni, a 2010 után született gyerekekről, akiknek a digitális élete már a születésük előtt 6-8 hónappal elkezdődött, amikor édesanyjuk a közösségi hálózaton bejelentette, hogy a gyerek majd egyszer meg fog születni. Ők már a tévéképernyőt is megpróbálják úgy húzkodni, mint az okostelefonokat, hiszen azt látták, hogy a képernyő reagál arra, amit tesznek. Ők azok, akiknek az életéhez elválaszthatatlanul hozzátartoznak a digitális eszközök.

## A hálózati társadalmak

Látható tehát, hogy ahogy a generációk felsorolásában haladunk előre, úgy a digitális technológiákhoz való hozzáállás is jelentős mértékben változik, ami arra kényszeríti a szolgáltatókat is, hogy alkalmazkodjanak ügyfeleikhez. Ennek a következménye, hogy kialakult az úgynevezett hálózati társadalom, melyet Manuel Castells, a fogalom megalkotója a következőképp írt le: „olyan társadalom, amelynek társadalmi struktúráját a mikroelektronikai alapú információs és kommunikációs technológiák által táplált hálózatok alkotják." (Castells 2004)

Azt, hogy hálózati társadalomban élünk, mi sem mutatja jobban, mint hogy jelenleg a világon körülbelül 7,8 milliárd ember él, ebből 55 százalék egyébként városokban, és körülbelül 5,2 milliárd ember használ mobiltelefont. Az emberek 67 százaléka tehát mobileszköz-használó. 4,5 milliárd ember, a teljes népesség 59%-a aktív internetfelhasználó, és 3,8 milliárd ember, a népesség 49 százaléka aktív a közösségi hálózatokon. Elmondható tehát, hogy a fizikai létünk mellett a digitális létünk is kialakult, ami óhatatlanul hatással van nemcsak a mindennapi életünkre, hanem a munkahelyi tevékenységeinkre és ezen keresztül a gazdaságunkra is.

Nem véletlen, hogy a digitáliseszköz-használók a hagyományos érte-

lemben vett okoseszközök használata mellett egyre inkább felokosítják a környezetüket is, azaz kialakulnak az okosotthonok, melyek száma körülbelül 150 millióra tehető jelenleg világszerte. Ez a szám azonban hónapról hónapra növekszik: egyre többen döntenek úgy, hogy az otthonukat is különböző okoseszközökkel látják el, ezzel növelve a dolgok internetének méretét. Az okosotthonok létrehozása körülbelül 70 milliárd dolláros iparág. (Kemp 2020)

De természetesen az okosotthonok mellett az okosotthont kiszolgáló infrastruktúra megteremtése is fontos feladat. Az okosotthonok egyik legfontosabb építőköve az okosasszisztens, a legismertebbek közé tartozik az Amazon Echo, az Apple HomePod vagy a Google Home megoldása. Ezek olyan eszközök, melyek az okosotthon középpontjaként a felhasználótól kapott szóbeli parancs vagy előre beállított feladat alapján irányítják, hogy mit csináljon az okosotthon, koordinálva a különböző okosotthon-felszereléseket. Az okoseszközök száma egyébként robbanásszerűen növekszik. 2017 és 2030 között a jóslatok szerint 27 milliárd eszközről várhatóan 125 milliárd eszközre fog növekedni a számuk. (IHS 2017)

Feltehetőleg azonban ezek az adatok mára már el is avultak, hiszen napról napra újabb és újabb forradalmi megoldások jelennek meg. Az olyan, társadalmat megrázó események, mint például a koronavírus-járvány, elősegítik az okoseszközök számának a növekedését, hiszen akár a gyógyászatban, akár a fertőzöttek követésében is elengedhetetlenül fontosak az embereket szolgáló és információkat szolgáltató eszközök. Így nem meglepő, hogy Kínában a koronavírus-járvány legyűrésében vitathatatlanul fontos szerepet játszottak a különböző okoseszközök, illetve hogy iparági elemzők szerint az okosasszisztensek számának jelentős növekedése várható a járvány „mellékhatásaként". (Shein 2020) Mindez európai szemmel komoly adatvédelemi és információbiztonsági kérdéseket vet fel, tekintettel arra, hogy az ilyen megoldások óhatatlanul sértik a személyek magánszféráját.

## Az IoT információbiztonsági kihívásai

Információbiztonság szempontjából tehát a kihívás adott. Egyre több hálózatba kapcsolt eszközt, okoseszközt látunk, melynek adatvédelme és információbiztonsága tervezési szinten finoman szólva is megkérdőjelezhető. Hiszen gondoljunk csak bele abba, hogy ma már egy egyszerű kábel is sok esetben tartalmaz néhány mikroprocesszort, melyről nem feltétlenül tudjuk, hogy konkrétan mit csinál, milyen adatokat forgalmaz, hogyan hat a működési környezetére. Vagy gondoljunk egy modern önvezető autóra, melynek működéséhez különböző beágyazott informatikai eszközök hálózatba kapcsolása szükséges, ezek irányítása pedig szoftveren keresztül történik. Ráadásul várhatóan nemsokára megjelennek majd az egymással, illetve a különböző forgalomirányító eszközökkel is kommunikáló önvezető autók, így egyértelmű, hogy egy hálózatba kapcsolt teljes ökoszisztémáról beszélhetünk, melynek ha bármelyik eleme is sérülékeny, az mindenképpen hatással lesz a teljes ökoszisztémára.

Azt, hogy milyen fenyegetést jelentenek a hálózatba kapcsolt eszközök, a legjobban a Mirai botnet bizonyítja, mely 2016-ban pusztított végig a világon. Működési mechanizmusára jellemző volt, hogy különböző, hálózatra kapcsolt okoseszközöket fertőzött meg, tipikusan IP-kamerákat, illetve sérülékeny routereket. A megfertőzött eszközök folyamatosan szkennelték az internetet, újabb és újabb gyenge eszközöket keresve pedig megtalálták azokat a réseket, sebezhetőségeket és tervezési hibákat, mint például a beépített gyenge jelszavak, melyeket kihasználva fel tudták telepíteni saját magukat ezekre az eszközökre. Ezután a távolról jövő utasításokat elfogadva hajtottak végre kibertámadásokat, melyek hatással voltak olyan globális digitális szolgáltatásokra is, mint például a legnépszerűbb videostreaming szolgáltatás. Ez jól tükrözi, mi történhet, hogyha tömegesen az uralma alá tud hajtani valaki ilyen, hálózatba kapcsolt okoseszközöket. (Bederna et. al. 2019)

További figyelmeztető jel a Wikileaksen 2017-ben megjelent, Vault 7 nevű szivárogtatás, mely az amerikai Central Intelligence Agency, a CIA kibertevékenységébe nyújtott bepillantást. Megmutatta, hogy ez a hírszerző szervezet is aktívan keresi a sebezhetőségeket olyan okoseszközökben, mint például az okostelefonok, okostelevíziók vagy éppen az önvezető autók. El lehet tehát mondani, hogy az okoseszközök mind a kiberbűnözés, mind pedig az államilag támogatott kiberkémkedés és kiberhadviselés célpontjai lehetnek. A probléma pedig az, hogy ez hatással van az okosotthonokon túl a létfontosságú rendszerekre is. (Wikileaks 2017)

## Okosvárosok biztonsága

Bár a hétköznapokban kevésbé látszik, az okosotthonok mellett kialakulóban vannak az okosvárosok is. Az okosvárosok, hasonlóan az okosotthonokhoz, okoseszközök hálózatba kapcsolásáról szólnak. Céljuk azonban nem az, hogy fel tudjuk húzni a redőnyünket szóban kimondott paranccsal, hanem az olyan közművek irányítása, mint például a villamos energetikai ellátás, a gázellátás, az egészségügy, a közbiztonság, az épületvezérlés. Ebbe a körbe tartozik az okos vízkezelés, azaz a vízi közművek is. Az okos vízi közművek megjelenése azt jelenti, hogy a víz kitermelése, tisztítása, célba juttatása, illetve szétosztása is egyre inkább „okossá válik", ezzel új, korábban nem látott lehetőséget, egyben biztonsági kihívást hozva a víziközmű-szolgáltatóknak.

Az okosvárosok esetében biztonsági szempontból több különböző, egymással párhuzamosan versengő aspektust kell figyelembe venni. Egy közlekedési példával lehetne mindezt a legjobban illusztrálni. Gondoljunk bele abba, mi történik, hogyha egy önvezető autóban valamilyen sebezhetőség jelenik meg, amit azonnal frissíteni kell. Ha egy Miraihoz hasonló kártékony kód képes volna elterjedni az okosközlekedés ökoszisztémájában, akkor az autóvezetés gyakorlatilag lehetetlenné válna. Az autókban azonban, hasonlóan bármilyen más létfontosságú rendszerhez, három különböző szempont verseng egymással: az üzembiztonság, a kiberbiztonság, illetve az adatvédelem.

Kiberbiztonsági szempontból tehát a probléma az, hogy ha egy súlyos informatikai sebezhetőség jelenik meg az önvezető autókban, és ha egy olyan, féreg típusú kártékony kód jelenik meg ezekre, mely automatikusan tud terjedni a hálózaton keresztül, akkor a fertőzés perceken belül globális méretben szétterjedhet a sebezhető gépjárműveken. Ez adott esetben több tíz millió autót is érinthet, éppen ezért az informatikában megszokott módon azonnal frissíteni kell a rajtuk futó szoftvert. Itt azonban szóba kerülnek az üzembiztonsági kérdések is, hiszen informatikai eszközökben egy új hibajavítás előre nem látható gondokat okozhat. Éppen ezért nem lehet menet közben frissíteni a gépjárműveket, meg kell várni, amíg leállnak. Az önvezető autókban ez egyszerű állapotinformáció, ami interneten lekérdezhető, meg kell tehát néznünk, hogy áll-e az autó. Csakhogy itt előjönnek azok az adatvédelmi kérdések, melyek korábban nem jelentettek problémát, hiszen ha a helyi adatokból és a szenzorokból kiderül, hogy mozgásban van az autó, az azt jelenti, hogy a gyártó figyelheti is az autó konkrét közlekedési helyzetét, ami adatvédelmi szempontból problémás lehet. Azaz a kiberbiztonság hatással van az üzembiztonságra, az üzembiztonság hatással van az adatvédelemre, és mindhárom szempontot egyenlően kell figyelembe venni az új típusú okosváros-megoldásoknál.

Természetesen az önvezető okosautók tömeges elterjedése még nem napjaink kihívása, de észre kell venni, hogy a technológia az abla-

kon kopogtat. A Society of Automotive Engineers (SAE) szövetség 2014-ben adott közre egy tanulmányt, melynek címe „J3016, Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems". Ebben írták le az autonóm autók különböző szintjeivel kapcsolatos követelményeket, és összesen hat szintet határoztak meg. Mester Gyula így foglalta össze őket: (Mester 2018)

- 0. szint: A hagyományos autó teljes mértékben emberi irányítás alatt áll, nincs automatizáltság, a vezetési környezetet az ember figyeli.
- 1. szint: Az autó teljes mértékben emberi irányítás alatt áll, autóvezetés támogatása kormányzás vagy fékezés/gyorsulás esetében, a vezetési környezetet az ember figyeli.
- 2. szint: Az autó teljes mértékben emberi irányítás alatt áll, részleges automatizáltság, az autóvezetés-támogató rendszer a kormányzási és a fékezési/gyorsítási műveleteket egyszerre átveheti, a vezetési környezetet az ember figyeli.
- 3. szint: Feltételes automatizáltság, az autót teljes mértékben ember irányítja, az autóvezetés-támogató rendszer a kormányzási és fékezési/gyorsítási műveleteket egyszerre átveheti, a vezetési környezetet az automata rendszer figyeli.
- 4. szint: Magas szintű automatizáltság, az automata autóvezető-rendszer irányítja az összes dinamikus vezetési műveletet, a vezetési környezetet az automata rendszer figyeli.
- 5. szint: Teljes automatizáltság, az automata autóvezető-rendszer folyamatosan irányítja az összes dinamikus vezetési műveletet, a vezetési környezetet az automata rendszer figyeli, az autó ember nélkül is közlekedhet.

2020-ban a legtöbb új autó az 1. szinten meghatározott automatizálási fokon van, de kereskedelmi forgalomban már kaphatók 2. szintet elérő gépjárművek is. A Tesla Autopilot megoldása például erre a szintre sorolható. A 3. szintet is elérő első gépjárművet az Audi jelentette be, A8L modelljét tekinti a követelményeknek megfelelőnek. A Gartner elemző cég „Hype Cycle for Emerging Technologies, 2019" jóslata szerint a 4. szint két éven belül, az 5. szint 2–5 év múlva várható. (Panetta 2019) Az okosvárosok autókkal kommunikáló intelligens vezérlési rendszerei pedig egyelőre csak tesztpályákon léteznek. Kijelenthető tehát, hogy ha figyelembe vesszük a gépjárművek életciklusát és az átlagos városfejlesztési sebességet, a feljebb vázolt kiberbiztonsági kihívások inkább a 2030-as, mint a 2020-as években jelentkeznek majd.

## Kiberbiztonság az okos vízi közműveknél

Orbók ezt így foglalja össze: „A kibertér biztonsági kockázatainak befolyása a fizikai világra jelentősen megnövekszik, így a kockázatok közvetlenül hatással lesznek majd a személyes biztonságunk és a közösség biztonságának minden területére, függőségünk és kiszolgáltatottságunk jelentősen megnő." (Orbók 2018) Ennek a kiszolgáltatottságnak a mértékét azonban egyelőre csak sejtjük, a bizonyosságot a következő évtizedek fogják elhozni. Az amerikai U.S. Department of Homeland Security „The Future of Smart Cities: Cyber-Physical Infrastructure Risk" című tanulmánya azonban megpróbálja előre jelezni, hogy mi vár a legfontosabb közművek üzemeltetőire a digitális átalakulás folyományaként. A kiadvány a közlekedés, az energiaellátás és a vízi közművek területén mutatja be, milyen kockázatokkal fognak szembesülni ezek az alapvető infrastruktúrák.

A vízi közművek területén az okos vízkezelésben két példát hoz a tanulmány kibertámadásra. Az egyik lehetőség, hogy kibertámadás éri a vízkezelő központot, és ezen keresztül olyan hatást érnek el a támadók, ami befolyásolhatja a közegészségügyet. A másik példa, amikor az információs rendszereken keresztül a támadó tönkreteszi a vízbázist, és ezzel okoz környezeti katasztrófát. A következő ilyen példa az okos vízelosztásnál jelentkezik. Az egyik esetben egy rosszindulatú támadó távolról behatol a rendszerbe, és lekapcsolja az érzékelő szenzorokat, így szennyezett víz kerül a háztartásokba, a másik esetben pedig a támadó rendkívüli időjárási helyzetben teszi lehetetlenné a felgyűlt csapadékvíz elvezetését. Az okos víztárolásnál a példatámadások úgy szólnak, hogy egy rosszindulatú támadó távolról manipulálja a víztárolók berendezéseit, ezzel áradást okoz, illetve egy rosszindulatú támadó az internetről behatolva zavarja meg a biztonsági berendezéseket, ezzel fedve el a potenciális vészhelyzetet. (Office of Cyber and Infrastructure Analysis 2015)

Mindhárom példa nagyon jól mutatja, hogy milyen problémákat okozhat az okoseszköz a vízi közművekben. De ha stratégiai szinten vizsgáljuk a közeljövőt, célszerű kitérni az államilag szervezett kibertámadásokra is! Ezen kihívások közül is azt érdemes figyelembe venni, hogy a negyedik ipari forradalommal párhuzamosan számos olyan, korábban nem látott lehetőség nyílik a nagy befolyású, elsősorban gyártó államok számára a kibertéri befolyásolásra, melyre sem a vízi közműveknél, sem általában a kritikus infrastruktúrák esetében nem vagyunk felkészülve. Gondoljunk itt például az ötödik generációs mobilhálózatok kérdéskörére: a kínai gyártókkal szembeni kétségek elsősorban azért merülnek föl, mert az okosvárosok, így az okos közművek kommunikációját ezeken az ötödik generációs mobilhálózatokon keresztül lehet a legideálisabban megoldani, és ha egy államnak lehetősége van hatni az ország területén működő gyártókon keresztül az okosváros-infrastruktúrákra, akkor ez nyilvánvalóan előre nem látott nemzetbiztonsági kihívást jelenthet majd.

Emellett a gyártók is okozhatnak nem várt kiberbiztonsági problémákat. Például a korábban említett okosasszisztensek mindegyikéről kiderült, hogy a gyártó nem az információbiztonság és az adatvédelem alapvető eljárásai szerint működik, hiszen az okosasszisztenseknek mondott parancsok több gyártó esetében is humán embernél landoltak. Állítólagos minőségbiztosítási okokból ugyanis emberek hallgatták végig, hogy mi minden történik a háztartásokban, így a gyártók korábbi állítása, miszerint csak mesterséges intelligencia dolgozza föl a hangot, bizonyítottan többeknél nem volt igaz. Gondoljunk csak bele, milyen kihívás lehet, ha az okosvárost felépítő alapinfrastruktúrákban is ilyen tervezési hibák vannak akár szándékosan, akár nem szándékosan, melyeken keresztül a gyártó is hathat az okos-infrastruktúra működésére! Gondoljunk csak bele, milyen kockázatot rejtene, ha az okosvárost építő infrastruktúra-elemek mögött rosszindulatú országot vagy rosszindulatú gyártót kellene sejtetni!

## A kiberbiztonság európai szabályozása

A megfelelően biztonságos okos-infrastruktúra kiépítése tehát nemcsak a közműszolgáltató érdeke, hanem nemzetbiztonsági kihívás is. Egyes közművek, mint például a villamos energetika esetében a komplex hálózatok európai szinten értelmezhetők. Nem csoda, hogy az Európai Unió 2013-ban kelt kiberbiztonsági stratégiájában célul tűzte ki a létfontosságú európai rendszerek egységesen magas kiberbiztonsági szintjének elérését. Az egyébként három lábon álló európai kiberbiztonsági szabályozásban az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről támaszt követelményeket, ez a NIS-direktíva. A másik két szabályozás egyébként a GDPR-ként ismert, ez az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezésé-

ről (általános adatvédelmi rendelet), továbbá az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről, azaz a kiberbiztonsági jogszabály.

Tikos Anita összefoglalása szerint „az irányelv célja, hogy megteremtse a gyors és hatékony európai szintű kiberbiztonsági együttműködés és (incidenskezelés- és -elemzésszintű) reagálóképesség alapjait, ami remélhetőleg hatékonyan alkalmazható lesz valamennyi lényeges biztonsági esemény és kockázat kezelésére. Annak érdekében, hogy egy ilyen hatékony és gyors együttműködési mechanizmus létrehozható legyen, a legkiemelkedőbb szektorokban meg kell teremteni a hálózati és információs rendszerek biztonsága általános védelmének alapjait uniószerte. Ezért az irányelv ezen szektorokra vonatkozóan megfogalmazza a legfontosabb védelmi szempontokat és minimumelvárásokat, valamint az EU-s együttműködési mechanizmusok megfelelő működéséhez szükséges nemzeti szakosított szervezeteket és azok minimumfeladatait, -képességeit." (Tikos 2019) Az irányelv hatálya egyébként kétfajta szolgáltatóra terjed ki, az alapvető szolgáltatókra, ahova a vízi közművek is tartoznak, és a digitális szolgáltatást nyújtó szolgáltatókra, mint például az online piacterek.

Az okosvárosok kiberbiztonsági szabályozása direkt módon nem következik egyébként a NIS-direktívából, indirekt módon viszont egyértelmű, hogy hosszú távon kikerülhetetlen lesz az okos-infrastruktúra és az európai követelmény összehangolása. A pontos meghatározás szerint a NIS-irányelv alá tartozik minden olyan szolgáltató, amely „a 98/83/EK tanácsi irányelv (17) 2. cikke 1. pontjának a) alpontjában meghatározott, emberi fogyasztásra szánt víz szolgáltatója és elosztója, kivéve azokat az elosztókat, amelyek esetében az emberi fogyasztásra szánt víz elosztása csupán egy részét teszi ki az egyéb, alapvető szolgáltatásoknak, nem tekinthető közszolgáltatások és áruk elosztására irányuló általános tevékenységüknek". Ezen szolgáltatók kijelölése a nemzeti hatóságok feladata. Viszont ahogy ezek a szolgáltatók áttérnek az okos-infrastruktúra használatára, a kiberbiztonsági szempontok figyelembevétele elkerülhetetlenné válik.

## Összefoglalás

Biztosak lehetünk abban, hogy a megelőzés minden körülmények között olcsóbb, mint hogyha utólag kellene a biztonságot beleépíteni az okosváros-infrastruktúrákba. Ehhez viszont szemléletváltásra van szükség! Először is a legfontosabb a tudatosság, azaz az okoseszközök beszerzésénél legyünk tisztában a kiberbiztonság kiemelt szerepével, és az anyagi megfontolások mellett mindenképpen tervezzünk az információbiztonsággal is. Második sarkalatos szempont a szabályozás megléte. Az NIS-direktíva fontos kötelezettséget ró az alapvető szolgáltatások üzemeltetőire. Eszerint lényeges, hogy olyan belső szabályozás is létrejöjjön a víziközmű- és más közműszolgáltatóknál, mely tervez a tanulmányban említett kibertéri veszélyekkel. A harmadik lépés pedig a műszaki védelem megvalósítása, hiszen egyre több olyan szolgáltatás, illetve termék érhető el, mely ezekben a speciális közműszolgáltatói szektorokban is emelni tudja a kiberbiztonsági szintet.

## Irodalomjegyzék


Bederna, Zs., Váczi, D., Pollner, P. & Szádeczky, T. (2019). Támadás hálózatba szervezve. *In Auer, Á. & Joó, T (Eds.). Hálózatok a közszolgálatban (pp. 223–247). Budapest: Dialóg Campus*

*Bondor, M. (2020). „The best smart water bottles of 2020". https://www.mbreviews.com/best-smart-water-bottle/ [Letöltve: 2020. április 14.]*

*Castells, M. (2004). Informationalism, Networks, and the Network Society: a Theoretical Blueprint. In The Network Society: A Cross-cultural Perspective, (pp. 3–45). Cheltenham, UK: Edward Elgar*

*Howe, N. & Strauss, W. (2007). The next 20 years: how customer and workforce attitudes will evolve. Harvard Business Review, 85(7-8), 41–52.*

*IHS Markit (2017). „The Internet of Things: a movement, not a market". https://cdn.ihs.com/www/pdf/IoT_ebook.pdf [Letöltve: 2020. április 14.]*

*Kemp, S. (2020). „Digital 2020: 3.8 Billion People Use Social Media". https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media [Letöltve: 2020. április 14.]*

*Mester, Gy. (2018). Önvezető robotautók újdonságai és biztonsági kérdései. XII. innováció és fenntartható felszíni közlekedés konferencia, XII. IFFK 2018, Budapest, Hungary. https://www.researchgate.net/publication/334599495_Onvezeto_robot_autok_ujdonsagai_es_biztonsagi_kerdesei*

*Office of Cyber and Infrastructure Analysis (2015). The Future of Smart Cities: Cyber-Physical Infrastructure Risk. https://www.us-cert.gov/sites/default/files/documents/OCIA%20-%20The%20Future%20of%20Smart%20Cities%20-%20Cyber-Physical%20Infrastructure%20Risk.pdf [Letöltve: 2020. április 14.]*

*Orbók, Á. (2018). Az okos város kiberbiztonsága. In Sallai, Gy. (Ed.). Az okos város (Smart City) (pp. 187–202). Budapest: Dialóg Campus*

*Panetta, K. (2019). „5 Trends Appear on the Gartner Hype Cycle for Emerging Technologies, 2019". https://www.gartner.com/smarterwithgartner/5-trends-appear-on-the-gartner-hype-cycle-for-emerging-technologies-2019/ [Letöltve: 2020. április 17.]*

*Shein, E. (2020). „COVID-19 pandemic impact pushing smart home voice control devices to predicted 30% growth". https://www.techrepublic.com/article/covid-19-pandemic-impact-pushing-smart-home-voice-control-devices-to-predicted-30-growth/ [Letöltve: 2020. április 14.]*

*Tikos, A. (2019). A magyar kibervédelemmel kapcsolatos szabályozás aktuális kérdései. In Deák, V. (Ed.) Kritikus információs infrastruktúrák védelme – Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára – 2019 (pp 11–39). Budapest: Nemzeti Közszolgálati Egyetem*

*WikiLeaks (2017): Vault 7: CIA Hacking Tools Revealed. Forrás: https://wiki- · leaks.org/ciav7p1/cms/page_13763790.html [Letöltve: 2020. április 14.]*