GAZDASÁG ÉS PÉNZÜGY • 10. ÉVF. 1. SZ. • 2023. MÁRC. • DOI: 10.33926/GP.2023.1.1

FÓKUSZBAN A PÉNZÜGYI BIZTONSÁG KIBERTÉRBEN IS – PÉNZ7

Terták Elemér – Kovács Levente[1]

ABSZTRAKT

2023. március 6. és 10. között kilencedik alkalommal rendezik meg a pénzügyi és vállalkozói tudatosságot interaktív eszközökkel fejlesztő PÉNZ7 eseménysorozatot. Örvendetes, hogy az idei pénzügyi tematikus témahéten köszönthetjük a másfél milliomodik diák résztvevőt, ez az eredmény közel egy évtized és mintegy 1700 iskola kitartó munkáját dicséri.

Az idei PÉNZ7 témahét fókuszába a projektgazda Belügyminisztériummal karöltve a Gazdaságfejlesztési Minisztérium, a Kulturális és Innovációs Minisztérium, a Pénzügyminisztérium, a Magyar Bankszövetség, a Pénziránytű Alapítvány, valamint a Junior Achievement Magyarország Alapítvány szakmai egyeztetés alapján a *„Korszerű pénzkezelés és digitális biztonság"* témáját állította. Cikkünk a pénzkezelés digitális biztonságának különböző vetületeit tekinti át. Célunk, hogy a tanárokkal és a diákokkal a témába vágó gyakorlati ismereteket és hasznos tanácsokat osszunk meg.

JEL-kódok: A20, G2, O30

Kulcsszavak: pénzügyi kultúra, kiberkockázat, pénzügyi biztonság

1. A DIGITÁLIS TÉR „FELFEDEZÉSE"

Az évszázadok alatt kialakult, majd megszokott gazdasági tér működési alapjainak a megváltozása az 1970-es években a számítógépek megjelenésével kezdődött, majd a 2000-es években az internet alapú szolgáltatások kiépülése és a széleskörű hozzáférés megjelenése (amely a családonként egy otthoni számítógépről a személyenként egy okos telefonra nőtt, azaz „a digitális szolgáltatások legalább alapszinten bekerülhettek a háztartásokba" (Terták–Kovács, 2020:376), új szolgáltatási, kereskedelmi, pénzügyi és információs teret nyitott meg. A digitális tér ter-

1 *Terták Elemér* elnökségi tag, Magyar Közgazdasági Társaság, felügyelőbizottsági elnök, K&H Bank Zrt. E-mail: elemertertak@gmail.com.
Kovács Levente főtitkár, Magyar Bankszövetség, tanszékvezető egyetemi tanár, Miskolci Egyetem. E-mail: kovacs.levente@bankszovetseg.hu.

mészetes adottságai révén költséghatékonyan tud a különböző meglevő, felkeltett vagy elképzelt fogyasztói igényeknek megfelelni. Azaz az új tér mind a szolgáltatások előállítói, mind a felhasználói számára vonzó lehetőségeket és feltételeket teremt, ráadásul folyamatosan fejlődik s megújul (*Poletaeva* et al., 2019).

A digitális tér folyamatos és gyors fejlődésének az egyik következménye, hogy a szüntelenül változó jogviszonyokkal a jogalkotók nem képesek lépést tartani. Tréfásan azt is mondhatnánk, hogy a rómaiak erre nem gondoltak. Így az ebben a térben zajló, hagyományos vagy újszerű szolgáltatások digitális változatának, eljárási szabályainak, folyamatainak, garanciális és felelősségi elemeinek, valamint kockázatainak a szabályozása nem tudott időben és kellő mélységben lépést tartani a fejlődéssel. Ez a hiány a globális szolgáltatások korában ráadásul csak globálisan pótolható – hiszen a nemzeti szintű keret már nem elégséges –, ennek megvalósítása viszont jóval több időt vesz igénybe.

A digitális tér fejlesztésének három korlátja lehet: a digitalizálható szolgáltatási megoldások szűkössége, a szolgáltatók digitalizált megoldásainak hiányosságai vagy a felhasználók nem kellő nyitottsága a digitális új megoldásokra. A fejlődés ütemének korlátait *Csányi Sándor* nevezte meg: „Hagyni kell az ügyfelet, hogy a saját szokásainak, igényeinek megfelelő módon tudja igénybe venni a termékeket és a szolgáltatásokat, azaz mindenki a maga tempójában mehessen keresztül a digitalizálódás egyes fázisain" (Kovács–Sipos, 2017:24). Azaz a digitalizáció térnyerésének legfőbb korlátja a fogyasztók alkalmazkodási képességének a gyorsasága. A pandémia kitörésével, az otthoni munkavégzés és tanulás általánossá válásával, az online bankolásra és a házhoz szállításos bevásárlásokra való áttéréssel stb. a digitális megoldások igénybevételétől való idegenkedés megszűnt, azaz néhány hónap alatt egy évtizedet léptünk előre. Ez a gazdaság minden területére hatást gyakorolt (Terták–Kovács, 2020).

A tömegszerűen használt digitális térbe a társadalom széles köréből tapasztalatlan felhasználók érkeztek, akiknek az új megoldásokkal szembeni fenntartásait a kezdők számára is érthető, kifejezetten ügyfélbarát informatikai megoldások révén kívánták enyhíteni. A digitális térbe való megérkezés és az új megoldások intenzív használata azonban nem járt együtt a digitális tér kockázatainak a felés megismerésével. Ez a körülmény a kibertér csalói számára szinte aranybányát teremtett, amennyiben a csalási kísérletek és kibercsalási típusok exponenciális bővülésére és sajnos eredményességének növelésére adott módot. Ez ellen csak széleskörű összefogással, a jogalkotói, az informatikai és a pénzügyi területek szakmai együttműködésével, valamint az ügyfelek pénzügyi ismereteinek elmélyítésével és magatartásuk tudatossá tételével lehet eredményesen védekezni.

2. A DIGITÁLIS PÉNZKEZELÉS KOCKÁZATAI

A pénz, illetve a pénzügyi rendszer legnagyobb hatású változását is a technológiai fejlődés már említett felgyorsulása hozta (*Bangó–Pintér*, 2022). Koncepcionális újdonságot az jelent, hogy míg a korábbi változások inkább a pénz megjelenési formáját érintették, a most zajló változásoknak inkább tartalmi vonatkozásai vannak. Az új technológiák fejlődése elsősorban hatékonysági és kényelmi változásokat hozott a pénzügyek terén is, és elterjedésüket nagyban segítette a fiatalabb generációknak a digitális megoldások iránti érdeklődése, fogékonysága és bizalma.

Az új technikai lehetőségek, különösen az azonnaliság azonban óhatatlanul új kockázatokat is teremtenek. Egyrészről azért, mert a megfelelő ismeret és kellő önkontroll nélkül sok fiatal könnyen enged az internetről őket érő kísértéseknek, és ez a lépés az azonnali fizetés/teljesülés mellett jellemzően visszafordíthatatlan. Az egyik pénzintézet tudatos vásárlás blogja[2] jól mutatja be ezeket a veszedelmeket: a csábító akciós lehetőségek gyakran még a legtudatosabb vásárlókat is képesek megtéveszteni. Egy hatalmas árengedmény ugyanis egy vissza nem térő lehetőség képzetét kelti, ami sokszor felesleges költekezésre ösztönöz. Valószínűleg a legtöbb olvasó találkozott már olyan akciókkal, ahol a vonzónak tűnő ajánlat (pl. tartalomszolgáltatás, részvételi díj stb.) egy idegen nyelvű regisztrációs oldalra vezet, ahol a meghirdetett kedvezmény megszerzéséhez meg kell adni a nevet, a bankkártya adatait és/vagy a mobiltelefon számát. Az ingyenes – ám nagyon rövid – próbaidőszak után egyszer csak aktiválódik egy előfizetés, ami emelt díjas SMS-eket kér, vagy havi 20–40 eurós előfizetési díjat emel le a számláról, ha a felhasználó nem gondoskodik időben a lemondásról. Ezt azonban megnehezíti az, hogy néhány alkalmazás és szolgáltatás értesítést sem küld az ingyenes próbaidőszak lejárta előtt, csak automatikusan terhel, ráadásul a szolgáltatás lemondása meglehetősen bonyolult, és többnyire kellő idegennyelv-ismeretet is igényel. Az ilyen „trükkös" applikációkat nevezi a szakirodalom „fleeceware"-nek (átverő szolgáltatásnak). Az Európai Bizottság és a tagállami hatóságok Fogyasztóvédelmi Együttműködési Hálózata (Consumer Protection Cooperation Network – CPC) már fellépett az ilyen kereskedelmi módszerekkel szemben, de még időbe telik, amíg sikerül teljesen visszaszorítani ezt a fajta rosszhiszemű gyakorlatot.

Ám még a teljesen tisztességes üzleti ajánlatok vagy az egyébként pénzügyileg megalapozatlan vágyak túlzott felcsigázása is az adósságcsapda fenyegető veszélyét jelenthetik a tizenévesek és a fiatal felnőttek számára a készpénz nélküli, azonnali fizetés lehetősége miatt. Az internetes kereskedelemben használatos

2 L. https://blog.provident.hu/tudatos-vasarlas.

olyan különböző fizetési módozatok, mint például az utánvét, a PayPal, a hitelkártyával történő fizetés vagy a kamatmentes részletfizetés lehetősége ugyanis csábítóvá teszi, mi több, előmozdítja a vásárlást, hiszen „mindössze" egy egérkattintással lehet fizetni, ami bizony egyszerűbb, mint a pénzt a saját pénztárcából előguberálni. A megfontolatlan vásárlásokat ugyan a biztonsági okokból bevezetett, kétlépcsős azonosítás megnehezítheti, de megakadályozni nem tudja. Ezért kinek-kinek magának kell kifejlesztenie azt a képességét, hogy hirtelen felindulásból ne költekezzen.

Azt, hogy a megfontolatlan internetes vásárlások milyen súlyos következményekkel járhatnak, a GfK Piackutató Intézet által a Német Bankok Szövetségének megbízásából 2015-ben készített felmérése mutatja[3]: eszerint a német fiataloknak a 31 százaléka már legalább egyszer eladósodott az interneten vásárolt áruk és szolgáltatások miatt, nyolc százalékuknak az adóssága pedig nagyobb volt annál, mint amennyit önerőből képes lett volna visszafizetni.

A szakképzés megkezdésével vagy a munkába állással szerzett jövedelem révén sok fiatal pénzügyi helyzete gyakran tovább romlik, mert az ösztöndíjjal vagy a keresettel ugyan saját bevételre tesznek szert, ám az addig megszokottnál nagyobb arányban kell maguknak gondoskodniuk a megélhetésükről (*Szakács* et al., 2016). A pénzügyi önállóvá válás „szabadságérzete" többeket visz kísértésbe, hogy a lehetőségeiken felül költekezzenek. Ennek rendszerint az lesz a következménye, hogy tartozásuk halmozódik fel a szülőkkel szemben, negatívvá válik a bankszámlájuk egyenlege, a magasra duzzadt folyószámlahitel-tartozás pedig súlyos kamatteherrel jár (*Lentner*, 2013). E kockázatok miatt szorgalmazzák a szakértők, hogy a fogyasztói és pénzügyi ismeretek oktatása kötelező tantárgy legyen az iskolákban – s ezt az elképzelést a legtöbb fiatal is üdvözli. A PÉNZ7 rendezvényeknek is az egyik fontos célja, hogy a pénzügyi ismeretek átadásával elősegítse a fiatalok számára a felelős pénzgazdálkodás elsajátítását.

A felelős pénzgazdálkodás, az intelligens pénzkezelés többről szól, mint az adósság elkerülése – és ezt a Z generációnak (18–25 évesek) is mielőbb meg kell tanulnia. Annak ellenére, hogy ez a korosztály az egyik leginkább adósságkerülő generáció, ők érték el a legalacsonyabb pontszámot a TIAA Intézet 2018-ban végzett pénzügyi műveltségi tanulmányában.[4]

3 https://www.schuldnerberatung.de/ebook-verschuldung-jugendlicher.pdf, 2019. Hasonló eredményekre jutott a svájci Statisztikai Hivatal 2020-ban: https://www.bfs.admin.ch/bfs/de/home/statistiken/wirtschaftliche-soziale-situation-bevoelkerung/einkommen-verbrauch-vermoegen/verschuldung.html.

4 https://gflec.org/wp-content/uploads/2018/04/TIAA-Institute-GFLEC-2018-PFinIndex-Press-Release-FINAL.pdf.

A Z generációnak csupán 46 százaléka érzi magát biztosnak a pénzügyi ismeretek terén, ami alacsonyabb arány annál, mint amit a baby boom korszak szülöttei (58–74 évesek), az X generáció (42–57 év közöttiek) és az Y korosztály (26–41 évesek) tagjai válaszoltak. A Z generáció az első olyan korosztály, amely számára az okostelefonok és a közösségi média már a mindennapi élet elválaszthatatlan részét jelenti, s akik naponta körülbelül 6,5 órát töltenek az okostelefonjukon. Ennek a korosztálynak a pénzügyi ismeretei mutatkoztak a kockázatfelfogás és a kockázat elleni védekezés terén a legalacsonyabbnak.[5]

Itt kerül a képbe a pénzügyi tudatosság, a pénzügyi kompetencia, ami a pénzügyi műveltségnél tágabb és sokrétűbb fogalom. Míg a pénzügyi ismereteket általában tanulással el lehet sajátítani, a pénzügyi tudatosságnak már köze van a gondolkodásmód, a dolgokhoz való hozzáállás és a viselkedés formálásához is – és ezek a tényezők vitathatatlanul sokkal fontosabbak a pénzügyi döntések meghozatalában (*Veresné–Varga*, 2018).

A pénzügyi ismeretek oktatása terén gyakran tapasztalható az, hogy a módszertan az egyszerű tanácsokra és általános iránymutatásokra összpontosít, holott a pénzügyi tudatosság fejlesztése során időt és teret kell szánni a komplexitásra, vagyis a dolgok mélységének és árnyaltságának a bemutatására és megértetésére is.

Napjainkban a pénzügyek nagyfokú digitalizáltsága miatt a pénzügyi kompetencia elképzelhetetlen a megfelelő digitális kompetenciák nélkül. Bár – mint már említettük – a legfiatalabb korosztályok már nagy digitális jártassággal rendelkeznek, az mégsem jelent automatikusan kellő felkészültséget a pénzügyek terén a kellő biztonság megteremtéséhez, fenntartásához.

2.1. Digitális kompetenciák

De nem csak a megfontolatlan pénzköltés fenyeget veszéllyel. A lakosság által egyre inkább igénybe vett digitális pénzügyi szolgáltatások használatáról készített felmérése alapján *Szobonya Réka*, a Budapesti Gazdasági Egyetem tanársegéde arra az eredményre jutott, hogy a válaszadóknak a digitális kompetenciákkal kapcsolatos helyes válaszai közel harminc százalékponttal gyengébb teljesítményt mutattak a pénzügyi tudásteszten elért eredményeknél (Szobonya, 2021), jóllehet a pénzügyi ismeretek és a digitális kompetenciák szintje között pozitív, közepes erősségű kapcsolat van. Külön megemlítendő, hogy a digitális kompetenciák egyes részterületein nagyon eltérő teljesítmények tapasztalhatók, a leggyengébbnek a digitális adatvédelem mutatkozik (*1. táblázat*).

5 https://www.tiaa.org/public/institute/publication/2018/millennial-financial-literacy-and-fintech-use.

1. táblázat
Digitális kompetenciák területein elért eredmények átlaga (%)

Kompetenciaterület	Férfi	Nő	Együtt	Szignifikancia
Kommunikáció, együttműködés	6,85	6,65	6,80	0,91
Információszerzés	34,90	30,79	32,60	0,25
Eszközvédelem	37,94	34,55	36,20	0,25
Digitális adatvédelem	84,44	84,70	84,50	0,91
Digitális kompetenciák együtt	41,05	39,19	40,05	0,27

Forrás: Szobonya, 2021

A digitális kompetencia különbségei területi alapon is számottevőek (l. *2. táblázat*):

2. táblázat
Válaszadók megoszlása az igénybe vett digitális pénzügyi szolgáltatások száma alapján településtípusonként és az egyes régiókban

	Igénybe vett digitális szolgáltatások száma (db)			
	3 vagy több	2	1	Nem használ
Főváros	13,8	14,9	36,2	35,1
Megyei jogú város	11,9	16,1	30,1	42,0
Város	7,8	18,6	27,1	46,5
Község	7,4	12,8	22,8	57,0
Budapest	13,8	14,9	36,2	35,1
Dél-Dunántúl	19,5	22,1	19,5	39,0
Közép-Dunántúl	15,8	18,7	25,2	40,3
Dél-Alföld	0,8	11,6	33,3	54,3
Észak-Alföld	0,0	10,5	25,0	64,5

Forrás: Szobonya, 2021

3. A KIBERBŰNÖZÉS A VILÁGBAN ÉS MAGYARORSZÁGON

A digitális kompetencia bemutatott szintjével nem lehetünk elégedettek. Már csak azért sem, mert az utóbbi években a kiberbűnözés világszerte és hazánkban is növekvő tendenciát mutat, mint arra már utaltunk. A kiberbűnözés minden olyan lehetséges rosszindulatú támadást magába foglal, amelynek célja az anyagi haszonszerzés vagy károkozás a személyes adatokhoz való jogellenes hozzáférés, a digitális műveletek megzavarása vagy az információk eltorzítása, megváltoztatása révén. A nem megfelelően tárolt vagy védett adatok könnyen válnak kibertámadások zsákmányává. Az igazán megdöbbentő tapasztalat azonban az, hogy 10 támadásból 9 esetben az emberi tényező – a felhasználók óvatlansága vagy hanyagsága – vezet a károk elszenvedéséhez. Felmérések szerint a kárt okozó események közel háromnegyede adathalász e-mailek megnyitásából ered, amelyekből világszerte naponta több milliárdot küldenek szét. Ugyan az internetszolgáltatók és a vállalati szerverek igyekeznek ezek terjedését különböző módszerekkel korlátozni, azonban sajnos közel egyötödük ennek ellenére átjut a biztonsági szűrőkön, ezeknek a felét pedig az óvatlan címzettek meg is nyitják, sőt még válaszolnak is rájuk.

A kiberbűnözést a legkülönbözőbb szereplők követik el, beleértve az elégedetlen alkalmazottakat, az ipari kémeket, a rosszhiszemű hackereket, a drogkereskedőket, a tiltott szerencsejátékot szervezőket, a bűnszervezeteket, a terrorista csoportokat vagy az ellenséges nemzetállamokat. Bűncselekményeiket számítógépek, számítógépes hálózatok és más digitális kommunikációs csatornák (pl. közösségi médiák) segítségével követik el. Az elkövetők áldozatul egyéneket, üzleti csoportokat vagy akár kormányokat szemelhetnek ki.

A világon 2017 és 2021 között közel háromszorosára nőtt az online térben elkövetett bűncselekmények száma, és majdnem ötszörösére emelkedett az általuk okozott kár. Egyedül 2021-ben az illetékes hatóságok több mint 847 000 eset bejelentését regisztrálták, ezek összesen 6,9 milliárd dolláros kárral jártak.

A magyar Büntető Törvénykönyvben nincs a kiberbűncselekményekről szóló önálló fejezet, és jó ideig valószínűleg nem is lesz. Ennek az az oka, hogy a bűnözők folyamatosan több olyan elkövetési módszert találnak ki, amelyek korábban nem is léteztek, ezeket pedig lehetetlen volna naprakészen törvénybe iktatni. Vannak azonban kapaszkodók a Büntető Törvénykönyvben: az információs rendszer vagy adat megsértésének a bűncselekménye.[6] Bár ez egy száraz jogi meghatározás, de a

6 A Büntető Törvénykönyv (2012. évi C. törvény) XLIII. fejezetében (Tiltott adatszerzés és az információ rendszer elleni bűncselekmények), a 423. §-ban meghatározott bűncselekmények.

gyakorlatban sok mindent lefed, s ezért a bűnüldöző szervek a legújabb elkövetési módszerekre is alkalmazni tudják.

Az említett okok miatt Magyarországon a kiberbűncselekményekre vonatkozó, külön statisztika sem készül. Azt persze rögzíti a bűnügyi statisztika, hogy milyen sűrűn fordult elő az „információs rendszer vagy adat megsértése" bűncselekmény, de ezek az adatok nem tesznek különbséget az elkövetés módszerei között, azaz hogy a zsarolóvírusoknak vagy a túlterheléses támadásoknak a száma növekedett-e, mert ugyanabba a tényállásba tartoznak. A Belügyi Statisztikai Rendszer (BSR) szerint az „információs rendszer vagy adat megsértése" nevű bűncselekményből 2018-ban még alig 200-at regisztráltak. 2020-ban ez az érték több mint a négyszeresére, 830-ra emelkedett, és a növekedés 2021-ben is folytatódott. A bővülés a rokon bűncselekménytípusoknál is látványos: az „információs rendszer felhasználásával elkövetett csalásból" 2018-ban valamivel több mint 1100 történt, 2020-ban viszont már 3400 ilyen bűncselekmény-típus jutott a rendőrség tudomására (MABISZ, 2022).

3.1. A kiberbűnözés elleni védelem hazánkban

Mivel a kiberbűnözés nálunk a közgondolkodásban egyelőre még elkülönül a klasszikus bűnözéstől, ezért sokan hiszik azt, hogy a rendőrségen belül külön egység foglalkozik ezekkel az ügyekkel. A valóságban viszont a kiberbűncselekmények ugyanolyan bűncselekménynek minősülnek, mint bármelyik másik, ezért a felderítésükkel ugyanúgy a rendőrkapitányságok, súlyosabb esetben a rendőr-főkapitányságok foglalkoznak. Ma már minden kapitányságon van egy-két olyan rendőr, aki otthonosan mozog a témában. Mindazonáltal – tekintettel a kiberbűnözés sajátos jellegére – a Nemzeti Nyomozó Irodán (NNI) belül működik egy Kiberbűnözés Elleni Főosztály, ahol jelenleg több mint 100 ember dolgozik. Ez az országos hatáskörrel rendelkező főosztály egyfajta szakértői központként foglalkozik a legsúlyosabb kiberbűncselekmények felderítésével, ugyanakkor szükség szerint szakmailag támogatja a rendőrkapitányságok nyomozási tevékenységét, valamint oktatja azok munkatársait. A rendőrségnek ez a szervezeti egysége nem keverendő össze a Nemzeti Kibervédelmi Intézettel (NKI).

A Nemzetbiztonsági Szakszolgálat (NBSZ) keretében létrehozott NKI általános kibervédelemmel foglalkozik: ha például egy kritikus infrastruktúrát támadás ér, akkor elemzi a logadatokat, megvizsgálja, honnan érkezett a támadás, segít visszaállítani a rendes működést, és ha bűncselekményt észlelnek, bejelentést tesznek a rendőrségnél. Az NKI feladatai közé tartozik továbbá az ún. „nemzeti kapcsolattartó pont" működtetése is, amelynek feladata az Európai Unión belüli nagy hatású kiberincidensek hazai koordinálása, az incidensekkel kapcsolatos

jelentések fogadása, küldése a nemzetközi partnerszervezetektől, illetve azok irányába (*Csaba*, 2019).

A fokozott digitalizálás növeli a kiberbiztonsági kockázatokat, ezek mérséklése érdekében a polgárok és a vállalkozások által használt digitális termékeket és szolgáltatásokat is jobban kell védeni a kiberfenyegetésekkel szemben. Ennek a védelemnek az egyik eszközeként a Kiberbiztonsági Ügynökségről, valamint az információs és kommunikációs technológia kiberbiztonsági tanúsításáról szóló (EU) 2019/881 rendelet alapján hazánkban a Szabályozott Tevékenységek Felügyeleti Hatósága (SzTFH) látja el a digitális termékek kiberbiztonságát tanúsító hatósági feladatokat. A tanúsítási tevékenység célja az, hogy az állampolgárok és a vállalkozások által megvásárolható, igénybe vehető infokommunikációs eszközök és szolgáltatások esetében garantálni lehessen a kiberbiztonság folyamatosan fejlődő követelményeinek való megfelelést.

Nemzetközi összehasonlításban a kiberbiztonság hazai jogi, műszaki, szervezeti és együttműködési háttere az ENSZ mellett működő genfi székhelyű Nemzetközi Távközlési Egyesület (International Telecommunication Union – ITU) 2020-ban készült felmérése szerint[7] közepesnek mondható. Hazánk helyezése a 63 országot felölelő rangsorban a 35. volt, közvetlenül Szlovákia után és Izrael előtt. Az EU-n belül 17 országnak volt jobb helyezése, mint Magyarországnak.

3.2. A leggyakoribb kiberbűncselekmények

Az EUROPOL évente elkészíti az internetes szervezett bűnözés fenyegetettségét felmérő kiadványát[8], amely 40–60 oldal terjedelemben arról számol be, hogy a kiberbűnözés milyen irányba fejlődik. E tekintetben elsősorban nem konkrét statisztikai adatokra, hanem inkább trendekre kell gondolni, ugyanis a kiberbűnözés területén nagy a latencia. E jelentésből jól kivehető az, hogy Magyarországra is az jellemző, ami a többi európai országra, vagyis az országhatárok nem számítanak, s a kiberbűnözés terén nincsenek kifejezetten magyar sajátosságok (*Halmai*, 2021).

Az elkövetett kiberbűncselekmények gyakorisága és módszerei azonban évről évre változnak. Az elmúlt évek három leggyakoribb bűnözési formáját az adathalász üzenetek, a nem fizetéses vagy nem szállításos csalások, illetve a személyes adatszivárgások jelentették. Az adathalász üzenetek célja az áldozat személyes vagy pénzügyi adatainak megszerzése és az azokkal való visszaélés. A csalók

7 ITU: Global Cybersecurity Index 2020.

8 Europol: Internet Organised Crime Threat Assessment (IOCTA). A legutóbbi kiadvány a 2021. évet öleli fel.

üzenettel vagy egy erre a célra kreált weboldal segítségével próbálják ezeket az adatokat megszerezni. A nem fizetéses vagy nem szállításos csalás esetén a csaló nem fizeti ki a megrendelt termék/igénybe vett szolgáltatás ellenértékét, vagy a másik oldalon nem teljesít egy fizetéssel egybekötött megrendelést. A személyes adatszivárgás esetén bizalmas információkat tartalmazó adatokat csalárd módon szereznek meg vírusok telepítésével vagy az áldozat megtévesztésével.

A kiberbűncselekményeknek jelentős hányada rejtve marad, egyrészt mert sokan szégyenükben nem tesznek bejelentést, ha ilyen bűncselekmény áldozataivá válnak. Másrészt sokan nem is ismerik fel, hogy kiberbűncselekmények áldozatai lettek. Így például túlterheléses támadások esetében (lásd később) a bűnözők botnethálózatokat használnak, ami azt jelenti, hogy több tízezer ember számítógépét fertőzik meg, és egy ilyen támadásnál ezeknek a számítógépeknek az erőforrásait használják fel. Az átlagos felhasználó ebből csupán annyit észlel, hogy lelassul a számítógépe, nehezebben tölti be az adatokat, de fogalma sincs arról, hogy mindennek voltaképpen egy vírusfertőzés az oka.

Melyek azok a leggyakoribb hibák, amelyeket a felhasználók elkövetnek, és ezáltal kiberbűncselekmények áldozatává válnak? A bűnüldöző szervek tapasztalatai szerint az alaposabban vagy akár csak közepesen felkészült felhasználókat csak kis eséllyel sikerül rászedni. A legtöbb próbálkozás ugyanis meglehetősen primitív, egy kaptafára készül, és ezért könnyen felismerhető.

Sok felhasználó csak azért esik csapdába, mert még a minimális körültekintést is elmulasztja. Például egy e-mailt kap egy olyan szolgáltatótól, amelynek nem is az ügyfele, s a szövegéből az is könnyen kitűnik, hogy azt nem is magyar anyanyelvű személy fogalmazta, ám ennek ellenére megadja a kért adatait. Az is gyakran előfordul, hogy olyan oldalakat keresnek fel a neten, vagy olyan programokat töltenek le, amelyekről azért sejteni lehet, hogy azok nagy valószínűséggel vírussal fertőzöttek, ám mégsem veszik komolyan a veszélyt: nem frissítik rendszeresen az operációs rendszert, vagy nem telepítenek vírusirtót. Mindez arra utal, hogy számos felhasználó átlagos tudatossági szintje meglehetősen alacsony, ugyanis az említett védekezési eszközök használatához nincs szükség különösebb számítástechnikai ismeretekre.

Az alacsony tudatosság kockázatát a koronavírus-járvány megsokszorozta, mert sokan, akik korábban nem használták az internetet, arra kényszerültek, hogy otthonról dolgozzanak, és ezért kevésbé voltak felkészülve az interneten lappangó veszélyekre. Az új „e-felületek” használatára való nyitottság nem járt együtt az „e-alkalmazások” mélyebb ismeretével, ezért sokszor megalapozatlan önbizalom jellemezte a tapasztalatlan felhasználókat. Ennek egyik következménye az, hogy az adatokat sokan nem jól védendő információnak tekintik, hanem csupán kényszerűen használandó munkaeszköznek.

Általános tapasztalat az is, hogy bár a bűnözők szüntelenül újnak tűnő elkövetési módszerekkel próbálkoznak, ha lecsupaszítjuk azokat, akkor rájövünk, hogy nincs igazán új a nap alatt: a kiberbűncselekmények többsége is a kiszemelt célszemélyek megtévesztésén alapul. Legtöbbször ugyanis valamilyen emberi gyarlóságra vezethető vissza az, hogy valaki kiberbűncselekmény áldozatává váljon. Ezért leginkább úgy lehet visszaszorítani ezeket a bűncselekményeket, hogy elejét vesszük az elkövetésük lehetőségének. Ez olyan közhelynek tűnhet, ami minden bűncselekmény-kategóriára igaz, ám gyakorlati haszna a kibertérben kiváltképpen nagy. A védekezés legeredményesebb módja ugyanis az, ha az internetfelhasználók tudatosan felkészülnek az őket érő esetleges támadások kivédésére, vagyis a számítógépeiket és az okostelefonjaikat rendszeresen frissítik, ellátják megfelelő vírusvédelemmel, s megszívlelik a bankjuktól, az internetszolgáltatójuktól vagy a kibervédelmi szervezetektől rendszeresen érkező ajánlásokat és tanácsokat.

A hathatós védekezés elősegítése céljából a cikk következő részében néhány olyan újabb módszert ismertetünk, amelyeket az elmúlt években alkalmaztak a bűnözők, s tanáccsal szolgálunk az ellenük való védekezéshez.

3.3. A legtöbb kárt okozó bűnözési módszerek

3.3.1. Eltereléses csalás

2021-ben a legtöbb kárt az eltereléses csalás (angol nevén Business Email Compromise – BEC) okozta mintegy 2,4 milliárd dollár értékben. Az ilyen típusú támadásoknál a csalók átveszik egy vállalat e-mail-szerverének az irányítását, majd erről az e-mail-címről küldenek üzeneteket a potenciális áldozatoknak azzal a céllal, hogy egy bizonyos összeg átutalására bírják rá őket mondvacsinált, de meggyőzően ható ürügyekkel. Egyre gyakoribb, hogy az e-mail-címeket a népszerű közösségimédia-platformok vagy levelezőrendszerek feltörésével szerzik meg a támadók. A gyanútlan áldozatok által átutalt összegeket egyből valamilyen kriptovalutába forgatják, megnehezítve ezzel a nyomon követést és a pénz visszaszerzését. Tisztességes cégek ritkán fordulnak e-mail-kampányban ügyfeleikhez pénz átutalásáért. Ezért ha egy ismert cég e-mail-címéről érkezik ilyen megkeresés, az utalás előtt kapcsolatfelvétel útján érdemes meggyőződni a kérés valódiságáról.

3.3.2. „Romantikus" csalások

Szintén jelentős összegekkel károsították meg a bizalmi vagy romantikus csalások áldozatait; ez a csalástípus hajtotta a harmadik legnagyobb hasznot az elkövetőknek. Bizalmi vagy romantikus csalásról akkor beszélünk, ha az elkövető társkere-

ső szolgáltatás felhasználásával romantikus szándék színlelésével közelíti meg az áldozatát, majd a kapcsolat elmélyítése után mondvacsinált ürügyekkel személyes adatokat vagy pénzt kér tőle. Védekezni az ilyen próbálkozásokkal szemben a józan ésszel lehet. Aki ugyanis a partnerétől már rövid ismeretség után jelentősebb összeget kér kölcsön ahelyett, hogy bankhoz fordulna, azzal kapcsolatban indokolt óvatosnak lenni.

3.3.3. Befektetési csalások

A digitális térben elkövetett csalások közül a befektetési csalások is „népszerűvé" váltak, gyakoriságuk az utóbbi években jócskán megnőtt. Ennél a módszernél az elkövetők rendkívül előnyösnek tűnő befektetési lehetőségeket ajánlanak a későbbi áldozatoknak. Legtöbbször valamilyen kriptovalutában eszközölt befektetésről van szó, amely a piacon elérhető hozam sokszorosát ígéri, s a befektetni kívánt összeget is általában kriptovalutában kérik. Kezdetben a busás hozam az elektronikus kimutatások szerint duzzasztja a befektetett összeg értékét, de amikor a befektetők zöme realizálni kívánja a látszólag elért hasznát, akkor a „lufi kipukkad", a befektetett összeggel és a vélt haszonnal a felszámolónál kell sorban állni vajmi csekély reménnyel, hogy bármi is megtérül. Védekezni az ilyen csalásokkal szemben csak a józan paraszti ésszel lehet: el kell gondolkodni azon, hogy vajon lehet-e a piaci hozamoknál tartósan magasabb hozamokat tisztességgel kigazdálkodni. S ha netán tényleg akadna ilyen lehetőség, akkor ugyan miért is osztaná meg bárki ezt az „ismeretet" mással ahelyett, hogy maga fölözné le a teljes hasznot?

3.3.4. Zsarolóvírusok

A zsarolóvírusok esetében a támadók nem kertelnek, egy rosszindulatú programmal egyből zárolják vagy titkosítják a megtámadott eszközökön vagy a teljes informatikai rendszerben tárolt adatokat. Az ilyen vírusokat többnyire pornográf oldalakról vagy szerencsejáték-oldalakról juttatják el az áldozatok gépeire. Nem véletlenül: az elkövetők abból indulnak ki, hogy csak kevesen lesznek azok, akik károsodás esetén be merik vallani a családjuknak vagy a rendőrségnek, hogy ilyen weboldalakat kerestek fel. A támadók célja itt is a pénzszerzés; az adatok „visszaszolgáltatásáért" a tulajdonostól cserébe váltságdíj megfizetését követelik. Az elmúlt időben évente közel több száz millió dollár összegű váltságdíjat fizettek ki az áldozatok. Védekezni az ilyesfajta támadások ellen úgy lehet, hogy kevésbé ismert, obskurus oldalra nem látogatunk el, de még kevésbé töltünk le onnan bármilyen fájlt, s ha mégis megtettük, akkor nem telepítjük azokat. Emellett rendkívül fontos, hogy a számítógépes rendszerről és a fájljainkról rendszeresen készítsünk biztonsági másolatot. Így akár egy zsarolóvírusos támadás,

akár a saját operációs rendszer összeomlása miatt újra kell telepíteni a rendszert, a biztonsági másolat révén a helyreállítás is gyors lehet, s az adatvesztés is minimalizálható.

3.3.5. Szolgáltatásmegtagadás

A szolgáltatásmegtagadás (Denial of Service – DoS) egy olyan típusú kibertámadás, amely haszontalan információkkal árasztja el a számítógépet vagy a hálózatot, így az nem tud válaszolni a felhasználói kérésekre. Az elosztott DoS (Distributed Denial of Service – DDoS) ugyanezt teszi, de a támadás közvetlenül a számítógépes hálózatról történik. Egyes számítógépes támadók a hálózat túlterhelésének az idejét más támadások indítására használják. A botnetek, amelyeket néha zombirendszereknek is neveznek, például megcélozzák és túlterhelik a célpont feldolgozási képességeit. A botnetek különböző földrajzi helyeken vannak, és ezért nehezen nyomon követhetők. Védekezni csak korlátozottan lehet az ilyen támadásokkal szemben. A legokosabb, amit a hálózat gyanús lassulása esetén tenni lehet, a számítógép lekapcsolása a hálózatról, hogy minél kisebb esélye legyen a vírusok becsempészésének.

3.3.6. A közbeékelődéses támadás

A közbeékelődéses támadás (man-in-the-middle – MITM) akkor következik be, amikor a hackerek egy kétszereplős kommunikáció közepébe „ékelődnek" be, ami által bizalmas adatok ellopása válik lehetővé. A MITM-támadások különösen gyakran a nem biztonságos wifihálózatok használata során fordulnak elő, amikor a támadók a látogató gépe és a nyilvános wifimodem közé „ékelik be" magukat, majd ellopják a bizalmas adatokat, vagy rosszindulatú programok segítségével adathalász szoftvereket telepítenek a látogató gépére. A védekezés kézenfekvő módja, hogy nyilvános wifihálózaton szenzitív adatokat ne kommunikáljunk, vagyis például ne kapcsolódjunk a bankunkhoz, vagy ne teljesítsünk fizetést.

3.3.7. Adathalászat

Az adathalász támadások megtévesztő kommunikációt, például e-mailt használnak ahhoz, hogy rávegyék a címzettet, nyissa meg és hajtsa végre a benne található utasításokat, például a hitelkártya PIN-kódjának és/vagy CVV-kódjának a megadását. A cél az érzékeny adatok, például hitelkártya- és a banki bejelentkezéshez szükséges adatok ellopása, vagy rosszindulatú programok telepítése az áldozat gépére. A védekezés legjobb módja, ha ilyen adatok kérése esetén rögvest élünk a gyanúperrel, és nem teljesítjük a kérést, ugyanis a bankok sohasem szoktak e-mailben érzékeny személyes adatot kérni (*Pásztor*, 2018).

3.3.8. Jelszótámadások

A megfelelő jelszavak megszerzésével a számítógépes támadó rengeteg bizalmas információhoz férhet hozzá. A bizalomra épülő manipuláció a jelszótámadásoknak a kibertámadások által használt egyik stratégiája, amely nagymértékben támaszkodik az emberi interakcióra, és gyakran magában foglalja az emberek becsapását a szokásos biztonsági szabályok megszegése végett. A jelszótámadások egyéb típusai közé tartozik a jelszóadatbázishoz való hozzáférés vagy a nyílt találgatás. A hackerek az utóbbi esetben az úgynevezett „credentials stuffing" módszert használják, aminek az a lényege, hogy más szolgáltatások feltört adatbázisaiban található belépési adatokat próbálgatnak végig több platformon. Ez főleg azok számára okozhat kellemetlenséget, akik ugyanazt a jelszót használják több helyen, a támadók ugyanis emiatt több profilba is behatolhatnak. A védekezés legcélszerűbb módszere, hogy az érzékeny kapcsolatoknál más és más jelszót használunk, s elkerüljük az olyan jelszavakat, ami a nevünkön, születési adatainkon vagy a lakcímünkön alapul.

3.3.9. Spoofing (megtévesztés hamis weboldallal)

A hackerek az ilyen típusú kibertámadásokhoz a kiszemelt áldozat által használt pénzügyi szolgáltató honlapját klónozzák, vagyis olyan weboldalt készítenek, amely mind megjelenésében, mind funkcionalitásában kísértetiesen hasonlít az eredetire. Az áldozatot egy e-maillel bírják rá arra, hogy felkeresse a klónozott oldalt, s azon figyelmetlenül megadja a belépéshez szükséges jelszavakat. Az ilyen támadás elleni védekezés a honlap webcímének a gondos ellenőrzésével történhet.

4. ZÁRÓGONDOLATOK

Az előzőekben bemutattuk a kibertérben ránk leselkedő veszélyeket. Ezek ellen irányított képzéssel és megfelelő gyakorlatokkal lehet védekezni. A 9. Pénz7-re a Magyar Bankszövetség megbízásából elkészült és a www.penz7.hu oldalon el is érhető a „Pénzügyi biztonság a kibertérben" előadás, amely a közoktatásban tanuló diákok számára a 2023. március 6–10. között megszervezett pénzügyi témahét tanórai anyaga. Az említett honlapról érdekes pénzügyi kvízek és népszerű vetélkedők anyaga is letölthető.

A pénzügyi témahét említett tanórai anyaga a Nemzeti Kibervédelmi Intézet és a Nemzeti Nyomozóiroda közreműködésével készült el. Szakértőik segítségének köszönhetően a tananyag életszerű példákat és praktikus tanácsokat is bemutat.

A tanóra egy izgalmas oldallal (https://threatmap.checkpoint.com) indul, amely élőben mutatja be a Földön a megnyitás pillanatában zajló kibertámadásokat.

Azaz honnan indul és mit, milyen volumenben céloz az éppen futó kibertámadás. A dinamikus térkép látványosan mutatja be, hogy egyetlen nap alatt több millió kibertámadás zajlik. A világ különböző részein zajló támadások folyamatosak; kormányokat, vállalatokat és magánszemélyeket egyaránt érintenek. Az aktuális támadásokban részt vevő fő kártevőtípusok is láthatóak a honlapon. A mozgó látvány mindenkit rádöbbenthet arra, hogy ő maga is lehet áldozat, ha nem védekezik. Habár Magyarország sok szempontból biztonságosnak mondható (pl. Európában nálunk van az egyik legkevesebb bankkártyás csalás), ennek ellenére bármikor veszélybe kerülhetünk, akár úgy, hogy a határon túli weboldalakra szörfölünk.

A sokkoló hatású oldallátogatás után gyakorlati tanácsok következnek a kibertérben való biztonságos közlekedésről. Például: hogyan lehet az internetes vásárlások fizetési kockázatait csökkenteni, melyek a legfontosabb védendő pénzügyi adatok, hol és hogyan tárolhatjuk adatainkat, hogyan fizessünk/fizethetünk az online térben, melyek az igénybe vehető fizetésbiztonsági megoldások, és az örök téma: a jelszó/PIN-kód megfelelő képzése is része ennek az előadásrésznek.

A tanóra befejező egysége a mostanában alkalmazott csalási kísérleteknek a típusok szerinti áttekintésével kezdődik. Majd a zsarolóvírussal kapcsolatos információk és az ajánlott megelőzési, illetve védekezési megoldások hangzanak el. Ezt a részt és az egész órát pedig a hihetetlen hozamot kínáló – természetesen átverést tartalmazó – befektetéseket és nyereményeket kínáló csalási típusok bemutatása zárja. Ilyenformán a cikkünk és a tananyag szervesen kiegészíti egymást.

A jelen tanulmány elkészítésével is az volt a célunk, hogy az elkészült tananyagra építve, hatékony segítséget nyújtsuk a pénzügyi tudatosság fejlesztéséhez, valamint a korszerű pénzügyi szolgáltatások kibertérben jelentkező kockázatainak a megfelelő kezeléséhez.

HIVATKOZÁSOK

Bangó Péter – Pintér Éva (2022): The digital financial solutions pathway for generations. In: Csiszárik-Kocsir, Ágnes – Popovics, Anett – Fehér-Polgár, Pál [eds.] (2022): XVII. FIKUSZ 2022 International Conference: *Proceedings*. Budapest, Magyarország: Óbuda University Keleti Károly Faculty of Business and Management, 622–636.

Csaba László (2019): A költségvetési és bankunió: vízválasztó a többsebességes EU-ban. In: Halmai Péter [szerk.] (2019): *Tagállami integrációs modellek: A gazdasági kormányzás új dimenziói az Európai Unióban*. Budapest, Magyarország: Ludovika Egyetemi Kiadó, 167–181.

Halmai Péter (2021): A Gazdasági és Monetáris Unió rendszerének egyes sajátosságai. In: Halmai Péter [szerk.] (2021): *A Gazdasági és Monetáris Unió jövője: Európai perspektívák*. Budapest, Magyarország: Ludovika Egyetemi Kiadó, 199–288.

Kovács Levente – Sipos József [szerk.] (2017): *Ciklusváltó évek, párhuzamos életrajzok*. Magyar Bankszövetség, ISBN 978-963-331-407-4.

Lentner Csaba [szerk.] (2013): *Bankmenedzsment: Bankszabályozás – pénzügyi fogyasztóvédelem*. Budapest, Magyarország: Nemzeti Közszolgálati és Tankönyv Kiadó Zrt. ISBN: 9789630855914.

MABISZ (2022): Kiberbűnözés Magyarországon: már a rendőrségi statisztikákban is kimutatható a dinamikus növekedés. *Biztosítási Szemle*, 2022.01.11., https://mabisz.hu/szemle/?p=49132.

Pásztor, Szabolcs (2018): The Future of Commercial Banks – Survival or Failure? *Izvestiya: Mezhdunarodnyy teoreticheskiy i nauchno-prakticheskiy zhurnal*, 23(4), 71–88.

Poletaeva, Vladislava – Perepelitsaí Denis – Arhangel'skaya, Tat'yana – Zaripov, Il'yas – Pásztor, Szabolcs (2019): The Research Task of Banks and Authorized Government Institution Interests in Manufacturing Companies' Investment Projects Congruence. *International Journal of Mechanical Engineering and Technology* (IJMET), 10(2), 1603–1609.

Szakács Attila – Szakács Zsolt – Zéman Zoltán (2016): A takarékoskodás, a biztosítások és a banki kölcsönök kapcsolata. In: Bene, Sz. [szerk.] (2016): XXII. Ifjúsági Tudományos Fórum. Keszthely, Magyarország: Pannon Egyetem Georgikon Mezőgazdaságtudományi Kar, 1–6.

Szobonya Réka (2021): Kompetenciák a pénzügyek területén – lakossági felmérés tapasztalatai. *Pénzügyi Szemle*, 66(2).

Terták Elemér – Kovács Levente (2020): A szociális védelem és a társadalmi kohézió kihívásai válsághelyzetben a pénzügyi szférában. *Pénzügyi Szemle* 65(3).

Veresné Somosi Mariann – Varga Krisztina (2018): Tudass tudatosan! A pénzügyi tudatosság, felelősség fejlesztése környezetünkben: Susánszky János Esettanulmánymegoldó verseny középiskolásoknak.Esettanulmány. Miskolci Egyetem Gazdaságtudományi Kar, 18 p.