IoT AND THE REGULATION OF CYBERCRIMES

IoT ÉS A KIBERBŰNCSELEKMÉNYEK SZABÁLYOZÁSA

MIKLÓS Gellért[1]

Abstract

The aim of this paper is to present the Hungarian regulation of cybercrime related to the information system, as well as the closely related international legal documents. The actuality of the topic is provided by the explosive growth of IoT devices and, in parallel, the number of cybercrimes. Given the cross-border nature of these offenses, it seems unavoidable to regulate minimum security standards for IoT devices in addition to criminal offenses. Recommendations, guidelines and standards have already been drawn up, but there are currently no such binding regulations.

Keywords

IoT, cybercrime, EU law, criminal law, information system

Absztrakt

Jelen írás célja bemutatni az információs rendszerrel kapcsolatos kiberbűncselekmények magyar szabályozását, valamit az azzal szorosan összefüggő nemzetközi jogi dokumentumokat. A téma aktualitását az IoT eszközök elterjedésének és ezzel párhuzamosan a kiberbűncselekmények számának robbanásszerű növekedése szolgáltatja. Tekintettel ezen bűncselekmények határokon átívelő jellegére, megkerülhetetlennek tűnik a bűncselekmények mellett az IoT eszközökre vonatkozó minimum biztonsági előírások nemzetközi szabályozása is. Ajánlások, iránymutatások, valamint szabványok már készültek, de jelenleg nincs érvényben ilyen jellegű kötelező érvényű szabályozás.

Kulcsszavak

IoT, kiberbűnözés, EU jog, büntetőjog, információs rendszer

[1] gellert.miklos@gmail.com | ORCID: 0000-0002-3757-6834 | doctoral candidate / doktorandusz hallgató | Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

A számítástechnika megállíthatatlan fejlődésével napjainkra már szinte majdnem minden jogi és természetes személy kapcsolódik valamilyen módon a globális hálózathoz. Magyarországon 2019-ben a háztartások 86%-a rendelkezett internet hozzáféréssel. [1] Napjaink egyik meghatározó globális megatrendje a digitalizáció, amelynek egyik velejárója, hogy olyan eszközök is intelligenssé váltak, amelyeket korábban nem érintett a számítástechnikai fejlődés. Az IoT felhasználási köre nem korlátozódik az iparra, mezőgazdaságra vagy a közlekedésre, hanem jelen van a háztartásokban is. Egy okostelefonról vezérelhető mosógép, vagy egy vízforraló tulajdonosának időt és energiát takaríthat meg az által, hogy lehetővé teszi a távoli irányítást, azonban legalább ekkora biztonsági kockázatot is jelent a felhasználójára nézve. Több, különböző meghatározás is született a tudományos világ és a gazdasági élet szereplőitől a dolgok internetének meghatározására. Ebben a cikkben a Nemzetközi Távközlési Egyesület (angolul International Telecommunication Union, ITU) által közzétett meghatározást fogom alkalmazni, amely alapján az IoT az információs társadalom globális infrastruktúrája, amely lehetővé teszi a fejlett szolgáltatásokat a (fizikai és virtuális) dolgok összekapcsolásával a meglévő és fejlődő interoperábilis információs és kommunikációs technológiák alapján. [2]

Jelen publikáció be kívánja mutatni a kiberbűncselekmények és azon belül is kifejezetten az információs rendszerek ellen elkövetett bűncselekményre vonatkozó főbb nemzetközi jogforrásokat, valamint a magyarországi büntetőjogi szabályozást, valamint rámutatni egy egységes szabványosítási és tanúsítási rendszer szükségességére.

A KIBERBŰNCSELEKMÉNYEK JOGI SZABÁLYOZÁSÁNAK FŐBB NEMZETKÖZI ÉS HAZAI FORRÁSAI

A kiberbűnözés a számítástechnika fejlődésével egyidejű, napjainkra pedig már magányos hackerek és szervezett bűnözői csoportok sora specializálódott az informatikai bűncselekmények elkövetésére. Megjelentek olyan, új bűncselekmények, amelyek csak információs rendszerekkel követhetők el, amelyeknek tárgya maga az információs rendszer. A digitalizáció azonban számos olyan hétköznapi bűncselekményt is befolyásolt, amelyek korábban is léteztek ugyan, de az információs rendszerek segítségével is elkövethetők, erre jó példa a csalás. Ezeknél a bűncselekményeknél az információs rendszerek az elkövetés eszközéül szolgálnak. [3] A technológia fejlődésével sem a jogi szabályozás, sem a felhasználók tudatossága nem tudja tartani a lépést.

A kiberbűncselekményeknek több olyan jellemzője is van, amelyek megnehezítik az érintettek és sokszor a hatóságok számára is a kiberbűncselekmények felismerését és azok elkövetőinek felkutatását, azonosítását. Ennek oka többrétű, amely szorosan összefügg a virtuális tér sajátosságaival, ezáltal pedig jellemzi IoT-t is. Egyrészt a technológia lehetővé teszi a bűnözők számára, hogy identitásukat elrejtsék és a bűncselekményeket anonim módon hajtsák végre. Ma már könnyedén megoldható, hogy az elkövetők titkosított csatornán keresztül tartsanak kapcsolatot egymással, saját azonosítóikat, nyomaikat pedig elrejtsék, megváltoztassák a hatóság fürkésző tekintete elől. A darkneten az illegális termékek és szolgáltatások széles köre érhető el magas fokú titkosítás mellett. Másrészt meghatározó ezen bűncselekmények vonatkozásában a nemzetközi jelleg. A hálózathoz csatlakozó rendszerek

és felhasználók előtt nincsenek fizikai határok, az információ a kibertérben szabadon áramolhat a felek között. Éppen ezért az IoT eszközök és felhasználóik ki vannak téve földrajzilag akár több ezer kilométerre, más kontinensen tartózkodó bűnözők támadásainak is. A kiberbűncselekmények ráadásul általában rendkívül gyorsan zajlanak le. Egy információs rendszerbe történő jogosulatlan belépés előkészítése ugyan az alkalmazott védelmi intézkedésektől és annak megkerülésének módszerétől (phising, social engineering, brute force jellegű támadások stb.) függően különböző ideig tarthat, azonban magába a rendszerbe történő belépés már csak pillanatok kérdése. Ezzel magyarázható a kiberbűncselekmények körében a magas fokú felderítetlenség, hogy az esetek nagy részében a hatóságok soha nem szereznek tudomást ezekről bűncselekményekről. Ez összefüggésben állhat azzal, hogy a sértettek gyakran nem észlelik a sérelmükre elkövetett kiberbűncselekményt, és elképzelhető az is, hogy bizonyos sértetteknek nem fűződik érdekük a bűncselekmény bejelentéséhez, ugyanis az incidens bejelentése hátrányosan befolyásolná az ügyfelek bizalmát és a sértett hírnevét, márkanevét. [4]

Az IoT eszközökre egyelőre nem vonatkozik olyan kötelező jogi követelményrendszer, amely meghatározná a védelem minimálisan kötelező szintjét. Vannak ugyan a védelmi intézkedésekre vonatkozó ajánlások, iránymutatások és szabványok, ezek alkalmazása azonban jelenleg önkéntes. A gyártók a költséghatékonyság és az eszközök korlátozott életciklusa miatt nem látják el az IoT eszközöket megfelelő védelemmel. Az IoT eszközök széleskörű alkalmazása ezért korábban nem ismert támadási lehetőségeket kínál a támadók, kiberbűnözők számára. Egy hálózatra kapcsolódó jármű felett menet a támadók akár menet közben is átvehetik az irányítást, teljesen kiszolgáltatva annak utasait. Az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (angolul European Union Agency for Cybersecurity ENISA) ajánlásában több, az intelligens gépjárművekre vonatkozó lehetséges támadási forgatókönyvet is ismertet. [5] Nem csak az intelligens gépjárművek, de az egyszerű háztartási eszközök is veszélyt jelenthetnek a felhasználóikra. Kutatások igazolták, hogy a legtöbb IoT zár feltörhető, annak ellenére, hogy a gyártók robosztus védelmet ígérnek a felhasználók számára. Egy ilyen hibát a bűnözők egyaránt használhatnak az ingatlanba történő bejutásra, de akár az ingatlanban tartózkodó személyek foglyul ejtésére is az ajtó bezárásával. A felsorolás szinte vég nélkül folytatható lenne, naponta jelennek meg híradások az IoT eszközök sérülékenységét feltáró tesztekről, incidensekről.

A kiberbűnözéssel kapcsolatos szabályozás egyik első és mindmáig meghatározó egyezménye az Európa Tanács által 2001. november 23-án elfogadott Számítástechnikai Bűnözésről szóló Egyezmény (angolul Convention on Cybercrime, a továbbiakban: Budapesti Egyezmény). [6] A Budapesti Egyezmény egyrészt definíciókat alkot és rögzíti a számítástechnikai rendszer, a számítástechnikai adat, a szolgáltató és a forgalmi adat fogalmát, másrészt négy címbe sorolva csoportosítja azokat a büntető anyagi jogi tényállásokat, amelyekre nézve az aláíró tagállamok kötelesek arányos, hatékony és visszatartó erejű büntetéseket alkalmazni, ideértve a szabadságelvonó büntetéseket is.

A Budapesti Egyezmény az alábbi bűncselekménykategóriákat különbözteti meg:

- I. Cím Számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények
- II. cím Számítógéppel kapcsolatos bűncselekmények
- III. cím Számítástechnikai adatok tartalmával kapcsolatos bűncselekmények

- IV. Cím Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények

Az Európai Unió Tanácsa 2005. február 24.-én fogadta el a 2005/222/IB Kerethatározatát a tagállamok büntető jogszabályainak az információs rendszerek elleni támadások terén történő közelítése érdekében. A kerethatározat érdeme, hogy abban a számítástechnikai rendszer helyett már az információs rendszer fogalma kerül meghatározásra. A Kerethatározatot a szorosabb integráció és a jogközelítés érdekében felváltotta az Európai Parlament és Tanács 2013/40/EU irányelve (a továbbiakban: Irányelv).[7] Az irányelvek az Európai Unió olyan jogalkotási aktusai, amelyek a tagállamok számára rögzítik elérendő célkitűzéseket, azokat azonban a tagállamok saját jogalkotásuk keretében elfogadott aktusokkal valósítják meg. Az Irányelv deklarált célja volt a tagállamok büntetőjogának harmonizációja, valamint az illetékes hatóságai közötti együttműködés erősítése. Az Irányelv Preambulumában hivatkozik továbbá a Budapesti Egyezményre, mint a számítástechnikai bűnözés, többek között az információs rendszerek elleni támadásokkal szembeni küzdelem irányadó jogi keretére, amelyre maga az Irányelv is épül.

Az irányelv az alábbi bűncselekményeket szabályozza:

- Információs rendszerekhez való jogellenes hozzáférés
- Rendszert érintő jogellenes beavatkozás
- Adatot érintő jogellenes beavatkozás
- Jogellenes adatszerzés

Az irányelv alapján jogellenes a hozzáférés valamely információs rendszerhez vagy annak egy részéhez, ha azt szándékosan és jogosulatlanul, valamely biztonsági intézkedés megsértésével követték el. Az Irányelv a bűncselekmények meghatározásán túlmenően minimum büntetési tételeket is meghatároz a tagállamok számára, amelyekhez képest azonban a tagállamok szigorúbb büntetési tételeket is kiszabhatnak [2]

Az irányelvnek való megfelelés érdekében Magyarországon a 2014. évi LXXII. Törvény módosította a Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 423. §-át. [8] A Btk. meghatározása alapján információs rendszer az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége3, amely meghatározás megfelel az Irányelvben foglaltaknak és magába foglalja számítógépeken túlmenően az IoT eszközöket, a hírközlési és telekommunikációs hálózatokat, rendszereket és a SIM kártyákat is. A meghatározás nem tesz különbséget a jelek továbbítása között, így egyaránt magába foglalja az elektronikus, az optikai, a rádióhullámok, az infravörös vagy rövidhullámok, valamint műholdas sugárzás útján létrejövő információs rendszereket. [9] Az Irányelvnek megfelelően átültetésre kerül az adat fogalma is, amely magába foglalja a programot is, mint olyan adatot, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.

[2] Irányelv 9. cikk
[3] Btk. 459. (1) 15. pontja

Az Információs rendszer vagy adat megsértése bűncselekmény alapesetét[4] az információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával történő jogosulatlan belépés, vagy az elkövető belépési jogosultsága kereteit túllépve vagy azt megsértve bent maradása valósítja meg. Az alapesetben foglalt bűncselekmény tehát már a védelmi intézkedés megsértésével vagy kijátszásával megvalósított jogosulatlan belépés, valamint a jogsértő bennmaradás ténye önmagában megvalósítja. A bűncselekmény elkövetési tárgya maga az információs rendszer, elkövetése pedig két évig terjedő szabadságvesztésbüntetéssel büntetendő. A fenti megfogalmazásból több fontos megállapítás is levezethető. Egyrészt amennyiben az információs rendszer védelmét technikai intézkedés nem biztosítja, úgy az elkövető információs rendszerbe történő jogosulatlan belépése nem valósítja meg a bűncselekményt. Az IoT eszközökre nézve jelenleg nincs kötelezően alkalmazandó magyar, vagy egységes európai vagy nemzetközi szabvány, amely kötelező jelleggel írná elő védelmi intézkedések, például jelszó vagy tűzfal alkalmazását ezen eszközökben. A forgalomban lévő és felhasználók számára elérhető legtöbb okoseszköz semmilyen fajta védelemmel nincs ellátva, az adattovábbítás pedig nem titkosított. A bűncselekmény alaki (immateriális) bűncselekmény, amely magával az elkövetési magatartás tanúsításával befejezetté válik. A kísérlet megállapítható amennyiben az elkövető megkísérli a védelmi intézkedés kijátszását, azonban az információs rendszerbe nem sikerült még belépnie. Ma már számos rendszer vezet nyilvántartást a sikertelen belépési kísérletekről is, amelyek bizonyítékul szolgálhatnak egy nyomozás során.

A bűncselekmény második alapesete akkor valósul meg, ha az elkövető az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza. Az akadályoztatás mibenlétéről a Btk. hallgat, azonban az értelmezés segíti mind a Budapesti Egyezményben[5], mind az Irányelvben[6] található akadályozás cselekményeket tartalmazó példálózó felsorolása, amely szerint adatok bevitele, továbbítása, megrongálása, törlése, minőségi rontása, megváltoztatása, elrejtése vagy hozzáférhetetlenné tétele az információs rendszert akadályozó cselekménynek minősül. Az akadályozásnak itt az információs rendszer rendeltetésszerű használatát kell megakadályoznia. Ebben az esetben is a kísérlet már az elkövetési magatartás – tehát az akadályozásra irányuló cselekmény – megkezdésével megvalósul. A bűncselekmény harmadik fordulata az adat jogosulatlan megváltoztatását, törlését vagy hozzáférhetetlenné tételét szankcionálja[7] az elkövetési tárgy pedig maga a számítógépes adat, beleértve a programot is. Az okos szenzorok, mérőegységek például a hálózathoz kapcsolódva továbbítanak adatokat a felhasználó fogyasztásáról, vagy különböző folyamatok állásáról. Támadók az IoT eszközbe belépve megváltoztathatják az érzékelő vagy mérőegység által továbbított jeleket, ezáltal jelentősen magasabb fogyasztási adatokat továbbíthatnak, vagy a magasabb mérési adatokkal (például hőmérséklet), kiválthatnak rendszerspecifikus válaszintézkedéseket, mindkét esetben kárt okozva a felhasználónak. Természetesen amennyire az IoT eszközök és felhasználásuk sokféle, úgy képtelenség számba venni és felsorolni az összes lehetséges károkozást. A törvény szövegéből egy-

[4] Btk. 423. § (1)
[5] Budapesti Egyezmény 5. cikk
[6] Irányelv 3. cikk
[7] Btk. 423. § (2) b)

értelmű, hogy már egyetlen adat megváltoztatása, törlése, hozzáférhetetlenné tétele megvalósítja a bűncselekményt, nem szükséges azonban, hogy a felsorolt cselekmények az adatfeldolgozást eredményét ténylegesen befolyásolják is. Az akadályozás és a megváltoztatás bűntette legfeljebb három évig terjedő szabadságvesztéssel büntetendő.

A törvény alapján a fentebb ismertetett bűncselekmény második és harmadik fordulata súlyosabban büntetendő, amennyiben az jelentős számú információs rendszert érint. A jelentős szám értelmezésére sem a törvény, sem a Budapesti Egyezmény, sem az Irányelv nem ad útmutatást, így annak kimunkálása a jogalkalmazói gyakorlatra hárul. Tekintettel arra, hogy a minősített eset megvalósulása az érintett információs rendszerek számától függ, ezért valószínűsíthető, hogy az érintett rendszerek számának a százas nagyságrendet el kell érnie. [9] A büntetés ebben az esetben egy évtől öt évig terjedő szabadságvesztés lehet. Az IoT eszközök sokfélesége miatt számtalan olyan felhasználási mód képzelhető el, ahol ezek az eszközök százas, ezres nagyságrendben kerülnek alkalmazásra akár egy létesítményen belül is. Ilyen esetekben a létesítmény elleni támadás már önmagában megvalósíthatja a minősített esetet. Megvalósulhat a minősített eset továbbá információs rendszer botnet hálózatba történő szervezésével is. A botnet, vagy más néven robothálózat egy fertőzött informatikai eszközökből – köztük IoT eszközökből - is álló hálózat, amelyet a botnet gazdája többféle károkozásra is alkalmazhat. [10] 2016-ban például egy kizárólag biztonsági kamerákból álló botnethálózattal hajtottak végre szolgáltatás megtagadást okozó támadást (Denial-of-Service ─ DoS) egy vállalkozás szerverei ellen. [11] A kamerák azért is bizonyultak a támadás szempontjából kézenfekvő választásnak, mert a felvételek továbbításához rendelkeztek szélessávú internet hozzáféréssel, azonban sem az eszközök, sem pedig hálózati szinten nem rendelkeztek semmiféle védelemmel.

Még súlyosabban büntetendő a bűncselekmény, ha azt közérdekű üzem ellen követik el. Közérdekű üzem alatt a törvény a közművet, a közösségi közlekedési üzemet, az elektronikus hírközlő hálózatot, az egyetemes postai szolgáltató közérdekű feladatainak teljesítése érdekében üzemeltetett logisztikai, pénzforgalmi és informatikai központok és üzemek, valamint a hadianyagot, haditechnikai eszközt termelőüzemet, energiát vagy üzemi felhasználásra szánt alapanyagot termelőüzemet érti. A törvény érthető okokból ezt a minősített esetet bünteti a legsúlyosabban, a büntetés két évtől nyolc évig terjedő szabadságvesztés. Amint arra tanulmányában Mezei Kitti is rámutat, a Btk. fogalomhasználata indokolatlanul szűkíti az Irányelv által meghatározott tényállást, ugyanis a közérdekű üzem és az irányelv által alkalmazott kritikus infrastruktúra fogalma eltér egymástól. [3] Ez különösen annak tükrében érdekes, hogy az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK irányelvet implementáló hazai jogszabály [12] pedig létfontosságú rendszerelemként jelöli a kritikus infrastruktúrákat. Így fordulhat elő, hogy a magyar szabályozásban két külön fogalom, eltérő jelentéstartalommal jelöli ugyan azt az uniós jogban meghatározott fogalmat. A minősített esetben foglalt cselekmény azonban nagyon is valós veszélyt jelent a társadalomra. Nagyszámú IoT eszköz egyidejű aktiválásával (például légkondicionáló berendezések, vízforralók és egyéb nagy áramfogyasztású háztartási elektronikai eszközök) ugyanis a támadók komoly terhelésnek tehetik ki az elektromos rendszert, amely szélsőséges esetben áramkimaradáshoz, áramszünethez is vezethet.

Tekintettel a kiberbűnözés természetére, valamint arra, hogy manapság az információs rendszer vagy adat megsértéséhez szükséges programok, tudás, felhasználói azonosítók

ellenérték fejében vagy akár ingyen is hozzáférhetőek az interneten, szükséges már az előkészítő cselekmény kriminalizálása is. A tagállamok kriminalizációs kötelezettségét az Irányelv is rögzíti.[8] A törvény alapján információs rendszer védelmét biztosító technikai intézkedés kijátszásának vétségét követi el aki az információs az információs adat vagy rendszer megsértéséhez szükséges jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez, vagy forgalomba hoz, illetve jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja. A vétség két évig terjedő szabadságvesztéssel büntetendő.

ELJÁRÁSI KÉRDÉSEK

A kiberbűnözés fentebb már ismertetett sajátosságai miatt nem egyszerű annak a kérdésnek megválaszolása, hogy a bűncselekmény elkövetését követően ki jogosult eljárni, mely szervek rendelkeznek hatáskörrel és illetékességgel. Elsősorban a joghatóságot kell megvizsgálni, azaz, hogy az adott bűncselekmény vonatkozásában mely állam jogosult megindítani a nyomozást és lefolytatni a büntetőeljárást. Erre vonatkozóan az Irányelv előírja, hogy a tagállamok megállapítják joghatóságukat az alábbi esetekben:

- az információs rendszer elleni bűncselekményt egészben vagy részben a területükön követték el, vagy
- egy állampolgáruk követte el, legalább azokban az esetekben, ha a cselekmény az elkövetés helyén bűncselekménynek minősül.

Egy bűncselekmény akkor minősül a fenti i) pont szerint az adott tagállam területén elkövetettnek, amennyiben az elkövető a bűncselekmény elkövetésekor fizikailag jelen van a területükön, függetlenül attól, hogy a bűncselekmény a területükön található információs rendszer ellen irányul-e; vagy a bűncselekmény a területükön található információs rendszer ellen irányul, függetlenül attól, hogy az elkövető a bűncselekmény elkövetésekor fizikailag jelen van-e a területükön. Az Irányelv alapján a tagállamok megállapíthatják joghatóságukat abban az esetben is, ha az elkövető szokásos tartózkodási helye a tagállam területén van, vagy a bűncselekményt a területükön letelepedett jogi személy javára követték el.[9] A Btk. területi és személyi hatályára vonatkozó rendelkezései alapján a magyar büntető törvényt kell alkalmazni a belföldön elkövetett bűncselekményre, a magyar állampolgár által külföldön elkövetett olyan cselekményre, amely a magyar törvény szerint bűncselekmény, valamint a magyar állampolgár, magyar jog alapján létrejött jogi személy és jogi személyiséggel nem rendelkező egyéb jogalany sérelmére nem magyar állampolgár által külföldön elkövetett olyan cselekményre is, amely a magyar törvény szerint büntetendő. A magyar hatóságok joghatósága tehát mind abban az esetben biztosított, amikor magyar állampolgárságú személyek belföldön vagy külföldön követik el az információs rendszerek elleni bűncselekményt, mind abban az esetben, amennyiben külföldi személyek magyar állampolgárok terhére külföldön követik el a bűncselekményt. Tekintettel a kiberbűnözés nemzetközi jellegére, a joghatóság megállapítása nem mindig olyan egyszerű, mint azt a fenti szabályok alapján gondolni lehetne. Ezek a bűncselekmények ugyanis gyakran több országban valósulnak meg, az áldozatok között több ország állampolgára is van (például egy nulladik napi

[8] Irányelv 7. cikk
[9] Irányelv 12. cikk

támadás érint egy IoT termék összes eszközét) vagy pedig maguk az elkövetők szerveződnek több országból.

A fent ismertetett információs rendszerrel kapcsolatos bűncselekményekre a rendőrség hatásköréről és illetékességéről szóló jogszabály [13] a Készenléti Rendőrséget jelöli ki [10], mint a nyomozásra hatáskörrel rendelkező szerv. A nyomozás során a nyomozó hatóság felkutatja, megismeri és rögzíti a bűncselekmény alapjául szolgáló adatállományt, az információs rendszerben megtalálható elektronikus nyomokat és bizonyítékokat. [14] Beszerzi továbbá a naplófájlokat és a regisztrált adatokat. Ezek a naplózott adatok kiemelt szerephez juthatnak a fentebb ismertetett bűncselekmények kísérletének bizonyítása során.

KÖVETKEZTETÉSEK

Amint arra a bevezetőben már utalás történt, a számítástechnika fejlődése és a mindent átszövő digitalizáció napjainkra már az élet minden részén érezteti hatását. Ennek a fejlődésnek azonban árnyoldalai is vannak, a kiberbűncselekmények és a kibertámadások száma ugyanis évről évre nő. Ez egyrészt összefügg azzal a ténnyel, hogy egyre több a felhasználó és egyre több a támadási felületként szolgáló információs rendszer, másrészt pedig azzal, hogy ezen cselekmények elkövetéséhez szükséges tudás, hardware és szoftverek átlagember számára is könnyedén hozzáférhetőek. A hackerek és a szervezett bűnözői csoportok jellemzően több országból szerveződve hajtanak végre bűncselekményeket nagy számú, különböző országban élő áldozattal szemben. Ebben a környezetben a rendkívül dinamikusan növekvő számú IoT eszköz jelentős információbiztonsági kihívást jelent. Amint az fentebb ismertetésre került, az Irányelv és az alapján a Btk. csak a védett eszközökbe történő jogosulatlan belépést szankcionálja. A büntetőszabályozás mindenképpen szükséges, de nem elégséges megoldása ennek az egyre növekvő problémának.

Az IoT eszközök egy jelentős részénél semmilyen védelmi mechanizmus nincs beépítve, az eszközökön futó szoftverek nem kerülnek frissítésre és az adatok továbbítása sem titkosított. Ebből adódóan a kiszivárgott, napvilágot látott hibák, sérülékenységek sem kerülnek sokszor javításra, kiszolgáltatva ezeket az eszközöket és felhasználóikat. Nem véletlen, hogy a különböző szakmai szervezetek által kidolgozott ajánlások, iránymutatások és szabványok mind tartalmazzák ezeket az alapvető védelmi intézkedéseket. Jelenleg az Európai Unióban egyedül Nagy-Britanniában van nyilvános konzultáció és kidolgozás alatt egy tervezet a fogyasztóknak szánt (angolul B2C vagy business to consumer) IoT eszközökre vonatkozó kötelezően alkalmazandó biztonsági követelményekről [15] Amennyiben ez a trend folytatódik és a nemzeti kormányok saját IoT keretrendszert fogadnak el eltérő módon szabályozva a védelmi intézkedésekkel szemben támasztott minimum követelményeket, akkor az az Európai Unió digitális belső piacának felaprózódásához vezethet. Ez a folyamat egyúttal jelentősen megnövelné a gyártók számára a piacra lépéssel és a jogszabályi megfeleléssel kapcsolatos költségeit. Erre megoldást jelenthetne egy egységes európai követelményrendszer, ilyen azonban jelenleg még nem került elfogadásra. Az Európai Távközlési Szabványosítási Intézet (angolul European Telecommunications Standards Institute vagy ETSI) 2020. június 30-án jelentette be az ETSI EN 303 645 szabványát, amely a fogyasztói IoT eszközök számára alapvető követelményeket határoz meg. [16] Ez az európai szabvány, amennyiben Európai Uniós jogforrás előírná alapul szolgálhatna egy egységes

[10] 2. Melléklet 22. k

európai tanúsítási mechanizmusnak, a védelem egységes minimumszintjét garantálva a belső piacon forgalomba bocsájtott IoT termékek esetén.

FELHASZNÁLT FORRÁSOK

[1] A digitális gazdaságra és társadalomra vonatkozó statisztikák – háztartások és magánszemélyek [Online] Elérhető: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals
[2] Recommendation ITU-T Y.2060, 2012. [Online] Elérhető: http://handle.itu.int/11.1002/1000/11559
[3] Mezei, Kitti (2018) A kiberbűncselekmények hazai szabályozásának aktuális kérdései. In: Magyar Jogászegyleti Értekezések. Magyar Közlöny Lap- és Könyvkiadó; Magyar Jogász Egylet, BUDAPEST, pp. 157-173.
[4] Gyaraki Réka (2018) A számítógépes nyomozás problémái, PhD értekezés, PÉCS
[5] Cyber Security and Resilience of smart cars - Good practices and recommendations. 201. [Online] Elérhető: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars
[6] 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről
[7] AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2013/40/EU IRÁNYELVE (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról
[8] Büntető Törvénykönyvről szóló 2012. évi C. törvény
[9] Akácz József; Belegi József; Katona Sándor; Kónya István; Márki Zoltán; Mészár Róza; Molnár Gábor Miklós; Soós László (2020) Magyar Büntetőjog I-III. - új Btk. - Kommentár a gyakorlat számára, HVG-ORAC Lap- és Könyvkiadó, Budapest
[10] Robothálózat (Botnet) [Online] Elérhető: https://nki.gov.hu/it-biztonsag/tudastar/robothalozat-botnet-2/
[11] IoT botnets might be the cybersecurity industry's next big worry [Online] Elérhető: https://bdtechtalks.com/2016/07/12/iot-botnets-might-be-the-cybersecurity-industrys-next-big-worry/
[12] 2012. évi CLXVI. Törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
[13] 25/2013. (VI. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről
[14] Kiss, Tibor, ed. (2020) Kibervédelem a bűnügyi tudományokban. Dialóg Campus Kiadó, Budapest. ISBN 9789635310302, p. 59.
[15] Mandating security requirements for consumer 'IoT' products [Online] Elérhető: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/798722/Secure_by_Design_Consultation_Stage_Regulatory_Impact_Assessment.pdf
[16] ETSI EN 303 645 V2.1.1 (2020-06) szabvány [Online] Elérhető: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf