GAZDASÁG ÉS PÉNZÜGY • 11. ÉVF. 4. SZ. • 2024. DEC. • DOI: 10.33926/GP.2024.4.2

ADATHALÁSZAT ÉS AZ ELLENE TÖRTÉNŐ EGYES VÉDEKEZÉSI LEHETŐSÉGEK

Biró Gabriella – Kiss Milán[1]

ABSZTRAKT

A kiberbűnözés a digitalizáció terjedésével, különösen a pénzügyi szektor esetében, az elmúlt évek egyik legnagyobb problémájává vált. Ezen folyamatokat az elmúlt évek eseményei, így például a Covid19-pandémia inkább katalizálta, mintsem fékezte volna. A kibertámadások egyik legelterjedtebb elkövetési módja az adathalászat, amelyet a gyakorisága miatt is érdemes megvizsgálni. A cikk célja az adathalászat jelenségének és a védekezési lehetőségeknek az áttekintése, különös tekintettel a pénzügyi szektor érintettségére és a jogi szabályozásra. Először elemeztük az adathalászathoz kapcsolódó legelterjedtebb elkövetési módokat, azok technikai, illetve technológiai hátterét. Jogi szempontból a többszintű szabályozás (nemzetközi jogi, európai uniós és magyar jogi szint) miatt külön vizsgáljuk az adathalászathoz kapcsolódó magán- és közjogi szabályozást, így különösen a belső piaci pénzforgalmi szolgáltatásokról szóló irányelvet (PSD2), valamint az ennek a hazai átültetését szolgáló pénzforgalmi törvényt. Ezen szabályozás objektivizált felelősséget telepít a pénzforgalmi szolgáltatókra, továbbá fogyasztónak és mikrovállalkozásnak minősülő ügyfelek esetében a pénzforgalmi szolgáltatók számára kedvezőtlen bizonyítási szabályokat tartalmaz. A cikk vizsgálja a kapcsolódó büntetőjogi kérdéseket is, vagyis azt, hogy az egyes elkövetési módok mely büntetőjogi tényállásba illeszkednek. Mindezek után áttekintjük a releváns bűnügyi és IT-biztonsági eredményeket, azaz milyen lehetőség van arra, hogy egy adathalász támadást egy pénzforgalmi szolgáltató megelőzzön, ideértve a szolgáltatói és az ügyféloldalt is. Valamint ha az esemény már bekövetkezett, akkor milyen lehetőségek vannak a következmények elhárítására.

JEL-kódok: K24, G21

Kulcsszavak: kiberbűnözés, adathalászat, pénzforgalom

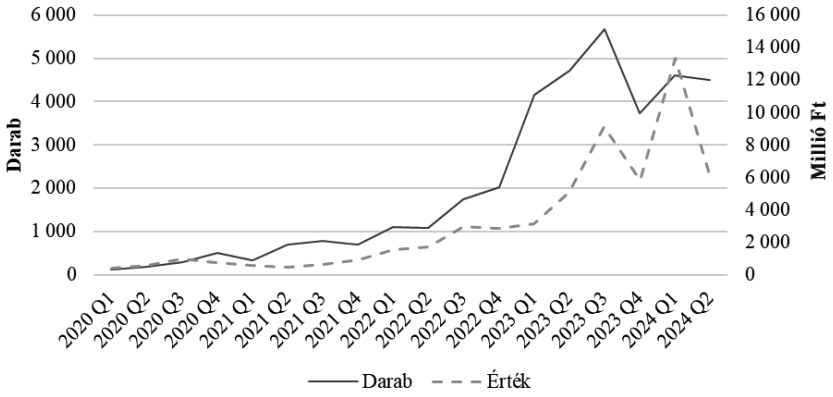
1 *Biró Gabriella* levelező szerző, IT-biztonsági szakértő, PhD-hallgató, Nemzeti Közszolgálati Egyetem. E-mail: biro.gabriella@uni-nke.hu.
Kiss Milán főosztályvezető, BinX Zrt., PhD-hallgató, Miskolci Egyetem. E-mail: milan.kiss@student.uni-miskolc.hu.

1. BEVEZETÉS

Napjainkban a kiberbűnözés a világ minden részén egyre növekvő tendenciát mutat, és jelentős gazdasági tényezővé vált (VISA, 2023). A Világgazdasági Fórum jelentése szerint a kiberbűnözés mértéke akkora, hogy ha államként fognánk fel, akkor a világ harmadik legnagyobb gazdasága lenne, csak Kína és az Amerikai Egyesült Államok előzné meg (World Economic Forum, 2024). Mindennek a legfőbb oka feltételezhetően az, hogy a technológiai fejlődéssel együtt járó digitalizáció nemcsak a legális felhasználásoknak kedvez, de a bűnözők számára is új, korábban nem látott lehetőségeket biztosít. A kiberbűnözés általános probléma, ugyanakkor a visszaélések legtöbb esetben a pénzügyi infrastruktúrákban, illetve készpénzben mozognak, amelyek közül az előbbit figyelhetjük meg (Anderson et al., 2019). Mindezek okán a jelenséget általánosságban a pénzügyi szektor érintettségén keresztül javasolt vizsgálni. Fontos azonban kiemelni, hogy a pénzügyi szektor, ezen belül a pénzforgalom különösen gyorsan fejlődik és változik (Kovács, 2010), amely megnehezíti a terület kutatását. Továbbá a szerzők is elismerik, hogy még ha a kiberbűnözés is az elemzés tárgya, amely természeténél fogva digitális, ugyanakkor ezen cselekményeknek is van a fizikai térben, illetve a készpénzzel történő fizetésekben (készpénzforgalomban) hatása. Mindazonáltal ezen hatások mérése, illetve statisztikai adatokon alapuló elemzése rendkívül bonyolult, ezért jelen tanulmányban az elektronikus pénzforgalom útján megfigyelhető visszaélésekre, különösen a magyar adatokra összpontosítunk.

A pénzügyi szolgáltatásokat igénybe vevők és a visszaéléseket elkövetők viselkedését nagymértékben meghatározza az említett szolgáltatásokra vonatkozó jogi keretrendszer. Ezen keretrendszer vizsgálata indokolt, mivel a szabályozás a bűnüldöző hatóságok eljárásán túl meghatározza a pénzügyi szolgáltatóktól a prudens működés kapcsán minimálisan elvárt intézkedéseket és eljárásokat, továbbá az ügyfelekkel, illetve egyéb szolgáltatókkal kötendő szerződéses viszonyokat is. Megjegyzendő ugyanakkor, hogy a szabályozási háttér nemzetközi jellege miatt kifejezetten bonyolult. Mindazonáltal hazánk európai uniós tagsága okán, a tagállamok jogharmonizációs kötelezettségei miatt a magyar jogszabályok, ideértve az Európai Unió közvetlenül alkalmazandó jogalkotási aktusait is, reprezentatívak lehetnek. Ezért jelen vizsgálatunk a magyar szabályozási keretrendszeren keresztül igyekszik bemutatni az adathalászat kapcsán irányadó joganyagot. A Magyar Nemzeti Bank (MNB) rendszeresen közöl statisztikai adatokat a pénzforgalmon keresztül megfigyelhető visszaélések mértékéről, amely adatok jelezhetik a probléma nagyságát, valamint annak dinamikáját.

1. ábra
Az elektronikus pénzforgalomban bekövetkezett sikeres visszaélések darabszáma és értéke



Forrás: MNB, 2024b

Ahogy az MNB által közölt adatok jól mutatják, a sikeresen végrehajtott visszaélések mind darabszámban, mind pedig értékben nagymértékben növekedtek az elmúlt öt évben. Azonban az is megállapítható, hogy a teljes elektronikus pénzforgalomhoz képest a visszaélésekkel érintett összegek még mindig elenyészőek. Az MNB megjegyzi, hogy „visszaélések során alkalmazott módszerek tekintetében 2023-ban az adathalász módszerek aránya volt a legmagasabb, az összes sikeres kártyás visszaélés 71 százalékát tette ki" (MNB, 2024a). Fontos kiemelni továbbá, hogy a CIB Bank Zrt. által megrendelt reprezentatív felmérés alapján a visszaélés áldozatává válás valószínűsége nem függ az adott személy társadalmi vagy demográfiai helyzetétől (CIB Bank, 2024).

Az MNB megállapításából is következően a kibertámadások között kiemelt jelentősége van az adathalászatnak. Az Europol[2] 2023-as IOCTA[3] jelentése szerint az adathalászat szinte tetszőleges online bűncselekménynek lehet az első lépése, előcselekménye; a 2024-es jelentés szerint pedig továbbra is ez a legelterjedtebb támadási vektor. Így például az adathalászat kulcsfontosságú az online csalási sémák és rosszindulatú programokon alapuló támadások legtöbb típusához, amely támadások célja az informatikai rendszerekbe való behatolás, az ott tárolt ada-

2 Bűnüldözési Együttműködés Európai Uniós Ügynöksége (Europol).

3 Internet Organized Crime Threat Assessment – Internetes szervezett bűnözési fenyegetettségi elemzés.

tok eltulajdonítása vagy bármilyen pénzügyi előny megszerzése (Europol, 2023; 2024c).

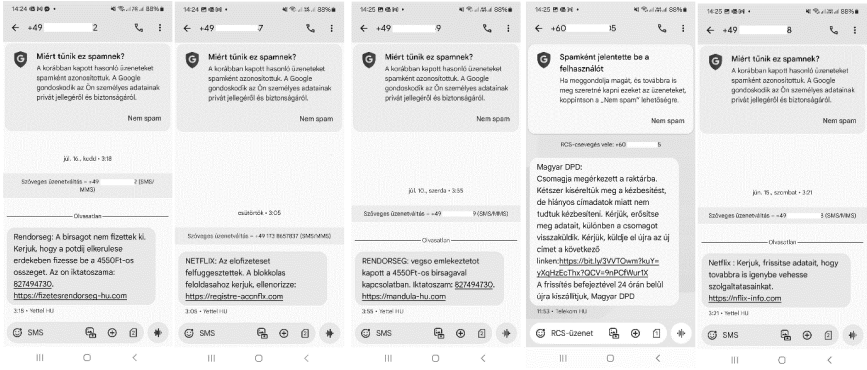
Az adathalászat jelenségének komplex vizsgálata során arra a kérdésre keressük a választ, hogy mely védekezési módok jöhetnek szóba az adathalászat elleni küzdelem során az elkövetési módokból adódóan, valamint a szabályozási, technológiai és eljárási megközelítésben, illetve ezek hogyan tudják együttesen támogatni a pénzforgalom biztonságos működését.

2. AZ ADATHALÁSZAT FOGALMI MEGHATÁROZÁSA ÉS ELKÖVETÉSI MÓDJAI

Az „adathalászat" kifejezés az angol nyelvű „phishing" magyarítása, jelentése pedig arra utal, hogy a támadók olyan adatokat, információkat próbálnak megszerezni a célpontoktól, amelyeket később fel tudnak használni anyagi haszonszerzés vagy további támadások céljából. Az adathalászat egyfajta pszichológiai manipulációs (social engineering) technika, ahol valamilyen csalit, például a célpont számára érdekesnek tűnő üzenetet (e-mail, SMS) alkalmaznak, hogy a felhasználókat rávegyék az adataik megadására vagy bizonyos káros tartalmak letöltésére, esetleg alkalmazások telepítésére, amelyek aztán technikai eszközökkel ellopják az adatokat (Oroszi, 2020).

Az adathalász támadásokat kategorizálhatjuk az üzenettovábbítási csatorna (e-mail, SMS, WhatsApp stb.), a célpontok köre (tömeges vagy célzott), valamint a megtévesztéshez használt módszer szerint. Általában, ha adathalászatról beszélünk, akkor elsősorban az elektronikus levelezésre gondolunk, de az Europol 2024-es IOCTA-jelentése szerint napjainkban a leggyakoribb adathalászati módszer a smishing, azaz SMS-adathalászat, amelyet a vishing (voice phishing), azaz csalárd telefonos hívások követnek. Szintén a 2024-es IOCTA-jelentés szerint egyre gyakoribb a quishing, azaz QR-kódos adathalászat, ahol az áldozatot arra veszik rá, hogy egy QR-kódban tárolt üzenetre reagáljon, például felkeressen egy weboldalt (Europol, 2024c). A telefonos hálózatokon keresztül végrehajtott adathalászat (smishing, vishing) esetében az elkövetők gyakran a hívószámot is meghamisítják (spoofing), így az üzenet vagy hívás címzettje azt gondolhatja, hogy valóban olyan intézmény keresi, amellyel kapcsolatban áll, pl. a pénzforgalmi szolgáltatója vagy a rendőrség.

2. ábra
Néhány példa adathalász SMS-üzenetre



Forrás: a szerzők saját gyűjtése

A köznapi életben legtöbbször tömeges adathalászattal találkozhatunk, amelyet az elkövetők minél szélesebb címzetti körhöz próbálnak eljuttatni abban a reményben, hogy a több ezer üzenetből néhány célba talál. A bűnözők többnyire nem saját költségen, hanem például feltört levelezőszervereken vagy korábbi adathalászatok áldozatainak telefon-előfizetését felhasználva küldik el az üzeneteket (György, 2021). Ezek a tömeges üzenetek többnyire nem nagyon kifinomultak, gyakran tartalmaznak elírásokat, nyelvtani hibákat vagy következetlenségeket, mivel sok esetben automatikus fordítással készülnek a magyar nyelvű változatok, bár az utóbbi években a mesterségesintelligencia-alapú megoldások elterjedésével határozott „fejlődés" figyelhető meg az üzenetek nyelvezetében. A célzott adathalászat (spear phishing vagy szigonyozás) ezzel szemben az értékes célpontokra fókuszál gyakran személyre szabott, név szerinti megszólítást tartalmazó és a célpont számára relevánsnak tűnő üzenetekkel. Egyik válfaja a bálnavadászat (whaling), mely a céges felső vezetőket veszi célba.

A célpont és a kommunikációs csatorna bizonyos mértékben meghatározza az elkövetési módot, azonban az adathalászat egyik jellegzetessége, hogy az üzenet küldője valaki mást személyesít meg az elkövetés során. A telefonhívások során gyakran valamely szolgáltató, például hitelintézet ügyintézőjének adják ki magukat az elkövetők, míg az SMS-ek többnyire állítólagos futárszolgálatoktól vagy a rendőrségtől érkeznek. E-mailben gyakoriak a közüzemi tartozásról szóló vagy szolgáltatók, esetleg hitelintézetek nevében érkező üzenetek. Az egyéb kommunikációs csatornákon (közösségi média, csevegőalkalmazások) keresztül komplexebb visszaélési forgatókönyvek valósíthatók meg, például online piactereken vevőnek adja ki magát az elkövető, és így szerzi meg az eladó egyes adatait (például hitelintézeti szolgáltatásokhoz tartozó autorizációs adatokat).

Az adathalász kommunikáció egyik ismérve, hogy az üzenet vagy hívás szerint mindig a potenciális áldozat érdekében szükséges megadni az adatokat, például azért, mert ezzel anyagi haszonhoz juthat, vagy mert veszteségeket kerülhet el, illetve előzhet meg. A hangnem szinte mindig sürgető, esetenként fenyegető is lehet, mivel az elkövetők célja, hogy az áldozatnak ne legyen ideje átgondolni a kérés jogosságát és észszerűségét. Ahogy korábban említettük, napjainkban már nem feltétlenül igaz, hogy az adathalász üzenetek könnyen felismerhetők a nyelvtani és stilisztikai hibákról, amelyek különösen a magyar nyelvű kampányokra voltak jellemzőek a korábbi években, amikor a bűnözők még nem tudtak ilyen egyszerűen jó minőségű, tetszőleges nyelvű szövegeket előállítani mesterségesintelligencia-alapú eszközök használatával.

A meggyőző szövegek nagy nyelvi modellek segítségével történő előállítása mellett a mesterséges intelligencia a kommunikáció egy másik aspektusában is a bűnözők kezére játszhat: létező kép- és hanganyagok segítségével az ún. deepfake technológia alkalmazásával lehetőség nyílik valódinak tűnő, az eredetihez nagyon hasonló videófelvételek, hanganyagok előállítására (Szabó, 2023). Ezen lehetőséget kihasználva a bűnözők akár valós idejű telefonbeszélgetést vagy videókonferenciát is kezdeményezhetnek, így még meggyőzőbben személyesíthetnek meg olyan feleket, akiknek az áldozatok gyanútlanul megadják az adataikat, vagy végrehajtják az utasításaikat. A sajtóban már több olyan dokumentált eset jelent meg, amikor online videókonferencián látszólag a cég vezérigazgatója vagy pénzügyi vezetője utasította ily módon nagyobb összegek átutalására a gyanútlan ügyintézőt (Magramo, 2024). Az Europol 2024-es tanulmánya szerint ez a forgatókönyv csak egy a mesterségei intelligencia bűnelkövetésre való felhasználásának lehetőségei közül, azonban várhatóan a jövőben az ehhez hasonló módszerek egyre elterjedtebbek lesznek (Europol, 2024a).

Az adathalász támadásokat a fenyegetések modellezésére és elemzésére széles körben használt MITRE ATT&CK® tudásbázis a felderítési és a kezdeti hozzáférés megszerzése szakaszba sorolja, amely egybevág az Europol azon megállapításával, hogy az adathalászat számos egyéb bűncselekmény előcselekménye lehet (mitre.org, 2024). Bár a két megközelítés teljesen eltérő szempontokon alapul, jól mutatják, hogy az adathalászat minden esetben csak a kezdeti lépése annak, ami a bűnüldöző szervek büntetőjogi szempontjából bűncselekmény, kiberbiztonsági szakértői szemmel pedig kibertámadás (Krasznay, 2023).

3. AZ ADATHALÁSZAT JOGI KONTEXTUSA

Az adathalászat meghatározása után érdemes lehet megvizsgálni, hogy a jogszabályok szabályozzák-e, és ha igen, akkor milyen keretrendszerben az adathalászatot és az ellene történő védekezést. Nem meglepő módon az adathalászatot a jogszabályok nem határozzák meg közvetlenül, ugyanakkor számos előírás vonatkozik a visszaélések ezen formájára.

Ulpianus óta a jogot közjogra és magánjogra szokás osztani. Ezt követően a közés magánjog jogágakra bontható tovább (Lábady, 2014). Ezek nyomán indokolt lehet a szabályozás klasszikus felosztást követő vizsgálata azzal, hogy a szabályozás nagymértékben nemzetközi, illetve európai uniós alapú. Ezen utóbbi esetében az elmúlt években egyre dominánsabbá vált a közvetlenül alkalmazandó jogalkotási aktusok használata, vagyis egyre több európai parlamenti és tanácsi rendelet alkalmazandó Magyarországon is.

3.1. Az adathalászat magánjogi megítélése és a kárviselés szabályai

Természetesen a Ptk.[4] általános szabályai szerint tilos a jogellenes károkozás (Ptk. 6:518. §–6:520. §). Ezen felelősségi szabályokat, a kapcsolódó dogmatikát, jogeseteket a jogtudomány, a közgazdáságtan részletesen feldolgozta, így például Szalai (2024). Ezen általános esetek ugyanakkor az adathalászat szempontjából nem annyira érdekesek, mivel az adathalászattal kárt okozó felet nagyon ritkán sikerül ténylegesen perbe fogni. Mindezek okán lényegesen relevánsabbak azok a károkozáshoz kapcsolódó igények, amelyek pénzforgalmi szolgáltatásokhoz kapcsolódnak. Hiszen a kibertérben elkövetett visszaélésekből származó pénzeszközöknek legvégül mindenképpen a pénzforgalmi szolgáltatókon kell keresztüláramolniuk. A szabályozás alapját a belső piaci pénzforgalmi szolgáltatásokról szóló irányelv: a PSD2[5], illetve a hazai jogba történő átültetésének – egyik elemét – szolgáló jogszabály, a Pft.[6] adja.

A kártérítés, ezen belül is a fizetési művelet összegének a megtérítése a pénzforgalom esetében elsősorban két körben fordul elő. Az első a fizetési megbízásokhoz kapcsolódó felelősségnek az az esete, amikor a kedvezményezett valamely adatát a fizető fél elrontotta a fizetési megbízás megadásakor. A Pft. a következőképpen

4 A Polgári Törvénykönyvről szóló 2013. évi V. törvény.

5 A belső piaci pénzforgalmi szolgáltatásokról és a 2002/65/EK, a 2009/110/EK és a 2013/36/EU irányelv és a 1093/2010/EU rendelet módosításáról, valamint a 2007/64/EK irányelv hatályon kívül helyezéséről szóló 2015. november 25-i (EU) 2015/2366 európai parlamenti és tanácsi irányelv.

6 A pénzforgalmi szolgáltatás nyújtásáról szóló 2009. évi LXXXV. törvény.

szabályozza a kérdést: a Pft. 48. § (1) bekezdése szerint, ha a fizetési művelet teljesítése egyedi azonosító használatával történik, a fizetési művelet az egyedi azonosító által megjelölt kedvezményezett vonatkozásában teljesítettnek minősül. A Pft. 48. § (3) bekezdésében foglaltak alapján a fizetési művelet nem teljesítéséért vagy hibás teljesítéséért hibás egyedi azonosító használata esetén a pénzforgalmi szolgáltatót nem terheli felelősség. Mindez tehát azt jelenti, hogy a pénzforgalmi szolgáltatók kizárólag a pénzforgalmi jelzőszámok, IBAN-ok, valamint másodlagos számlaazonosítók mint egyedi azonosítók alapján azonosítják a kedvezményezettet; a kedvezményezett nevét csak hatósági átutalások és átutalási végzések esetén kell ellenőrizniük. Amennyiben tehát a pénzforgalmi szolgáltató az ügyfél által hibásan megadott egyedi azonosító, például pénzforgalmi jelzőszám segítségével adja meg a fizetési megbízást, úgy a pénzforgalmi szolgáltató nem felel a fizetési művelet esetleges hibás teljesítéséért. Ezért lehet az, hogy egy ún. munkahelyi csalás, illetve számlaváltós csalás[7] esetében a pénzforgalmi szolgáltatók felelősségének fennállása nagymértékben kérdéses lehet. Hiszen a fizető fél (ez esetben a vállalkozás) maga adja meg az egyedi azonosítót, amely vonatkozásában a fizetési művelet teljesítettnek minősül.

A legtöbb kártérítéshez kapcsolódó vita ugyanakkor az ún. készpénz-helyettesítő fizetési eszközökhöz kapcsolódik (pl. fizetési kártya, mobilbank vagy netbank minősül ilyen eszköznek), mivel a Pft. szabályai nagymértékben eltérnek a Ptk. felróhatóságon alapuló felelősségi szabályaitól. A kiindulópont a Pft. esetében is a felelősségi mérce kijelölése. Ez a Pft. 40. § (1) és (2) bekezdésében történik meg, amely szerint a pénzforgalmi szolgáltató ügyfele köteles a készpénz-helyettesítő fizetési eszközt a (pénzforgalmi) keretszerződésben foglaltak szerint használni, és a készpénz-helyettesítő fizetési eszköz és annak használatához szükséges személyes biztonsági elemek – így a személyazonosító kód (PIN-kód) vagy egyéb kód – biztonságban tartása érdekében az adott helyzetben általában elvárható magatartást tanúsítani. Az ügyfél a pénzforgalmi szolgáltatónak vagy a pénzforgalmi szolgáltató által megjelölt harmadik félnek haladéktalanul köteles bejelenteni, ha észleli a készpénz-helyettesítő fizetési eszköz birtokából történő kikerülését, ellopását, valamint jogosulatlan vagy jóvá nem hagyott használatát. Mivel a pénzforgalmi keretszerződés tartalmát a jogszabály előírja, így tulajdonképpen a Pft. esetében is az általában elvárható magatartás a mérce. Ha a jóvá nem hagyott fizetési művelet nem készpénz-helyettesítő fizetési eszközzel történik, akkor a pénzforgalmi szolgáltató haladéktalanul megtéríti az ügyfele kárát. Ez a helyzet a gyakorlatban

7 További részletekért ezen visszaélések kapcsán a https://kiberpajzs.hu/csalastipusok/telefonos/munkahelyi-csalas-hamis-ugyfel-beszallito/ és https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/matrix-projekt/kozel-90-millios-utalast-kert-egy honlapok lehetnek irányadók.

akkor fordulhat elő, hogyha a pénzforgalmi szolgáltató informatikai rendszerébe hatolnak be illetéktelenek (Pft. 44. § (1) bekezdés). Amennyiben a kárt készpénz-helyettesítő fizetési eszköznek minősülő olyan személyre szabott eljárással okozták, amely információtechnológiai eszköz vagy távközlési eszköz használatával történt, vagy a készpénz-helyettesítő fizetési eszközt személyes biztonsági elemek nélkül használtak, akkor a kárt teljes mértékben a pénzforgalmi szolgáltató viseli. Ilyen eszköz lehet egy virtuális fizetési kártyás fizetés. Ezen szabály tulajdonképpen internetes fizetések kapcsán elkövetett csalások esetében telepíti a felelősséget a pénzforgalmi szolgáltatókra. Mindezeken túl a Pft. a pénzforgalmi panaszkezelésre alkalmazandó kormányrendelettel[8] együtt megadja a kártérítés megfizetésének legkésőbbi időpontját is. Természetesen lehetséges a felelősség alóli kimentés, azonban az európai jogalkotói szándékkal összhangban, nagymértékben korlátozottan. Ezekkel a szabályokkal a Pft. tulajdonképpen objektívvé teszi a pénzforgalmi szolgáltató felelősségét, hiszen már a kár bekövetkezésének a ténye megalapozza a felelősségét, ráadásul eléggé rigorózus eljárási szabályok szerint teljes kártérítésre köteles, amely felelősség alól a kimentés – fogyasztónak vagy mikrovállalkozásnak minősülő ügyfelek esetében – rendkívül szigorú. Az MNB az ún. Anti-fraud ajánlásában[9] – egyebek mellett – részletesen bemutatja a a Pft. 44. §–45. §-ához tartozó elvárásait, amely elsősorban az ajánlás kiadásakor ismert bírósági gyakorlaton, valamint a PSD2 előírásain alapul. A fentiek okán az ügyfelek által elszenvedett, sikeres adathalász támadások által okozott kárt bizonyos esetekben a pénzforgalmi szolgáltatók viselik.

3.2. Az adathalászat elleni védekezés közjogi eszközei

Közjogi oldalról elsősorban a pénzügyi jogi, illetve a büntetőjogi joganyag releváns az adathalászat szempontjából. Figyelemmel arra, hogy a pénzügyi jog, amely elsősorban a szolgáltatók prudens működésére vonatkozik, nagyon nagy terjedelmű, és számos szintje van, ezért a terjedelmi korlátok miatt jelen cikkben csak a legrelevánsabb pénzügyi jogszabályokat említjük.

8 A befektetési vállalkozások, a pénzforgalmi intézmények, az elektronikuspénz-kibocsátó intézmények, az utalványkibocsátók, a pénzügyi intézmények és a független pénzügyi szolgáltatás közvetítők panaszkezelésének eljárásával, valamint panaszkezelési szabályzatával kapcsolatos részletes szabályokról szóló 435/2016. (XII. 16.) Korm. rendelet.

9 A pénzforgalmi szolgáltatásokon keresztül megfigyelhető visszaélések megelőzéséről, észleléséről, megakadályozásáról és kezeléséről szóló 5/2023. (VI.23.) MNB-ajánlás (https://www.mnb.hu/letoltes/5-2023-penzforgalmi-visszaelesek-ajanlas.pdf).

Természetesen az adathalászat szempontjából kiemelten fontos az adatvédelem kérdése, mindazonáltal ez önmagában is önálló kutatási téma, különösen az adatvédelmi jog extraterritoriális jellege miatt (Molnár, 2021).

3.2.1. A pénzügyi jogban elvárt IT-biztonsági követelmények

A pénzforgalom biztonságát – ideértve azt is, hogy az ügyfeleket lehetőség szerint ne érje kár – a PSD2 (vagyis az irányelvet a hazai jogba átültető jogszabályok, elsősorban a Pft.), illetve a kapcsolódó felhatalmazáson alapuló bizottsági rendeletek szabályozzák. Így például a pénzforgalmi szolgáltatók számára előírt működési és biztonsági kockázatok kezelési (Pft. 55/A. § és 55/B. §), illetve hitelesítési előírások (Pft. 55/C. §). Informatikai biztonsági oldalról fontos megemlíteni a IT-biztonsági kormányrendeletet[10], valamint az MNB két témába vágó ajánlását: az informatikai rendszer védelméről szóló és az ún. Felhő-ajánlást.[11] Jelen cikk írásakor ugyan még nem alkalmazandó, de informatikai biztonsági szempontból kiemelten fontos a DORA-rendelet[12], amely 2025. január 17-től alkalmazandó. Az előbbiekben említett jogszabályok nagy részletességgel szabályozzák – egyebek mellett – azt, hogy a pénzforgalmi szolgáltatóknak milyen módon kell kialakítaniuk az informatikai rendszereiket, azokat (legalább) milyen eszközökkel védjék meg a külső és belső támadások ellen. Természetesen mindez csupán egy minimumszintet jelent, azonban az elmondható, hogy a magyar pénzügyi szektort érintő informatikai szabályozás nagyon jól fejlett, és ehhez kapcsolódóan a magyar pénzügyi szektor a kiberbiztonság szempontjából ellenállónak mondható (MNB, 2022). Ezzel magyarázható az is, hogy a visszaéléseket elkövetők elsősorban az ügyfeleket célozzák, nem pedig a pénzforgalmi szolgáltatókhoz próbálnak betörni.

Fontos kiemelni két olyan jogszabályi változást, amely célzottan a pénzügyi szektornak a visszaélésekkel szembeni hatékony fellépését támogatja. Ezek közül az első a 2024. augusztus 1-től hatályos Pmt.[13] 37/A. §-ban foglalt előírások, amelyek a pénzforgalmi szolgáltatók tájékoztatását írja elő egyfajta „riadólánc" formájában. Vagyis amennyiben az egyik pénzforgalmi szolgáltató ügyfele visszaélés áldozata

10 A pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló 42/2015. (III. 12.) Korm. rendelet.

11 A közösségi és publikus felhőszolgáltatások igénybevételéről szóló 4/2019. (IV.1.) MNB-ajánlás, illetve az informatikai rendszer védelméről szóló 8/2020. (VI.22.) MNB-ajánlás.

12 A pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról 2022. december 14-i (EU) 2022/2554 európai parlamenti és tanácsi rendelet.

13 A pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvény.

lesz, úgy a számlavezető pénzforgalmi szolgáltató – megfelelően biztonságos csatornán – tájékoztatja az illetékes hatóságot, valamint a fizetési művelet teljesítésében érintett többi pénzforgalmi szolgáltatót. A második fontos változás – egyebek mellett – a a Pft. előírásaiba foglalt, ún. központi visszaélésszűrő rendszer működését megalapozó jogszabályi előírás (Pft. 55/D. §). A jogszabálycsomag 2025. július 1-től hatályos, és lehetővé teszi majd, hogy a fizetési rendszert működtető pénzügyi vállalkozás, tehát Magyarországon a GIRO Elszámolásforgalmi Zrt. adatokat kapjon és adjon át a rendszertag pénzforgalmi szolgáltatóktól és az ő részükre azért, hogy a belföldi forintfizetési forgalomban minél hatékonyabban meg lehessen előzni a fizetési műveletekkel kapcsolatos visszaéléseket (GIRO, 2024).

3.2.2. Az adathalászat büntetőjogi megítélése a jelenlegi joggyakorlatban

Ha az adathalászat jogi szempontú vizsgálatára kerül sor, akkor mindenképpen szót kell ejteni az egyik legnagyobb közjogi jogágról, amelynek az alkalmazása sajnálatos módon elkerülhetetlen. Ez a jogág pedig a büntetőjog. Ahogy a legtöbb digitalizációhoz kapcsolódó szabályozás esetében indokolt, az informatikai bűnözés elleni fellépés esetében is többszintű a szabályozás. A legmagasabb szinten a nemzetközi szerződések vannak, amelyek közül a tárgyban a legjelentősebb a 2001. november 23-án kelt, a Számítástechnikai Bűnözésről szóló Egyezmény (Budapesti Egyezmény), amely többek közt segít abban, hogy a csatlakozó országok egységesen ítéljenek meg bizonyos tényállásokat, ideértve az adathalászatot is (Krasznay, 2021). Ezt követik az Európai Unió jogalkotási aktusai, amelyek közül a két legfontosabb az 2013/40/EU irányelv[14], illetve az (EU) 2019/713 irányelv[15]. Végül természetesen Magyarország esetében a legjelentősebb jogforrás a büntetőjogi kódex, a Btk.[16] Mivel a technológia folyamatosan változik és fejlődik, ezért a bűncselekmények elkövetésére használt módszerek és megoldások is módosulnak. Mindezt szabályozási oldalról rendkívül nehéz követni, valamint az elmúlt évtizedekben számos szabályozási esemény is történt. Jelen tanulmánynak nem célja bemutatni a kapcsolódó jogtörténetet, csupán utalunk a téma jelentőségére (Mezei, 2018; 2020).

Az adathalászat mint bűncselekmény büntetőjogi megítélésekor – a hatályos szabályozás alapján – több tényállás vizsgálata szükséges lehet.

14 Az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról szóló 2013. augusztus 12-i 2013/40/EU európai parlamenti és tanácsi irányelv.

15 A készpénz-helyettesítő fizetési eszközzel elkövetett csalás és a készpénz-helyettesítő fizetési eszközök hamisítása elleni küzdelemről, valamint a 2001/413/IB tanácsi kerethatározat felváltásáról szóló 2019. április 17-i (EU) 2019/713 európai parlamenti és tanácsi irányelv.

16 A Büntető Törvénykönyvről szóló 2012. évi C. törvény.

A Btk.-ban az informatikai bűncselekmények a jelentős hasonlóságok és szoros összefüggések okán önálló fejezetet alkotnak. A Btk. 423. §-ban három – részben eltérő tárgyi súlyú – külön fordulattal határozza meg a tisztán informatikai bűncselekménynek minősülő információs rendszer vagy adat megsértésének elkövetési magatartásait. Ezen fordulatok elkövetési tárgya az információs rendszer. A Btk. 423. § (1) bekezdésének értelmében büntetendő, aki az információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad; vétség miatt két évig terjedő szabadságvesztéssel büntetendő. A bűncselekmény alanya az első fordulatban a belépésre jogosultsággal nem rendelkező személy lehet, míg a második fordulat esetén az adott személy rendelkezik erre vonatkozó engedéllyel, amelyet nem rendeltetésszerűen használ, például jogosultságkiterjesztés (privilege escalation) révén. Az ezen elkövetési magatartásokat tanúsító elkövetőket gyakran nevezi a köznyelv hackereknek. Fontos kiemelni, hogy az információs rendszerbe történő jogosulatlan belépés irányulhat az elkövető által felhasznált számítógépre vagy a rajta keresztül elérhető, védett számítógépes hálózatra, így például egy pénzforgalmi szolgáltató ügyfele által használt online szolgáltatásokra. Ahhoz, hogy a bűncselekményt meg lehessen állapítani, szükséges, hogy az információs rendszer technikai intézkedéssel biztosított védelemmel legyen ellátva, és ez a védelem aktív legyen. Mindez tehát azt jelenti, hogy ha a rendszert pl. egy tűzfal vagy biometrikus hitelesítés ugyan védi, de az nincs aktiválva, akkor a bűncselekményt nem lehet megállapítani (Belovics, 2023). A Btk. 423. § (1) bekezdés kapcsán az elkövetési módot is meghatározták, ezért a bűncselekmény megvalósul akkor, ha a belépés a védelmi intézkedés megsértésével vagy ennek kijátszásával történik, például a biztonsági rendszer hiányosságait kihasználva lépnek be jogosulatlanul, vagy a jogosult jelszavával vagy belépési kódjával, amelynek megszerzési módja azonban közömbös. Ezen megszerzési módra lehet példa az adathalászat. A bűncselekmény elkövetésének továbbá nem feltétele, hogy károkozás, haszonszerzés vagy egyéb hasonló célzat történjen (nem célzatos bűncselekmény), így az ideológiai vagy politikai okból elkövetett támadások is büntethetőek.

A Btk. 423. § (2) bekezdése szerint aki az informatikai rendszer működését zavarja meg jogosulatlanul vagy a jogosultsága kereteit túllépve, az büntetendő. Figyelemmel arra, hogy ezen fordulatok elsősorban az informatikai rendszer rendeltetésszerű használatát hivatottak megvédeni (pl. zsarolóvírusok vagy túlterheléses támadások ellen), ezért az adathalászat kapcsán nem releváns a vizsgálatuk. Fontos kiemelni továbbá, hogy a Btk. XLIII. fejezete egy további deliktumot is tartalmaz. A Btk. 424. § (1) bekezdése a) és b) pontjai szerint, aki – többek között a 375. §-ban vagy a 423. §-ban meghatározott bűncselekmény elkövetése céljából – az ehhez szükséges vagy ezt könnyítő jelszót vagy számítástechnikai programot ké-

szít, átad, hozzáférhetővé tesz, megszerez vagy forgalomba hoz, illetve jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja, vétség miatt két évig terjedő szabadságvesztéssel büntetendő. Mindez tehát azt jelenti, hogy a különböző rosszindulatú programkódok elkészítése és terjesztése önmagában is bűncselekmények minősül (Mezei, 2019).

A Btk. kodifikáláskor új tényállásként határozták meg az információs rendszer felhasználásával elkövetett csalást (Btk. 375. §). A Btk. javaslatához fűzött miniszteri indoklás szerint az információs rendszer felhasználásával elkövetett, kárt okozó csalások elsősorban vagyoni érdekeket sértő cselekmények, illetve ezek a csalásszerű magatartások azért kerültek a csalástól eltérő, önálló tényállásba, mert hiányzik belőlük a klasszikus értelemben vett tévedésbe ejtés vagy tévedésben tartás. Ezek alapján a Btk. 375. § (1) bekezdése úgy rendelkezik, hogy 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 (Ambrus, 2021). Mindezeken túl a pénzügyi visszaélések esetén kiemelten fontos az ún. készpénz-helyettesítő fizetési eszközökhöz kapcsolódó deliktum pönalizálása. A Btk. 375. § (5) bekezdése szerint büntetendő, aki hamis, hamisított vagy jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz felhasználásával vagy az ilyen eszközzel történő fizetés elfogadásával okoz kárt. A dogmatikai és jogalkalmazási részletekbe nem elmerülve, jelen cikk nem vizsgálja a kár fogalmát, mivel a napi pénzügyi gyakorlatban a számlavezetett ügyfelek fizetési és egyéb (pl. betéti vagy értékpapírszámláin) történő egyenlegek teljes eltulajdonításáról lehet szó, illetve újabban akár kölcsönfelvételről is (Herman, 2024). A Btk. 459. § (1) bekezdés 19. pontja határozza meg a készpénz-helyettesítő fizetési eszköz fogalmát, amely szerint készpénz-helyettesítő fizetési eszköznek minősül a Hpt.-ben[17] meghatározott készpénz-helyettesítő fizetési eszköz és a forgatható utalvány, a kincstári kártya, az utazási csekk, a kifizetőt terhelő adó mellett vagy adómentesen adható, korlátozott körű áruk vagy szolgáltatások ellenértékének kiegyenlítése céljából törvény alapján kibocsátott utalvány és a váltó, feltéve, hogy kivitelezése, kódolása vagy a rajta lévő aláírás folytán a másolás, a meghamisítás vagy a jogosulatlan felhasználás ellen védett. Vagyis a Hpt. előírásai alapján az ügyfelek által a leggyakrabban használt készpénz-helyettesítő fizetési eszközök (Hpt. 6. § (1) bekezdés 55. pont a) és c) alpont), amelyeket a pénzügyi közvetítőtőrendszer felügyeletét ellátó Magyar Nemzeti Bank a Hpt. alapján ilyennek tekint: a mobil-

17 A hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény.

banki, internetbanki alkalmazások, a fizetési kártyák, valamint az elektronikus pénz (Bárdits, 2021).

A fentiek alapján tehát a gyakorlati jogalkalmazás során az egyes bűncselekmények elhatárolása kapcsán merülhetnek fel kérdések, ugyanakkor az kijelenthető, hogy általánosságban az informatikai rendszerek ellen vagy azok útján elkövetett cselekmények büntetendők, ezért tilosak. Ideértve az egyik leggyakoribb elkövetési módot, az adathalászatot is, függetlenül attól, hogy történt-e tényleges károkozás, avagy a készpénz-helyettesítő fizetési eszközzel (pl. mobilbanki alkalmazással vagy fizetési kártyával megadott fizetési megbízás jogtalan teljesítése), esetleg személyes adattal visszaélés (Btk. 219. §). Tehát kijelenthetjük, hogy büntetőjogi szempontból rendelkezésre állnak azon eszközök, amelyek büntethetővé teszik az adathalászatot.

4. BŰNÜGYI MEGKÖZELÍTÉS AZ ADATHALÁSZAT ELLENI FELLÉPÉSBEN

Az adathalászattal szembeni fellépés szempontjából kiemeletlen fontos a bűnmegelőzés, amely elsősorban figyelemfelhívás, biztonságtudatossági kampányok révén valósul meg (Gyaraki, 2022). A rendőrség bűnmegelőzési szakterületei mellett az ilyen kommunikációban jelentős szerepet vállalnak a pénzügyi tudatossággal foglalkozó szakemberek, vállalkozások és egyéb szervezetek is (Terták–Kovács, 2023; Kovács–Terták, 2024). A hagyományos (pl. személyes, írott formában, nyomtatott sajtóban, televízióban megjelenő) figyelemfelhívás mellett az adathalászattal szembeni fellépés során különösen fontos az online megjelenés, a közösségimédia-posztok és reklámok, a rövid videók vagy hosszabb podcastok, az influenszerek, illetve véleményvezérek felhasználása az üzenet célba juttatásához, mivel az adathalászat potenciális áldozatai éppen az online pénzügyi tevékenységük miatt kerülnek célkeresztbe. A komplex, széles körű összefogás révén létrejött biztonságtudatossági kampányra jó példa a magyar KiberPajzs program (NKI, 2023).

A már bekövetkezett, sikeres adathalászatok és a hozzájuk kapcsolódó bűncselekmények felderítése és az esetleges vagyonvisszaszerzés azért is nehéz feladat, mert maguk a cselekmények teljesen más sebességgel történnek, mint a nyomozás. Adott esetben a sértett néhány kattintással átadja a rendelkezést a számítógépe, mobiltelefonja, fizetési számlája felett, a pénze pedig pár másodperc alatt eltűnik a hatékony, modern fizetési rendszereknek köszönhetően. Az elkövetők ráadásul gyakran péntek esti vagy ünnepnapra eső időpontot választanak a fizetési, megtakarítási vagy értékpapírszámlák megterhelésére, hogy ezzel is megnehezítsék a kapcsolatfelvételt a pénzforgalmi szolgáltatóval és a hatóságokkal. Mivel ezek a

bűncselekmények az online térben történnek, ha sikerül is azonosítani az elkövetőket, a nyomozás folyamata gyakran nehézkes, mivel nemzetközi együttműködésre van szükség. A bűnözők is gyakran határon átnyúló bűnszervezetekben dolgoznak, az adathalászathoz és a csalások elkövetéséhez kész, szolgáltatásként igénybe vehető infrastruktúrákat használhatnak, a telefonos csalásokhoz pedig a valódi (pénzforgalmi szolgáltatói) telefonos ügyfélszolgálatokhoz hasonló call centereket üzemeltetnek.

A 2024-es év szerencsére a bűnüldözés szempontjából bővelkedik a sikertörténetekben, az Europol 19 ország nyomozóhatóságainak együttműködésével számolt fel egy adathalász szolgáltatásokat (phishing-as-a-service) nyújtó platformot és az azt üzemeltető bűnszervezetet (Europol, 2024b), a magyar hatóságok pedig az ukrán rendőrséggel együttműködve egy magyar nyelvterületre szakosodott, call centert is üzemeltető bűnözői csoportra csaptak le (police.hu, 2024). Jellemzőbb azonban, hogy a jól szervezett bűnszövetkezetekben csak az alacsonyabb szintű strómanokat, azokat a „kishalakat" kapják el, akiket az ellopott pénzeket fogadó fizetési számlák megnyitásával vagy a pénz felvételével bíznak meg a bűnözők.

Érdemes szót ejteni a vagyonvisszaszerzésről, azaz az ellopott pénz jogos tulajdonosához való visszajuttatásáról is. A gyakorlatban akkor van esély a pénz visszaszerzésére, ha minden szereplő – az ügyfél, illetve sértett, a pénzforgalmi szolgáltató és a hatóságok, pl. a rendőrség is – haladéktalanul cselekszik. Ha a számlavezetett ügyfél által jóvá nem hagyott fizetési művelet vagy bármilyen, nem az ügyfél által kezdeményezett módosítás megtörténte után az ügyfél a kapott tájékoztatás (pl. SMS vagy pushüzenet) kézhezvétele után haladéktalanul jelzi számlavezető pénzforgalmi szolgáltatójának, hogy nem ő kezdeményezte a tranzakciót (pl. fizetési műveletet, betétfeltörést vagy értesítésicsatorna-változást), a fizetési művelet lebonyolításában érintett pénzforgalmi szolgáltatók és a rendőrség pedig szorosan, késedelem nélkül, 0–24 órában együttműködik a pénz feltartóztatásában, akkor előfordulhat, hogy sikerül megállítani a pénzt, és idővel visszakerülhet a jogos tulajdonosához (lásd a 3.2.1. pontban említett „forródrótot").

5. INFORMATIKAI BIZTONSÁGI ESZKÖZÖK AZ ADATHALÁSZAT MEGELŐZÉSÉBEN ÉS FELISMERÉSÉBEN

Az adathalászat informatikai biztonsági szempontú kezelésének lehetőségei sokrétűek, a biztonságtudatossági képzésektől és kampányoktól kezdve a technikai megoldásokig terjednek. A már említett rendőrségi bűnmegelőzési programok és a KiberPajzs kezdeményezés mellett általában a cégek belső IT-biztonsági oktatásai is kitérnek az adathalász támadások felismerésére, megelőzésére és az észlelt esetek megfelelő helyre (a cég biztonsági csapatához) történő bejelentésére, sőt

adott esetben szimulált adathalász kampányokkal is tesztelik a dolgozók biztonságtudatosságát. Ezek mellett számos ismeretterjesztő anyag elérhető az interneten, például a teljesség igénye nélkül a következők: a Nemzetközi Gyermekmentő Szolgálat (NGYSZ) által fenntartott saferinternet.hu oldalon vagy a Nemzeti Média- és Hírközlési Hatóság (NMHH) által üzemeltetett digipedia.hu-n.

Az adathalász e-mailek kiszűrését nagyban segítheti a megfelelően beállított spamszűrő és antivírus szoftver használata. A spamszűrő – amely a nagy, sok esetben felhőalapú levelezési szolgáltatóknál és gyakran a levelezést biztosító internetszolgáltatóknál is alapból elérhető – gyakran kéretlen levélként azonosítja az adathalász üzeneteket is, amivel azok technikai sajátosságai (rejtett vagy módosított feladó, tömeges címzettek, gyanús feladó stb.) hasonlítanak a kéretlen reklámokra. A vírusirtó szoftverek többsége képes megjelölni a levelezésben vagy a böngészőben a gyanús linkeket, így felhívja a felhasználók figyelmét arra, hogy ne kattintsanak az adathalász oldalakra. Emellett a vírusirtók az adathalászat során esetlegesen használt kártékony szoftverek futását is képesek megakadályozni. Céges környezetben az internetes tartalomszűrő is jelent bizonyos fokú védelmet, a lakossági ügyfelek számára pedig egyes internetszolgáltatók nyújtanak hasonló szűrési szolgáltatásokat.

Az elektronikus levelezéssel kapcsolatban jó gyakorlat, ha a kiküldött leveleket elektronikus aláírással vagy bélyegzővel látják el, ami lehetővé teszi a feladó szerver hitelesítését, így a fogadó meg tud győződni a feladó szervezet azonosságáról és arról, hogy nem adathalászattal van dolga. A tartományalapú üzenethitelesítés, jelentéskészítés és megfelelőség (Domain-based Message Authentication, Reporting & Conformance – DMARC) használata is segít abban, hogy meggyőződjünk a levél feladójának valódiságáról (MNB, 2022). Ezen túl az e-mailek fejléce még számos olyan információt tartalmaz, amely a levél technikai vizsgálata és statisztikai elemzése során segít annak eldöntésében, hogy legitim, jól karbantartott környezetből érkezik-e az üzenet (Kumar Birthriya–Jain, 2022). Az Amerikai Egyesült Államokban a Kiberbiztonsági és Infrastruktúra Biztonsági Ügynökség[18], a Nemzeti Biztonsági Ügynökség[19], a Szövetségi Nyomozó Iroda[20] és az Államközi Információmegosztó és Elemző Központ[21] közös ajánlást adott ki az adathalászat elleni védekezés támogatására, amelyben a biztonságtudatossági oktatás mellett kiemelik a többfaktoros hitelesítés használatának fontosságát (így a sikeres adathalá-

18 Cybersecurity and Infrastructure Security Agency – CISA.

19 National Security Agency – NSA.

20 Federal Bureau of Investigation – FBI.

21 Multi-State Information Sharing and Analysis Center – MS-ISAC.

szathoz nem elég egy felhasználónév-jelszó párost megszereznie a támadónak), és további technikai védelmi intézkedéseket is javasolnak (CISA, 2023).

Az SMS-ben kapott adathalász üzenetek és a telefonhívások esetében a korszerű mobiltelefonokon beállítható a kéretlen hívások és spam elleni védelem, amelynek a segítségével a telefon megjelöli a gyanúsnak tartott üzeneteket és hívásokat. Magyarországon jelenleg még nem adott a jogi környezet ahhoz, hogy ugyanezt a távközlési szolgáltató tegye meg, vagy szűrést végezzen, de például az Egyesült Királyság távközlési felügyelete[22] ajánlásokat fogalmazott meg a témában, és külön programot indítva vizsgálja a távközlési szolgáltatók gyakorlatát (Ofcom, 2024), Lengyelországban pedig 2023-ban törvény született az elektronikus kommunikációs csatornákkal való visszaélés elleni küzdelemről[23].

A beérkezett e-mailes vagy SMS-es adathalász üzenetek tartalmával kapcsolatban is tehetünk lépéseket: a üzeneteket megjelölhetjük a telefonunkon vagy a levelezőrendszerünkben spamként, tilthatjuk a hívószámot (amit a vishing hívások esetében is megtehetünk), illetve bejelenthetjük az adathalászatot a két magyar internet forródrót (NMHH, NGYSZ) valamelyikén, vagy a rendőrségen. A céges címre érkező adathalász leveleket az adott belső eljárásrend szerint kell kezelni, jellemzően a cég informatikai biztonsági felelősének vagy kiberbiztonsági csapatának kell jelezni. Amennyiben az adathalász üzenet hamis weboldalra – például lemásolt pénzforgalmi szolgáltatói oldalra – mutató hivatkozást tartalmaz, megfelelő informatikai ismeretek birtokában jó gyakorlat felvenni a kapcsolatot a weboldal tárhely- vagy domainszolgáltatójával, hogy távolítsa el a tartalmat, mivel ezek az oldalak nagyon gyakran legitim szolgáltatásokat tartalmazó, feltört weboldalak mellett találhatók, ahol a tényleges tulajdonos, illetve üzemeltető nincs is tudatában annak, hogy mire használják a szerverét. A gyanús üzeneteket, internetcímeket, domaineket vagy csatolmányokat ellenőrizhetjük ingyenes megoldásokkal is, például a virustotal.com oldalon, amely több mint 70 antivírus szoftver segítségével ellenőrzi a feltöltött tartalmakat.

A fentiek alapján elmondható, hogy az informatikai biztonság területén a tudatosítás és oktatás mellett számos technológiai eszköz áll a cégek, informatikai és távközlési szolgáltatók rendelkezésére, hogy megakadályozzák felhasználóik, ügyfeleik adathalászat áldozatává válását.

22 Office of Communications – Ofcom.

23 Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej.

6. AZ ADATHALÁSZAT ÁLTAL OKOZOTT KÁROK MEGELŐZÉSE ÉS CSÖKKENTÉSE

Ha megtörtént a baj, a felhasználó megadta az adatait, vagy telepített egy alkalmazást, akkor azonnal fel kell vennie a kapcsolatot a pénzforgalmi szolgáltatójával, meggyőződni arról, hogy történt-e jóvá nem hagyott fizetési művelet, és megtenni a szükséges intézkedéseket a nem kívánt fizetési művelet megelőzésére. Ez az internetbanki és mobilbanki hozzáférések esetében a hozzáférések felfüggesztését, majd az azonosítók és jelszavak cseréjét jelenti, fizetési kártyáknál pedig a kártya tiltását és cseréjét. Fontos, hogy az azonnali felfüggesztés után csak akkor szabad aktiválni az új hozzáféréseket, ha a felhasználó ügyfél meggyőződött arról, hogy a mobiltelefonja vagy számítógépe már nem hozzáférhető illetéktelenek számára. Ha az ügyfélnek több pénzforgalmi szolgáltatónál van számlája, amely érintett lehet (például a számítógépére telepített távoli hozzáférést lehetővé tevő alkalmazás révén), akkor az összes számla esetén meg kell tenni az óvintézkedéseket. Ugyanígy, ha több ügyfél számlája felett rendelkezik a felhasználó, vagy több családtag használja ugyanazt a számítógépet, akkor is az összes potenciálisan érintett számla hozzáférését korlátozni kell.[24] Az ügyfelek részére a teendők közérthető leírását a – már hivatkozott – KiberPajzs oldal tartalmazza.

A pénzforgalmi szolgáltatók feladataira vonatkozó részletes ajánlásokat a 3.1. pontban már említett MNB Anti-fraud ajánlása tartalmazza, amely feladatok részletezésére jelen tanulmányban nem vállalkozunk. A fentiekből látható, hogy még egy sikeres adathalász támadás esetén is van esély a károk mérséklésére, az ehhez szükséges lépések pedig ismertek a folyamat szereplői (pl. pénzforgalmi szolgáltatók, nyomozó hatóságok) számára, amelyek igyekeznek az ezzel kapcsolatos tájékoztatást megadni a potenciális visszaéléssel érintett ügyfelek számára. Ugyanakkor azt is kijelenthetjük, hogy az adathalászat következményei elleni védekezésnek ez a módja kevésbé hatásos, mint a megelőzés.

7. ÖSSZEGZÉS

A digitális térben elkövetett visszaélések egyre nagyobb kárt okoznak a gazdaságban, amely kár a pénzügyi közvetítőrendszeren keresztül manifesztálódik. Ezen visszaélések közül kiemelkedik az adathalászat, amely támadási forma az összes visszaélés, illetve ezek kísérletének a döntő többségét (Magyarország esetében mintegy 70 százalékát) adja. Adathalászat során a támadók tömeges üze-

24 Az elektronikus csatornán keresztüli, meghatalmazotti hozzáférésekhez kapcsolódó visszaélések megelőzéséről és a kapcsolódó tájékoztatási elvárásokról szóló MNB vezetői körlevél.

netküldéssel (például e-mail- vagy SMS-üzenetek útján) vagy telefonhívással, pszichológiai manipuláció útján próbálnak személyes adatokat, valamint pénzügyi szolgáltatókhoz tartozó hitelesítési adatokat megszerezni, amelyeket később anyagi haszonszerzésre vagy további támadásokra használnak fel. Az adathalász támadások lebonyolítására számos módszer áll a bűnözők rendelkezésére, de manapság az sem ritka, hogy mindezt „szolgáltatásként" (ún. phishing-as-a-service) vásárolja meg a visszaélést elkövető (McNee, 2024). Az elkövetési módok sokrétűsége miatt az adathalászat elleni védekezésnek minél általánosabbnak kell lennie, hogy ne csak egyes módszerek ellen nyújtson védelmet.

Az adathalászat jogi megítélése rendkívül bonyolult, mivel számos jogág érintett a kérdésben. Magánjogi szempontból az adathalászat elsősorban a kártérítési felelősség kérdéseihez kapcsolódik, különösen a pénzforgalmi szolgáltatások esetén, de egyéb szolgáltatások is relevánsak lehetnek (pl. hitel- és pénzkölcsönnyújtás). A pénzforgalmi szolgáltatások esetében a pénzforgalmi szolgáltatók felelőssége rendkívül szigorú. A vonatkozó EU-s és magyar szabályozás, valamint a bírósági gyakorlat alapján a pénzforgalmi szolgáltatókat egyfajta objektivizált felelősség terheli az ügyfél által jóvá nem hagyott fizetési műveletek teljesítése kapcsán. Fogyasztónak és mikrovállalkozásnak minősülő ügyfelek esetében pedig ez alól az objektivizált felelősség alól csak akkor mentesülhetnek, ha maguk bizonyítják az ügyfél súlyosan gondatlan magatartását. Ugyanakkor fogyasztónak vagy mikrovállalkozásnak nem minősülő ügyfelek esetében a pénzforgalmi szolgáltató és az ügyfele eltérhet a Pft.-ben megfogalmazott bizonyításra vonatkozó előírásoktól. A magánjoghoz hasonlóan a közjogi szabályozás is szigorú előírásokat tartalmaz az informatikai rendszerek védelmére és az ezekhez kapcsolódó visszaélésekre vonatkozóan. A pénzügyi jogot vizsgálva, számos prudenciális és informatikai biztonsági előírásnak kell megfelelnie a pénzforgalmi szolgáltatóknak, amelyeknek az a célja, hogy a pénzforgalom zavartalanul lebonyolódhasson, valamint a pénzügyi közvetítőrendszerbe vetett bizalom ne rendülhessen meg. Ami a gyakorlatban azt is jelenti, hogy ezek a szabályozók alkalmasak az adathalászat megelőzésére.

Az adathalászat büntetőjogi megítélése során számos bűncselekmény releváns lehet, például az információs rendszerekhez való jogosulatlan hozzáférés és azok működésének befolyásolása, de készpénz-helyettesítő fizetési eszközökkel (például mobilbanki vagy internetbanki alkalmazásokkal, illetve fizetési kártyával) történő visszaélésekhez kapcsolódó tényállások is felmerülhetnek. Kijelenthetjük tehát, hogy a büntetőjog eszközei megfelelőek az adathalászat elleni küzdelemhez. Jelen cikkünk az adathalászat vonatkozásában egyik legfontosabb jogterülettel, az adatvédelmi joggal csak érintőlegesen foglalkozott. Ugyanakkor a jogterületnek és a kapcsolódó gyakorlatnak részletes irodalma van.

Az adathalászat elleni fellépésben a bűnmegelőzés fontos szerepet játszik, amely figyelemfelhívó kampányok és a pénzügyi tudatosság előmozdítása révén történik. Az elkövetett bűncselekmények felderítése kihívást jelent, mivel az elkövetők gyakran gyorsan és határokon átívelve működnek, ami megnehezíti a nyomozást és a nemzetközi együttműködést. A pénzügyi közvetítőrendszer szereplőinek, például a pénzforgalmi szolgáltatóknak vagy a Magyar Bankszövetségnek mint érdekképviseleti szervnek, illetve állami intézményeknek és szerveknek (például a Magyar Nemzeti Bank vagy az illetékes minisztérium, továbbá egyéb hatóságok) szerepe kiemelkedő az edukáció kérdése kapcsán. Számos kiberbiztonságot, illetve pénzügyi tudatosságot növelő kezdeményezés indult el az elmúlt években. Ilyen például a PÉNZ7[25] vagy a KiberPajzs kezdeményezés. Ezek sikerét nehéz pontosan leméri, ugyanakkor a pénzforgalomban tapasztalható visszaélések értéke alapján feltételezhető, hogy a kampányoknak van pozitív, megelőző hatása.

Az adathalászat megelőzésében az IT-biztonsági oktatás és a technikai megoldások kulcsfontosságúak, és bizonyítottan hatásosak. A megfelelő spamszűrők, antivírus szoftverek és a többfaktoros hitelesítés alkalmazása segít csökkenteni a kockázatot. Az adathalász üzenetek felismerése és a megfelelő bejelentés is segíthet az ilyen támadások elleni védekezésben, míg az olyan eszközök, mint a szerverek közötti üzenetek elektronikus aláírása biztosítják az üzenetek hitelességét. Fontos kiemelni: ha egy pénzforgalmi szolgáltató ügyfele adathalászat áldozata lett, akkor azonnal fel kell vennie a kapcsolatot a pénzforgalmi szolgáltatójával, ellenőriznie kell a jóvá nem hagyott fizetési műveleteket, ezzel – lehetőség szerint – elejét venni a további jogosulatlan fizetéseknek. Internetbanki és mobilbanki hozzáférések esetén a hozzáférések felfüggesztése, az azonosítók és jelszavak cseréje, míg a kártyák esetén a kártyák tiltása és cseréje is szükséges lehet. Fontos, hogy az új hozzáférések aktiválása előtt biztosítani kell a mobiltelefon vagy számítógép biztonságát.

Mindezek okán tehát elmondható, hogy az adathalászat egy rendkívül összetett probléma, amelynek a vizsgálata több szinten lehetséges. Érdemes megvizsgálni és megérteni az elkövetési módokat és a kapcsolódó technikákat a hatékony védekezéshez. Fontos megvizsgálni a terület jogi szabályozását, különös tekintettel az IT-biztonsági előírásokra, amelyeket a DORA-rendelet következtében az egész Európai Unió szintjén harmonizálják 2025 januárjától. Mindazonáltal megállapítható, hogy az adathalászat elleni védekezés számos szinten és eszközzel lehetséges. A jogi, bűnmegelőzési, bűnüldözési, biztonságtudatossági, IT-biztonsági és eljárásrendi eszközök együttes alkalmazása a leghatékonyabb, ugyanakkor to-

25 Lásd a https://www.penz7.hu/ oldalt.

vábbra is a megelőzés – mind a (pénzügyi) szolgáltatásokat igénybe vevő ügyfelek, mind pedig a (pénzforgalmi) szolgáltatók oldalán – a legbiztosabb védelem.

HIVATKOZÁSOK

Ambrus, I. (2021): Mezei Kitti: A kiberbűnözés aktuális kihívásai a büntetőjogban (2020, Budapest: TK JTI–L'Harmattan, p. 284.) *Állam- és Jogtudomány*, 62(4), 128–133. https://doi.org/10.51783/ajt.2021.4.06.

Anderson, R. – Barton, C. – Böhme, R. – Clayton, R. – Gañán, C. – Grasso, T. – Levi, M. – Moore, T. – Vasek, M. (2019) Measuring the Changing Cost of Cybercrime. https://www.repository.cam.ac.uk/items/a9e1b7b4-03c6-43b5-ae0c-b5b59e0d4684.

Bárdits, Z. (2021, február 27): Bankkártya, üzemanyagkártya, Revolut, Bitcoin – Mi számít elektronikus pénznek? *portfolio.hu*. https://www.portfolio.hu/bank/20210227/bankkartya-uzemenyagkartya-revolut-bitcoin-mi-szamit-elektronikus-penznek-471486.

Belovics, E. (2023): *Büntetőjog II.* (különös rész). 9., hatályosított kiadás (2023. szeptember). Budapest: ORAC Kiadó.

CIB Bank (2024): Telefonon próbálkoznak a leggyakrabban a kibercsalók. CIB Bank Zrt. https://www.cib.hu/Maganszemelyek/rolunk/sajtoszoba/sajtokozlemenyek/240509-kibercsalas.html (letöltve: 2024.06.16).

CISA (2023): Phishing Guidance: Stopping the Attack Cycle at Phase One. https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one (letöltve: 2024.06.16).

Europol (2023): IOCTA, internet organised crime threat assessment 2023. European Union Agency for Law Enforcement Cooperation. LU: Publications Office. https://data.europa.eu/doi/10.2813/587536.

Europol (2024a): *Facing reality? Law enforcement and the challenge of deepfakes: an observatory report from the Europol innovation lab.* LU: Publications Office. https://data.europa.eu/doi/10.2813/158794

Europol (2024b): International investigation disrupts phishing-as-a-service platform LabHost. https://www.europol.europa.eu/media-press/newsroom/news/international-investigation-disrupts-phishing-service-platform-labhost.

Europol (2024c): Internet Organised Crime Threat Assessment (IOC-TA) 2024. European Union Agency for Law Enforcement Cooperation. LU: Publications Office. https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024.

GIRO (2024): Összefogással a biztonságos banki tranzakciókért. https://www.giro.hu/news/biztonsagos-banki-tranzakciok.

Gyaraki, R. (2022): A biztonságtudatosság szerepe, avagy kérdések a kiberbiztonságról. *Magyar Rendészet* 22(2): 245–261. https://doi.org/10.32577/mr.2022.2.16.

György V. (2021): A csomagküldős vírus itthon is tarolt. https://index.hu/belfold/2021/03/30/csalas_sms_kibervedelem (letöltve: 2024.07.24.).

Herman, B. (2024, július 18): Újabb fontos intézkedést vezetnek be az online banki csalások ellen. *bank360.hu*. https://bank360.hu/blog/ujabb-fontos-intezkedest-vezetnek-be-az-online-banki-csalasok-ellen.

Kovács, L. (2010): *Az európai pénz- és elszámolásforgalom jövő*je. Miskolc: ME GTK.

Kovács, L. – Terták, E. (2024): A kiberbűnözés legjobb ellenszere a pénzügyi műveltség. *Gazdaság és Pénzügy* 11(1), 6–29. https://doi.org/10.33926/GP.2024.1.2.

Krasznay, C. (2021): Húsz év a globális kiberbűnözés elleni küzdelemben. A Budapesti Egyezmény értékelése. *Külügyi Szemle,* 20 (különszám), 191–214. https://doi.org/10.47707/Kulugyi_Szemle.2021.2.09.

Krasznay, C. (szerk.). (2023): *Taktikák és stratégiák a kiberhadviselésben.* Budapest: Ludovika Egyetemi Kiadó.

Kumar Birthriya, S. – Jain, A. K. (2022): A Comprehensive Survey of Phishing Email Detection and Protection Techniques. *Information Security Journal: A Global Perspective*, 31(4), 411–440. https://doi.org/10.1080/19393555.2021.1959678.

Lábady, T. (2014): *A magánjog általános tana.* 2. kiadás. Budapest: Szent István Társulat.

Magramo, H. C., Kathleen (2024): Finance worker pays out $25 million after video call with deepfake 'chief financial officer'. CNN, https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html (letöltve: 2024.10.17.).

McNee, S. M. (2024): How Cybercrime Empires Are Built. darkrea-ding.com. https://www.darkreading.com/vulnerabilities-threats/how-cybercrime-empires-are-built (letöltve: 2024.06.16.).

Mezei, K. (2018): Az informatikai bűnözés elleni nemzetközi fellépés – különös tekintettel az Európai Unió és az Egyesült Államok szabályozására. *JURA*, 24(1), 349–360.

Mezei, K. (2019): A kiberbűnözés szabályozási kihívásai a büntetőjogban. *Ügyészek Lapja*, 26(4-5), 21–33.

Mezei K. (2020): A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre. *Állam- és Jogtudomány*, LXI(4), 65–81.

mitre.org (2024): MITRE ATT&CK®. https://attack.mitre.org/ (letöltve: 2024.07.24).

MNB (2022): A magyar pénzügyi szektor kiberfenyegettségi térképe 2022. Magyar Nemzeti Bank. https://www.mnb.hu/letoltes/kiberfenyegetettsegi-terkep-2022.pdf.

MNB (2024a): Fizetési Rendszer Jelentés 2024. Magyar Nemzeti Bank. https://www.mnb.hu/letoltes/fizete-si-rendszer-jelente-s-2024-hun-digitalis-vegleges.pdf.

MNB (2024b): Pénzforgalmi visszaélések. https://statisztika.mnb.hu/idosor-3644.

Molnár, P. (2021): Comparison of the new Chinese Personal Data Protection Law (PIPL) with GDPR and CCPA. KRE-DIt (2021.02): https://www.kre-dit.hu/tanulmanyok/peter-molnar-comparison-of-the-new-chinese-personal-data-protection-law-pipl-with-gdpr-and-ccpa/ (letöltve: 2024.07.14.).

NKI (2023): Mi ellen véd a KiberPajzs? (tudatosan). Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet. https://kibertamadas.simplecast.com/episodes/mi-ellen-ved-a-kiberpajzs

Ofcom (2024): Enforcement programme into phone and text scams. https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/enforcement-programme-phone-and-text-scams/ (letöltve: 2024.07.26.).

Oroszi, E. D. (2020): Social Engineering a koronavírus tükrében, avagy a rendkívüli helyzetet kihasználó támadási technikák és megelőzésük. *Dunakavics*, VIII(V), 5–20.

police.hu (2024): Közel 90 milliós utalást kért egy álpartnercég. https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/matrix-projekt/kozel-90-millios-utalast-kert-egy.

Szabó, H. (2023): A mesterséges intelligencia biztonsági kockázatai egy új korszak kezdetén. *Nemzetbiztonsági Szemle*, 11(4), 35–46. https://doi.org/10.32561/nsz.2023.4.3.

Szalai, Á. (2024): A deliktuális felelősség joggazdaságtana. Budapest: ORAC Kiadó. https://doi.org/10.21862/ELTEJKT69.

Terták, E. – Kovács, L. (2023): Fókuszban a pénzügyi biztonság kibertérben is – PÉNZ7. *Gazdaság és Pénzügy*, 10(1), 5–20. https://doi.org/10.33926/GP.2023.1.1,

VISA (2023): Visa Payment Fraud Disruption Biannual Threats Report, December 2023. https://usa.visa.com/content/dam/VCOM/regional/na/us/run-your-business/documents/pfd-biannual-threats-report-december-2023.pdf.

World Economic Forum (2024): Global Cybersecurity Outlook 2024. https://www.weforum.org/publications/global-cybersecurity-outlook-2024.