DOI: 10.38146/BSZ.2018.7-8.3

MÁTÉ ISTVÁN ZSOLT

Informatikai rendszerek elleni támadások szakértői vizsgálata – a digitális nyomok rögzítésének szerepe

Az igazságügyi informatikai szakértők munkájában az informatikai rendszerek elleni támadások vizsgálata az elmúlt tíz évben a kimutathatóság határán mozgott egy nem reprezentatív, de a trendeket vázoló empirikus kutatás adatai[1] szerint. A kutatás adatgyűjtési periódusa után gyűjtött információk arra utalnak, hogy az informatikai rendszereket érő támadások – amelyek a büntetőeljárás során szakértői vizsgálat hatókörébe is kerülnek – mértéke növekszik. Ez a tény nemcsak az igazságügyi informatikai szakértőket készteti a vizsgálati területükre vonatkozó módszerek és eljárások frissítésére és megújítására, hanem a nyomozó hatóságok munkatársait is új típusú – korábban nem tapasztalt – próbák elé állítja.

Jelen írásmű az alapfogalmi környezet tisztázása után esettanulmányok formájában mutatja be azokat a tevékenységeket, amelyek jelentősen befolyásolhatják az igazságügyi informatikai szakértői vizsgálat eredményességét. A tanulmány a tipikus problémák bemutatása mellett megoldási és továbblépési javaslatokat is megfogalmaz elsősorban amerikai egyesült államokbeli és ausztráliai példák és jó gyakorlatok felhasználásával.

Cybernetics – Cyberpunk – Cybercrime

Akár önállóan, akár szóösszetételben használva a kiber vagy cyber szó az informatikával, a számítógépes hálózatokkal, de legalábbis az elektronikus rendszerekkel kapcsolódik össze az olvasók gondolatvilágában. E kapcsolódást az ógörög κυβερνητης (kybernetes) szó jelentése alapozza meg, mely kormányzót, irányítót jelent, s e jelentéstartalommal került a komplex önszerveződő rendszerek matematikai leírásának címébe.[2] A nagy távolságú számí-

1 Máté István Zsolt: Az igazságügyi informatikai szakértő a büntetőeljárásban. PhD-értekezés. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Pécs, 2017, 33–40. o.

2 Norbert Wiener: Cybernetics. Or Control and Communication in the Animal and the Machine. Hermann & Cie, Paris, Cambridge, Massachusetts, 1948

tógép-hálózatok kialakulásával közel egy időben a fogalom rövid művészeti kitérő után – amely érintette a képzőművészetet[3] és az irodalmat[4] egyaránt – a múlt század kilencvenes éveitől kezdődően került jelenlegi értelmezési tartományába: nevezetesen a globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerekkel[5] kapcsolatos fogalomkörbe.

Amint a GoogleBooks rendszer Ngram Viewer szolgáltatása segítségével lekérhető adatokból[6] is kitűnik, a cyber szó használta a GoogleBooks angol nyelvű szövegkorpuszában az előző évezred végén dinamikus növekedést mutatott, ez egyben arra is utal, hogy a fogalom szerteágazóan kapcsolódott az emberi tevékenységekhez.

A megjelenő új szóösszetételek (legalább 457 kifejezés) közül a cybercrime (kiberbűncselekmény) fogalma kapcsolódik jelen tanulmány tárgyához: az informatikai közegben elkövetett és az informatikai rendszerre irányuló bűncselekmények szakértői vizsgálatához.

Kiberbűncselekmények

A kiberbűncselekmény fogalma az 1960-as években elkövetett első számítógépes rendszereket érintő csalások[7] után formálódott, jórészt párhuzamosan a számítógépes bűncselekmény *(computer crime)* fogalmával. Egységes tudományos meghatározás a mai napig sem jött létre, így a jelenségre a cselekménytípusok és -fajták felsorolásával hivatkoznak a szerzők.

A típusmeghatározás során a kiberbűncselekményeket jellemzően két nagy csoportba sorolják:

– közvetlenül a számítógépes rendszerre irányuló cselekmények; illetve
– azok a cselekmények, amelyekben a számítógépek a cselekmény részei.[8]

Az Interpol szóhasználatában az előbbi elkülönítés a következőképpen jelenik meg:

3 http://www.kunstkritikk.no/kommentar/the-reinvention-of-cyberspace/
4 Veronica Hollinger: Cybernetic deconstructions: Cyberpunk and postmodernism. Mosaic: A Journal for the Interdisciplinary Study of Literature, vol. 23, no. 2, 1990, pp. 29–44.
5 2013. évi L. törvény 1. § 22.
6 https://books.google.com/ngrams/graph?content=cyber&year_start=1940&year_end=2000 &corpus=15&smoothing=3&share=&direct_url=t1%3B%2Ccyber%3B%2Cc0
7 Thomas A. Johnson (ed.): Forensic Computer Crime Investigation. CRC Press, Boca Raton, 2005
8 https://www.acorn.gov.au/learn-about-cybercrime

– fejlett, vagy csúcstechnológiás kiberbűncselekmények *(advanced cybercrime);* illetve
– kapcsolódó kiberbűncselekmények *(cyber-enabled crime).*[9]

A tudományos megközelítés árnyalja a bemutatott képet:
– számítógép-központú bűnözés *(computer centred crime)* esetén a célpont maga a számítógépes rendszer, hálózat, adattároló, vagy egyéb eszköz (például kereskedelmi weboldal tartalmának módosítása). Ez tekinthető egy új bűncselekménytípusnak is, amely új eszközrendszert használ (tudniillik a számítógépet);
– számítógéppel támogatott bűnözés *(computer assisted crime),* amikor is a számítógépet mint eszközt használja az elkövető a cselekmény során, amely „segíti" a tevékenységét, de nem feltétlenül szükséges hozzá (például gyermekpornográfia). Itt hagyományos bűncselekményekről beszélhetünk, új módszerek alkalmazása mellett;
– járulékos számítógépes bűnözés *(incidental computer crime),* amikor a számítógépes rendszer a bűncselekmény szempontjából mellékes, lényegében egy hagyományos eszköz kiváltását jelenti (például könyvelés számítógéppel, papíralapú dokumentáció helyett).[10]

Az egyes típusokon belüli elkülönítés a cselekmények tételes felsorolásával történhet, ezekre jellemző példát szolgáltat a már idézett kiberbűncselekmények ausztráliai online bejelentési hálózata *(Australian Cybercime Online Reporting Network; ACORN)* által alkalmazott elkülönítés:
1. Számítógépes rendszer elleni támadás
   a) illetéktelen hozzáférés, vagy a rendszer feltörése,
   b) kártékony kódok (vírusok, férgek, kémprogramok stb.),
   c) túlterheléses támadások;
2. Online zaklatás
   a) sértő üzenetek, képek és videók küldése,
   b) nem kívánt üzenetek küldése (spam),
   c) gyalázkodó üzenetek, vagy e-mailek küldése,
   d) online kirekesztés, vagy megfélemlítés,
   e) hamis közösségi hálózati profilok és sértő weboldalak létrehozása,
   f) rosszindulatú híresztelések online terjesztése,

9 https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
10 Ewa Huebner – Derek Bem – Oscar Bem: Computer Forensics – Past, Present And Future. University of Western Sydney, Sydney, 2007

g) a digitális kommunikáció bármely olyan formája, amely kirekesztő, megfélemlítő, szándékos fájdalom- vagy félelemkeltési célzatú;

3. Tiltott illegális tartalom közzététele
   a) gyermekek szexuális kizsákmányolására vonatkozó tartalmak,
   b) terrorszervezeteket vagy -cselekményeket támogató anyagok,
   c) gyűlöletkeltő tartalmak;
4. Gyermekek online zaklatásával kapcsolatos tartalmak
   a) gyermekpornográfiával összefüggő tartalmak birtoklása, terjesztése, gyártása, hirdetése vagy hozzáférés lehetővé tétele ezekhez,
   b) tizenhat év alatti[11] fiatalokkal szexuális tevékenység folytatása, vagy erre vonatkozó kommunikáció folytatása;
5. Személyiséglopás
   a) adathalászat,
   b) online hozzáférés megszerzése, feltörése,
   c) személyes adatok visszakeresése szociális médiából,
   d) üzleti adatokhoz történő engedély nélküli hozzáférés;
6. Online kereskedelemmel kapcsolatos ügyek
   a) online eladással kapcsolatos csalás (megvásárolt termék nem érkezik meg a vásárlóhoz),
   b) meghirdetettnél magasabb vételár kikényszerítése a vásárlótól,
   c) csodálatos gyógymód felkínálása,
   d) nem kért üzleti szolgáltatások terjesztése kisvállalkozások számára,
   e) adománygyűjtéses csalás jótékonysági szervezetek nevében;
7. Elektronikus levelezéssel kapcsolatos visszaélések
   a) kéretlen elektronikus levelek küldése,
   b) adathalászat;
8. Online csalás
   a) nyereményekkel kapcsolatos csalások,
   b) társkereséssel kapcsolatos csalások,
   c) fenyegetésekkel és zsarolással kapcsolatos esetek,
   d) munkalehetőséggel és befektetésekkel kapcsolatos csalások,
   e) személyiséglopás[12].

11 Ausztrál szabályozás szerinti életkor, lásd CRIMES ACT 1900 – SECT 55 Sexual intercourse with young person.
http://www8.austlii.edu.au/cgi-bin/viewdoc/au/legis/act/ consol_act/ ca190082/s55.html

12 https://www.acorn.gov.au/learn-about-cybercrime

Amint az a részletes felsorolásból is látszik, az egyes cselekményfajták között átfedés, azonosság is található, amely arra utal, hogy a vizsgált jelenség még nem ágyazódott be sem a büntetőjog, sem általában a társadalomtudományok fogalomkészletébe.

Mindamellett valamennyi felsorolt cselekmény közös vonásaként értékelhető az a tény, hogy kibertérben digitális nyomokat, digitális bizonyítékokat[13] hagynak maguk után, amelyek alkalmasak lehetnek a cselekmények részletes feltárására. Ezt a tevékenységet a nyomozó hatóságok kirendelése alapján az igazságügyi informatikai szakértők végzik, akik a *„a tudomány és a műszaki fejlődés eredményeinek felhasználásával”*[14] készített szakértői véleményükben foglalják össze az álláspontjukat. Tevékenységük megismeréséhez nélkülözhetetlen néhány alapfogalom – mint a digitális bizonyíték és kapcsolódó fogalmak – megismerése.

A digitális bizonyítékok

A digitális bizonyíték tételes meghatározása a digitális bizonyítékokkal foglalkozó amerikai tudományos társaságtól *(Scientific Working Group on Digital Evidence; SWGDE)* származik, e szerint: Bizonyító erejű információk, amelyeket bináris formában tároltak, vagy továbbítottak[15].

A definícióval csaknem szó szerint egyező szöveg került a digitális bizonyítékok azonosítására, összegyűjtésére, kinyerésére és megóvására vonatkozó nemzetközi szabvány szövegébe a következők szerint: Binárisan tárolt, vagy továbbított információ vagy adat, amelyre bizonyítékként lehet hivatkozni.[16]

Az előzőekben körülírt fogalom Magyarországon az új büntetőeljárási törvény révén került be a bizonyítás eszközei közé elektronikus adat elnevezéssel a következőképpen: *„Elektronikus adat a tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer*

13 A tanulmányban a digitális bizonyíték az angolszász *digital evidence* kifejezés értelmében szerepel, ez megfelel a magyar jogi szaknyelv bizonyítási eszköz fogalmának.

14 Az igazságügyi szakértőkről szóló 2016. évi XXIX. törvény 3. § (1) bek.

15 SWGDE/SWGIT Digital & Multimedia Evidence Glossary Version: 1.0 (July 25, 2005), p. 5. https://www.swgde.org/documents/Archived%20Documents/SWGDE-SWGIT%20Digital%20and%20Multimedia%20Evidence%20Glossary%20v1-0

16 ISO/IEC 27037:2012(E) Information technology – Security techniques – Guidelines for identification, collection, acquisition, and preservation of digital evidence. International Organization for Standardization, Geneva, 2012, p. 10.

általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja."[17]

Ahhoz, hogy valamely számítógépes adat digitális bizonyítékká váljon, elsőként át kell hogy essen az azonosítás *(idetification)* folyamatán, amelynek során eldől, hogy a binárisan tárolt vagy továbbított információ vagy adat releváns-e a vizsgálat szempontjából[18]. Így válik a potenciális digitális bizonyítékból digitális bizonyíték.

A digitális bizonyítékok beszerzésének lehetőségei és módjai a korábbiakban felsorolt kiberbűncselekmények esetén jelentős eltérést mutathatnak: míg a helyi eszközökön megjelenő nyomokat a *computer forensics* hagyományos eszközeivel nyeri ki a szakértő, addig a számítógépes hálózatokban megjelenő potenciális digitális bizonyítékokat a *network forensics,* vagy *cloud forensics* eszközrendszerével kell azonosítania és értékelnie.

A *computer forensics* kissé leegyszerűsítve a szó szoros értelmében kézzelfogható adattárakból történő adatkinyerésen és adathelyreállításon alapul, míg a *network* és *cloud forensics* esetén a számítógépes hálózati forgalom egyes hozzáférhető adatainak elemzésével szerezhető meg a digitális bizonyíték. Mindezekhez járul még a potenciális digitális bizonyítékok változékonyságában mutatkozó különbség is: míg a *computer forensics* módszereivel vizsgált adatok kevésbé változékonyak, addig a *network* és *cloud forensics* módszereinek alkalmazásakor gyakran rendkívül tünékeny adatokkal kerül kapcsolatba a szakértő.

A következőkben a digitális bizonyítékok azonosításának, kinyerésének és elemzésének három különböző esetén keresztül kerül sor a tevékenységhez használt eszközök, szabványok és jó gyakorlatok egy-egy példájának bemutatására.

Online zaklatás szakértői vizsgálata – esettanulmány

A vizsgált esetben a nyomozó hatóság a büntető törvénykönyvről szóló 2012. évi C. törvény 222. § (1) bekezdésébe ütköző, és a (3) bekezdés a) pontja szerint minősülő házastárs volt házastárs, élettárs, volt élettárs sérelmére elkövetett zaklatás vétségének megalapozott gyanúja miatt ismeretlen tettes ellen

17 A büntetőeljárásról szóló 2017. évi XC. törvény 205. § (1) bek.

18 ISO/IEC 27042:2015(E) Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence. International Organization for Standardization, Geneva, 2015, p. 3.

induló büntetőügyben felmerülő informatikai szakkérdés megválaszolására rendelte el igazságügyi informatikai szakértői vizsgálat lefolytatását.

Ez az ügytípus a korábbiakban vázolt osztályozás szerint a számítógéppel támogatott bűnözés *(computer assisted crime)* körébe sorolható, hiszen a kérdéses esetben a zaklatás közege volt a kibertér, maga a cselekmény pedig „hagyományos" bűncselekmény.

Az ügyben lefoglalták a sértett és a terhelt hordozható számítógépét, valamint a terhelt megrongált állapotú okostelefonját.

A digitális eszközök esetén – amelyek a digitális adatok feldolgozására vagy tárolására használatos eszközök[19] – kiemelten fontos a dokumentálás. Ha a vizsgálat alá vont eszközök állapota (például sérülésmentessége) nincs megfelelően dokumentálva, akkor a későbbiekben felvetődhet – akár a nyomozó hatóság, akár a szakértő részéről – a szándékos vagy véletlen rongálás megtörténte. Ezért kiemelten fontos a potenciális digitális bizonyítékok (tudniillik digitális eszközök) összegyűjtésekor az állapot rögzítése, majd ennek az állapotnak az ismételt feljegyzése a keletkező dokumentumokban, így a szakértőt kirendelő határozatban is.

Az SWGDE sérült mobileszközök összegyűjtésének jó gyakorlatai című ajánlása[20] szerint a következő feladatok elvégzése és körülmények figyelembevétele szükséges:

– Mivel az eszköz áramellátása további károkat okozhat, nem szabad azt semmiféle áramforráshoz csatlakoztatni (akkumulátor, hálózati adapter).
– A fizikai sérülés nem feltétlenül jelenti a készülék üzemképtelenségét vagy az adat-helyreállítás meghiúsulását.
– A sérülés jellegét minden esetben dokumentálni kell, és arról tájékoztatni szükséges a vizsgálatot végző személyt.
– Bármilyen az eszköz fizikai megtisztítását célzó tevékenység előtt egyeztetni kell a műveletek sorrendjét (például DNS, nem látható nyomok kinyerése) a vizsgálatot végzőkkel.[21]

Az előbbiek mellett, a dokumentálás a digitális bizonyítékok értékelésénél is fontos szerepet kap, hiszen egy adott digitális nyom másként értékelendő akkor, ha a sértett, és másként, ha a terhelt digitális eszközén találja meg a szakértő.

19 ISO/IEC 27037:2012(E) i. m. 2. o.

20 SWGDE Best Practices for Collection of Damaged Mobile Devices, v1.1. 2016, p. 4. https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Collection%20of%20Damaged%20Mobile%20Devices

21 Az ajánlás további részletes útmutatást ad az egyes sérüléstípusok esetén követendő tevékenységekről.

Jelenleg a lefoglalt eszközök részletes és pontos dokumentálása nem ritkán hiányos – mint a vizsgált esetben is –, így a szakértői vizsgálat ezen adatok beszerzésével kell hogy elkezdődjön. A probléma kezelésére az SWGDE már idézett, illetve további elérhető ajánlásainak átvétele és/vagy adaptálása adhat megoldást.

Visszatérve a konkrét ügyre, az adott esettípus vizsgálata a hagyományos *computer forensics* eszközökkel történik, amelynek során a szakértő – dokumentált módon – eltávolítja az egyes készülékek tárolóeszközeit[22], majd írásblokkoló eszközön *(forensic write blocker)* keresztül megkezdi a vizsgálatot és a releváns adatok kinyerését *(aquisition)*.

A kinyerés során – amely a vizsgált eszköz adatkészletén belüli adat vagy adatok másolását jelenti[23] – teljes fizikai, vagy részleges logikai mentésre kerülhet sor. Előbbi olyan bitazonos mentés, amelynek során az eredeti tárolómédián található valamennyi adatterület bekerül egy lemezképállományba *(forensic image)*. Ez a lemezképállomány lesz a későbbiekben a részletes elemzés tárgya. A logikai kinyerés esetén célzott adatterületek – például egyes könyvtárak és/vagy fájlok – mentése történik meg.[24]

A vizsgált ügyben a zaklatás elektronikus levelezés útján történt, illetve felmerült Gmail- és Facebook-fiókokhoz történő illetéktelen hozzáférés, valamint billentyűzetleütést naplózó alkalmazás telepítése is, így a szakértői vizsgálat elsődlegesen ezekre a körülményekre koncentrált.

Mivel a szakértő a részletes vizsgálatot alapvetően az egyes eszközök bekapcsolása nélkül, írásvédelem alkalmazása mellett végzi, minden olyan körülmény feltárására sor kerül, amely az adott eszköz lefoglalásának időpontja és a szakértői vizsgálat megkezdésének ideje közötti adatmódosulásra utalhat. Ebből adódóan az eszközök nem dokumentált bekapcsolása a nyomozó hatóság munkatársa és/vagy az ügyész részéről a digitális bizonyíték hitelességét gyengítheti, vagy akár meg is semmisítheti.

Az ilyen beavatkozást az angolszász szakirodalom *tampering* (illetéktelen hozzáférés) néven ismeri, és tartalmát a már idézett ISO/IEC 27037:2012(E) szabvány 3.21 pontja rögzíti a következők szerint: *„Az illetéktelen hozzáférés a digitális bizonyíték módosítására vonatkozó szándékos cselekmény, vagy erre adott engedély.”*[25]

22 Mobil- és okostelefonok esetén a vizsgálati eljárás eltérő.

23 ISO/IEC 27037:2012(E) i. m. 2. o.

24 SWGDE Best Practices for Computer Forensic Acquisitions. v1.0. Scientific Working Group on Digital Evidence, 2018

25 ISO/IEC 27037:2012(E) i. m. 4. o.

Ezért fontos a potenciális digitális bizonyítékokkal közvetlenül kapcsolatba kerülő munkatársak felkészítése és továbbképzése, különösen annak tükrében, hogy egy friss felmérés szerint az informatikai eszközökkel kapcsolatos eljárásrendek ismerete – tehát a felhasználói szintnél magasabb hozzáértés – csak a megkérdezettek 3,4 százalékát jellemezte a saját megítélése szerint.[26]

A vizsgált esetben a részletes szakértői vizsgálat során a sértett hordozható számítógépén található operációs rendszer rendszerleíró adatbázisa *(registry)* elemzésével megállapítható volt, hogy a kérdéses eszközön billentyűzetleütés-megfigyelő program nem működött. A sértett és a terhelt közötti kommunikáció egyes elemeinek mentésével – mind a sértett, mind a terhelt számítógépéről – alátámasztható volt a cselekmény időbeli és tartalmi lefolyása. A böngészőprogramok (Google Chrome) és azonnali üzenetküldő programok (Skype) naplóadatai, valamint a kommunikációt dokumentáló képernyőképek és digitális fényképek metaadatai (létrehozó eszköz, dátum és idő, GPS-koordináták) révén a szakértői vizsgálat releváns adatokat tudott szolgáltatni a nyomozó hatóság elemző és értékelő tevékenységet végző munkatársainak.

A vizsgált ügyben és a hasonló ügytípusok esetén a kinyert adatok hagyományos átadási médiája az optikai adathordozó – jellemzően CD-R, DVD-R vagy DVD-R DL –, különösen jelentős adatmennyiség esetén pedig külső merevlemez (egy munkapéldány, egy biztonsági másolat).

A hasonló ügyekben szereplő digitális bizonyítékok mennyiségének növekedésével már a közeljövőben változtatni kell a szakértői vizsgálat során kinyert adatok átadási módján, hiszen több száz gigabyte-nyi adat kezelése optikai adathordozón már akadályozhatja a nyomozó hatóság értékelő- és elemzőmunkáját. A megoldást várhatóan a mágneses és/vagy elektronikus külső tárolók vagy a központosított biztonságos tárolást és elérést nyújtó bűnügyiadat-tárházak jelenthetik.

Információs rendszer elleni kibertámadás szakértői vizsgálata – esettanulmány

A következő esettanulmány átmenetet mutat a számítógép-központú bűnözés *(computer centred crime)* és a számítógéppel támogatott bűnözés *(computer assisted crime)* között. Ebből adódóan a szakértői vizsgálat eszközei részben a *computer forensics,* részben a *network forensics* eszközkészletéből származnak.

26 Simon Béla: A rendőrség állományának felkészültsége a kiberbűnözésre. Hadtudományi Szemle, 2018/1., 402–403. o.

A kérdéses ügyben a vidéki nagyváros rendőrkapitánysága a büntető törvénykönyvről szóló 2012. évi C. törvény 423. § (2) bekezdés b) pontjába ütköző, és a (2) bekezdés b) pontja szerint minősülő információs rendszer vagy adat megsértésének bűntette elkövetésének gyanúja miatt folytatott büntetőügyben rendelte el igazságügyi informatikai szakértő bevonását.

Az ügyben szereplő informatikai rendszer egy hálózatra csatolható tárolóegység *(Network Attached Storage; NAS)* volt, amely biztosította a sértett gazdasági társaság részére az alaptevékenységhez kötődő adatok központosított tárolását oly módon, hogy azok az internet irányából történő bejelentkezés után elérhetők legyenek a feljogosított munkatársak számára.

A NAS tároló a cselekmény feltételezett időpontjában elérhetetlenné vált a munkatársak részére, így a gazdasági társaság alaptevékenysége akadályoztatást szenvedett.

A kirendelő hatóság az ügy szakértői vizsgálatához a feltételezés szerint megtámadott informatikai rendszer naplóállományát küldte meg a szakértőnek (26 oldal terjedelemben, papír alapon, az eszköz tényleges azonosítása – értsd: gyártó és típusmegjelölés – nélkül), valamint a terhelt által használt hordozható számítógépet, amelynek lefoglalására a feltételezett kibertámadást követő 157. napon került sor. A szakértői vizsgálat a lefoglalást követő 19. napon kezdődött meg.

Az ügytípus jellemzője ebben az esetben az, hogy a feltételezett támadást elszenvedett rendszer (informatikai eszköz) rendelkezésre áll, így annak tartalma részletesen vizsgálható, amennyiben a nyomozó hatóság lefoglalja – erre a vizsgált esetben, a rendelkezésre álló adatok alapján nem került sor. Az eszköz rendszernaplójának a feltételezett támadás időszakára vonatkozó részét azonban lefoglalták, ez tartalmazta a feltételezett támadást megelőző tizenkét nap, valamint az utána következő egy nap rendszereseményeit.

A szakértői vizsgálat a rendszernaplót létrehozó eszköz beazonosításával kezdődött, amelyet a kirendelő hatóság munkatársa végzett el a sértett gazdasági társaságtól történő adatbekéréssel. A kérdéses eszköz D-Link gyártmányú DNS-320L modellszámú készülék. Az eszközre vonatkozó további fontos adat a készülék ismert sérülékenységeinek *(well known vulnerabilities)* megismerése (ha van ilyen). Az eszköz közvetlen vizsgálhatóságának hiányában a szakértő a releváns szakmai adatbázisokat – jelen esetben SecurityFocus Vulnerability Database[27] – vizsgálja át. Az adatbázis szerint – amely gyártói információkon alapult – a kérdéses eszközre jellemző volt egy úgynevezett tá-

27 https://www.securityfocus.com

voli parancsbejuttatási sérülékenység *(Remote Command Injection Vulnerability),* amely a feltételezett kibertámadás időpontja előtt három évvel már ismert volt, és a sérülékenység kiküszöbölésére vonatkozó javítócsomag is rendelkezésre állt.

Amint az jól látható, a megtámadott eszköz részletes dokumentálásának és lefoglalásának, vagy bitazonos mentésének hiánya nehezítette a készülék azonosítását, ebből adódóan a támadhatóságra vonatkozó szakértői megállapítások megalapozhatóságát, valamint azt is, hogy az adott készülékről eldönthető legyen, megvolt-e az ismert sérülékenysége, vagy nem.[28]

A feltételezés szerint megtámadott eszköz lefoglalásának hiányából adódóan a szakértő számára feltett egyik kérdésben megfogalmazódott az a feltételezés, miszerint a támadó a „TXT fájl küldésével az – sértett-gazdasági-társaság – Kft. – települési címén lévő szerverén lévő adatokat elérhetetlenné tette", megvizsgálhatatlanná vált (tudniillik a kérdéses állomány nem állt rendelkezésre).

A bemutatott problémákat a részletes dokumentálás mellett megoldhatja a szaktanácsadó igénybevétele:

„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."[29]

Az angolszász gyakorlatban a szaktanácsadó feladatkörét a nyomozó hatóság munkatársa, a digitális bizonyítékok helyszíni vizsgálója *(Digital Evidence First Responder; DEFR)* végzi, aki *„képzettséggel és jogosultsággal rendelkezik arra vonatkozóan, hogy egy esemény helyszínén elsőként elvégezze a digitális bizonyítékok összegyűjtését és megszerzését"*[30]. Ugyanezt a tevékenységet az európai uniós Hálózat- és Információbiztonsági Ügynökség kiadványa elsősorban a számítógépes vészhelyzetkezelő csoportok *(computer emergency response team)* tagjainak munkaterületeként értelmezi, és részükre teszi közzé a jó gyakorlatokat összefoglaló kiadványait, amilyen az

28 A sérülékenységi adatbázis tartalmazta a készülékre vonatkozóan a sérülékeny és biztonságos működtetőprogramok verziószámait, ezek alapján a sérülékenység kihasználásának lehetősége valószínűsíthető vagy kizárható lett volna.

29 2017. évi XC. törvény 270. § (1) bek.

30 ISO/IEC 27037:2012(E) i. m. 2. o.

elektronikus bizonyítékok – alapvető segédlet azonnali beavatkozók részére *(Electronic evidence – a basic guide for First Responders*[31]*)*.

A hiteles képzési anyagok – forráshelyüktől függetlenül – javíthatják a kiberbűncselekmények szakértői vizsgálatát megalapozó információk minőségét, ezért az ajánlások és jó gyakorlatok magyar nyelvre és jogi környezetre történő adaptálása elkerülhetetlen lesz a közeljövőben.

A vizsgált esethez visszatérve: az alapadatok tisztázása után kerülhet sor a cselekmény körülményeit tartalmazó rendszernapló elemzésére. Az összesen 800 bejegyzést tartalmazó – elsőként papír alapon átadott, majd elektronikus formában is beszerzett – napló kinyerése a szakértő által nem ismert (vele nem közölt) körülmények között zajlott, így annak hitelessége, teljeskörűsége megkérdőjelezhető.

A hasonló helyzetek elkerülését oldhatja meg a korábbiakban bemutatott DEFR szerepkörnek megfelelően kiképzett munkatársak alkalmazása, akik a lehetséges digitális bizonyítékokra vonatkozó döntések és tevékenységek mellett fenntarthatnák a felügyeleti láncot is *(chain of custody)*. Utóbbi *„végigvonul a bizonyítékok kezelésének teljes életútján, mely alapján végig követhető marad, hogy mely időszakban hol, kinek a felügyelet alatt volt a bizonyíték, történt-e változás annak állapotában”*[32].

A rendszernapló bejegyzéseit a szakértő értelmezhetővé teszi az elemző- és értékelőmunkát végző szakemberek részére oly módon, hogy annak műszaki tartalmát és a hozzá fűzött magyarázatokat a rendelkezésükre bocsátja. A tárgyalt esetben az egyes rendszerfolyamatokhoz tartozó leírásokat – köztük kiemelten az energiaellátásra és a bejelentkezésre vonatkozó bejegyzéseket – lefordították, és megtörtént ezek részletes magyarázata például a következők szerint *(táblázat)*.

A működési körülmények mellett kiemelten fontos a külső bejelentkezések forrásának azonosítása, amely elsődlegesen az IP-címek alapján történik. A rendszernapló adataiból (automatizált folyamattal) kigyűjtött IP-címek szolgáltatóit *(Internet Service Provider; ISP)* és az IP-címekhez kapcsolódó geolokációs információkat az interneten elérhető tömeges lekérdezést lehetővé tevő adatbázisokból szerezheti meg a szakértő. A megkapott információkat a rendszernaplóval összefűzve könnyen értelmezhető és elemezhető adatsorok kerülhetnek a nyomozó hatóság munkatársaihoz, akik az adatsort a

31 Electronic evidence – a basic guide for First Responders, Good practice material for CERT first responders. European Union Agency for Network and Information Security, 2014

32 Máté István Zsolt: i. m. 100. o.

A rendszernapló bejegyzései

Bejegyzés tartalma	Magyarázat
mail_daemon: System Has Rebooted From A Power Failure.	Rendszer újraindulását követő hibaüzenet küldése: elektromos tápellátás hibája
rtc: System Time Is Updated By RTC.	A real-time-clock áramkör beállítja a rendszeridőt
fan_control: Set Fan Speed To “LOW”.	A ventilátorvezérlő ALACSONY sebességre kapcsolja a ventilátort
fan_control: Set Fan Speed To “HIGH”.	A ventilátorvezérlő MAGAS sebességre kapcsolja a ventilátort
fan_control: Set Fan Speed To “STOP”.	A ventilátorvezérlő LEÁLLÍTJA a ventilátort
fan_control: Set Fan-Control Mode To “Auto(Off/Low/High)”	A ventilátorvezérlő AUTOMATIKUS üzemmódba kapcsolja a ventilátorvezérlést
system_daemon: System is rebooted or power up successfully.	Rendszerüzenet: a rendszer újraindult, a bekapcsolás sikeres

hagyományos nyomozati eszközökkel összegyűjtött információkkal összevetve igazolhatják vagy cáfolhatják a terhelttel kapcsolatos feltételezéseiket. Ha a terhelt részéről rendelkezésre áll egy digitális eszköz – jelen esetben hordozható számítógép –, az adatok köre tovább bővíthető a hagyományos *computer forensics* eljárásaival kapott információkkal. Ez még akkor is jelentős lehet, ha – mint a vizsgált esetnél is – az adatkinyerés nem szolgáltatott további digitális bizonyítékokat, ugyanis a lefoglalt HP dv6-3107eg laptopon megtalált operációs rendszert a feltételezett kibertámadást követő 53. napon telepítették egy olyan adathordozóra (KINGSTON SHFS37A SSD), amely nem volt része az eredeti konfigurációnak. Ilyen és hasonló esetekben a szakértő jelezheti a nyomozó hatóság munkatársainak a tényt, miszerint a készülék eredeti adathordozóját lecserélték, és javaslatot tehet annak felkutatására.

Összefoglalva: a vizsgált ügyben összegyűjtött digitális bizonyítékok nem tették lehetővé a biztonsági esemény kategorikus azonosítását, ezért két valószínűsíthető eseménysor bemutatására került sor a szakértői véleményben:

1. A D-Link DNS-320L tárolórendszer firmware-ének sérülékenységét kihasználva 2017 (hónap, nap) 15.59:04-kor távoli parancsbejuttatás történhetett a tárolórendszer működtető rendszerébe, ez érinthette a jogosultságkezelési alrendszert is. A támadó a megszerzett jogosultságot felhasználva 2017 (hónap, nap) 18.48:56-kor adminfelhasználóként bejelentkezett, majd lekapcsolta a tárolórendszer áramellátását.
2. A D-Link DNS-320L tárolórendszer firmware-ének sérülékenységétől függetlenül több bejutási kísérlet is történt az eszközre különböző időpontok-

ban. Egyes esetekben sikertelen volt a megosztott könyvtárak felcsatolása az egyes regisztrált felhasználók részéről. A tárolórendszer működésének – a rendszernapló által rögzített – utolsó periódusában több alkalommal megtörtént elektromos tápellátás kiesése, amelynek következtében a tárolórendszer újraindult. A biztonsági esemény bekövetkezésekor 2017 (hónap, nap), vasárnap 18.49:39 után az újraindulás – ismeretlen okból – nem következett be. A tárolórendszer – szakértő feltevése szerint – a hétvégi időszakban nem volt közvetlenül fizikailag hozzáférhető az kft. irodája (a rendelkezésre álló adatok szerint irodaház található az adott címen), így a tárolórendszer áramellátása nem volt visszakapcsolható. Az áramellátás legkésőbb az esemény utáni napon 09.36:26-kor helyreállt.

Amint az jól látszik a bemutatott esettanulmány adataiból, a hatékonyságot növelhette volna a kirendelő hatóság vizsgálatának első szakaszában alkalmazandó szaktanácsadó, valamint a folyamatos dokumentálás és információátadás a szakértőnek.

Beékelődéses támadás szakértői vizsgálata – esettanulmány

A harmadik esettanulmány a kiberbűncselekmények egyik klasszikus változatát mutatja be: az informatikai rendszer elleni közvetlen támadást.

A kérdéses ügyben a vidéki kisváros rendőrkapitánysága a büntető törvénykönyvről szóló 2012. évi C. törvény 375. § (1) bekezdésébe ütköző, és az (1) bekezdése szerint minősülő információs rendszer felhasználásával elkövetett csalás bűntettének megalapozott gyanúja miatt ismeretlen tettes ellen induló büntetőügyben felmerülő informatikai szakkérdések megválaszolására rendelt ki igazságügyi informatikai szakértőt.

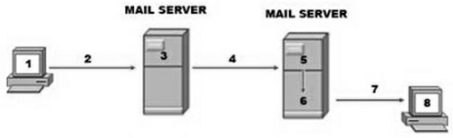
Az esettípusra jellemző, hogy közvetlenül nem fér hozzá sem a nyomozó hatóság munkatársa, sem a kirendelt igazságügyi informatikai szakértő a megtámadott rendszerhez és a támadásban érintett egyéb rendszerekhez. Az ügyben a sértett fél külföldi partnerének levelezőrendszerét érte kibertámadás a feltételezések szerint, amikor is a sértett és partnere kommunikációjában a partner helyét a támadó vette át, aki a partner helyett eljárva az igénybe veendő szolgáltatásért pénzt csalt ki a sértettől. A kommunikáció a sértett gmail-fiókjában volt.

A kérdéses ügyben tehát a potenciális digitális bizonyítékokat egy felhőszolgáltatásból – *software as a service,* azaz felhőből szolgáltatott szoftver – kellett kinyerni, amihez a sértett együttműködését vette igénybe a szakértő. A művelet során a sértett belépett a saját Gmail-fiókjába, ahol a levelezési szolgáltatásban a szakértő közreműködésével megjelölte az ügy szempontjából releváns levélpéldányokat, amelyeket a szakértő *SZAKÉRTŐ* címkével (tag) látott el. Az így megjelölt levélpéldányokat a szakértő a Google saját archiválási szolgáltatása felhasználásával m-box formátumú, zip tömörítéssel ellátott archívumfájlba exportálta. A vizsgálat alapját mindössze a kinyert elektronikus levélpéldányok fejlécében *(header)* található továbbítási információk jelentették.

A vizsgálat nagyságának felméréséhez érdemes tisztázni néhány alapfogalmat, így az elektronikus levélküldés folyamatát is (lásd az *ábrá*t), amelynek alapvető lépései a következők:

– elektronikus levél megszerkesztése a küldő számítógépén (1);
– elektronikus levél továbbítása a küldő fél postafiókját kezelő levelezőszerver *(mail server)* felé valamilyen kommunikációs csatornán (2);
– a küldő fél postafiókját kezelő levelezőszerver fogadja, majd továbbítja a levelet a címzett postafiókját kezelő levelezőszervernek (3, 4);
– a címzett postafiókját kezelő levelezőszerver az elektronikuslevél-példányt elhelyezi a címzett postafiókjába (5, 6);
– a címzett letölti az üzeneteit valamilyen kommunikációs csatornán keresztül a saját számítógépére (7, 8).

Az elektronikuslevél-küldés folyamata



Forrás: http://ccnaq.blogspot.hu/2013/01/Refer-to-the-exhibit-The-diagram-represents-the-process-of-sending-e-mail-between-clients.html

A vázolt kommunikációs folyamatba úgynevezett beékelődéses támadással *(man-in-the-middle attack)* lehet bekapcsolódni, amelynek során a támadó informatikai alapú megtévesztést[33] használva (például címfeloldás hamisítása – *ARP spoofing;* dinamikus IP-cím-hamisítás – *DHCP spoofing,* vagy kap-

33 Chad Calvert – Taghi M. Khoshgoftaar – Maryam M. Najafabadi – Clifford Kemp: A Procedure for Collecting and Labeling Man-in-the-Middle Attack Traffic. International Journal of Reliability, Quality and Safety Engineering, vol. 24, no. 1, 2017

csolódásipont-lopás – *port stealing*) veszi át a kommunikációban részt vevő szerepét, majd az ő nevében folytatja a kommunikációt.

A vizsgált ügyben a sértett szóbeli tájékoztatása és a rendelkezésre álló adatok alapján a levelezőpartner postafiókjának jogszerű felhasználója oldalán történt beavatkozás az informatikai rendszerbe. Ebből adódóan a beavatkozással kapcsolatos digitális bizonyítékok is a postafiók jogszerű felhasználójának rendszerében keletkeztek. A fogadó (sértett) oldalán megjelenő digitális nyomok a kommunikáció során keletkezett elektronikus levelek fejlécében található továbbítási információkból származnak. Ezek alapján az a tény volt megállapítható, hogy mely IP-címekről kezdeményezték a kommunikációt a sértettel. Az IP-címeket az adott időben használó természetes személyek azonosítása az adott szolgáltatók megkeresésével és az IP-címek, valamint a küldési időpontok megadásával történhet meg az adott szolgáltató együttműködése esetén.

A vizsgálat adataiból e következtetések vonhatók le:

1. A sértett által küldött levelek nem tartalmaznak az adott postafiókot használóra vonatkozó IP-cím- és helyszínadatokat.
2. A postafiókból érkező elektronikus levelek azonosítható forráscímei a következő hálózatokból származtak:
   a) 177.209.×××.×××, 201.18. ×××.××× Oi Velox / Telemar Norte Leste S.A, Boa Vista város (Brazília, Amazonas szövetségi állam),
   b) 190.103.×××.×××, Axesat Peru S.A.C., Lima város (Peru, Lima tartomány),
   c) 181.41.×××.×××, Guyana Telephone & Telegraph Co., Georgetown város (Guyana, Demerara-Mahaic régió);
3. A postafiókból érkező elektronikus levelek továbbításában a következő kiszolgálók és szolgáltatók vettek részt:
   a) InternetNamesforBusiness.com, Fort Lauderdale város (Florida, Amerikai Egyesült Államok),
   b) ××× Kft., Budapest (Magyarország).

A rendelkezésre álló digitális bizonyítékokból az említetteknél több információ nem nyerhető ki az ügyre vonatkozóan.

Amint megfigyelhető, a feldolgozott ügyben az önálló, elszigetelt vizsgálat alig hoz eredményt. Feltételezve, hogy a csalás több sértettet is érinthetett, az információk összegyűjtése és megosztása – a nemzetközi bűnügyi adatcsere – lehet a megoldás a bizonyítás hiányosságaira.

Mivel a sértetti oldalon az Európai Unió és más európai országok állampolgárai mellett dél-amerikai gazdasági társaság is megtalálható (tudniillik a magyarországi sértett üzleti partnere) és az elkövetői oldalon álló személyek kiléte az elszigetelt vizsgálat adataiból nem állapítható meg, feltételezhető, hogy a nemzetközi együttműködés megszervezése és lebonyolítása nem lesz egyszerű folyamat. Ez a kérdés ugyanakkor messze túl mutat jelen tanulmány vizsgálati körén, mindamellett rendkívül fontos és a büntetőeljárások eredményét is jelentősen befolyásoló körülményről van szó, különösen a tárgyalt kiberbűncselekmény-típus esetén.

A GDPR várható hatásai a kiberbűncselekmények szakértői vizsgálatára

Amikor kiberbűncselekmények igazságügyi informatikai szakértői vizsgálatáról és a cselekmények felderítésének lehetőségeiről beszélünk, nem hagyhatjuk figyelmen kívül a jogi környezet aktuális változását, amely akár jelentősen is befolyásolhatja a vizsgálatok sikerességét.

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.), amely a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (*General Data Protection Regulation; GDPR* – általános adatvédelmi rendelet) szól, 2018. május 25-től alkalmazandó az unió tagországaiban.

Már többen is felhívták a figyelmet – ahogy azt a legutóbb az Európai Jogi Szaktanácsadói Hálózat *Digitalizáció* című konferenciájának büntetőjogi szekciójában megtartott előadásában[34] *Kökényesi-Bartos Attila* ügyész is megtette – arra, hogy megszűnik az IP-címekhez kapcsolódó információk – amelyek közül az egyik legfontosabb a doménregisztrációt végző személy(ek) adatai – visszakeresésére használt WHOIS-adatbázisok nyilvános elérése. Mivel a WHOIS-adatbázisokhoz történő hozzáférés elengedhetetlen a kiberbűncselekmények elleni hatékony fellépés és a felderítés területén, zavar keletkezhet a büntetőeljárás során a nyomozó hatóságok és az igazságügyi informatikai szakértők munkájában.

34 Kökényesi-Bartos, Attila: Overview of cybercrimes & European Judicial Cybercrime Network. Digitalisation – Criminal Law Section. Budapest, 05. 23. 2018.

Az IP-cím-tartományok kiosztásáért és a tartománynév-regisztrációért felelős szervezet *(Internet Corporation for Assigned Names and Numbers; ICANN)* úgy döntött, hogy a nyilvánosan elérhető WHOIS rendszert offline állapotba helyezi a személyes adatokhoz történő hozzáférés tekintetében a GDPR előírásainak megfelelően.[35] Az ICANN a GDPR alkalmazásának megkezdése utáni időszakra átmeneti modellt[36] javasol a rétegzett hozzáférés érdekében, ez egy akkreditációs rendszerbe történő bejelentkezést jelent a szolgáltatást igénybe venni kívánó szervezetek – például nyomozó hatóságok – részéről.

A Számítástechnikai Bűnözés Elleni Európai Igazságügyi Hálózat *(European Judicial Cybercrime Network; EJCN)* nyilatkozatban figyelmeztette az Eurojustot[37] és az Európai Tanácsot a WHOIS-adatbázisokhoz történő jogszerű hozzáférés várható következményeiről, amelyek között büntetőügyekben folyó nyomozások akadályoztatása, valamint a biztonságra és az áldozatok jogaira gyakorolt káros hatások is szerepeltek.[38]

Az előbbiekben írtak gyakorlatban tapasztalható hatásaként említhető, hogy a második és a harmadik esettanulmányban szereplő kiberbűncselekmények feltárásához alapvető fontosságú a Regionális Internetregiszterek *(Regional Internet Registries; RIRS)* adataihoz történő hozzáférés, amely meggyorsíthatja a kérdéses ügytípusok felderítését.

Összegzés

A bemutatott példák csupán szűk szegmensét fogták át a kiberbűncselekmények széles skálájának, mindamellett rámutattak azokra a fontos és néha kritikus pontokra, amelyek esetében nélkülözhetetlen az igazságügyi informatikai szakértők és a nyomozó hatóságok munkatársainak szorosabb együttműködése. Ennek az együttműködésnek a formája még vitatott[39], mindazonáltal nyilvánvalóan szükséges is.

Ugyancsak szükségesnek látszik a nyomozó hatóság potenciális digitális bizonyítékokkal kapcsolatba kerülő munkatársainak képzése, továbbképzése

35 Uo. 48–50. o.

36 Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to the European Union's General Data Protection Regulation – For Discussion. ICANN, 01. 12. 2018. https://www.icann.org/en/system/files/files/interim-models-gdpr-compliance-12jan18-en.pdf

37 Az bűnözés súlyos formái elleni fokozott küzdelem céljából a tanács 202/187/IB határozatával létrehozott európai uniós szerv.

38 Kökényesi-Bartos Attila: i. m. 50. o.

39 Simon Béla: i. m. 399. o.

is. Végső célként megfogalmazható a digitális bizonyítékok helyszíni vizsgálója tudásszint elérése, rövid és középtávú célként pedig ennek megközelítése, de legalább az ez irányba történő elmozdulás.

A képzés és továbbképzés információhordozóiként olyan eszközöket kell használni, amelyek akár a napi gyakorlatban is használhatók, s amelyekre találhatunk jó és követendő példákat.[40] Ezek meghonosítása a hazai gyakorlatban olyan szereplőkre – szellemi műhelyekre – hárul, mint a milyen a Nemzeti Közszolgálati Egyetem Rendészettudományi Karán újonnan alakult kiberbűnözés elleni tanszék, illetve a Magyar Igazságügyi Szakértői Kamara Informatikai és Hírközlési Szakmai Tagozata.

40 Best Practices For Seizing Electronic Evidence v.3 A Pocket Guide for First Responders. U.S Department of Homeland Security / U.S. Secret Service, 2006. https://publicintelligence.net/u-s-secret-service-best-practices-for-seizing-electronic-evidence/