Kiberbiztonság a negyedik ipari forradalom korában

KRASZNAY CSABA
Nemzeti Közszolgálati Egyetem
krasznay.csaba@uni-nke.hu

Kulcsszavak: Ipar 4.0, IoT, kiberbiztonság, NISD, GDPR, Ibtv., Cybersecurity Act, kiberfizikai rendszerek

A negyedik ipari forradalom alapvető építőkövei kétségkívül a hálózatba kapcsolt digitális eszközök, melyek milliárdszámra jelentek meg az elmúlt években. Az okos városok, okos otthonok és okos gyártás elterjedésével számuk bizonyosan exponenciálisan fog növekedni a következő évtizedben. Biztonságos működésük éppen ezért alapvető követelmény mind gazdaságunk, mind társadalmunk szempontjából. A „biztonság" kifejezés azonban a tervezők fejében leginkább a „safety", azaz üzembiztonság értelemben jelenik meg, melyre természetszerűen komoly erőforrásokat fordítanak. A „cybersecurity", azaz kiberbiztonság megvalósítása viszont az Ipar 4.0 területén inkább kérdéseket vet fel egyelőre, tekintettel arra, hogy sokkal kevesebb tapasztalat áll rendelkezésre a komplex ipari rendszerek, azaz a kiberfizikai rendszerek informatikai szempontú védelmével kapcsolatban, mint a hagyományos, fizikai térben történő fenyegetések kezelésében. Jelen tanulmány áttekinti azokat az európai és hazai stratégiákat és jogszabályokat, melyek célja a kiberbiztonság megerősítése, egyben rámutat, milyen szabályozói eszközök állnak rendelkezésre a negyedik ipari forradalom szereplőinek támogatására és kontrollálására.

1. Bevezetés

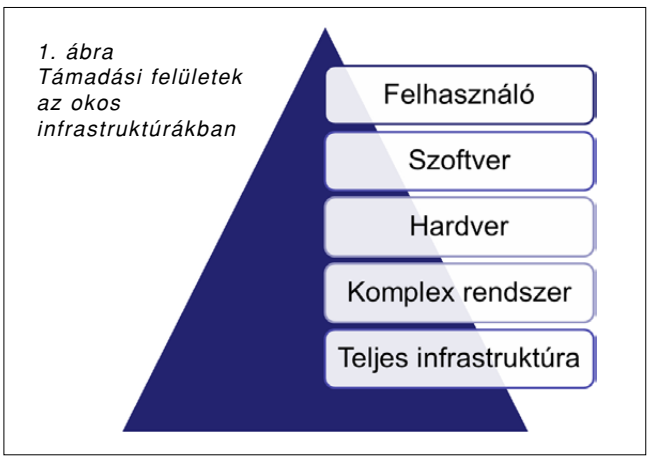
Az átlagos hírfogyasztó ma már nem nagyon tudja úgy megnyitni kedvenc hírportáljának kezdőoldalát, hogy azon ne lenne híradás valamilyen komoly kiberbiztonsági incidensről. Folyamatosan olvashatunk országok elleni kibertámadásokról, százmilliókat érintő adatszivárgásokról vagy éppen olyan egzotikusnak tűnő információs rendszerek manipulálásáról, mint egy erőművi rendszer ipari irányítástechnikája. 2017 márciusában azonban a Wikileaks által közzétett, az amerikai hírszerző ügynökségtől, a CIA-tól származó kiszivárgott anyagokból az is kiderült, hogy akár az okostévék vagy személygépjárművek informatikai rendszerei ellen is léteznek sikeres támadási technikák [1]. Tekintettel arra, hogy az egyik az okos otthonok, a másik az okos városok tipikus eszköze, felmerül a kérdés, mennyire lehetnek informatikai értelemben biztonságosak az úgynevezett Internet of Things (IoT), azaz Dolgok Internetét alkotó megoldások? Tágabban értelmezve, megvalósítható-e a Dolgok Internetére épülő negyedik ipari forradalom olyan eszközökkel, melyek támadhatók és megfelelő erőforrásokkal rendelkező entitások sikerrel is támadják azokat?

Az információbiztonsági szakértők körében az IoT rövidítés közkeletű feloldása az Internet of Threats, azaz a Fenyegetések Internete, utalva arra, hogy a szakértői közösségnek komoly aggályai vannak mind az egyes eszközök, mind pedig az ezekből felépülő ökoszisztéma védelmi szintjével kapcsolatban. Az elmúlt évek kibertámadásainak köszönhetően ebben a félelemben ma már a stratégiai védelemmel foglalkozó szakemberek is osztoznak, így egyre több ország nemzeti biztonsági és kiberbiztonsági stratégiája említi a kibertéri fenyegetéseket kiemelt nemzetbiztonsági problémának. A kockázatok enyhítése céljából pedig folyamatosan jelennek meg azok a szabályozók, melyek kötelezik az okos infrastruktúrák építőit és üzemeltetőit bizonyos informatikai védelmi intézkedések megtételére.

2. Ipari rendszereket érintő fenyegetések

Mérnöki nézőpontból hajlamosak vagyunk arra koncentrálni, hogy az egyes rendszerelemek biztonságát vizsgáljuk, nem véve figyelembe, hogy az adott rendszerelem egy komplex rendszer részeként működik, melyet emberek üzemeltetnek. Így bár egyes modulokat lehet, hogy a rendelkezésre álló legátfogóbb információbiztonsági szemlélettel valósították meg, azonban a teljes ellátási lánc valamelyik elemének gyengesége alááshatja az egyes részegységek nyújtotta megfelelő védelmi szintet.

Az *1. ábra* bemutatja, milyen támadási felületek mutatkoznak egy komplex kiberfizikai rendszer esetén.



1. ábra
Támadási felületek az okos infrastruktúrákban

Vegyük példaként az okos közlekedést, és vizsgáljuk meg, mit jelent az ábrán vázolt támadási felület egy autonóm, önvezető gépjármű szempontjából! A hardver az egyes szenzorokat, beavatkozóegységeket jelenti, melyek tömegével találhatók meg az autóban. Ezek hálózatokon keresztül juttatnak el adatot a gépjármű központi számítógépéhez, mely az adatokból a szoftver segítségével információkat állít elő, ezzel irányítva a személygépjárművet, mint komplex rendszert. Ez a komplex rendszer azonban egy okos közlekedési infrastruktúra esetén folyamatosan kommunikál az őt körülvevő környezettel, így a közlekedés-irányító infrastruktúrával és a többi autóval, melyek a teljes rendszert alkotják. Ebben az infrastruktúrában pedig jelen vannak az emberek, mint sofőrök vagy mint rendszerüzemeltetők.

Ennyire komplex ökoszisztémában kiberbiztonsági szempontból hibátlan rendszert megvalósítani szinte lehetetlen. Sokszor már az egyes rendszerelemek is tartalmaznak olyan sebezhetőségeket, melyeket a megfelelő motivációval és szakértelemmel rendelkező támadó ki tud használni és ezzel a teljes rendszert nem tervezett működésre tudja bírni. Az ipari irányítástechnikai rendszerek fejlesztői gyakran hivatkoznak arra, hogy rendszereik zárt környezetben működnek és speciális szakértelem szükségeltetik azok megismeréséhez. Ehhez képest az amerikai kritikus információs infrastruktúrák incidenskezeléséért felelős ICS-CERT szervezet statisztikái alapján évről évre egyre több olyan sebezhetőség kerül napvilágra, mely a speciális kiberfizikai rendszerelemek szoftvereinek hibáit tárja fel, ahogy az a *2. ábrán* is látható.

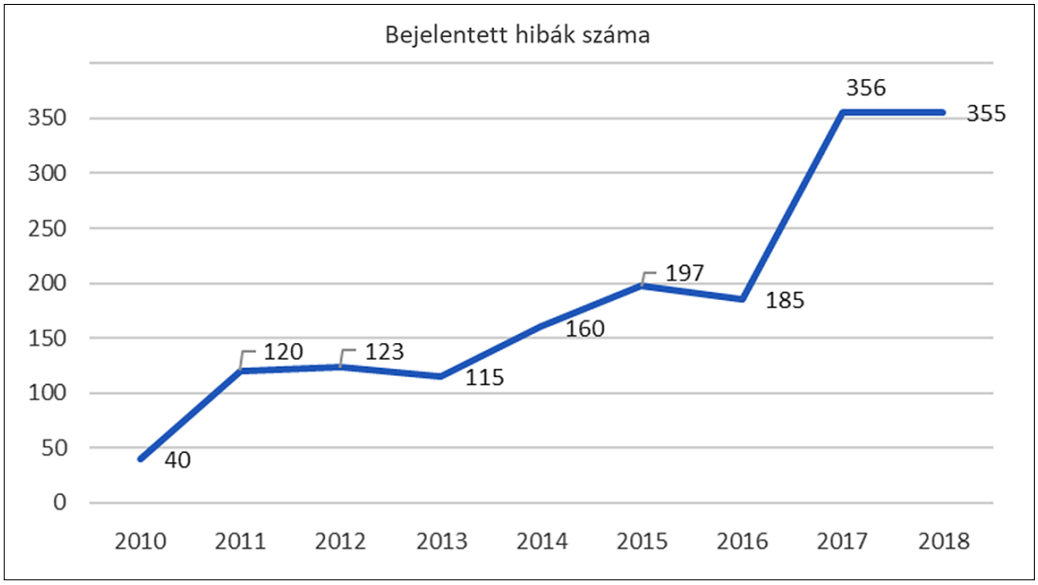
Nincs okunk kételkedni abban, hogy a negyedik ipari forradalom kiberfizikai eszközeit egyre inkább a biztonságos szoftverfejlesztés elveit felhasználva fogják létrehozni, ám ezek számosságuk és hálózati kapcsolatuk miatt könnyebben elérhetők lesznek, így feltételezzük, hogy a bennük felfedezett hibák száma az évek során monoton növekedni fog, hasonlóan az ipari irányítási rendszerekhez.

De ki kell emelni az emberi tényező fontosságát is! Bányász Péter az ellátási láncok kiberbiztonságáról szóló művében a következőket példát említi: *„Tegyük fel, a külső támadás lehetetlenné vált, olyan mértékű védelmet valósítottak meg. Ilyen esetben van szerepe a social engineeringnek, hiszen, maradva a hipotetikus példánál, a kikötő takarítószemélyzetéből egy dolgozó megzsarolásával/megtévesztésével a támadók elérhetik, hogy a takarító az informatikai eszközökhöz hozzáférést biztosítson egy pendrive számítógépbe történő helyezésével, amivel a támadók olyan hátsó kapukat nyithatnak, amellyel átvehetik az irányítást az eszköz felett."* [3] A napvilágra került, kritikus infrastruktúrákat érintő támadások során szinte minden esetben sejthető, hogy szándékos vagy gondatlan emberi tevékenység nélkül a támadás kivitelezése lényegesen nehezebb vagy egyenesen lehetetlen lett volna.

A támadási felületek közül nem került megemlítésre a hardver, a komplex rendszer és a teljes infrastruktúra. Nem véletlenül. Ezek esetében ugyanis hiányoznak azok a megbízható statisztikák, adatforrások, melyekkel szemléltetni lehet a kitettségüket. A hardverek esetében például tudjuk, hogy tervezési sajátosságok miatt számos CPU elméletileg lehetőséget biztosít a számítógépen feldolgozott bizalmas adatokhoz való hozzáféréshez (lásd a Spectre és Meltdown hibákat), de csak elképzeléseink lehetnek arról, hogy ezek valójában mekkora kockázatot jelentenek. De a kínai távközlési gyártók angolszász országokból való távoltartásának szándéka is mutatja, milyen nemzetbiztonsági kihívást érzékelnek a stratégiai védelemért felelős vezetők abban, ha az 5G távközlési rendszerek infrastruktúráját ellenérdekelt országok gyártói szállítják.

3. Kiberbiztonság az Európai Unióban

Belátható, hogy a támadási felületek csökkentése, pusztán a mérnökök eszköztárával csak tyúklépésekben lenne megvalósítható, a veszély viszont reális és azonnali, széles körű cselekvést kíván. Be kell tehát vonni azokat a közpolitikai és diplomáciai eszközöket, melyek egy-



2. ábra
Az ICS-CERT-hez bejelentett SCADA/ICS sebezhetőségek száma éves bontásban.

Forrás:
ICS-CERT Annual Vulnerability Coordination Report [2]

részt a támadók motivációját törik le, másrészt rendszerszinten várnak el cselekvést az Ipar 4.0 szereplőitől. Fogalmi szinten ez azt jelenti, hogy az egyes rendszerelemeket érintő információbiztonság mellett az ennél szélesebb körű kiberbiztonság megvalósítása is kívánatos.

A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról jól mutatja a két fogalom közötti különbséget. Eszerint az elektronikus információs rendszer biztonsága, „az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos", míg a kiberbiztonság „a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez" [4].

Hasonló következtetésekre jutottak az Európai Unió döntéshozói is. Szükséges az információbiztonság erősítése termék- és szervezeti szinten, de támogatni kell a kiberbiztonsággal kapcsolatos lépéseket is. Ennek érdekében az elmúlt években számos olyan szabályozás született, illetve lett előkészítve, melyeket minden EU-tagországnak kötelező honosítani. Az Európai Unió kiberbiztonsági reformról szóló összefoglalójában az alábbi területeket emeli ki, utalva a Kiberbiztonsági Jogszabály, vagyis a Cybersecurity Act által lefedett területekre:

• **Kiberbiztonsági tanúsítási rendszer:** Az Európai Bizottság a 2017. szeptemberi reformcsomagban javaslatot tett az IKT-termékekre, -szolgáltatásokra és -folyamatokra vonatkozó uniós tanúsítási rendszerek bevezetésére. A kezdeményezés célja az uniós kiberbiztonsági piac növekedésének elősegítése. E tanúsítási rendszerek szabályok, műszaki követelmények és eljárások formájában valósulnának meg. Szerepük az lenne, hogy csökkentsék a piac széttagoltságát és felszámolják a szabályozási akadályokat, továbbá segítsék a bizalomépítést is. A rendszereket valamennyi tagállam elismerné, ami megkönnyítené a vállalkozások számára a határokon átnyúló kereskedelmet.

• **Az uniós kiberbiztonsági ügynökség megerősítése:** A Bizottság javasolta továbbá azt is, hogy a meglévő Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) struktúráját felhasználva jöjjön létre egy erősebb uniós kiberbiztonsági ügynökség. Az új ügynökségnek az lenne a feladata, hogy segítséget nyújtson a tagállamok, az uniós intézmények és a vállalkozások számára a kibertámadások kezelésében.

• **A kompetenciatámogatástól a csalás elleni küzdelemig:** Az Európai Bizottságnak az uniós kiberbiztonság megerősítését célzó javaslata további kezdeményezéseket is tartalmaz:

– A nagy kiterjedésű kibertámadásokra adandó válaszlépéseket meghatározó terv.
– Európai Kiberbiztonsági Kutatási és Kompetenciaközpont, kiegészülve a hasonló központok tagállami szintű hálózatával.
– Hatékonyabb büntetőjogi fellépés a kiberbűnözéssel szemben a készpénz-helyettesítő fizetési eszközökkel összefüggő csalás és hamisítás elleni küzdelemről szóló új irányelv révén.
– A globális stabilitás erősítése nemzetközi együttműködés útján [5].

Fontosak tehát mind az információbiztonsági, mind a kiberbiztonsági szempontú tevékenységek. Első lépésben az Európai Unió két olyan szabályozást alkotott, melyek komoly hatással vannak a nemzeti jogrendre is és az Ipar 4.0 szereplőinek is érdemben figyelembe kell ezeket vennie. Ezek egyrészt az Európai Parlament és a Tanács (EU) 2016/679 Rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, közkeletű nevén a GDPR), másrészt az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, azaz az NIS Direktíva.

Míg a GDPR célja a személyes adatok védelmének biztosítása, akár olyan környezetben is, ahol nagy mennyiségű adat keletkezik, tehát tipikusan egy IoT-rendszerekből álló okoskörnyezetben, az NIS Direktíva kijelöli azokat a kritikus információs infrastruktúrákat, melyek védelme európai szinten kiemelten fontos, amilyenek például az olyan digitális infrastruktúra szolgáltatók, mint az Internet Exchange Point-ok, DNS-szolgáltatók vagy legfelső szintű doménnév-nyilvántartók (TLD). A közlekedési infrastruktúra tekintetében a 2010/40/EU európai parlamenti és tanácsi irányelv 4. cikkének 1. pontjában meghatározott intelligens közlekedési rendszerek üzemeltetőit nevesíti a Direktíva, mely a meghatározás szerint *„olyan rendszerek, amelyekben információs és kommunikációs technológiákat alkalmaznak a közúti közlekedés területén, beleértve az infrastruktúrát, a járműveket és a felhasználókat is, a forgalomirányításban és a mobilitás kezelésében, valamint a más közlekedési módokhoz való kapcsolódási pontok vonatkozásában"* [6].

Ha ezekhez hozzávesszük a Kiberbiztonsági Jogszabályt is, egyértelműen kirajzolódik az Európai Unió törekvése. Olyan termékek és szolgáltatások kialakítását szeretnék ösztönözni innovációs és regulációs eszközökkel az európai piacon, különösen a kritikus információs infrastruktúrát alkotó kiberfizikai rendszerek esetében, melyek egyszerre veszik figyelembe az adatvédelmi és kiberbiztonsági szempontokat. Tekintettel arra, hogy a negyedik ipari forradalom infrastruktúrája és szolgáltatásai éppen kialakulófélben vannak, az európai okosinfrastruktúrában érintett szereplőknek ezt a politikai szándékot mindenképpen érdemes figyelembe venni!

4. A magyar kibervédelmi szabályozás változása

Természetesen a hivatkozott európai szabályozások mélyen érintik a magyar jogrendet is. 2018 folyamán a GDPR végrehajtásához szükséges részletszabályozásokkal módosult a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.), az NIS Direktíva miatt pedig pontosításra került a 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.), és a 2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről (Ektv.) is. A 271/2018. (XII. 20.) Korm. rendelet az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól pedig tovább centralizálta a hazai intézményrendszert, kiemelt szerepet adva a Nemzeti Kibervédelmi Intézetnek.

Jelen cikk szempontjából azonban a legfontosabb új jogszabály a *1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról,* ugyanis ez részletezi, hogy hazánk milyen stratégiai lépéseket kíván tenni az NIS Direktíva és általánosságban az európai kiberbiztonsági stratégia végrehajtása érdekében. Mindezt oly módon teszi, hogy ágazati stratégiaként illeszkedik a továbbra is hatályban maradó korábbi, 1139/2013. (III. 21.) Korm. határozathoz, mely Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szól. Az új stratégia főbb területeit a *3. ábra* foglalja össze.

Sajnálatos módon az új magyar stratégia explicit módon nem foglalkozik a negyedik ipari forradalom jelentette technológiai változásokkal, kiolvasható belőle viszont az a szándék, hogy Magyarország részese legyen az Európai Unió kezdeményezéseinek.

A Kiberbiztonsági Jogszabály tervezete így fogalmaz: *„Az új technológiák, például a mesterséges intelligencia, a dolgok internete, a nagy teljesítményű számítástechnika, a kvantum-számítástechnika, a blokklánc és a biztonságos digitális személyazonosításhoz hasonló koncepciók nem csupán új kihívásokat támasztanak, de megoldásokat is kínálnak a kiberbiztonság területén. A meglévő és jövőbeni IKT-rendszerek ellenálló képességének felméréséhez és igazolásához szükséges lesz, hogy a biztonsági megoldásokat nagy teljesítményű és kvantumszámítógépekről levezényelt támadásokkal szemben teszteljék. A kompetenciaközpont, a hálózat és a kiberbiztonsági kompetenciaközösség feladata az is, hogy segítséget nyújtson a legújabb kiberbiztonsági megoldások kifejlesztéséhez és elterjesztéséhez. Emellett fontos, hogy a kompetenciaközpont és a hálózat a létfontosságú szektorokban (pl. közlekedés, energetika, egészségügy, pénzügy, kormányzat, telekommunikáció, gyártás, védelem és űrkutatás) tevékenykedő fejlesztők és szolgáltatók rendelkezésére álljon, és segítse őket a kiberbiztonsági kihívások leküzdésében."* [7]

Magyarország ehhez egyrészt a hazai innováció támogatásával, másrészt a kritikus információs infrastruktúra védelmével kíván csatlakozni. A hálózati és információs rendszerek biztonságáról szóló stratégia a következő intézkedéseket tűzi ki a kibervédelmi intézményrendszer számára:

- 33.) legyenek szabadon hozzáférhetők ágazatközi, illetve ágazat-specifikus konszenzust képviselő ajánlások és jó gyakorlatok a biztonsági célok elérésére vonatkozóan;
- 35.) álljon a kritikus infrastruktúrák üzemeltetőinek minél szélesebb köre rendelkezésére a védelmet kiegészíteni képes egységes szolgáltatáscsomag;
- 36.) a létfontosságú rendszerek, létesítmények és szolgáltatások fizikai és kiberbiztonsága területén a hatékony megelőzés és gyors reagáló képesség

3. ábra A hálózati és információs rendszerek biztonságáról szóló stratégia főbb területei

fejlesztésére célzott pályázati lehetőségek biztosítása szükséges az üzemeltetők, a szolgáltatást nyújtók, az érintett hatóságok és az eseménykezelő központok működésének fejlesztésére;

- 45.) létre kell hozni egy kiberbiztonsági szakterületet érintő kutatási stratégiát, melynek célja – a magyar intézményrendszer kiberbiztonságának erősítése érdekében – a magyar fejlesztésű kiberbiztonsági eszközök, szoftverek és termékek alkalmazásának fokozása;
- 46.) kerüljenek azonosításra a kapcsolódó kutatás-fejlesztési témakörök, továbbá kerüljenek megteremtésre az állami ösztönzési lehetőségek, beleértve a magyar korai fázisú vállalkozások ösztönzését is;
- 47.) a 45. pontban leírt kiberbiztonsági kutatás-fejlesztési-innovációs stratégia kiemelten kezelje az Európai Unió 2021-2027 között meghirdetésre kerülő K+F+I felhívásainak témáit, ezzel segítve az innovatív magyar szervezeteket abban, hogy a kiemelten tudjanak részt venni a nemzetközi projektekben. [8]

5. Összefoglalás

A negyedik ipari forradalom elengedhetetlen előfeltétele a (kiber)biztonságosan működő digitális infrastruktúra létrehozása. Ez azonban nem csupán műszaki feladat, a digitális ökoszisztéma minden szereplőjének, így az államoknak is komoly feladatai és felelősségei vannak a kibertéri fenyegetések kezelésében. Mivel az Ipar 4.0-át érintő fejlesztésekben az amerikai és kínai vállalatok jelentős előnyre tettek szert az európai versenytársakkal szemben, nem utolsósorban a célzott állami beavatkozásnak köszönhetően, az Európai Unió elemi érdeke olyan környezet létrehozása, mellyel az európai vállalkozások is versenyben tudnak maradni és az európai gazdaságok képesek lehetnek csökkenteni a tengerentúli digitális megoldásoktól való függőségeiket, ezzel pedig az államilag támogatott kibertámadásokkal szembeni kitettségüket is.

Az Unió ezt felismerve olyan szabályozások megalkotása mellett döntött, melyek ösztönzik az okosinfrastruktúrák üzemeltetőit a kiber- és adatvédelem implementálására már a tervezési szakaszban. Magyarország, mint minden EU-s tagország, adaptálta a már létrejött jogszabályokat és részt vesz az új szabályozások megalkotásában. A már elfogadott joganyag, így elsősorban a hálózati és információs rendszerek biztonságáról szóló stratégia konzervatív módon közelít a negyedik ipari forradalom jelentette kiberbiztonsági kihívásokhoz, azt nem nevesíti, csak közvetve utal arra, hogy a hazai fejlesztők és szolgáltatók sem maradnak ki az Uniós tevékenységekből.

Figyelembe véve az olyan hazai kormányzati törekvéseket, mind például az okos városok létrehozásának szándéka, ez az óvatos megközelítés nem feltétlenül szerencsés és magában hordozza a kockázatát annak, hogy direkt szabályozási lépések nélkül az újonnan létrejövő okosinfrastruktúrák nem készülnek fel a 2020-as évek kibertérből érkező kihívásaira.

Hivatkozások

[1] A. Greenberg, "How the CIA can hack your phone, PC, and TV (says Wikileaks)" Wired, March 7, 2017. *https://www.wired.com/2017/03/cia-can-hack-phone-pc-tv-says-wikileaks/* [Accessed January 10, 2019.]

[2] National Cybersecurity and Communications Integration Center, ICS-CERT Annual Vulnerability Coordination Report.

[3] Bányász P., Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai. In: Csengeri János; Krajnc Zoltán (szerk.) Humánvédelem – békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése, Budapest, Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, (2016) p.918.

[4] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

[5] European Council, Council of the European Union, "Reform of cybersecurity in Europe", General Secretariat of the Council, *https://www.consilium.europa.eu/en/policies/cyber-security/* [Accessed: January 11, 2019.]

[6] Az Európai Parlament és a Tanács 2010/40/EU Irányelve az intelligens közlekedési rendszereknek a közúti közlekedés területén történő kiépítésére, valamint a más közlekedési módokhoz való kapcsolódására vonatkozó keretről.

[7] Javaslat Az Európai Parlament és a Tanács rendelete az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózatának létrehozásáról.

[8] 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról.

A szerzőről

DR. KRASZNAY CSABA a Nemzeti Közszolgálati Egyetem adjunktusa, kutatási témája a kiberbiztonság, jelenleg az egyetem Kiberbiztonsági Akadémiájának programigazgatója. A Magyary E-közigazgatástudományi Egyesület és az Önkéntes Kibervédelmi Összefogás elnökségi tagja. 2003-ban szerezte meg diplomáját a Budapesti Műszaki és Gazdaságtudományi Egyetem Villamosmérnöki és Informatikai Kar villamosmérnöki szakán, majd PhD-jét az NKE-n 2012-ben katonai műszaki tudományok területén. 2011-ben az „Év Útmutató Biztonsági Szakemberének" választották. Felsőoktatási tevékenysége mellett folyamatosan dolgozik piaci közegben is.