GAZDASÁG ÉS PÉNZÜGY • 12. ÉVF. 3. SZ. • 2025. SZEPT. • DOI: 10.33926/GP.2025.3.4

A PÉNZÜGYI KIBERBŰNÖZÉS RENDSZERTANA

Kiss Milán – Kovács Levente[1]

ABSZTRAKT

A kibertámadásokkal szembeni hatékony védekezés egyik kulcseleme egy olyan strukturált osztályozási rendszer, amely nemcsak a jogalkotókat, a szabályozó hatóságokat és a pénzügyi szervezeteket, hanem az ügyfeleket is segíti a fenyegetések felismerésében és kezelésében, valamint a pénzügyi szektorral ismerkedő hallgatók képzését is támogathatja. A tanulmány a pénzügyi szektort érintő kibertérben elkövetett visszaélések rendszertani megközelítését végzi el, különös figyelmet fordítva a visszaélések csoportosítási lehetőségeire és a védekezési mechanizmusokra. A digitális pénzügyi ökoszisztéma fejlődésével párhuzamosan a kiberfenyegetések száma és összetettsége is dinamikusan növekszik. A tanulmány különböző szempontok alapján rendszerezi a kiberbűncselekményeket, így a támadás módszere (pl. kártékony kód, adathalászat, sebezhetőségek kihasználása), a támadó profilja (pl. APT, szervezett bűnözés, hacktivisták), a célpont típusa (pl. természetes személyek, vállalatok, kritikus infrastruktúra), a védelem fázisai szerinti jellege (preventív, detektív, korrektív), valamint a támadás automatizáltsági szintje alapján. A szerzők emellett egyéb, kevésbé tárgyalt osztályozási lehetőségeket is bemutatnak, például a jogszabályi relevancia, az architektúra szintje vagy a támadási fázisok mentén (kill chain model alapján). Kiemelt figyelmet kapnak a pénzforgalmon keresztül megfigyelhető visszaélések, amelyek elsősorban a végfelhasználókat érintik. A kutatás rámutat arra, hogy a technológiai védekezés, a bűnüldözés fokozása nem elegendő: szükség van a pénzügyi tudatosság és a kibervédelmi ismeretek fejlesztésére is.

JEL-kódok: E50, K24, K49

Kulcsszavak: kiberbűnözés, csoportosítás, bankolás

1 *Kiss Milán* PhD hallgató, Miskolci Egyetem, levelező szerző. E-mail: milan.kiss@student.uni-miskolc.hu.
Kovács Levente főtitkár, Magyar Bankszövetség, tanszékvezető egyetemi tanár, Miskolci Egyetem. E-mail: kovacs.levente@bankszovetseg.hu.

1. BEVEZETÉS

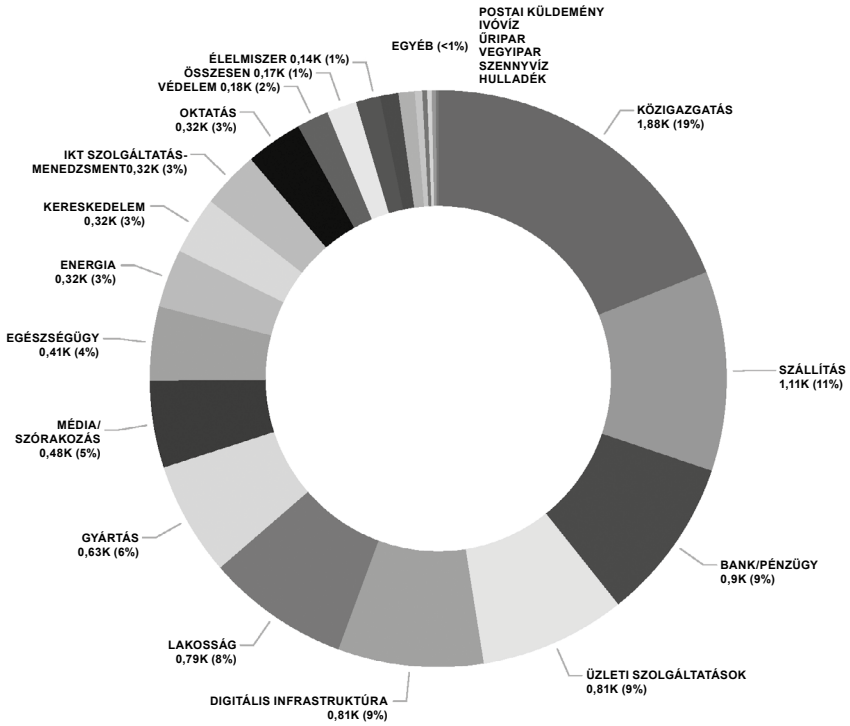
A kiberbűnözés, és azon belül is a pénzügyi típusú visszaélések jelentős hatással vannak a nemzetgazdaságra, valamint a pénzügyi rendszerbe vetett általános bizalomra. Ezért különösen fontos ezek vizsgálata abból a célból, hogy mind a bűnüldöző szervek, a különböző felügyeleti hatóságok, mind pedig a pénzügyi szervezetek, illetve a pénzügyi szolgáltatásokat igénybe vevők hatékonyan léphessenek fel, vagy védekezhessenek ezen visszaélésekkel szemben. Fontos továbbá, hogy a kiberbiztonsággal foglalkozó következő generáció oktatása magas színvonalú legyen. Ahhoz, hogy a védekezés és a megelőzés hatékonyságát megfelelő szintre emeljük, egy olyan rendszertan kidolgozása lehet szükséges, amelynek segítségével átláthatóan lehet osztályozni, azaz típusba sorolni az egyes kibertérben elkövetett visszaéléseket. Ezen csoportosítás segítséget nyújthat a jogalkotó számára, hogy megfelelő normaszövegek készülhessenek, de kibervédelmi szakértők számára is, amikor a kibervédelmi rendszereket megtervezik. Hozzájárulhat továbbá a kommunikáció, azon belül is az ügyféledukáció hatékonyabbá tételéhez, például egyedi pénzforgalmi szolgáltatói szinten, de akár közös fellépés[2] esetén is. Ezen felül segíthet az egyetemi és egyéb szakképzések keretében az oktatóknak, hogy az általuk készített vagy előadott tananyagban t a megértést és a tanulást hatékonyabban tudják támogatni.

Az elmúlt években, évtizedben a pénzügyi bűnözés átalakult. A fizikai térben elkövetett bűncselekmények, mint például pénzlopás, bankrablás áttevődtek a kibertérbe (Jaishankar, 2007). Ahogy a Mastercard „*A kiberbűnözés kora*" című kiadványban megjegyzi, „[a] kiberbűnözés olyan, mint bármely más bűncselekmény, ezért ennek megfelelően kell kezelnünk. Ha pénzt hoz, felível"; mindezt úgy, hogy ezek a vagyon elleni bűncselekmények nemzetköziek lettek (Mastercard, 2025). Ennek eredményeként a kiberbűnözés napjaink egyik legégetőbb problémájává vált. Lassan nem telik el úgy nap, hogy valamilyen online vagy offline médiumban ne hallhatnánk vagy olvashatnánk olyan hírt, amely valamilyen online térben elkövetett bűncselekményről, vagy kibertámadásról szól. A Szabályozott Tevékenységek Felügyeleti Hatósága honlapján elérhető információk alapján Magyarországon 2024-ben tizenháromezer ember vált kiberbűnözők áldozatává, amellyel mintegy 30 milliárd forint anyagi kár keletkezett (SZTFH 2024), ezzel szemben a Magyar Nemzeti Bank (MNB) közel 42 milliárd forint kárt említ (MNB 2025b). Ugyan az adatokban nagy a látencia, de az megállapítható, hogy a kiberbűnözés a 2020-as évekre jelentős és általános problémává vált. Mindazonáltal a kiberbűncselekmények nem egyformán érintik a különböző gazdasági

2 Lásd például a KiberPajzs kezdeményezést a https://kiberpajzs.hu/ oldalon.

szektorokat. Az Európai Uniós Kiberbiztonsági Ügynökség (The European Union Agency for Cybersecurity – ENISA) adatai szerint a kibertámadások mintegy 19 százaléka a közszektor ellen irányul, míg 11, illetve 9 százalék a közlekedési, illetve a pénzügyi szolgáltatók ellen. A legfőbb veszélyeket pedig a zsarolóprogramok (ransomware), rosszindulatú szoftverek (malware), az ún. social engineering (pszichológiai manipuláció), adatok elleni fenyegetések, elosztott szolgáltatásmegtagadással járó támadások (Distributed Denial-of-Service – DDoS), információmanipulálás és -befolyásolás, valamint az ellátási láncok elleni támadások jelentik (ENISA 2024).

1. ábra
A kibertámadások által megcélzott szektorok az incidensek száma szerint (2023. július – 2024. június)

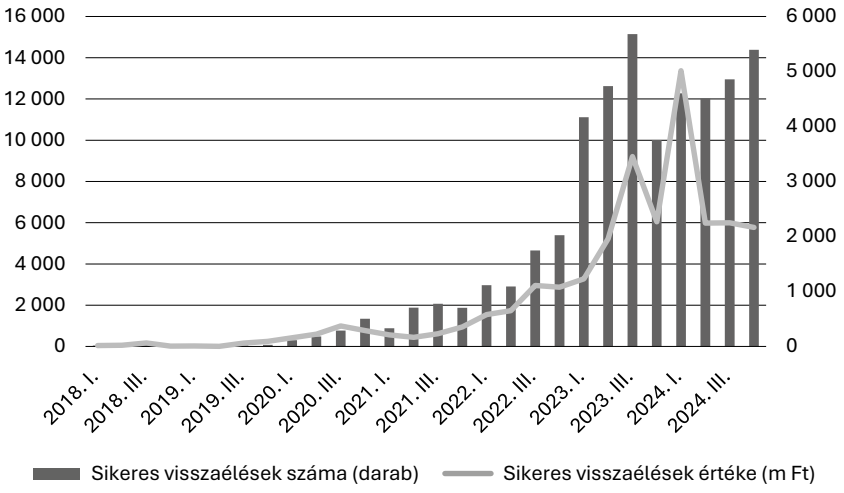


Forrás: (ENISA 2024)

A pénzügyi szektor esetében megállapítható, hogy a sikeres kibertámadások jellemzően nem a pénzügyi szervezeteket, azaz a szolgáltatókat érintik, hanem a pénzügyi szolgáltatásokat igénybe vevő ügyfeleket. Mindez elsősorban azért lehet,

mert Magyarországon az IT biztonságot érintő jogi keretrendszer magasan fejlett[3], valamint ezen jogi elvárásoknak a pénzügyi szektor nagymértékben meg is felel (MNB 2022). Azaz, az „általános" kiberveszélyek a pénzügyi szektorban speciálisan érvényesülnek. Vagyis kijelenthető, hogy például egy bankot vagy egy fizetési rendszert működtető szervezetet nagyon nehéz lehet „meghekkelni", míg az ügyfelek részéről nem mindig biztosított a hasonló szintű védelem. Ebből kifolyólag a kibertámadásokat elkövetők elsősorban a pénzügyi szolgáltatásokat igénybe vevő ügyfeleket támadják. Ezen visszaéléseket elsősorban az (elektronikus) pénzforgalmon keresztül lehet megfigyelni, mivel az elkövetők a visszaélések során eltulajdonított összegeket a pénzforgalmi rendszerek útján tudják megszerezni.

2. ábra
A pénzforgalmon keresztül megfigyelhető visszaélések száma és értéke



Forrás: (MNB 2025a)

A 2. ábra is alátámasztja és sajnálatos módon elmondható, hogy az elmúlt években a pénzforgalmon keresztül megfigyelhető visszaélések mind számosságban, mind pedig értékben folyamatosan növekedtek. Az MNB adatai alapján a sikeres

3 Az európai jogalkotó 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 szóló 2022. december 14 (EU) 2022/2554 európai parlamenti és tanácsi rendelet (Digital Operational Resilience Act – DORA) megalkotásával teremtette meg a korábbi magyar szabályozáshoz hasonló egységes követelményrendszert.

visszaélések száma folyamatosan növekedett, még a visszaélések értéke is kimagasló maradt az elmúlt negyedévek korrekciója után is.

2. A KIBERFENYEGETÉSEK CSOPORTOSÍTÁSI SZEMPONTJAI

A szakirodalomban számos olyan tanulmány található, amely valamilyen ismérv szerint rendszerezi a kiberbűncselekményeket. Ilyen tanulmány lehet például (Gordon–Ford, 2006; Onwubiko, 2020; Nagy, 2022), ugyanakkor ezen tanulmányok meglehetősen absztraktak, azaz általában a kibertámadásokra fókuszálnak, amelyekbe az információs rendszerek elleni támadásoktól kezdve a pornográf tartalmak is beletartoznak. Mindezek természetesen hasznosak a bűnüldöző és a szabályozó hatóságoknak, de a pénzügyi szervezetek számára a gyakorlati szempontok miatt kevésbé relevánsak.

Ezért indokolt olyan kategóriákat meghatározni, amelyek elősegítik a pénzügyi szervezetek, az őket felügyelő hatóságok, a kiberbiztonsági tananyagokat és kommunikációkat készítők, valamint a pénzügyi tárgyú törvényeket megalkotók számára a gyakorlati használhatóságot.

2.1. A támadás módszere szerinti csoportosítás[4]

A kiberbűncselekményeket csoportosíthatjuk a támadás típusa szerint. Ez a megközelítés azt vizsgálja, milyen jellegű a támadás vagy a fenyegetés, amely a célcsoportot éri. A csoportok főként a támadás eszközei szerint különülnek el.

A fenyegetés típusa szerint három kategóriát különböztethetünk meg:

- Malware támadások:
  Malware támadások keretében valamilyen rosszindulatú kód kerül az áldozat eszközére telepítésre (pl. ransomware – olyan zsarolóprogram, amely valamilyen fenyegetéssel próbál pénzt kicsikarni a felhasználótól; adware – reklámokat jelenít meg kéretlenül, néha megfigyeléssel kombinálva; keylogger – billentyűleütéseket rögzít érzékeny adatok megszerzéséhez; killware – fizikai károkozásra is alkalmas rosszindulatú szoftver, például kórházak elleni támadásokban). Kapcsolódó fogalmak: adware, backdoor, beaconing, binder, bot,

4 Az egyes csoportosítási szempontoknál példákat közlünk és azokat meg is magyarázzuk, hogy ezzel elősegítsük az adott szempont megértését. Ezt követően egy lista következik, amely az adott kategóriában található fogalmakat sorolja fel. A felsorolt fogalmak magyarázata megtalálható a jelen tematikus lapszámban, Kovács–Terták: Kibervédelmi fogalmak és értelmezésük c. tanulmányában.

botnet, cryptojacking, cryptotrojan, dkom, exploit, féreg, keylogger, killware, ransomware, time bomb, trojan, virus, worm.

- Szociális manipulációk:
  Ez esetben az informatikai eszköz használóját támadják és próbálják meg befolyásolni (pl. phishing /adathalászat/ – megtévesztő levelek bizalmas információkért; baiting /csalizás/ – ajándék vagy letöltés ígéretével csalogatja az áldozatot; whaling /bálnavadászat/ – kiemelt célpontokat, pl. CEO, támadnak megtévesztő módon). Ezen támadások sokszor az emberi mohóságra (nyereményekre vagy hatalmas hozamot ígérő befektetések ígéretére) építenek. Kapcsolódó fogalmak: adathalászat, angler phishing, baiting, bálnavadászat, business email compromise, célzott adathalászat, doxing, evil twin phishing, hoax, phishing, smishing, spoofing, vishing, whaling.
- Egyéb támadások:
  Elsősorban az informatikai rendszerek hiányosságait vagy sebezhetőségét érintik (DoS/DDoS – az informatikai rendszer túlterhelését okozó támadás; zero-day támadás – ismeretlen sebezhetőség kihasználása; exploit – célzott kódrészlet, amivel sérülékenységet használnak ki). Kapcsolódó fogalmak: DoS/DDoS támadás, exploit, zero-day támadás, SQL injection, cross-site scripting, DNS spoofing, DNS tunneling.

A támadás eszköze lehet tehát egy valaki által megírt rosszindulatú kód, a már meglévő informatikai hiányosság kihasználása, vagy a felhasználó közvetlen támadása.

2.2. A támadó profilja szerinti csoportosítás

A támadó profilja szerinti csoportosítás a kiberfenyegetések rendszerezésének egy emberközpontú megközelítése, amely a támadók szándékai, képességei, szervezettsége és erőforrásai alapján osztályozza őket. Ez a szempont különösen hasznos kockázatelemzéshez, védelmi stratégiák kialakításához és fenyegetésmodellezéshez. A támadók különféle motivációval, szakértelemmel és eszközkészlettel rendelkeznek. Ezek alapján a következő fő kategóriák különíthetők el:

- Állami támogatású / fejlett fenyegetési szereplők (APT – Advanced Persistent Threat):
  Szervezett csoportok, gyakran állami vagy katonai háttérrel, amelyek magas technikai színvonalat képviselnek (pl. saját sebezhetőség kihasználási módokat és ún. zero-day /nulladik napi/ támadásokat fejlesztenek). Jellemzően hosszú távú, rejtett és célzott műveleteket végeznek. Célpontjaik általában kormányzati szervek, hadiipar, nagyvállalatok, kritikus infrastruktúra, pél-

dául pénzügyi infrastruktúrák, pénzforgalmi szolgáltatók. Kapcsolódó fogalmak: APT, cyber warfare, cyber weapon.

- Szervezett bűnözői csoportok:
  Ezek jellemzően „profitorientált" szervezetek, céljuk pénz vagy pénzügyi zsaroláshoz adatok megszerzése. Kihasználják az adathalászat, BEC (Buesiness Email Compromise), malware, zombihálózatok lehetőségeit. Sok esetben „szolgáltatásként" működnek (pl. malware-as-a-service), ezzel kisebb tudású kiberbűnözők is nagy károk okozására válnak képessé. Kapcsolódó fogalmak: business email compromise, bot, botnet, cryptojacking, cryptotrojan, black hat hacker.
- Hacktivisták:
  Jellemzően politikai vagy ideológiai célokat követnek, amely célok elérése miatt feltörnek informatikai rendszereket, weboldalakat, adatokat szivárogtatnak ki, illetve weboldalak megjelenését változtatják meg (ún. website defacement). Céljuk legtöbbször a figyelemfelkeltés, nem feltétlenül az anyagi haszonszerzés. Kapcsolódó fogalmak: hacktivist, doxing.
- Script kiddie (kezdő támadók):
  Kevés saját technikai tudással rendelkeznek, általában mások által írt kódokat, szoftvereket használnak. Céljaik lehetnek: hírnév, szórakozás, bosszú. Ilyen támadásra példa lehet a KRÉTA rendszert „meghekkelő" 15 éves fiú. Kapcsolódó fogalmak: phishing.

A fenti csoportosítás kapcsán érdemes még megemlíteni az etikus hackerekeket és a biztonsági szakembereket, akik a megfelelő engedélyek birtokában, legális keretek között tesztelik egyes rendszerek biztonságát abból a célból, hogy javítsák az informatikai rendszerek védelmét. Ilyen tesztre lehet példa a penetrációs teszt, vagy a jogszabály, illetve az Európai Unió közvetlenül alkalmazandó jogalkotási aktusa által előírt teszt (pl. a DORA 26. cikkében említett fenyegetés alapú behatolási tesztelés, TLPT - threat-led penetration testing).

2.3. A célpont típusa szerint csoportosítás

A kiberfenyegetések célpontjai különböző típusú szereplők lehetnek: természetes személyek, vállalkozások (mikrovállalkozások, KKV-k, de nagyvállalatok is), vagy akár nemzetbiztonsági szempontból kiemelt infrastruktúrák.

- Természetes személyek elleni kibertámadások:
  Ezen támadások esetében a cél jellemzően a pénzügyi visszaélés mellett a személyes adatok megszerzése vagy privát információk ellopása. Jellemző támadások: keylogger, phishing, doxing (személyes vagy egy adott szerve-

zetre vonatkozó információk nyilvánosságra hozása, lejáratás céljából), nigériai típusú csalás (romantikus vagy segélykérő történettel pénzt csalnak ki), cyberbullying (online zaklatás közösségi platformokon vagy egyéb üzenetküldő alkalmazások útján). Az emberi kapzsiságra építő támadások (váratlan nyeremények vagy magas hozamot ígérő befektetések ígérete) szintén jellemzőek. Kapcsolódó fogalmak: keylogger, phishing, doxing, cyberbullying, evil twin phishing, angler phishing, baiting, smishing, vishing, spoofing.

- Vállalkozások:

  A vállalkozások vagy egyéb szervezetek, például alapítványok vagy non profit szervezetek[5] elleni támadások célja elsősorban pénzszerzés üzleti adatok ellopásával, rendszerek megbénítása váltságdíjért (ransomware), beszállítói lánc kompromittálása, versenyelőny szerzése vagy bizalmas adatok kiszivárogtatása. Jellemző támadások lehetnek a Business Email Compromise (BEC) – céges levelezések manipulálása, hamis számlaadatokkal történő csalás, spear phishing / whaling –, amely nem más, mint célzott adathalászat döntéshozók ellen, illetve rosszindulatú kódokkal történő támadások (pl. ransomware támadás, amely fájlok titkosítása után a feloldásért váltságdíj követelésével jár). Kapcsolódó fogalmak: business email compromise, spear phishing, whaling, ransomware, cryptojacking, botnet, backdoor, exploit, binder, payload.

- Kritikus infrastruktúrák:

  Ezek az ágazatok a társadalom működéséhez alapvető fontosságúak: egészségügy, közlekedés, energia, vízellátás, kormányzati rendszerek stb. A pénzügyi szervezetek esetében példák lehetnek erre a fizetési és értékpapírelszámolási rendszerek[6], de akár jelentős lakossági ügyfélállománnyal rendelkező hitelintézetek is. A támadások célja rendszerint: fizikai vagy gazdasági károkozás, politikai destabilizálás, illetve a lakosság ellátásának megzavarása. A támadásokat jellemzően killware, APT támadások és DoS/DDoS támadások útján hajtják végre. Kapcsolódó fogalmak: APT, DoS/DDoS, cyber weapon, cyber warfare.

A célpont szerinti elhatárolás nagyon fontos, mivel a támadott célpontok eltérő szintű védelemmel és válaszlépési lehetőséggel rendelkeznek. A lakosság védelme

5 Egyes kutatás-fejlesztési területen tevékenykedő, magas hozzáadott értéket termelő szervezetek az Európai Unióban nonprofit vagy alapítványi formában működnek.

6 Az MNB által működtetett Valós Idejű Bruttó Elszámolási Rendszer (VIBER), a GIRO Elszámolásforgalmi Zrt. által üzemeltetett Bankközi Klíring Rendszer (BKR), továbbá a KELER Központi Értéktár Zrt. és a KELER KSZF Központi Szerződő Fél Zrt. értékpapírelszámolásokhoz és nyilvántartásokhoz kapcsolódó infrastruktúrái.

természetesen teljesen más eszközöket igényel, mint például a magyar pénzforgalom biztonságának a szavatolása.

2.4. A védekezés fázisa szerint csoportosítás

Az informatikai rendszer védelme három jól elkülöníthető részre osztható (Gyaraki, 2023).

- Preventív intézkedések:

  Ezen intézkedések célja a támadások megelőzése, azaz, hogy a támadók ne férhessenek hozzá az informatikai rendszerhez. Preventív kontrollok lehetnek fizikai behatolást megakadályozó, adminisztratív vagy egyes logikai kontrollok. Kapcsolódó fogalmak: Anti-phishing, Bug bounty.

- Detektív intézkedések:

  Céljuk, hogy a támadások „ismertté" váljanak, azaz beavatkozni ugyan nem tudnak, de a kibertámadást láthatóvá teszik. Kapcsolódó fogalmak: IDS, SIEM.

- Korrektív intézkedések:

  Az észlelt kibertámadásra reagáló intézkedések, amelyek célja a támadás kiterjesztésének, illetve magának a támadásnak a megállítása, valamint a további károk megelőzése. Kapcsolódó fogalmak: CIRT.

2.5. A támadáshoz használt eszköz jellege szerint

A támadások egyik alapvető jellemzője, hogy milyen mértékben támaszkodnak automatizmusokra, illetve mennyire igényelnek emberi közreműködést, döntéshozatalt. A két fő kategória: automatizált és manuális/interaktív támadások. Megjegyezzük, hogy egyes eszközök, mint a mesterséges intelligencia ilyen kategorizálása nehézkes lehet.

- Automatizált támadások:
  Ezen támadások jellemzően nagy volumenben zajlanak – több ezer vagy akár millió támadást hajtanak végre egy célponttal szemben. Tipikusan nem vagy minimális emberi beavatkozást igényel maga a támadás, amely gyors, ismételhető és skálázható. Ilyen támadásra példa lehet a botnet támadás, amely nagy számú fertőzött eszközből álló hálózat, melyet egy központi irányító irányít. A botneteket használják DDoS támadások lebonyolítására, spamküldésre, vagy ún. brute force jelszótörésre, amely esetében egyszerű „nyers erővel", azaz próbálgatással próbálnak informatikai eszközökhöz hozzáférni. Kap-

csolódó fogalmak: botnet, ddos-támadás, cryptojacking, ransomware, brute force, worm, beaconing, backdoor, spam, exploit.

- Manuális támadások:
  Manuálisan általában célzott támadások történnek, gyakran konkrét szervezetek vagy személyek ellen. A manuális támadások emberi megfigyelést, döntéshozatalt és taktikai tervezést igényelnek. Jellemzőjük a részletes előkészület, intelligens kivitelezés. Gyakran komplex támadási lánc részeként valósulnak meg. Típusai lehet például a spear phishing, amely kifejezetten egy szervezetre vagy személyre szabott adathalászat. Információgyűjtés után célzott e-mail küldés, gyakran vezetőknek (a vezetőket támadó phishing az ún. whaling). A támadó türelmesen épít bizalmat, majd ezt követően próbálja megszerezni az érzékeny adatokat. Kapcsolódó fogalmak: spear phishing, whaling, phishing, doxing, angler phishing, evil twin phishing, baiting, smishing, vishing, social engineering.

A két támadástípus ellen más jellegű védelem kialakítására lehet szükség.

2.6. Egyéb csoportosítási szempontok

A korábbiakban ismertetett főbb csoportosítási szempontokon túlmenően a kiberbiztonsági fogalmak osztályozására további dimenziók is alkalmazhatók. Ezek segítenek a fenyegetések mélyebb megértésében és a védekezési stratégiák finomhangolásában.

a) A támadás helye az informatikai architektúrában

Az egyik további szempont az, hogy a támadás melyik informatikai komponensre irányul:

- Kliensoldali támadások: Ez esetben a felhasználó által használt eszköz vagy szoftver a célpont. Ilyen típusú fenyegetés lehet az adware (reklámalapú szoftverek), vagy a keylogger, amely a felhasználó billentyűleütéseit rögzíti. Kapcsolódó fogalmak: adware, keylogger, baiting, phishing, doxing, smishing, vishing, angler phishing, evil twin phishing, spyware, ransomware (ha kliensoldali fájlokat titkosít).
- Szerveroldali támadások: Ebben az esetben a szolgáltatást biztosító rendszer (pl. web- vagy adatbázisszerver) ellen indítanak támadást. Jellemző példák: DoS-támadások (szolgáltatásmegtagadásos támadás), ransomware (zsarolóprogram). Kapcsolódó fogalmak: DoS/DoS-támadások ransomware, backdoor, exploit, brute force.
- Hálózati szintű támadások: ez esetben a kommunikáció és az adatátvitel a támadás célpontja. Tipikus példa a DNS tunnelling, amikor a DNS-protokollt

rosszindulatú programok adatátvitelére használják, vagy az evil twin jelenség, ahol egy hamis Wi-Fi hálózatot hoznak létre az áldozatok megtévesztésére. Kapcsolódó fogalmak: DNS tunnelling, evil twin phishing, spoofing, beaconing, mitm (man-in-the-middle), sniffing.

Ezen csoportosítás elsősorban IT biztonsági szakértők számára lehet releváns, mivel a védendő eszközök képezik a csoportosítás alapját. Megjegyzendő ugyanakkor, hogy az ún. zero trust biztonsági stratégia esetében a csoportosítás nem releváns.

b) Jogszabályi megközelítés

Szempont lehet az is, hogy az adott cselekedet jogilag megengedett, tiltott vagy bizonytalan megítélés alá esik:

- Kifejezetten büntetendő cselekmények: Ide tartozik például a fizetési kártyák klónozása, amely a büntetőjog szerint készpénz-helyettesítő fizetési eszköz elleni visszaélésnek minősül. Megjegyezzük, hogy egyes esetekben az adott cselekmény büntetőjogi megítélése nem egyértelmű, amelyre példa lehet a phishing (Biró–Kiss, 2024). Kapcsolódó fogalmak: phishing, spear phishing, whaling, ransomware, keylogger, backdoor, botnet, ddos-támadás, dos-támadás, spoofing, smishing, vishing, angler phishing, evil twin phishing, cryptojacking, exploit, doxing.
- Jogszerű tevékenység speciális keretek között: szerződés vagy egyéb megállapodás alapján végzett etikus hacking (pl. penetrációs teszt) jogszabályi elvárásra is történhet, tehát nem szankcionálandó, hanem előírt tevékenység. Kapcsolódó fogalmak: etikus hackelés, bug bounty.
- Szürkezóna: Az OSINT (Open Source Intelligence) alkalmazása, azaz nyilvánosan elérhető adatok gyűjtése hírszerzési céllal, egyes esetekben a kockázatos zónába eshet, mivel jogilag nem tilalmazott, azonban erkölcsileg nem igazolható. Kapcsolódó fogalmak: OSINT, cyber threat intelligence, gray hat hacker, digitális lábnyom gyűjtése.

A jogalkotók és a jogalkalmazó pénzügyi szervezetek és hatóságok számára bírhat relevanciával ez a csoportosítás, mivel alapja lehet a joghézagok azonosításának, illetve a pénzügyi ágazati titkok megvédésének.

c) A fogalom jellege szerint

A kiberbiztonsági fogalmak jellegük szerint is csoportosíthatóak.

- Technikai fogalmak: például az exploit, malware, amelyek informatikai szakmai terminusok. Kapcsolódó fogalmak: exploit, malware, ransomware, keylogger, botnet, backdoor, DNS spoofing, dns tunneling, ddos-támadás,

dos-támadás, beaconing, brute force, payload, phishing, spear phishing, spam, VPN, SSL, TLS, IDS, IPS, antivírus, Indicator of Compromise, cyber weapon, firewall, sniffin.

- Köznyelvi vagy szlengkifejezések: például hoax, ami álhíreket vagy megtévesztő tartalmakat jelent, amelyeket főleg a felhasználók manipulálására használják. Kapcsolódó fogalmak: hoax, baiting, smishing, vishing, evil twin phishing, angler phishing, gray hat hacker, black hat hacker, white hat hacker, script kiddie, whaling, hacker, spoofing.
- Jogi terminológia: például elektronikus információs rendszer, elektronikus pénz, készpénz-helyettesítő fizetési eszköz, amelyeket jogszabályok vagy Európai Uniós jogalkotási aktusok határoznak meg. Kapcsolódó fogalmak: kiberbűnözés, etikus hackelés, digitális lábnyom, személyes adat, információs rendszer, OSINT.

Ezek a további szempontok lehetővé teszik a fogalmak többdimenziós vizsgálatát, ami segíthet a kiberbiztonsági fenyegetések komplexebb elemzésében, valamint a szabályozási, oktatási és védelmi mechanizmusok hatékonyabb kialakításában.

d) A támadás fázisa szerint

A támadás fázisai szerinti csoportosítás az egyik leggyakrabban alkalmazott módszer a komplex, célzott kibertámadások megértésére és modellezésére. Ezt a szemléletet a híres Cyber Kill Chain modell alapozta meg (Lockheed Martin, 2025), amely jól bemutatja, hogyan bontakozik ki egy támadás lépésről lépésre.

A modell szerint a támadás a következő fázisokból áll:

- Felderítés: A támadó információt gyűjt a célpontról, annak rendszereiről, alkalmazottjairól, e-mailcímeiről, technológiai környezetéről. Ennek célja, hogy a támadó megértse a célpont működését, hogy a támadás testre szabható legyen. Kapcsolódó fogalmak: OSINT, doxing, social engineering, whaling, spear phishing.
- Belépés / Inicializálás: a támadó kiválasztja és eljuttatja az eszközt, amely lehetővé teszi a hozzáférést, pl. social engineering segítségével. Célja a kártékony kód bejuttatása vagy a felhasználó rávétele, hogy „megnyissa az ajtót". Kapcsolódó fogalmak: phishing, smishing, vishing, baiting, angler phishing, evil twin phishing, spoofing, malware, exploit.
- Installálás: A támadó stabil hozzáférést alakít ki, és megpróbál magasabb jogosultságot szerezni. Innen „mozogni kezd" a hálózaton belül. Cél: az infrastruktúra mélyebb rétegeihez való hozzáférés biztosítása és a jelenlét elrejtése. Kapcsolódó fogalmak: backdoor, keylogger, botnet, cryptojacking, ransomware, beaconing, worm, binder, rootkit, payload.

- A cél elérése és kivonulás: A támadó végrehajtja a valódi célját (pl. adatlopás, zsarolás), majd elhagyja a rendszert – lehetőleg nyom nélkül. Ezen fázis célja az adatok megszerzése, zsarolás vagy más támadási cél teljesítése, a felfedezés minimalizálása mellett. Kapcsolódó fogalmak: data exfiltration, ransomware, spyware, identity theft, exfiltration, killware.

Természetesen a fent felsorolt csoportosítási szempontokon túlmenően számos egyéb csoportosítás is elképzelhető (pl. MITRE ATT&CK® keretrendszer[7]).

3. A PÉNZFORGALMON KERESZTÜL MEGFIGYELHETŐ VISSZAÉLÉSEK

Az MNB számos alkalommal kijelentette, hogy a magyar pénzügyi rendszer európai összehasonlításban is biztonságosnak számít (MNB 2023). Többek között ez az oka, hogy a 5/2023. (VI.23.) MNB ajánlás (Anti-fraud ajánlás) címében a pénzforgalmi szolgáltatásokon keresztül megfigyelhető, és nem a pénzforgalmi szolgáltatásokat érintő visszaélések szerepelnek. Mindazonáltal a pénzforgalmi szolgáltatásokat igénybe vevő ügyfelek találkozhatnak kiberbűncselekményekkel. Ezek a kiberbűncselekmények a fentiekben ismertetettek szerint csoportosíthatók.

1. táblázat
A leggyakoribb, pénzforgalmon keresztül megfigyelhető visszaélések

Típus	Fő célpont	Eszköz	Célja
Business Email Compromise	Vállalkozások	E-mail, számla	Átutalás manipulálása
CEO-fraud / Social engineering	Vállalkozások pénzügyei	E-mail, pszichológiai manipuláció	Belülről utalás kezdeményeztetése
Phishing / Smishing / Vishing	Magánszemélyek	E-mail, SMS, telefon	Hozzáférés adatlopással
Kártyacsalás	Pénzforgalmi szolgáltatók ügyfelei	Kártyaadatok	Jogosulatlan vásárlás
Ál-webáruházak	Vásárlók	Hamis oldal	Pénz vagy adat megszerzése
Ransomware	Vállalkozások, intézmények	Káros kód és kriptofizetés	Váltságdíj
Előrefizetéses csalás	Bárki	E-mail	Pénz kicsalása ígéretért

Forrás: (OECD 2022; CISA 2023; FBI 2023; Kovács–Terták 2024)

7 Lásd https://attack.mitre.org/ weblapot.

Megjegyzendő továbbá, hogy az *1. táblázatban* bemutatott támadási módok csupán jelenleg, 2025 nyarán a leggyakoribbak. Természetesen, ahogy általában a kibertámadások esetében, a pénzforgalmi úton megfigyelhető visszaélések esetében is folyamatos a változás. Míg 2020-ban a hagyományos módszerek domináltak, például fizikálisan eltulajdonították az ügyfelek fizetési kártyáit, addig 2025-re lényegesen kifinomultabb csalások váltak gyakoribbá és nem ritka a mesterséges intelligencia használata sem. Például a rendőrség az ún. Mátrix projekt keretében számolt fel egy banki ügyfélközpontokhoz hasonló rendszert működtető csoportot (ORFK 2024).

A fentiek alapján kijelenthető, hogy a leggyakrabban előforduló, a pénzügyi szervezeteket is érintő, a kibertérben elkövetett visszaélések számos, az előzőekben ismertetett csoportosítás szerint klasszifikálhatóak. Megállapítható továbbá az is, hogy ezen csoportosításokra szükség van, mivel jelentősen elősegíthetik a visszaélések elleni védekezést azáltal, hogy hatékonyabb kommunikációt, illetve egyértelműbb jogalkotást tesznek lehetővé.

A visszaélések elleni védekezés korántsem egyszerű. A napi pénzügyi tapasztalat a pénzügyi tudatosság növelését hangsúlyozza, ahogy (Hergár–Kovács–Németh, 2024) teszik tanulmányukban. Míg más szerzők a technológia és jogszabályok nyújtotta lehetőségeket emelik ki (Doeland, 2019). A hazai szabályozó, az MNB a második pénzforgalmi irányelv (PSD2 – Payment Services Directive 2[8]) hazai jogba történő átültetése és az azonnali átutalások bevezetése óta egy négy elemből álló komplex keretrendszer mentén igyekszik fellépni a visszaélések megelőzésének érdekében (Kiss, 2023).

ÖSSZEGZÉS

A tanulmány áttekintést nyújt a pénzügyi szektort érintő kiberbűnözés aktuális helyzetéről, annak rendszerezési lehetőségeiről és a védekezési mechanizmusok szükségességéről. A digitális tér egyre hangsúlyosabb szerepe, a mindennapi pénzügyek elektronikus kezelése, valamint az online szolgáltatások térnyerése jelentősen megnövelte a kibertámadások lehetőségét, és ezzel párhuzamosan azok súlyát és társadalmi-gazdasági hatását is.

Az első fejezetek rávilágítanak arra, hogy a bűnözés szerkezete az elmúlt évtizedben jelentős mértékben eltolódott a fizikai térből a kibertér irányába. Ez a változás különösen érzékelhető a pénzügyi visszaélések területén, ahol a hagyományos bűncselekményeket – például rablásokat – felváltották az online környezetben

8 (EU) 2015/2366 európai parlamenti és tanácsi irányelv

elkövetett, technológiai eszközökkel támogatott visszaélések, támadások. A tanulmány kiemeli, hogy a magyar pénzügyi szervezetek IT-védelme európai viszonylatban is fejlett, ezért a támadások jelentős része az ügyfelek ellen irányul, akiknek kevesebb védelemre fordítható erőforrásuk van, ezért alacsonyabb az önvédelmi képességük, és gyakran még információhiányosak is.

A kutatás során a rendszertani megközelítést alkalmaztuk, amelynek célja, hogy átfogó és a gyakorlatban is alkalmazható csoportosításokat kínáljon a kiberbűncselekmények típusaira. Ez a megközelítés több szempont mentén valósul meg:

1. A támadás módszere szerint: ebben a kategóriában különböznek a technikai eszközökkel végrehajtott (malware, exploit), a felhasználói megtévesztésen alapuló (phishing, baiting), valamint a rendszerhiányosságokat kihasználó (DoS/DDoS, zero-day) támadások. E csoportosítás segíti a védelmi mechanizmusok célzott kiépítését, hiszen más megközelítést igényel egy technikai támadás, mint egy pszichológiai manipuláció.
2. A támadó profilja szerint: ebben az esetben a támadók motivációi, eszközei és szervezettségi szintje alapján történik a rendszerezés. Az állami hátterű APT-k, a szervezett bűnözői csoportok, a hacktivisták, valamint a kevésbé képzett script kiddie-k eltérő veszélyszintet és fenyegetettséget jelentenek. A támadók tipizálása különösen fontos a célzott megelőzés és fenyegetésmodellezés szempontjából.
3. A célpont típusa szerint: a természetes személyek, vállalkozások és kritikus infrastruktúrák eltérő jellegű és volumenű támadásoknak vannak kitéve. A tanulmány részletesen bemutatja, milyen típusú visszaélések jellemzőek ezekre a szereplőkre – a keyloggertől és phishingtől kezdve egészen a ransomware támadásokig vagy beszállítói láncok kompromittálásáig.
4. A védekezés fázisai szerint: a védekezés három részre bontása. A klasszikus felosztás szerint preventív, detektív és reaktív kontrollokra bontható az informatikai rendszer védelme.
5. A támadáshoz használt eszközök automatizáltsága szerint: nagy volumenben lebonyolított automatikus támadások, továbbá célzott, egy-egy célpontot támadó manuális akciók.
6. Egyéb csoportosítási szempontok is bemutatásra kerülnek, pl. jogi relevancia szerinti vagy a támadott eszköz szerint, illetve az ún. kill chain modell szerint a támadás fázisai alapján.

A tanulmány külön figyelmet szentel annak, hogy a pénzforgalmon keresztül megfigyelhető visszaélések miként illeszkednek a fenti csoportosítási keretrendszerbe. A gyakorlati példák – mint a Business Email Compromise, phishing, CEO-fraud vagy ál-webáruházak – jól illusztrálják, hogyan fonódnak össze a tá-

madási formák a technológiai és pszichológiai manipulációs elemekkel, és hogy ezek a pénzügyi ökoszisztéma mely pontjain fejtenek ki hatást.

Az elmúlt években bevezetett Európai Uniós jogalkotási aktusok, jogszabályok és jogszabályi erővel nem rendelkező ajánlások – különösen a PSD2, DORA és az Anti-fraud ajánlás bevezetése – erősítik a védekezési keretrendszert, ugyanakkor a technológiai fejlődés üteme szükségessé teszi a folyamatos adaptációt. A védekezés nem lehet kizárólag technológiai alapú; legalább ennyire fontos az ügyfelek pénzügyi tudatosságának fejlesztése, az edukáció, valamint a célzott kommunikációs kampányok.

A kiberbűnözés elleni küzdelem sikeressége érdekében elengedhetetlen egy jól strukturált és a gyakorlatban is használható rendszertan kidolgozása. Ez nemcsak a kiberbiztonsági szakemberek és jogalkotók munkáját segíti, hanem a pénzügyi szolgáltatók és ügyfelek számára is pontosabbá teszi a fenyegetések természetét és a lehetséges védekezési stratégiákat.

A tanulmány egyik fő érdeme, hogy a nemzetközi szakirodalom általánosabb megközelítésétől eltérően kifejezetten a pénzügyi szektor sajátosságait és gyakorlati igényeit helyezi fókuszba. Ennek eredményeként olyan csoportosítási szempontokat alkalmaz, amelyek közvetlenül támogathatják a pénzügyi szolgáltatók belső kockázatkezelési, ügyfélkommunikációs és technológiai fejlesztési folyamatait.

Zárógondolat

A kiberfenyegetettség dinamikusan változó környezetében a bűnüldözés támogatása, illetve a megelőzés érdekében a pénzügyi szektor szereplőinek – legyen szó szabályozó hatóságokról, szolgáltatókról vagy ügyfelekről – összehangolt, proaktív és tudatos fellépésére van szükség. Az ehhez vezető út egyik alapköve a támadások rendszerezése, megértése és előrejelzése. A bemutatott rendszertani megközelítés olyan alapot biztosít, amelyre a jövőben hatékony védekezési és szabályozási struktúrák épülhetnek, és amely egyaránt szolgálja a pénzügyi stabilitást, az ügyfelek biztonságát és a digitális ökoszisztéma fenntarthatóságát.

HIVATKOZÁSOK

Biró, G. – Kiss, M. (2024): Adathalászat és az ellene történő egyes védekezési lehetőségek. *Gazdaság és Pénzügy* 11(4): 417–439. https://doi.org/10.33926/GP.2024.4.2.

CISA (2023): #StopRansomware Guide. https://www.cisa.gov/sites/default/files/2025-03/StopRansomware-Guide%20508.pdf.

Doeland, M. (2019): How to keep payments safe and secure in a changing world. *Journal of Payments Strategy & Systems* 13(2): 132. https://doi.org/10.69554/FSLK7337.

ENISA (2024): ENISA threat landscape 2024: July 2023 to June 2024. *LU: Publications Office*. https://data.europa.eu/doi/10.2824/0710888.

FBI (2023): Internet Crime Report. https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf

Gordon, S. – Ford, R. (2006): On the definition and classification of cybercrime. *Journal in Computer Virology* 2(1): 13–20. https://doi.org/10.1007/s11416-006-0015-z.

Gyaraki, R. (2023): Az információbiztonság alapjai. https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/az_informaciobiztonsag_alapjai_konyv_kesz_2.pdf.

Hergár, E. – Kovács, L. – Németh, E. (2024): A pénzügyi kultúra helyzete és fejlődése Magyarországon. *Hitelintézeti szemle* 23(1): 5–28. https://doi.org/10.25201/HSZ.23.1.5.

Jaishankar, K. (2007): Establishing a theory of cyber crimes. *International journal of cyber criminology* 1(2): 7–9. https://www.cybercrimejournal.com/IJCC-July-December-2007-Vol1-No2.php.

Kiss, M. (2023): Az MNB szerepe a pénzforgalmon keresztül megfigyelhető visszaélések kezelésében. *HANTOS PERIODIKA* 4(2): 279–290.

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.

Lockheed Martin (2025): Cyber Kill Chain. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Mastercard (2025): A kiberbűnözés kora 2025. https://www.mastercard.hu/content/dam/public/mastercardcom/eu/hu/pdfs/A%2520kiberb%25C5%25B1n%25C3%25B6z%25C3%25A9s%2520kora%25202025.pdf&ved=2ahUKEwjvkaPF09ONAxUt9rsIHeGvCQ0QFnoECBgQAQ&usg=AOvVaw1960KT7grbPA6T5Bb30sXw.

MNB (2022.12.): A magyar pénzügyi szektor kiberfenyegettségi térképe 2022. *Magyar Nemzeti Bank*. https://www.mnb.hu/letoltes/kiberfenyegetettsegi-terkep-2022.pdf.

MNB (2023, június): Fizetési Rendszer Jelentés 2023. *Magyar Nemzeti Bank*. https://www.mnb.hu/letoltes/fizetesi-rendszer-jelentes-2023-hun-0626.pdf.

MNB (2025a): Pénzforgalmi táblakészlet. https://statisztika.mnb.hu/publikacios-temak/penzforgalmi-adatok/penzforgalmi-adatkozlesek/tajekoztato---penzforgalom.

MNB (2025b, július 17): Fizetési Rendszer Jelentés 2025. *Magyar Nemzeti Bank*. https://www.mnb.hu/letoltes/mnb-fizetesi-rendszer-jelentes-2025-hun-digitalis-vegleges.pdf.

Nagy, Z. A. (2022): Kibernyomozói kézikönyv. Budapest: Nemzeti Közszolgálati Egyetem *Ludovika Egyetemi Kiadó*.

OECD (2022): Online Consumer Fraud in the Digital Age. https://one.oecd.org/document/DSTI/CP(2021)7/FINAL/en/pdf.

Onwubiko, C. (2020): Fraud matrix: A morphological and analysis-based classification and taxonomy of fraud. *Computers & Security* 96 101900. https://doi.org/10.1016/j.cose.2020.101900.

ORFK (2024): MÁTRIX Projekt: Borult az első Call Center. https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/matrix-projekt-borult-az-elso-call-center.

SZTFH (2024): Mintegy 30 milliárd forintnyi kárt okoztak a kibercsalások hazánkban. https://sztfh.hu/mintegy-30-milliard-forintnyi-kart-okoztak-a-kibercsalasok-hazankban/.