MEZEI KITTI[1]

A kiberbűncselekmények hazai szabályozásának aktuális kérdései

1. Bevezetés

A számítógépek[2] mindenütt jelen vannak az életünkben, az egyes társadalmi és gazdasági folyamatok egyre inkább függnek az információs rendszerektől. Az informatikai és technológiai fejlődésnek az előnyei mellett megvannak a veszélyei is, hiszen a modern technológiák adta lehetőségeket a bűnözők is kihasználják. Ennek köszönhetően egy új típusú bűnözés jelent meg: az informatikai vagy másnéven kiberbűnözés *(cybercrime).* Különösen veszélyes, határokon átívelő bűnözésről van szó, amelyet magas fokú látencia jellemez, az anonimitás kedvez a bűncselekmény elkövetőinek, az elkövetés gyorsasága miatt a bűnelkövetők helyzete könnyű, míg a nyomozóhatóságok szempontjából nehéz a felderítés, a sértettek nagy száma köszönhető az Internet, az új technológiák mint a mobil eszközök és az Internet of Things népszerűségének, illetve a könnyelmű felhasználók sértetti közrehatásának.[3] Az Internet használatának elterjedése színteret biztosít a hagyományos és új típusú, informatikai bűncselekmények vagy kiberbűncselekmények elkövetéséhez, amelyeknek nincs egységes elnevezése, sem fogalommeghatározása. Azonban két fő kategóriájuk különböztethető meg: az egyik azon deliktumok csoportja, amelyeknek tárgya az információs rendszer, tehát amikor a támadás számítógépek ellen irányul (ún. *„cyber-dependent"* bűncselekmények), míg a másik, amikor hagyományos bűncselekményeket valósítanak meg az információs rendszerek felhasználásával mint például ilyen a csalás, gyermekpornográfia, zaklatás stb. (ún. *„cyber-enabled"* bűncselekmények), ekkor az információs rendszer a bűncselekmény eszköze.[4]

A tanulmány a hazai szabályozását mutatja be a kiberbűncselekményeknek, azonban először röviden kitér azokra a nemzetközi dokumentumokra, amelyek meghatározóak voltak az új Büntető Törvénykönyvről szóló 2012. évi C. törvényre (a továbbiakban: Btk.). A 2001-es *Számítástechnikai Bűnözésről szóló Egyezményt* (a továbbiakban: Budapesti Egyezmény) írta

[1] tudományos segédmunkatárs (MTA Társadalomtudományi Kutatóközpont Jogtudományi Intézet), doktorandusz (Pécsi Tudományegyetem Állam- és Jogtudományi Kar)

[2] A számítógép kifejezést alatt értem a laptopokon és asztali gépeken kívül a mobil és okoseszközöket is mint a táblagépeket, okostelefonokat vagy a szervergépeket és akár egyes nyomtatókat is és még sorolhatnám.

[3] GYARAKI Réka: Aszámítógépes környezetben elkövetett gazdasági báncselekmények – A PIN kód megadása sikeres vagy biztonságos az internet?! Pécsi Határőr Közlemények XIII. Pécs, 2012. 235-236. o.

[4] CLOUGH, Jonathan: Principles of cybercrime. Cambridge University Press, 2015. 10-11. o.
POLT Péter: A számítógépes bűnözés. Belügyi Szemle. 1983/6. 60-64. o.

alá és ratifikálta a legtöbb ország. A Budapesti Egyezmény volt az első olyan multilateriális jogi dokumentum e területen, amely egységes definíciót nyújtott a számítástechnikai fogalmakhoz, valamint rendszerezte a büntető anyagi jogi tényállásokat és már eljárásjogi kérdésekkel is foglalkozott. Az Európai Unióban *az információs rendszerek elleni támadásokról szóló 2013/40/EU irányelv* váltotta a 2005/222/IB tanácsi kerethatározatot, amely két fő célt tűzött ki: a minimumszabályok meghatározását az információs rendszer elleni bűncselekményekre, valamint a büntetőjogi szankciókra vonatkozóan és az együttműködés elősegítését a tagállamok illetékes hatóságai, illetve az Unió illetékes szakosított ügynökségei és szervei között.

A tanulmány a Budapesti Egyezmény csoportosítása szerinti I. címben szereplő „számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekményekkel" foglalkozik, illetve az irányelv 3-7. cikke szerinti bűncselekményekkel: az információs rendszerekhez való jogellenes hozzáféréssel, a rendszert és adatot érintő jogellenes beavatkozással, a jogellenes adatszerzéssel és a bűncselekmények elkövetéséhez használt eszközök biztosítása. Ezen belül is a következő büntetendő magatartásokkal, amelyek tisztán informatikai bűncselekménynek minősülnek:

1. jogosulatlan belépés (az ún. *hacking*),
2. információs rendszer jogosulatlan akadályozása (pl. DDoS támadás),
3. információs rendszerben tárolt adat jogosulatlan megváltoztatása, törlése vagy hozzáférhetetlenné tétele (pl. rosszindulatú programok révén).

Ezek a műveletek technikailag lehetnek rendkívül bonyolultak vagy kifejezetten egyszerűek. Az elkövetők lehetnek „külső" személyek, akár tapasztalt hackerek[5], akik valódi veszélyt jelentenek, azonban ugyanúgy a „belső" emberek is forrásai lehetnek a támadásoknak.

2. Az információs rendszer elleni bűncselekmények

2.1. Az információs rendszer és adat megsértése

Az uniós irányelvnek megfelelően – eleget téve a jogharmonizációs kötelezettségnek - az új Btk. átalakította az informatikai bűncselekményekre vonatkozó szabályozást mind elnevezésben és mind tartalmilag: külön a XLIII. fejezetbe kerültek a *„A tiltott adatszerzés és információs rendszerek elleni bűncselekmények"* címmel, illetve a korábbi „számítástechnikai rendszer" terminológia helyébe az „*információs rendszer"* lépett, ami a kor kihívásainak jobban

[5] A hacker nem szinonim kifejezés a bűnözővel. Vannak etikus hacker, (angol kifejezéssel „white hat hacker" képzés), akikre honvédelmi, rendőrségi feladatok teljesítése hárul. Létezik önkéntes kiberhadsereg is, amely együttműködik a megfelelő szervezetekkel.

megfelel. Az új Btk. a 423. §-ban szabályozza az információs rendszer vagy adat megsértését, mely bűncselekménynek a jogi tárgya az információs rendszerek megfelelő működéséhez és a bennük tárolt, feldolgozott, továbbított adatok megbízhatóságához, hitelességéhez, valamint a titokban maradásához fűződő érdek.[6] Lényeges azonban kiemelni, hogy ez a tényállás továbbra is csak a számítástechnikai jellegű, szoftveres úton elkövetett támadások ellen biztosít büntetőjogi védelmet. Magának a számítógépnek a mechanikus védelmét tehát ma is a rongálás törvényi tényállása látja el.[7]

A törvény három külön fordulattal határozza meg a bűncselekmény elkövetési magatartásait és valamennyi fordulatának az elkövetési tárgya *az információs rendszer*, amelynek a betöltött funkciója a meghatározó.[8] Információs rendszer minden olyan berendezés - vagy egymással kapcsolatban lévő ilyen berendezések összesége -, amely automatikusan végez adatfeldolgozást, azaz adatok bevitelét, kezelését, tárolását, továbbítását látja el.[9] Az információs rendszerek körébe tartoznak a számítástechnikai adatfeldolgozásra épülő memóriával rendelkező olyan egységek is, amelyek megjelenésükben eltérnek a "hagyományos" számítógépektől (pl. közcélú távbeszélő-szolgáltatás, információs rendszerek felhasználásával működő hírközlési, telekommunikációs rendszerek stb.).[10]

A Btk. 423. § (1) bekezdésében szabályozott első fordulata értelmében büntetendő, *aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad,* vétség miatt két évig terjedő szabadságvesztéssel büntetendő. A *jogosulatlan belépés* megvalósulhat egyszerűen egy engedély nélküli, jogosulatlan belépéssel vagy összetettebb módon is például, amikor az elkövetők egy számítógépes hálózatot használnak fel arra, hogy távoli hozzáférést szerezzenek, mindez gyakran különböző joghatóság alá tartozó számítógépek közbeiktatásával történik. Ezek megvalósulhatnak felhasználó szintű műveletekkel, vagyis amikor az átlag felhasználónak megfelelő hozzáféréssel történik, vagy ún. *„root level access”*, illetve *„god level access”* szintű hozzáféréssel, amikor ugyanazokkal a jogosultságokkal rendelkeznek mint a rendszergazda, és ezáltal lehetőségük van a rendszerben tárolt valamennyi fájl, adat megtekintéséhez és

[6] KARSAI Krisztina: XLIII. fejezet Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In: Karsai Krisztina (szerk.): Kommentár a Büntető Törvénykönyvhöz. Complex Kiadó. Budapest, 2013. 898. o.
[7] MOLNÁR Gábor: XLIII. fejezet – Tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In: Kónya Sándor (szerk.): Magyar Büntetőjog - Kommentár a gyakorlat számára (Harmadik kiadás). HVG-ORAC Budapest, 2016. 946. o.
[8] TÓTH Mihály: Alkothatók-e az informatikai bűnözés változatos formáit lefedni képes büntetőjogi tényállások? In: Gál István László–Nagy Zoltán András (szerk.): Informatika és büntetőjog. PTE ÁJK. Pécs, 2006. 184. o.
[9] Btk. 459.§ (1) bekezdés 15. pont
[10] MOLNÁR: i.m. 946. o.

módosításához. A szoftverek gyors ütemű fejlesztésének köszönhetően elkerülhetetlenek a programhibák, amiket az elkövetők sokszor kihasználnak mielőtt még ezeket a szoftverfejlesztők kijavítanák például különösen veszélyesek az *ún. nulladik napi („zero-day") támadások*, amelyek olyan, eddig nem ismert sebezhetőséget használnak ki, amitől még nem tudnak a programkészítők, illetve a felhasználók.

Az (1) bekezdésben meghatározott enyhébb súlyú alapeset az információs rendszerbe történő jogosulatlan belépést nyilvánítja büntetendő cselekménnyé, amelynek két esete különböztethető meg. A jogosulatlan belépés irányulhat az elkövető által felhasznált számítógépre vagy az ezen keresztül elérhető védett számítógépes hálózatra (pl. intézményi belső hálózat, ún. intranet vagy az Internet részét képező hálózat mint egy banki hálózat stb.).

A bűncselekmény megállapításához szükséges, hogy *az információs rendszer technikai intézkedésekkel biztosított védelemmel legyen ellátva és ez a védelem aktív legyen*, azaz rendelkezzen felhasználó azonosítóval és jelszóval, tűzfallal vagy egyéb védelemmel. Tehát nem jogosulatlan a belépés, ha az információs rendszer nem védett, illetve a védelem nincs aktiválva, mert ezek konjuktív feltételek.[11] Az (1) bekezdésben meghatározásra került az *elkövetési mód* is, így a bűncselekmény megvalósul, akkor ha, a belépés a védelmi intézkedés megsértésével vagy kijátszásával történik például a biztonsági rendszer hiányosságait kihasználva lép be jogosulatlanul vagy a jogosult jelszavával vagy belépési kódjával, amelynek megszerzési módja azonban közömbös (pl. megtévesztéssel, kifürkészéssel, kódtörő programmal, *social engineering*, vagyis pszichológiai manipulációval[12] vagy a felhasználó hanyagsága folytán jut hozzá az elkövető). Különösen veszélyesek *az adathalász (phishing)* támadások, mert alkalmasak a könnyelmű felhasználók adatainak a megszerzésére például amikor az elkövetők megtévesztő módon a pénzintézetek nevében küldenek adatkérő e-mailt.

A jogosulatlan belépésnek egy tipikus esete az ún. *„wardriving"* vagy „*wireless hacking"*, amikor a vezeték nélküli hálózatot használják jogosulatlanul. A WiFi kapcsolatok kialakításának több formája van: vannak a nyilvános hálózatok, amelyekhez bárki szabadon csatlakozhat, mindenféle korlátozás nélkül. Nyilvános, de zárt hálózatok is lehetnek, amelyek esetében egy speciális szoftver gondoskodik arról, hogy a hálózatot egy kód ismeretében lehet

[11] NAGY Zoltán András: XLIII. fejezet tiltott adatszerzés és az információs rendszer elleni bűncselekmények. In: Tóth Mihály – Nagy Zoltán András (szerk.): Magyar Büntetőjog: Különös rész. Osiris Kiadó, Budapest 2014. 594-595. o.

[12] MITNICK, Kevin D.: A megtévesztés művészete című könyvnek a borítója: „A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja, vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni."

használni korlátozott ideig. Emellett vannak privát hálózatok, amelyek esetében a hozzáférést titkosítás, tűzfal és jelszó használatával korlátozzák. Ezek a hálózatok saját használatra lettek kialakítva és jelszóvédelemmel vannak ellátva, amelynek ismeretében lehet ezekhez csatlakozni. Azonban előfordul, hogy a tulajdonos akaratlanul a hálózatot védelem nélkül „nyitva" hagyja. Amennyiben a felhasználó az adatforgalom után fizet a szolgáltatója felé, akkor jelentős kárt okozhat nála a jogosulatlanul rácsatlakozó személy. A WiFi hálózatok további veszélyforrást jelentenek, mert rajtuk keresztül jogosulatlanul betudnak lépni a számítógépes rendszerekbe, illetve lehetőség van a hálózaton keresztül továbbított kommunikáció kifürkészésére is. Azonban csak akkor valósítja meg a hálózatot jogosulatlanul használó személy a 423. § (1) bekezdését a „WiFi-lopással"[13], ha a hálózat aktív védelemmel van ellátva és ezt sérti meg, különben nem.[14]

A második eset, amikor megvalósul a bűncselekmény, ha az elkövető az engedélyezett belépést követően *a jogosultságának terjedelmi vagy időbeli kereteit meghaladja*, illetve a jogosultságot más módon megsérti *az információs rendszerben való bennmaradással* szándékosan. A büntetőjog alapelveivel összhangban a jogosultság keretein való túllépés is akkor minősül bűncselekménynek, ha az egyben a rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával történik, ugyanis akkor, ha valakinek van jogosultsága az információs rendszerbe történő belépéshez, akkor pusztán e jogosultság kereteinek túllépése nem éri el azt a veszélyességi szintet, mint amit az első fordulat megkíván.[15] Tehát önmagában a jogosultság kereteinek túllépésével való belépés vagy bennmaradás nem büntetendő, amennyiben nem valamely biztonsági intézkedés megsértésével valósul meg, vagy nem kapcsolódik össze semmilyen további célzattal - pl. jogtalan hátrányokozási, haszonszerzési célú adatszerzéssel vagy manipulálással, vagy a rendszer megzavarásának a szándékával -, mert a magatartás társadalomra veszélyessége csekély.[16] E fordulat alaki bűncselekményt határoz meg. Kísérlet - egyebek mellett - akkor állapítható meg, ha az elkövető megpróbálja kijátszani a számítógép védelmét, de még nem sikerült belépnie. E fordulat kísérletének gyakorlati jelentősége egyre jelentősebb, különösen annak függvényében, hogy az egyes rendszerek az eredménytelen belépési kísérleteket is regisztrálják.[17]

[13] Lásd BLUTMANN László - KARSAI Krisztina - KATONA Tibor: Miért nem lehet a vezeték nélküli internet a lopás elkövetési tárgya? Bűnügyi Szemle, 2008/1. I. évfolyam 1. szám 42-49.o.
[14] NAGY Zoltán András: Bűncselekmények a számítógépes környezetben. Ad librum. Budapest, 2009. 272-273. o.
[15] BH 2017.12.392.
[16] PARTI Katalin: Gondolatok a számítástechnikai adatok és rendszerek elleni bűncselekmények tényállásairól. Büntetőjogi Kodifikáció 2005/2. 38. o.
[17] MOLNÁR: i.m. 947. o.

Az egyes jogosulatlan belépések mögött húzódó motivációk különbözőek lehet, de alapvetően a következőket érdemes kiemelni, mert leggyakrabban a következők fordulnak elő: információhoz hozzáférés, adat módosítás, a számítógép használata.[18]

Az adat az új olaj. Napjainkban tömérdek mennyiségű adatot tárolnak az információs rendszereken és hálózatokon, ami egyértelműen megadja a motivációt e információkhoz való jogosulatlan hozzáféréshez. Jellemző, hogy erre éppen ezért kerül sor, hogy bizalmas gazdasági, üzleti vagy államtitkokat szerezzenek meg vagy személyes adatokat (pl. egészségügyi nyilvántartásban tárolt adatokat, bankkártya adatokat stb.). A felhő-alapú tárhelyeknek a magán és üzleti célú használata is egyre népszerűbb, ezért ezek is egyre gyakrabban válnak a támadások célpontjaivá.[19] Az elkövető további célja lehet a jogosulatlan belépés révén, hogy az információs rendszerben tárolt adatokat módosítsa. Ha a belépést követően az információs rendszerben tárolt, feldolgozott, továbbított adatok megváltoztatására, törlésére is sor kerül, akkor ez a cselekmény már a (2) bekezdés b) pontja szerinti bűncselekményt valósítja meg, amelybe a jogosulatlan belépés beleolvad a súlyosabb jogtárgysértésre figyelemmel.[20]

Az információs rendszerrel való visszaélés másik gyakori esete, amikor a jogosulatlan belépésre azért kerül sor, hogy a célzott számítógépet használják, amire nem lennének jogosultak. Számos eset van, amikor nincs szükség a büntetőjog alkalmazására, mert nincs jelentős következménye a jogosulatlan használatnak mint például a nem munkavégzési céllal történő számítógép használat esetében a munkajogi rendelkezések alkalmazása a célravezető, azonban vannak olyan körülmények, amikor a jogosulatlan használatnak jelentős következményei vannak. Például a használat során hozzáférnek kereskedelmi adatbázisokhoz, amellyel az elkövetők ingyen hozzájuthatnak értékes szolgáltatásokhoz. A jogosulatlan belépés irányulhat arra is, hogy sokkal erősebb számítógépeket tudjon használni az elkövető azzal a céllal, hogy olyan programokat futtasson (pl. ún. *„brute-force”* jelszó feltörő programokat), amelyekhez nagyobb kapacitású hardverrel felszerelt számítógépre van szükség. Ezzel kapcsolatban újdonságként említhető további példa, amikor a számítógépeket Bitcoin bányászásra használják fel.

Az elkövető továbbá szándékosan, jogosulatlanul hozzáférhet több számítógéphez azért, hogy a közbeiktatásuk révén elrejtse a személyazonosságát és/vagy a bűncselekmény

[18] CLOUGH: i.m. 31-38. o.
[19] CLOUGH: i.m. 33-34. o.
[20] SZATHMÁRY Zoltán: A számítástechnikai bűncselekmények és rendszertani elhelyezésük. Jogtudományi Közlöny 2012/4. 173-174. o.

elkövetésének helyét. Az információs rendszerekben különböző módon tudnak kárt okozni: aki jogosulatlan hozzáférést szerez a számítógép felett, képes olyan parancsot küldeni, ami a számítógép működéséhez szükséges fájlok törlését vagy a számítógép leállítását eredményezi. Az elkövetők különféle *„malware”*-t vagyis rosszindulatú programokat továbbíthatnak, amivel a gyanútlan felhasználók számítógépét fertőzhetik meg. A malware a „malicious software” angol megfelelőjének a rövidítése, a rosszindulatú szoftver szavak összevonásából áll. Általában arra használják ezeket a kártevő programokat, hogy jogosulatlanul behatoljanak az információs rendszerekbe, vagy módosításokat végezzenek, kárt okozzanak az adatokban, de egyre gyakoribb, hogy azzal a céllal használják fel ezeket, hogy bizalmas adatokhoz férjenek hozzá, amelyek elősegítik a további csalásokat vagy egyéb jogsértéseket.[21] Amennyiben a jogosulatlan belépést követően olyan meg nem engedett műveleteket hajt végre az elkövető, aminek következtében az információs rendszer működését akadályozza, akkor a (2) bekezdés a) pontja szerinti fordulatot valósítja meg, így ha az elkövető az információs rendszer adatfeldolgozás eredményét a vírusok becsempészésével tudatosan befolyásolja, hogy ezáltal a programok működésre képtelenné váljanak, akkor is megvalósítja ezt a fordulatot.[22]

Különböző típusú malwareket ismerünk és sokszor alig különböznek egymástól, ezért nehéz csoportosítani őket, de az alábbi fő kategóriák határozhatók meg: vírusok[23], férgek[24], trójai programok[25], kémprogramok[26].[27]

A legnagyobb veszélyt az elmúlt években *a zsarolóvírusok (ransomware)* jelentették, mely kártékony programok úgy működnek, hogy a megfertőzött számítógépen vagy mobil eszközökön tárolt fájlokat, akár a teljes adatállományt letitkosítják, ezáltal a sértett számára teljesen elérhetetlenné téve azokat, majd rendkívül magas, akár milliós nagyságrendű

[21] CLOUGH: i.m. 36-38. o.
[22] BH 1999.145.
[23] A számítógépes vírusok olyan kártékony szoftverek, amelyek képesek önmaguk lemásolására és megfertőzni a számítógépeket, amelyhez szükségük van egy hordozóra, gazdagépre, ami a számítógépes kód, tehát lényegében úgy viselkednek mint a biológiai vírusok.
[24] A számítógépes férgek ezzel szemben önmagukat reprodukálják anélkül, hogy fertőznének - és ezért nincs szükségük hordozóra. A számítógépes hálózatok hibáit, vagy hiányos biztonsági beállításokat használják fel, hogy terjeszkedjenek. Manapság a legveszélyesebb programok ebből a típusból kerülnek ki, elsősorban a gyors terjedésük miatt. Az önsokszorosításon kívül a férgek többféle dologra is programozhatóak. Egyik jellemző következményük, hogy hátsó ajtót (backdoor) nyitnak a rendszerekre, amin keresztül adatokat szereznek meg, illetve botnet hálózat részévé tehetik a megtámadott számítógépet.
[25] A trójai programok ártalmatlannak tűnnek, - sőt sokszor más hasznos programnak álcázzák magukat, így a gyanútlan felhasználósaját maga tölti le ezeket - de rejtett káros tevékenységet végeznek anélkül, hogy önmagukat sokszorosítanák. Ezeket programokba, e-mail mellékletekbe, weboldalakba illeszthetik vagy terjedhet adathordozón keresztül is. A trójai is alkalmas lehet a hátsó ajtó létrehozására az érintett rendszerben.
[26] A kémprogramok (sypware) olyan káros szoftverek összessége, amelyek a megfertőzött számítógép felhasználójának bizalmas adatait (pl. személyazonosító, banki vagy más személyes adatokat) igyekeznek megszerezni. Ezeket általában böngészési szokásaink megfigyelésére – és az így megszerzett információ alapján célzott reklámokat, hirdetéseket küld a felhasználó gépére -, illetve visszaélések elkövetésére használják fel.
[27] CLOUGH: i.m. 39. o.

váltságdíjat követelnek a helyreállító, titkosítást feloldó kódért cserébe. A szoftver fizetési határidőt is szabhat, melynek lejárta után akár végérvényesen elérhetetlenné teszik az adatokat. Az elkövetők kilétének megismerése szinte lehetetlen, mert általában a „váltságdíjat" a nehezen lenyomozható *virtuális valutában, ún. kriptovalutában*[28] *mint a Bitcoin*[29] *vagy valamely altcoinban kérik.* A pénz kifizetése sem garancia arra, hogy a zsaroló a titkosítást feloldja. 2017-ben a WannaCry zsarolóvírus az egész világon végig söpört, mert egyedi módon féregként viselkedve egy hálózaton belül valamennyi számítógépet megfertőzött így például Nagy-Britanniában kórházak, illetve Németországban a vasútvállalat gépeit blokkolta teljesen.[30]
Különösen veszélyes még az adathalászatnak a célzott változata az ún. *spear phishing*, amikor kisszámú, kiszemelt felhasználók (pl. banki alkalmazottak, könyvelő stb.) személyre szabott e-maileket kapnak egy kártékony csatolmánnyal és a cél, az hogy az áldozat a mellékletet megnyissa és aktiválja a rosszindulatú programot, ezért az üzenet célzott, ami azt jelenti, hogy tartalma valamilyen valós élethelyzetre, eseményre, tevékenységre utal, ami miatt a célpont azt hiszi, hogy az üzenet valós.[31]

További kiberbiztonsági kockázatot az egyedi hatású és célzott támadásokra kifejlesztett rosszindulatú programok jelentik különösen, amelyek a kritikus infrastruktúrákat támadják. 2010-ben a *Stuxnet* volt az első komoly célzott támadás, amelyet ipari rendszerek ellen vetettek be. Az első kártékony kód volt, amely a kritikus infrastruktúra elemeinek a fizikai károkozásával is járt – sőt ezzel a céllal fejlesztették ki- és, ezáltal Irán atomprogramját lényegében megbénították, mert több év kellett ahhoz, hogy egy atomfegyver előállításához

[28] A kriptovaluta egy olyan digitális fizetőeszköz, amit nem szigorúan szabályozott keretek között, felügyeleti engedéllyel, vagy a kormány felhatalmazásával rendelkező intézmény bocsát ki, hanem komplex matematikai feladatokat megoldó számítógépek hálózata. A blockchain a kriptovaluták alapjául szolgáló technológia, egy decentralizált, megosztott adatbázis, de hívják megosztott főkönyvnek is, amiből nem csak egy példány van, egy központi helyen tárolva és megosztva sok emberrel, hanem a nyilvántartási könyv másolatának ezrei találhatóak világszerte, otthon a számítógépen, vagy üzleti szervereken. Ebben a megosztott nyilvántartási könyvben egy blokk egy adatcsomagot takar, ami a pénzügyi tranzakciók esetében a tranzakciók listáját jelenti. A blokkot minden esetben időbélyeggel zárják le és digitális aláírással látják el. https://fintechzone.hu/bevezeto-kriptovalutak-es-blockchain-titokzatos-vilagaba/ [2018.04.21.]

[29] A Bitcoin elnevezés az első decentralizált elektronikus fizetési rendszerre és a kriptovalutára is utal. Decentralizált rendszer, mert a felhasználók közvetítő nélkül, közvetlenül egymással tudják lebonyolítani a tranzakciókat (Peer-to-Peer). A működése a felhasználók közös megegyezésén, bizalmán alapul és független, mert nem áll mögötte egyetlen ország, bank vagy más szervezet sem. A kliensszoftverre ingyenes és nyílt forráskódú, a tranzakciók nyilvánosak és nyomon követhetők. A tranzakciók lebonyolításához egy Bitcoin címre és privát kulcsra van szükség, utóbbival tud a felhasználó a Bitcoin pénztárcájához – ami nem más mint egy fájl „wallet.dat" néven - hozzáférni és utalásokat végezni. A privát kulcs egyfajta elektronikus aláírásként funkcionál. Pszeudoanonimitást biztosít, mert azonosítás és hitelesítés, illetve központi felügyeleti szerv nélkül működik, továbbá a Bitcoin cím egy fiókként funkcionál és nem köthető személyekhez. Kihívást jelent, mert nincs egységes jogi szabályázása még. Lásd: Eszteri Dániel: Bitcoin – Az anarchisták pénze vagy a jövő fizetőeszköze? Infokommunikáció és jog 2012/2. 71-78. o.

[30] http://www.hirado.hu/2017/05/15/vilagszerte-terjed-a-virusfertozes/ [2018.02.21.]

[31]https://www.hwsw.hu/hirek/49634/kaspersky-lab-rec-october-biztonsag-kartevo-sebezhetoseg.html [2017.02.28.]

szükséges dúsított uránt legyártsanak. Ma már tudjuk, a Stuxnet csak az első ilyen eszköz volt a sorban, testvérei a Duqu, a Gauss vagy a Flamer bizonyítják ezt.[32]

A 423. § (2) bekezdés a) pontja értelmében, *aki az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza* bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

A törvény azonban nem határozza meg a releváns elkövetési magatartásokat, ezért bármely cselekmény tényállásszerű lehet, amely az információs rendszer működésének akadályozását eredményezi. *Akadályozáson* nem kizárólag azt kell érteni, hogy a rendszer nem működik, vagy nem megfelelően működik, hanem azt is, *ha a rendszer nem alkalmas a rendeltetésének megfelelő feladat ellátására*. Amennyiben az információs rendszer pl. közhiteles nyilvántartás vagy más, az adatok hiteles igazolására szolgáló nyilvántartás, akkor akár a valótlan, akár a valódi adat jogosulatlan bevitele, megváltoztatása, törlése e nyilvántartások rendeltetésszerű használatát, működését is gátolhatja. Az elkövető tudatának át kell fognia azt a tényt, hogy cselekményével jogosulatlanul akadályozza az információs rendszer működését. Az elkövetési magatartás megkezdésével a kísérlet valósul meg és a tényállásszerű eredmény, az akadályozás bekövetkezésével válik befejezetté a bűncselekmény. A bűncselekmény e fordulatát nem csak az adatok bevitelére, megváltoztatására, törlésére és egyéb műveletek végzésére jogosulatlan személy, hanem arra jogosult személy is elkövetheti, azonban ehhez feltétel, hogy a beavatkozást szándékosan nem a jogosultsága keretei között, nem a rendeltetésének megfelelően, hanem a reá vonatkozó rendelkezések megsértésével végezze.[33]

A jogosulatlan akadályozásra példaként említhetők az *ún. elosztott szolgáltatásmegtagadással járó túlterheléses támadások* (angol megfelelője: *DDoS, avagy Distributed Denial of Service*). A DDoS támadás egy olyan támadási forma, amelynek a célja az információs rendszerek vagy hálózatok erőforrásainak oly mértékben történő túlterhelése, hogy azok elérhetetlenné váljanak, vagy ne tudják ellátni az alapfeladatukat (pl. ez eredményezheti a rendszer teljes leállását vagy nagymértékű lassulását). Az ilyen típusú elektronikus támadást intézők a jogosult felhasználókat akadályozzák a szolgáltatás igénybevételében[34] (pl. a honlap elérésében, e-mail fiókhoz, más banki vagy egyéb fiókokhoz való hozzáféréshez).[35] A DDoS támadás és egyben a kiberbűnözői infrastruktúra alapját az ún.

[32] NAGY Zoltán András: A kiberháború új dimenzió – a veszélyeztetett állambiztonság (Stuxnet, DuQu, Flame – a Police malware). Pécsi Határőr Tudományos Közlemények XIII., 2012. 225–226. o.
[33] MOLNÁR: i.m. 948. o.
[34] NAGY (2009): i.m. 115. o.
[35] http://www.cert-hungary.hu/ddos [2017.02.21.]

botnet[36] képezi, ami az egymással összekapcsolt ún. *„zombigépekből”* áll, amik a felhasználók tudta nélkül megfertőzött és távolról irányítható számítógépeket foglalják magukban. A kialakított botnet hálózatok különösen veszélyesek, mert mérhetetlen erőforrást biztosítanak az elkövetők számára a rendelkezésre álló számítógép kapacitás és sávszélesség tekintetében, amit feltudnak használni különféle kibertámadások végrehajtásához.[37] Az 2013/40/EU uniós irányelv először hívta fel a figyelmet *a botnetekre mint veszélyforrásokra*, mert felismerték, hogy általuk egyre veszélyesebb, ismétlődő és átfogó támadásokat tudnak végrehajtani, melyek gyakran kulcsfontosságú információs rendszereket (pl. kritikus infrastruktúrákat) érintenek. Az irányelv először állapított meg büntetőjogi szankciót a botnetek létrehozására, és ezek révén végrehajtott támadásokra, melyek súlyos kárt képesek okozni.

A honlaprongálás (defacement) is e fordulat szerint minősül, amikor a weboldal tartalmát alakítják át, írják felül a saját – szöveges vagy vizuális - tartalommal.

A (2) bekezdés b) pontja szerint büntetendő, *aki az információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz* bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.
A harmadik fordulatnak az elkövetési tárgya *az információs rendszerben lévő adat*. E § alkalmazásában adat: „információs rendszerben tárolt, kezelt, feldolgozott vagy továbbított 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.”

A büntetendő cselekmény *elkövetési magatartása* az adat megváltoztatása, törlése vagy hozzáférhetetlenné tétele, melyek tehát adatbevitellel történhetnek.

Az adat megváltoztatásán az adat tartalmának bármilyen módon történő módosítását értjük, amely akár megvalósulhat az adat felülírásával, kiegészítésével vagy részleges törlésével. A Legfelsőbb Bíróság ezt az elkövetési magatartást állapította meg abban az ügyben, ahol az ETR rendszerben a nem teljesített vizsgát jelölő adatot az elkövető eredményes vizsgára változtatta meg és ehhez a megfelelő érdemjegyet is hozzárendelte. Az információs rendszer és adat megsértésének tényállását valósítja meg a főiskola számítástechnikai hálózatának felügyeletét ellátó informatikusa, aki a hallgatók vizsgakötelezettségét és vizsgaeredményeit nyilvántartó

[36] A botnetek a DDoS támadások indításán kívül alkalmasak spamküldésre, adathalászatra, hálózat-figyelésre, billentyűzet-figyelésre, különböző rosszindulatú programok, ún. malware-k (pl. ransomware) terjesztésére, illetve az internetes reklámokhoz a klikkelések begyűjtésére.
[37] European Parliament’s Policy Department for Citizens’ Rights and Constitutional Affairs: Cybersecurity in the European Union and Beyond: Exploring the Threaths and Policy Responses. 2015. 36. o. http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf [2017.03.24.]

számítástechnikai rendszerben levő adatok jogosulatlan megváltoztatásával a vizsgát előírás ellenére nem tett hallgatóval kapcsolatban olyan adatokat rögzít a rendszerben, amelyek szerint a hallgató a meghatározott tantárgyból eredményes vizsgát tett.[38]

A törlés az adat megsemmisítését, teljes eltávolítását jelenti.

Az adat hozzáférhetetlenné tétele esetén nem valósul meg törlés, a rendszer továbbra is tárolja, de az elkövető az adatnak az elérhetőségét akadályozza meg például azzal, hogy jelszóval védett könyvtárban elrejti, titkosítja az adatállományt, vagy az általa ismert helyre (FTP-, cloud-, raid szerverre) másolja. A törvény már egyetlen adat megváltoztatását, törlését vagy hozzáférhetetlenné tételét büntetni rendeli. Az adat megváltoztatásának, törlésének, hozzáférhetetlenné tételének szándékos előidézésén túl a cselekmény tényállásszerűségének a megállapításához szükséges még, hogy e magatartásokat a megfelelő jogosultság (engedély) hiányában, illetve a jogosultság kereteit megsértve kövessék el. E körben *a rendszergazda rendelkezése az irányadó.*

A bűncselekmény az adat bármilyen módon történő módosításával befejezetté válik. Nem szükséges, hogy a cselekmény az adatfeldolgozás eredményét befolyásolja, vagy bármely egyéb hátrányos következmény bekövetkezzen.[39]

A minősített eset állapítható meg, ha a (2) bekezdésben meghatározott bűncselekmény *jelentős számú információs rendszert érint*, azonban a törvény nem határozza meg, hogy mi tekinthető jelentős számúnak, tehát a jogalkalmazókra hárul ez a feladat, hogy egy erre vonatkozó gyakorlatot dolgozzanak ki.[40] A minősített esetre is a DDoS támadás jó példa, hiszen a végrehajtása során a támadó sok száz vagy több ezer felhasználó gépei felhasználásával kísérel meg kapcsolatot létesíteni a megtámadott számítógéppel. E sok száz vagy ezer zombigép egy botnetet alkot, amit a támadó vezérel távolról. Az egyszerre küldött nagy mennyiségű adatkérés és továbbítás bénítja a megtámadott információs rendszert, ami kimerítheti a jelentős számú információs rendszer fogalmát.[41] A másik minősített eset esetén a büntetés két évtől nyolc évig terjedő szabadságvesztés, ha *a bűncselekményt közérdekű üzem ellen követik el*. A Btk. az értelmező rendelkezések között a 459.§ 21. pontjában meghatározza exemplifikatív felsorolással, hogy mi minősül közérdekű üzemnek: a közmű, a közösségi közlekedési üzem, az elektronikus hírközlő hálózat, az egyetem és a postai szolgáltató közérdekű feladatainak teljesítése érdekében üzemeltetett logisztikai, pénzforgalmi és informatikai központok és

[38] EBH 2009.2033. I.; BH 2009.264. I.
[39] MOLNÁR: i.m. 947-948. o.
[40] MOLNÁR: i.m. 950. o.
[41] NAGY (2014): i.m. 598. o.

üzemek. Ezzel a probléma az, hogy *a közérdekű üzem és a kritikus infrastruktúra fogalma*[42] *nem fedi egymást,* így a cselekmény minősítése vitatott lehet, különösen a szociális jólét, a közegészség intézményei ellen intézett támadások esetében. Erre azért is fontos felhívni a figyelmet, mert 2017 óta bevezetésre került az elektronikus egészségügyi rendszer, ami azt jelenti, hogy ettől kezdve valamennyi személyes adatot és az intézményi ellátási dokumentumokat elektronikus úton tárolnak, ezáltal fokozott veszélynek vannak kitéve az esetleges informatikai támadásokkal szemben. Az uniós irányelv is a kritikus infrastruktúra fogalmát alkalmazza, valamint súlyosabb szankció megállapítását teszi lehetővé, ha az információs rendszer elleni támadást bűnszervezetben követik el. A személyazonosság-lopást is büntetni rendeli, amikor az információs rendszer elleni bűncselekményt egy másik személy személyes adataival visszaélve követték el egy harmadik fél bizalmának elnyerése céljából, és ezáltal kárt okoztak a személyazonosság jogos tulajdonosának. Súlyosító körülményként kell figyelembe venni, ha az elkövetőnek alkalmazotti minőségében hozzáférése van az érintett információs rendszerek részét képező biztonsági rendszerekhez.[43]

A bűncselekmény valamennyi fordulata *szándékos bűncselekmény*, amely egyenes és eshetőleges szándék mellett egyaránt tényállásszerű. A *tettes* bárki lehet, aki a tényállásszerű elkövetési magatartásokat tanúsítja. Ennek megfelelően valamennyi fordulatát a megfelelő jogosultsággal rendelkező, illetve az ilyen jogosultsággal nem rendelkező személy tettesként egyaránt elkövetheti.

A bűncselekmények *rendbelisége* az informatikai rendszerek számához igazodik. A törvény valamennyi informatikai rendszer önálló büntetőjogi védelmét biztosítja függetlenül attól, hogy azok tulajdonosa, illetőleg üzemeltetője azonos vagy különböző természetes vagy jogi személy, illetőleg jogi személyiség nélküli szervezet.

Az egyes informatikai rendszerek sérelmére megvalósított akár azonos, akár különböző elkövetési magatartások száma a rendbeliséget rendszerint nem érinti. A következetes ítélkezési gyakorlatnak megfelelően a természetes egység keretében nyerhet értékelést.[44] Folytatólagosan elkövetett információs rendszer vagy adat megsértésének bűncselekménye állapítható meg, ha

[42] A Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló 2080/2008. (VI. 30.) kormányhatározat 1. sz. melléklet 3.2. pontja: „kritikus infrastruktúrának minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére".

[43] NAGY Zoltán András: A 2013/40-es uniós direktíva az informatikai rendszereket érő támadásokról. http://www.rendeszetelmelet.hu/Graphics/pdf/Nagy_Zoltan_Andras_A_2013_40_es_Unios_direktiva.pdf [2018.01.24.]

[44] MOLNÁR: i.m. 950-951. o.

az elkövető egységes akaratelhatározásból az azonos helyzetből (hozzáférésből) fakadó lehetőséget kihasználva, azonos számítástechnikai rendszer sérelmével, különböző alkalmakkal követi el a vizsgált bűncselekményt.[45]

Az információs rendszer vagy adat megsértésének bűncselekménye alapesetének három fordulata egymás mellett, illetve egymást követően is megvalósulhat. Az azonos jogtárgysértés a valódi alaki halmazat megállapítását rendszerint kizárja. A különböző alkalmakkal elkövetett, egymással összefüggésben nem álló cselekmények esetén azonban a valódi anyagi halmazat megállapítását nem zárja ki önmagában az a körülmény, hogy az egyes bűncselekményeket azonos informatikai rendszer használatával (felhasználásával, sérelmével) hajtották végre.[46]

2.2. Az információs rendszer felhasználásával elkövetett csalás

Az információs rendszer felhasználásával elkövetett csalás nóvumként jelent meg az új Btk. 375. §-ában a vagyon elleni bűncselekmények között. A javaslat indokolása szerint az információs rendszer felhasználásával elkövetett, kárt okozó csalások elsősorban vagyoni érdekeket sértő cselekmények, illetve ezek a csalásszerű magatartások azért kerültek a csalástól eltérő önálló tényállásba, mert hiányzik belőlük a klasszikus értelemben vett tévedésbe ejtés vagy tévedésben tartás. Ennélfogva az információs rendszer felhasználásával elkövetett csalás nem speciális bűncselekmény a csaláshoz viszonyítva, hanem egyszerűen egy olyan másik bűncselekmény, amelynek elkövetése esetén a csalás nem is állapítható meg.[47]

A 375. § (1) bekezdésében szabályozott *károkozó adatvisszaélési alakzat* szerint, *aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz,* bűntett miatt három évig terjedő szabadságvesztéssel büntetendő. Tehát az elkövetési magatartás megvalósul a már korábban az információs rendszer vagy adat elleni bűncselekménynél részletesen elemzett cselekményekkel. Azonban e bűncselekmény szerint minősül az elkövető magatartása, ha a célzatos befolyásolását a rendszernek *jogtalan haszonszerzés céljából* követi el, melynek *eredményeként kár*[48] is bekövetkezik. Nem szükségszerű, hogy a kár az információs rendszer tulajdonosánál vagy rendszergazdájánál következzen be. Gyakori elkövetési magatartás, hogy értékes adatokat törölnek vagy megváltoztatnak annak érdekében, hogy megtévesszenek

[45] Legf. Bír. Bf. II. 74/2008/5.
[46] MOLNÁR: i.m. 951. o.
[47] A Btk. javaslatának 375. §-ához fűzött indokolás
[48] A Btk. 459. § (1) bekezdésének 16. pontja értelmében: a kár e törvény eltérő rendelkezése hiányában a bűncselekménnyel a vagyonban okozott értékcsökkenés.

másokat azzal a céllal, hogy jogtalan haszonhoz jussanak például jellemző, hogy az elkövető pénzügyi rendszerhez fér hozzá és bankszámla egyenleggel vagy hitelkerettel manipulál. A bíróság egyik ügyben azért marasztalta az elkövetőt, mert számítástechnikai rendszerbe vitt be olyan adatokat, melyek nem voltak valósak és melyeket a rendszerbe nem kellett volna bevinnie és e folytatólagosan elkövetett cselekményét gyakorlatilag egy évtizeden keresztül, havi rendszerességgel valósította meg, kihasználva a bér és munkaügyi előadói munkaköréből adódó lehetőséget. E magatartásával az volt a célja, hogy őt meg nem illető jövedelemhez jusson, azaz cselekményét jogtalan haszonszerzés végett fejtette ki. Az átutalások megtörténte után az adatokat törölte, amivel az volt a célja, hogy a jogtalan haszonszerzés érdekében véghezvitt magatartására ne derüljön fény, így végső soron a törlés célzata is jogtalan haszonszerzés volt.[49]

Másik döntésben azonban kimondták, hogy a pénzintézet internetes felületén végrehajtott olyan pénzügyi műveletek, amelyek a pénzintézettel megkötött NET számlacsomagnak, illetve az internetbanki szerződésben foglaltaknak megfelelnek, a számítógépes rendszer rendeltetésszerű igénybevételét jelentik, ezért az információs rendszer felhasználásával elkövetett csalás különös részi tényállását nem valósítják meg.[50]

A bűncselekmény célzatos, ezért csak egyenes szándékkal követhető el. *A bűncselekmény eredménye,* a kár bekövetkezése tekintetében azonban elegendő az eshetőleges szándék is. A haszonszerzés mindig jogtalan, ha más(ok) megtévesztésével károkozásra irányul. A jogtalan haszon megszerzése azonban nem szükséges, már a tényállás körén kívül esik. A cselekmény rendszerint a jogellenes számítógépes manipuláció megkezdésével jut a kísérlet szakaszába, és a kár bekövetkezésével fejeződik be.[51]

A (2)-(4) bekezdés a bűncselekmény súlyosabban minősülő eseteit - a vagyon elleni bűncselekmények szabályozási technikájához hasonlóan - a bekövetkezett kár összegéhez[52] igazodóan határozza meg. *A minősítési rendszert* a kár összegén kívül még a bűnszövetségben, illetve az üzletszerűen történő elkövetés határozza meg. Az alapeset átfogja mind a kisebb, mind a nagyobb kár bekövetkezését, a minősített esetek a jelentős kártól kezdődnek. A

[49] Fővárosi Törvényszék B.687/2012/11. számú határozata
[50] BH 2017.8.252.
[51] SZOMORA Zsolt: XXXV. A vagyon elleni bűncselekmények. In: Karsai Krisztina (szerk.): Kommentár a Büntető Törvénykönyvhöz. Complex Kiadó. Budapest, 2013. 788. o.
[52] Btk. 459.§ (6) bekezdés: E törvény alkalmazásában az érték, a kár, valamint a vagyoni hátrány
a) ötvenezer-egy és ötszázezer forint között kisebb,
b) ötszázezer-egy és ötmillió forint között nagyobb,
c) ötmillió-egy és ötvenmillió forint között jelentős,
d) ötvenmillió-egy és ötszázmillió forint között különösen nagy,
e) ötszázmillió forint felett különösen jelentős.

bűncselekmény bármely csekély összegű kár bekövetkezte esetén tényállásszerű, tehát nincs alsóértékhatára. E tényállásnak szabálysértési alakzata nincs.[53]

2.3. Halmazati, elhatárolási kérdések

A 375. § (1) bekezdésben írt információs rendszer felhasználásával elkövetett csalás bűntettének *szükségszerű eszközcselekménye* a Btk. 423. § (2) bekezdésének b) pontja szerinti információs rendszer vagy adat megsértésének vétsége (bűntette), ezért bűnhalmazatot nem képeznek.

Amennyiben a hivatalos személyként eljáró ügyintéző anyagi ellenszolgáltatásért valótlan adatokat jegyez be közhiteles nyilvántartásba, és ezzel összefüggésben valótlan tartalmú közokiratok kerülnek kiadásra, akkor egyetlen magatartással - a valótlan adatok bevitelével - a már abban rögzített közokiratokra vonatkozó adathalmazokat jogosulatlanul megváltoztatja. Egységes cselekménye a Btk. 413. § (1) bekezdésének b) pontja szerinti információs rendszer és adat elleni bűntettét, valamint a Btk. 343. § (1) bekezdés b) pontja szerinti hivatalos személy által elkövetett *közokirat-hamisítás* bűntettének törvényi tényállását egyaránt megvalósítja, mert sérti mindkét bűncselekmény védett jogi tárgyát, feltéve, ha a bűncselekményt egyenes szándékkal, magatartásának előre látott következményeit kívánva hajtja végre.[54]

Az információs rendszer és adat elleni bűncselekmény, valamint *a közokirat-hamisítás és a vesztegetés bűncselekményeinek* anyagi halmazata valóságos, ha az információs rendszer és adat elleni bűncselekményt az EBH 2033.I. alatti módon megvalósító elkövető ezért a tevékenységéért az érintett hallgatóktól előnyt kér, továbbá a számítástechnikai rendszerben valótlanul rögzített adatok közlésével közreműködik abban, hogy a valóságban le nem tett vizsgáról valótlan adat kerüljön a leckekönyvbe.[55]

Ha a pénzintézet ügyintézője az ügyfelek által a pénzintézetnél lekötött vagy lekötni kívánt pénzösszegeket a sajátjaként kezeli és a sikkasztás leplezése érdekében az információs rendszerben e betétekre vonatkozó adatokat jogosulatlanul megváltoztatja, akkor a *sikkasztással* (Btk. 372. §) halmazatban a Btk. 423. § (1) bek. b) pont szerint minősülő és büntetendő információs rendszer és adat elleni bűntett megállapításának van helye. Az elkövető cselekménye két, egymástól független védett jogi tárgyat sért, és a két bűncselekmény nem kapcsolódik szükségszerűen egymáshoz. Mindkét bűncselekmény egyaránt elkövethető a

[53] SZOMORA: i.m. 789. o.
[54] Legf. Bír. Bfv. II. 74/2008/5.
[55] EBH 2009.2033. II.; BH 2009.264. II.

másik nélkül. Ez irányadó lehet más bűncselekmények (pl. csalás) mellett megvalósult információs rendszer és adat elleni bűncselekmény halmazatának a megítélése körében is.[56]

Az egyik legaktuálisabb kérdés a zsarolás és az információs rendszer elleni bűncselekmények kapcsolata. Előfordulhat, hogy az elkövetők jogosulatlanul belépnek a sértett számítógépébe a biztonsági intézkedések kijátszásával, malware aktiválásával – gondoljunk csak a zsarolóvírusokra - és megszerzik az azon tárolt bizalmas adatokat például akár személyes adatot, értékes gazdasági vagy üzleti titkot, kompromittáló képeket vagy a betörést követően hozzáférve a beépített webkamerához, illetve mikrofonhoz saját maguk készítenek olyan kép- és hangfelvételeket, amelyek a zsarolás alapját képezhetik. Ezután a zsarolási fázis következik, amikor az elkövető azzal fenyeget, hogy például az Interneten (pl. közösségi oldalakon, fórumokon) megosztja az adatokat vagy család, barátok részére elküldi a felvételt, amennyiben a sértett nem fizet egy meghatározott pénzösszeget a részére. A Btk. 367. § (1) bekezdése szerint, aki jogtalan haszonszerzés végett mást erőszakkal vagy fenyegetéssel arra kényszerít, hogy valamit tegyen, ne tegyen vagy eltűrjön, és ezzel vagyoni hátrányt okoz az a zsarolás tényállást valósítja meg. A zsarolás olyan fenyegetéssel is elkövethető, mely csupán hajlítja a sértett akaratát, annak cselekvési szabadságát csak kisebb-nagyobb mértékben befolyásolja. Ezzel mintegy lehetőséget nyújt számára, hogy az erőszak vagy fenyegetés erejét, komolyságát összevesse az őt fenyegető hátránnyal, amely lehet vagyoni jellegű, de érinthet akár egzisztenciát, becsületet, családi együttélést. Jelen esetben a zsarolást fenyegetéssel követik el, amely a súlyos hátrány kilátásba helyezésével, alkalmas arra, hogy a megfenyegetettben komoly félelmet keltsen. A zsarolás célzatos bűncselekmény és eredménye a vagyoni hátrány, ha a fenyegetés alkalmazása megtörtént, de az eredmény még nem állt be, akkor a zsarolás kísérlete valósul meg.[57]

Külön érdekesség, hogy a DDoS támadásokat zsarolásra is felhasználják, amely során olyan cégek oldalait választják ki, amelyek folyamatos és zavartalan működést követelnek meg (pl. webshopok, online szerencsejáték és fogadó cégek, energia- és pénzügyi szféra) és ezekkel szemben kisebb támadást indítanak, és a további erőteljesebb – akár teljes rendszer leállást eredményező - támadások elkerülése érdekében Bitcoint kérnek fizetségért.[58]

[56] Szegedi Ítélőtábla Bf.I. 180/2006/3.
[57] AKÁCZ József: XXXV. A vagyon elleni erőszakos bűncselekmények. In: Kónya István (szerk): Magyar büntetőjog I-III. – Kommentár a gyakorlat számára. 3. kiadás HVG-ORAC Lap- és Könyvkiadó. Budapest, 2017.
[58] URCUYO, Michael S.: From Internet trolls to seasoned hackers: protecting our financial interests from Distributed-Denial-Of-Service attacks. *Rutgers Computer & Technology Law Journal Vol. 42.*, 2016, 300–330. o.

Ezek alapján a jogosulatlan, engedély nélküli informatikai műveletek végzése az információs rendszer és adat elleni bűncselekménynek az elkövetési magatartásait megvalósítják és a *zsarolással halmazatban megállapítható* e bűncselekmény.

Személyes szívességtétel okán az információs rendszerbe belépési jogosultság kereteinek túllépésével való belépés vagy bennmaradás - és az ezúton történő adatszerzés - a hivatalos személy részéről *hivatali visszaélést* valósít meg, ha annak célja jogtalan előnyszerzés vagy hátrányokozás. Ez a bűncselekmény valósul meg akkor is, ha az adat jogosultsági feltételekhez kötötten bárki által megismerhető. Amennyiben a hivatalos személy személyes adattal visszaélésben megnyilvánuló jogtalan előnyszerzési vagy hátrányokozási célú magatartása egyszersmind jogtalan haszonszerzésre is irányul - a specialitás elve alapján - e magatartásával a *személyes adattal visszaélés* bűncselekményét valósítja meg.[59]

Jogtalan haszonszerzés célzata nélkül a rendőrség informatikai rendszeréből jogosulatlanul lekérdezett adatok más részére történő továbbadása nem a hivatali visszaélés bűntettét, hanem az információs rendszer megsértésének vétségét valósítja meg.[60]

2.4. Az információs rendszer védelmét biztosító technikai intézkedés kijátszása

A kiberbűnözés napjainkra egy *szolgáltatás-alapú üzleti modellé vált*, a különféle támadások indítására szolgáló eszközöket, programokat mint egy szolgáltatásként lehet igénybe venni vagy akár megvásárolni *az online feketepiacokon és fórumokon keresztül*. A bűnözők olyan üzleti rendszert alkalmaznak, amely hasonlóságot mutat a legálisan működő vállalkozásokéhoz. Az előbb említett digitális feketegazdaság részét képező online feketepiacok *a Darkneten keresztül érhetők el*, ami egy elosztott, magas fokú anonimitást biztosító hálózat és az Internet részét képezi *a Deep Weben*[61] *belül*, valamint speciális böngésző használatával érhető el mint például *The Onion Router (TOR)*. Fontos megjegyezni, hogy ezek az online platformok legális tevékenységek folytatására és a bizalmas üzleti tevékenységeknek, illetve kapcsolatoknak a fokozottabb védelmére lettek kifejlesztve, azonban a profit-orientált bűnözők is felismerték a bennük rejlő lehetőséget, hogy alacsony kockázat mellett – könnyedén elrejtve a személyazonosságukat és a bűnözői tevékenységüknek az infrastruktúráját - magas nyereségre tudnak könnyedén szert tenni a használatuk révén. Ezeket az illegális feketepiacokat és

[59] BH 2015.11.296.
[60] Kúria Bfv. I. 1.357/2014/11.
[61] Az Internet két részre bontható a hagyományos böngészőkkel elérhető Surface Web-re és a nagyobb részét képező Dark Web-re, ami egy rejtett hálózat és speciális szoftverekkel érhető csak el.

oldalakat együttesen *„hidden services”*-nek vagyis rejtett szolgáltatásoknak is hívják. Például a következő szolgáltatásokat lehet igénybe venni ezeken keresztül:

A malware és DDoS mint szolgáltatás *(Malware-as-a-Service és DDoS-as-a-Service)*: szinte bármilyen célnak megfelelő rosszindulatú program elérhető a Darkneten (pl. zsarolóvírus, botnet vírus vagy exploit stb.), illetve a DDoS támadások indítására szolgáló botneteket vagy a létrehozásukra szolgáló programokat bérelni lehet napi vagy havi díjjal átlagosan 5$ és 1000$ közötti áron. A szolgáltatás igénybevételével a hozzá nem értő felhasználók is olcsón, egyszerűen és gyorsan tudnak támadást indítani, mert sokszor csak a célpontot kell kiválasztaniuk és egy egérkattintás az egész, sőt még technikai segítséget is kaphatnak. *Pay-per-install szolgáltatások* pedig népszerű módszerei a malware terjesztésnek. A szolgáltatás nyújtói terjesztik a rosszindulatú programot tartalmazó fájlokat, amiket a szolgáltatást igénybe vevők biztosítanak a számukra és a letöltések száma után fizetnek nekik. Az ilyen szolgáltatások országspecifikus forgalmat biztosíthatnak.

Infrastruktúra mint szolgáltatás *(Infrastructure-as-a-Service)*: az informatikai támadások végrehajtásához szükség van *egy védett infrastruktúrára*, ami biztosítja a biztonságot, az anonimitást és rugalmasságot a bűnüldöző hatóságok beavatkozásaival szemben (pl. a VPN, vagyis a virtuális magánhálózat és a proxy szolgáltatások fontos szerepet játszanak ebben). *Tárhelyszolgáltatóknak* is kiemelt szerepük van, mert biztonságos tárhelyet biztosítanak az ellopott adatok (pl. jelszavak, személyes vagy pénzügyi adatok) és az ún. crimeware részére, ami egy gyűjtőfogalom és magában foglalja azokat a rosszindulatú programokat, amelyek használatával az elkövetők célja, hogy jogtalan haszonra szert tegyenek és egyúttal a felhasználók pénzügyi jólétét vagy értékes információit veszélyeztessék (pl. vírus, keylogger alkalmazásával), amik lehetőséget teremtenek a bizalmas információk ellopásához és azokkal való kereskedéshez.

A jogosulatlan belépés mint szolgáltatás *(Hacking-as-a-Service)*: alap szinten ez magában foglalhatja az e-mail vagy közösségi oldalak fiókjainak a feltörését vagy összetettebb támadásokat mint a gazdasági kémkedést vagy személyes adatok gyűjtését egy meghatározott célponttól.

Pénzmosás mint szolgáltatás *(Money laundering-as-a-Service)*: annak érdekében, hogy a bűnözők anyagi előnyre tegyenek szert az illegális tevékenységükből származó, egyúttal a digitális vagy hagyományos pénzügyi rendszeren keresztül érkező „piszkos” pénzek tisztára mosásához különféle szolgáltatásokat vesznek igénybe annak érdekében, hogy ezeket a legális

gazdaságba vissza tudják forgatni.[62] Ezek a szolgáltatások magukban foglalják az online és offline megoldások kombinációit, amelyeknek a középpontjában általában a pénz futárok, ún. „*money mule*" hálózatok állnak.[63]

Tovább nehezíti a helyzetet, hogy az elkövetők általában *pszeudoanonimitást biztosító*, szinte lenyomozhatatlan *digitális fizetőeszközöket használnak* mint például a Bitcoin a pénzügyi tranzakciók során. Az új 2017. évi XC. törvény a büntetőeljárásról 315. §-ban kialakította az ún. virtuális vagyontárgyak biztosításának a keretszabályait, amely alapján a virtuális fizetőeszközök mint a Bitcoin, valamint az elektronikus pénz egyes típusai is a jövőben lefoglalás tárgyát képezhetik

Összeségében a kibertámadások kivitelezését rendkívül megkönnyíti, hogy könnyen hozzá lehet jutni a bűncselekmények elkövetéséhez szükséges ismeretekhez, programokhoz, akár a már kész botnet infrastruktúrához, és ezért is fontos, hogy már az *előkészületi cselekmények sui generis bűncselekményként kerüljenek meghatározásra*. Ennek megfelelően a Btk. 424. §-ban szabályozza *az információs rendszer védelmét biztosító technikai intézkedés kijátszásának vétségét*. A bűncselekmény elkövetési tárgya az információs rendszer felhasználásával elkövetett csaláshoz vagy az információs rendszer vagy adat megsértésének *elkövetéséhez szükséges, vagy azt megkönnyítő jelszó, számítástechnikai program, valamint az ezek készítésére vonatkozó gazdasági, műszaki, szervezési ismeret.* A (3) bekezdés értelmező rendelkezése meghatározza, hogy a jelszó: „az információs rendszerbe vagy annak egy részébe való belépést lehetővé tevő, számokból, betűkből, jelekből, biometrikus adatokból vagy ezek kombinációjából álló bármely azonosító".

A bűncselekmény elkövetési magatartásai két fordulatban kerülnek meghatározásra. Az a) pont szerinti fordulat *elkövetési magatartásai a jelszó vagy számítástechnikai program készítése, átadása, hozzáférhetővé tétele, megszerzése vagy forgalomba hozatala. A készítés* eredménye például a kész program. Az átadás történhet a birtokba adáson kívül, a rendelkezésre bocsátással, illetve a megfelelő ismeret átadásával. *A hozzáférhető tételnek* minősül minden olyan tevékenység vagy mulasztás, amelynek köszönhetően hozzáférhetővé válik a jelszó vagy program az arra nem jogosult részére. *A megszerzés* a rendelkezési lehetőség megteremtését foglalja magában. A forgalomba hozatal esetén az elkövető több személynek juttatja el a jelszót vagy a programot.

[62] TÓTH Mihály: Gazdasági bűnözés és bűncselekmények KJK-KERSZÖV Jogi és Üzleti Kiadó Kft. Budapest, 2002. 375. o.
[63] Europol: The Internet Organised Crime Threat Assessment (IOCTA) 2014. 19-21. o.

A b) pont szerinti fordulat *elkövetési magatartása a jelszó vagy számítástechnikai program készítésére vonatkozó szervezési ismeret másnak a rendelkezésére bocsátása. A rendelkezésre bocsátás* azt jelenti, hogy az érintett személy a tényállásba foglalt ismeret birtokába jut. Ezt kimeríti a tudomásszerzés, de előfordulhat az is, hogy az ismereteket valamely tárgy tartalmazza, és ezt bocsájtják a rendelkezésére.

A Btk. büntethetőséget megszüntető okot is meghatároz: nem büntethető az (1) bekezdés a) pontjában meghatározott bűncselekmény elkövetője, ha - mielőtt a bűncselekmény elkövetéséhez szükséges vagy ezt megkönnyítő jelszó vagy számítástechnikai program készítése a büntető ügyekben eljáró hatóság tudomására jutott volna - tevékenységét a hatóság előtt felfedi, az elkészített dolgot a hatóságnak átadja, és lehetővé teszi a készítésben részt vevő más személy kilétének megállapítását.

A bűncselekmény rendbelisége az információs rendszerek számához igazodik. A tényállás mindkét fordulata *csak szándékosan – egyenes szándékkal - követhető el* és az elkövető szándéka arra kell, hogy irányuljon, hogy akár ő maga vagy tőle különböző személy az információs rendszer felhasználásával elkövetett csalást vagy az információs rendszer vagy adat megsértését elkövesse.[64] Aki a tárgyalt bűncselekmények elkövetése céljából jelszót vagy programot készít (átad, hozzáférhetővé tesz stb.), a Btk. 424. §-ában írt vétséget valósítja meg. Ha azonban a tettes ezeket az adatokat alkalmazva az információs rendszer felhasználásával elkövetett csalást megkíséreli vagy véghez is viszi, az említett előkészületi magatartás a tettesi cselekményhez nyújtott bűnsegélyként értékelendő.

3. Zárógondolatok

A kibertámadások száma évről évre növekszik, egyre gyakoribbak a célzott és komplexebb támadások, különösen, amelyek a kritikus infrastruktúrákat érintik.

Az információs rendszereket érintő támadásoknál az egyik legnagyobb gondot az elkövetők felderítése jelenti, mert a nyomozó hatóságok sokszor nem tudják meghatározni a pontos fizikai helyét az elkövetőknek, vagy a bűnözői infrastruktúrának, az elektronikus bizonyítéknak, amelyek a nyomozás szempontjából kiemelt jelentőségűek. Az információs rendszerek elleni támadások esetén általában az elkövetők hamis IP-címeket használnak, ami miatt a támadók, vagy akár a támadás céljából felhasznált számítógépek nem vagy nehezen azonosíthatók. További problémát jelent, hogy sokszor az elkövetők, a sértettek, az adatok és a bűnözői infrastruktúra részei különböző országokban találhatók, ami pedig joghatósági kérdést vet fel,

[64] MOLNÁR: i.m. 946–954. o.

még pedig, hogy melyik ország jogosult eljárni az ügyben és mely ország jogrendszere szerint. Ez eredményezheti azt is, hogy az ügyben érintett országok párhuzamosan indítanak büntető eljárást. A másik probléma a szabályozás hiánya egyes kérdésekben például az online feketepiacokra és a virtuális fizetőeszközökre vonatkozóan.

Fontos belátni, hogy a kiberbűnözés egy komplex problémakört foglal magában, mellyel szemben többlépcsős stratégiának az alkalmazása vált indokolttá. Ebben kiemelt jelentősége van elsődlegesen a prevenciónak, különösen a felhasználókhoz igazított oktatásnak, ismeretterjesztésnek, mert még mindig az ember a leggyengébb láncszem a kiberbiztonság szempontjából. Fontos a harmonizált, egységes nemzetközi szabályozás megteremtése mind büntető anyagi, mind eljárásjogi tekintetben. A fokozott együttműködés elősegítése is lényeges elem a magánszektor és a bűnüldöző hatóságok között, illetve az egyes bűnüldöző hatóságok között. Szükséges továbbá, hogy az új kihívásokra a jogalkotók adekvát módon és gyorsan reagáljanak és a jogalkalmazókat is felkészítsék erre, mert a technológiai fejlődés új elkövetési módokat teremt meg, amelyeknek jogi minősítése vitatott lehet.

A 2013/40/EU irányelv kijelöli a hazai törvényhozás feladatát, így de lege ferenda szükségesnek mutatkozik például a Btk. 423.§ minősített eseteit bővíteni a szervezett bűnözés keretében, illetőleg alkalmazottak által történő elkövetéssel továbbá a személyiség-lopás szankcionálására.