DOI: https://doi.org/10.12700/btsz.2025.7.3.63

THE FINANCIAL SECTOR IN CYBERSPACE: RISKS, TRENDS, AND STRATEGIC RESPONSES FOR PROTECTING CRITICAL INFRASTRUCTURE

PÉNZÜGYI SZEKTOR A KIBERTÉRBEN: KOCKÁZATOK, TRENDEK ÉS VÁLASZLEHETŐSÉGEK A KRITIKUS INFRASTRUKTÚRA VÉDELMÉBEN

GULYÁS Olivér[1] – KISS Gábor[2]

Abstract

This study examines cyberattacks targeting the financial sector, aiming to explore why financial institutions have become primary targets of attacks. The analysis provides an overview of the main types of cyberattacks, their technological, economic, and social impacts, as well as the relevant regulatory frameworks at both and international and EU levels. The research draws on the most recent reports from the European Union Agency for Cybersecurity, the European Parliament, and other professional organizations. Special attention is given to sector-specific vulnerabilities, targeted attack patterns—such as phishing, ransomware, DDoS attacks, and social engineering techniques—and their long-term consequences. An important finding is that cybersecurity vulnerabilities in the financial sector not only result in direct financial losses but may also undermine social stability and political trust. The study concludes with policy recommendations aimed at strengthening regulatory frameworks, enhancing technological defenses, and improving cybersecurity awareness and education for both financial institutions and users.

Keywords

cyber attack, financial institution, cyber resilience, critical infrastructure, cyber security

Absztrakt

A tanulmány a pénzügyi szektort érintő kibertámadásokat vizsgálja. Megpróbálja megválaszolni miért váltak a támadások elsődleges célpontjaivá. Az elemzés áttekinti a kibertámadások típusait, azok technológiai, gazdasági és társadalmi hatásait, valamint a nemzetközi és uniós szintű szabályozási kereteket. A kutatás az Európai Unió Kiberbiztonsági Ügynökség, az Európai Parlament és más szakmai szervezetek legfrissebb riportjaira támaszkodik. A tanulmány külön figyelmet fordít a pénzügyi szektor specifikus kockázataira, az azokat célzó célzott támadási mintázatokra – adathalászat, zsarolóvírusok, DDoS támadások és *social engineering* technikák – valamint azok hosszú távú következményeire. Fontos megállapítás, hogy a pénzügyi szektor kiberbiztonsági sérülékenységei nem csupán anyagi károkat okoznak, hanem közvetve a társadalmi stabilitásra és a politikai bizalomra is hatást gyakorolhatnak. A tanulmány zárásként javaslatokat fogalmaz meg a szabályozási környezet erősítésére, a technológiai védekezés fejlesztésére, valamint a pénzintézeti és felhasználói edukáció fokozására.

Kulcsszavak

kibertámadás, pénzintézet, kiberreziliencia, kritikus infrastruktúra, kiberbiztonság

[1] gulyaso@gmail.com | ORCID: 0000-0001-6945-2222 | doctoral candidate, Óbudai University | doktorandusz, Óbudai Egyetem

[2] kiss.gabor@bgk.uni-obuda.hu | ORCID: 0000-0002-0447-9376 | associated professor, Óbudai University | egyetemi docens Óbudai Egyetem

BEVEZETÉS

A digitalizáció térnyerésével a gazdaság és a társadalom mind nagyobb részét befolyásolja a számítástechnikai rendszerek megbízhatósága és biztonsága. A kibertámadások már nemcsak technológiai kihívást jelentenek, hanem komoly gazdasági, társadalmi és politikai következményekkel is járhatnak. Különösen igaz ezutóbbi a pénzügyi szektorra. A pénzintézetek a gazdaság gerincét képező mechanizmusokat szolgálják ki, és mint ilyenek, fokozottan kitettek a rosszindulatú támadásoknak.

Jelen tanulmány célja, hogy átfogó képet nyújtson a kibertámadások fogalmáról, típusairól és a pénzügyi ágazatra gyakorolt hatásaikról. Különös tekintettel arra, hogy ezen ágazat miként vált napjainkra egyik elsődleges célpontjává a modern kiberfenyegetéseknek. Az Európai Unió, az Egyesült Államok és különböző nemzetközi szervezetek jelentései alapján bemutatásra kerülnek a legfrissebb trendek, támadási módszerek és szabályozási kihívások, amelyek meghatározzák a pénzintézetek kiberrezilienciáját a 21. században.

A KIBERTÁMADÁSOK FOGALMA ÉS JELENTŐSÉGE

A kibertámadás megnevezés alatt kell érteni minden számítógépek, számítógépes rendszerek ellen indított műveletet. Egy-egy ilyen művelet az adatlopást, az adatok megsemmisítését, de akár a teljes informatikai rendszer elérhetetlenségét, végső esetben teljes tönkre tételét is célozhatja.

Az Európai Parlament egyik elemzésében a kibertámadások demokráciára gyakorolt hatását vizsgálja. Véleményük szerint a „kibertámadások által okozott károk túlmutatnak a gazdaságon és a pénzügyeken, mivel veszélyeztetik a társadalom alapvető működését” [1].

A pénzügyi szektor évszázados működése során már megismerte, felkészült a tradicionális veszélyforrásokra – rossz hitelek, csalások stb. A 21. századtól viszont új veszélyforrásokkal kell szembenézniük. A 2020-as évektől már majdnem minden, a pénzügyi szektort vizsgáló jelentés a kibertámadások veszélyét emeli ki. Jerome Powell, az Amerikai Egyesült Államok központi bankjának szerepét betöltő Federal Reserve elnöke, egy beszédében arra hívta fel a figyelmet, hogy a kiberfenyegetések már nagyobb veszélyt jelentenek az Egyesült Államok gazdaságára, mint a 2008-as, egész világot érintő gazdasági válság [2].

Az épített környezetünket, infrastruktúránkat, az alapvető szolgáltatásokat fenyegető emberi tényezők közé bekerült a magán és állami infrastruktúrát egyaránt veszélyeztető terrorizmus mellé a kiberbűnözés, mint hangsúlyos tényező [3]. 2020-ban az Egyesült Államok kongresszusa a 2001. szeptember 11-i eseményekkel emelte azonos szintre a kiberfenyegetések által jelentett veszélyt. Ugyanez a jelentés azonban arra is figyelmeztetett, hogy az ország nem készült fel ezekre a támadásokra [4].

A számítógépes rendszerekbe való erőszakos behatolás már majdnem minden országban bűncselekmény. Mára már közhelynek számít, de az informatika és az Internet fejlődésével megszűntek a földrajzi korlátok. Ez természetesen igaz a hackertámadásokra is, azok sem maradnak országhatáron belül. Az ilyen támadások felderítésében komoly nehézség a hatóságok tevékenységének összehangolása, hiszen a támadó az egyik ország joghatósága alá tartozik, míg a megtámadott esetében más állam az illetékes. A támadások felderítése akkor válik (szinte) lehetetlenné, ha a támadó mögött az adott ország kormánya áll. A

kormányzati inspirációra elkövetett cselekmények tetteseit így, ha megtalálják, akkor sem vonják felelősségre [5]. A pénzintézetek gazdaságban betöltött szerepüknél fogva emiatt sokszor kormányzatilag szervezett behatolások célpontjaivá válnak [6].

Az Európai Unió Kiberbiztonsági Ügynöksége (ENISA) évről évre elemzi a kiberfenyegetéseket. A vizsgálatuk mind az európai, mind pedig a globális folyamatokra is kiterjed. Az ENISA legutolsó, 2024-es riportja kiemelte, hogy 2023. július – 2024. június között a kibertámadások száma jelentősen megnőtt. Mind az incidensek sokfélesége, azok száma mind pedig azok következménye „rekordszintre" emelkedett. A folyamatban lévő regionális szintű konfliktusok továbbra is meghatározóak maradtak. A „hacktivizmus" jelensége folyamatosan terjed, számos új csoport jelent meg ezen a területen. A riport kiemeli, hogy a nemzeti vagy európai szinten zajló jelentős események adtak motivációt a megnövekedett „hacktivista" tevékenységhez a vizsgált időszakban (pl. európai választások) [7]. Az ENISA jelentés kiemelte, hogy a kiberincidensek egyre inkább a létfontosságú ágazatokat érintik.

Az ENISA riport hét fő fenyegetést azonosított, ezek közül a három legfontosabb a rendelkezésre állás elleni fenyegetés, ezt követte a zsarolóvírusok és az adatok elleni fenyegetés.

2023. július és 2024. júniusi időszakban a támadások által leginkább érintett ágazatok:

1. Közigazgatás (19%)
2. Közlekedés (11%)
3. Banki/pénzügyi ágazat (9%)
4. Üzleti szolgáltatások (8%)
5. Digitális infrastruktúra (8%)
6. Lakosság (8%)
7. Gyártás (6%)
8. Média (5%)
9. Egészségügy (4%)

Forrás: Európai Parlament [8]

PÉNZÜGYI SZEKTOR, MINT KRITIKUS INFRATRUKTÚRA

A kibertámadások fő motivációi a pénzügyi haszonszerzés, a kémkedés, a rombolás és az ideológiai okok voltak [9]. A pénzügyi szektor pont a korábbiakban említettek gazdaságban betöltött szerepe miatt kerül sokszor a támadások kereszttüzébe.

A pénzügyi rendszerek a gazdaságban betöltött szerepük miatt nemcsak a szó átvitt, de tisztán jogi értelmében is kritikus infrastruktúrák. 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény egyértelműen nevesíti azokat az úgynevezett létfontosságú rendszerelemeket, amely ágazatokba tartozó szolgáltatások elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához. A törvény alapján az „1. mellékletben meghatározott ágazatok valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához." A listán belül kiemelt az egészségügy, a lakosság személy- és vagyonbiztonsági

sága, a gazdasági és szociális közszolgáltatások biztosítása, az ország honvédelme. A jogszabály szövege szerint „ezek kiesése a feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna".

2012. évi CLXVI. törvény 1. sz melléklete kifejezetten nevesíti: „20. Pénzügy pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei 21. bank- és hitelintézeti biztonság 22. készpénzellátás".

Az előzőek alapján a pénzintézetek kritikus infrastruktúrának számítanak. A pénzintézetek átfogó szabályozása emiatt elengedhetetlen. Néha azonban nehéz megtalálni a szabályozás megfelelő mértékét. Szubjektív tapasztalat, hogy amit a pénzintézetektől elvár a szabályozó, például tájékoztatás vagy adatvédelem tekintetében, ugyanazt már nem követeli meg minden szolgáltatótól, például távközlési cégektől.

Bármely pénzintézetet, annak rendszereit érintő kibertámadásnak lehet:

- gazdasági hatása: mert a banki és pénzügyi termékek és szolgáltatások működését érintheti.
- társadalmi hatása: áttételesen a köznyugalmat is megzavarhatja egy bankot érintő kibertámadás – Postabank-pánikhoz hasonló hatása is lehet annak, ha az ügyfelek azt gondolják, hogy nem tudnak hozzáférni a bankban „tárolt" pénzükhöz, mert egy bank rendszere „megsérült" vagy a bank rendszerét „feltörték".
- politikai hatása: áttételesen az állam és intézményei iránti közbizalmat is érintheti, amennyiben egy bankot érintő kibertámadás az adott bank teljes működését is veszélyeztetheti vagy a közvélekedés azt feltételezi, hogy a teljes működést veszélyeztetheti. Az ezáltal kiváltott pánik már a közbizalmat is érintheti.

A pénzintézetek által biztosított pénzügyi műveletek lényegében a reálgazdaság véráramát jelentik. A pénzintézeteket érő kibertámadások így nemcsak a pénz absztrakt áramlását, hanem a mögöttük meghúzódó valós gazdasági tevékenységeket is veszélyeztetik. Az egyébként adatcserére használt kommunikációs hálózaton, fertőzési csatornákon tovaterjedő támadások rendszerszintű problémákat eredményezhetnek. A problémák pedig az ügyfelek bizalmát ingathatják meg. Mivel a pénzügyi szakma alapja a bizalom, a bizalom megingása az adott szolgáltatókon túl mások számára is károkat okozhat. Egy, a bankszektor, vagy más pénzügyi intézmények elleni, összehangolt módon elvégzett kibertámadással akár globális likviditási krízis is okozható [10].

Van azonban egy (al)szektor, ahol sérülnek a pénzügyi rendszerekkel kapcsolatos szigorú szabályozói elvárások. A szabályozás kettős mércéjét mutatja az új típusú digitális, vagy neobankok helyzete. A szereplők sokszor ugyanazokon a piacokon működnek, ugyanazokat a szolgáltatásokat nyújtják, mint a hagyományos vagy divatos szóval „kőbankok". A neobankokra vagy fintech cégekre vonatkozó szabályozás azonban sokkal megengedőbb, mint a „klasszikus" pénzintézetekre vonatkozó. Nincsenek olyan szigorú szabályok, a működésük kevésbé átvilágított, nincsen masszív tőkekövetelmény vagy céltartalékolási elvárás, nem történik meg a rendszerek folyamatos auditja stb. Ez az, ami miatt sokszor rugalmas(abb) szolgálatást tudnak nyújtani. Egy fintech cég csődje esetén azonban hiábavaló lenne a helyi jegybanktól vagy betétbiztosítótól ugyanazt a helytállást elvárni. Ezen cégek esetében nincs szigorú szabályozás, ugyanakkor csőd esetén állami szerepvállalás sem.

Bár egy nagyon fontos iparágról beszélünk, de tekintettel a téma mélységére, jelen vizsgálatnak nem képezi tárgyát a fintech cégek speciális szabályozása.

KIBERTÁMADÁSOK A PÉNZÜGYI SZEKTORBAN

A kibertámadások fejlődéstörténetét egy korábbi cikkben bemutattuk [11]. A pénzügyi intézmények tekintetében általánosságban elmondhatjuk, hogy a „nagyüzemi", nem igazán válogatós vírus- (féreg) támadások mellett, a célzott, egyedi felhasználókra irányuló offenzívák is megjelentek. Közvetlen támadási célok lehetnek (i) az online vagy offline identitáslopás, (ii) személyes és üzleti adatok ellopása, (iii) bankkártyák és bankszámlák adatainak eltulajdonítása, (iv) illetéktelen behatolás az online felhasználói fiókokba. Bár a fentiek is komoly károkat okoznak, nem ritkák már azok a súlyosabb támadások sem, amelyek célja maga a pénzügyi rendszer megbénítása.

A sok millió dolláros/eurós anyagi veszteség mellett a kibertámadások egyéb károkat is okozhatnak. Legfontosabb talán az ügyfél bizalmának ideiglenes, vagy végleges elvesztése. A különböző technikákkal kivitelezett támadások mára már minden naposakká váltak, ezért a megfelelő színvonalú védelmi intézkedések mellett a vállalat minden dolgozójának éberségére szükség van. A professzionális szinten kivitelezett támadások szükségessé teszik az érintettek közötti együttműködés javítását. A várható haszon nagysága miatt megéri, hogy a pénzintézetek elleni támadásokhoz komoly, időigényes előkészületeket tegyenek [12]. A következőkben a kibertámadások átalakulását fogjuk vizsgálni.

PÉNZINTÉZETEKET ÉRINTŐ TÁMADÁSOK JELLEMZŐI

Az elmúlt években a pénzügyi szektort érintő kibertámadások olyan mértéket öltöttek, hogy 2024-ben elkészült az első, kifejezetten a pénzügyi szektort vizsgáló ENISA riport is [13]. A riport egyik legfontosabb megállapítása egybecseng a mi korábbi, 2022-es vizsgálatunkkal. A pénzügyi ágazat továbbra is a kiberfenyegetések egyik legfontosabb célpontja marad mivel:

- az intézményekben tárolt (pénzügyi) adatok érzékenyek, nagy értékűek és
- azok ellopásával a támadók jelentős pénzügyi haszonra tehetnek szert.

ENISA 2023. július és 2024. júniusi időszakban 488 nyilvánosan bejelentett, az európai pénzügyi szektort érintő incidenst elemzett. Az ezekből készült riport fő megállapításai az alábbiak [13]:

- Az európai bankok voltak a támadások leggyakoribb célpontjai – 46 %-os arányban. Ezt követik a kormányzati ügynökségek és a pénzügyi szektorban működő közszférabeli szervezetek (13 %). A magánszemélyeket (10 %) pénzügyi jellegű *social engineering* kampányokkal csapták be.
- A pénzügyi szektorban a terheléses, DDoS-tevékenységek a geopolitikai eseményekhez, különösen Oroszország ukrajnai inváziójához kapcsolódtak. A hacktivisták gyakran európai hitelintézeteket (58%) és a kormányzati, pénzügyekkel kapcsolatos weboldalakat (21%) támadták. Céljuk, hogy működési zavart okozzanak és aggodalmat keltsenek a lakosság körében a kiberbiztonsággal, kiberrezilienciával kapcsolatban.

- Kiberincidensek – például csalás, zsarolóvírusok vagy adatvédelmi incidensek – következtében a pénzintézetek gyakran szenvedtek jelentős veszteségeket. Ezeket a veszteségeket tovább növelték a helyreállítással kapcsolatos költségek, a jogi költségek és a hatósági büntetések.
    - Az adatszivárgás továbbra is kritikus kérdés maradt. A támadók pénzügyi haszonszerzés céljából csalás, ellátási láncot érintő támadások (*supply chain attack*) vagy *social engineering* révén használták ki a kritikus sebezhetőségeket. A vizsgált esetek 39 százalékában az európai hitelintézetek voltak az elsődleges célpontjai azon támadásoknak amikor az incidensek effektív pénzügyi veszteségekhez, a szabályozó hatóságok által kiszabott büntetésekhez és „hírnévkárosodáshoz" (*reputational damage*) vezettek.
    - A kiberbűnözők a *social engineering* módszereket alkalmazták legsűrűbben. Az adathalászat (*phishing*), a sms-adathalászat (*smishing*) és a hanglapú adathalászat (*vishing*) voltak a legelterjedtebbek a vizsgált időszakban. Ezen incidensek célja érzékeny információk ellopása és ezeken keresztül pénzügyi csalások elkövetése volt. Az érintettek 38 százaléka magánszemély, 36 százaléka hitelintézet.
    - A csalások az összes incidens 6 százalékát tették ki, elsősorban magánszemélyeket (40 %) és hitelintézeteket (35 %) érintve. Bár a bejelentett esetek száma alacsonynak tűnik, a riport feltételezése, hogy nem került minden incidens lejelentésre. Az egyéb kibertámadásokból eredő másodlagos következmények szélesebb körű problémára utalnak. A kriptovalutákkal kapcsolatos incidensek esetében a lopások, csalások és a pénzmosás száma szintén jelentős mértékben nőtt.
    - A zsarolóvírus támadások elsősorban a kevésbé fejlett pénzügyi szervezeteket, például a szolgáltatókat (29 %) és a biztosítókat (17 %) célozták. A végeredmény: pénzügyi veszteség (38 %), adatszivárgás (35 %) és működési zavarok (20 %).
- A mobiltelefonokat érintő támadások darabszáma és komplexitása tovább emelkedett. A támadó programok egyre kifinomultabbak. A trójai banki programok és a kémprogramok növekvő fenyegetést jelentettek. Segítségükkel a hackerek át tudták venni az uralmat az eszközök felett, képessé váltak az ügyfél nevében tranzakciók végrehajtására. A hitelintézetek (36 %) és a magánszemélyek (24 %) voltak a leginkább érintettek ezekben a támadási típusokban.
- A beszállítói láncot érintő támadások, főként az adatlopás és a zsarolóvírusok, az érzékeny adatok eltulajdonítását és értékesítését (63 %), működési zavarokat (26 %) és pénzügyi veszteséget (11 %) eredményeztek.

TÁMADÁSOK JÖVŐKÉPE, JAVASLATOK

Ahhoz, hogy a pénzintézetek hosszútávú védelmi stratégiát tudjanak kialakítani nem kell feltétlenül üveggömb. Igaz, hogy a gyorsan változó világ, még gyorsabban változó szegmenséről beszélünk, de nagyon sok támadási vektor már évek óta jelen van. Szeretnénk azt hinni, hogy „személyre szabott" támadás áldozatai vagyunk. De sajnos a legtöbbször

még mindig a régi „trükkök" működnek a legjobban, a régi hiányosságokat használják ki a támadók. Ez várhatóan a jövőben is így fog maradni.

Jelszókezelés

Továbbra is azt tapasztaljuk, hogy bár a felhasználók valódiságának ellenőrzésekor már sokszor többlépcsős azonosítást alkalmaznak a bankok, még mindig vannak hiányosságok. A jelszóhasználatban, a lehetséges jelszó erősségben még van hova fejlődni. Hiába szigorodnak a jelszóházirendek, az évről évre megjelenő „leggyakrabban használt jelszavak listája" továbbra is komoly hiányosságokat mutat. Továbbra is letaszíthatatlan a trónról az '123456' [14]. A nem megfelelő jelszóházirendeknek van pénzintézeti oldala – nem szabad engedni a túl gyenge jelszavak használatát –, de az egyének személyes felelőssége nem elvitatható.

Talán ez az egyik olyan információ biztonsági terület, ahol bár nagy a lemaradás, a leggyorsabban lehetne eredményeket elérni. Azonban, ami ritkán képezi a felhasználói edukáció részét, az a személyes és a munkahelyi rendszerekben használt jelszavak szétválasztása. Hiába talál ki egy erős céges jelszót a felhasználó, ha utána ugyanazt használja az otthoni infrastruktúrában is. Előfordul, hogy a jól megjegyzett bonyolult jelszót adja meg a felhasználó az összes felhasználási területen – így a véletlenül felkeresett adathalász oldalakon is.

Hamis oldalak

Az adathalászaton belül, a hamis banki oldalak elterjedtsége még mindig magas. Ezt a folyamatot támogatja a kártékony hirdetések és a keresőoptimalizálás-mérgezés (*malvertising* és a *SEO poisoning*). A bűnözők a keresőoptimalizálással, a keresési listák élére kerülő hamis oldalak segítségével lopják el a banki adatokat. A folyamatra egy aktuális példa az elmúlt időszakban végbement hazai bankegyesülés. Az egyesülés után új névvel, új entitás született. Az új bank weblapját, netbankját stb. a jogelőd pénzintézetek ügyfelei még nem ismerték. Az új netbanki oldalt sokan keresőalkalmazások segítségével próbálták megtalálni. A keresési listák élén azonban egy hamis weboldal szerepelt. Az igazira kísértetiesen hasonló oldalon az azonosító, majd a jelszó megadása után a bűnözőknek már könnyű dolga volt. A jelszavakkal végre tudták hajtani a szükséges változtatásokat és hozzáfértek az ügyfelek pénzéhez [15].

Informatikai támogatás

A hazai és a nemzetközi pénzintézetek robosztus informatikai rendszereken futnak, az alap-, számlavezető-rendszerek (*core* rendszerek) azonban általában régiek. Azok cseréje szinte lehetetlen a bonyolultság, az évek során végrehajtott sok apró változtatás – kivételkezelések például –, az üzletmenet folytonosság fenntartása miatt. A régi programnyelvek, összetett architektúra, bonyolult szabályrendszerek, redundáns folyamatok miatt a modernizálás, *upgrade*-elés szinte lehetetlen, de mindenesetre nagyon költséges.

Új technológiák térnyerése

A pénzügyi szervezetek számára elkerülhetetlen, hogy fejlett(ebb) fenyegetésérzékelő rendszereket építsenek ki. Az olyan új generációs eszközök, mint a behatolásérzékelő-, a behatolásmegelőző rendszerek és a biztonsági információ- és eseménykezelő megoldások képesek lehetnek észlelni az anomáliákat és valós időben reagálni azokra. A mestersé-

ges intelligencia és a gépi tanulás integrálása az előre jelző, elemző és az automatizált védekező rendszerekbe fokozza a kiberrezilienciát. Nem szabad viszont megfeledkezni arról, hogy már a támadók is a mesterséges intelligenciát hívják segítségül.

A következő jelentős kihívást a kvantumszámítógépek fogják jelenteni. A jelenleg működő titkosítási protokollokat teljes mértékben felboríthatják ezek a nagyteljesítményű számítógépek. A kvantumszámítógépek számítási kapacitás, sebessége milliárdszorosa a hagyományos számítógépeknek. Néhány évtizeden (?) belül a ma még „feltörhetetlen" titkosítási algoritmusok néhány perc alatt feltörhetővé válnak. Ráadásul ezek az eszközök nem csak a későbbi titkosításokat fogják ostromolni, hanem a már lemásolt, ma még védett rendszereket, adatokat fogják a jövőben feltörni. Hiába titkosítottunk ma egy adatot. Ez ma még lehet, hogy használhatatlan a tolvajoknak. De lehet, hogy a jövőben már fel fogják tudni törni az ellopott adatokat az új számítógépek segítségével.

Szolgáltatásként nyújtott támadások

A kiberbűnözés, ha egy több dimenziós döntési mátrixban figyelembe vesszük a költségeket – a megtérülést – a lebukás kockázatát, jó „alternatívát" jelent a bűnözőknek. Régen talán szempont volt, hogy a megfelelő tudás rendelkezésre álljon. Mostanra azonban már egy teljes specializált hálózat épült fel kiberbűnözési-szolgáltatások nyújtására. Ezen szolgáltatások a legális piacok üzleti modelljeit másolják. Szolgáltatásként nyújtott zsarolóvírusok és kártevők (*Ransomware-as-a Service* – RaaS, *Malware-as-a-Service* – MaaS) már viszonylag alacsony összegekért – havi 100-200 dollárért – már elérhetőek az internet sötét bugyraiban, a *Dark Weben* [16].

Bűnözői ellátási lánc

A kiberbűnözési szektorban is megtörtént a specializáció. A különböző lépéseket, már különböző aktorok hajtják végre. Nem ugyanaz a támadó szerzi meg az adatokat, mint aki a végén fel is fogja használni azokat. Lehet, hogy egy hacker célzott támadását megelőzően, egy másik hacker, aki csak figyeli, gyűjti és elemzi az adatokat már hónapok óta a feltört rendszerben „ül". Ezutóbbi alapján egy feltört vállalati jelszó, nem csupán egy fiók kompromittálódását jelenti. Lehet, hogy oldalirányú mozgással a teljes vállalati infrastruktúra, vagy akár több összekapcsolt vállalat megtörését is eredményezi. A támadók gyorsabban mozognak, mint valaha. A CrowdStrike jelentése szerint az átlagos „kitörési idő" – az időablak, mielőtt a támadók megkezdik az oldalirányú mozgást – 2024-ben az előző évi 62 percről mindössze 48 percre csökkent, a leggyorsabb megfigyelt idő pedig 51 másodperc volt. Ezutóbbi azt jelenti, hogy a „védőknek" kevesebb mint egy percük lehet a felderítésre és reagálásra, mielőtt a támadók még mélyebbre hatolnának a vállalati rendszerben. A generatív mesterséges intelligencia kulcsszerepet játszott a folyamat gyorsulásában [17].

A Verizon DBIR riportja szerint az adattolvaj naplók, feketepiacokon közzétett bejegyzések és a zsarolóvírus-áldozatok *domain* neveinek korrelációja azt mutatja, hogy az áldozatok 54 százalékánál már korábban megjelentek hitelesítő adatok a *Dark Weben*. Az áldozatok 40 százalékánál a vállalati e-mail címek voltak a kompromittált hitelesítő adatok [18].

Sajnos mind az *as-a-Service* szolgáltatások, mind pedig a bűnözői ellátási lánc kialakulása nagyon megnehezíti a védelmi szektor működését. Tény, hogy ezekre a folyamatokra is van már védelmi szolgáltatás. A kiszivárgott belépési adatokat, jelszavakat monitorozzák a *Dark Weben* – ha találnak céges adatokat, az előrejelez(het) egy jövőbeni támadást.

Amennyiben azonban mégis megtörténik a baj, elkezdődik a védekezés, majd azt követően a visszaállítás, akkor újabb problémával szembesülhetünk. Mivel a törés és a támadás időben, térben nagyon elválhat egymástól nagyon nagy odafigyelést igényel amikor egy támadás után megpróbáljuk visszaállítani a rendszereinket. Ne forduljon elő, hogy a még mindig fertőzött biztonsági mentésekre térünk vissza.

Szabályozás

Az olyan szabályozási keretek, mint a GDPR, a NIS-irányelv és a pénzügyi szereplőkre vonatkozó DORA betartása kulcsfontosságú a kiberbiztonsági ellenálló képesség fenntartásához. Ezek a jogszabályok szigorú elvárásokat támasztanak a pénzintézetek szabályzataival, eljárásaival kapcsolatban. A jogszabályoknak való megfelelés érdekében rendszeres megfelelési ellenőrzéseket, auditokat kell végezni(ük) [13]. A korábbi évek tapasztalata azt mutatja, hogy a szabályozás szigorodása szükséges rossz. Újabb fejlesztési költségek önkéntes vállalása, vagy akár a hamis banki oldalakkal kapcsolatos védekezésben az aktívabb pénzintézeti részvétel nem lenne kikényszeríthető szigorú törvényi előírások nélkül. Amit nem ír elő jogszabály, azt az ügyfelek nem fogják tudni kikényszeríteni.

Egy pénzintézet ritkán tud azzal ügyfelet nyerni, hogy ő a legbiztonságosabb. Az is igaz, hogy azzal már rengeteget tud veszíteni, ha kiderül, hogy nem-biztonságos. Ugyanakkor fontos kiemelni, hogy nehéz meghatározni hol húzódik az egyén felelőssége és hol kell a pénzintézetnek szerepet vállalnia – esetleg anyagilag is helytállnia. Például a korábban említett hamis banki oldal esetében az egyén felelőssége elvitathatatlan. Ugyanakkor vannak olyan vélemények is, amelyek szerint a pénzintézet nem tett meg mindent, hogy eltűnjön a hamis oldal, illetve nem tájékoztatta megfelelően az ügyfeleit.

Képzés, oktatás

Nem győzzük hangsúlyozni az egyének, pénzintézeti dolgozók, felhasználók stb. oktatásának fontosságát. „Az ember a leggyengébb láncszem”. Az alkalmazottak képzése, tudatosságnövelő programok alapvető fontosságúak, például a *social engineering* támadások kockázatának csökkentéséhez. A pénzintézetek (vagy általánosságban a vállalatok) folyamatos kiberbiztonsági képzésekkel, szimulált adathalász gyakorlatokkal tudják a kibertudatosságot növelni. Hogy egy előremutató példát is bemutassunk. Nagyon jó kezdeményezés például a KiberPajzs - https://kiberpajzs.hu/.

BCP - DRP

Az incidensekre való felkészülés egyik része annak kidolgozása, hogy mit tegyünk, ha már megtörtént a baj. Az incidensekre reagáló működés folytonossági vagy üzletmenet helyreállítási programok, reagálási tervek, jó esetben kommunikációs *roadmap* készítése nagyon fontos. A pénzintézeteknek jól meghatározott incidens tervekkel kell rendelkezniük. Ezek a tervek részletesen kell, hogy meghatározzák a kibertámadás során, majd azt követően a végrehajtandó lépéseket. Ezeket a terveket rendszeresen frissíteni és tesztelni kell. A hatékony tervek pontos intézkedéseket tartalmaznak a kiberincidensek észlelésére, megfékezésére, felszámolására, helyreállítására és a kommunikációjára vonatkozóan [13]. A tervek létrehozása nem önkéntes alapú, azokat a jogszabályok (NIS2, DORA) is előírják.

Fontos kiemelnünk, hogy az utolsó pontok esetében nem elégséges az adott pénzintézet keretein belül maradni. Az oktatásokat, jogszabályi előírásokat vagy akár a helyreállítási terveket ki kell terjeszteni a pénzügyi intézményekkel szimbiózisban, velük „összenőve" működő vállalatokra, harmadik felekre is – *supply-chain security*.

Együttműködés és információmegosztás

A pénzügyi intézmények közötti együttműködés és információmegosztás növeli az általános kiberellenálló-képességet. Például az iparági fórumokon való részvétel, a fenyegetésekkel kapcsolatos információk megosztása és a köz- és magánszféra közötti partnerségek (*Public Private Partnership*) segítenek az intézményeknek naprakésznek maradni a felmerülő fenyegetésekkel és a „legjobb gyakorlatokkal" kapcsolatban [13].

ÖSSZEFOGLALÁS

Összefoglalóan elmondhatjuk, hogy a kibertámadások jelentős veszélyt jelentenek nemcsak gazdasági, hanem társadalmi és politikai szempontból is. A támadások célpontjai között kiemelt helyen szerepel a pénzügyi szektor, amely jogilag is kritikus infrastruktúrának minősül. A kibertámadások célja lehet az adatlopás, de súlyosabb rendszerleállás vagy akár rendszerszintű pusztítás is.

A legtöbb ország kiemelten kezeli ezeket a fenyegetéseket, mivel kihathatnak a társadalmi stabilitásra és a demokráciára is. Azonban a határokon átnyúló támadások felderítése továbbra is nehéz, különösen, ha állami szereplők állnak mögöttük.

A pénzintézetek továbbra is gyakori célpontok pénzügyi értékük, érzékeny adatállományuk miatt. A bizalomvesztés, a működési zavarok és a likviditási problémák rendszerszintű gazdasági válságokat is okozhatnak. A fő támadási formák továbbra is DDoS, adathalászat, *social engineering*, és zsarolóvírusok. Növekedik azonban a mobilos trójai, valamint ellátási lánc támadások száma. A politikai eseményekhez „kapcsolódóan" pedig a hacktivista támadások intenzitása emelkedett.

Régi IT-rendszerek és elavult programnyelvek lassítják a védekezés modernizálását. A jelszóhasználattal kapcsolatos hiányosságok, a hamis banki oldalak továbbra is nagy problémát jelentenek. Bemutattuk, hogy a kiberbűnözés már szolgáltatásként működik (RaaS, MaaS), valamint kialakultak bűnözői „ellátási láncok" is.

A támadók gyorsabbak és szervezettebbek, sokszor már mesterséges intelligenciát használnak. Várhatóan a jövő egyik legnagyobb fenyegetése a kvantumszámítógépek elterjedése lesz, mert ezek képesek lesznek a mai titkosítási módszerek feltörésére.

Szabályozási környezettel kapcsolatban megállapítottuk, hogy a GDPR, a NIS vagy a DORA-irányelvek betartása nagyon fontos a pénzügyi szektor ellenálló képességének biztosításához A szabályozás célja, hogy a pénzügyi rendszer szereplői megfelelő védelmet és reagálási képességet építsenek ki a kibertámadásokkal szemben.

FELHASZNÁLT IRODALOM

[1] „Európai Parlament," 12 10 2021. [Online]. Available: https://www.europarl.europa.eu/topics/hu/article/20211008STO14521/miert-fontos-a-kiberbiztonsag-es-mibe-kerulhet-egy-kibertamadas-az-erintettnek. [Hozzáférés dátuma: 05 07 2025].

[2] J. Clay, „Trend Micro, Security News - April 16, 2021," 16 04 2021. [Online]. Available: https://www.trendmicro.com/en_hk/research/21/d/this-week-in-security-news-april-16-21.html. [Hozzáférés dátuma: 02 07 2025].
[3] N. R. Somogyi Tamás, „Kiberbiztonsági kihívások és megoldások a hazai pénzügyágazat járványhelyzet alatti szabályozási környezetének változása alapján," Biztonságtudományi Szemle, pp. 107-118, 2025. VII. évf. 1. szám.
[4] D. E. S. Julian E. Barnes, „Congress, Warning of Cybersecurity Vulnerabilities, Recommends Overhaul," 11 03 2020. [Online]. Available: https://www.nytimes.com/2020/03/11/us/politics/congress-cyber-solarium.html. [Hozzáférés dátuma: 02 07 2025].
[5] D. H. G. K. Oliver GULYAS, „Impact of cyber-attacks on the financial institutions," CENTERIS – International Conference on ENTERprise Information Systems, Procedia Computer Science Vol. , pp. 84-90, 2022.
[6] L. Evans, Cybersecurity: An Essential Guide to Computer and Cyber Security for Beginners, Including Ethical Hacking, Risk Assessment, Social En, New York: Bravex Publications, 2020.
[7] European Union Agency for Cybersecurity, „ENISA Threat Landscape 2024," July 2023 to June 2024, p. 4, 09 2024.
[8] „Európai Parlament," 27 01 2022. [Online]. Available: https://www.europarl.europa.eu/topics/hu/article/20220120STO21428/kiberbiztonsag-fo-es-ujonnan-felmerulo-fenyegetesek. [Hozzáférés dátuma: 02 07 2025].
[9] European Union Agency for Cybersecurity, „ENISA Threat Landscape 2024," July 2023 to June 2024, p. 4, 09 2024.
[10] Nemzeti Kibervédelmi Intézet, „A bankszektoron keresztül globális krízist okozhatnak a kibertámadások," Nemzeti Kibervédelmi Intézet, 11 02 2020. [Online]. Available: https://nki.gov.hu/it-biztonsag/hirek/a-bankszektoron-keresztul-globalis-krizist-okozhatnak-a-kibertamadasok/. [Hozzáférés dátuma: 02 07 2025].
[11] G. Olivér, „A kiberbiztonság és a banki kibervédelem fejlődése," Biztonságtudományi Szemle, %1. kötet2022. IV. évf. 2. szám, pp. 1-13, 2022.
[12] BaFin - Bundesamt für Sicherheit in der Informationstechnik, BaFin Perspektiven, Berlin: Bundesamt für Sicherheit in der Informationstechnik, 2020.
[13] I. L. R. N. A. M. Marianthi Theocharidou, „ENISA Threat Landscape: Finance Sector," European Union Agency for Cybersecurity, 2024.
[14] NordPass, „Top 200 Most Common Paswwords," [Online]. Available: https://nordpass.com/most-common-passwords-list/. [Hozzáférés dátuma: 05 07 2025].
[15] T. S. Zsuzsanna, „24.hu," 23 05 2025. [Online]. Available: https://24.hu/fn/gazdasag/2025/05/23/dobbenetes-banki-csalasok-mbh-mobilapp-netbank-sms-kod-eszrevetlen-tranzakciok/. [Hozzáférés dátuma: 04 07 2025].
[16] F. Ferenc, „CyberThreat Report," 19 06 2025. [Online]. Available: https://www.cyberthreat.report/p/milliardnyi-kiszivargott-hitelesito. [Hozzáférés dátuma: 04 07 2025].
[17] CrowdStrike, „2025 Global Threat Report," 2025.
[18] Verizon DBIR Team: C. David Hylender, Philippe Langlois, Alex Pinto, Suzanne Widup, „2025 Data Breach Investigations Report," Verizon Business, 2025.