DOI: 10.38146/BSZ.2022.1.3

Herédi István

A kiberbűncselekmények felderítésének nehézségei

Challenges of cybercrime investigations

Absztrakt

A bűnüldöző szervek jelenkori kihívásai közül kiemelkedik a kiberbűncselekmények eredményes felderítésének biztosítása. Általánosságban elmondható, hogy ezt a bűncselekményi kategóriát a nagyfokú látencia mellett olyan felderítési nehézségek is jellemzik, amelyek az eljárás ügymenetét jelentősen lassíthatják, vagy akár lehetetlenné tehetik annak sikeres befejezését.

Az internet lakossági penetrációjának növekedésével újabb és újabb felületek és szolgáltatások jelennek meg az online térben, amely egyben lehetőséget teremt újfajta elkövetési magatartások megjelenésének is. A kibertér által biztosított anonimitás ösztönző jelleggel hat az elkövetők számára, hiszen a kontaktelkövetésekhez képest jóval kisebb a lebukás esélye, illetve vagyont érintő bűncselekmények esetében jóval nagyobb az okozott kár is.

A kiberbűncselekmények különböző kategóriáinak felderítési nehézségei azonosak, legyen szó akár egy egyszerűbb, információs rendszer felhasználásával elkövetett bűncselekmény, akár egy szofisztikált módon kivitelezett kibertámadást érintő eljárásról. Ezek a nehézségek a legtöbb esetben az online identitást elfedő szolgáltatások használatához, a technikai újdonságokhoz, illetve a nemzetközi hatósági együttműködésből fakadó hiányosságokhoz kapcsolódnak.

A megoldási lehetőségek a közvetlen nemzetközi együttműködési formák – különös tekintettel a 24/7-es kapcsolati hálózatok – alkalmazásában, a nyílt forrású adatgyűjtés és az online profilalkotás aktív használatában, illetve a rendvédelmi szervek állományának rendszeres továbbképzésében rejlenek. Ha az adott szakkérdés még ezek mellett is meghaladja a felderítő szerv állományának ismereteit, úgy célszerű lehet különleges szakismerettel rendelkező szaktanácsadókat, illetve szakértőket is bevonni az eljárásba.

Kulcsszavak: kiberbűnözés, kiberbűncselekmény, kibertámadás, információs rendszerek, OSINT

Abstract

One of the current challenges law enforcement agencies are facing, is ensuring the effective and proactive fight against cybercrime. This category of crime is characterized by its latent nature and detection difficulties that can significantly slow down the prosecution process or even make it impossible for the law enforcement agencies to conduct successful investigations.

With the growing of the number of the active internet-users, new interfaces and services are emerging in the online space, which also creates opportunities for the rise of new types of crime. In general, cybersecurity threats are on the rise. The anonymity provided by cyberspace acts as an incentive for offenders, as they are much less likely to be caught as if they were committing a contact-based crime, and the damage caused is much greater if we are speaking about cybercrime affecting assets.

Detection difficulties do not depend on the complexity/seriousness of the cybercrime. Simple cyber-enabled crime is just as difficult to uncover as sophisticated cyber-attacks. The main difficulties are related to the use of online identity masking services, technical innovation and gaps in international cooperation among authorities.

Possible solutions can offer the use of direct international cooperation, in particular 24/7 (always available) contact networks, the active use of open-source investigations and online profiling, and the regular training of law enforcement personnel. If the specific issue at stake is beyond the knowledge of the intelligence services' staff, it may be appropriate to involve specialized advisers or experts with specific expertise.

Keywords: cybercrime, cyber-dependent crime, cyber-attacks, information systems, OSINT

Kiberbűnözési tendenciák

Az információs rendszereket érintő, vagy azok felhasználásával elkövetett bűncselekmények száma folyamatosan nő (Lella, Theocharidou, Tsekmezoglou & Malatras, 2021). Ez a tendencia nem csupán Magyarországra jellemző, hanem az egész világon általános érvényű szabályként írható le (URL2). Az elkövetett

bűncselekményeknek csupán a töredéke jut a hatóság tudomására, a többség feljelentés – vagy akár észlelés – nélkül növeli a statisztikát (ISACA, 2019). A látencia jól szemléltethető a túlterheléses támadásokkal, melyek az információs rendszer működését ugyan akadályozzák, mégis jellemző, hogy az úgynevezett határvédelmi eszköz – másnéven tűzfal – a kérések számának emelkedésével kiszűri az indokolatlannak tűnőket, így az üzemeltető nem is jelzi a támadást a hatóságoknak.

A hatóságok tudomására jutott bűncselekmények elkövetőinek felderítése sokszor nem egyszerű feladat: nem csupán komoly nemzetközi együttműködést igényel bármilyen – az elkövetőkre vonatkozó – releváns információ beszerzése, hanem a nyomozás egyben türelemjáték is, hiszen a nemzetközi jogi aktusokon alapuló eljárási cselekmények teljesítése akár több hónapot is igénybe vehet.

A Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztályán napi rendszerességgel találkozunk azokkal a jellemző akadályokkal, amelyek egy-egy bűncselekménytípus felderítését megnehezítik vagy lehetetlenné teszik. Melyek ezek az akadályok, és mi jelenthetne megoldást az áthidalásukra?

A kiberbűncselekmények kategorizálására a nemzetközi szakirodalom nagy általánosságban a következő elhatárolást alkalmazza:

- kizárólag a kibertérben követhetők el azok a cselekmények, amelyek valamely információs rendszert közvetlenül érintenek, a bűncselekmény csak ezeken a rendszereken valósulhat meg. Ilyen például a túlterheléses támadás, a rosszindulatú kódsorok alkalmazása, illetve e rendszerek feltörése;
- míg a kibertér felhasználásával elkövetett cselekmények olyan „klasszikus" bűncselekmények, amelyek esetében az elkövetés eszköze az információs rendszer. Ilyen lehet például az online csalás, zsarolás vagy zaklatás (Furnell, 2016).

Álláspontom szerint utóbbi kategóriába sorolhatjuk a sok esetben külön kezelt gyermekek online szexuális kizsákmányolását, illetve a bankkártyabűnözést is.

Egy aktív internetfelhasználó átlagosan legalább havi rendszerességgel szembesül kiberbűncselekmény elkövetésével (Lella et al., 2021), azonban ezt ignorálja, vagy nem jelzi a hatóságoknak. A jelzés elmaradásának egyik oka lehet a hatósági vizsgálat járulékos elemeitől való félelem – így különösen az információs rendszer adattartalmának átvizsgálása –, míg az ignorálásra jó példa lehet az adathalász oldalak észlelése, amelyek oly mértékben szaporodtak el (Lella et al., 2021), hogy a legtöbb felhasználó egyszerűen tovább navigál az oldalakról, vagy a kínált szolgáltatás – például zeneletöltés – érdekében megadja a szenzitívnek nem ítélt személyes adatait. A bűncselekményi kategória azonban rendkívül tág, hiszen akár egy online hirdetésben vagy álprofilban megjelenített

személyes adat is felvetheti a személyes adattal visszaélés bűncselekmény elkövetésének gyanúját – a törvényi tényállási elemek megvalósulása esetén. Nincs jelentős különbség egy ilyen, egyszerű megítélésű cselekmény, és egy jóval összetettebbnek gondolt kibertámadás felderítése között a potenciális nehézségek tekintetében, így érdemes ezeket összességében vizsgálni.

Online anonimitás

A mindennapi gyakorlatunkban a kiberbűncselekmények alapvető sajátosságai közül talán a legkiemelkedőbb az a nagyfokú anonimitás, amit a kibertér teremt meg az elkövető számára. Az anonimitás azonban csak egy lehetőség, amivel az elkövető élhet, hiszen akarva-akaratlanul személyére közvetlenül vagy közvetve utaló identitással is követhet el jogsértéseket.

A valós identitás elrejtésének egyik legkézenfekvőbb módja az online avatárok használata. Az avatár egy olyan, kizárólag az online világban létező személyes profil, amely nem a tulajdonosának valós adataira építkezik. A legtöbb felhasználó azonban lustaságból vagy nemtörődömségből személyére vagy valós, illetve egyéb álprofiljaira közvetetten vagy közvetlenül utaló elemeket is felhasznál az avatárok megalkotásakor, amelyek segítségével járulékos információk szerezhetők be a profilt ténylegesen használó személy kilétére vonatkozólag. Ezen túl természetesen a szolgáltatói adatkérések is a hatóság rendelkezésére állnak, melyeken keresztül az adott profilt használó személy hálózati kapcsolatára, illetve az általa megadott személyes adatokra vonatkozó információk szerezhetők be.

Az online rejtőzködés technikai szempontból egy távoli szerver közbeiktatásával valósulhat meg, amely jellemzően valamely VPN-szolgáltatóhoz köthető privát hálózatot jelent. Az elkövető a saját hálózati kapcsolatát ebben az esetben egy olyan szolgáltató szerverein keresztül irányítja át, amely kifejezetten az online anonimitás biztosítása érdekében kínálja e szolgáltatását.

A hatóság ilyenkor csupán a szolgáltató tartományába eső – és jellemzően külföldön található – kiszolgálószerver hálózati címét tudja beszerezni, annak tekintetében pedig további szolgáltatói megkeresések, vagy nemzetközi jogsegélykérelem kibocsátása szükséges.

A probléma az, hogy a VPN-szolgáltatók – népszerűségük megőrzése érdekében – a legtöbb esetben nem működnek együtt a hatóságokkal, vagy egyáltalán nem is válaszolnak ilyen jellegű megkeresésekre, így kizárólag nemzetközi hatósági együttműködés keretében lehet bármilyen jellegű információt beszerezni tőlük. Ehhez azonban szükséges a kiszolgáló szerver pontos helyének

azonosítása is, majd az érintett állam hatóságainak megkeresésével kerülhet sor az esetleges forgalmi adatok lefoglalására. A VPN-szolgáltató gazdasági társaságokat azonban sok esetben olyan országban jegyzik be, amellyel az adatkérő államnak nincs jogsegélyegyezménye, hatóságai pedig nem vesznek részt a nemzetközi bűnügyi együttműködési formákban.

Nemzetközi együttműködés

A jogsegélykérelem kibocsátására irányuló előterjesztés elkészítését követően – amelyben az illetékes ügyészség intézkedik annak a fogadó állam részére történő megküldéséről – több hónap is eltelhet addig, amíg a hatóság értesül arról, hogy egyáltalán nincs is lehetőség adatokat beszerezni az érintett szolgáltatótól. Ennek egyfajta áthidalását jelentheti az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye (a továbbiakban: Budapesti Egyezmény) (The Convention on Cybercrime of the Council of Europe; URL1) alapján üzemeltett nemzeti 24/7-es kapcsolati pontok irányába kiküldött adatmegőrzésre irányuló megkeresés. Ennek keretében egy tagállam az egyezményben részes másik tagállam a hét minden napján, huszonnégy órában elérhető hatósági kapcsolati pontjait megkeresheti, hogy annak illetékességi területén működő szolgáltatót kötelezze az üggyel összefüggő elektronikus adatok megőrzésére legfeljebb 90 napig, illetve a jogsegélykérelem megérkezéséig. Ez utóbbi feltétel különösen fontos, hiszen a megőrzésre irányuló kérelem megküldése mellett intézkedni kell az adatok beszerzése iránt is – azaz a jogsegélykérelem előterjesztéséről.

Hazai kapcsolattartási pontként a Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztálya került kijelölésre, saját tapasztalataink pedig azt mutatják, hogy egyes tagállamok nem csupán a megőrzés tényéről értesítik hatóságunkat, hanem a kérelmezett elektronikus adatokat – például előfizetői adatokat – is több esetben rendelkezésünkre bocsátják válaszukban. Ez felgyorsíthatja az ügymenetet, hiszen a válaszban megérkezett adatok tekintetében további eljárási cselekmények végezhetők, nem szükséges a jogsegély keretében adott válasz bevárása.

Ugyanebben a körben értékelendő a megkeresett állam hatóságai és gazdasági társaságai eljárási jogának, illetve gyakorlatának különbözősége a hazaitól. Az Amerikai Egyesült Államokban székhellyel rendelkező gazdasági társaságok saját eljárási gyakorlatában például megszokott, hogy a hatósági megkeresés tényéről értesítik az érintett felhasználót. Ez komoly aggályokat jelenthet a büntetőeljárás eredményes lefolytatása szempontjából, így e szolgáltatókat a

nekik címzett adatkérésben külön fel kell hívni arra, hogy ne értesítsék az érintett személyt a megkeresés tényéről.

Szintén fontos, hogy a külföldi hatóságok jellemzően akkor szolgáltatnak – gyorsan – adatot, ha azon keresztül az elkövetőre utaló közvetlen információk birtokába kerül a megkereső hatóság. Ha azonban a bűncselekmény és a kért információ közötti kapcsolat csupán közvetett, vagy a megkeresésben megjelölt tényállásból egyértelműen nem ismerhető fel, a megkeresett állam vagy megtagadhatja a válaszadást, vagy az adatkérés kiegészítésére hívhatja fel a megkereső államot saját jogrendjére hivatkozva.

Kvalifikált elkövetők, új módszerek

Saját tapasztalatunk alapján, valamint a nemzetközi trendeket szemlélve (Lella et al., 2021) a kibertérben elkövetett bűncselekmények további jellemzője, hogy az online szolgáltatások bővülésével, a technológiai újítások felszínre kerülésével új elkövetési magatartások jelennek meg, valamint az elkövetők is új eszközökhöz jutnak. A felderítő szerveknek így rendkívül naprakész ismeretekkel kell rendelkezniük a technológiai fejlesztések terén, amelynek felépítése időigényes feladat, így jellemzően csak reaktív válasz adására nyílik lehetőség.

A dark weben – az internetnek csak speciális célszoftverrel elérhető részén – a felhasználók a VPN-szolgáltatás használatához hasonló fokú anonimitást élveznek, hiszen e hálózat egy kiterjesztett privát hálózatként is értelmezhető, azonban nincs olyan központi szolgáltató, aki felé a hatóság megkereséssel élhetne, ellentétben a VPN-kapcsolódást biztosító szolgáltatókkal.

A dark webes hálózatokon elkövetett bűncselekmények szolgáltatói oldalról történő felderítése így kizárólag az átirányítások számának megfelelő szolgáltatói adatkérés kiküldésével valósulhat meg, amely jellemzően legkevesebb három szolgáltatót, és akár ennek megfelelő számú államot érint.

A dark webes hálózatok részeiként üzemelő kiszolgálók általában nem tárolnak forgalmi adatokat, így a megkeresések a legtöbb esetben nem is vezetnek eredményre. Éppen ezért az ilyen hálózatokon megvalósuló bűncselekmények felderítése szolgáltatói oldalról sok esetben kivitelezhetetlen, azt egyéb technikai, humán és leplezett eszközök alkalmazásával érdemes megkezdeni.

A kiberbűncselekmények felderítésének komoly kihívása, hogy a kibertámadásokat – mely jelzővel jellemzően a kizárólag kibertérben elkövetett bűncselekményeket illetik – szofisztikált informatikai ismeretekkel rendelkező, sok esetben akár állami támogatással rendelkező elkövetők vagy elkövetői csoportok hajtják végre. Az elkövetéshez így nem csupán többszörös VPN-, hanem

korábban már megfertőzött számítógépekből álló botnet-hálózatokat is felhasználnak, amely jelentősen növeli az eredményes felderítéshez elengedhetetlen idő- és kapacitás szükségletet is.

Amennyiben az attribúció során egy vélhetően államilag szponzorált hackercsoport jelenik meg feltételezett elkövetőként, úgy a büntetőjogi felelősségre vonás lehetősége elenyésző, hiszen az érintett állam nem fog adatot szolgáltatni az elkövetők vonatkozásában.

A kriptovalutákhoz köthető blokklánc-technológia megjelenése egy felületet teremtett a kiberbűncselekmények elkövetői számára ahhoz, hogy anonim módon hajtsanak végre online pénzügyi tranzakciókat, melyek visszakövetése, illetve a használt kriptotárcák konkrét személyhez társítása sok esetben lehetetlen (URL2).

A blokklánc-technológia egy olyan tranzakciós modellt jelent, melyben az egyes tranzakciókat könyvelő „főkönyv" nem centralizált módon egy központi nyilvántartónál található meg – mint például a bankok esetében –, hanem minden olyan felhasználónál, aki a rendszer működtetésében részt vesz. Ezek a felhasználók – a kriptobányászok – jutalékot kapnak a tranzakciós díjakból, amiért informatikai eszközeik számítási teljesítményét a blokklánc működtetésére áldozzák. Az egyes tranzakciók úgynevezett kriptotárcák között történnek, amit egy egyszerű regisztrációt követően bárki szabadon létrehozhat. A tranzakciós láncolat, vagyis a blokklánc az egyes műveletek tekintetében csak az azokban érintett tárcák azonosítóját és a tranzakciós értéket tartalmazza, melyet egyes kriptovaluták tervezői ráadásul titkosított formában tesznek csak megjeleníthetővé (Möser et al., 2017).

A kriptotranzakciók elemzése rendkívül időigényes feladat, és a különböző kriptoszolgáltatások – mint például az úgynevezett „coinjoin", mely esetben egy gyűjtőtárca üzemeltetője vállalja, hogy a tárcájába utalt kriptovalutákat egy másik céltárcába utalja tovább, megnehezítve ezzel a forrástárca azonosítását – alkalmazása ezt csak tovább bonyolítja, így ennek vizsgálatára szoftveres eszközök beszerzése vagy különleges szakértelemmel rendelkező szakértő, illetve szaktanácsadó közreműködése válhat szükségessé.

Nyílt forrású adatgyűjtés – a megoldás?

Az információs rendszereket érintő bűncselekmények összes kategóriájában jellemző, hogy az internetről származó nyílt forrású adatok felhasználásával sok esetben több információ szerezhető be, mint akár a szolgáltatói megkeresések, akár a hatósági adattárakból történő lekérdezések során. A rendvédelmi

szervek rendelkezésére álló adattárak statikusak, azokat kizárólag a személy hatósági érintkezései során frissítik, amennyiben ilyenre nem kerül sor, az adatok akár több évig is érintetlenek maradnak. Az online felületeken ezzel szemben a felhasználók és ismerőseik is aktívan osztanak meg szöveges, grafikus vagy egyéb tartalmakat, mely a megosztások rendszerességétől függően egy jóval dinamikusabb adatbázist jelent.

A nyílt forrású adatgyűjtés, angol szavakkal Open Source Intelligence (a továbbiakban: OSINT), olyan adatok beszerzését és feldolgozását jelenti, amelyek nyílt forrásból bárki számára hozzáférhetők, tehát nyilvánosak (NATO, 2001). Az adatok forrásának felkutatása, begyűjtése és elemzése egy előre meghatározott cél érdekében történik.

A „nyílt forrás" további értelmezésre szorulhat: nem beszélhetünk nyílt forrásról akkor, ha egy olyan adatbázisból szerzünk adatokat, amelyhez kizárólagos vagy szervezeti szintű hozzáféréssel rendelkezünk, például lakcímnyilvántartás; nyílt forrásról beszélünk azonban akkor, amikor egy regionális vagy hozzáférés-korlátozással ellátott adatbázishoz regisztrációval, vagy külföldi IP-cím használatával férünk hozzá, például kínai közösségi média.

Az elérhető adatok köre rendkívül változatos: személyes adatok, gazdasági társaságok adatai, műszaki specifikációk, technológiai információk, dokumentumok, fájlok stb.

A jól megtervezett, rendszerezett formában végrehajtott adatgyűjtés csökkentheti az egyéb adatszerzésre irányuló igényt, így kizárólag olyan adatokat kell beszerezni más eljárási cselekményekkel, amelyekhez nyílt forrásokból nem lehet hozzáférni. Az eljárás eredményességének és időszerűségének biztosítása mellett az online felderítési módszerek alkalmazásával a rendelkezésre álló erőket is hatékonyabban lehet felhasználni, hiszen a kibertérből is beszerezhető információk összegyűjtése már nem terheli az állományt.

A rendvédelmi szervek tekintetében az OSINT nem kizárólag önmagában kell, hogy az adatgyűjtés alapját képezze, hanem a beszerzett információkat a rendelkezésre álló más adatforrásokkal – hatósági nyilvántartásokkal, leplezett eszközökkel – kiegészítve, egymással összefüggésben kell vizsgálni.

A bűnügyi felderítésben az online beszerezhető személyes adatok köre a leginkább hangsúlyos kategória, hiszen a személyekre és kapcsolataikra vonatkozó információk gyűjtése talán a legegyszerűbb – különös tekintettel a közösségimédia-felületek népszerűségére. Fontos azonban nyomatékosítani, hogy a releváns adatok köre nem merül ki az alapvető személyes és kapcsolati információkban, hiszen sok esetben akár a célszemély hálózati kapcsolatára, online jelenlétére, felhasználási, nyelvhasználati szokásaira tekintettel is lehetséges további adatokat gyűjteni.

Általánosságban kijelenthető, hogy annál több információ szerezhető be egy entitásról, minél nagyobb az online aktivitása (entitás alatt személyeket, gazdasági társaságokat, földrajzi helyeket, eszközöket, illetve bármely olyan dolgot érthetünk, amely az adatgyűjtés szempontjából releváns). Nem kizárt azonban, hogy olyan személyről szerezzünk online információkat, aki egyébként nem internetfelhasználó.

A bűnüldöző szervek számára kiemelt lehetőséget teremt az internet mint potenciális, nyílt felderítési adatok forrása. Jelentősége nem csupán abban áll, hogy nagy mennyiségű adat szerezhető be, hanem abban, hogy relatíve alacsony ráfordítással olyan adatok is beszerezhetők, amelyek leplezett eszközök alkalmazásával sem kerülnének a felderítő szerv birtokába.

A felderítés hatékonysága abban mérhető, hogy a beszerzett információkat milyen mértékben képes feldolgozni az adatgyűjtést végző szerv. Előnyös helyzetet jelent számukra, hogy a nyílt forrásból beszerzett adatokat a rendelkezésükre álló mögöttes adatbázisokban – például személyek nyilvántartása – ellenőrizni tudják, így az adatgyűjtés eredménye pontosabban validálható.

A nyílt forrásból beszerzett információk önmagukban is szolgálhatnak bizonyító erővel, ugyanakkor könnyen elképzelhető, hogy akár az adatgyűjtés folyamán, akár annak befejezését követően szolgáltatói megkeresések vagy nemzetközi jogsegély teljesítése válik szükségessé.

Az aktív – tehát a célszemély irányában valamely interakció felhasználásával végrehajtott – adatgyűjtő eszköz alkalmazásának tervezésekor számolni kell azzal, hogy elképzelhető, hogy az így beszerzett adat nem tehető a nyomozati iratok részévé, csak operatív információként használható fel. Amennyiben az adatgyűjtéshez használt eszközt az OSINT-dokumentációban a felderítő szerv megjeleníti, úgy a nyomozati iratok megismerésekor egyértelművé válhat a célszemély számára is az információ forrása, amely annak jövőbeli alkalmazását lehetetlenítheti el.

Egy megfelelően felépített anonim profil esetében további, különleges szakismeretekre is szükség lehet annak érdekében, hogy azt egy konkrét személyhez lehessen kötni. Jó példa lehet erre a felhasználó nyelvhasználati szokásainak elemzése, mely a társadalmi, közösségi hovatartozására, származására, képzettségére vonatkozó információkkal is szolgálhat (Omar, 2019).

Szakmai továbbképzés

Végezetül a hatóság tagjainak szakismerete az, amely sok esetben az eljárás folytatásának akadályát képezheti, hiszen a technológiai fejlődést nem minden

esetben tudja lekövetni a rendvédelmi szervek oktatásszervezési tevékenysége, emiatt jellemzően az új elkövetési magatartások felderítése akad el.

A kiberbűnözés területén a szakmai ismeretek közvetítése tekintetében kiemelkedő a szakirányítás szerepe, amely vezérfonallal szolgálhat egy-egy új bűncselekménytípus felderítése vonatkozásában.

Mivel a kiberbűncselekmények száma folyamatosan nő, biztosítani kell a felderítő állomány részére a folyamatos szakmai továbbképzés lehetőségét is, melynek keretében megismerkedhetnek az online térben megjelenő újfajta lehetőségekkel, illetve bepillantást nyerhetnek a felderítés folyamatába is.

Általánosságban pedig, amennyiben az eljárást folytató szerv nem rendelkezik kellő szakértelemmel a bűncselekmény felderítéséhez, célszerű megfontolni szakértő vagy szaktanácsadó bevonását az eljárásba. Példaként említhető a kriptovalutákhoz kötődő bűnözés, hiszen a blokkláncelemzés különleges szakértelmet igénylő feladat, mely ismeretekkel nem biztos, hogy rendelkezik a kirendelni kívánt informatikai szakértő. Szaktanácsadóként azonban a területen különleges szakismerettel rendelkező személy is bevonható az eljárásba[1], így további értékes információkhoz juthat a hatóság anélkül, hogy eszközt vagy szoftvert vásárolna, illetve különleges szakértelemmel rendelkező munkavállalót foglalkoztatna. A szaktanácsadó büntetőeljárásba történő bevonásának lehetőségéről a büntetőeljárásról szóló 2017. évi XC. törvény 270. §-a rendelkezik.

1 2017. évi XC. törvény a Büntetőeljárásról, 270. § *„(1) Az ügyészség, a nyomozó hatóság, illetve a rendőrség belső bűnmegelőzési és bűnfelderítési feladatokat ellátó szerve, valamint a rendőrség terrorizmust elhárító szerve szaktanácsadó közreműködését veheti igénybe, ha a bizonyítási eszközök felderítéséhez, felkutatásához, megszerzéséhez, összegyűjtéséhez vagy rögzítéséhez különleges szakismeret szükséges. A vádemelés után az ügyészség a bizonyítási indítvány megtétele, bizonyítási eszköz felkutatása és biztosítása érdekében vehet igénybe szaktanácsadót.*
(2) Ha a szaktanácsadó eljárása során a személy testének sérthetetlenségét érintő cselekmény elvégzése szükséges, erről az ügyészség vagy a nyomozó hatóság külön rendelkezik.
(3) Az ügyész, illetve a nyomozó hatóság tagjának kizárására vonatkozó rendelkezéseket a szaktanácsadóra megfelelően alkalmazni kell.
(4) A szaktanácsadó közreműködésének a tényét, a közreműködés módját és tartalmát az eljárási cselekményről készült jegyzőkönyvben vagy feljegyzésben fel kell tüntetni.”
(5) A szaktanácsadó a közreműködésével végzett eljárási cselekményre vonatkozóan tanúként hallgatható ki.

Felhasznált irodalom

Furnell, S. (2016). The evolving landscape of technology-dependent crime In McGuire, M. R. & Holt, T. J. (Eds.), *The Routledge Handbook of Technology, Crime and Justice* (p. 13–25). Routledge Handbooks. https://doi.org/10.4324/9781315743981-4

Information Systems Audit and Control Association (ISACA) (2019). *State of Cybersecurity Part 2.*

Lella, I., Theocharidou, M., Tsekmezoglou, E. & Malatras, A. (2021). *ENISA Threat Landscape Report 2021.* European Union Agency for Cybersecurity.

Möser, M., Soska, K., Heilman, E., Lee, K., Heffan, H., Srivastava, S., Hogan, K., Hennessey, J., Miller, A., Narayanan, A. & Christin, N. (2017). *An Empirical Analysis of Traceability in the Monero Blockchain.* Princeton University. https://doi.org/10.1515/popets-2018-0025

North Atlantic Treaty Organisation (NATO) (2001). *NATO Open Source Intelligence Handbook.*

Omar, A. & Deraan, A. B. (2019). Towards a Linguistic Stylometric Model for the Authorship Detection in Cybercrime Investigations. *International Journal of English Linguistics, 9*(5), 182–192. https://doi.org/10.5539/ijel.v9n5p182

A cikkben található online hivatkozások

URL1: *Európa Tanács, Számítástechnikai Bűnözésről szóló Egyezmény 2001.* https://www.coe.int/en/web/cybercrime/the-budapest-convention

URL2: *EUROPOL: Internet Organised Crime Threat Assessment (IOCTA) 2020.* https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Alkalmazott jogszabályok

2017. évi XC. törvény a Büntetőeljárásról

A cikk APA szabály szerinti hivatkozása

Herédi I. (2022). A kiberbűncselekmények felderítésének nehézségei. *Belügyi Szemle*, *70*(1), 47–57. https://doi.org/10.38146/BSZ.2022.1.3