GAZDASÁG ÉS PÉNZÜGY • 10. ÉVF. 2. SZ. • 2023. JÚN. • DOI: 10.33926/GP.2023.2.5

KIBERBIZTONSÁG ÉS A MESTERSÉGES INTELLIGENCIA KAPCSOLATA

Bagó Péter[1]

ABSZTRAKT

A kiberbiztonság az egyik legfontosabb kihívás az információs technológia korában, amely különösen fontos a pénzügyi szektorban, ahol a biztonság kulcsfontosságú az ügyfelek és az intézmények számára egyaránt. Az adatvédelem, a csalás elleni küzdelem és a kibertámadások elhárítása mind-mind olyan terület, ahol a mesterséges intelligencia és az automata rendszerek jelentős segítséget nyújthatnak. Az AI és a gépi tanulás alkalmazása a kiberbiztonság terén lehetővé teszi a rendszerek gyors és hatékony helyreállítását a kibertámadások után. Az AI-algoritmusok segítségével a szakemberek képesek lesznek a károk mértékének azonnali felmérésére, és az AI segítségével azonnal reagálni tudnak a kiberincidensekre. Az alábbi cikkben bemutatjuk a kibervédelem mesterséges intelligenciával történő támogatását a pénzügyi szektorban. Az átfedések jelentős mértékűek az infrastrukturális védelemmel, az egyéni biztonsági szintekkel és az adatok megfelelő védelmével.

JEL-kódok: G00, O33, Q55

Kulcsszavak: mesterséges intelligencia, kibervédelem, pénzügyi szektor, fintech

1. KIBERBIZTONSÁG A PÉNZÜGYI SZEKTORBAN

Lényeges megkülönböztetni a kiberbiztonságot és annak alkalmazását a mesterséges intelligenciával párosítva, de előtte érdemes áttekinteni a 2023-ban fontos biztonsági szabályokat, amelyeket minden pénzügyi szolgáltatást használónak be kellene tartani:

- Erős jelszavak használata: fontos, hogy minden felhasználó használjon erős jelszavakat a fiókjaihoz. Az erős jelszavak tartalmaznak kis- és nagybetűket, számokat, valamint speciális karaktereket, és legalább 8 karakter hosszúak.

1 *Bagó Péter* egyetemi adjunktus, tanszékvezető, Budapesti Corvinus Egyetem, Vállalkozás és Innováció Intézet, Innováció és Üzleti Inkubáció Tanszék. E-mail: peter.bago@uni-corvinus.hu.

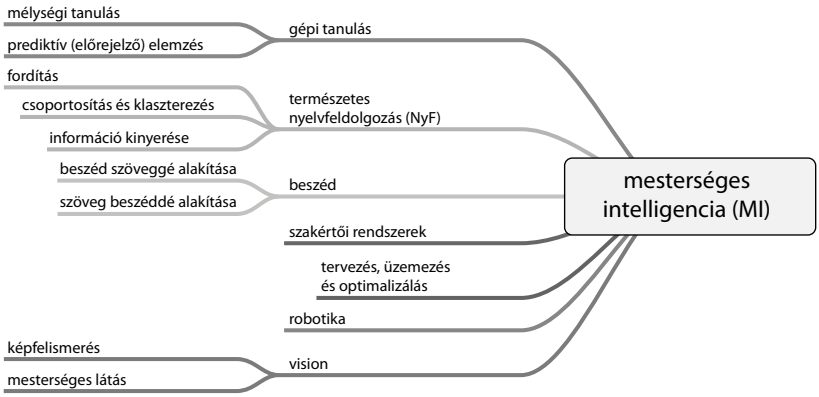
- Kétlépcsős azonosítás: a kétlépcsős azonosítás nagyon fontos a kiberbiztonság szempontjából. Ez azt jelenti, hogy az azonosítás során két különböző faktor használatával kell igazolni az azonosságot, például a jelszó mellett egy egyedi kóddal vagy ujjlenyomattal.
- Szoftverfrissítések: minden szoftverfrissítést telepíteni kell, hogy biztonságban legyenek a számítógépünk és az adataink.
- Tűzfal és vírusvédelem: fontos, hogy a számítógépen és a hálózaton tűzfal és vírusvédelem legyen telepítve, hogy megakadályozzák a kártékony szoftverek behatolását.
- Adatmentés: az adatok rendszeres biztonsági mentése fontos, hogy biztosítva legyen az adatok megőrzése egy esetleges adatvesztés vagy kár esetén.
- Felhasználói oktatás: az alkalmazottak oktatása és felvilágosítása a kiberbiztonsági kockázatokról és a helyes biztonsági gyakorlatokról kulcsfontosságú a szervezet biztonsága szempontjából.
- Állandó monitorozás: a kiberbiztonság folyamatos monitorozása fontos annak érdekében, hogy időben észrevehetőek legyenek a veszélyek, és megfelelően lehessen reagálni.

Ha megvizsgáljuk, a mesterséges intelligencia miben segíthet a pénzügyi szektoron, akkor a lista sokkal szélesebb körű, ugyanakkor azt is lehet mondani, alapvető infrastrukturális kérdéseket feszeget:

- Észlelés és reakció: az AI-rendszerek képesek nagy mennyiségű adatot gyűjteni és elemezni a rendszerek biztonsága érdekében. Ezen felül képesek azonosítani azokat a veszélyeket, amelyeket a hagyományos biztonsági rendszerek könnyen elmulasztanának, és riasztást küldeni a megfelelő személyeknek.
- Jelentéskészítés: az AI képes olyan jelentéseket készíteni, amelyek segítenek a kiberbiztonsági csapatoknak jobban megérteni a rendszerek sebezhetőségeit, illetve azokat a területeket, amelyekre kiemelt figyelmet kell fordítani.
- Automatizált válaszok: az AI segítségével olyan automatizált válaszokat lehet létrehozni, amelyek azonnal reagálnak a biztonsági fenyegetésekre. Például ha egy biztonsági esemény történik, az AI-rendszer képes lehet automatikusan megváltoztatni a jelszavakat, letiltani a fiókokat vagy visszavonni a hozzáféréseket.
- Folyamatos tanulás és frissítés: az AI-algoritmusok folyamatosan tanulnak az előző tapasztalatok alapján, és frissülnek a legújabb kiberbiztonsági fenyegetésekkel kapcsolatos információkkal. Ez lehetővé teszi, hogy az AI-rendszerek mindig naprakészek legyenek, és megfelelően reagáljanak a legújabb kihívásokra.

- Hálózati biztonság: az AI képes az összes hálózati forgalmat ellenőrizni, azonosítani és elemezni, hogy azonosítsa azokat a potenciális fenyegetéseket, amelyek más módon könnyen elkerülhetők lennének. Ezen felül az AI-rendszerek képesek a hálózatokat folyamatosan monitorozni, és ellenőrizni a biztonsági szinteket.
- Átfogó elemzés: az AI képes összehasonlítani a nagy adatmennyiségeket, és elemzéseket végrehajtani a rendszeren belül. A rendszeren belül felderíti azokat az anomáliákat, amelyek a hagyományos biztonsági rendszerek számára nehezen vagy egyáltalán nem azonosíthatók.
- Adathalászat észlelése: az AI lehetővé teszi az adathalász támadások észlelését és a hamis e-mailek, weboldalak, alkalmazások azonosítását, így segítve a vállalatokat a biztonságosabb adatkezelésben.
- Felhőalapú biztonsági megoldások: az AI és a felhőalapú technológiák együttes használatával a vállalatok javíthatják a biztonsági megoldásaikat, mivel a felhőalapú rendszerek hatékonyabban képesek kezelni a nagy mennyiségű adatokat, és azonnali reakcióra képesek az esetleges biztonsági incidensek esetén.
- Intelligens hálózatvédelem: az AI alkalmazása a hálózatvédelem terén lehetővé teszi a kibertámadások felderítését és megakadályozását. Az intelligens hálózatvédelem képes automatikusan azonosítani és megállítani a kibertámadásokat, valamint lehetővé teszi a hálózat folyamatos monitorozását és a gyors reagálást a biztonsági incidensekre.
- Magasabb szintű autentikáció: az AI segítségével a vállalatok erősíthetik az autentikációt azonosítási és hitelesítési megoldásokkal. Az arc- és hangazonosítás, biometrikus adatok és más innovatív megoldások alkalmazása a felhasználók azonosítását és hitelesítését teszi könnyebbé és hatékonyabbá, ezzel növelve a biztonságot.
- Gyorsabb és hatékonyabb válaszreakció: az AI lehetővé teszi a gyorsabb és hatékonyabb reakciókat a biztonsági incidensekre. Az automatikus esemény- és biztonsági incidenskezelő rendszerek képesek azonnal jelentést készíteni az eseményekről, valamint lehetővé teszik a gyors beavatkozást és a hibaelhárítást, csökkentve ezzel a káros hatásokat.

1. ábra
A mesterséges intelligencia fejlődése



Forrás: Ray, 2022

A kiberbiztonság rendkívül fontos a pénzügyi szektorban a pénzügyi adatok érzékeny és bizalmas jellegéből adódóan. Az utóbbi években az elemzők azt tapasztalták, hogy a mesterséges intelligencia használata a kiberbiztonságban egyre népszerűbb, és sok pénzügyi intézmény az AI segítségével erősíti kiberbiztonsági képességeit. Az AI lehetőségei átalakíthatják a kiberbiztonsági tájképet a pénzügyi szektorban. Az AI-t lehet használni nagy mennyiségű adat elemzésére, észlel anomáliákat és mintákat, amelyek jelzik a kiberfenyegetéseket. A gépi tanulási algoritmusok képzése segíthet abban, hogy felismerjük a csalási tevékenységre utaló viselkedésmintákat, például a phishingtámadásokat, a zsarolóvírus-támadásokat és az azonosítási csalásokat. Az AI-t lehet használni a fenyegetések észlelésének és az azonnali válaszadás sebességének és pontosságának a növelésére. A hagyományos kiberbiztonsági rendszerek szabályokon alapuló algoritmusokra támaszkodnak, amelyek előre programozva érzékelik a konkrét fenyegetéseket. Azonban ezek a rendszereket könnyen megkerülhetik azok a támadók, akik új és fejlődő támadási technikákat használnak. Az AI-alapú kiberbiztonsági rendszerek képesek alkalmazkodni és tanulni az új fenyegetésektől, ami hatékonyabbá teszi a kiberfenyegetések észlelését és enyhítését. Továbbá, az AI-alapú biztonsági rendszerek valós idejű fenyegetési információkat nyújthatnak a pénzügyi intézményeknek, lehetővé téve számukra, hogy gyorsan reagáljanak a kiberfenyegetésekre. Az AI-t lehet használni a biztonsági feladatok automatizálására is, felszabadítva a kiberbiztonsági szakembereket az olyan összetettebb feladatokra, amelyek emberi szakértelmet igényelnek.

Az AI használatával kapcsolatban felmerülnek aggodalmak is, különösen a pénzügyi intézmények szempontjából. Az egyik legnagyobb aggodalom az AI meg-

bízhatósága, amely szintén összefügg a felelősségvállalással. Az AI-rendszerek működése olyan adatokon alapul, amelyeket korábban bevittünk, és ha ezek az adatok torzultak vagy hibásak, az AI nem működik megfelelően. Az AI használata a kiberbiztonságban szintén magában foglalja a megfelelő adatvédelmi intézkedések alkalmazását. A pénzügyi intézményeknek biztosítaniuk kell, hogy a AI által kezelt adatok védettek legyenek, és a felhasználói jogokat és az adatok hozzáférhetőségét szigorúan ellenőrizzék. Az AI-alapú kiberbiztonsági rendszerek képesek azonosítani a fenyegetéseket, és azokat azonnal és hatékonyan elhárítani, csökkentve ezzel a kockázatot és a veszteséget a pénzügyi intézmények számára. A fenyegetések gyorsabb és pontosabb azonosítása végett az AI alkalmazásával a kiberbiztonsági szakemberek időt és energiát takaríthatnak meg, lehetővé téve számukra, hogy a többi feladatra koncentráljanak. Összességében elmondható, hogy az AI jelentős előnyöket kínál a pénzügyi szektorban a kiberbiztonság terén. Az AI segítségével a pénzügyi intézmények képesek azonosítani a kockázatokat és azokat gyorsan és hatékonyan elhárítani, csökkentve a veszteségeket és javítva a pénzügyi intézmények ügyfélélményét. Az AI alkalmazása azonban szigorú adatvédelmi és felelősségbiztosítási intézkedéseket igényel, hogy biztosítsa a pénzügyi intézmények és az ügyfelek biztonságát.

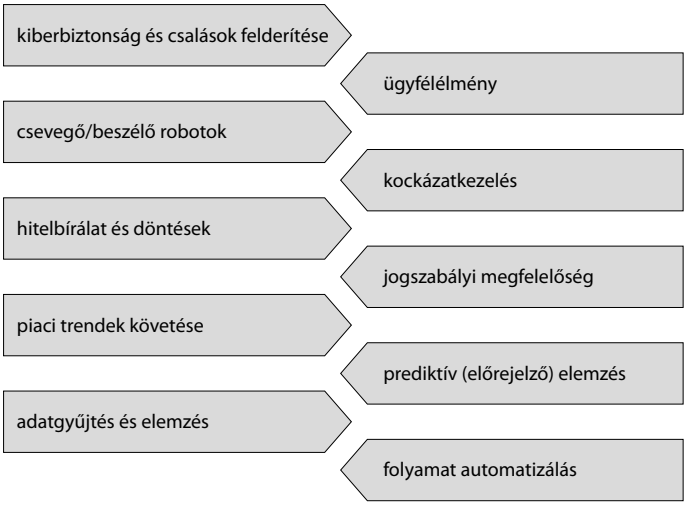
A gépi tanulás segítségével az algoritmusok képesek az adatok feldolgozására és azokból tanulni, ami lehetővé teszi az automatizálást és a hatékonyság növelését. A mesterséges intelligencia pedig lehetővé teszi a gépi tanulás által generált adatok intelligens felhasználását a döntéshozatali folyamatokban, valamint az emberi intelligencia szintjének elérését a pénzügyi területeken. Összességében mindkét technológia fontos szerepet játszik a pénzügyi területeken, és együttesen alkalmazva hatékonyabbá és eredményesebbé tehetik az adatok elemzését és feldolgozását a pénzügyi szolgáltatások nyújtásában (Ray, 2022; *Pintér*, 2008).

A következő, *2. ábra* a banki szektorban alkalmazott AI-alkalmazások öt fő kategóriáját mutatja be.

- Az *első kategóriában* a chatbotok és a virtuális asszisztensek szerepelnek, amelyek a bankok ügyfeleinek személyre szabott szolgáltatásokat nyújtanak a vásárlások kezelésétől az átutalásokig.
- A *második kategória* a csalásellenes AI-technológiákat mutatja be, amelyek segítenek azonosítani és csökkenteni az átverések és csalások kockázatát.
- A *harmadik kategóriában* az automatizált döntéshozatali rendszerek találhatóak, amelyek segítségével a bankok hatékonyabban tudják kezelni a nagy mennyiségű adatokat, és előrejelzéseket készíteni az üzleti döntésekhez.
- A *negyedik kategória* a robothitelesítés, amelynek a célja az emberi munkaerő megtakarítása és a folyamatok hatékonyságának javítása.

– Az *ötödik* és utolsó *kategóriában* az AI-alapú érzékelési technológiákat mutatják be, mint például az arc- és ujjlenyomat-azonosítást, amelyek javítják az azonosítási folyamatokat, és biztonságosabbá teszik a banki tranzakciókat.

2. ábra
A banki szektorban alkalmazott AI-technológiák



Forrás: Appinventiv, 2023

Az AI egyik legfontosabb alkalmazása a banki ügyfélszolgálatban érvényesül. A bankok chatbotokat és hangasszisztenseket használnak, hogy éjjel-nappal vásárlói támogatást és segítséget nyújtsanak. Ezek a virtuális asszisztensek AI- és természetes nyelvfeldolgozási (NLP) technológiával működnek, amelyek lehetővé teszik számukra, hogy megértsék a vásárlói kérdéseket, és releváns válaszokat adjanak. Ez nemcsak javítja a vásárlói élményt, hanem csökkenti az emberi ügyfélszolgálati ügynökök munkaterhelését is. A bankok AI-jal működő algoritmusokat alkalmaznak, hogy érzékeljék és csökkentsék a különböző típusú kockázatokat, például a hitelkockázatot, piaci kockázatot és működési kockázatot. Az AI-algoritmusok nagy adatmennyiségek elemzésével képesek azonosítani az esetleges kockázatokat jelző mintázatokat és anomáliákat. Ez segíti a bankokat az informált döntések meghozatalában és a veszteségek csökkentésében.

Az AI-t továbbá a csalások észlelésére is használják a banki szektorban. Az AI-alapú csalásérzékelő rendszerek valós időben képesek elemezni a tranzakciós adatok nagy mennyiségét és észlelni a gyanús tevékenységet. Ez segíti a ban-

kokat a korai csalások észlelésében és a veszteségek megelőzésében. Az AI-t az értékpapírpiaci előrejelzésben is alkalmazzák. Az AI-algoritmusok képesek az elemzett piaci adatok alapján előrejelzéseket adni a részvényárakról és más piaci mutatókról. Ez segíti a befektetőket abban, hogy informáltabb döntéseket hozzanak a portfólióik kezelésével kapcsolatban.

1.1. Kiberbiztonsági trendek

Számos kihívás létezik ezen a téren, az egyik ilyen kihívás a személyes adatok védelme és az adatbiztonság. Az AI a nagy adatmennyiségek elemzésével működik, amelyek jelentős mennyiségű személyes adatot tartalmaznak. Ezért az AI alkalmazása során a bankoknak és a pénzügyi intézményeknek gondoskodniuk kell az adatvédelemről és az adatbiztonságról. Az AI egyre inkább kulcsszereplővé válik a digitális transzformáció folyamatában. Az AI által biztosított előnyök, mint a hatékonyság és a kockázatkezelés javítása, segítenek a bankoknak az új digitális technológiák bevezetésében és az ügyfélélmény javításában. Az AI alkalmazása jelentős előnyöket biztosít a bankok számára, beleértve a hatékonyság és a kockázatkezelés javítását, valamint a vásárlói élmény fokozását. Azonban az AI alkalmazása során felmerülő kihívásokat és az emberi munkaerőre gyakorolt hatásokat is kezelni kell ahhoz, hogy az AI-t sikeresen be lehessen vezetni a banki szektorban (Appinventiv, 2023).

További kutatások is alátámasztják, hogy a kibertámadások növekvő tendenciát mutatnak, különösen a vállalatoknál és az állami szerveknél. Az automatizált és fejlett kiberfenyegetések, például a mesterségesintelligencia-alapú támadások várhatóan növekedni fognak 2023-ban. A Deloitte kutatása hangsúlyozza a fenyegetéskezelés, az incidenskezelés, az adatvédelem és az alkalmazottak kiberbiztonsági oktatásának fontosságát a vállalatok számára az eredményes kiberbiztonsági stratégiák kialakításában és végrehajtásában. Emellett részletesen foglalkozik az adatvédelem jogszabályi és szabályozási változásaival, valamint az üzleti és technológiai trendekkel, amelyek befolyásolhatják a kiberbiztonsági környezetet 2023-ban (Deloitte, 2023).

A McAfee szerint is fokozódni fognak a kibertámadások, különösen az ipari szektorban, az oktatásban és az egészségügyben. Az új technológiák, például az IoT- (Internet of Things) eszközök és az 5G hálózatok elterjedése újabb biztonsági kihívásokat jelent majd. A fenyegetések között említik a mesterségesintelligencia- és gépitanulás-alapú támadásokat, a közösségi hálózatokon való manipulációt és a ransomware-támadások további terjedését. A McAfee kifejti a szervezetek előrejelzések alapján felállított proaktív kiberbiztonsági intézkedéseinek jelentőségét, beleértve az erősített azonosítást, az oktatást és az incidenskezelési képességek

fejlesztését a sikeres védekezés érdekében. Továbbá hangsúlyozza a szervezetek közötti együttműködés és információcsere fontosságát a fenyegetések hatékony megelőzéséért és a sikeres reagálásért (McAfee, 2023).

Az Accenture (2023) úgy gondolja, a bankok általában jobb védelmet biztosítanak a külső támadások ellen, de a belső veszélyekre való felkészültségük alacsonyabb. A kutatás szerint (Accenture, 2023) az adatok védelme és a jogosulatlan hozzáférés elleni védelem továbbra is az elsődleges kihívás a bankok számára.

Az egész pénzügyi szektor érintett; az Allianz minden évben kiad egy „Allianz Risk Barometer" jelentést, amelyben az egyik legkomolyabb támadás a „business interruption", vagyis amikor leállítják az üzletmenetet. Alapvetően egy túlterheléses támadás is ebbe a kategóriába eshet, ezért ez inkább csak a jelenlegi támadások másik nézőpontból való megközelítése.

Ugyanakkor az Allianz jelentése azt is jelzi, hogy nemcsak a banki szektor, hanem az egész pénzügyi szektor áll a támadások fókuszában (Allianz, 2023). A CyberEdge (2023) szerint 2023-ban tovább növekszik majd az adatvédelmi és biztonsági szabályozások szigorúsága, különösen az Európai Unióban, ahol az adatvédelmi alaprendelet (GDPR) továbbra is hatással lesz az üzleti szektorra. Az adatvédelem fontossága továbbra is növekedni fog, és a vállalkozásoknak szigorúbb védelmi intézkedéseket kell bevezetniük az adatveszteség, az adathalászat és más kibertámadási típusok elleni védelem érdekében.

A CyberEdge is kiemeli, hogy az okoseszközök és az IoT-eszközök jelentős biztonsági kihívásokat fognak okozni 2023-ban. Az okosotthonok, az ipari és az egészségügyi IoT-eszközök gyors térnyerése azt eredményezi, hogy azokat a támadók is gyakran használják célzott kibertámadásokhoz. A távmunka továbbra is népszerű és széles körben alkalmazott munkamódszer marad 2023-ban, azonban a távmunka biztonsági kockázatai továbbra is fennállnak, és a szervezeteknek biztosan megnövekedett költségeket jelenthet a távmunkához tartozó eszközök biztonságossá tétele (CyberEdge, 2023).

Vannak olyan kutatások is, amelyek szerint az ember, pontosabban az alkalmazottak vannak a támadások fókuszában, nem pedig a rendszerek. Gondolnak itt olyan támadásokra, amelyek az e-maileket vagy a felhő-előfizetéseket kompromittálják (Proofpoint, 2023). Ehhez a gondolkodáshoz kapcsolódhat az ESET kutatása is, amely szerint a kiberbiztonsági trendek 2023-ban a szép új hibrid világban elmosódó határvonalakat hoznak létre, komplex problémákat jelentenek az adatbiztonság és a magánélet védelme terén, valamint a munka és a szociális élet egyre szorosabb összekapcsolódását jelentik (ESET, 2023). A TÜV SÜD szerint 2023-ban a legfontosabb tényezők közé tartoznak a költséghatékony kiberbiztonsági megoldások, a szabályozás megkezdése a digitális bizalom szabványosítása segítségével, a célcsoport-orientált képzés és a kritikus infrastruktúra

(KRITIS) fókuszba kerülése (TÜV, 2023). A Microsoft kiberbiztonsági szakértője, *Paula Januszkiewicz* szerint 2023-ban a kiberbiztonságot érintő legfontosabb változások a fenyegetésekre történő felkészültség körül fognak sűrűsödni. A szervezeteknek folyamatosan készen kell állniuk egy támadásra, behatolási kísérletre, és rendelkezniük kell azokkal az eszközökkel, amelyekkel ezeket kontroll alatt képesek tartani. Az év másik kiemelt témája a privilegizált hozzáférés és a felhasználóazonosítás szigorú ellenőrzése lesz (Microsoft, 2023).

2. PÉNZMOSÁS ÉS A MESTERSÉGES INTELLIGENCIA

A pénzmosás nagy hatással van a globális pénzügyi rendszerre, és a Nemzetközi Valutaalap (IMF) becslései szerint évente mintegy 2–5 milliárd dollár értékű pénzt mosnak tisztára a világon. Ez azt jelenti, hogy a pénzmosás mértéke magasabb lehet, mint más pénzügyi csalásoké, például az adóelkerülésé vagy az értékpapír-manipulációé. Ezért ha a mesterséges intelligencia a fenti érték töredékét megvédi, a bűnmegelőzés terén olyan előrelépést mutathatnak fel az államok, a szervezetek, a vállalatok és az egyének is, amely bőven megalapozza, hogy érdemes ezzel kiemelten foglalkozni. A kibervédelem és a pénzmosás közötti kapcsolat azon alapul, hogy a pénzmosók gyakran használnak kibertámadásokat, számítógépes csalásokat és más kiberbűnözési módszereket a tisztára mosott pénz elfedéséhez és azonosításának a megakadályozásához. Például a pénzmosók gyakran használnak hamis webhelyeket és számítógépes programokat a banki adatok, az ügyfél-azonosítók és a tranzakciók eltulajdonítására. Ezután ezeket az adatokat felhasználhatják hamis számlák nyitására, pénzátutalásokra vagy más pénzmosási módszerekre. A kibervédelem tehát kulcsfontosságú szerepet játszik a pénzmosás elleni harcban. A bankoknak és más pénzügyi intézményeknek szigorú biztonsági intézkedéseket kell alkalmazniuk a személyes és pénzügyi adatok védelme érdekében, valamint fel kell készülniük a kiberbűnözésre és az azt követő pénzmosásra. Azok az országok, amelyek magas szintű kibervédelmi képességgel rendelkeznek, könnyebben tudják felismerni és megakadályozni a pénzmosást és más pénzügyi bűncselekményeket. Ezért fontos a kibervédelemmel kapcsolatos oktatás és fejlesztés, hogy csökkentsük a kiberbűnözés és a pénzmosás kockázatát.

A McKinsey (*Biswas* et al., 2020) készítette tanulmány szerint az AI lehetővé teszi a bankok számára, hogy hatékonyabbá és eredményesebbé tegyék az üzleti folyamataikat, javítsák a termék- és szolgáltatásportfóliójukat, valamint növeljék a fogyasztói elégedettséget. Az AI használata számos előnyt jelent a bankok számára, mint például az ügyfélszolgálat javítása, a kockázatkezelés hatékonyságának növelése, a tranzakciók felügyelete és a csalások megelőzése. Az elemzés hangsúlyozza, hogy az AI továbbfejlesztése segíthet a bankoknak abban, hogy

azonnali döntéseket hozzanak a tranzakciók felügyelete és a kockázatkezelés területén. Ezenkívül az AI használata lehetővé teszi a bankok számára, hogy személyre szabott és hatékony ajánlatokat tegyenek ügyfeleiknek. Az elemzés azt is megállapítja, hogy a bankoknak elő kell segíteniük az AI használatának terjedését a szervezetükben, és biztosítaniuk kell, hogy a szükséges erőforrások, technológiai képességek és szakértői tudás rendelkezésre álljanak. Emellett a bankoknak további kihívásokkal kell szembenézniük, mint például a személyes adatok védelme és a jogszabályi környezet. Az elemzés szerint az AI alkalmazása átfogó stratégiai megközelítést igényel a bankok részéről, amely lehetővé teszi az AI-rendszerek integrálását az üzleti folyamatokba, az alkalmazások szélesebb körű használatát, valamint az AI fejlesztési és működési költségeinek optimalizálását. Az AI-rendszerek és technológiák használata jelentős hatással lesz a bankokra és az ügyfeleikre, és hosszú távon azok a bankok, amelyek képesek lesznek az AI megfelelő alkalmazására, versenyképesebbek és sikeresek lesznek a piacon. A cikk következtetése az, hogy az AI-megoldásoknak fontos szerepe van a pénzügyi szolgáltatók jövőjében, mivel azok hatékonyabbá és ügyfélbarátabbá teszik a banki folyamatokat. Az AI segítségével a pénzügyi intézmények nagyobb pontossággal és hatékonysággal értékelhetik a kockázatokat, javíthatják az átfutási időt és fejleszthetik az ügyfélszolgálatot. Azonban a cikk rámutat arra, hogy az AI bevezetése jelentős kihívásokat is jelent, például az adatvédelem és a biztonság kérdéseit, valamint az új technológiákban való képzést és befektetéseket illetően. A cikk szerint a pénzügyi szolgáltatóknak fel kell készülniük az AI-megoldások kihívásaira és lehetőségeire ahhoz, hogy sikeresek legyenek a jövőben.

2.1. Mi a pénzmosás?

A pénzmosás egy olyan bűncselekmény, amelynek során az illegális eredetű pénzt átváltoztatják olyan pénzzé, amelyet úgy lehet feltüntetni, mintha törvényesen szerezték volna. Ez a folyamat azért fontos, hogy az illegális pénzek nyomait eltüntessék, és a pénz forrása és útja ne legyen nyomon követhető. Az illegális tevékenységből származó haszon eredetének leplezését jelenti a pénzmosási folyamat, és ez a bűncselekmény jelentős veszélyt jelent a gazdaságra és a társadalomra, mivel a pénzmosás hozzájárulhat a terrorizmus finanszírozásához és más bűncselekményekhez is. Ezért fontos, hogy az illetékes hatóságok és a pénzügyi intézmények figyeljenek, megakadályozzák a pénzmosást, és ennek érdekében megfelelő szabályozásokat és eszközöket alkalmazzanak (Wolters, 2018)

A pénzmosás folyamatát, azt, hogy miként is tud megvalósulni a pénz eredetének egyértelmű visszakövethetősége, vagyis a pénz legalizálásának útját egy háromfázisú modellel tudjuk szemléltetni. Ez a modell az Amerikai Egyesült Államokból származtatott. A folyamat lépései:

- Elhelyezés
- Rétegzés
- Integrálás (*Gál*, 2007).

Az első lépésben a tisztára mosni kívánt pénz – jellemzően készpénz – elhelyezése történik a pénzügyi rendszerben valamilyen formában. Jellemzően a cél a bankrendszer. Manapság erre a lépésre már világszerte felkészült a pénzügyi szektor. Mindig a legnagyobb indikátor és veszélyjelző a nagy összegű készpénz megjelenése. Ekkor a legfontosabb a pénz forrásáról valahogy meggyőződni, ami hitelesen igazolja, hogy milyen eredetű összeg fog a bankrendszerbe bekerülni. Sok esetben láthatunk adásvételi szerződést, végkielégítést, vagy akár családi örökséget is.

A folyamat második része a rétegzés. Ennek az a lényege, hogy bonyolult, több számlán, több érintett ügyfélen keresztüli tranzakciókat végeznek. Jellemzően több különböző banknál vezetett számlákon, akár különböző devizákban, több országot érintve, amelyeknél az sem baj, ha olyan országot is érintenek a tranzakciók, ahonnan nehezebb banki információkat szerezni. Ez a folyamat azért is fontos, mert bárki szeretné az átutalásokat visszakeresni, rengeteg erőfeszítésbe kerül, és sokszor közel lehetetlen az eredetét megtalálni. Egy-egy tranzakcióra lehet bekérni információt az ügyfelektől, de a teljes lánc visszafejtéséhez akár nemzetközi együttműködés is szükséges. Viszont ha az utalásoknak csak egy kis szeletét nézzük, csak annyit látunk, hogy egy ügyfél egy másiknak utalást teljesít, akár átlagos mértékűt, és ha van információnk az utalás hátteréről, készségesen válaszolnak, akár még számlákat, szerződést is be tudnak mutatni. Ezen a ponton már nehéz helyzetben van a pénzmosás-megelőzés.

A harmadik lépés az elhelyezés és a rétegzés után az integrálás, a második pontban sokáig forgatott összegek felvétele vagy befektetése. Ez valójában már az a lépés, amikor tiszta bevételként kerül feltüntetésre, vagy épp egy nagyobb értékű beruházást végez az ügyfél ebből a pénzből. Forrása tisztának mondható, hiszen az ellenkezőjére sincs bizonyíték. A mosógépes történetben ez az a lépés, amikor a könyvelő plusz, megnövekedett bevételként könyveli szét egy-két hónapra a hozzárakott pénzt. Nagyon sok esetben a folyamat készpénzfelvétellel zárul, adófizetéssel színezett, ezzel még inkább a legalitás látszatát keltve. Jellemző napjainkra is, hogy az ügyfelek az ATM maximális kapacitásának megfelelően több részletben felveszik a kívánt összeget, csak a fiókba vagy pénztárba ne kelljen bemenni, mert ott van egy számukra veszélyes tényező: a banki dolgozó, aki mint elsődleges pénzmosás-megelőzési védelmi vonal, bizony érdeklődni fog az összeggel kapcsolatban. A befizető automaták népszerűsége is jelentősnek mondható, hasonló okokból kifolyólag. Erre természetesen a bankoknak fel kell készülniük, és az eljárásrendben foglaltaknak megfelelően valamilyen szűrés alapján figyelniük szükséges rá.

A fenti folyamatból is jól látható néhány figyelmeztető jel: a legelső lépésben a készpénz elhelyezésénél nyílik a legnagyobb lehetőség arra, hogy megakadályozzák a folyamatot. A folyamat vége az esetek többségében szintén egy készpénzfelvétel vagy nagy értékű beruházás lesz. A pénzmosás-megelőzési folyamat nagyon nagy részét kell kitöltenie a tranzakciók eredetét és célját érintő vizsgálatoknak. Összességében kijelenthetjük, hogy a legnagyobb indikátor a pénzmosás jelenlétére a kiemelkedő készpénzforgalom.

2.2. Monitoring vagy filtering?

A fenti folyamatokból látható, hogy minél több, minél nagyobb számban szükséges az ügyfelek folyamatos figyelemmel kísérése, a tranzakciók vizsgálata.

Az MNB rendelete a következőképpen szabályozza a folyamatot:

„33. §:

automatikus szűrőrendszer: az ügyfél és az ügylet pénzmosás és terrorizmus finanszírozása szempontjából előzetes paraméterezés alapján történő, emberi beavatkozást nem igénylő leválogatására alkalmas informatikai rendszer."[2]

A fent idézett jogszabályban látható, hogy a szolgáltatóknak kötelessége szűrőrendszert alkalmazni, amely a pénzmosás-megelőzési tevékenységben támogatja, és emberi beavatkozás nélkül jelzések generálására alkalmas. Nagyon fontos ezzel kapcsolatban meghatároznunk, hogy mi a különbség a monitoring- és a filteringrendszer között.

A monitoringrendszer utólagos, úgynevezett posztmonitoring tevékenységre alkalmas. Ebben az esetben a megtörtént tranzakciókat utólagosan vizsgálja előre beállított szabályok, szcenáriók alapján. Ez a gyakorlatban úgy kivitelezhető, hogy az ügyfelek tranzakcióit folyamatosan betöltik a monitoringrendszerbe, amely megszűri azokat, és a beállított szabályoknak megfelelően jelzéseket, riasztásokat generál. Természetesen önmagában a rendszer még nem egy mesterséges intelligencia, amely egyértelműen meg tudja mondani számunkra, mi pénzmosás vagy mi nem az, azonban minél pontosabb beállításaink és szabálymeghatározásaink vannak, annál pontosabb szűrési eredményeket kapunk, és annál valószínűbb, hogy egy ilyen riasztás valós. Ennek egyetlen hátránya, hogy ilyen mélységű sza-

2 26/2020-as (VIII.25.) MNB rendelet a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló törvény végrehajtásának az MNB által felügyelt szolgáltatókra vonatkozó, valamint az Európai Unió és az ENSZ Biztonsági Tanácsa által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtásáról szóló törvény szerinti szűrőrendszer kidolgozásának és működtetése minimumkövetelményeinek részletes szabályairól (https://net.jogtar.hu/jogszabaly?docid=a2000026.mnb).

bályrendszert valós időben lehetetlen működtetni, amikor néhány másodperc van egy utalás teljesítésére. Ahogy a fenti példánkban is láthattuk, a problémát az generálja ebben az esetben, hogy a tranzakció már messze több számlán és országon túl lehet, mire a vizsgálat megvalósul. A riasztások kivizsgálására az MNB által meghatározottan 30 vagy 20 munkanap áll rendelkezésre.

A filtering, vagyis szűrőrendszer némileg másképp működik. Az kifejezetten a forgalom valós idejű szűrését hivatott elvégezni. A valós idejű szűrésnél elvárt a szankciós érintettség vizsgálata nemzetközi forgalom esetén. Ezeket az utalásokat naponta több ciklusban engedik ki. Bármilyen hasonlóságot fedez fel a rendszer egy szankciós entitással, szintén egy riasztás generálódik, és a vizsgálat függvényében folytatódik a tranzakció, vagy elutasítják. Így szűrni lehet a bejövő és kimenő utalásokat is.

Jellemzően a filteringrendszer karakteregyezőséget vizsgál a szankciós listákkal összevetve, miközben az előző, a monitoring pedig előre meghatározott paramétereket. A filteringrendszernél nemcsak gyanús tranzakciókat keres a rendszer, hanem gyanús ügyfeleket is. A monitoringrendszer a beállított szabály szerint gyanús tranzakciókat detektál részünkre. Egy táblázatban összefoglalva jól összehasonlítható a két rendszer működése, feladata:

1. táblázat
Szűrőrendszerek csoportosítása

	Jogszabály	
	Kit. **2017. évi LII. Törvény**	**Pmt.** **2017. évi LIII. Törvény**
Feladat	Szankciók alá eső ügyfelek és tranzakciók kiszűrése és megakadályozása	Pénzmosási szokatlanság felismerése
Adatforrás	Szankciós listák	Letárolt historikus adatok
Módszer	Összevetés (karakteregyezőség)	Szokatlanságok keresése előre meghatározott paraméterek alapján
Intézkedés	Gyanús ügyfelek és tranzakcióik megállítása, intézkedés megtétele	Gyanús tranzakciók kiszűrése és ellenőrzése, intézkedés megtétele
Időpont	Valós időben, folyamatba építve	Utólagosan, nem valós időben

Forrás: Lukács (2022) alapján

Természetesen a hazai és egyéb nemzetközi szabályozások messze bővebbek, mint amire a jelen cikk lehetőséget ad, valamint nem képezi a téma részét ezek bemutatása; a téma szempontjából talán látható, hogy a monitoringrendszerben lesz szükséges valamilyen szabály megalkotására, hogy a kriptovaluták forgalma látható legyen.

2.3. Hatósági bejelentés

A 2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról az alábbi tevékenységet várja el a szolgáltatóktól:

„30. § (1) A szolgáltató vezetője, foglalkoztatottja és segítő családtagja

a) pénzmosásra,

b) terrorizmus finanszírozására, vagy

c) dolog büntetendő cselekményből való származására

utaló adat, tény, körülmény (a továbbiakban együtt: bejelentés alapjául szolgáló adat, tény, körülmény) felmerülése esetén köteles a 31. § (1) bekezdésében megjelölt személynek haladéktalanul írásban bejelentést (a továbbiakban: bejelentés) tenni.

(2) Az (1) bekezdésben meghatározott bejelentésnek tartalmaznia kell

a) a szolgáltató által a 7-14/A. § alapján rögzített adatokat,

b) a bejelentés alapjául szolgáló adat, tény, körülmény részletes ismertetését és

c) a bejelentés alapjául szolgáló adatot, tényt, körülményt alátámasztó dokumentumokat, amennyiben azok rendelkezésre állnak.

(3) A szolgáltató vezetője, foglalkoztatottja és segítő családtagja pénzmosásra, terrorizmus finanszírozására vagy dolog büntetendő cselekményből való származására utaló adat, tény, körülmény felmerülését a végrehajtott vagy végrehajtandó ügylet és az ügyfél által kezdeményezett, de végre nem hajtott ügylet esetében, valamint a 13. § (8) bekezdésében meghatározott esetben is köteles vizsgálni."

A fenti törvényi részlet határozza meg elsősorban, hogy mi is pontosabban a hatósági bejelentés. Amennyiben a fentebb említett szűrőrendszerek esetében a szolgáltató valamilyen gyanús körülményt vél felfedezni, kötelessége a c) pont értelmében haladéktalanul írásos bejelentést tenni. Ebből az idézetből az nem derül ki, hogy valójában kinek a részére kell ezt megtennie. Minden bejelentést a Nemzeti Adó- és Vámhivatal Pénzmosás és Terrorizmusfinanszírozás Elleni Iroda (továbbiakban: NAV PEI) részére szükséges megküldeni. A jogszabályi részletből látszik, hogy egy teljes, a szolgáltatók által elérhető összes információt tartalmazó

vizsgálati anyagot szükséges megküldeni a riasztás és a gyanús tevékenység tudomásunkra jutását követően azonnal, vagyis haladéktalanul.

Mindig kérdés, hogy ezekkel a bejelentésekkel valójában a NAV oldalán mi történik, hiszen a bejelentett esetek többségéről nincs visszajelzése a szolgáltatónak. Néha küld a NAV egy levelet, amelyben a bejelentés azonosítójára hivatkozva tájékoztatja a szolgáltatót, hogy a bejelentését a hatóság „sikeresen felhasználta", jelentsen ez bármit is. A NAV-nak a nemzetközi pénzmosás elleni hatóságokkal is kapcsolata van, így képes nem csak országon belüli mélyebb vizsgálatokra, de nemzetközi együttműködésre is. Ez természetesen a másik oldalról is igaz, a hazai NAV PEI-hez is érkeznek nemzetközi hatósági megkeresések, amelyek megválaszolásában, vagy akár egy folyamatban lévő nyomozásban is részt kell venniük.

Egy-egy ilyen bejelentésben magánszemélyek, egyéni vállalkozók, illetve céges ügyfelek is szerepelhetnek, akár külön-külön bejelentésben, vagy teljes cégláncolatok egyben küldésével is teljesíthető ez a bejelentési kötelezettség. Az elvárt minimum adattartalom a következő, ennél optimális esetben csak több információt kapnak, mint kevesebbet. Esetfüggő, hogy ezekből minden rendelkezésre áll-e, de törekedni kell ezek meglétére:

- a tranzakció ténye,
- gyanúra okot adó tényállás kifejtve,
- kapcsolódó partnerek,
- nyilvános céginformációk,
- ha volt, társbanki jelzés,
- ha volt, tranzakció visszahívását kísérő üzenet,
- tranzakció forrását igazoló dokumentum.

Összességében a hatósági bejelentések kulcsfontosságúak. Ezzel a tevékenységgel ajánljuk a számunkra gyanús tevékenységet folytató ügyfeleket a hatósági vizsgálat figyelmébe. Minél kifinomultabb szűréseket és munkafolyamatokat alakít ki egy szolgáltató, annál nehezebb lesz nála megvalósítani pénzmosást. Minél szofisztikáltabb kockázatérzékenységgel rendelkezik az adott szolgáltató, annál mélyebb elemzéseket tud elvégezni optimális esetben már a saját szűrőrendszerében vagy kiegészítő riportok és információk segítségével. A kapott információkat pedig haladéktalanul továbbítja a NAV PEI részére, akik vagy egyetértenek a gyanúval, és eljárást kezdeményeznek, vagy megköszönik a figyelmeztetést, és a vizsgálatot lezárják. A szolgáltatók kizárólag egy gyanús esetet jelentenek be, magának a cselekedet törvénytelenségének kimondására nem ők hivatottak (NAV, 2022).

3. FENYEGETETTSÉGEK AZ EURÓPAI UNIÓBAN

Az EU-ban, ezen belül Magyarországon is az alábbi fenyegetettségekkel kell szembenéznie a pénzügyi szektornak, amelyet az ENISA (2022), az Európai Unió Kiberbiztonsági Ügynöksége tesz közzé éves riportjaiban:

1. Ransomware (zsarolóvírusok)
2. Malware (rosszindulatú programok)
3. Social Engineering threats (pszichológiai manipuláció)
4. Threats against data (adatokkal való visszaélés)
5. Threats against availability: Denial of Service (túlterheléses támadás)
6. Threats against availability: Internet threats (általános internetes támadások)
7. Disinformation – misinformation (dezinformáció)
8. Supply-chain attacks (ellátási láncok támadása).

A 2022-es listát átolvasva észre lehet venni, hogy a harmadik helyre „katapultált" a pszichológiai visszaélések régi technikája, amely az ENISA 2021-es listáján nem volt megtalálható. Még pontosabban azt lehetne mondani, a cryptojacking helyet cserélt a social engineering threatsszel. Ez két dologra utal. Az első, hogy a kriptovaluták árfolyama lassan egy éve a töredékére esett vissza, ezért az érdeklődés is ugyanígy csökkent irántuk. A másik tartalom a covid lehet, azaz megváltozott az emberek hozzáállása, és újra előkerült a social engineering lehetősége. Az ESET vírusirtó gyártója szerint a két legfőbb social engineering módszer a spam és az adathalászat (ESET, 2022). A social engineering ennél sokkal több technikát is magában foglal, van olyan, aminek alig van köze az informatikához is, például a baiting (csalogatás, beetetés), amikor jutalmat ajánl a bűnöző az információkért cserébe (Terranova, 2022). Érdemes megjegyezni, hogy a világ egyik leghíresebb hackere, *Kevin Mitnick* a '90-es években social engineering technikákkal, pontosabban rábeszéléses technikákkal jutott be számítógépes rendszerekbe (Mitnick, 2022).

A pénzügyi intézmények, szolgáltatások ellen irányuló támadások egyre szofisztikáltabban működnek és egyre szélesebb körű megoldásokkal rendelkeznek. Magyarországon az NBSZ NKI monitorozza és kezeli a támadásokat, de sajnos, nem osztanak meg a nyilvánossággal részletes információkat, a heti hírleveikben is csupán olyan adatot osztanak meg, mint hogy mekkora az adott fenyegetettségi fok, vagyis 2022. 50. hetében a zsarolóvírusok fenyegetettségi szintje közepes (NBSZ, 2022). Ugyanakkor az MNB közölt ennél pontosabb adatokat, amelyek az NBSZ NKI-tól származnak, de számosítva olvashatjuk. 2022. február 1.–július 31. között összesen 21 db fenyegetettséget követtek nyomon, de ennél részletesebb információt ott sem kapunk, többek között azt sem tudjuk

meg, hogyan sikerültek ezek a támadások, és mely intézettel szembeni támadás történt, gondolok itt arra, hogy bank, pénzügyi intézmény vagy fintech elleni támadásról beszélhetünk (MNB, 2022). Mindez azt jelzi, hogy Magyarországon is jelen vannak ezek a támadások: az előbbi statisztika azt mutatja, hogy havonta négy-öt ilyen támadásról szerez tudomást a hatóság. A fenti riport a védelemben részt vevő összes hatóságtól is kapott információt, az MNB az említett 5 hónap alatt 765 incidensről tud, ami már aggasztóan magas mértékű tevékenységeket feltételez.

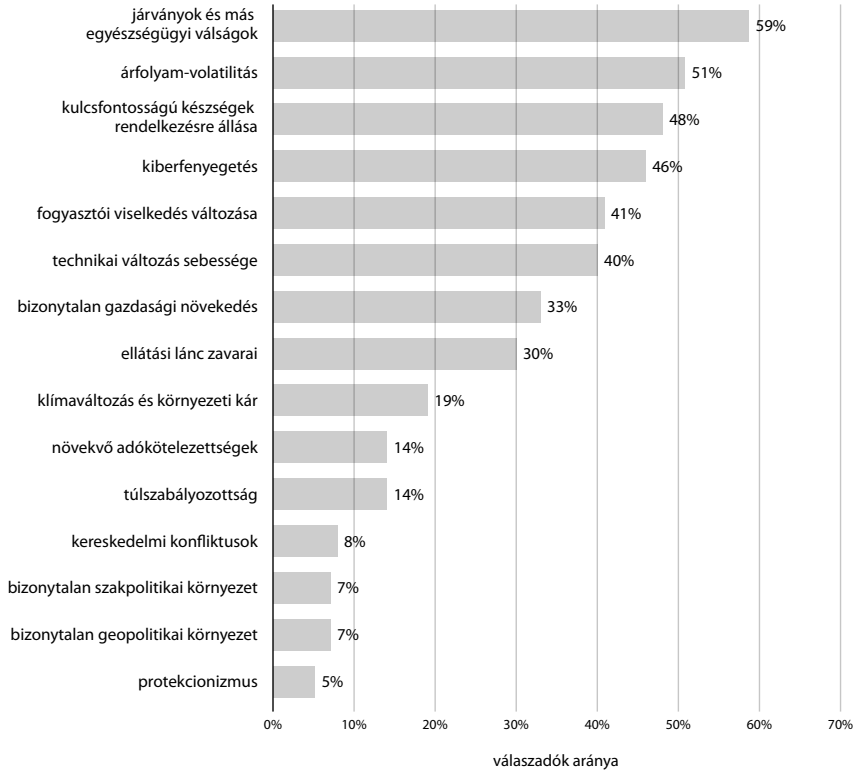
Az előbb említett ENISA-jelentésen túl az alábbi területekkel foglalkozik még az EU:

- Kiberbiztonsági kihívásokra adott intézkedések
- Kiberreziliencia
- Kiberbűnözés elleni uniós küzdelem
- Kiberdiplomácia fokozása
- Kibervédelmi együttműködés
- Finanszírozás és kutatás
- Kritikus infrastruktúra kiberbiztonsága (ET, 2023).

3.1. A vállalatok és a kiberbiztonság

Érdemes megvizsgálni, hogy a vállalatok hogyan vélekednek ebben a témában, a következő, *3. ábra* a vállalatok alaptevékenységébe beépített veszélyeket mutatja. Mint látható, majdnem minden második vállalat számol az online fenyegetéssel:

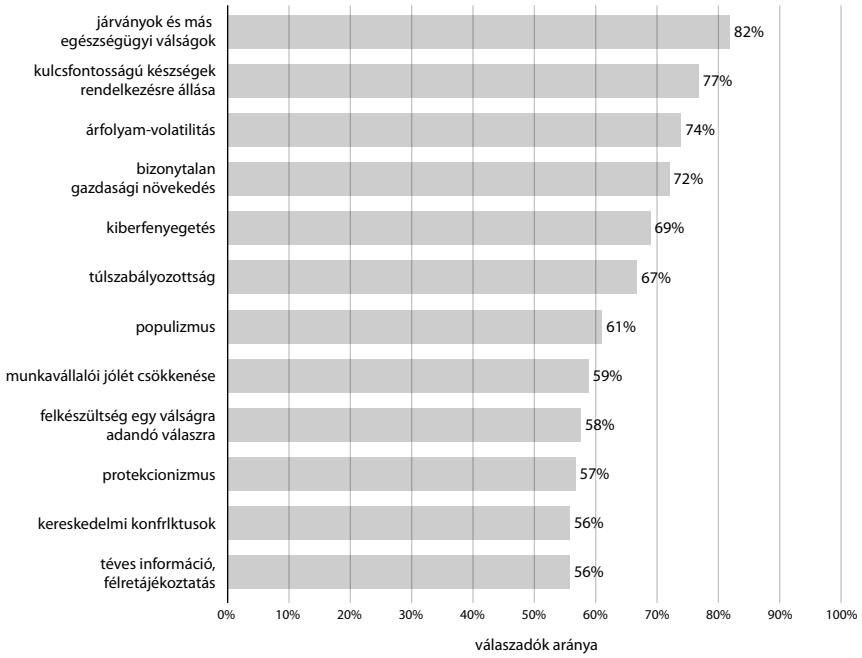
3. ábra
Vállalati veszélyek Magyarországon 2021-ben



Forrás: Statista, 2022a

A következő ábra még inkább hangsúlyozza a fenyegetések kezelésének fontosságát, mivel a vállalatvezetők majdnem kétharmada szerint hatással lehet ez a fenyegetettségi módszer a növekedésre:

4. ábra
Vállalatvezetők által a vállalati növekedésre kockázatosnak ítélt folyamatok



Forrás: Statista, 2022b

Az ügyfél-felhőszolgáltatások folyamatosan bővülnek, és az azok kínálta előnyök a pénzügyi szolgáltatóknak is rendkívül fontosak. Az ügyfélfelhők azonban már nem csupán egyszerű értékesítési csatornák, hanem inkább az ügyfélkapcsolatok alapvető építőkövei. Ezen szolgáltatások és technológiák megjelenése kihívást jelent a pénzügyi szolgáltatók számára, mivel az ügyfélfelhők fokozatosan új területeket hódítanak meg a pénzügyi szolgáltatási iparban.

Az ügyfélfelhőkben rejlő lehetőségek kiaknázása és az ügyfélkapcsolatok hatékonyabbá tétele érdekében az AI-bankok bevezetését javasolják a McKinsey & Company tanácsadói. Az AI-bankok előnyei közé tartozik, hogy az ügyfelek számára könnyebben hozzáférhetővé válnak a pénzügyi szolgáltatások, javul a digitális élmény, és megszűnik az ügyfelek körében általában tapasztalt hosszadalmas és nehézkes banki ügyintézés. Az AI-bankok azonban nemcsak az ügyfélélmény javítására és a pénzügyi szolgáltatások elérhetővé tételére szolgálnak, hanem segítenek a pénzintézeteknek az üzleti folyamatok automatizálásában is, ami hosszú távon költségcsökkentést eredményezhet. Az AI-bankok képesek lehetnek az ügyfélszolgálati kérdések automatizálására, az ügyfélkérdések gyorsabb és ponto-

sabb megválaszolására és az ügyfélkapcsolatok elemzésére, ami lehetővé teszi az ügyfélszolgálat és a marketing munkatársainak, hogy jobban megértsék az ügyfelek igényeit. Az AI-bankok alkalmazása azonban nem csak az ügyfélfelhők és az ügyfélszolgálati folyamatok automatizálása miatt fontos. Az AI-bankok lehetővé teszik a pénzintézetek számára, hogy az ügyfelek viselkedését elemezve, személyre szabott ajánlatokat tegyenek, amelyek megfelelnek az ügyfél igényeinek és preferenciáinak. Ahogy az előzőekben is említettük, az AI-bankoknak biztosítaniuk kell a megfelelő adatvédelmet és a személyes adatok védelmét. Azonban az AI által nyújtott előnyök még mindig jelentősebbek, mint az esetleges kockázatok. Az AI használata lehetővé teszi a bankok számára, hogy testreszabottabb ügyfélszolgálatot nyújtsanak, javítsák a csatornákat, valamint az ügyfélmegtartást. Az AI alkalmazása az ügyfelek digitális utazásainak megértéséhez és optimalizálásához vezethet. Jelentős hatással lesz a pénzügyi szektorra, és azok a bankok, amelyek nem alkalmazzák ezt a technológiát, valószínűleg hátrányba kerülnek versenytársaikkal szemben. Az AI-ban rejlő lehetőségek kimeríthetetlenek, és a bankoknak fel kell készülniük arra, hogy az AI-t használják az üzleti életben. Az AI bankjai azok a bankok lesznek, amelyek képesek alkalmazni azt, és alkalmazni az ügyfelek igényeit kiszolgáló, legújabb technológiákat. Az AI használata lehetővé teszi a bankok számára, hogy javítsák az ügyfélmegtartást, testreszabottabb ügyfélszolgálatot nyújtsanak, és hatékonyabban kezeljék az ügyfelek igényeit. Az AI alkalmazása azonban magával hozza az adatvédelmi kockázatokat is, és a bankoknak fel kell készülniük az ilyen kockázatok kezelésére. A személyes adatok védelme és az adatvédelem fontos tényezők a bankok AI által történő továbbfejlesztésében. A bankoknak át kell gondolniuk az adatvédelmi rendszerüket, és biztosítaniuk kell, hogy a személyes adatok védelme és az adatvédelem mindenkor biztosított legyen (McKinsey, Biswas et al., 2020).

A szabálykövetési kockázatokkal kapcsolatos hiányosságok súlyos következményekkel járhatnak, mint például pénzbírságok, vagy akár a vállalat hírnevének csorbulása (*Deutsch*–Pintér, 2018). Azonban a szabálykövetési kockázatok hatékony kezelése hatalmas lehetőséget kínál a pénzügyi és banki szektor számára. A banki szektorban egyre nagyobb szükség van az adatvédelemre és a megfelelőség ellenőrzésére. A pénzügyi szektorban az adatvédelmi szabályozások fokozatosan szigorodnak, ami újabb kihívásokat jelent a szektor szereplői számára. Azonban a szabályozások betartása nemcsak kötelező, hanem egyben lehetőséget is teremt a szektor számára a versenyképesség javítására. Az idézett cikk azonban megemlíti azt is: a szabályozások betartása mellett fontos, hogy az adatvédelemre és a szabálykövetési kockázatokra vonatkozó folyamatok hatékonyan legyenek bevezetve és karbantartva. Ez azt jelenti, hogy a szektor szereplőinek figyelmet kell fordítaniuk a megfelelőségi ellenőrzések és az adatvédelmi kérdések hatékony kezelésére. Végül a cikk azt is kiemeli, hogy a technológiai fejlődés új lehetősé-

geket kínál a pénzügyi és banki szektor számára az adatvédelem és a szabálykövetési kockázatok hatékonyabb kezelésére. Az adatelemzés és az automatizálás lehetőségei segítségével a szektor szereplői hatékonyabban tudják kezelni az adatvédelmi szabályozásokat, valamint a szabálykövetési kockázatokat is. Az automatizált eszközök és az AI segíthetnek a kockázatkezelésben és a pénzügyi rendszer hatékonyságának javításában. Az ilyen eszközök képesek az adatok elemzésére és az anomáliák azonosítására, ami lehetővé teszi a bankok számára, hogy korábban felismerjék a kockázatot, és megfelelő intézkedéseket hozzanak annak kezelésére. Emellett az automatizált folyamatok csökkentik az emberi hibák lehetőségét, ami további előnyöket jelenthet a pénzügyi szektorban.

A pénzügyi szektorban a compliance kihívásokat és kockázatokat számos új technológia, köztük az AI és az automatizálás segítségével lehet kezelni. Azonban fontos, hogy a bankok továbbra is figyelmesek maradjanak a változó jogszabályi környezetben, és folyamatosan frissítsék és javítsák compliance programjaikat annak érdekében, hogy megfeleljenek az előírásoknak, és minimalizálják a kockázatokat (*Qureshi*, 2019).

A pénzügyi szektorban az adatok és az azokból levont következtetések fontos szerepet játszanak a sikeresség és az üzleti növekedés szempontjából. A hagyományos adatelemzési módszerek azonban gyakran korlátozottak, és nem nyújtanak elegendő információt. Az AI és az ML alkalmazása azonban forradalmasíthatja az adatelemzési folyamatokat, segítve a pénzügyi szervezeteket az üzleti teljesítmény javításában és az ügyfél-elégedettség növelésében. Az AI és az ML képes nagy mennyiségű adatot gyűjteni és értelmezni. Az adatelemzési folyamatok automatizálása csökkenti az emberi hibák kockázatát, és növeli a hatékonyságot. Az ilyen technológiák lehetővé teszik az adatok pontosabb és gyorsabb elemzését, ami segíthet a pénzügyi szervezeteknek a hatékonyabb döntéshozatalban. Az AI és az ML alkalmazása továbbá lehetővé teszi az előrejelzések és a trendek pontosabb elemzését, ami támogatja a pénzügyi szervezeteket az üzleti stratégiák kialakításában. Az ilyen technológiák lehetővé teszik a személyre szabott ajánlatok készítését is, ami növelheti az ügyfél-elégedettséget és hűséget.

Az AI és az ML alkalmazása azonban számos kihívást is felvet. A pénzügyi szervezeteknek biztosítaniuk kell az adatvédelmet és az adatbiztonságot, valamint a technológiák etikai alkalmazását. Az adatvédelmi előírásoknak és a jogszabályoknak való megfelelés kulcsfontosságú, különösen a pénzügyi szolgáltatások esetében. Az AI és az ML alkalmazása azonban megoldást kínálhat az adatok hatékonyabb kezelésére és az üzleti folyamatok javítására. A pénzügyi szervezeteknek meg kell találniuk a megfelelő egyensúlyt a technológiai előnyök és a kockázatok között, hogy a legjobb eredményt érjék el az ügyfelek számára és a versenyképességük növelése érdekében. Az AI és ML alkalmazásaiban rejlő lehetőségek egyértelműek, és az ágazat számára valódi versenyelőnyt jelenthetnek

azok, akik az új technológiák bevezetésével és felhasználásával új megközelítéseket és eredményeket érnek el. Az AI és ML alkalmazásai a banki és pénzügyi szolgáltatások terén nagyobb hatékonyságot, nagyobb ügyfél-megelégedettséget és nagyobb biztonságot kínálnak, és segítenek javítani az üzleti folyamatokat. Azonban az AI és ML alkalmazásainak sikeres bevezetése és felhasználása nem egyszerű feladat, és az intézményeknek meg kell érteniük a technológiák előnyeit és korlátait, valamint fel kell készülniük a bevezetésükre és az alkalmazásukra. Ha azonban az intézmények sikeresen alkalmazzák ezeket a technológiákat, jelentős előnyöket érhetnek el a piacon, és megfelelhetnek a szabályozó hatóságok és az ügyfelek követelményeinek (*Narayanan*, 2019).

4. AZ OPEN BANKING KAPCSOLATA A MESTERSÉGES INTELLIGENCIÁVAL

Az Open Banking és a mesterséges intelligencia között szoros kapcsolat van, mivel mindkét technológia lehetővé teszi a pénzügyi szolgáltatások és termékek jobb kezelését és személyre szabottabbá tételét az ügyfelek számára. Az Open Banking lényege, hogy a bankok megosztják a felhasználók banki adatait az ügyfelek által engedélyezett harmadik fél alkalmazásokkal. Az ilyen alkalmazások segítségével az ügyfelek egyetlen felületen keresztül kezelhetik a számláikat és más pénzügyi termékeiket, így egyszerűbbé válik a pénzügyek intézése. Az AI ebben az összefüggésben segíthet a bankoknak és az alkalmazásoknak az adatok hatékonyabb kezelésében, elemzésében és felhasználásában, így még inkább személyre szabott ajánlatokat kínálhatnak az ügyfeleknek. Az AI számos területen hasznos lehet az Open Bankingben, például az ügyfélszolgálatok automatizálásában, a tranzakciók elemzésében és a pénzügyi visszaélések megelőzésében. Az AI alkalmazása segíthet a bankoknak a pénzmosás és a csalások elleni küzdelemben is azáltal, hogy felismeri az anomáliákat a tranzakciókban és a számlák kezelésében.

Mindenképpen meg kell említeni, hogy a GDPR és a PSD2 egyaránt fontos irányelvek a pénzügyi szolgáltatások terén. A GDPR célja az egyének személyes adatainak védelme, míg a PSD2 a pénzügyi tranzakciók biztonságának és hatékonyságának javítását célozza. Azonban ezek az irányelvek gyakran ellentmondhatnak egymásnak.

A PSD2 (Payment Services Directive 2) egy európai uniós irányelv, amely a pénzügyi szolgáltatásokat szabályozza, és lehetővé teszi az ügyfelek számára, hogy megosszák pénzügyi adataikat a harmadik fél alkalmazásokkal. Az irányelv célja az volt, hogy növelje a versenyt a pénzügyi szolgáltatások piacán, és elősegítse az innovációt az iparágban (Pintér, 2022). Az AI szerepe a PSD2-ben az adatok hatékonyabb elemzésében és kezelésében rejlik. Az AI képes elemzéseket végezni

a nagy mennyiségű adatokon, és azonosítani az ügyfelek igényeit és szokásait. Ez lehetővé teszi a bankok és az alkalmazások számára, hogy személyre szabottabb ajánlatokat kínáljanak az ügyfeleknek, és jobban megértsék a pénzügyi piacot. Az AI használata a PSD2-ben segíthet a pénzügyi csalások és a pénzmosás elleni küzdelemben is. Képes azonosítani azokat az ügyfeleket, akik nagyobb valószínűséggel fognak csalni vagy pénzmosást végezni, és figyelmeztetni a bankokat, hogy tegyenek intézkedéseket. Az AI segítségével a bankok és az alkalmazások képesek azonosítani azokat az ügyfeleket, akiknek a tranzakciói eltérnek a szokásos pénzügyi viselkedéstől, és figyelmeztetni a bankokat, hogy ellenőrizzék ezeket a tranzakciókat. Az AI képes azonosítani az ügyfelek kérdéseit és problémáit, és azonnal válaszolni rájuk chatbotok és más automata megoldások segítségével. Ez lehetővé teszi a bankok és az alkalmazások számára, hogy hatékonyabban és gyorsabban kezeljék az ügyfelekkel kapcsolatos kérdéseket és problémákat. Összességében az AI használata a PSD2-ben lehetővé teszi a bankok és az alkalmazások számára, hogy hatékonyabban és biztonságosabban kezeljék az ügyfelek pénzügyi adatait, és jobban megértsék az ügyfelek igényeit és szokásait.

4.1. Veszély vagy lehetőség?

Az AI használata az Open Bankingben mind veszélyt, mind lehetőséget jelenthet a pénzügyi szolgáltatók számára, attól függően, hogyan alkalmazzák. A mesterséges intelligencia használata az Open Bankingben lehetővé teszi a bankok és a fintechvállalkozások számára, hogy jobban megértsék az ügyfelek pénzügyi szokásait és igényeit. Ugyanakkor az AI használata az Open Bankingben veszélyt is jelenthet, ha az ügyfelek pénzügyi adatait nem megfelelően kezelik. Az AI-készülékek hibája vagy az AI hibás programozása esetén az adatvédelem megszegésének és a kiberbűnözők hozzáférésének a kockázata növekszik. Az ügyfelek pénzügyi adataihoz való jogosulatlan hozzáférést ki kell zárni, hogy a bizalom fenntartása és a jogi szabályozás betartása érdekében az ügyfél adatai megfelelően legyenek védve. Az AI alkalmazása tehát lehetőséget jelenthet a hatékonyabb és személyre szabottabb pénzügyi szolgáltatások és termékek nyújtására az Open Bankingben, de az adatvédelem és a biztonság szempontjából kiemelt figyelmet igényel. A bankoknak és a fintechvállalkozásoknak megfelelő adatvédelmi és biztonsági intézkedéseket kell alkalmazniuk az AI használata során, és biztosítaniuk kell, hogy az ügyfelek pénzügyi adatai biztonságosan kezelhetők legyenek.

A GDPR (általános adatvédelmi rendelet) és a mesterséges intelligencia közötti kapcsolat az adatvédelem és a személyes adatok kezelése szempontjából fontos téma. A GDPR célja, hogy védelmet biztosítson az uniós állampolgárok személyes adatainak kezelése során, az AI pedig egy olyan technológia, amely lehetővé teszi az adatok elemzését és felhasználását.

Az AI alkalmazása számos adatvédelmi kihívást vet fel a GDPR szempontjából. Az AI-hoz szükség van az adatok feldolgozására, és az adatok gyűjtése és tárolása során az ügyfelek beleegyezése és az adatok védelme kulcsfontosságú. Az adatvédelmi rendeletek követelményei között szerepel, hogy az adatokat biztonságosan kell tárolni, védelmezni és biztosítani a személyes adatokhoz való hozzáférés jogát. Az AI alkalmazása során a személyes adatokat az adatvédelmi rendeleteknek megfelelően kell kezelni. Alkalmazása számos előnyt is kínál az adatvédelem szempontjából. Az AI képes a személyes adatok védelmére és az adatok pontosabb elemzésére, ami javítja a biztonságot és az adatvédelmet. Az ügyfeleknek személyre szabottabb szolgáltatásokat és termékeket kínál, ami elősegíti az ügyfelek bizalmát és lojalitását. A GDPR és az AI kapcsolata tehát azt jelenti: a pénzügyi szolgáltatóknak biztosítaniuk kell, hogy az adatkezelési folyamatok megfeleljenek az adatvédelmi rendeletek követelményeinek.

5. ÖSSZEFOGLALÁS

A mesterséges intelligencia alkalmazása jelentős előnyöket nyújthat a pénzügyi szolgáltatások terén. Néhány példa:

- Csökkentett költségek: az AI-alapú automatizált folyamatok segítségével a pénzügyi intézmények csökkenthetik a költségeiket és növelhetik a hatékonyságukat.
- Jobb ügyfélszolgálat: az AI lehetővé teszi a személyre szabott ügyfélszolgálatot és javíthatja az ügyfél-megelégedettséget.
- Kockázatkezelés: az AI-alapú analitikák lehetővé teszik a jobb kockázatértékelést és az időben történő beavatkozást a problémák elkerülése érdekében.
- Betörésvédelem: az AI segítségével a pénzintézetek felismerhetik a biztonsági fenyegetéseket, és csökkenthetik a csalási eseteket.
- Javított adatelemzés: az AI-alapú analitikák segíthetnek a jobb adatelemzésben, ezáltal a pénzügyi intézmények jobban megérthetik az ügyfél- és piaci trendeket.

Az AI folyamatos fejlődése valószínűleg további innovációkat és fejlesztéseket fog eredményezni a jövőben. A mesterséges intelligencia használata a pénzügyi szektorban számos területen segíthet, többek között a csalások és visszaélések felderítésében, a kockázatkezelésben, a befektetési döntések meghozatalában, az ügyfélkapcsolatokban és a hatékonyabb belső működésben. Az AI-alapú eszközök és algoritmusok lehetővé teszik a pénzintézetek számára, hogy nagy mennyiségű adatot gyűjtsenek, elemezzék és értékeljék azokat annak érdekében, hogy hatékonyabb döntéseket hozzanak.

Az AI-alapú rendszerek például képesek nagy sebességgel felderíteni és azonosítani a gyanús tranzakciókat, amelyek pénzmosáshoz vagy más illegális tevékenységekhez kapcsolódhatnak. Az ilyen rendszerek segítenek a pénzintézeteknek megakadályozni a pénzmosást és a terrorizmus finanszírozását. Az AI és a gépi tanulás hasznos a kockázatkezelési folyamatokban is, ahol az algoritmusok segítenek a pénzintézeteknek azonosítani a kockázatos tranzakciókat és a magas kockázatú ügyfeleket. Ez lehetővé teszi, hogy a bankok hatékonyabban kezeljék a kockázatot, minimalizálják a veszteségeket és optimalizálják a tőkekihelyezést. Az AI használata a befektetési döntésekben is hatékony lehet, ahol az algoritmusok képesek gyorsan elemezni a nagy mennyiségű adatot, például a tőzsdei adatokat, a vállalati pénzügyi jelentéseket, a makrogazdasági mutatókat, és így tovább. Az ilyen rendszerek lehetővé teszik a befektetési döntéshozóknak, hogy időben és hatékonyan tájékozódjanak a piaci helyzetről, és ezáltal növeljék a befektetési hozamokat. Az AI és a gépi tanulás használata szintén lehetőséget nyújt a pénzügyi szektor számára, hogy javítsa az ügyfélkapcsolatokat és a vevőszolgálatot. Az algoritmusok és az AI segítik a pénzintézeteket abban, hogy személyre szabott ajánlatokat és megoldásokat kínáljanak ügyfeleiknek, ezáltal javítsák a vevő által érzékelt élményt.

HIVATKOZÁSOK

Accenture (2023): Accenture: Cybersecurity for Financial Services – Balancing External Threats and Internal Challenges.

Allianz (2023): Allianz Risk Barometer. https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html.

Appinventiv (2023): AI in Banking – How Artificial Intelligence is Used in Banks. https://appinventiv.com/blog/ai-in-banking/.

Biswas, S. – Carson, B. – Chung, V. – Singh, S. – Thom, R. (2020): AI-bank of the future: Can banks meet the AI challenge? McKinsey, https://www.mckinsey.com/industries/financial-services/our-insights/ai-bank-of-the-future-can-banks-meet-the-ai-challenge.

CyberEdge (2023): Cyberthreat Defense Report. https://cyber-edge.com/cdr/.

Deloitte (2023): Global Future of Cyber Survey, Building long-term value by putting cyber at the heart of the business. https://www.deloitte.com/global/en/services/risk-advisory/content/future-of-cyber.html.

Deutsch, N. – Pintér, É. (2018): A társadalmi felelősségvállalás és a pénzügyi teljesítmény közötti kapcsolat a magyar bankszektorban a globális válságot követő években. *Hitelintézeti Szemle*, 17(2), 124–145. DOI: http://doi.org/10.25201/HSZ.17.2.124145.

ESET (2022): Hogyan veszélyezteti ez a támadási forma vállalkozását? https://www.eset.com/hu/it-biztonsagi-temak-cegeknek/social-engineering/.

ESET (2023): Cybersecurity Trends 2023: Securing our hybrid lives. https://www.eset.com/int/business/resource-center/reports/eset-cybersecurity-trends-2023/.

Európa Tanács (2023): Kiberbiztonság: hogyan kezeli az EU a kiberfenyegetéseket? https://www.consilium.europa.eu/hu/policies/cybersecurity/.

ENISA (2022): ENISA Threat Landscape 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

Gál, I. L. (2007): A pénzmosás hatályos büntetőjogi szabályozása Magyarországon. https://www.mnb.hu/letoltes/pszafhu-rtfkonf-gali.pdf

Lukács, Zs. (2022): Budapest Institute of Banking (prezentáció).

Mitnick, K. (2022): The History of Social Engineering. https://www.mitnicksecurity.com/the-history-of-social-engineering.

Microsoft (2023): Top 10 questions on Cybersecurity in 2023. https://news.microsoft.com/en-cee/2023/02/01/top-10-questions-on-cybersecurity-in-2023/.

McAfee (2023): McAfee 2023 Threat Predictions: Evolution and Exploitation. https://www.mcafee.com/blogs/security-news/mcafee-2023-threat-predictions-evolution-and-exploitation/?gclid=EAIaIQobChMIwNDZ9on8_gIVgqzVCh28NwJbEAAYASAAEgK9kvD_BwE.

MNB (2022): A magyar pénzügyi szektor kiberfenyegetettségi térképe 2022. https://www.mnb.hu/letoltes/kiberfenyegetettsegi-terkep-2022.pdf.

Narayanan, K. (2019): Harnessing the power of AI & ML for Analytics in Banking and Financial Services. OneGlobe, https://www.oneglobesystems.com/blog/harnessing-the-power-of-ai-ml-for-analytics-in-banking-and-financial-services.

NAV (2022): NAV PEI Iroda. https://pei.nav.gov.hu/penzmosas-es-terrorizmusfinanszirozas-elleni-iroda/penzmosas-es-terrorizmusfinanszirozas-elleni-iroda.

NBSZ (2022): Nemzetközi IT biztonsági sajtószemle. Nemzeti Kibervédelmi Intézet (NKI), https://nki.gov.hu/wp-content/uploads/2022/12/Sajtoszemle_50.-het.pdf.

Pintér, É. (2022): Az innováció természetrajza. In Stukovszky, Tamás – Illyés, Péter (szerk.) (2022): *A kis- és középvállalkozások innovációja: Elmélet és gyakorlat*. Budapest: Akadémiai Kiadó, 81–96.

Pintér, É. (2008): A pénzügyi szolgáltatások reintegrációja – a bankbiztosítási tevékenységet befolyásoló tendenciák. Doktori értekezés, Pécsi Tudományegyetem Közgazdaságtudományi Kar, Gazdálkodástani Doktori Iskola, https://pea.lib.pte.hu/handle/pea/15208.

Proofpoint (2023): Cyber Security Focused on "People".

Qureshi, M. W. (2019): Understanding Compliance Risk in Finance and Banking. *ISACA Journal*, 3, 1–7, https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2019/volume-4/understanding-compliance-risk-in-finance-and-banking_joa_eng_0719.pdf.

Ray, T. (2017/2022): Scopes of Machine Learning and Artificial Intelligence in Banking & Financial Services |ML & AI – The Future of Fintechs. https://www.stoodnt.com/blog/scopes-of-machine-learning-and-artificial-intelligence-in-banking-financial-services-ml-ai-the-future-of-fintechs/.

Statista (2022a): Threats explicitly factored into companies' strategic risk management activities in Hungary 2021. https://www.statista.com/statistics/1239649/hungary-threats-factored-into-companies-strategic-risk-management/.

Statista (2022b): CEOs' opinion on potential economic, policy, social, environmental and business threats to companies' growth prospect in Hungary 2021. https://www.statista.com/statistics/1234133/hungary-potential-threats-to-companies-growth/.

Terranova (2022): 9 Examples of Social Engineering Attacks. https://terranovasecurity.com/examples-of-social-engineering-attacks/.

TÜV (2023): IT Security Act & KRITIS. https://it-tuv.com/en/leistungen/security-and-value-of-information/it-security-act-kritis/.

Wolters (2018): *Wolters Kluwer Adó-kódex*, XXVII(6), 2.