Pajzs és iránytű két világ közt – ahol a pénzügyi racionalitás találkozik a kibertér fenyegetéseivel

Pintér Éva[1]
DOI: https://doi.org/10.35551/PFQ_2026_1_7

Terták Elemér és Kovács Levente: Kiberbiztonság – kibertér

Az elmúlt években több tucat konferencián, workshopon és zárt szakmai egyeztetésen vettem részt, ahol banki és vállalati vezetőkkel beszélgetve újra és újra ugyanaz a mondat hangzott el: *„A kiberbiztonság már nem IT-kérdés, hanem vezetői szintű stratégiai kockázat."* Legyen szó egy nagybank digitális transzformációjáért felelős vezérigazgató-helyetteséről, egy középvállalkozás CIO-járól, vagy egy pénzügyi infrastruktúrát üzemeltető cég kockázatkezelési vezetőjéről – mindenhol ugyanaz a feszültség és felismerés érződött.

Ahogy egy tavaly őszi panelbeszélgetés után fogalmazott egy bank biztonsági igazgatója: *„Ma már nem az a kérdés, hogy erős-e a pajzsunk, hanem az, hogy észrevesszük-e időben, ha valaki megkerüli."* Ez a mondat azóta is eszembe jut, mert pontosan összefoglalja azt a mentalitásváltást, amelyen a pénzügyi és vállalati szektor nap mint nap keresztülmegy. A kibertér fenyegetései ugyanis ma már nem technikailag távoli, elvont jelenségek. A felsővezetői döntések legszűkebb terében vannak jelen, és a pénzügyi stabilitás egyik legfontosabb tényezőjévé váltak. Tehát ma már nem az a kérdés, hogy megtámadnak-e minket a kibertérben, hanem az, hogy mikor vesszük észre.

Ezek az élmények jutottak eszembe akkor is, amikor Terták Elemér és Kovács Levente *Kiberbiztonság – kibertér* című kötetét a kezembe vettem. A könyv pontosan azt a világot írja le, amely ezeknek a találkozóknak a háttérrezgését adja: azt a valóságot, amelyben bankok, vállalkozások, szolgáltatók és szabályozók ugyanannak a láthatatlan, de minden korábbinál összetettebb kockázati térnek a szereplői.

1 Pintér Éva PhD habil, Budapesti Corvinus Egyetem, Vállalkozás és Innováció Intézet, egyetemi docens **eva.pinter@uni-corvinus.hu** https://orcid.org/0000-0003-0149-8421

A szerzők által felvázolt helyzetkép és a gyakorlati tapasztalatok sok ponton összeérnek. A konferenciákon hallott esettanulmányok, a vezetői félelmek és dilemmák, a taktikai és stratégiai viták mind visszaköszönnek a könyv lapjairól – csak rendszerezettebben, átgondoltabban és szakmailag egységes keretbe rendezve. Ezért vált a kötet olvasása számomra nem csupán szakmai élménnyé, hanem egyfajta értelmezési kapaszkodóvá is: segít megérteni azt a kiberbiztonsági ökoszisztémát, amelyben ma Magyarországon és Európában minden pénzügyi szereplő működik.

Ebben a könyvismertetőben arra teszek kísérletet, hogy ezt a világot feltárjam: hogyan épül fel a szerzők gondolatrendszere, miként illeszkednek a kötet fejezetei egymáshoz, és hogyan rezonál mindez a nemzetközi kiberbiztonsági gyakorlatokkal és a hazai banki valósággal.

Az egyre növekvő kiberfenyegetés árnyékában a pénzügyi szektor szereplői új kihívásokkal néznek szembe. A kötet szerzői szerint a digitális pénzügyi szolgáltatások térhódítása párhuzamosan kiberbiztonsági „hadviselést" indukált: egy 2024-es ENISA-tanulmány szerint az európai pénzintézetek eseteinek 46%-át kiber incidensek tették ki. Ez rávilágít arra, hogy ma már bárki szenvedhet el veszteségeket nem csak a tőzsdén, hanem a számítógépes hálózatokon keresztül is.

A jelen kötet célja épp az, hogy a pénzügyi szakemberek és döntéshozók számára megalapozott összefüggésrendszert nyújtson. A szerzők, akik a magyar bankszektor és pénzügyi oktatás ismert alakjai, széles spektrumú elemzésben mutatják be a kibertér kihívásait és a védelem hazai lehetőségeit. A könyvismertetésünkben áttekintjük a kötet főbb fejezeteit, értékeljük annak lexikális mellékletét, és nemzetközi összevetésben vizsgáljuk a benne tárgyalt témákat.

A *Kiberbiztonság – kibertér* kilenc fő fejezetre tagolódik, amelyek egymásra épülnek, nem öncélúan elválasztva a témákat. Az első négy fejezet tényfeltáró jellegű: a kiberbűnözés történetétől és globális trendjeitől indul, majd a nemzetközi együttműködés, a jogi statisztikák, végül a kiberincidensek okozta pénzügyi károk részletes vizsgálata következik.

A bevezető a digitális ökoszisztéma vétlen szereplőjétől a profi kiberbűnözőig mutatja be, mit jelent a hatalmas adatmennyiség (Big Data) feldolgozása, a mesterséges intelligencia (MI), a gépi tanulás (ML), az adatbányászat és a prediktív elemzés technológiai forradalma. E technológiák egyidejűleg nyitnak meg új piacokat, teremtenek üzleti lehetőségeket, ám exponenciálisan növelik az informatikai rendszerek támadhatóságát is. A pénzügyi szektor számára ez azt jelenti, hogy az ügyfélszolgálat automatizálódása, a fizetési formák digitalizálódása, a transzkontinentális adatáramlások mindig kívülről támadhatóvá válnak. A bevezető kiemeli azt a paradoxont is, amely az utolsó évtizedet jellemzi: míg a pénzügyi intézmények biztonsági beruházásai évente akár 15-20%-kal nőnek, addig a sikeres támadások száma és hatékonysága még ennél is gyorsabban eszkalálódik. Ez nem a pénzügyi szektor hiányosságára, hanem a támadók gyorsuló szofisztikáltsága, és az ellátási láncok összefonódása miatt van. A bevezető tehát nem félelmetes, hanem reálisan értékelő bevezetés a fejezetek felé.

Az első fejezet a kiberbűnözés fejlődéstörténetéről rendkívül érdekes és tanulságos. A szerzők az első eset – az 1834-es francia Société Générale-ban elkövetett távközlési hálózati csalás – felderítésével kezdik. Ez azt mutatja, hogy a kiberbűnözés nem új jelenség, csak a formáit változtatta meg az idő és a technológia. A fejezet kronologikus fejlődésén végighaladva megismerkedhetünk az olyan történelmi fontosságú eseményekkel, mint a Creeper-vírus (1971), a Morris Worm (1988), az ILOVEYOU-vírus (2000), amelyek egykor az egész számítógépvezérelt világot megrendítették. Ezután következnek a felvásárlások, a kiszivárogtatások, az adathalászat kiterjesztése, az első nagyobb bankhackerek ügyei, és végül a 21. századi szofisztikált támadások: Stuxnet (2010), NotPetya (2017), WannaCry (2017), Petya (2017), CrowdStrike (2024). A nemzetközi szabályozási és technológiai válaszok sem maradhatnak el, az USA NIST keretrendszere, az EU GDPR-ja (2018), az ISO/IEC 27001 és 27005 standardok (2005-2022), valamint az FSB és az OECD ajánlásai. A fejezet rámutat, hogy minden fenyegetésre válaszként született egy erősebb szabályozás, de az összeegyezhetetlenség problémája – az eltérő jogi rendszerek, a geopolitikai ellentétek és a kiberbűnözés transznacionális volta – továbbra sem oldódott meg.

Magyar vonatkozásban pedig olvashatunk a hazai banki hackelés történelméről az elmúlt 10-15 évben, a Szegedi Egyetem 2012-es feltöréséről, a kormányzati rendszerek elleni támadásokról, majd az elmúlt 2-3 évben a Magyar Bankszövetség tagjait ért jelentősebb incidensekről (ügyfélcsalások, belső hálózatok feltörése). Ez a fejezet rendkívül hasznos „példatár" lehet, amely tanítja a szervezeti emlékezetet és a tanulságok beépülését egy szervezetbe.

A második fejezet a kiberbűnözést immár egy összetett ökoszisztémaként értelmezi. Rendszerbe foglalja a globális együttműködés kereteit a kiberbűnözés elleni harcban. Kiemelten foglalkozik a Budapesti Kiberbűnözés Elleni Egyezménnyel, annak globális kiterjedésével, valamint a különböző nemzetközi szervezetek (EU, ENSZ, NATO stb.) együttműködésével. A szerzők bemutatják az elektronikus bizonyítékszerzés nemzetközi kereteit és újításait, és részletezik az összehasonlító statisztikai terminológia bevezetésének (ICCS, azaz International Classification of Cybercrime Statistics) indokoltságát. Ennek kapcsán idézik, hogy az Európa Tanács világszerte több mint 90 országot tömörítő programirodája is támogatja a kiberbűnözés elleni küzdelmet. A fejezet végén egy átfogó táblázat mutatja be az EU jelenleg hatályos kiberbiztonsági jogszabályait és intézményrendszerét (ENISA rendelet, NIS/NIS2 irányelv, Európai kiberválság-hálózat stb.), jelezve, hogy a pénzintézeteknek ezeket az előírásokat is figyelembe kell venni.

A harmadik fejezet áttekinti a kiberbűnözés nemzetközi „mérőszámait". Érinti a globális kiberbűnözési rangsorokat, beleértve az ENSZ által gyűjtött adatok alapján a leginkább érintett államokat és földrészeket. Részletezi az Egyesült Államok, az EU és a volt Szovjetunió utódállamainak helyzetét. Teret kapnak az amerikai statisztikák – kiderül, hogy a vállalati szektor jelentős célponttá vált, s bár ott magasabb a védettségi szint, a panaszok és bejelentések szerint még mindig jelentős kár realizálódik. Végül a szerzők bemutatják a magyar

helyzetet: külföldi összehasonlításban Magyarország kiberbiztonsági mutatóit térképezik fel. Érdekes megjegyezni, hogy az NKI (Nemzeti Kibervédelmi Intézet) stratégiája szerint Magyarországon a vállalatok kiberérettsége jelenleg alacsony szintű, különösen a kkv-k körében, akiknél alacsonyabb a tudatos kiberbiztonsági szemlélet.

A negyedik fejezetben a kiberincidensek pénzügyi vetületét elemzik a szerzők. Kiszámolják az incidensek közvetlen és közvetett költségeit, részletezik a tőzsdei reakciókat és a hírnévvesztés hatásait. Szó esik a beszállítói lánc miatti rendszerszintű kockázatról és a késedelmes bejelentés költségeiről is. Végkövetkeztetésként fontos javaslatokat fogalmaznak meg, pl. az átlátható kárfelmérés és gyors bejelentés szabályozási ösztönzésére vonatkozóan. Mindehhez külföldi példákat is idéznek (például ipari szereplők kiberbiztosítási költségeit ismertetik) a nemzetközi szakirodalomból.

A mű második felében a megoldásorientált megközelítés dominál, a technológiai lehetőségek, az új irányelvek és módszerek bemutatására koncentrálnak a szerzők.

Az ötödik fejezet áttekinti a vállalati kibervédelemben alkalmazható új technológiákat és módszereket. A technológiai innováció szerepének vizsgálata a könyv egyik legösszetettebb, legelemzőbb része, amely azt vizsgálja, hogyan változtatja meg a digitális innováció a kiberbiztonság működését, kockázatait, védelmi lehetőségeit és döntési pontjait. A technológiai innováció kettős természetét mutatja be: egyrészt a digitalizáció és az olyan új megoldások, mint a mesterséges intelligencia, a big data-analitika vagy a felhőalapú szolgáltatások hatalmas hatékonyságnövelést tesznek lehetővé, másrészt azonban új sebezhetőségeket és kockázatokat is teremtenek a vállalati környezetben. A fejezet a pénzügyi szektor és a vállalati gyakorlat szemszögéből közelít, de megállapításai egyértelműen illeszkednek a nemzetközi kiberbiztonsági trendekhez is (CISA, ENISA, WEF), és részletesen bemutatja mindazt, ami a modern vállalatok kockázati térképét alakítja. Külön kiemelt blokként tárgyalja a NIS2 irányelv pénzügyi szektorra gyakorolt hatását, összevetve az ismertetett magyar banki helyzettel. Például a 2024-ben elfogadott NIS2 szigorúbb kockázatkezelést és vezetői felelősségvállalást ír elő. E fejezet részleteiben kitér a kockázatmérési módszerekre, azok korlátaira és értelmezési nehézségeire (pl. a kvantitatív mutatókkal való játék buktatóira). Fontos elem a kibertámadások tanulságainak levonása, ismertetésre kerül a tudatos biztonsági stratégia szükségessége, hangsúlyozva a védekezési rendszerek. A szerzők részletesen bemutatják a modern védekezési technológiákat, elsősorban a viselkedéselemzésre és gépi tanulásra épülő UEBA- és SIEM-rendszereket, amelyek képesek mintázatokat felismerni, kockázati pontszámokat generálni és azonosítani a gyanús viselkedést. A fejezet tárgyalja az oldalirányú mozgás jelenségét is, amely a kibertámadások egyik legkritikusabb eleme, mivel a támadók így tudnak több rendszeren át terjedni a hálózaton belül. Külön kitér a kiberbiztosítás szerepére, hangsúlyozva, hogy bár hasznos kiegészítés, nem helyettesítheti a megfelelő műszaki és szervezeti védekezést, és bizonyos kockázatokra – például bennfentes támadásokra – nem

is nyújt fedezetet. A fejezet egyik alapvető üzenete, hogy a technológiai innováció nemcsak technikai, hanem humán és szervezeti kérdés is, ezért a védekezésben legalább akkora szerepe van az emberi tényezőnek, mint a fejlett eszközöknek.

A hatodik fejezet a kiberfenyegetések rendszerezett, taxonómiai megközelítését mutatja be, amely elengedhetetlen a támadások azonosításához és a hatékony védekezés kialakításához. A szerzők hangsúlyozzák, hogy a kiberbűnözés gyorsan növekvő mértéke – különösen a pénzügyi visszaélések területén – jelentős gazdasági és bizalmi kockázatot jelent, ami indokolttá teszi a pontos kategorizálást. A fejezet bemutatja a különféle támadástípusokat, többek között a kliensoldali, szerveroldali vagy célzott, emberi közreműködésen alapuló támadásokat, valamint az ellátási láncokat és kritikus rendszereket érintő fenyegetéseket. A szerzők külön kitérnek a bennfentes fenyegetésekre és azok tipikus eseteire, amelyek gyakran rejtve maradnak, mégis súlyos következményekkel járhatnak. Összességében a fejezet azt hangsúlyozza, hogy a gyorsan változó, egyre összetettebb fenyegetési környezetben csak egy világos, többdimenziós rendszertan segítségével lehet megalapozott megelőzési és reagálási stratégiákat kialakítani.

A kiberbűnözés egyik veszélyes, gyorsan terjedő formáját, a szociális manipulációt mutatja be a hetedik fejezet, amely manipulációs forma a technikai támadások helyett az emberek óvatlanságát, hiszékenységét és érzelmi reakcióit használja ki. A szerzők hangsúlyozzák, hogy a kiberincidensek jelentős része nem technikai hiányosságokra, hanem emberi hibákra vezethető vissza, így a tudatos felhasználói magatartás kulcsfontosságú védelmi vonal. A kiberpszichológia területén bemutatja a social engineering technikákat – adathalászattól a „bálnavadászaton" át a mindentudó meggyőzésig –, majd ajánlásokat tesz a védekezésre, pl. rendszeres kockázattudatos-képzés, tesztelés, etikus hackerek bevonása. A szerzők kitérnek az ügyfélkezelés gyakorlatára is: leírják, hogyan kell a banki ügyintézőknek empatikusan, mégis professzionálisan támogatni az áldozatokat, és hogyan lehet visszaállítani a bizalmat. A fejezet fő üzenete, hogy a szociális manipuláció elleni védelem alapja a tudatosítás, a megfelelő kommunikáció, valamint az ügyfelek és a vállalati dolgozók széles körű oktatása.

A nyolcadik fejezet a kiberbiztonsági védekezés gyakorlati alapelveit és módszereit foglalja össze, elsősorban a mindennapi felhasználók szemszögéből. A szerzők hangsúlyozzák, hogy a támadások jelentős része egyszerű óvatlanságból, hiszékenységből vagy figyelmetlenségből fakad, ezért a legfontosabb védekezési eszköz a tudatos, körültekintő digitális magatartás. A fejezet részletes tanácsokat ad a jelszavak kezelésére, az online fiókok biztonságos használatára, az adathalász üzenetek felismerésére és a gyanús megkeresések kezelésére, külön kitérve arra, hogy a felhasználók hogyan csökkenthetik a személyes adataikhoz való illetéktelen hozzáférés kockázatát.

A szerzők kiemelik, hogy a modern technikai megoldások – például a kétfaktoros hitelesítés vagy a rendszeres szoftverfrissítések – csak akkor hatékonyak,

ha megfelelő felhasználói fegyelem és tudatosság társul hozzájuk. Végül a fejezet hangsúlyozza, hogy a biztonság nem egyszeri állapot, hanem folyamatos odafigyelést és rendszeres kockázatértékelést igénylő folyamat. A biztonsági kultúra kialakítása mellett reakciós cselekvési tervek kialakítása szükséges, a biztonsági gyakorlatok javításának lépéseit kidolgozva.

A kötet lezárásaként 36 oldalas fogalomtárat kapunk, amely részletes meghatározásokat tartalmaz a legfontosabb kiberbiztonsági és informatikai kifejezésekre. A könyv ezen lexikális melléklete külön figyelmet érdemel. A szerzők kiemelik, hogy a terminológia-változás gyorsulásának következtében nélkülözhetetlen a kulcsszavak folyamatos definiálása. A kötet záró fejezetében található kifejezésjegyzék valójában a teljes mű esszenciáját is összefoglalja: minden fontos fogalmat közérthetően magyaráz, így segítve az újonc olvasó felzárkózását és a szakember fogalmismeretének egységesítését. Ahogy a szerzők írják, ez a fogalomtár adja a *digitális immunrendszer* alapját. A lexikális melléklet külön hasznos azon pénzügyi szakemberek számára is, akik eddig nem találkoztak részletes kiberbiztonsági szakszöveggel: rövid útmutatóként szolgál, ha valaki elakad egy idegen kifejezésnél, és egyben ellenőrzést nyújt a közös szaknyelv kialakításához. Összességében a fogalomtár a kötet egyik leggyakorlatiasabb eleme, amely növeli a kézikönyv alkalmasságát mind oktatási, mind naprakész hivatkozási célokra.

A könyv kiemelkedő aktualitását az adja, hogy Magyarországon – hasonlóan más uniós országokhoz – az utóbbi években felerősödött a kiberbiztonsági szabályozás és tudatosság. A magyar nemzeti kiberbiztonsági stratégia például kimondja, hogy a biztonságos kibertér megvalósítása „közös feladat” minden érintett számára. A *Kiberbiztonság – kibertér* tehát időszerűen érkezik a magyar olvasókhoz. A kötet nem pusztán az informatikusoknak szól, hanem a bankok és pénzügyi intézmények döntéshozóinak, jogászainak és kockázatkezelőinek is hasznos olvasmány. Bemutatja, hogyan kapcsolódik a globális kiberszabályozás a hazai gyakorlatokhoz, és rámutat arra, hogy a magyar pénzintézetek belső szabályai és nemzetközi ajánlásaik összehangolása sürgős feladat. Ugyanakkor a könyv önálló tudományos eredményt is kínál: szerepel benne olyan friss hazai statisztikai és jogi adatelemzés, amely más magyar könyvben nem, valamint a szerzők számos, magyarul nehezen elérhető nemzetközi forrást (európai statisztikák, ENSZ/Europol-adatok) foglalnak össze. A kiadvány összetett, hídat képez a magyar pénzügyi és infotechnológiai szakma között. Számos hazai kézikönyv foglalkozik egy-egy részterülettel (például kiberkockázat-kezelés, jogi környezet vagy információbiztonság), de ez a kötet komplexen átfogja a pénzügyi dimenziót is. Összevetve a hazai szakirodalommal, hiánypótló, a banki vezetők szemszögéből íródott és pénzügyi összefüggésekre reflektál – így magyar vonatkozásokban is újdonságokat tartalmaz. Nem csak az üzleti, hanem a jogalkotói, szabályozói és az oktatási szférában is sürgető kérdés, hogyan ismerhetők fel és kezelhetők hatékonyan a mind újabb, egyre kifinomultabb kiberfenyegetések. Az európai és magyar pénzügyi szektorban az utóbbi években bekövetkezett jelentős jogszabályváltozások (NIS2, DORA, MNB-i irányelvek), valamint

az incidensek számának drasztikus emelkedése egyaránt sürgették egy ilyen, átfogó kézikönyv elkészültét. Érdekességként említhető, hogy 2024-ben például a CrowdStrike hibája nyomán világszerte több mint 8 millió rendszer omlott össze – ez a példa élesen rávilágít, mekkora jelentősége van a proaktív, szakmailag megalapozott kiberbiztonsági irányításnak a kritikus infrastruktúrák esetében is.

A könyv messzemenően érzékelteti, hogy a magyar pénzügyi digitalizáció szintje az európai átlag felett van, de ezzel együtt aránytalanul megnőttek a támadási felületek is. Egyedülállóan hasznos a bankvédelmi rendszerek mellett a KiberPajzs program, valamint a Pénzügyi Navigátor és KiberPajzs edukációs projektek példáin keresztül bemutatni, hogyan lehet a lakosság pénzügyi tudatosságát erősíteni a kiberbűnözéssel szemben. A könyv bizonyos fejezetei közvetlenül használhatók egy oktató, compliance, digitalizációs átalakulást kezelő, vagy akár fogyasztóvédelmi stratégiát kidolgozó szakmai team számára is. ■