DOI: 10.38146/BSZ.2018.7-8.5

NAGY TAMÁS

Business E-mail Compromise, avagy az átutalásokhoz kapcsolódó csalások

Az információs társadalom[1] korában az információ olyan önálló értékké kezd válni, amely a termelésben, a gazdaságban, illetve a társadalmi működésben is egyre fontosabb szerepet tölt be. Az információ, illetve ezzel szoros összefüggésben annak előállítása, elosztása, terjesztése és használata mára a technológiai fejlődés alapja. E folyamat eredménye, hogy az információfeldolgozáshoz szükséges technológiák globális szinten is beépültek a mindennapjainkba, ami a gazdasági, szociális vagy akár kulturális tevékenységeinket is nagymértékben megkönnyíti. A társadalmi átalakulás pozitív hatása mellett azonban fontos megemlíteni azokat a nehézségeket is, amelyek a technikai átalakulás következtében kerültek előtérbe. A gazdaság és a pénzügyi szektor legtöbb tevékenységét – kiváltva az emberi tényezőt – immár számítógépek végzik, ez azonban korántsem jelenti azt, hogy e rendszerek sérthetetlenek lennének. A biztonsággal kapcsolatos értelmezések viszonylag új eleme a kiberbiztonság, amely az adatokra és az információs rendszerekre leselkedő veszélyekre fókuszál.[2] A technológiai környezet folyamatos változása olyan új fenyegetéseket idézett elő ugyanis, amelyek közös jellemzője, hogy jogilag viszonylag meghatározatlanok, előfordulásuk tömegességéből adódóan azonban jelentős károkat képesek okozni.[3] A felvetődő kockázatok kezelése összetett és sokrétű feladat, amely az átfogó intézkedések mellett (ilyen például Magyarország Nemzeti Kiberbiztonsági Stratégiája[4], illetve az EU 2016/1148 irányelve[5]) egy-egy terület önálló felkészítését is szükségessé teszi. Véleményem szerint ebből a szempontból kiemelt szerep jut a nyomozó hatóságoknak, mivel a biztonság e for-

1 Az információs társadalom fogalmát *Fritz Machlup* amerikai közgazdász vezette be a *The production and distribution of knowledge in the United States* (A tudás termelése és elosztása az Egyesült Államokban) című, 1962-ben megjelenő művében.

2 Robert Fischer – Edward Halibozek – David Walters: Introduction to security. Elsevier Inc., New York, 2013, p. 435.

3 Nagy Zoltán András: Bűncselekmények számítógépes környezetben, Ad Librum Kiadó, Budapest, 2009, 21. o.

4 1139/2013. (III. 21.) kormányhatározat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.

5 Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész unióban egységesen magas szintjét biztosító intézkedésekről.

májának megteremtésében a bűnüldözés szerepe megkérdőjelezhetetlen. Az új típusú nehézségek kezelésének időszerűségét jelzi, hogy a büntető törvénykönyv önálló fejezetében (XLIII. fejezet) foglaltak mellett[6] manapság már szinte valamennyi intellektuális bűncselekmény kapcsolódik az információs rendszerekhez. E mű középpontjában a csalás olyan újonnan megjelent formája áll, amelynek egyedi jellegét az adja, hogy az információs rendszerek működése mellett nagymértékben épít azokra az emberi tényezőkre is, amelyek megfelelő eszközökkel könnyedén befolyásolhatók. A következő oldalakon igyekszem röviden bemutatni a cselekménnyel kapcsolatos ismérveket és tapasztalatokat, továbbá olyan gyakorlati ajánlásokat megfogalmazni, amelyek – megfelelő körülmények között – elősegítik a megelőzést és a bűncselekmények felderítését.

Business E-mail Compromise a bűnügyi terminológiában

Az angolszász rendvédelmi terminológiában a Business E-mail Compromise (a továbbiakban: BEC) olyan bűncselekményi kört jelöl, amely kifejezetten a rendszeres pénzügyi tranzakciókat lebonyolító gazdasági szereplőket célozza. E bűncselekménytípus különleges jellemzője, hogy a pénzügyi átutalási[7] (vagy kifizetési) rendszerek működését befolyásolják a rendszert kezelő vagy irányító személyeken keresztül. Ahogy utaltam rá, a megnevezés összetett fogalmi kategóriát jelöl, amiben a legtipikusabb elkövetési módok a következők:

a) A cselekmény legjellemzőbb formája elsősorban a külföldi beszállítókkal dolgozó cégek esetében jelent valós veszélyt, mivel itt gyakorlati akadályai is lehetnek az ellenőrizhetőségnek. A támadók ebben az esetben hamis számlázási adatokat adnak meg a beszállítók nevében (és e-mail-címét felhasználva), jellemzően adatváltozásra vagy egyéb külső körülményre hivatkozva. Az adatváltozással érintett számlaszám természetesen nem a beszállítóhoz, hanem az elkövetőkhöz kapcsolódik.
b) Nem sokban különbözik az előbbi esettől az, amikor valamely vállalati vezető jogosultságait felhasználva adnak hamis utasítást a kifizetésre vagy pénzügyi ellenjegyzésre jogosult alkalmazottaknak.

6 A büntető törvénykönyvbe 1994-ben került be önálló bűncselekményi kategóriaként a számítógépes bűncselekmények normatív fogalma.

7 A bankszámla-tulajdonos (kifizető) kezdeményezésére teljesített olyan átírás, amely során a pénzintézet fizetés céljából pénzösszegeket vezet a kifizető bankszámlájáról a kedvezményezett bankszámlájára. Az átutalásokat belföldi és nemzetközi pénzforgalomban egyaránt használják.

c) Előfordulhat olyan eset is, amikor a kifizetésre vagy ellenőrzésre jogosult e-mail-fiókját feltörik, majd az onnan beszerzett adatokat felhasználva kérnek kifizetést valamely valós pénzügyi partnernek oly módon, hogy a számlaadatokat előzetesen megváltoztatták.
d) Bizonyos esetekben, az e-mailben a csalók olyan bizalmi személynek (adótanácsadó, ügyvéd, könyvelő stb.) adják ki magukat, aki az általános működésben részt vesz, azt a látszatot keltve, hogy az általuk kért átutalás hozzá tartozik a cég nem rendszeres pénzügyi tevékenységéhez.
e) Az előbbieken túl azokat a cselekményeket is a BEC körébe szokták sorolni, amikor a személyzeti vagy könyvelési alkalmazottakon keresztül szereznek azonosításra alkalmas személyes adatokat, amelyeket a korábban említett módokon használhatnak fel.[8]

Ahogy az egyes példák is mutatják, valamennyi elkövetési séma osztozik bizonyos közös jellemzőkön. Ilyen például az, hogy

– az elkövetők célja az anyagi haszonszerzés, amit a pénzügyi átutalások révén kívánnak megvalósítani;
– az elkövetés eszköze maga az elektronikus levél (e-mail), amelyet formailag és tartalmilag is úgy hoznak létre, hogy annak egyedi vonásai ne keltsenek gyanút (az e-mail nem tartalmaz olyan rosszindulatú hivatkozást vagy csatolmányt, ami miatt fennakadhatna a biztonsági rendszereken);
– az elkövetők minden esetben befolyásolnak olyan személyeket, akik a pénzügyi tevékenységben közreműködnek, vagy azokat irányítják.

A cselekménynek nincs általánosan elfogadott meghatározása, valószínűleg azért, mert maga az elkövetési mód sem egységes. A leírásra használt (és mára általánosan elterjedt) Business E-mail Compromise (BEC/AEC) elnevezést először az FBI[9] kezdte el használni, az egyes bűncselekményekkel kapcsolatos útmutatóiban. Mivel a BEC világszerte egyre elterjedtebb formája a csalásnak, ezért az ügynökség minden évben kiad egy olyan jelentést, amely összefoglalja a cselekménnyel kapcsolatos irányvonalakat, tendenciákat és teendőket. A legutóbbi, 2017-ben készült kiadvány statisztikai összefoglalója alapján a 2013 októberétől 2016 decemberéig eltelt időszakban több mint 40 203 olyan incidens történt világszerte, aminek elkövetési módszere meg-

8 Forrás: www.fbi.gov

9 Federal Bureau of Investigation (Szövetségi Nyomozóiroda) = az amerikai igazságügyi minisztérium (Department of Justice) alá tartozó, szövetségi szintű nyomozószerv, a legkiterjedtebb nyomozati jogkörrel az Amerikai Egyesült Államok területén.

egyezett a leírtakkal. A rendelkezésre álló adatok alapján e bűncselekmények mintegy 5 302 890 448 dollár kárt okoztak világszerte.[10] A jelentés alapján világosan körvonalazódik az a tendencia, miszerint a BEC nemcsak világméretűvé vált, hanem egyúttal nemzetközi jelleget is öltött. Az elmúlt években 131 országban követtek el ilyen cselekményeket úgy, hogy az elkövetőkhöz kapcsolódó bankszámlákat 103 országban azonosítottak.

Az elkövetés különleges jegyei

A Business E-mail Compromise gyakorlati szempontból a csalás nagyon kifinomult formájának tekinthető, amelyet nemcsak az tesz veszélyessé, hogy az alapvető eszközként használja a információs rendszerek nyújtotta előnyöket, hanem az is, hogy az elkövetés szinte valamennyi esetben jól megtervezett. Ez a tervszerűség magában foglalja azt, hogy az elkövetők sokszor akár több hónapos felkészülés után hajtják végre a cselekményt, ezzel egyidőben pedig megfigyelik, illetve adatot gyűjtenek a leendő célpontról. Az adatgyűjtés célja az érintett vállalkozással kapcsolatos információk beszerzése, a célpont releváns körülményeinek (különösen a pénzügyi szokások) felderítése, ami különösen a következőkre terjedhet ki:

– a vállalkozás tevékenységének és üzleti kapcsolatrendszerének feltérképezése (a vállalkozással üzleti/pénzügyi kapcsolatban álló egyéb vállalkozások és magánszemélyek);
– az állandó pénzügyi partnerek, illetve az egyes partnerekhez kapcsolódó részletes pénzügyi adatok beszerzése (szolgáltatás/tevékenység jellege, fennáll-e szerződéses jogviszony a felek között, kapcsolattartó adatai stb.);
– a főkönyvi számlákon szereplő egyéb azonosítható bejegyzések adatainak beszerzése (ki- és befizetések, csoportos beszedési megbízások, jóváírások és terhelések összege, jogcíme, kamatai stb.);
– a pénzügyi tranzakció önálló indítására és/vagy jóváhagyására jogosult személyek beazonosítása, illetve az e jogosultakra vonatkozó személyes adatok beszerzése;

10 Forrás: www.ic3.gov FBI-Internet Crime Compliant Center (internetes bűncselekmények panaszközpontja). A kiadvány statisztikai összefoglalójához nemcsak az egyes országok rendvédelmi szerveinek, hanem a nemzetközi pénzintézeteknek és gazdasági szereplőknek a beszámolóit is felhasználják, ezért a téma kapcsán általánosan elfogadott hivatkozási pontnak tekinthető.

– a vállalkozás által használt informatikai vagy hírközlő hálózat sajátosságainak (például levelezési program, operációs rendszer stb.) azonosítása, illetve az ezekhez való – korlátozás nélküli – hozzáférés biztosítása.

A gyakorlati tapasztalatok alapján az ilyen jellegű nyomozások általános jellemzője, hogy a hatékony felderítés, illetve az ahhoz kapcsolódó vagyonvisszaszerzés sikere nagyrészt azon múlik, hogy a rendelkezésre álló adatokat milyen gyorsan képesek a hatóságok beszerezni és értékelni. Ezzel összefüggésben fontos megjegyezni, hogy a BEC esetében – a pénzforgalmi adatok mellett – a levelezéshez kapcsolódó információk egyúttal a cselekmény felderítésének kulcsmomentumai is. Természetesen joggal vetődik fel a kérdés: miért is fontos ezt kiemelni?

A cselekmény szűkebb értelemben vett elkövetési eszköze az a megtévesztő jellegű e-mail, amelynek célja a címzett tévedésbe ejtése annak érdekében, hogy a kifizetésre jogosult az eseti vagy visszatérő jellegű tranzakció során az elkövető által megadott – e-mailben szereplő – számlaszámot tüntesse fel a tranzakció során.[11] A BEC esetében, függetlenül attól, hogy a cselekmény megelőzése vagy felderítése a cél, elengedhetetlen a cselekményhez kapcsolódó alapvető technikai kérdések tisztázása. A hazai és a nemzetközi gyakorlat azt mutatja, hogy a kompromittáló e-mailek azért alkalmasak a csalás elkövetésére, mert a legtöbb esetben formailag és tartalmilag is azt a látszatot keltik, hogy egyrészt a küldőként megjelölt személytől vagy pénzügyi partnertől származnak, másrészt valós követelésre vagy pénzügyi teljesítésre vonatkoznak. Ahhoz, hogy az elkövető ezen e-maileket kellőképpen előkészíthesse, be kell szereznie azokat az egyedi információkat, amelyek például a felek közötti kapcsolattartás jellegére, formájára vagy rendszerességére utalnak. Ennek kézenfekvőbb eszköze valamely felhasználó adatainak megszerzése, illetve az SMTP-szerverhez[12] kapcsolódó számítógép ellen végrehajtott vírustámadás. Ha az elkövető hozzáférése biztosított, a levelezési rendszer adatai alapján kiválasztja azt a partnert, amelynek inkognitóját a csalás elkövetéséhez felhasználja. Hogy az érintett felek ne fogjanak gyanút, az elkövető a kommunikációs csatorna (vagyis a számítógépes hálózat) átirá-

11 Az ilyen típusú csalásoknak létezik olyan formája is, amely esetén az e-mail lakossági szolgáltatások kisebb összegű elmaradásáról tájékoztat. Az e-mail a szövegtörzsében szereplő linken keresztül – hitelesnek tűnő – fizetési felületet biztosít, ennek kitöltése révén azonban az elkövetők megszerzik a sértett kártyaadatait.

12 A Simple Mail Transfer Protocol rövidítése, amely azt a szervert jelöli, amely a levelezéshez kapcsolódó szolgáltatást lehetővé teszi.

nyításával eléri, hogy a rendszer a kimenő üzeneteket minden esetben az általa kiválasztott (vagy létrehozott) címre továbbítsa. A gyakorlatban ezt közbeékelődéses támadásnak[13] nevezik, mivel a felek közötti kommunikációt úgy befolyásolja a támadó, hogy mindkét szereplő számára a másik félnek adja ki magát. Az üzenetváltások során a felek így valójában nem egymással, hanem a támadóval állnak kapcsolatban, aki az így beérkező üzeneteket (különösen azok tartalmát) felhasználja az átutalások manipulálására.

Az előbbiek is jól mutatják, hogy a nyomozó hatóságok számára miért is nélkülözhetetlen a levelezőrendszerekhez kapcsolódó adatgyűjtés (lefoglalás), majd az ezzel összefüggő elemző-értékelés. Ha a hálózatba történő behatolás módja (például trójai vírus vagy külső bejelentkezés) meghatározható, akkor az elkövetés helye, illetve az elkövetők személye nagyobb bizonyossággal azonosítható, mint az utalásokhoz kapcsolódó adatok önálló elemzésével. Mivel a kedvezményezetti számlaszám tulajdonosa általában olyan személy, aki pénzügyi – vagy egyéb – ellenszolgáltatásért cserébe létrehozza és fenntartja az érintett számlát, ezért utóbbi elsősorban e személyek azonosításához elegendő.

A cselekmény időszerűsége

A pénzügyi szektort vagy a gazdaság szereplőit célzó csalások hazai viszonylatban is egyre elterjedtebbek, miközben az ezekkel kapcsolatos, a cselekmények önálló felismerését célzó ismeretek kevésbé kimunkáltak. A BEC nagyobb számban először az Amerikai Egyesült Államokban jelent meg (a cselekmény leírására használt műszót is innen vette át például az Europol), ahol évről évre a kiberbűncselekmények egyre nagyobb hányada célozza az átutalási rendszereket, illetve okoz közvetlen károkat a pénzügyi szektorban. Mivel a cselekmények technikai összetettsége sok esetben szinte lehetetlenné teszi az utólagos felderítést, ezért az elmúlt években – a prevenciót hangsúlyozva – több olyan összefoglaló is napvilágot látott, amely a bűncselekmények fontosabb elemeinek bemutatását célozza. Ezek közül az FBI által készített prezentációs anyag az, amely a legkidolgozottabb formában tárja elénk, és – időrendben – egyúttal négy fontos mozzanatát különbözteti meg a cselekménynek.

13 Azonos jelentéssel bír a szakmai gyakorlatban szintén elterjedt *man-in-the-middle* angol kifejezés is.

A célpont kiválasztása

Az elkövető (vagy elkövetői csoport) kiválasztja azt a vállalkozást vagy személyt, amelynek pénzügyi portfóliója, illetve alkalmazotti (vagy vezetői) köre előzetesen megfelel azoknak a feltételeknek, amelyek alkalmassá teszik a kompromittálásra (ilyen például a nemzetközi ügyfélkör, a széles tevékenységi kör vagy az angol munkanyelv). A kiválasztás során nyílt adatgyűjtéssel is könnyen feltérképezhető a célpont profilja. Jelentős szerepet kaphatnak például azok a közösségi tartalmak, amelyekkel – közvetve vagy közvetlenül is – a vállalkozás működésére vonatkozó információ szerezhető be (például kapcsolati háló, munkarend, munkahelyi szokások stb.).

Célzott támadások

Az előzetesen beszerzett információk birtokában az elkövető célzott támadásokat indít vezető beosztású, vagy a pénzügyi területen tevékenykedő és a kifizetésekre jogosult személyek ellen. Az elkövetők az e személyekhez kapcsolódó tevékenységük során a manipuláció és nyomásgyakorlás különböző eszközeire építenek. Az ehhez szorosan kapcsolódó fiktív e-mailek vagy telefonhívások mellett (amely az emberi tényezőt célozza) megjelennek azok az eszközök is, amelyek például az informatikai rendszereket támadják. Ennek eszközei például az úgynevezett trójai vírusok vagy egyes kémprogramok, amelyek célja a rendszerbe való bejutás, valamint a rendszer sebezhetőségének felmérése. Fontos körülmény, hogy az említett kibertámadások célja nem a zavarkeltés, hanem a rendszer felhasználói adatainak – különösen az egyes profilokhoz kapcsolódó felhasználónevek, jelszavak és kódok – megszerzése, mivel ezek birtokában fizikai jelenlét nélkül is lehetséges a számítógépes hálózat közvetlen befolyásolása.

A pénzügyi ügylethez kapcsolódó adatok cseréje

A szükséges adatok beszerzése után az elkövető az általa kiválasztott pénzügyi partner arculatát (logó, elnevezés, karakterek, szimbólumok stb.) és e-mail-címét felhasználva[14] célzott e-mailt küld a vállalkozás munkavállalójának vagy tisztviselőjének. E levelek azt a látszatot keltik, hogy a küldőként megjelölt személytől vagy szolgáltatótól származnak és – a felek között fennálló üzleti

14 Az üzenetek eltérítésével vagy hamis e-mail-kliens (például közbeiktatott karakter) létrehozásával.

kapcsolat alapján – valós követelésre vagy pénzügyi teljesítésre vonatkoznak. Gyanúra adhat okot a kedvezményezett számlaadatainak változásáról szóló értesítés, vagy a küldő e-mail-címében felbukkanó eltérés is (például diamond-techniques@diamond.com helyett diamondtechniques@dyamond.com).

Átutalás, továbbutalás

Az e-mailben foglaltak alapján a megtévesztett személy utalást indít vagy utalást hagy jóvá a csalók által megadott kedvezményezetti számla vonatkozásában. Az eddig feltárt magyarországi esetek azt mutatják, hogy az átutalások a legtöbb esetben belföldi pénz- vagy hitelintézetek által vezetett folyószámlára érkeznek. A számlatulajdonosként bejegyzett vagy az ezek felett rendelkező személyek jellemzően olyan strómanok, akik anyagi ellenszolgáltatásért cserébe létrehozzák és fenntartják a számlát. A vagyoni hátrány megtérítése kapcsán e személyek szerepe sem mellékes, mivel a számla kezelésével összefüggésben ők azok, akik a továbbutalással vagy készpénzfelvétellel az elkövetők rendelkezésére bocsátják a megszerzett összeget. (Itt fontos megjegyezni, hogy a számla fenntartása, kezelése, illetve az annak egyenlegét érintő pénzügyi műveletek alkalmasak lehetnek a Btk.[15] 399–400. § szerint meghatározott pénzmosás bűntettének megállapítására.)

A normatív háttérről

A Business E-mail Compromise, vagyis az átutalásokhoz kapcsolódó csalások nem sokban különböznek a bűncselekmény más formáitól, egyedileg vizsgálva mégis olyan jellemzőkkel bírnak, amelyek felismerése a nyomozás kapcsán kiemelten fontos. Mivel a cselekmény felismerése kéz a kézben jár annak jellegzetes vonásaival, ezért érdemes lehet a fontosabb jellemzőit külön is kiemelni:

– a cselekmény célpontja a legtöbb esetben olyan – előre kiválasztott – természetes vagy jogi személy (gazdasági társaság, befektető stb.), akinek, illetve amelynek tranzakciós forgalma jelentős (számszerűségét, illetve az egyes tranzakciók értékeit figyelembe véve);
– a cselekmény előkészítésének lényeges eleme az adatszerzés, amelynek része a célpont informatikai rendszerének célzott támadása is;

15 A büntető törvénykönyvről szóló 2012. évi C. törvény.

– e támadások elsődleges célja az alkalmazotti kör feltérképezése, továbbá a felhasználói adatok megszerzése;
– az elkövető az előkészítés során azonosítja azokat a személyeket, akik átutalások kezdeményezésére vagy jóváhagyására jogosultak, majd valótlan pénzügyi teljesítésre vonatkozó célzott e-mailt küld részükre;
– a kifizetésre jogosult – abban a hitben, hogy valós kötelezettséget teljesít – utalást kezdeményez az e-mailben megjelölt számlaszámot felhasználva;
– a tranzakció jóváírása után a számla kezelője továbbutalással vagy a készpénz tényleges felvételével a csaló rendelkezésére bocsátja az így megszerzett összeget.

A hasonló jellegű bűncselekményeket vizsgálva egyértelműen megállapítható, hogy a legtöbb esetben – figyelembe véve a cselekménnyel összefüggésben keletkező eredményt, illetve az ehhez felhasznált eszközöket is – a Btk. 373. §-ában meghatározott csalás bűntette állapítható meg, így a cselekmény büntetőjogi értékelése kapcsán is ennek jellemzőit érdemes elsőként megvizsgálni:
– a cselekmény célzatos, az elkövető az általa megvalósított magatartással jogtalan haszonszerzésre törekszik;
– a cselekmény tettese bárki lehet;
– a bűnsegédi magatartás abban az esetben állapítható meg, ha valamely személy megteremti a tévedésbe ejtés vagy tévedésben tartás feltételeit;
– a csalás eredmény-bűncselekmény, eredményként az elkövetési magatartás következményét, vagyis a bekövetkezett kárt kell értékelni [Btk. 459. § (1) bek. 16. pont];
– az elkövetési magatartás része más személy tévedésbe ejtése vagy tévedésben tartása;
– amennyiben a kár nem annál a (természetes vagy jogi) személynél keletkezik, akivel, illetve amellyel szemben a tévedésbe ejtést vagy tévedésben tartást megvalósították, a bűncselekmény sértettje az a személy, akinél a kár ténylegesen bekövetkezett;
– a cselekmény rendbeliségét a sértettek száma határozza meg.

A cselekmény átutalásokhoz kapcsolódó (pénzügyi) jellegét a csalás tényállási elemeinek értékelésén túl elsősorban a – nyomozás során felvetődő – szituációs elemek vizsgálata alapján lehet megállapítani. Ezek tisztázása azért sem mellőzhető, mivel a hasonló cselekmények eltérő jogi minősítése – va-

lamint a bűncselekményi egység és halmazat kérdése – az eljárás nyomozati szakaszában is releváns szerepet játszik:

a) hely: az elkövetési magatartás megvalósításának helye (jelentőségét az illetékesség kapcsán fontos kiemelni)[16];
b) idő: mivel a cselekmény időben két jól elkülöníthető mozzanatra bontható, ezért az elkövetés ideje elsősorban a kísérlet és a befejezett bűncselekmény elkülönítésében játszik szerepet (befejezetté a hamis vagy megtévesztő e-mail elküldésével válik a bűncselekmény); ha az ehhez kapcsolódó pénzügyi tranzakció nem jön létre, befejezett kísérletről beszélhetünk;
c) mód: az elkövetési magatartáshoz kapcsolódó szituációs elem, amely ebben az esetben a hamis vagy megtévesztő – fizetési kötelezettségről tájékoztató vagy arra felszólító – elektronikus üzenet (e-mail) elküldését jelenti;
d) eszköz: szűkebb értelemben a hamis vagy megtévesztő tartalmú e-mail, tágabb értelmezésben pedig az a fizikai kiterjedésű informatikai eszköz vagy rendszer, amelyet ehhez felhasználnak.

Elhatárolások

Az eljárásokban a cselekmény jogi megítélése mellett fontos szerepet játszik az is, hogy a rendelkezésre álló információk birtokában a hasonló bűncselekményeket megfelelő módon lehessen egymástól elhatárolni. A BEC kapcsán ez több okból sem mellékes: egyrészt több olyan vonással is bír, amelyek miatt könnyen előfordulhat a cselekmény téves jogi megítélése, ami a hatékony hatósági fellépést is nehezíti (például a nem megfelelő elektronikus adatok lefoglalásával), másrészt nem kizárt több olyan bűncselekmény megállapítása az elkövetés kapcsán, amelyek utólag halmazatként értékelhetők. Az elhatároláshoz szükséges legfontosabb érdemi különbségeket – a teljesség igénye nélkül – a következő felsorolás tartalmazza.

Gazdasági csalás

„Aki jogtalan haszonszerzés végett színlelt gazdasági tevékenységet végez, és ezzel vagyoni hátrányt okoz, gazdasági csalást követ el.”[17]

A gazdasági csalás célzata (jogtalan haszonszerzés), illetve az elkövetési magatartással összefüggésben bekövetkező eredmény (kár) azonos ugyan, azonban

16 Az ügyészek a nyomozás, illetve a vádemelés során – általánosságban – a magatartás megvalósításának helyére alapítják az illetékességet (KF.6908/2005/7-II.).
17 Btk. 374. §

a gazdasági csalás elkövetési magatartása minden esetben valamilyen színlelt gazdasági tevékenységhez[18] kapcsolódik (ez összetettségében túlmutat a tévedésbe ejtésen vagy tévedésben tartáson). Az elhatárolás alapja az, hogy a hamis vagy megtévesztő elektronikus üzenet – hiába utal gazdasági tevékenység alapján fennálló követelésre – nem értékelhető színlelt gazdasági tevékenységként.

Információs rendszer felhasználásával elkövetett csalás[19]

„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.”[20]

Az információs rendszer felhasználásával elkövetett csalás célzata szintén a jogtalan haszonszerzés, a büntetőjogi szabályozás által védeni kívánt jogi tárgyként azonban – a vagyoni viszonyok mellett – megjelenik az információs rendszerek, és a készpénzkímélő fizetés zavartalan működéséhez fűződő társadalmi érdek is. Az e-mailek felhasználásával elkövetett csalást különösen a Btk. 375. §-ában megjelenő tényállás első és második fordulatától szükséges elhatárolni. Elviekben ugyanis elképzelhető a jogtalan haszonszerzés átutaláshoz kapcsolódó olyan formája, amikor az elkövető fizetési vagy pénzügyi elszámolórendszerek befolyásolásával (például könyvelési rendszerben új kedvezményezett rögzítésével vagy a hozzá kapcsolódó számlaszám megváltoztatásával) valósítja meg az utalást.

Tiltott adatszerzés

„Aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából

c) más közlést tartalmazó zárt küldeményét felbontja vagy megszerzi, és annak tartalmát technikai eszközzel rögzíti,

18 Gazdasági tevékenységnek valamely tevékenység üzletszerű, illetve tartós vagy rendszeres jelleggel történő folytatása minősül, amennyiben az ellenérték elérésére irányul vagy azt eredményezi, és annak végzése független formában történik. A személyi jövedelemadóról szóló 1995. évi CXVII. tv. 3. § 46. pont.

19 A cselekmény önálló szabályozása a korábbi Btk. (1978. évi IV. tv.) 1994. évi módosításával, számítógépes csalás néven került be a szabályozási környezetbe. Az önálló szabályozás szükségességének indoka az volt, hogy az elkövetési magatartásból hiányzik a klasszikus értelemben vett tévedésbe ejtés vagy tévedésben tartás.

20 Btk. 375. §

d) elektronikus hírközlő hálózat – ideértve az információs rendszert is – útján másnak továbbított vagy azon tárolt adatot kifürkész, és az észleleteket technikai eszközzel rögzíti, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő."[21]

A tiltott adatszerzés törvényi tényállása számos esetben lefedi azt a tevékenységet, amely a csalás kapcsán az elkövető előkészületi tevékenységeként is értékelhető (személyes adatot, illetve – a sértett gazdasági tevékenységével összefüggésben – gazdasági vagy üzleti titkokat derítenek fel). A tiltott adatszerzés a csalással, illetve más – az információs rendszereket sértő – bűncselekményekkel halmazatban is megállapítható.

Információs rendszer vagy adat megsértése

„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.
(2) Aki
a) az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza, vagy
b) információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz,

bűntett miatt három évig terjedő szabadságvesztéssel büntetendő."[22]

A családhoz kapcsolódó adatgyűjtő tevékenység büntetőjogilag önálló formában úgy is értékelhető, ha az elkövető által megvalósított magatartás – amennyiben tiltott adatszerzés nem valósul meg – az információs rendszerek vagy adat sérelmével jár. A Btk. 423. § (1)–(2) bekezdésében foglalt tényállás elkövetési tárgya az információs rendszer vagy adat, amely egyúttal a tiltott adatszerzéstől való elhatárolásának alapja is (az elkövetési magatartás ebben az esetben nem célzatos).

Az előbbiekben nevesített bűncselekményeken túl érdemes megjegyezni azt is, hogy az átutalásokhoz kapcsolódó csalás esetén az okozott kár a sértett pénzforgalmi számláin keletkezik. Ezzel összefüggésben az elkövető

21 Btk. 422. § (1) bekezdés c) és d) pontja
22 Btk. 423. §

szándéka nemcsak a téves tranzakció megvalósítására, hanem a tévesen utalt összeg feletti rendelkezésre is kiterjed. A kedvezményezetti számla lehet az elkövető saját nevén fenntartott számlaszám, jellemzőbb azonban, hogy a számla felett olyan – az elkövetővel kapcsolatban álló – személy diszponál, aki az arra beérkező összeg(ek) kezeléséért – anyagi vagy egyéb – ellenszolgáltatásban részesül. Abban az esetben, ha a számla felett rendelkezési jogot gyakorló személy az alapcselekmény elkövetésében nem vett részt, a számla kezelésével kapcsolatos magatartása (megőrzés, használat, kezelés, felhasználás vagy annak felhasználásával más anyagi javak beszerzése) a pénzmosás[23] bűntettének megállapítására lehet alkalmas.

A hatáskör és illetékesség vizsgálata

A BEC kapcsán folytatott belföldi nyomozások során a hatáskör és illetékesség vizsgálata az általános szabályoktól nem tér el. A hatáskör és az illetékesség vizsgálata kapcsán azonban – a büntetőeljárásról szóló törvényben[24] megfogalmazott, valamint az ehhez kapcsolódó végrehajtási rendeletben szereplő egyéb rendelkezések[25] mellett – érdemes figyelembe venni azokat a jogforrásokat is, amelyek a joggyakorlat egységesítése kapcsán relevanciával bírhatnak. Kifejezetten a csalásra vonatkoztatva, ilyen egyedi forrás a Kúria – büntetőjogi működésével összefüggésben keletkezett – BH 2009.11.317. számú határozata, amely kimondta, hogy az elkövetési magatartás (tévedésbe ejtés) kifejtésének és az eredmény (kár) bekövetkezésének helye mellett a károkozó magatartás kifejtésének a helye is megalapozhatja a bíróság illetékességét. A bíróság érvelésének hátterében az a nézőpont állt, miszerint a terhelt tevékenységének lényegi eleme a kár okozása, ennek megfelelően pedig a kár bekövetkezésének helye az illetékesség szempontjából sem lehet közömbös, holott azt a befejezett eredmény-bűncselekményeknél nem szokás vizsgálni.[26]

A nyomozások során az ilyen és hasonló rendelkezések figyelembevétele abban az esetben lehet releváns, ha az illetékesség szempontjából fontos tényállási elemek vagy körülmények vitatottak, vagy nem állapíthatók meg megnyugtató bizonyossággal.

23 Btk. 399. § (2) bekezdés b) pontja

24 A büntetőeljárásról szóló 1998. évi XIX. törvény.

25 A rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló 25/2013. (VI. 24.) BM rendelet 2–3. §.

26 Forrás: www.kuriaidontesek.hu

Célszerű intézkedések

A hasonló jellegű bűncselekmények felderítése során – különös tekintettel a tényállás teljes körű tisztázására – elengedhetetlen a cselekmény alapvető feltételeinek ismerete, illetve ezzel összefüggésben azon technikai jellegű bizonyítékok beszerzése, amelyek az eljárás érdemi eredménye szempontjából elengedhetetlenek. Ahogy arról korábban már szó volt, a nyomozás sikere kapcsán kritikus szerepe van az idő múlásának, vagyis a nyomozó hatóságnak – a tudomásszerzés után – haladéktalanul meg kell tennie azokat az intézkedéseket, amelyek az elkövetéshez kapcsolódó (elsősorban elektronikus) adatok megőrzését szolgálják. E körben gondoskodni kell

– a felhasználói rendszerekhez kapcsolódó belépési és műveleti adatok lementéséről;
– az egyes felhasználók adatainak beszerzéséről (különösen a felhasználónevek, jelszavak és jogosultságok tekintetében);
– a sértett korábbi számlaforgalmi adatainak teljes körű beszerzéséről (mivel a cselekményt sok esetben több hónapos előkészítés előzi meg, illetve a folytatólagos elkövetés sem kizárt, ezért indokolt a nagyobb időtartamra vonatkozó adatgyűjtés);
– a belső informatikai rendszerről, az azt kiszolgáló eszközök, illetve az egyes munkaállomásokon (vagy a munkaállomások többségén) használt programokkal kapcsolatos állapotfelmérésről;
– az elektronikus/informatikai rendszert érintő korábbi támadások, illetve az ezekkel kapcsolatban tapasztalt következmények feljegyzéséről;
– annak megállapításáról, hogy milyen adat- és vírusvédelmi megoldásokat alkalmaztak a számítógépes hálózattal összefüggésben;
– annak megállapításáról, hogy milyen könyvelési, elszámolási vagy fizetési rendszert használnak;
– a levelezési rendszert kiszolgáló (SMTP-) szerver adatainak lementéséről (ezt a sértett mellett indokolt azon vállalkozás szerverére is kiterjeszteni, amely az e-mail alapján az utalás kedvezményezettje volt)[27].

Az informatikai rendszerekben fellelhető adatok lefoglalásával és elemzésével párhuzamosan a következő nyomozati cselekmények végrehajtása indokolt:

27 Ez azért elengedhetetlen, mert a rendszer által naplózott folyamatok (hibaüzenetek, bejövő és kimenő adatok, bejelentkezések stb.) adataiból kiszűrhetők az olyan bejelentkezések, amelyek a felhasználói adatokat felhasználva, ám kívülről történtek, vagyis – bizonyos esetben – ezekből következtetni lehet a rendszer kompromittálására.

– a kedvezményezetti számlaszámhoz kapcsolódó adatok beszerzése (számla felett rendelkező személy adatainak, az általa kezelt más számlák adatainak, a számlavezető pénzintézet, a számlanyitás időpontja, valamint a kapcsolódó szolgáltatások és a teljes számlatörténet beszerzése);
– előzménykutatást kell végezni az azonos, vagy hasonló módon elkövetett bűncselekmények kapcsán;
– azonosítani kell, hogy milyen forrásból és partnerektől érkezik egyéb jóváírás a számlára;
– a vagyonelkobzás biztosítása érdekében a bűncselekménnyel összefüggésben fel kell mérni, hogy a számlatulajdonosnak milyen nagyobb értékű ingó vagy ingatlantulajdona, vagy tartozása van (a közhiteles nyilvántartások, például gépjármű- és ingatlan-nyilvántartás, illetve a KHR adatainak beszerzése);
– az azonosított számlán vagy számlákon kezelt – a bűncselekménnyel összefüggően beérkező – összegre indokolt a zár alá vétel elrendelése;
– a számlaforgalmi adatok alapján (beérkező és kimenő utalások) azonosítani kell a számlatulajdonos pénzügyi partnereit;
– listázni kell a készpénzfelvételek helyét, összegét, továbbá be kell szerezni az ezzel kapcsolatban elérhető ATM- vagy egyéb kamerafelvételeket (ha voltak ilyenek) a közreműködő személyek azonosítása érdekében.

Egy hazai példa

A Készenléti Rendőrség Nemzeti Nyomozó Iroda 2015 júniusában eljárást indított a Btk. 373. § (1) bekezdésébe ütköző, és az (5) bekezdés a) pontja szerint minősülő, különösen jelentős kárt okozó csalás gyanúja miatt. A nyomozás elrendelésére a Robert Bosch Elektronikai Kft. feljelentése alapján került sor, mivel ismeretlen személy vagy személyek a vállalat üzleti partnere, a KCE Singapore Ltd. képviselőjének nevében elektronikus levelet juttattak el a Bosch pénzügyi ügyintézőjének, ebben arra kérték, hogy a felek között fennálló (beszállítói) szerződés alapján esedékes számlák ellenértékét a megszokottól eltérő számlaszámra utalják, mivel a cég folyamatban lévő auditálása miatt a számla kezelése bizonytalanná vált. Az ügyintéző az e-mailben szereplő tájékoztatás alapján – 2015. május 6-tól június 10-ig – összesen tíz átutalást indított a megadott számlaszámra mintegy 2,2 millió dollár értékben.

A nyomozás során a következő tényállást sikerült rekonstruálni. A csalók az e-mail elküldését megelőzően a partnercég (KCE Singapore Ltd.) belső

rendszerét feltörték, majd az onnan megszerzett adatokat felhasználva támadást intéztek a Bosch belső rendszere ellen. Ennek következtében a Bosch több alkalmazottjának egyedi adatait is sikerült megszerezniük. Az elkövetők ezek birtokában több postafiókot, például az ügyintéző által kezelt belső fiókot is lemásolták, így egyebek között a cég levelezési rendszerébe beérkező, onnan kiküldött, valamint az abban kezelt levelezéshez is hozzáfértek (az egyes partnerek eltérő anyanyelve miatt az üzenetváltás angolul folyt). A levelezés, illetve a pénzügyi tevékenység adatait felhasználva a csalók kiválasztották a KCE Singapore Ltd.-t, mivel a Boschnak e céggel – nagy értékű utalások formájában – állandó pénzügyi kapcsolata volt. Az e-mailben megadott számlát a Lengyelországban működő PEKAO Bank vezette. A beszerzett pénzügyi és egyéb adatok elemzése rámutatott, hogy a számla egy fiktív lengyel cég nevén van, illetve arra is, hogy a számla felett kizárólag a cég ügyvezetőjének van rendelkezési joga (aki az Egyesült Királyság állampolgára).

A nyomozás elrendelése után a lengyel hatóságok – jogsegélykérelem alapján – zárolták a számlán lévő összeget, így a tévesen utalt összeg jelentős részét sikerült visszaszerezni (a fennmaradó kárérték közel 690 ezer dollár). Ezzel kapcsolatban fontos megjegyezni, hogy ez nagymértékben a hatóság gyors intézkedésének, illetve a külföldi hatóságok együttműködésének volt köszönhető. Az e-mail nyomozás során történő elemzése nem hozott érdemi eredményt, azt ugyanis egy olyan kanadai cégnél regisztrálták, amelynek szerverszolgáltatóját az Amerikai Egyesült Államokban jegyezték be. Az átutalásban közreműködő alkalmazottak tanúkihallgatása, illetve a rendszeradatok és naplófájlok adatai a feljelentésben szereplő tényállást támasztották alá, ezzel összefüggésben nem vetődött fel az ügyintéző vagy más személyek szándékos közreműködésének gyanúja.

A nyomozás során megállapítható volt, hogy az e-mail feladója közvetlenül nem azonosítható, mivel az üzenet egy külső szerveren keresztül, átirányítás útján került a címzetthez. A beszerzett adatok arra utaltak, hogy az e-mail eredeti feladója feltehetően Indiában él.

Mivel a jogsegély útján beszerzett dokumentumok alapján az Egyesült Királyságban és Lengyelországban is tettek feljelentést olyan csalások miatt, amelyek összefüggésbe hozhatók az érintett lengyel céggel, ezért az érintett külföldi hatóságok által feltárt adatok beszerzése érdekében a Nemzeti Nyomozó Iroda jogsegélykérelmet terjesztett elő. Az ebben foglalt nyomozati cselekmények, illetve az egyes kérdésekre vonatkozó adatok begyűjtéséig és továbbításáig az eljárást az illetékes ügyészi szerv felfüggesztette.

Következtetés

A bűnügyi rendészet szerepe kapcsán általánosan elfogadott tézis, hogy annak célja a büntető igazságszolgáltatás előkészítése, tágabb értelmezésben pedig az állam büntetőjogi igényének biztosítása.[28] Különösen fontos ez abban a folyamatosan változó környezetben, amely egyre újabb és újabb feladatok elé állítja a nyomozó hatóságokat. A bűncselekmények mögött megbúvó emberi szándék szinte semmit sem változott ugyan az elmúlt évtizedekben, az elkövetési módszerek tekintetében mégis szembetűnő különbségek tapasztalhatók. A nyomozások egyre fontosabb része tehát az az elméleti tudás és gyakorlati ismeret, amely megfelelő reakciót jelenthet a megváltozott e környezetben. Ahogy a korábbi összegzés is mutatja, a Business E-mail Compromise és a hasonló jellegű bűncselekmények veszélye nemcsak a tömeges előfordulásban rejlik, hanem abban is, hogy a sikeres hatósági eljárásokhoz új típusú szemlélet szükséges. A BEC kapcsán tett bejelentések száma 2016-ban világszerte ötven százalékkal nőtt.[29] Ez a tendencia is azt sugallja, hogy a hatékony fellépés igénye egyre sürgetőbb. Meglátásom szerint a hasonló nyomozások sikerének záloga – a megfelelő felkészítés mellett – mindazon szereplők bevonása, akik a tudásközösség kialakítása révén hatékony fellépésre képesek. A megelőzés mellett a jövőben célszerű lehet tehát a nemzetközi együttműködés olyan formáinak fejlesztése is, amelyek elméleti (például a büntetőjogi normák uniós szintű harmonizációjával) és gyakorlati szinten (például közös nyomozó csoportok[30] felállításával) is lehetővé teszik a hatóságok közötti együttműködést.

28 Finszter Géza: Rendészetelmélet. Nemzeti Közszolgálati és Tankönyv Kiadó Zrt., Budapest, 2014, 242. o.

29 Forrás: www.ic3.gov

30 Olyan nyomozó csoportok, amelyeket az Európai Unió két vagy több tagállamának hatóságai hozhatnak létre, előre meghatározott céllal, korlátozott időtartamra.