DOI: https://doi.org/10.12700/btsz.2025.7.1.107

CYBER SECURITY CHALLENGES AND SOLUTIONS IN THE HUNGARIAN BANKING INDUSTRY DURING THE PANDEMIC BASED ON THE CHANGED REGULATIONS

KIBERBIZTONSÁGI KIHÍVÁSOK ÉS MEGOLDÁSOK A HAZAI PÉNZÜGYÁGAZAT JÁRVÁNYHELYZET ALATTI SZABÁLYOZÁSI KÖRNYEZETÉNEK VÁLTOZÁSA ALAPJÁN

SOMOGYI Tamás[1] – NAGY Rudolf[2]

Abstract

In the early 2020's crises occurred that we never saw before. The COVID-19 pandemic has changed our life, e.g., the way we enjoy the essential services of the banking industry. However, the level of cyber threat has also increased significantly. Banks and their customers experienced more cyber attacks than before. The aim of this paper is to explore the solution to this problem that was provided in 2020 or in 2021 by the new regulations of the banking industry. It will be demonstrated in this study that the window of opportunity was opened in these years: regulations has been introduced in order to make the information security more matured by defining minimum mandatory standards. However, the new regulations are mainly focusing on the banks and the security of their digitalised services. Cyber threat to customers are not covered properly by the regulations introduced in the examined period.

Keywords

cyber security, banking industry, coronavirus pandemic, Multiple Stream Approach

Absztrakt

A 2020-as évek elején rendkívüli kihívások jelentek meg. A koronavírus-járvány megváltoztatta mindennapi életünket, többek között a pénzügyágazat alapvető szolgáltatásainak igénybe vétele is túlnyomórészt digitálisan történt. Ezzel párhuzamosan drasztikusan emelkedett a kiberfenyegetettség. Megnövekedett kibertámadást tapasztalhattak meg a pénzintézetek és az ügyfelek. Kutatásunk célja megválaszolni a kérdést, hogy erre a problémára 2020-ban és 2021-ben milyen válasz született a hazai pénzügyágazat szabályozásában? Igazoljuk, hogy ebben az időszakban megnyílt a lehetőségek ablaka: megoldási javaslatok kerültek a szabályozó napirendjére, és megszülettek a vonatkozó szabályok, melyek célja az ágazat információbiztonságának fejlesztése, minimum követelmény meghatározása. A vizsgált időszakban született szabályok, mint megoldások, a pénzintézetek nyújtotta alapvető szolgáltatások digitalizációjára és a biztonságos működésre helyezik a hangsúlyt. Az ügyfeleket érő kibertámadásokkal nem foglalkoznak részletesen a szabályok.

Kulcsszavak

kiberbiztonság, pénzügyágazat, koronavírus-járvány, közpolitikai változások modell

[1] somogyi.tamas@phd.uni-obuda.hu | ORCID: 0000-0003-1397-697X | PhD student, Óbuda University Doctoral School of Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] nagy.rudolf@bgk.uni-obuda.hu | ORCID: 0000-0001-5108-9728 | habil. senior lecturer, Óbuda University, Donát Bánki Faculty of Mechanical and Safety Engineering, Budapest, Hungary | habil. adjunktus, Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

Az épített környezetünket, infrastruktúránkat, az alapvető szolgáltatásokat fenyegető tényezők kettő csoportba sorolhatóak: emberi és nem emberi [1]. Az első csoportban hangsúlyos a magán és állami infrastruktúrát egyaránt veszélyeztető terrorizmus elleni védekezés [2] és a kiberbűnözés [3]. A nem emberi tényezők között a szakirodalom leggyakrabban a természeti események fenyegetését említi [4], és ide tartoznak a járványok is. Környezetünkkel, földünk rendszereivel együtt élünk, ebben létezünk [5]. A természeti erők hatása alól nem vonhatjuk ki magunkat, azokkal számolni kell [6], különösen a létfontosságú rendszerelemek esetében, hiszen nemzetbiztonsági kérdés ezek zavartalan működtetése és a szolgáltatásaikhoz való hozzáférés [7]. Az ókori római költő, Ovidius korszakfelosztását felidézve Lentner mai világunkat az ezüstkorhoz hasonlítja: az aranykorral szemben itt van hőség és fagy, ugyanakkor az ember képes felülkerekedni a nehézségeken [8]. A kétségtelen, hogy a 2020-as évek elején olyan események és változások történtek, melyek hatására még több nehézséggel kellett megküzdeni. Különösen igaz volt ez az alapvető szolgáltatást biztosító létfontosságú rendszerelemek és ezek felhasználói esetében.

A 2020-as évek elején növekedtek a kiberbiztonsági kihívások. Ennek oka lehet egyfelől az internetes szolgáltatások és az okoseszközök terjedése [9], másfelől külső okként a támadások is szaporodnak. A külső támadások növekedéséhez a 2020-ban kitörő koronavírus-járvány is hozzájárult. Az Europol jelentése szerint Európában a kiberbűnözés megnövekedett a koronavírus-járvány idején [10]. Ezt a szektoroktól független jelenséget a pénzügyágazat is észlelte: kutatás igazolta (például [11]), valamint az Európai Központi Bank is a kiberbűnözés növekedő tendenciáját jelentette [12]. Másrészről a kibertér biztonságát a 2020-as évek első felében további események is befolyásolták: az Ukrajnában zajló háború és a közel-keleti konfliktus [13], [14], [15]. A NATO a kiberteret műveleti térnek tekinti [16], a NATO-val és szövetségeseivel szemben álló erők pedig bizonyítottan végre is hajtanak műveleteket a kibertérben [17], [18], [19], melyek a létfontosságú rendszerelemekben zavarokat okozhatnak. Sőt, ezen támadások kimondott célja lehet üzemzavar előidézése létfontosságú rendszerelemben [20]. Az információs hadviselésre és a kibertámadások elmúlt évekbeli növekvő tendenciájára több kutatás is felhívta a figyelmet [21], [22], [23], [24]. Az igaz, hogy a nemzeti kiberbiztonság fontossága már 2020 előtt is ismert volt [25], azonban a 2020-as évek elejének változásai alátámasztották ezen terület kritikusságát. A kiberbiztonság a 2020-as évek elejére stratégiai kérdésként jelent meg a vezető országokban [26], az alapszolgáltatások biztosításának kérdésköre pedig kutatási témává vált [27] és a felsőoktatási képzésben is hangsúlyos szerepet kapott [28]. Az információs infrastruktúra védelme EU szinten egységes jogszabályokban is megjelenik [29].

A digitalizáció és kiberbiztonság kérdésköre hangsúlyosan van jelen a pénzügyágazatban is. A pénzügyágazat alapvető szolgáltatásokat is nyújt, létfontosságú rendszerelemként azonosított [30], ráadásul esszenciális a nemzetgazdaság működése és fejlődése szempontjából [31]. Ennek a támadásoknak mindig is kitett ágazatnak a védelme kiemelten fontos, különösen, amikor a kibertámadások is sújtják [32], [33].

Az alapvető szolgáltatások biztosítása, a létfontosságú rendszerelemek üzemelése kiemelt fontosságú, ezért a kapcsolódó kiberbiztonsági kérdések kutatása rendkívüli jelentőségű. Ehhez a témához járulunk hozzá jelen cikkünkkel. Célunk egy létfontosságú rendszerelem, a pénzügyágazat példáján keresztül szemléltetni a koronavírus-járvány hatását a

kiberbiztonság területére, valamint feltárni, hogy a szabályozói környezet hogyan reagált ezen kihívásokra.

KUTATÁSI MÓDSZERTAN

Kutatási kérdésként tettük fel, hogy a hazánkban is megjelenő koronavírus-járvány milyen kihívásokkal szembesítette a pénzügyágazat alapvető szolgáltatásainak folyamatos biztosítását és azok igénybe vételét a kibertérben?, és ezen kihívásokra milyen válaszokat adott a szabályozói környezet? Kutatásunk során a szakirodalom mellett a járványhoz kapcsolódó ágazat-specifikus szabályozást tekintettük át, melyek érintik az elektronikus alapszolgáltatásokat és a kiberbiztonságot. A pénzügyágazat stabil működését felügyelő Magyar Nemzeti Bank (MNB) 2020-ban és 2021-ben kiadott különböző szintű vonatkozó témájú dokumentumait a www.mnb.hu honlapon kerestük. Az MNB szorosan együttműködik az európai uniós társszerveivel és az Európai Bankhatósággal (EBA) [34]. Igaz ez az alapszolgáltatásnak tartott pénzforgalom esetében is. Az EBA pénzforgalmi területtel foglalkozó bizottságának az MNB is tagja, az ott megfogalmazott európai uniós szintű iránymutatások a hazai ágazat szabályozásának részévé válnak. A szabályozás mellett a pénzforgalmi csalásokhoz kapcsolódó EU szintű tudásmegosztás is biztosított az EBA-n keresztül. Ezért kutatásunkhoz az MNB kibocsátotta dokumentumokat használtuk fel.

Kutatásunkhoz Kingdon közpolitikai változásokról szóló modelljét (angol eredetiben: Multiple Stream Approach, a továbbiakban: MSA) választottuk, mely a folyamati szabályozásokhoz kapcsolódó kutatások során alkalmazható. Ezen modell szerint a közpolitikai változás úgy írható le, mint három folyamat vagy áramlat találkozása [35]. Az első áramlat a *probléma* (problem) melyben megfogalmazódik egy megoldandó probléma. A *közpolitika* (policy) áramlat azon megoldást, szabályozást jelképezi, mely a szakértők válasza, megoldási javaslata a felmerült problémára. A *politika* (politics) áramlat foglalja magába a jogszabályalkotót, felügyeleti szervet, vonatkozó hatóságot. Ahogyan Demszky megfogalmazza [36], egy kritikus ponton jelenik meg a *lehetőségek ablaka*, mely során a három áramlat találkozik. Ekkor a probléma és a megoldási lehetőség a politikai szereplők napirendjére kerül, és elindul a cselekvés, megtörténik a szükséges - szabályozási - változás.

Feltételezésünk szerint a koronavírus-járvány olyan kritikus pont volt, mely során megjelent a lehetőségek ablaka. Következésképpen, ebben az időszakban olyan szabályoknak (megoldásoknak) kellett születniük, melyek választ adtak a járvány előidézte vagy felerősítette kihívásokra (problémára).

A 2020-BAN KITÖRŐ KORONAVÍRUS-JÁRVÁNY HATÁSA A PÉNZÜGYÁGAZAT ALAPVETŐ ELEKTRONIKUS SZOLGÁLTATÁSAINAK KIBERBIZTONSÁGÁRA

Járványok időről időre megjelennek és befolyásolják mindennapi életünket [37]. Járványok idején speciális folyamatok, eljárásrendek lépnek életbe (például karantén és távmunka [38]), mely hatására megváltoznak a szolgáltatások igénybe vételével kapcsolatos szokások (például megugrik a távoli üzletkötések száma). Ráadásul a járványos megbetegedések veszélyt jelentenek a munkavállalók rendelkezésre állására [39]. A járványok terjedésének megelőzése érdekében bevezetett eljárások pedig kihívás elé állítják a gazdaságot és kormányzati szerveket [40]. Egy ilyen helyzetben a gazdasági fejlődés megtorpan vagy

csökken, ráadásul a gazdaság visszafejlődése évekig elhúzódó folyamat is lehet [41]. Ahogyan Vida rámutatott, egy járvány a nemzetek gazdasági-, társadalmi- és politikai biztonságát fenyegeti [42]. Ráadásul, egy kutatás szerint a komoly hatású járványok előfordulási valószínűsége nagyobb, mint azt sokan gondolnák [43]. Mindezek megerősítik, hogy hazánk Nemzeti Biztonsági Stratégiája kockázatként azonosította a járványos megbetegedéseket [44], hiszen azok az előbbi módokon hatással bírnak a szolgáltatásokat nyújtó infrastruktúra üzemeltetésére. Erre példával szolgált a 2020-as évek legelején tomboló koronavírus-járvány.

A koronavírus-járvány következményeit az életünk szinte minden területén érezhettük. Természetszerűleg hatott az egészségügy és munkabiztonság területére [45], de például átalakította a közlekedési szokásokat és szabályokat [46] és újszerű megoldásokat kényszerített a közigazgatásra [47]. Az oktatásban ösztönözte a távoktatáshoz kapcsolódó megoldások széles körű elterjedését [48], [49]. Mindezek mellett a koronavírus-járvány kétség kívül hatással volt a pénzügyágazat szolgáltatásaira is, különösen az alapvető szolgáltatásnak tekinthető elektronikus fizetési megoldásokra.

A Magyar Nemzeti Bank (MNB) az ágazatra vonatkozó adatok alapján úgy látja, hogy a digitális banki csatornák meghatározóvá váltak a koronavírus-járvány alatt [50]. Egyértelmű, hogy a korábban a bankfiókokat preferáló ügyfelek nagy számban tértek át az elektronikus bankolásra. Az pénzintézetek IT területeit is felügyelő MNB meglátása szerint a hirtelen megugró elektronikus bankolási igényeket a pénzintézetek infrastruktúrája zökkenőmentesen tudta kielégíteni. A stabil működés pozitív élménye is hozzájárulhatott a digitális megoldások szélesebb körű elterjedéséhez. Mindez pedig további digitalizációra ösztönözte a pénzintézeteket. A hazai pénzügyágazat szereplői 60 százalékánál erősítette meg és gyorsította fel a digitalizációt a járványhelyzet, vagyis a szektorban a többség hosszabb távon is középpontba helyezi a digitális átállást és az elektronikus megoldásokat. A járvány utáni számadatok tükrében az MNB úgy látja, hogy hazánkban az ügyfeleknek már csak kisebb része intézi ügyeit bankfiókban. Meg kell említeni, hogy a járványtól független, de időben azzal egybe eső lényeges változás történt az átutalási rendszerben 2020. márciusában. Ekkor került bevezetésre hazánkban az Azonnali Fizetési Rendszer, melyre a bevezetésétől kezdve a hazai Forintalapú fizetési forgalom 40%-a terelődött át [50]. Ráadásul az ügyfeleknek a hazai pénzügyágazatba vetett bizalma a koronavírus-járvány alatt is megmaradt, beleértve a bankok innovációs, környezetvédelmi és digitális újításait is [51]. Bizonyosnak tekinthető, hogy mindez hozzájárult az ügyfelek oldalán az elektronikus bankolás nagyobb mértékű használatához.

A járvány időszakában a szektor munkavállalói oldalán is teret hódított a digitalizáció: a távmunka a pénzügyágazatban is elterjedt, a pénzintézetek pedig ehhez igazítják eszközbeszerzési terveiket. A folyamatokban is változások történtek: a belső információáramlás, a jóváhagyás és aláírás is elektronikus módon valósult meg, és ez a pénzintézetek többségnek tervei szerint hosszabb távon is így marad [50].

A digitalizáció terjedésének az árnyoldalának tekinthető, hogy a digitális térben megnövekedett jelenléttel párhuzamosan a kiberbűnözés növekedése is látható volt [52]. Az MNB Kiberfenyegetettségi térképe szerint a 2020-ban pénzügyágazatban felgyorsuló digitalizációs folyamatok általánossá tették a kiberbiztonsági fenyegetést is [53]. Az MNB összegzése szerint 2020. áprilisa és 2021. júliusa között megnövekedett a hazai pénzügyágazatot érintő kiberbiztonsági fenyegetések és támadások száma. A nemzeti bank ebbe a körbe

sorolja a megtévesztésen alapuló támadást, az ügyfelek adataival szembeni fenyegetéseket, valamint az alapvető szolgáltatások rendelkezésre állása elleni fenyegetéseket, mint például a DDoS támadást [53]. Ahogyan az MNB hangsúlyozza, a támadók egyre szofisztikáltabb megoldásokat alkalmaznak. A sikeres támadások után anyagi erőforrás áll a támadók rendelkezésére, amit felhasználhatnak még komolyabb támadásokhoz. Ezáltal a csalási kísérletek, támadási szcenáriók bonyolultabbá és hitelesebbé válnak az ügyfelek számára, így a sikeres támadások száma tovább növekedhet.

Az MNB a pénzügyágazat szereplőinek jelzésén túl ügyfélpanaszokból is képet kap a trendekről. Az ügyfélszolgálatán megtett, kibervisszaélés témájú ügyfélbejelentések száma megugrott a koronavírus-járvány időszakában. A Kiberfenyegetettségi térképben közzétett adatok szerint 2019. negyedik negyedévében 4 ügyfélbejelentés történt, míg 2020. második negyedévétől kezdve negyedévenként 10 feletti, 2021-ben negyedévenként már 20 feletti volt az ügyfélpanasz [53]. Az MNB 2020. év adatait feldolgozó éves jelentése szerint az érzékeny fizetési adatok (jelszó, egyszer használatos kód) megszerzése támadási módszer a koronavírus-járvány időszakában továbbra is kiemelkedő volt [53]. Ugyanakkor újdonságként jelent meg 2020. tavaszán azon megtévesztéses csalástípus, mely során az ügyfeleket rábírták átutalásra olyan egészségügyi eszközök megvásárlásának ígéretével, melyek kereskedelmi forgalomban akkor hiánycikknek számítottak.

Elmondható tehát, hogy a koronavírus-járványra válaszul bevezetett intézkedések hatására elterjedtebbé váltak a digitális szolgáltatások, megnövekedett a kibertér használata. Igaz ez a pénzügyágazat nyújtotta alapvető szolgáltatásokra is. Ezzel párhuzamosan megnövekedett a kiberbiztonsági fenyegetések és támadások száma, illetve fejlődtek a támadók alkalmazta módszerek. Kingdon közpolitikai változásokról szóló modelljének kifejezéseivel élve, megjelent vagy hangsúlyosabbá vált a probléma, a pénzügyágazat alapvető szolgáltatásainak kiberbiztonsága. Felmerül a kérdés, hogy ebben az időszakban eljött-e a kritikus pont, amikor megjelenik a lehetőségek ablaka? Más szóval, a szakértők megoldási javaslata (közpolitika) a politika napirendjére kerül-e, és elindul-e a cselekvés a probléma megoldására? A hazai pénzügyágazat szabályozói környezetének a kiberbiztonság fokozása érdekében történő változását a következő rész vizsgálja.

ÚJ KÖVETELMÉNYEK A HAZAI PÉNZÜGYÁGAZAT SZABÁLYOZÓI KÖRNYEZETÉBEN

A 2020-ban megjelenő koronavírus-járvány a megszokott életünkben hirtelen jött változásokat idézett elő, melyek között szerepel az elektronikus fizetési megoldások szélesebb körű használata. Ahogyan arra fentebb rámutattunk, a kiberbiztonság jelentősége is megnövekedett. Felmerül a kérdés, hogy mindez a hazai pénzügyágazatban indukált-e változást, fejlődést 2020-ban és 2021-ben?

Az MNB 2020-ban és 2021-ben több, a biztonság témájával foglalkozó ajánlást tett közzé. Első helyen említendő *Az informatikai rendszer védelméről* szóló 8/2020. (VI. 22.) MNB ajánlás és *A pénzügyi szervezetek működésének fizikai biztonsági és humánkockázatkezelési feltételeiről* szóló 11/2020. (X.20.) MNB ajánlás. Ahogyan a 11/2020 sz. ajánlás *I. Az ajánlás célja és hatálya* c. részben írja, az MNB ebben a kettő ajánlásában „*összefoglalja azokat az eljárásokat, amelyeket a pénzügyi szervezeteknek a biztonságos működésük érdekében alkalmazni célszerű*“. Ez a kettő ajánlás együtt fedi le a fizikai és a logikai biztonsági követelményeket, beleértve a kiberbiztonság területét is. Az informatikai védelemről szóló

ajánlás részletesen leírja az informatikai biztonsági elvárásokat a tervezéstől és szabályozástól a kockázatelemzésen, fejlesztésen, beszerzésen, tesztelésen át az üzemeltetésig, külön kitérve a szolgáltatás-folytonosságra és a független ellenőrzésre. Érdemes itt megemlíteni, hogy a 16.3.4. pontban elvárja az MNB az ügyfél adatainak és vagyonának védelme érdekében, hogy a pénzintézet a visszaélések észlelésére és megelőzésére csalásfelderítő rendszert működtessen.

Fentiek mellett az MNB kiadta *A távmunka és távoli hozzáférés informatikai biztonsági követelményeiről* szóló 12/2020. (XI.6.) számú ajánlását is, melynek *I. Az ajánlás célja és hatálya* című része szerint a pénzügyágazatban a távmunkát „*a kényelmen túl más gazdasági és társadalmi szempontok is kikényszerítették, a pandémiás helyzet okozta kijárási korlátozások miatt olyan intézményeknél is megjelent a távmunka tömeges igénye, ahol korábban nem, vagy csak korlátozott keretek közt éltek a munkavégzés ilyen formájával.*“ A távmunka széles körű megjelenését tapasztalva, az ajánlás célja, hogy a pénzügyágazat intézményei kezeljék a távmunkához köthető kiberbiztonsági kockázatokat, beleértve az adatvédelmi kérdéseket is. Ez utóbbi érdekében a 8. a) pont előírja, hogy „*a távoli hozzáférés minden esetben titkosított csatornán keresztül történjen*“. Lényeges továbbá a 8. i) pontja, mely elvárja a távoli felhasználó és eszköze (mely kizárólag az intézmény által menedzselt eszköz lehet) hitelesítéséhez a többfaktoros autentikációt. A kiberbiztonsági kockázatok kötelező elemzése után azokat megfelelően kezelni kell adminisztratív szabályozással; az intézmény kezelte eszközök konfigurálhatóságának korlátozásával; a nem az intézmény felügyelte eszközök kitiltásával; hálózatvédelmi megoldásokkal; a napi üzemeltetési feladatok folyamatos ellátásával; a távoli hozzáférés és tevékenység folyamatos figyelésével.

A koronavírus-járvány alatti átmeneti védekezési intézkedések korlátai is hozzájárultak a digitális szolgáltatások szélesebb körben történő igénybe vételéhez. Ahogyan fentebb rámutattunk, ez is ösztönözte a digitális átalakulást. Az MNB ebben a témakörben is kibocsátott ajánlást. *A hitelintézetek digitális transzformációjáról* szóló 4/2021 (III.30.) MNB ajánlás célja a pénzügyágazat digitális átalakulásának biztonságos keretek között történő elősegítése. Ezen ajánlás 2. pontjában megfogalmazottak szerint az MNB elvárja egy digitális transzformációs stratégia kialakítását célkitűzésekkel és azok megvalósulásának nyomon követésével. A 3. a) és b) pontok szerint ezen stratégia célkitűzései között szerepelnie kell a digitálisan elérhető termékek és szolgáltatások körének bővítésének, valamint a különböző digitális csatornák használatának ösztönzésének. Az MNB ajánlása ugyanakkor a biztonságra is kitér, amikor a 3. j) pontban elvárja az informatikai biztonság fejlesztését is. Az 5. pont pedig megfogalmazza azt az elvárást, hogy a digitális transzformációs stratégia és az IT stratégia legyen egymással összhangban. Ezen felül lényeges az ajánlás 13.3. pontja: „*az MNB a csalás elleni kockázatok feltérképezése, kiértékelése és kezelése kapcsán – a vonatkozó jogszabályi megfelelés mellett – elvárja, hogy a hitelintézet a digitalizáció növekedése kapcsán esetlegesen újonnan megjelenő csalási eseteket is beépíti a kockázatkezelési módszereibe*“. A 15. pont külön kiemeli az informatikai biztonsági fejlesztések esetében a fentebb említett 8/2020. (VI. 22.) MNB ajánlást. A digitalizáció részeként a távoli ügyintézés ösztönzése és terjedése kapcsán érdemes még megemlíteni, hogy 2020. októberében az MNB közzétett egy állásfoglalást is az elektronikus csatornákon keresztül előterjesztett panaszok kezelésének módjára vonatkozóan [54].

2020-ban és 2021-ben a hazai pénzügyágazatban megjelenő, IT biztonsági témájú új elvárások és ajánlások bemutatása után a következőkben kerül sor következtetések levonására.

KÖVETKEZTETÉSEK

Fentiekben bemutattuk, hogy a hazánkban 2020-ban kitört koronavírus-járvány felgyorsította a pénzügyágazat digitalizációját és növelte az elektronikus banki szolgáltatások igénybe vételét. A járvány időszakában, illetve a digitalizációval összhangban az ügyfelek bankfiók felkeresése nélkül, távolról intéztek banki ügyeket a korábbinál nagyobb mértékben. Ugyanakkor, ezzel párhuzamosan a kibertámadások és visszaélések száma is megnőtt. A pénzügyágazat tapasztalata szerint az alapvető szolgáltatások rendelkezésre állása elleni támadások gyakoribbá váltak. Továbbá az ügyfelek elleni támadások is megnövekedtek, melyek célja adatok vagy pénz megszerzése. Ebben a körben új csalástípus is megjelent a járvány időszakában.

Az alkalmazott MSA modell terminológiáját használva, megjelent egy probléma: az elektronikus banki szolgáltatások biztonságát veszélyeztető tényezők jelentőssé váltak. Talán legfontosabb következtetésünk, hogy a problémára válaszul az információbiztonság szintjének emelését célzó előírások és a szektorban alkalmazandó megoldások megjelentek az ágazat-specifikus szabályzatokban. Igazoltuk tehát, hogy a koronavírus-járvány alatt tapasztalt kiberbiztonsági kihívások megjelenése kritikus pont volt, 2020-ban és 2021-ben megnyílt a lehetőségek ablaka, a szabályozó cselekedett. Az MNB ajánlásokat bocsátott ki az informatikai és a fizikai biztonság területén, az ágazatban a távmunka terén, valamint a digitalizáció kérdéskörében, továbbá, vonatkozó állásfoglalást is közzé tett.

Látható, hogy a vizsgált időszakban megnyílt a lehetőségek ablaka, de ebből nem következik az, hogy előtte ne cselekedett volna a szabályozó. Az informatikai rendszerek védelme terén korábban is létezett ágazatspecifikus ajánlás, mivel a fentebb említett 8/2020-as MNB rendelet lecserélte a korábbi 7/2017. (VII. 5.) számú ajánlást. Ugyanakkor a távmunka tárgykörében nem létezett korábban ajánlás, tehát ebben az esetben a vizsgált időszakban nyílt meg először a lehetőségek ablaka. A WHO vissza-visszatérően aktualizált, 2009-es kiadású járványügyi ajánlása felhívta a nem egészségügyi szektor szereplőinek figyelmét járványhelyzeti terv készítésére, benne az erőforrások átcsoportosítására az alapvető szolgáltatások biztosítása érdekében [55]. Ebben a témában mégsem nyert teret a kérdés ezen aspektusa a kockázatkezelésben korábban.

Részleteiben megnézve a szabályozói választ (politika), látható, hogy az MNB ajánlásai hangsúlyt fektetnek a pénzintézetek fizikai- és informatikai biztonságára. A kiberbiztonság terén megfogalmazott elvárások, mint minimum követelményszint, komplex választ adnak a külső támadásokra vonatkozóan. Lefedik az informatikai biztonság minden területét a bankok oldalán. Ehhez kapcsolódik a járvány hatására a pénzügyágazatban széles körben elterjedt távmunka informatikai biztonságának követelményeiről szóló ajánlás is, mely az alkalmazottak biztonságos munkavégzésének követelményeit adja meg. Az ágazatban tapasztalható, a járvány is ösztönözte digitális transzformációra válaszul megjelent ajánlás pedig a digitalizáció további terjedését célozza, előírva a biztonsági követelményeket, az IT stratégiához és információbiztonsági ajánláshoz kapcsolódva. Mindezzel az MNB, mint szabályozó, komplex választ ad az ágazat alapvető szolgáltatásait fenyegető kiberbiztonsági problémára.

Ugyanakkor a kutatásunk során fellelt MNB ajánlásokban kevés szó esik a kiberbiztonsági probléma másik részéről, az ügyfeleket fenyegető támadásokról. A koronavírus-járvány időszakában megnövekedett csalásra az MNB külön ajánlást nem fogalmazott meg, a csalásmegelőzés banki oldali részével csak kismértékben foglalkozott ajánlásaiban. Erre magyarázatot nem találtunk. Lehetséges, hogy ennek oka a közpolitikai áramlatban keresendő, vagyis az ügyfeleket érő támadásokra megfelelő megoldási javaslat nem született a vizsgált időszakban, hiszen új csalástípus is megjelent. Esetleg a politikai áramlat nem volt megfelelő, vagyis a szabályozói oldalon nem kezelték kellő hangsúllyal a problémát, és nem fogalmaztak meg megfelelő szabályozói elvárást. Mindenesetre látható, hogy a vizsgált időszakban erre a részproblémára vonatkozóan nem nyílt meg a lehetőségek ablaka, vagy csak részlegesen, elsősorban más témájú ajánlásokban. Ez a jelenség további kutatások témája lehet.

ÖSSZEFOGLALÁS

A 2020-as évek első éveiben rendkívüli kihívásokkal szembesültünk, köztük a koronavírus-járvánnyal. Ahogyan bemutattuk, a járvány időszakában a pénzügyágazat alapvető szolgáltatásai közül az elektronikus szolgáltatások igénybe vétele hirtelen megnövekedett. Ezzel párhuzamosan azonban drasztikusan emelkedett a kiberfenyegetettség is, mind a pénzintézetekkel szemben, mind pedig az ügyfelekkel szemben. Kutatási kérdésként tettük fel, hogy a hazánkban is megjelenő koronavírus-járvány milyen kihívásokkal szembesítette a pénzügyágazat alapvető szolgáltatásainak folyamatos biztosítását és azok igénybe vételét a kibertérben?, és ezen kihívásokra milyen válaszokat adott a szabályozói környezet?

Kutatásunkhoz a közpolitikai változások modellt (Multiple Stream Approach) választottuk. A hazai pénzügyágazatban 2020-ban és 2021-ben megjelenő szabályozást áttekintve igazoltuk, hogy ebben az időszakban megnyílt a lehetőségek ablaka. A kiberfenyegetettség problémájára megoldási javaslatok kerültek a szabályozó napirendjére, és megszülettek a vonatkozó szabályok, melyek célja az ágazat információbiztonságának fejlesztése, minimum követelmény meghatározása. Az igaz, hogy az informatikai rendszerek védelmének területén korábban is jelent meg MNB ajánlás (korábban is megnyílt a lehetőségek ablaka). Ugyanakkor a távmunka terén a vizsgált időszakban nyílt meg először a lehetőségek ablaka, a WHO korábbi ajánlása ellenére ez a terület kevés figyelmet kapott.

Rámutattunk továbbá, hogy a vizsgált időszakban megszületett szabályok, mint megoldások a pénzintézetek nyújtotta alapvető szolgáltatások digitalizációjának jelenségére és a biztonságos működésre helyezik a hangsúlyt. Az ügyfeleket érő kibertámadásokra válaszul külön szabályozás nem jelent meg a vizsgált időszakban, ezt a kérdést részletesen nem tárgyalják a megjelent szabályok.

FELHASZNÁLT IRODALOM

[1] Faramondi, L., Oliva, G. and Setola, R. "Multi-criteria node criticality assessment framework for critical infrastructure networks." *International Journal of Critical Infrastructure Protection*, 28, 2020, https://doi.org/10.1016/j.ijcip.2020.100338

[2] Besenyő J., Sinkó G. „Terrorist Organizations' Activities Against Crucial Installations: Al-Shabaab's Attacks on Critical Infrastructure in Kenya", In: Besenyő, János;

Khanyile, Moses B.; Vogel, David (szerk.) *Terrorism and Counter-Terrorism in Modern Sub-Saharan Africa*, Cham, Svájc : Springer Nature Switzerland (2024) pp. 169-193. https://doi.org/10.1007/978-3-031-56673-8_8

[3] Márton Z., Rajnai Z. „A social engineering fejlődése és jövője: a pszichológiai sebezhetőségek kihasználása a digitális korban”, *Biztonságtudományi Szemle*, 6(4), 2024. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/525

[4] Teknős L. „Természeti katasztrófák tendenciális változásainak elemzése, értékelése”, *Belügyi Szemle*, 72(2), 2024. https://doi.org/10.38146/BSZ.2024.2.5

[5] Bándi Gy. „A teremtésvédelem egyetemessége“ In: Komáromi L., Szabó P., Birher N., Cserey Gy., Puskás A. (szerk.) *Munus et dilectio*. Pázmány Press, Budapest, pp. 75-83. (2024) ISBN 9789633085028

[6] Földi L., Halász L. „Investigation of Climate Vulnerability of Domestic Natural and Artificial Ecosystems”, *Hadmérnök*, 14(2), 2019. https://doi.org/10.32567/hm.2019.2.14

[7] Demény, Á., Tollár, T., Endrődi, I. „Biztonsági, nemzetbiztonsági kihívások hatásai a Magyarországi nemzetgazdaságra”, *Polgári Védelmi Szemle*, XVI, 2024. https://mpvsz.hu/pvszemle/

[8] Lentner Cs. „Ezüstkor”, *Polgári Szemle*, 19(1–3), 2023. https://doi.org/10.24307/psz.2023.0901

[9] Mandic, D., Kiss, G., Rajnai, Z. „Password Usage among Users of Smart Devices in Hungary and Serbia”, *2024 IEEE 18th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, Timisoara, Romania, 2024. https://doi.org/10.1109/SACI60582.2024.10619863

[10] Europol. „COVID-19 sparks upward trend in cybercrime” Press release 5 October 2020. https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime

[11] Gulyás O., Kiss G. „Kiberbiztonság 2021-ben a bankszektorban és a pénzügyi szervezeteknél”, *Biztonságtudományi Szemle*, 4(1), 2022. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/205/181

[12] European Central Bank. „Supervision newsletter, IT and cyber risk: a constant challenge”, 18 August 2021, https://www.bankingsupervision.europa.eu/press/publications/newsletter/2021/html/ssm.nl210818_3.en.html

[13] Brožič L. „Modern Warfare”, *Contemporary Military Challenges*, 26(3), 2024. https://doi.org/10.2478/cmc-2024-0017

[14] Pavel Tal „Avoiding a ‘Digital 7 October’: a study on cyberwarfare against Israel during the October 2023 war”, *Contemporary Military Challenges*, 26(3), 2024. https://doi.org/10.2478/cmc-2024-0022

[15] Horváth D. „The background of the Russian-Ukrainian war in terms of new methods and warfare”, *National Security Review*, 2024/1, https://www.knbsz.gov.hu/hu/letoltes/szsz/2024_1_NSR.pdf

[16] Reveron, D.S., Savage, J.E. „Cybersecurity Convergence: Digital Human and National Security”, *Orbis*, 64(4), 2020. https://doi.org/10.1016/j.orbis.2020.08.005

[17] Lendvai T. „A Kínai Népköztársaság feltételezett kiberhírszerzési műveleteinek értékelése: eljárások és a nemzetközi hatások áttekintése”, *Nemzetbiztonsági Szemle*, 12(2), 2024. https://doi.org/10.32561/nsz.2024.2.4

[18] Strucl, D. „Russian aggression on Ukraine: cyber operations and the influence of cyber space on modern warfare”, *Contemporary Military Challenges*, 24(2), 2022. https://doi.org/10.33179/bsv.99.svi.11.cmc.24.2.6
[19] Besenyő J. „Újfajta háború? Internetes hadviselés Grúziában”, *Sereg Szemle*, 6(3), 2008.
[20] Kovács L. „Nyomásgyakorlás a kritikus információs infrastruktúrák támadásán keresztül: A Digital Pearl Harbortól a digitális ökoszisztéma teljes támadásáig”, In: Krasznay Csaba (szerk.) *Taktikák és stratégiák a kiberhadviselésben*, Budapest, Magyarország : Ludovika Egyetemi Kiadó (2023) 304 p. pp. 151-168.
[21] Dér A., Busa A. „Kritikus információs infrastruktúra rendszerei ellen intézett támadási trendek”, *Biztonságtudományi Szemle*, 6(1), 2024. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/434
[22] Pál A.B. „Információs műveletek és információs hadviselés”, *Biztonságtudományi Szemle*, 5(1), 2023. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/308
[23] Jagodics I., Kollár Cs. „21. századi social engineering támadások, védekezés és szervezeti hatások Európában”, *Belügyi Szemle*, 71(1), 2023. https://doi.org/10.38146/BSZ.2023.1.6
[24] Beregi A.L., Babos T. „Security and Military Relevancies of Digitisation, Globalisation and Cyberspace”, *Academic and Applied Research in Military and public management Science*, 20(1), 2021. https://doi.org/10.32565/aarms.2021.1.6
[25] Kovács L. „National cyber security as the cornerstone of national security”, *Revista Academiei Fortelor Terestre*, 23(2), 2018. https://doi.org/10.2478/raft-2018-0013
[26] Csiki Varga T., Tálas P. „Erő és diplomácia – Az Egyesült Államok stratégiai érdekei és lehetőségei a Biden-kormányzat időszakában”, *Nemzet és Biztonság*, 2022/1, 2022. https://doi.org/10.32576/nb.2022.1.2
[27] Vass Gy., Ambrusz J., Restás Á., Varga F., Kátai-Urbán L. „A katasztrófavédelmi kutatások eredményei és fejlesztése a rendészettudomány rendszerében”, *Belügyi Szemle*, 72(5), 2024. https://doi.org/10.38146/BSZ-AJIA.2024.v72.i5.pp815-833
[28] Bakos T., Pető R. „A biztonságtechnikai mérnöki képzés múltja és jövője”, *Műszaki Katonai Közlöny*, 34. évf. különszám, 2024. https://doi.org/10.32562/mkk.2024.ksz.15
[29] Bederna Zs., Rajnai Z. „Review of the advacement of critical information infrastructures and their structural analysis”, *National Security Review*, 2020/2, 2020. https://www.knbsz.gov.hu/hu/letoltes/szsz/2020_2_NSR.pdf
[30] Bakos T. „A létfontosságú rendszerek azonosításáról, kijelöléséről és védelméről szóló hatályos magyar jogi dokumentumok”, *Műszaki Katonai Közlöny*, 34. évf., különszám, 2024. https://doi.org/10.32562/mkk.2024.ksz.17
[31] Kenesey Zs., Pataki L., Tóth R. „A banki szabályozói követelmények szigorításának hatása az Európai Unió bankszektorának jövedelmezőségére és a nemteljesítő hitelek arányára”, *Polgári Szemle*, 17(1–3), 2021. https://doi.org/10.24307/psz.2021.0710
[32] Gulyás O., Kiss G. „Cybersecurity threats in the banking sector”, *2022 8th International Conference on Control, Decision and Information Technologies (CoDIT)*, Istanbul, Turkey, 2022. https://doi.org/10.1109/CoDIT55151.2022.9804140
[33] Ubaldo, A.L.V., Barreto, V.Y.G., Albines, J.A.B., Andrade-Arenas, L., Bellido-García, R.S. „Information Security in the Banking Sector: A Systematic Literature Review

on Current Trends, Issues, and Challenges", *International Journal of Safety and Security Engineering*, 13(1), 2023. https://doi.org/10.18280/ijsse.130111
[34] MNB. „Fizetési Rendszer Jelentés 2021". 2021. ISSN 2498-7077 https://www.mnb.hu/letoltes/fizetesi-rendszer-jelentes-2021.pdf
[35] Kern, F., Rogge, K.S. „Harnessing theories of the policy provess for analysing the politics of sustainability transactions: a critical survey", *Environmental Innovation and Societal Transitions*, 27, 2018. https://doi.org/10.1016/j.eist.2017.11.001
[36] Demszky A. „A tapasztalat alapú tudás szerepe a politikai döntéshozatalban" In: Erőss, Gábor és Berényi, Eszter és Neumann, Eszter, (szerk.) *Tudás és politika: A közpolitikaalkotás gyakorlatának nyomában*, L'Harmattan, Budapest, 2013, ISBN 978 963 963 236 651 7
[37] Nagy R., Boda P. „Security policy and social challenges of epidemics in our days", *Polgári Védelmi Szemle*, XIV., 2022. https://mpvsz.hu/pvszemle/
[38] Petri B. „Az Európai Parlament működése a koronavírus-járvány idején: valódi megoldás-e a távmegoldás?", *Európai Tükör*, 23(3), 2020. https://doi.org/10.32559/et.2020.3.4
[39] Zellei G. „Veszélyes üzemek humán kockázatai: összefüggések, hazai helyzet, és a közeljövő feladatai", *Polgári Védelmi Szemle*, XIII., 2020. https://mpvsz.hu/pvszemle/
[40] Domokos L. „A koronavírus-járvány közpénzügyi kihívásai és a számvevőszéki válaszok", *Polgári Szemle,* 17(4-6), 2021. https://doi.org/10.24307/psz.2021.1204
[41] Posgay I., Regős G., Horváth D., Molnár D. „A koronavírus-járvány gazdasági hatásairól", *Polgári Szemle*, 16(4–6), 2020. https://doi.org/10.24307/psz.2020.1004
[42] Vida Cs. „A koronavírus-járvány hatása a biztonságra - paradigmaváltás a biztonsági rendszerben", *Felderítő Szemle*, 19(1), 2020. https://www.knbsz.gov.hu/hu/letoltes/fsz/2020-1.pdf
[43] Sabelli, C. „Le epidemie estreme sono più probabili di quanto si pensasse", *Nature Italy*, 2021, https://doi.org/10.1038/d43978-021-00106-6
[44] Horváth Z., Tóth R. „A stratégiai szabályozás elméleti és gyakorlati kérdései a hivatásos katasztrófavédelemnél", *Katonai Logisztika*, 31(3-4), 2023. https://doi.org/10.30583/2023-3-4-185
[45] Simon M. „A COVID-19 munkabiztonsága", *Biztonságtudományi Szemle*, 4(2), 2022. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/227/197
[46] Shatnawi, M., Rajnai, Z. "Assessment of the impact of the covid-19 crisis on transportation and mobility – analysis of applied restrictions", *Interdisciplinary Description of Complex Systems*, 21(4), 2023. https://doi.org/10.7906/indecs.21.4.6
[47] Jónás K. „A koronavírus-járvány hatása a magyar közigazgatásra, különös tekintettel a pártfogó felügyelői eljárásokra", *Belügyi Szemle*, 72(4), 2024. https://doi.org/10.38146/bsz-ajia.2024.v72.i4.pp611-628
[48] Altaleb, H., Shatnawi, M., Rajnai, Z. „Digital Education: Governments' Strategies, Teaching Tools in the European Union and a Case Study of Digital Transformation in Budapest", *Interdisciplinary Description of Complex Systems*, 21(2), 2023. https://doi.org/10.7906/indecs.21.2.3
[49] Kádár Z., Rácz A. „A Covid19-járvány hatásai a társadalmi jóllét tekintetében - avagy miként adaptálódtak a járvány szülte új kívánalmakhoz a szegedi egyetemisták 2020

tavaszán", In: Szécsi Gábor, Tóth I. János (szerk.) *Társadalom a világjárvány hálójában : Alkalmazott filozófiai tanulmányok a pandémia társadalmi és kulturális hatásairól*. Budapest, Magyarország: Gondolat Kiadó (2023) 227 p. pp. 189-202.

[50] MNB. „Fintech és digitalizációs jelentés", 2021. ISSN 2732-3137 https://www.mnb.hu/letoltes/fintech-e-s-digitaliza-cio-s-jelente-s-2021.pdf

[51] Boros A., Lentner Cs., Nagy V., Tőzsér D. „Perspectives by green financial instruments – a case study in the Hungarian banking sector during COVID-19", *Banks and Bank systems*, 18(1), 2023. https://doi.org/10.21511/bbs.18%281%29.2023.10

[52] Katona G. „A Covid-19 kiberbiztonsági kihívásai az első hullám idején", *Hadmérnök*, 16(3), 2021. https://doi.org/10.32567/hm.2021.3.12

[53] MNB. „A magyar pénzügyi szektor kiberfenyegetettségi térképe 2022", 2022. ISSN 2939-7383 https://www.mnb.hu/letoltes/kiberfenyegetettsegi-terkep-2022.pdf

[54] MNB. „Állásfoglalás az elektronikus csatornákon keresztül előterjesztett panaszok minősítéséről", 2020. https://alk.mnb.hu/data/cms2483747/tmpCB06.tmp(25189558).pdf

[55] WHO. „Pandemic Influenza Preparedness And Response", 2009. ISBN 9789241547680, https://www.who.int/publications/i/item/9789241547680