PANNON EGYETEM
GAZDÁLKODÁSI KAR ZALAEGERSZEG

Pénzbiztonság és bankbiztonság a fizikai és virtuális térben

Témavezető: Fejes Judit Katalin

Külső konzulens: Koczor Szilárd

Mentes Dominik Attila
alapképzés
Nappali tagozat
Pénzügy és számvitel szak
Vállalkozások pénzügyei szakirány

2024

PANNON EGYETEM
GAZDÁLKODÁSI KAR ZALAEGERSZEG

SZERZŐI NYILATKOZAT A DOLGOZAT BENYÚJTÁSÁHOZ*

Hallgató neve:	Mentes Dominik Attila		
Képzési szint:	alapképzés		
Szak:	Pénzügy és számvitel		
Szakirány (ha van):	Vállalkozások pénzügyei		
Neptun kód:	HS52E6	Védés éve:	2024
Dolgozat címe:	Pénzbiztonság és bankbiztonság a fizikai és virtuális térben		
Egyetemi témavezető:	Fejes Judit Katalin		
Gyakorlóhelyi konzulens:	Koczor Szilárd		
Öt kulcsszó a dolgozatról:	Bankbiztonság, Pénzbiztonság, Fizikai védelem, Virtuális védelem, Visszaélés		

Kérjük a szerzői döntésnek megfelelő opciót aláhúzni:

Hozzájárulok / nem járulok hozzá, hogy szakdolgozatomat az Egyetem az interneten a nyilvánosság számára repozitóriumában közzétegye.

A hozzájárulás szerzői feltételei:
- a dolgozat magáncélra letölthető, a forrás megjelölésével szabadon idézhető, de az idézés szokásos terjedelmét meghaladó felhasználás (átvétel) tilos,
- hozzájárulásom időtartamra nem korlátozott és bármikor visszavonható.

(Hozzájárulás hiányában a dolgozat csak az Egyetem arra kijelölt számítógépein, képernyős megtekintéssel kutatható. Egyéb hozzáférés, többszörözés nem engedélyezett.)

Büntetőjogi felelősségem tudatában nyilatkozom az alábbiakról:
- dolgozatom mindenben eleget tesz a vonatkozó és hatályos intézményi előírásoknak,
- a dolgozatban foglalt tények és adatok a valóságnak megfelelnek, a leírtak saját, önálló munkám eredményei,
- a dolgozatban felhasznált adatokat, forrásokat a szerzői jog figyelembevételével alkalmaztam,
- a dolgozat nem került felhasználásra korábban oktatási intézmény más képzésén felsőoktatási szakképzés, diplomaszerzés vagy szakirányú továbbképzés során.

Tudomásul veszem az alábbiakat:
- a dolgozat szerzői jogtisztaságának ellenőrzésére az Egyetem szoftveres ellenőrzést (plágiumszűrést) végezhet és eredményét a dolgozat értékelésében felhasználhatja,
- a dolgozat elektronikus formában, az Egyetem repozitóriumában kerül elhelyezésre és a hatályos jogszabályok, intézményi szabályzatok szerint, valamint fentebbi szerzői rendelkezésemnek megfelelően biztosítható a kutatási célú hozzáférése,
- a dolgozat metaadatai és szerzői összefoglalója online nyilvánosak.

Zalaegerszeg, 2023. 12. 15.

Mentes Dominik

hallgató aláírása

**Szövegszerkesztővel töltendő ki, formai és tartalmi változtatások nélkül. Gépírással aláírható. Ebben az esetben kéjük a Családnév Keresztnév s. k. alakot használni. Kézi aláírás és szkennelés esetén a dokumentum csak kifogástalan minőségű digitalizált változat lehet!*

Tartalomjegyzék

Bevezetés: A pénzbiztonság és a bankbiztonság

Az elmúlt pár évben a világunk állandó, gyors változásnak és ezzel együtt fejlődésnek volt kitéve. Ez az életünk minden területére kihat, így természetesen a gazdaságra és még inkább a technológiára is. Az egyre felgyorsuló információcserének egyik nagy hozadéka az elektronikus pénzügyi ügyintézés. Az emberek egyre többször választják ezeket digitális megoldásokat a hagyományos lehetőségekkel szemben, főként gyorsasági és kényelmi szempontok miatt. Ezekhez a pénzintézetek és a bankok is partnerek, ugyanis egyre jobban ők is a digitalizálásra helyezik át a hangsúlyt, hiszen ez nekik is számos előnyt jelenthet.

Ámde a pénzügyek digitalizálásának elterjedésével együtt számos új megoldandó probléma és kihívás elé állnak mind a bankok, mind az ügyfelek, különösen a biztonság terén. A pénzügyek biztonsága napjainkban az egyik legkritikusabb pontja a vállalatoknak és a magánembereknek is. A számos új technológiai fejlesztések, mint például az elektronikus fizetési rendszerek, a kriptovaluták vagy az online bankolás remek új pénzügyi lehetőségeket biztosítanak, de ahogy ez lenni szokott új lehetőségekhez általában új veszélyek, kockázatok is párosulnak és így van ez ebben ez esetben is. Főképp a pénzügyi és személyes adatok, illetve a tranzakciók digitális továbbítása, megőrzése és tárolása ad sok lehetőséget a kiberbűnözők, illetve csalók számára, akik számtalan módszerrel próbálnak hozzáférni ezekhez az adatokhoz, hogy utána vissza tudjanak élni azokkal.

Ebben a szakdolgozatban a pénzintézetek, bankok és a pénz biztonságára szeretnék összpontosítani, cél a jelen korunk kihívásainak és veszélyeinek megállapítása, továbbá annak vizsgálata, hogy miként lehet minél biztonságosabbá tenni a pénzügyi környezetet mindenki számára. A dolgozatbank részletezni szándékozom a pénzügyi adatvédelmet, a kiberbiztonságot, a kriptovaluták veszélyeit és bemutatom a legújabb technológiai megoldásokat, amelyek segítenek megőrizni a pénzügyi stabilitást és biztonságot a gazdaság digitalizációja után is. Továbbá kitérek majd a hagyományos, fizikai térben lévő gyakori veszélyekre és azok esetleges megoldásaira is.

Úgy gondolom ez a témakör nem csupán a pénzügyi szektor dolgozóinak vagy szakértőinek lehet fontos, hisz az egész társadalom érintett ebben a témakörben. Ezért is választottam ezt a témát a szakdolgozatom tárgyaként, ugyanis a jól és biztonságosan működő pénzügyi rendszerek elengedhetetlenek a gazdaság stabilitása és így a társadalmi jólét szempontjából is.

Pénzbiztonság megfogalmazása és annak jelentősége

A pénzbiztonság

A pénzbiztonság kifejezés alatt számos olyan intézkedést és gyakorlatot értünk, amelyek célja a pénzügyi eszközök, tranzakciók és adatok védelme. Ez többek közt magában foglalja a fizikai pénz, a digitális tranzakciók és az adatvédelmet is. A pénzbiztonság kiemelkedően fontos mind egyéni, szervezeti és nemzetgazdasági szinten is. Az egyén szintjén az emberek és háztartások pénzügyi stabilitását adja meg. Része a bankjegyek, bankkártyák és más pénzügyi eszközök fizikai és digitális védelme is. Továbbá fontos az ATM-ek biztonságos használata is.

A pénzbiztonság kapcsolata és befolyása a gazdaságra

A pénzbiztonság nagyban hozzájárul a gazdasági stabilitáshoz. Az embereknek fontos, hogy biztonságba érezzék pénzügyi eszközeiket, mert ez növeli a pénzpiaci aktivitást és a gazdaság fejlődését. Továbbá a pénzbiztonság a pénzügyi rendszer és az egyén közötti bizalom egyik alapvető építőköve. Ezért a legtöbb országban szigorúan szabályozzák a pénzpiacot és annak biztonságát. Ezentúl a befektetők és a vállalkozások is csak akkor hajlandóak részt venni pénzpiaciakon, ha azt kellően biztonságosnak és megbízhatónak tartják. A pénzbiztonság hiánya az egész országra negatívan képes hatni, így kiemelten fontos egy ország gazdaságában.

A bankbiztonság és annak jelentősége

A bankbiztonság

„*A hétköznapi ember számára a bankbiztonság egyet jelent a bankfiókokban található riasztórendszerekkel, rácsokkal, zárokkal, páncélszekrényekkel és fegyveres biztonsági őrökkel. A felsorolt védelmi berendezések és a személyi vagyonőrök alkalmazása ugyanakkor csak egy részét képezik annak a komplex rendszernek, melyet a bankbiztonság ma jelent. A vagyonvédelmi eszközök csak fizikai védelmet nyújtanak, emellett ugyanolyan fontos szerepet játszanak a megfelelő informatikai háttér és a kellő szakértelemmel kidolgozott biztonsági stratégia. Bankbiztonsági szempontból a pénzintézetek számára az ügyfél adatainak védelme legalább olyan fontos, mint a megfelelő értéktárolás, vagy a diszkrét be- és kifizetés, a bűncselekmények elkerülése*."[1]

Tehát a bankbiztonság két fő részre bontható, a fizikai és a virtuális, avagy informatikai biztonságra. Mivel a fizikai veszélyek már az első bankok megjelenése óta jelen vannak, azokban a pénzintézetek több százéves tapasztalata van, így ezek megoldása okozza a kisebb gondot. Ezzel ellentétben az online, virtuális fenyegetettség csak néhány éve van igazán jelen a bankok életében, tehát az ilyenféle kockázatok csökkentésének lehetőségei még nem olyan kiforrottak és talán még nem annyira biztonságosak. Persze az összes pénzintézet mindent megtesz annak érdekében, hogy védje az ügyfeleit és saját magát.

A pénzintézetek megbízhatóságának jelentősége a gazdaság szempontjából

A bankok biztonságának kiemelt szerepe van a gazdaságban, mivel a pénzügyi rendszer egyik legfontosabb tagjai. A biztonságos, átlátható és stabil banki környezet nagyban elősegítheti a gazdaság megfelelő és hatékony működését. Az alábbiakban több szempontból bemutatom, hogy miért is fontos a bankbiztonság a gazdaság számára.

---

[1] *Zsigrai bankbiztonsági és vagyonvédelmi KFT.: Bankbiztonság [online]. Hozzáférés: https://www.zsigraikft.hu/bankbiztonsag [megtekintve 2023.12.09.]*

Betétbiztonság: Sok ember és vállalat, cég is bankokban helyezi el a pénzét és megtakarítását. Ezeket a pénzintézeteknél elhelyezett betéteket az Országos Betétbiztosítási Alap (OBA) biztosítja egy bizonyos határösszegig, ami általában kellően magas az átlagos magánszemélyeknek, illetve vállalkozásoknak. Tehát ezzel is megbízhatóbbá és biztonságosabbá válnak a bankok, így nagyobb valószínűséggel bíznak meg bennük az ügyfelek és hajlandóak a pénzüket bankszámlákon tartani. Ez pedig hozzájárul a pénzpiacok stabilitásához és a likviditás fenntartásához. Habár még mindig akad olyan, aki otthon tartja a pénzét, mert annyira „fél" a bankoktól. Ezek a személyek feltehetően nincsenek tisztába az ilyen biztosításokkal.

Hitelek és befektetések: A biztonságos banki környezet elengedhetetlen ennél a szempontnál is, hiszen akár egy visszaélés vagy egy egyéb más biztonsági hiányosságból keletkezett probléma könnyen csökkentheti például a hitelképességet. A gazdaság fejlődéséhez pedig elengedhetetlen, hogy a cégek, biztonságosan tudjanak hitelt felvenni, illetve befektetni.

Általános pénzügyi stabilitás: A pénzügyi rendszer stabilitása közvetlen hatással van az ország gazdasására. A pénzügyi válságok, amelyek a bankbiztonság hiányából adódnak, súlyos gazdasági zavarokat okozhat. A bankok biztonsági intézkedései hozzájárulnak az egész pénzügyi rendszer stabilitásához, ezzel tehát a gazdasági válságok esélyének csökkentéséhez is.

Adatvédelem és személyi biztonság: A bankok nagy mennyiségű érzékeny adatot kezelnek az ügyfelekről. A személyes adatokkal való visszaélés és egyéb internetes csalások nagy veszélyt jelentenek a gazdaságra és az egyénekre is. A bankbiztonság adatvédelme és személyvédelme nagy mértékben hozzájárul a társadalom digitális védelméhez, hiszen itt a szolgáltatást igénybe vevők a bankra bízzák pénzügyi és személyes adataikat is.

Korrupció: A bankok jelentős mértékben segíteni tudják a pénzmosás, a korrupció és a fekete pénz elleni küzdelmet. A bankok felelőssége ezek felderítése és jelentése a hatóságok felé.

Gazdasági növekedés: A banki környezetnek hatalmas szerepe van a gazdaság fejlődésében és az új technológiai fejlesztésekben a pénzügyi szektorban. Továbbá ezek biztonságos bevezetése nagyban elősegíti a gazdaság fejlődését.

Összeségében tehát a bankbiztonság nem csak a vállalatok és a magánemberek érdekeit szolgálja, hanem létfontosságú szerepet játszik a gazdaság stabilitásában és fejlődésében is.

A fizikai és virtuális biztonság aspektusai

Ahogy már feljebb említettem, a bankbiztonságot én két fő egységre bontanám, fizikai és virtuális részre. Mindkettő területen számtalan intézkedés és technológia használata szükséges ahhoz, hogy a bankok megfelelő védelmet tudjanak nyújtani az ügyfelek és azok pénzeszközeinek részére. Az alábbiakban bemutatom a fizikai és virtuális bankbiztonság fontosabb jellemzőit.

Fizikai bankbiztonság:

A fizikai része a bankbiztonságnak az épületek, az infrastruktúra és az egyéb más valóságbéli, kézzel megfogható eszközök védelmével foglalkozik. Fő célja az ügyfelek és a banki eszközök fizikai integritásának megőrzése. Az ilyen típusú biztonsági intézkedések közé tartoznak többek közt a kamerák, a különböző érzékelők, fizikai akadályok, kóddal zárt acélbetétes ajtók.

A bankfiókokhoz és az azokban található berendezésekhez telepített modern biztonsági berendezések lehetővé teszik a bankszemélyzetnek és a hatóságoknak, hogy a lehető leghamarabb észleljék és így nagyon gyorsan reagálni tudjanak a vészhelyzetekre. Az érzékelők és a riasztórendszerek segítségével a bankok képesek észlelni az illetéktelen behatolásokat és egyéb fizikai fenyegetéseket.

Virtuális bankbiztonság:

A virtuális bankvédelem a digitális világban történő tranzakciók és tevékenységek biztonságára összpontosít. Az online bankolás elterjedésével párhuzamosan a bankoknak kiemelten foglalkozni kell a virtuális védelemmel, mivel hatalmas fenyegetést jelentenek az internetes csalók és az adathalászok.

A virtuális bankbiztonságot újabb kettő fő területre osztanám: az adatvédelemre és a tranzakciók biztonságára. Az adatvédelmi intézkedések olyanokat foglalnak magukba, mint például a titkosított kommunikáció, az adatbázisok állandó megfigyelése vagy a hozzáférési jogosultságok erősítése, illetve állandó ellenőrzése. A tranzakcióbiztonságban pedig kiemelt szerepet játszik az állandó tranzakciós felügyelet, de segíti a kétlépcsős azonosítás vagy az IP-cím ellenőrzés is.

Az jelenti a legnagyobb kihívást a bankoknak ebben a témakörben, hogy állandóan fejlődnek és változnak a fenyegetések és ezekhez minél előbb alkalmazkodniuk kell. Ehhez a pénzintézeteknek állandóan frissíteniük kell a biztonsági szabályokat, illetve fejleszteni kell a technológiájukat, hogy lépést tudjanak tartani az egyre bonyolultabb kiberbűnözői módszerekkel. Ugyanis ez egy emberi aggyal már szinte felfoghatatlanul gyorsan fejlődő „iparág", így egy kisebb lemaradás is nagyban növeli a kockázatot.

A digitalizáció hatása a pénz és bankbiztonságra

A digitalizáció rengeteget alakított a bankbiztonságon, ezekből mutatok most be pár lényeges tényezőt.

Adatvédelem:
A digitalizáció nagyban megnövelte az adatok generálódásának mennyiségét, így megnehezítve azok tárolását. A bankoknak sokkal nagyobb hangsúlyt kell fektetniük ezek kezelésére, hogy megakadályozzák az adatszivárgást és az illetéktelen hozzáférést.

Kiberbiztonság:
A digitális térben egyre nő a kiberbiztonsági fenyegetés, amikkel szembe kell nézni a bankoknak. Rengetek kártékony szoftver, online csalás és adathalász próbálkozásnak kell ellenállnia a bankok rendszerének. Ezek megkövetelik a fejlett, adaptív és intelligens biztonsági rendszerek használatát, amik csökkentik a kockázatot és minimalizálják a károkat.

Kétlépcsős azonosítás:
Ebben a digitalizált világban már az egyszerű, hagyományos jelszavak nem elegendőek a biztonság eléréséhez. A kétlépcsős azonosítás ebben segít a felhasználókat, ugyanis ez a módszer plusz egy réteget képez a felhasználók azonosításához, ezáltal nehezebbé teszi az illetéktelen hozzáférést. Ilyen kétlépcsős azonosítás például a különböző hitelesítő alkalmazások használata vagy az smsben, illetve emailben kapott kódok megadása belépéskor.

Big Data elemzés:
A digitalizáció elősegítette azt is, hogy a bankok óriási mennyiségű adatokat tudjanak elemezni ügyfélesemények vagy akár tranzakciók terén is. Így könnyen észrevehetőek anomáliák, amik egy esetleges csalást vagy illetéktelen hozzáférést jelezhetnek. Ennek következtében még időben megállíthatóak folyamatok, amik a pénzügyi szektorban sokszor nagy veszteségektől mentik meg az ügyfelet.

Blockchain és kriptográfia alkalmazása:
Ez az óriási digitális fejlődés felgyorsította a blockchain technológia és kriptográfia terjedését is, amelyek forradalmi változásokat hoztak a pénzügyi biztonság területén. Továbbá a decentralizált és elosztott ledger rendszerek lehetővé teszik a tranzakciók átláthatóságát és biztonságát, így csökkentve a csalások kockázatát.

Összegezve tehát a digitalizáció egyértelműen előnyös lehet a bankok és ügyfeleik számára, abban az esetben, ha képesek megbirkózni az ezzel járó nehézségekkel a bankbiztonság terén. A fent említett intézkedések és technológiák bevezetése elengedhetetlen ahhoz, hogy az ügyfelek és a pénzügyi intézmények egyaránt biztonságba érezzék magukat a digitális világban.

Fizikai pénzbiztonság és bankbiztonság:

Fizikai pénzeszközök biztonsága

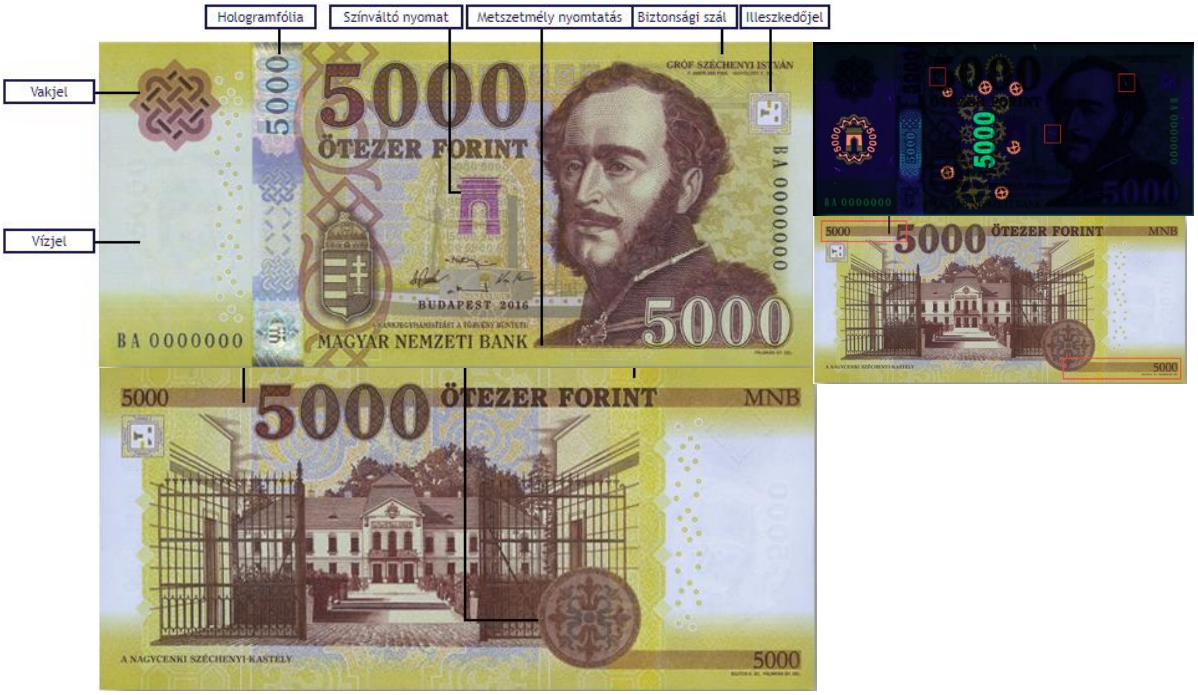
Hamisítás

A bankok fizikai biztonságában kiemelt helyen van a hamisítás elleni védekezés. Többféle hamisításra is figyelnie kell a bankoknak. Amire mindenki gondol először az a fizikai pénz hamisítása, de emellett még előfordul személyes dokumentumok hamisítása is. A következőkben részletesen vizsgáljuk, hogyan alakulnak ki és milyen intézkedésekkel próbálja meg kezelni a bank ezt a lehetséges kockázatot.

Pénzhamisítás

A pénzhamisítás már több évszázada kihívást jelent mindenki, de főként a pénzintézetek számára. Az egyre fejlődő nyomdai technológiák és egyéb másolási módszerek lehetővé teszik a bankjegyek másolását. Ez nem csak a bankokra, de a gazdaság stabilitására is fenyegetést jelent.

Az egyik alapvető védekezési módszer magukban a bankjegyekben rejlik, amelyeket számos biztonsági elemmel lát el a Magyar Nemzeti Bank. Ezek meglétét különböző módokon lehet ellenőrizni. Vannak olyanok, amiket a pénz fény felé tartásával lehet láthatóvá tenni: vízjel, biztonsági szál, illeszkedő jel. Találhatóak olyan biztonsági elemek is a bankjegyeken, amiket mozgatással lehet észrevenni ilyen például: a színváltó nyomat, a hologramfólia, az irizáló nyomat vagy a rejtett kép. Továbbá vannak olyan részletek is, amelyek meglétét tapintással lehet ellenőrizni, a vakjel vagy a metszetmély nyomtatás ilyen. Mindemellett léteznek olyan biztonsági elemek, amelyeket csak különböző eszközök segítségével lehet ellenőrizni, például különböző UV fények alatt vagy nagyító segítségével válnak láthatóvá[2].



1. ábra Az ötezer forintos bankjegy biztonsági elemei

Emellett a pénzintézetek az alkalmazottjaiknak bizonyos időközönként pénzhamisítás témakörű tréningeket tartanak, amelyeken felhívják a figyelmet az éppen legújabb hamisítási technológiákat lebuktató jellemzőkre, ezzel is növelve az esélyt, hogy kiszűrjék az ilyen próbálkozásokat.

[2]*Magyar Nemzeti Bank: FORINTBANKJEGYEK BIZTONSÁGI ELEMEI [online]. Hozzáférés: https://www.mnb.hu/static/kpl/u5000/u5000.htm [megtekintve 2023.12.09.].*

Dokumentumok hamisítása

A különböző személyes dokumentumok és okmányok hamisítása egy másik veszélyforrás a fizikai bankbiztonságban. Az igazolványok, útlevelek és egyéb hivatalos személyes dokumentumok hamisítása pénzügyi intézményeknél és más ügyfélszolgálatoknál is előforduló jelenség. Ezek ellen a bankok rengetek átvilágítással és bizonyos időközönként történő adategyeztetéssel próbálnak védekezni leginkább. Ugyanis ez is egy módja lehet az illetéktelen hozzáférésnek, amivel más emberek pénzügyi adataihoz, rosszabb esetben megtakarításaikhoz és pénzükhöz férhetnek hozzá idegen rosszakarók.

ATM-ek védelme, pénzlopás

A pénzlopás és az ATM-ek kirablása állandó és már régóta fennálló kockázata a bankoknak, pénzintézeteknek.

A pénzautomaták kirablása a fizikai pénz lopásnak egy speciális fajtája, ahol az elkövetők erőszakot vagy egyéb más módszert használva próbálnak meg hozzáférni az automatában tárolt pénzhez. Az ATM-ek megóvásáért számos intézkedést alkalmaznak azok üzemeltetői. Legalapvetőbb az ATM-ek megfelelő elhelyezése, illetve az adott hely védelme. Legtöbbször nyilvános, világos helyen vannak elhelyezve, így ezek is növelik a biztonságot. A robbanásálló burkolat vagy a megerősített épületrész, nagyban megnehezíti a primitívebb rablási módok végrehajtását. Továbbá a videómegfigyelés és az ATM-ben beépített intelligens riasztórendszerek is egy védővonalat jelentenek. Ezenfelül a rendszeres ellenőrzés is segíti észlelni a manipulációkat vagy a szokatlan tevékenységeket. Ráadásul egy esetleges feltörés esetén festékpatronok vannak elhelyezve a pénz mellé, amik felrobbannak és így egyértelműen jelzik mindenki számára, hogy az lopott pénz vagy éppen a rablón, hogy ő volt az elkövető.

A bank fizikai biztonsága

Bankfiókok

A bankfiókok biztonsága kulcsfontosságú a pénzintézetek és az ügyfelek számára egyaránt. A fiókon belüli és kívüli biztonsági intézkedések összesége alkot egy megfelelő védelmet, ami elengedhetetlen ahhoz, hogy megvédje a bank az ügyfeleknek a vagyonát, az adatait, valamint a pénzintézet stabilitását és nem utolsó sorban hírnevét. Hiszen senki nem vinné a pénzét egy olyan helyre, amit esetleg már többször kiraboltak vagy egyéb más biztonsági szempontból nem megfelelő. A bankfiók biztonsága számos elemre bontható, például az épületek tervezése, technológiai védekezés, személyzet képzése és vészhelyzeti készültség.

Az épületek tervezésénél az egyik legfőbb a bankfiók biztonsága. Ennél a folyamatnál olyan szempontokat kell figyelembe venni többek közt, mint a környezet, ahol a fiók található, a megfelelő világítás vagy a könnyű átláthatóság. Ugyanakkor az ablakok és az ajtók tervezése különösen fontos, hogy ellenálljanak az esetleges betörési kísérleteknek. Az épületek biztonságát növelik még az elektronikus biztonsági rendszerek. Modern technológiai megoldások, mint például a riasztórendszerek, a zártkörű kamerarendszerek és a beléptető lehetőségek, hatékonyan hozzájárulnak a fiókok védelméhez. A kamerák nem csak az épület belső tereit figyelik meg, hanem monitorozzák az épület külső környezetében történő eseményeket is, ezzel is megakadályozva és dokumentálva a lehetséges fenyegetéseket.

A belső tér kialakítása és az elrendezése is lényeges tényező a bank létesítményeinek biztonságában. Az ügyféltér és a pénzkezelő területek megfelelő szétválasztása, az érzékeny területek korlátozott hozzáférésének biztosítása, valamint a pénzkezelő helyiségek és személyzet védelme mind-mind prioritást élveznek. A biztonsági pultok, a szakaszok és az egyéb fizikai akadályok is hozzájárulnak az értékek megfelelő biztonságához.

A személyzet megfelelő kiképzése és felkészítése egy újabb elengedhetetlen komponense a fizikai biztonságnak is. Az alkalmazottaknak egytől-egyig ismerniük kell a biztonsági eljárásokat, protokollt, vészhelyzeti tervet és a kockázatkezelési stratégiát. Ezek elsajátítását a bankok rendszeres oktatásokkal és szimulációs játékokkal segítik elő, így biztosítva, hogy az dolgozók megfelelően tudjanak reagálni kritikus helyzetekben, például egy rabláskor vagy betöréskor.

A pénzszállító és egyéb hasonló folyamatok speciális figyelmet igényelnek a bankfiókoktól. Az értékek szállítása során erősített járműveket és alaposan tapasztalt biztonsági személyzetet kell alkalmazni. Továbbá a modern technológia itt is segítségükre van, hiszen a GPS segítségével könnyen nyomot lehet követni a pénzszállítók mozgását, illetve a különböző titkosított kommunikációs eszközök segítségével könnyebb és biztonságosabb a kapcsolattartás.

Az alkalmazottak fizikai biztonságának fenntartásának érdekében szigorú azonosítási és beléptetési folyamatokat kell alkalmazni. A munkatársaknak pontosan a szabályzatnak és protokollnak megfelelően kell eljárnia és a személyzet hozzáférését az érzékeny területekhez korlátozni kell. Ezen felül a belső auditok és ellenőrzések egyaránt fontosok, annak érdekében, hogy biztosítva legyen a szabályok betartása és az eljárások átláthatósága, illetve észlelhessék az esetleges kockázatokat.

Összegezve, a bankfiókok fizikai biztonsága egy roppantul összetett védelmi rendszer. Elvégre a pénzintézetek biztonsága a gazdaság számára is felettébb fontos, mert egy-egy nagyobb bank összeomlása egy egész ország pénzügyi stabilitását is megingathatja.

A bankok biztonsági protokolljai, szabályai

A bankfiókok protokolljai, szabályai legalább olyan meghatározó részét jelentik a bankbiztonságnak, mint a technológiák vagy a fizikai akadályok. A bankfiók munkatársainak tudniuk kell az esetleges vészhelyzetekben mi a teendő, merre vannak a riasztó berendezések. Továbbá a riasztó berendezések működösét állandó időközönként ellenőrizni kell, illetve a dolgozók tudását is tesztelik. Vannak olyan szabályok, amiket a Nemzeti Bank ír elő és ezeket egészítik ki a gazdasági bankok saját igényük szerint. Ezek a dokumentumok részletes irányelveket, előírásokat tartalmaznak a pénzintézet minden területére. Az egyik irányelv általában az, hogy az emberi élet mentése az elsődleges. A bankoknak szigorú szabályozásra van szüksége a kockázatok maximális csökkentése érdekében. Kiterjednek ezek a szabályzások a jelszóval, PIN kóddal zárt ajtók, illetve egyéb eszközök frissítési gyakoriságára, illetve kötelező komplexitására.

A fizikai tranzakciók biztonsága

A banki tranzakciók védelme alapvető fontosságú az ügyfelek és a bankfiók részére is. A banki fizikai tranzakciók magukban foglalják azokat a pénzügyi műveleteket, amelyek során az ügyfelek személyesen részt vesznek, például készpénzfelvétel vagy befizetés, esetleg csekk kibocsátása vagy csekk befogadása.

Készpénzes tranzakciók védelme

A készpénzes tranzakciók biztonságos lebonyolításához elengedhetetlen az épület és a belső tér biztonsága, amit már ez előzőekben kifejtettem. Ezen felül az alkalmazottaknak mindenekelőtt azonosítani kell az ügyfelet, így meggyőződhetnek arról, hogy a megfelelő személy ül előttünk nem pedig visszaélni akarnak a személyes adatokkal. Ilyenkor van jelentősége a szintén már feljebb tárgyalt dokumentum hamisításnak, illetve annak kiszűrésének. Ennek a problémának a megoldására, illetve a folyamat felgyorsítására nagyszerű megoldás lehetnek a biometrikus azonosítási technológiák, mint ujjlenyomat- vagy arcfelismerés, amelyek már kezdenek elterjedni a fizikai azonosításkor, bár még egyelőre nem a bankfiókokban. Továbbá, ilyen esetben válik kiemelten fontossá a bankjegyhamisítás elleni védelem is, többek között egy készpénz befizetési ügylet esetén.

Pénzutalások és csekkek fizikai biztonsága

A pénzutalások és csekkek biztonsága egy specifikus része a bankok védelmének, ugyanis ezek a fizetési formák közvetlenül érintik az ügyfelek vagyonát, így nagy kockázatot hordoznak az átverések és visszaélések szempontjából. A pénzintézeteknek és az ügyfeleknek egyaránt fontos, hogy megfelelő intézkedésekkel és protokollal védelmezzék az ilyen fajta ügyleteket.

Bár a csekkek, mint fizetési forma már szinte teljesen kihalt a pénzügyi világból, mégis kitérnék rá, mivel a lehetősége a mai napig meg van az embereknek a használatára. A csekkek biztonságára vonatkozó szabályok kiterjednek a csekkírók és a csekkfogadókra is. A csekkíró felel a csekkfüzete biztonságáért és azért, hogy ne férje hozzá illetéktelen személy. Azonnal jelentenie kell a tulajdonosoknak, ha elveszett a csekkfüzetük. Továbbá a csekkhamisítás is egy valós veszély lehet így ez ellen is védekezni kell a pénzintézeteknek és a csekkel üzletelőknek is.

Virtuális bankbiztonság

A banki online tranzakciók biztonsága

Manapság talán fontosabbá vált a bankok virtuális biztonsága, mint maga a fizikai biztonság. Ugyanis rengetek pénzügyi tranzakció megy végbe online. Ennek megfelelően többen próbálkoznak virtuális támadni, pénz kicsalni. *„Általános az egyetértés abban, hogy az elektronikus úton történő bankhasználat legalább olyan biztonságos, mint a hagyományos, sőt még biztonságosabb is lehet. A hagyományoshoz képest azonban az elektronikus banki szolgáltatások igénybevétele során új veszélyek és hibaforrások keletkezhetnek, és ezeknek a hibáknak a kiküszöbölésére fel kell készülniük a bankoknak. A veszély jelentkezhet a banki oldalon, ügyféloldalon és a kommunikációs csatornában. A szakemberek általános véleménye, hogy az egyéb okokon túlmenően az elektronikus banki szolgáltatások igénybevételének legnagyobb gátló tényezője a kommunikációs csatornák iránti bizalom hiánya.”*[3]

Titkosítás és védelmi mechanizmusok a banki tranzakciók során

A titkosítás és más védelmi mechanizmusok kulcsfontosságú szerepet játszanak a bank tranzakciók során, mert ezek felelnek az ügyfelek pénzügyi adataiért, illetve a kiberbiztonság fenntartásáért. A modern pénzügyi rendszerben a legkifinomultabb kiberfenyegetésekkel kell szembenézni a bankoknak, így a titkosításnak és egyéb védelmi funkcióknak is a legújabbnak és legjobbnak kell lennie. Az elsődleges védelmi réteg a banki tranzakciók során a titkosítás.

Felhasználónév és jelszó védelme, kétlépcsős azonosítás

A felhasználónév és a jelszó védelme a digitális biztonság egyik alapvető biztonsági kérdése, az online platformokon való adatainkhoz való hozzáférés első védelmi vonala. A felhasználónév és a jelszó valaha egy kifinomult védelmi rendszernek számított, de mára már nem elegek az egyre nagyobb kiberfenyegetettség és szüntelenül fejlődő technológiák mellett a korszerű biztonság kielégítésére. A kétlépcsős azonosítás az egyik leggyakoribb és legeffektívebb módja ennek a védelemnek a kiegészítésére.

---

[3] *Szatmári Ferenc: Az elektronikus banki csatornák biztonsági kérdései és a fejlődési irányok [online]. BUDAPESTI GAZDASÁGI FŐISKOLA – MAGYAR TUDOMÁNY NAPJA, 2003. Hozzáférés: https://publikaciotar.uni-bge.hu/446/1/tek_2003_20.pdf [megtekintve 2023.12.09.].*

A felhasználónév és jelszó kombinációja a pénzügyek és bankok területén is az első védelmi vonal. A felhasználónevek sokszor nyilvánosak is lehetnek, de a jelszavak titkosak és csak a felhasználók számára hozzáférhetők. Ez egyben az ügyfélnek egy felelősség is, hogy senkivel ne ossza meg a jelszavát és lehetőleg ne is írja le sehova, a kockázat csökkentésének érdekében. Mindemellett, olyan erős jelszavak használata ajánlott vagy sok esetben már kötelező, ami tartamaz kisbetűt, nagybetűt, számokat, valamint speciális karaktert is. Továbbá a jelszavak hossza is nagyon fontos tényező. Ellenben a több helyen azonos jelszó használata és hosszú ideig változatlan jelszó mind a kiberbűnözők malmára hajtja a vizet.

2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

GIF HIVE SYSTEMS › Learn about our methodology at hivesystems.io/password

2020

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	61tm years	100tn years	7qd years

GIF HIVE SYSTEMS › Learn about our methodology at hivesystems.io/password

2. ábra Ennyi idő alatt törhetőek fel a jelszavak 2020, 2022

Hatalmas fejlődés tapasztalható a jelszavak feltörési idejében is sajnos. A Hive Systems frissítette a jelszavak brute-force, azaz automatizált találgatásával való feltöréséhez szükséges időt megbecsülő táblázatát. A 2022-es adatok alapján manapság 11 karakternél rövidebb jelszót nem érdemes használni, ráadásul kisbetű + nagybetű + szám komplexitás esetén is „csak" 3 évig tart a feltörés, míg a mixbe legalább egy különleges karaktert bedobva 34 évre ugrik a kitaláláshoz szükséges idő. Viszont fontos látni, hogy a hardverek számítási képességeinek gyors növekedése miatt rendkívüli sebességgel csökken a jelszavak kitalálásához szükséges idő. „*Természetesen ezek csak elméleti értékek, azonban a biztonság tudatosoknak manapság nem érdemes 12 karakter alá menniük, méghozzá kisbetű + nagybetű + szám + különleges karakter összetételben, ennek a feltörési idejét 2022-ben 3000 évre saccolta a Hive Systems. Ez orbitálisnak tűnhet, de ha így folytatódik a törési idő csökkenése, akkor 2030-re már nem sokat érnek majd ezek a jelszavak, előreláthatóan nyolc év élettartam racionálisnak mondható egy jelszó esetében.*"[4]

Ebben a táblázatban pedig jól látható, hogy még jobban csökkentek ezek az idők 2023-ra. Például, ha egy 10 egység hosszú, az összes ajánlott karaktert tartalmazó jelszót nézünk, akkor annak az utóbbi egy évben 5 hónapról 2 hétre csökkent a feltörési ideje, ami körülbelül tízszeres gyorsulást jelent. Ez is jól megmutatja, hogy a jelszavak nem elegendőek pénzügyi és személyes adataink védelméhez a digitális világban.

3. ábra Ennyi idő alatt törhetőek fel a jelszavak 2023

[4] *ORIGO: Ennyi idő alatt törhetőek fel a jelszavak [online]. 2022.03.21. Hozzáférés: https://www.origo.hu/techbazis/20220321-eros-jelszo-feltoresi-ido.html [megtekintve 2023.12.09.].*

A kétlépcsős azonosításnak az a célja, hogy egy plusz további réteget képezzen a fiókhoz való hozzáférések védelmében. Azon az elven alapul, hogy annak, aki belépni kíván az adott fiókba annak a jelszó és felhasználónév megadása mellett egy másik tényezőt is be kell mutatnia, így már legalább két különböző módon kell igazolnia az azonosságát. A szakirodalomban történelmileg három különböző faktort, kategóriát különböztetünk meg:

1. amit tudok (jelszó, PIN kód, születési dátum…)
2. amim van (SMS, telefonhívás, hardver token…)
3. aki vagyok (ujjlenyomat, retina, arc…)

Ugyanakkor egyre inkább terjed az alábbi két faktor is, amelyek nem teljesen sorolhatóak be a fenti három kategóriába, inkább azok mellett érdemes használni ezeket, de érdemes lehet külön beszélni róluk:

4. felhasználó jelenlegi és korábbi viselkedésén alapuló azonosítás (eszköz, szolgáltató, belépés időpontja…)
5. tartózkodási hely (GPS, IP cím geolokáció…)

Többfaktoros azonosítás esetén ezen faktorok/kategóriák közül minimum kettőből választunk minimum egy-egy elemet. Ez azért lényeges, mert mindegyik kategória esetén más-más gyengeségek vannak, amit a faktorok kombinálásával lehet kikerülni.

Az, amit tudok például általában időben állandó, vagy ritkábban változik és gyakran akár máshonnét is megszerezhető, más által is ismert, így, ha valaki egyszer hozzájutott, akkor később többször is fel fogja tudni használni észrevétlenül.

Ezzel szemben az, amim van kategóriába tartozó eszközök illetéktelen kezekbe jutását általában egyszer csak észreveszi a felhasználó, hiszen tipikusan egy megfogható valami, ami egyszerre csak egy embernél lehet ott. A következő belépésnél legkésőbb hiányozni fog. Egy hardver kulcs viszont bármilyen biztonságos második faktor, nem jó, ha önmagában is belépésre jogosít, hiszen elvesztése, ellopása esetén akármikor belépést biztosítana a tolvajnak.

Az, aki vagyok kategóriába tartozó azonosítók előnye, hogy elvileg nem ellophatók. Ugyanakkor általában komplex, drágább hardvert igényelnek (vagy az olcsó megoldások könnyen megkerülhetőek), ráadásul az ember élettartama alatt általában állandóak, nem megváltoztatható, ha „ellopják”. Ujjlenyomatot ma már például bármelyik politikustól lehet szerezni egy nyilvános eseményen készült, jó minőségő teleobjektíves fényképező segítségével, ezért fontos a jó minőségű – a biometrikus azonosítás esetén az élő embert, szövetet is ellenőrző eszköz használata. A biometrikus azonosítás általában nem egzakt, az olvasók gyengék, nem a teljes arcot, ujjlenyomatot látják, azok kicsit változnak, így gyakori, hogy annak ellenére, hogy a megfelelő ember szeretné magát azonosítani, az nem sikerül. Ennek lehet számos oka, fáradt arc, maszkhasználat, megvágott ujj, ugyanakkor a legtöbb gyártó ezt úgy küszöböli ki, hogy hasonlóságot néz, azaz kisebb-nagyobb eltéréseket enged, ez is gyengíti a biometrikus azonosítás minőségét. A biometrikus azonosításokra kiemelten igaz, hogy minél pontosabb, annál gyakrabban nem engedi be a tulajdonost se, és minél kevésbé szigorú, annál könnyebb megkerülni vagy enged be olyat, akit nem kéne.

A biometrikus azonosítóknak van még egy további hátránya, tárolásuk kockázatos, hiszen elvesztésük esetén a tulajdonosaik nem tudják kicserélni a tulajdonságaikat (ujjlenyomat, írisz…), és jogi akadálya is lehet (GDPR). Amennyiben egy adott fizikai eszközben tároljuk biztonságosan, akkor meg nem nyújt univerzális belépésre lehetőséget, csak azon az eszközön vagy annak az eszköznek a segítségével, ahol rögzítettük, amiben tároljuk.

A felhasználó jelenlegi és korábbi viselkedésén alapuló azonosítás egy komplex módszer akár több tíz, különböző, a felhasználóra és az eszközére jellemző tulajdonságot, és annak időbeli változását figyeli, és ebből von le következtetéseket, ez alapján ítéli meg a belépés kockázatát. Ilyen tulajdonságok lehetnek:

- eszközlenyomat (operációs rendszer, böngésző, képernyőméret, …),
- korábban már használt eszközök felismerése (pl. böngésző sütik segítségével),
- korábban használt internet szolgáltató, IP cím, geolokáció, időzóna,
- bejelentkezésre használt IP cím vagy szolgáltató reputációja,
- felhasználónévvel történt korábbi belépési kísérletek, incidensek,
- viselkedés alapú biometria (pl.: mobil tartás, képernyőkezelés, mozgás, egér használat, gépelési dinamika).

Ha nagyon szigorúan vesszük, akkor ezek jelentős részben az, amit tudok (pl. eszközlenyomat) és amim van (pl. szolgáltató/IP cím) kategóriákba tartoznak, de mivel számos rendszerben külön állítható, szűrhető és egyben alkotnak egy egységet, ezért érdemes külön kategóriaként, elemként tekinteni rá.

A viselkedés alapú faktort arra szokták használni, hogy egyfajta kockázatot mérjen és bizonyos kockázati szint alatt akár egy faktorral is beengedi, felette második faktort is kér, bizonyos szint felett pedig akár meg is tagadhatja a belépést vagy riasztást generálthat.

A felhasználó tartózkodási helyét is érdemes kiemelni külön faktornak, ugyanakkor mivel ezt általában nehéz megállapítani, illetve a felhasználó kontrollja alatt lévő eszköz esetén könnyű hamisítani, így külön faktorként ritkán alkalmazzák. Inkább az IP cím alapján a viselkedés alapú faktor része szokott lenni.

Azonosítási módok előnyei és hátrányai

Mindegyik lehetséges faktornak vannak előnyei és hátrányai, és vannak gyengébb és jobb megoldások is egy-egy lehetőségen, faktoron belül. Ez nem jelenti azt, hogy csak akkor érdemes bevezetni a második faktort, ha találunk egy tökéletesen biztonságos megoldást. A leggyengébb kétfaktoros megoldás is sokkal erősebb, mint az egyfaktoros, így a bevezetése mindenképp javasolt, számos esetben pedig alkalmazása jogszabályi kötelezettség is. A gyengébb ujjlenyomat olvasókat egy egyszerű fénymásolattal át lehet vágni ugyan, de már ehhez is meg kell szerezni az illető ujjlenyomatát, ki kell nyomtatni, odamenni a gépéhez, ami például már egy külföldön tartózkodó támadónak nem fog sikerülni.

Most nézzük sorra a különböző lehetséges faktorokat, illetve ezek közül a leggyakrabban használtakat, legrelevánsabbakat.[5]

[5] *OTP bank, Kibervédelmi Osztály: Többfaktoros azonosítás*

Amit tudok

PIN kód

A mobiltelefonok és bankkártyák miatt nagyon elterjedt, széles körben használt megoldás. Tipikusan egy 4-6 jegyű számsor. Vehetjük úgy is, hogy a csak számokból álló, rövid jelszavakat hívjuk PIN kódnak.

Tipikusan olyan helyen szoktuk használni, ahol a próbálkozások száma erősen korlátozott, és ha valaki sokszor próbálkozik, akkor a fiók, eszköz végleg zárol, és csak valami komplexebb, bonyolultabb módszerrel lehet utána bemenni.

Előnye:

- Nagyon egyszerűen használható.
- Könnyen megjegyezhető.

Hátránya:

- Sok felhasználó valami triviális kódot ad meg, ha ő választhatja (születési dátum, számsorozat).
- Könnyű kitiltani a felhasználót 3-5 hibás próbálkozással.
- Gyenge, általában csak másik faktorral együtt használható.

Hogyan lehet biztonságosabbá tenni:

- Mindenképp erősen limitálni kell a próbálkozások számát, mert egy 4 jegyű PIN kód esetén pl. csak 10 000 kombináció létezik.
- Másik faktorral együtt szabad csak használni.
- A leggyakoribb, legtriviálisabb pár PIN kódot le kell tiltani (születési dátum, 0123, 1234).
- Ha lehet inkább 6 hosszúságú PIN kódot használjunk.

Személyes adatok

A személyes adat tipikusan születési dátum, név, anyja neve szokott lenni, de van, hogy valamelyik személyazonosító irat vagy kártya száma is szóba jön egyes rendszerek esetében.

Előnye:

- Fejből tudják az emberek, vagy kéznél van az irat, amin rajta van.
- Tipikus ügyintézési szituációkban mindkét fél számára rendelkezésre áll, és ezért könnyű rákérdezni.

Hátránya:

- Nagyon sok személy által ismert (rokonok, ismerősök).
- Az internet és közösségi hálók világában könnyen kideríthető, akár idegenek számára is.
- Nem tekintenek úgy rá a felhasználók, mint védendő adatra, így könnyen ki is adják.

Hogyan lehet biztonságosabbá tenni:

- Önmagában ne használjuk.
- Igyekezzünk olyan adatokat bekérni, amelyek nem derülnek ki egy tipikus közösségi hálós profilból.
    - rossz: név, születési dátum
    - jobb: anyja leánykori neve, személyi igazolvány száma, lakcímkártya száma, valamelyik utolsó banki művelet adatai

Biztonsági kérdések

Valamilyen szinten a személyes adatok egy halmaza, de mivel a felhasználási terület eltér, ezért érdemes kiemelni itt is. Tipikusan több előre megadott kérdés közül kell első belépéskor 3-5 darabra megadni a megfelelő választ, és az elfelejtett jelszó esetén az felhasználó ezen kérdések helyes megválaszolásával vissza tud jutni a rendszerbe és meg tudott adni egy új jelszót.

Tipikusan ilyen kérdések szoktak lenni, hogy kedvenc zenekar, első házikedvenc neve, első tanár neve. Ezek olyan kérdések, amelyekre legtöbb ember esetében a barátai jelentős része akár fejből tudja a választ, de akik aktívan használják a közösségi hálókat, azok esetében akár mindenki más is.

Előnye:

- Fejből tudják az emberek a választ.

Hátránya:

- Nagyon sok személy által ismert (rokonok, ismerősök).
- Az internet és közösségi hálók világában könnyen kideríthető, akár idegenek számára is.
- Nem tekintenek úgy rá a felhasználók, mint védendő adatra, így könnyen ki is adják.
- Időben változhat, így egy évekkel ezelőtti választ nem biztos, hogy újra eltalál a felhasználó.

Hogyan lehet biztonságosabbá tenni:

- Sehogy. Ne használjuk! A biztonsági kérdéseket ne használjunk.

Bankkártya száma

Fontos megkülönböztetni a bankkártyát és a bankkártya számát. Előbbi egy fizikai eszköz, amelyen van egy nehezen, vagy egyáltalán nem másolható chip, így nem duplikálható, míg utóbbi (a száma) könnyen megosztható, másolható és mint ilyen nem is jelent akkora védelmet.

Előnye:

- Általában kéznél van.
- Időnként változik, változhat.
- Ritkán osztjuk meg, titokként kezeljük.

Hátránya:

- Internetes vásárlás esetén meg kell adni a fizetésnél, így mások által is ismert lehet.
- Boltban is elővesszük a kártyát és egy eltökélt támadó meg tudja szerezni egy mobiltelefon/fényképező segítségével.

Hogyan lehet biztonságosabbá tenni:

- Önmagában ne használjuk azonosításra.
- Vigyázzunk rá, a bankkártya adatok megadása semmilyen esetben nem teljesen biztonságos. Ezzel a szokással az adathalászok malmára hajtjuk a vizet.

Amim van

SMS üzenet

Valószínűleg kijelenthetjük, hogy ez a legelterjedtebb második faktor. Ma már majdnem mindenki rendelkezik mobiltelefonnal, így univerzálisan használható. Az SMS üzenetet a SIM kártya miatt kapjuk meg, azaz amikor visszaigazoljuk, begépeljük az SMS-ben megkapott kódot, akkor ezzel azt bizonyítjuk, hogy nálunk van a SIM kártya, hozzánk tartozik.

Előnye:

- Majdnem mindenki rendelkezik már mobiltelefonnal.
- Könnyen használható.

Hátránya:

- Kiküldése pénzbe kerül.
- Többféle támadással is megszerezhető. Akár felhasználói interakció nélkül is.

Hogyan lehet biztonságosabbá tenni:

- Az SMS üzenet végére kell tenni a kódot, hogy a zárolási képernyőn ne jelenjen meg.
- Az SMS üzenetbe bele kell tenni minél több információt, hogy ki és hol kérte a kódot, hogy lehessen látni, hogy miért jött (internetbanki belépés, 10e Ft átutalása…).

Telefonhívás

Nagyon hasonlít az SMS-hez, csak nem egy SMS-ben kapott kódot küldünk vissza, hanem egy telefonhívást veszünk fel, és nyomunk meg egy gombot, amivel visszaigazoljuk, hogy mi kezdeményeztük a belépést, mienk az adott telefonszám.

Előnye:

- Majdnem mindenki rendelkezik már mobiltelefonnal.
- Asztali telefonok esetében is jól működik.
- Könnyen használható.

Hátránya:

- Pénzbe kerül.
- Többféle támadással is megszerezhető. Akár felhasználói interakció nélkül is.
- Érzékeny „kifárasztásos támadásra”, ahol a támadók addig próbálnak belépni (hívogatják a felhasználót) amíg ő meg nem unja és jóvá nem hagyja, hogy legyen vége a hívásoknak.

Hogyan lehet biztonságosabbá tenni:

- Korlátozni kell a hívások számát.
- Ha nem mindig ugyanazt kell begépelni, hanem az a felület, amelyiken be szeretnénk lépni ad egy kódot, amit vissza kell írni, akkor azzal jelentősen növeltük a biztonságát, mert akkor a felhasználó tudja, hogy mit hagy jóvá, nem csak jön egy hívás, körülbelül akkor, amikor úgyis épp be szeretne lépni.

IP cím

A legtöbb felhasználó az IP címét nem tudja megválasztani, és időben változhat is, de vállalati felhasználók, cégek esetében gyakran állandó. Ha más módszer nincs az adott belépés ellenőrzésére, akkor a megfelelő IP cím ellenőrzése, kikényszerítése jó védelem lehet egy ellopott hozzáféréssel való visszaélés vagy elbocsátott munkavállaló általi csalás megelőzésére.

Előnye:

- Általában könnyen implementálható.
- A felhasználó számára átlátszó.

Hátránya:

- Van, akinek nem állandó az IP címe.
- Home Office esetén nem működik, csak ha megfelelő VPN szolgáltatása van a felhasználónak.
- Időnként változhat a fix IP cím is (pl. szolgáltató váltás).

Hogyan lehet biztonságosabbá tenni:

- Az IP cím szűrés egy hatékony eszköz lehet a jelszólopások elleni védekezésben, de egyéb második faktor mellett, harmadik elemként kell használni.

Bankkártya

Ez alatt a fizikai bankkártyát értjük. Fontos megkülönböztetni a bankkártya számától, amit használunk bizonyos esetekben azonosításra. Bankkártyát csak fizetéseknél, pénzfelvételnél használunk. Ott a PIN kóddal együtt már kétfaktoros azonosításnak számít. Ellenben internetes fizetésnél már nem a bankkártyát használjuk, hanem annak az adatait.

Előnye:

- Nehezen másolható, biztonságos.
- Van hozzá tartozó második faktor.

Hátránya:

- A bankkártya tipikusan csak POS terminálokban és bankautomatákban használható.
- Kártyaolvasó kell hozzá.
- Drága a beszerzése.
- Napi használat esetén törik, kopik, rendszeres időnként cserélni kell.

Hogyan lehet biztonságosabbá tenni:

- Felhasználók azonosítására, informatikai rendszerben (ha most a bankautomatát nem vesszük annak) nem használjuk a bankkártyát, de az egyéb smart card-ok erre alkalmasak és használatosak is.

Időalapú kód (authenticator app)

Az időalapú kód egy olyan megoldás, ahol tipikusan 30 másodpercenként új, egyszeri azonosításra használt kódot generál egy alkalmazás. A kliens és szerver az első alkalommal megállapodnak egy véletlen számban, amit tipikusan a szerver ad át egy számsor vagy QR kód formájában a kliensnek, és később ennek a birtokában, és a pontos idő segítségével tudják minden időpillanatban, hogy éppen melyik az aktuális kód.

Előnye:

- Viszonylag egyszerű használat.
- Internet nélkül, offline is működik.
- Több készüléken is működhet párhuzamosan.

Hátránya:

- Több készüléken is működhet párhuzamosan. Nehéz ellopni, de ha megtörténik, akkor nem veszi észre a felhasználó.
- Van asztali gépre készült változata, nem kényszeríthető ki, hogy egy biztonságos alkalmazásban, egy biztonságos telefonra telepítse, azon használja a felhasználó.

Hogyan lehet biztonságosabbá tenni:

- Naprakész frissítéssel rendelkező, nem feltört mobiltelefonon legyen fent.
- Ne az asztali gépen vagy laptopon fusson, mert akkor egy eszköz kompromittálásakor mindkét faktor sérülhet.
- Fontos, hogy egy adott kód csak egyszer fogadható el (különben lopható/másolható lenne). Ha újabb belépést kell jóváhagyni, meg kell várni a következő kódot.
- Próbálkozások számát korlátozni kell, hiszen 1 000 000 a lehetséges kombinációk száma (sőt az időeltolódást kiszűrendő tolerancia miatt néha egy időben két kód is van, amit elfogad a rendszer).
- Az alkalmazás feloldását érdemes jelszóhoz, PIN kódhoz vagy biometrikus azonosításhoz kötni.
- Önmagában azonosításra, védelemre nem alkalmas.

Időalapú kód (fizikai token)

Létezik hardver alapú megvalósítása is az OTP-nek, itt is bizonyos időközönként új, egyszeri azonosításra használt kódot generál az eszköz, amit le kell olvasni a kijelzőről és be kell gépelni a megfelelő helyre.

Előnye:

- Viszonylag egyszerű használat.
- Nem másolható le/át másik készülékre.

Hátránya:

- Drága hardver.
- Fizikai eszközöket kell menedzselni, kiosztani, támogatni, pótolni, ha ellopják, elveszítik.

Hogyan lehet biztonságosabbá tenni:

- A biztonsága alapvetően adott, ezek általában kulcsrakész megoldások.
- Ha mi implementáljuk a szerver oldali részét, akkor ugyanazokra kell figyelni, mint a szoftveres OTP esetén.
- Azon eszközök, amelyek PIN kódot kérnek a feloldáshoz biztonságosabbak, magukban megvalósítanak két faktort.

Push üzenetek (mobiltelefon applikáció)

A felhasználó egy telepített mobiltelefon alkalmazásban kap egy push üzenetet, és vagy jóvá kell hagynia vagy elutasítania a belépést, vagy valamilyen számsort kell beírni a mobiltelefonba a jóváhagyáshoz, amelyik azon a képernyőn jelenik meg, amelyiken a kétfaktoros belépést kezdeményeztük.

Előnye:

- A felhasználó általában valamilyen módon be van léptetve az alkalmazásba, így ellenőrizhető, hogy milyen készüléken futtatja és megakadályozható a két készüléken való párhuzamos működés.
- A számellenőrzős megoldással kimondottan biztonságosnak számít.

Hátránya:

- Aktív internet kapcsolatot igényel a mobiltelefonon.
- Számellenőrzés nélkül érzékeny „kifárasztásos támadásra”, ahol a támadók addig próbálnak belépni (küldenek push üzenetet a felhasználónak) amíg ő meg nem unja és jóvá nem hagyja, hogy legyen vége a felugró ablakoknak.

Hogyan lehet biztonságosabbá tenni:

- A számellenőrzés jelentősen javítja a biztonságát, ha műszakilag megoldható be kell kapcsolni.
- Naprakész frissítéssel rendelkező, nem feltört mobiltelefonon legyen fent.
- Lehetőleg ne az asztali gépen/laptopon fusson, mert akkor egy eszköz feltörése esetén mindkét faktor sérülhet.
- Amennyiben befolyásolható, akkor a push üzenetbe bele kell tenni minél több információt, hogy ki és hol kérte, hogy lehessen látni, hogy miért jött (internetbanki belépés, 10e Ft átutalása…).

Hardver kulcs (FIDO)

A hardver kulcsos azonosítás a felhasználó számára tulajdonképpen azt jelenti, hogy amikor a szerver felszólítja erre, akkor bedugja az USB-be, vagy a telefonjához közel tartja a hardver kulcsot, megnyom rajta egy gombot és ezzel kész is az azonosítás. A gombnyomás helyett van amelyik kulcs például PIN kódot kér, vagy ujjlenyomatot ellenőriz.

A legismertebb a FIDO protokoll, amelyik úgy működik, hogy a kliens generál egy publikus és privát kulcsot, és a privát kulcsot megtartja (ez van a fizikai kulcson) a publikusat meg megosztja a szerverrel vagy szolgáltatással. Az ellenőrzéskor a kliens egy a szerver által adott műveletet végez el, amivel bizonyítja, hogy nála van a privát kulcs. A privát kulcsot a legtöbb eszköz védi, és csak valamilyen felhasználói interakció után használható aláírásra a kulcs, ezzel is megakadályozva, hogy a gépben felejtett eszköz mindent aláírjon, ami szembe jön vele. A protokoll úgy működik, hogy a hardver kulcs minden egyes rendszerhez egy egyedi kulcspárt generál, azaz nem lehet a különböző rendszerekben tárolt kulcsok alapján a felhasználókat összerendelni.

Előnye:

- Nagyon biztonságos.
- Modern böngészők már támogatják.

Hátránya:

- Drága hardver.
- Fizikai eszközöket kell menedzselni, kiosztani, támogatni, pótolni, ha ellopják, elveszítik.
- Nem minden belépési mód támogatott vele, régi eszközök, mobiltelefonok esetében gondot okozhat a használatuk.

Hogyan lehet biztonságosabbá tenni:

- Alapvetően az egyik legbiztonságosabb második faktor. Alapból is megfelelő a biztonsága.
- Tovább növelhető a biztonsága, ha pin kódot vagy ujjlenyomatot is megkövetelünk, nem csak gombnyomást.

Szoftver kulcs, tanúsítvány

Hasonló, mint a hardver kulcs, csak a privát kulcs nem egy célhardveren kerül eltárolásra, hanem a kliens eszközön. Vagy szerver, vagy a kliens generálnak kulcspárokat és a kliens megkapja a saját privát kulcsát, a szerver pedig ismeri a publikusat. Ezek alapján tudja azonosítani.

A jelszavakhoz képest nagy előrelépés a biztonság szempontjából, de legtöbbször, ahogy a jelszót is, önmagában, „egyfaktorosan” használják.

Vannak olyan megoldások, ahol a hardver/szoftver kulcs kicsit keveredik, ilyen a legújabb Passkey10 authentikáció. Ahol a privát kulcsot tipikusan az adott eszköz biztonsági hardver moduljába tárolják le. De a Passkey ezt nem követeli meg, így lehet máshogy is tárolni, jelszókezelők is támogatják, azok is el tudják tárolni, és a felhasználó eszközei között meg is osztják.

Előnye:

- Egyszerű implementáció.
- Passwordless belépésnél egy jó faktor, mert jól elrejthető a felhasználó elől.

Hátránya:

- Nem olyan elterjedt még. Kevés eszköz/rendszer támogatja.
- A privát kulcsok tárolásának a módja erősen befolyásolja a biztonságát.
- Amennyiben több eszközről is be szeretnénk lépni, akkor vagy több privát kulcs kell, amit a szervernek támogatnia kell, vagy meg kell oldani a privát kulcs biztonságos eljutását a felhasználó összes eszközére (sok megoldás ezt tudja alapból).

Hogyan lehet biztonságosabbá tenni:

- Másik faktor mellett alapvetően biztonságos.
- A privát kulcsok tárolását minél biztonságosabbá kell tenni, lehetőleg hardver modulba.
- Eszközönként egyedi kulcs is növeli a biztonságot, mert akkor egy támadó nem tud / nehezen tud új eszközt hozzáadni egy létező kulccsal.

Aki vagyok

Ujjlenyomat

Az ujjlenyomattal való azonosítás a modern mobiltelefonok elterjedésével vált igazán hétköznapivá. Számos egyéb helyen is megtalálható (laptopok, hardver kulcsok, beléptetőrendszerek), de arányaiban sokkal kevesebb eszközön.

Előnye:

- Mindig kéznél van.
- Elvileg teljesen egyedi minden ember esetében.
- Könnyű a használata.
- Gyakran a lokális eszköz hardver moduljában kerül tárolásra/ellenőrzésre, így nem képződik egy nagy központi tár ujjlenyomatokkal.

Hátránya:

- A gyakorlati megvalósítás általában gyengébb, támadható.
- A kliens oldal sértetlenségének ellenőrzése, az ellenőrzés megbízhatósága kulcsfontosságú, amennyiben a teljes folyamat kliens oldalon történik.
- Ha megsérül, nedves, száraz valaki keze, akkor gyakran nem működik.
- Van, akinek foglalkozásából vagy korából adódóan gyengébbek, rosszabbul láthatóak az ujjlenyomatai, és az érzékelő nem, vagy nagyon nem megbízhatóan ismeri fel.
- Legtöbb számítógép nem rendelkezik olvasóval, vagy nem jó minőségű olvasóval rendelkezik.
- Tárolása kockázatos és jogi akadálya is lehet.

Hogyan lehet biztonságosabbá tenni:

- Jó hardvert kell beszerezni.
- Minden esetben érdemes másik faktorral együtt használni, nem önmagában.

Arcfelismerés

Ez az azonosítás is a mobiltelefonokkal terjedt el igazán. A legegyszerűbb megoldások csak egy képet néznek, azok bármilyen fényképpel megkerülhetőek. A jobb megoldások már térbeli alakot is néznek, így sokkal biztonságosabbak. Utóbbi megoldást fogadja el a Microsoft is a Windows Hello belépéshez is.

Előnye:

- Mindig kéznél van.

Hátránya:

- Bizonyos helyzetekben nem megy: reggeli álmos fej, maszk…
- Legtöbb számítógép nem rendelkezik megfelelő minőségű (infra) kamerával.
- A jó minőségű kamerák drágák.
- Tárolása kockázatos és jogi akadálya is lehet.

Hogyan lehet biztonságosabbá tenni:

- Jó minőségű, 3D-s, infra kamera és megfelelő szoftver/algoritmus használata.
- Minden esetben érdemes másik faktorral együtt használni, nem önmagában.

Hangfelismerés

A hangfelismerés főleg telefonos ügyfélszolgálatok esetében használt azonosítási módszer, ugyanakkor a mesterséges intelligencia és a hanggenerátorok elterjedésével egyre inkább kérdéses a megbízhatósága. Extra védelemnek jó lehet, ugyanakkor ma már pár tíz másodpercnyi beszédből is létre lehet hozni valaki hangjának a másolatát, és a technika folyamatosan fejlődik.

Előnye:

- Mindig kéznél van.
- Nagyon egyszerű a használata.

Hátránya:

- Bizonyos helyzetekben nem működik: rekedtség, betegség.
- Be kell tanítani.
- Könnyen hamisítható.
- Tárolása kockázatos és jogi akadálya is lehet.

Hogyan lehet biztonságosabbá tenni:

- Alacsony kockázatú műveletek esetén használható másik faktorral együtt.
- Egyéb megbízható azonosítási folyamat mellett kiegészítő biztonságnak jó lehet.

Graboxy

A Graboxy egy biometrikus azonosítási módszer, amely az egérmozgást használja fel a személyek azonosítására. A betanításhoz, illetve a belépéshez egy kis útvesztőn kell végig vezetni a kurzort, ami közben az elemzi az egérkurzor mozgását, majd döntést hoz, hogy beléphetünk-e. Amennyiben nem sikerül az azonosítás, ami lehet egy hardverváltozás, vagy a kéz sérülése, változása is, akkor egy biztonsági második faktor szükséges.

Útvesztő az azonosításhoz, betanításhoz

A másik mód, ahogy használható, hogy munka közben figyeli az egérmozgást, és elemzi, hogy az egyezik-e a felhasználóról eltárolt adatokkal. Ha azt veszi észre, hogy változott a felhasználó személye, akkor képes riasztani, és zárolni a gépet.

Előnye:

- Viszonylag egyszerű működés.
- Képes a folyamatos azonosításra és a lezárolatlan gépek átvételéből eredő kockázatok csökkentésére.

Hátránya:

- Bizonyos helyzetekben nem működik: más beviteli eszköz, kézbetegség.
- Be kell tanítani.
- Mivel nem annyira megbízható, csak más faktor mellet egy kényelmesebb alternatívaként működőképes.
- Jogi akadálya is lehet.
- Még nem teljesen kiforrott, nem dobozos termék, fejlesztés is szükséges lehet.

Hogyan lehet biztonságosabbá tenni:

- Egyéb megbízható azonosítási folyamat mellett kiegészítő biztonságnak jó lehet. (Ha harmadik faktornak használjuk, a munkamenet védelmére, akkor erősítheti a védelmünket.)

„Fél” faktor

Bizonyos rendszerekbe csak nagyon nehezen vagy egyáltalán nem lehet második faktort bevezetni. Ennek lehetnek műszaki, anyagi okai, vagy akár a felhasználók köre nem teszi lehetővé, hogy ilyen adatokat bekérjünk vagy rájuk kényszerítsük. Ilyenkor érdemes olyan második lépcsőket bevezetni, amelyek nem teljesen vagy nem függetlenek az elsőtől, így nem számítanak rendes második faktornak, de a megszokott egyfaktoros belépéshez képest jelentősen javítják a fiókok biztonságát.

Ilyen „fél” faktor lehet az e-mailre kiküldött kód vagy link. Mivel nem kizárt, hogy egy felhasználó ugyanazt vagy hasonló jelszót használ az e-mail postafiókjába való belépésre is, mint az adott rendszerben, így ez lehet, hogy nem ad plusz védelmet, de a legtöbben azért már az e-mail postafiókjukat jobban védik, mint az egyéb adataikat. Ráadásul a nagy szolgáltatók legtöbbször kikényszerítik a kétfaktoros belépést, és elég erős védelemmel rendelkeznek illetéktelen belépések ellen is. Ma már egy Gmail postafiókba a jelszó ismeretében se biztos, hogy bejut egy támadó. Nagyon jó védelem lehet ez a jogosultság alap szintű ellenőrzésére is, hiszen egy üzleti partner vagy akár banki alkalmazott, a munkaviszonya befejeztével a céges levelezéséhez már nem fér hozzá, azaz ilyenkor már a korábban használt felhasználónév-jelszó páros ismeretében se fog tudni belépni az adott rendszerbe, mivel az e-mail címére kiküldött ellenőrző lépést nem fogja tudni megkerülni.

Előnye:

- Mindenki rendelkezik e-mail címmel.
- Széles körben elterjedt, ismert megoldás.
- Könnyű implementálni és bevezetni.
- Hivatali e-mail címek esetén azt is lehet vele ellenőrizni, hogy még ott dolgozik-e valaki.

Hátránya:

- Nem kétfaktoros belépés, általában nem független az első faktortól.

Hogyan lehet biztonságosabbá tenni:

- Csak akkor használjuk, ha a rendes kétfaktoros belépés bevezetésének komoly akadálya van.
- Önmagában ne használjuk beléptetésre.
- Jelszó kiváltására, egy független (nem, amit tudok) és biztonságos második faktor mellett használható.
- Harmadik lépcsőnek, kétfaktoros belépés kiegészítésére, főleg partnerek céges fiókjaihoz kötve, ajánlott a használata nagyobb kockázatú belépésekre.

Banki weboldal és alkalmazások biztonsága

Hogyan tudják a bankok biztosítani, hogy a szolgáltatásaik biztonságosak legyenek? Az alábbi megoldásokat használhatják, hogy az internetbank és a mobil netbank biztonságosabb legyen mindenki számára.

Internetbank

A banki rendszerek tűzfalak mögött működnek, ezek feladata, hogy kiszűrjék az illetéktelen és a nem biztonságos internetkapcsolódásokat, így segítenek megvédeni azokat az adatokat, amelyeket az ügyfél a banknak küld, illetve a bank a felhasználókról tárol. Az ügyfél és a bank között utazó adatokat az internetbank használatakor titkosított csatorna segítségével védi meg attól, hogy azokat mások megismerjék, megváltoztassák. Az internet nyílt természete miatt a rajta közlekedő adatok menet közben elfoghatók, módosíthatók, mivel számos eszközön haladnák át, amíg elérik a céljukat. Egy átutalás esetén az Ön által megadott adatokat mind a lehallgatástól, mind a menet közben történő átírástól védeni kell. A netbanki oldalak elérésekor és használatakor a titkosítatlan http helyett védett https kapcsolat épül fel az ügyfél gépe és az intézmény webszervere között. Erről a böngésző címsorában megjelenő https:// feliratból lehet megbizonyosodni. A felhasználónak tudnia kell továbbá, hogy az internetes művelet során az adatait valóban a bankja részére adja át, ezt a címsor mellett található lakat ikon jelzi, és részleteit az ikonra kattintás segítségével tudja megtekinteni. Ennek során ellenőrizheti azt is, hogy a független szolgáltató által kibocsátott tanúsítvány az adott bank nevére szól-e és érvényes-e. Természetesen itt is ajánlott a kétlépcsős azonosítási folyamat használata, ami tovább nehezíti a csalók dolgát.

Mobilbank

Mobilbank esetében az internetbankhoz hasonló biztonsági eszközöket alkalmazhatnak az intézmények. Tűzfalvédelem és titkosított kommunikációs csatorna annak érdekében, hogy az ügyfelek adatait más ne hallgathassa le és ne módosíthassa. A mobilbank aktiválásához és használatához egyszer használatos kód küldése a felhasználó által megadott telefonszámra. Továbbá az alkalmazás csak arról az eszközről használható, amelyre a mobilalkalmazást regisztrálták. Ezenfelül a feloldásához szükséges PIN-kód vagy minta, hogy az eszköz esetleges megszerzésével más ne adhasson utasítást a tulajdonos bankjának, és a személyes adatok biztonságban legyenek. Mindemellett a tárolt adatok titkosítása, hogy az ügyfél által megadott bejelentkezési és egyéb adatokat más alkalmazás segítségével se lehessen kinyerni. Egyes bankok, annak érdekében, hogy az adatok titkosságát megőrizzék, korlátozzák, hogy milyen eszközön futtatható az alkalmazás. Azonkívül a bank rendszerei figyelik az azonosítási, illetve belépési próbálkozások számát, és meghatározott sikertelen próbálkozás után kitiltják az ügyfelet a rendszerből, továbbá inaktív ügyfél esetén néhány perc után bontják a kapcsolatot. A bankok rendszerei a mobileszközről indított kapcsolódásokat, utasításokat is naplózzák a visszaélések felderítése céljából.

Telebank

Telefonos ügyintézés esetén a felhasználó adatait többszintű ügyfél-azonosítási rendszer védi, amely általában ügyfélkódot és jellemzően megváltoztatható telefonos PIN-kódot tartalmaz. A személyre szóló információk és bizonyos megbízások telefonos intézése kizárólag személyre szóló ügyfélkód és telefonos PIN-kód megadásával lehetséges. A rendszerbe való meghatározott számú sikertelen azonosítási, belépési próbálkozás csak úgy, mint a mobilbank esetében a szolgáltatás ideiglenes letiltását eredményezi. A Telebankon keresztül folytatott beszélgetéseket rögzítik, tartalmuk utólag ellenőrizhető.[6]

---

[6] *Magyar Nemzeti Bank: Intézményi biztonság [online]. Hozzáférés: https://www.mnb.hu/fogyasztovedelem/bankszamlak/elektronikus-banki-szolgaltatasok/intezmenyi-biztonsag [megtekintve 2023.12.09.].*

Személyes adatok és online identitás védelme

A személyes adatok védelme az egyik legfontosabb kihívás a digitális korban, ahol az emberek többsége részt vesz különböző online tevékenységbe, amikbe az online bankolás, pénzügyi ügyintézés is beletartozik. Az internet használat számos előnnyel jár, de ugyanakkor növeli az adatbiztonsági kockázatot is.

Az erős jelszóválasztás, a kétlépcsős azonosítás és egyéb más védelmi mechanizmusok itt is rendkívül fontosok. Ezek már nagyban csökkentik a veszélyeztetettséget. Továbbá a személyes adatok online megosztásának körültekintő kezelési elengedhetetlen. Az embereknek tisztában kell lenniük azzal, hogy milyen információkat osztanak meg magukról az online platformokon, akár a bankkal vagy egyéb pénzügyi ügyintézés során. Továbbá arra is felkell készülni, hogy milyen következményekkel járhat különböző adatok nyilvánosságra kerülése. Kerülni kell az érzékeny adatok, például születési dátum, lakcím vagy személyigazolvány szám megadását megosztását, nyilvánosságra hozását, illetve amennyiben nem lehet kitérni ezek megadása elől, akkor csak a minimális, kötelezően kért adatokat ajánlott megadni.

Ezenfelül az emberek oktatására és tájékoztatására is nagy hangsúlyt fektet számos bank. Ugyanis nem csak a pénzügyek terén, de általánosságba is a biztonságos internetes böngészési szokások kialakítási is kiemelten jelentős a személyes adatok védelmében. A biztonságos internetezés magában foglal olyanokat, mint megbízható webhelyek használata, URL-ek figyelmes ellenőrzése, valamint a kétes e-mailek vagy sms-ek felismerése és elkerülése. Az embereknek lehetőségük van többféle olyan szoftveres megoldást is alkalmazni online identitásuk védelmében, mint vírusirtók vagy tűzfalak.

A személyes adatok védelmi rendszerében szerepe van az államilag meghozott adatvédelmi jogszabályoknak és szabályozásoknak. Ezek célja, hogy megadják, hogy a szolgáltatók, miképpen használhatják és tárolhatják a felhasználók adatait és garantálják az egyének jogait. A GDPR (General Data Protection Regulation) az Európai Unióban példa a személyes adatok védelmét szigorúan szabályozó jogszabályra.

Adatlopás elleni intézkedések

Az adatlopás, különösen a pénzügyi szektorban, komoly kihívás elé állítja a pénzintézeteket. A pénzügyi intézmények számára az ügyfelek bizalmának megőrzése és az érzékeny adatok védelme kulcsfontosságú. Az adatlopás elleni intézkedések kialakításában és fenntartásában a pénzügyi szektor számára számos stratégia merül fel.

Egyik alapvető megközelítés a szigorú titkosítási rendszerek bevezetése. Az érzékeny adatok, mint például banki tranzakciók vagy személyes információk, erős kriptográfiával kell védeni, hogy megelőzzük az illetéktelen hozzáférést. A modern titkosítási technológiák alkalmazása nélkülözhetetlen a pénzügyi szolgáltatások online térben történő nyújtásában, ahol az adatok számos ponton mozognak.

Az aktív és passzív kiberbiztonsági megoldások bevezetése is fontos lépés. Az aktív védekezés magában foglalja a folyamatos figyelést és az esetleges fenyegetésekre való azonnali reagálást, például a kiberfenyegetéseket szimuláló gyakorlatokat és a rendszeres biztonsági frissítéseket. A passzív védekezés részeként a pénzintézeteknek részletes és átfogó kiberbiztonsági protokollokat kell kidolgozniuk, beleértve az adatvédelmi irányelveket és az alkalmazott biztonsági intézkedéseket.

Az ügyfelek tudatosságának növelése és az oktatás is kulcsfontosságú. A pénzügyi intézményeknek aktívan kell részt venniük az ügyfelek felvilágosításában, hangsúlyozva az online biztonság fontosságát, és javasolva az erős jelszavak használatát, valamint a kétlépcsős azonosítást. Az ügyfelek felvilágosítása és az online biztonság iránti tudatosság növelése hozzájárulhat az adatvédelem erősítéséhez.

A kiberbiztonság terén a szektoron belüli együttműködés is létfontosságú. A pénzintézeteknek és más érintett feleknek meg kell osztaniuk az információkat a kiberfenyegetésekről és a biztonsági incidensekről, hogy minél gyorsabban és hatékonyabban reagálhassanak az esetleges támadásokra. Az iparágon belüli szabványok kialakítása és az egységes protokollok alkalmazása is elősegítheti a kiberbiztonsági védelmi rendszerek összehangolását.

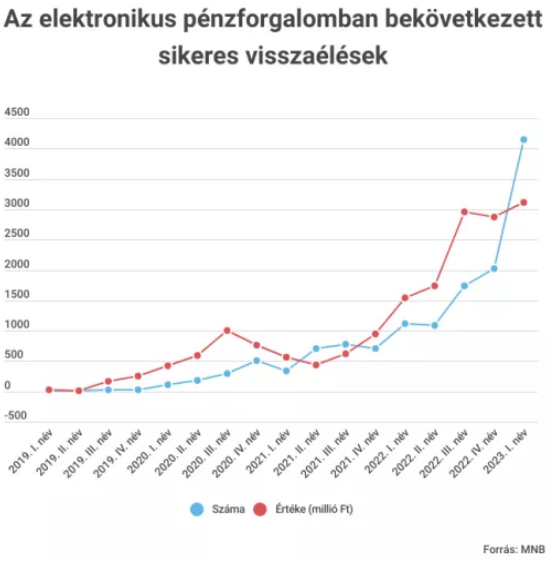
Végezetül, a folyamatos fejlesztés és innováció is elengedhetetlen. A pénzügyi szektorban mindig lépést kell tartani az új technológiákkal és azok kiberbiztonsági kihívásaival. A mesterséges intelligencia és gépi tanulás alkalmazása a kiberbiztonsági rendszerek fejlesztésében segíthet az ismeretlen fenyegetések gyorsabb azonosításában és azok elleni hatékonyabb védekezésben.

Ezen intézkedések kombinációja teszi lehetővé a pénzügyi szektor számára, hogy erős védelmi rendszert hozzon létre az adatlopások ellen. A pénzintézeteknek folyamatosan fejleszteniük kell a kiberbiztonsági stratégiáikat, figyelembe véve az új kihívásokat és a technológiai változásokat annak érdekében, hogy az ügyfelek pénzügyi adatait hatékonyan védelmezzék.

Bankvédelem Magyarországon

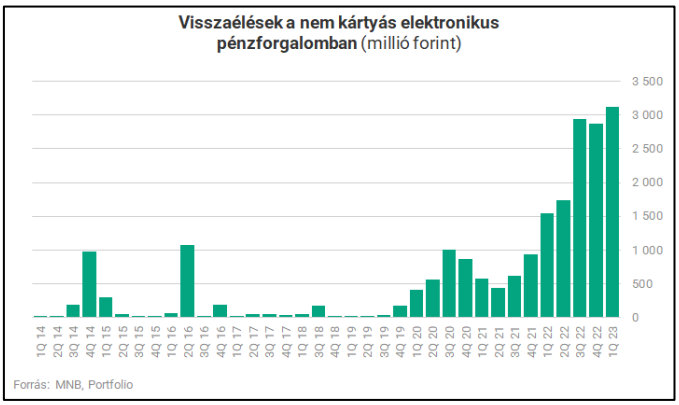
A Magyarországon elkövetett csalások fajtái, statisztikái

A mellékelt diagrammon jól látható, hogy 2022 3. negyedévében elkezdtek abba az irányba elmenni a csalással, visszélésekkel próbálkozók, hogy inkább többször próbálnak kisebb összegeket kicsalni az emberekből, ugyanis ennek köszönhető, hogy az elmúlt időkben a visszaélések száma rohamosan nőtt, míg az értéke stagnált. Valószínűsíthető, hogy ennek az állhat a hátterében, hogy ez embererek a kisebb összegek után nem mennek annyira, így nagyobb valószínűséggel usszák meg az elkövetők.

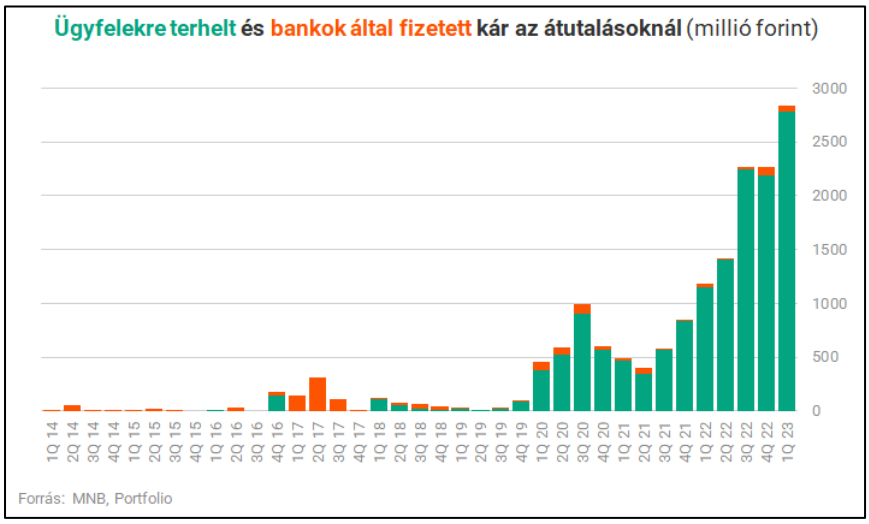


4. ábra Az elektronikus pénzforgalomban bekövetkezett sikeres visszaélések 2019-2023 I. félévig

Ezen a grafikonon, megfigyelhetjük, hogy a nem kártyás visszaélések értéke az elmúlt 3 évben nagyon gyorsan nőtt. Ez azt jelenti, hogy míg régebben a legnagyobb visszaélések kártyán keresztül történtek, addig az elmúlt években más módon is nagy összegeket csalnak ki az ügyfelektől az elkövetők.



5. ábra Visszaélések a nem kártyás elektronikus pénzforgalomban



6. ábra Ügyfelekre terhelt és bankok által fizetett kár az átutalásoknál

Ez az ábra pedig azt mutatja meg, hogy a visszaélések és csalások által okozott kár, hogy változott és arányaiban, hogy oszlott meg az ügyfelek és a bankok között. Láthatjuk, hogy 2017-ben szinte a károk teljes részét átvállalták a bankok. Utána viszont mindig az ügyfelekre terhelt összegek voltak a nagyobbak, illetve 2020-től az összes kár összege is jelentősen megugrott és utána is egy kis stagnálás után tovább nőtt. Ez feltehetően azért alakult így, mert amíg viszonylag kis összegű és kevés ilyen visszaélés volt, addig a bankok nem foglalkoztak igazából vele. Azonban mikor ezeknek a száma és összege is megnőtt, akkor kidolgozták a pénzintézetek az ennek megfelelő szabályzatot és protokollt. Ami általában tartalmaz olyan leírást, hogy amennyiben az áldozat bármilyen szinten segíti az elkövetőt vagy megad akármilyen információt akár akaratán kívül is, abban az esetben a bank nem vállalja át a károkat semmilyen esetben. A legtöbb esetben sajnálatos módon az áldozatok kiadnak valamilyen érzékeny adatot, ami által meg tud történni a visszaélés, csalás és ennek köszönhető az adatok ilyen fajta alakulása. Ugyanis a legtöbb esetben az embert támadják, mivel az a leggyengébb tényező egy ilyen pénzügyi védelemben. Sokkal egyszerűbb egy esetlegesen kevésbé képzett, az aktuális csalási viszonyokat nem ismerő, naiv ember hasába lyukat beszélni, mint egy nagyon komplex banki rendszerbe betörni vagy egyéb más módon próbálkozni.

Mit tehetünk befektetéseink, vagyonunk védelméért

Befektetéseink és vagyonunk védelme kulcsfontosságú a pénzügyi stabilitás és jólét szempontjából. Ebben az összefüggésben több lépést is megtehetünk annak érdekében, hogy hatékonyan védelmezzük pénzügyi eszközeinket. Első lépésként érdemes diverzifikálni a befektetéseinket, azaz ne koncentráljunk egyetlen eszközosztályra vagy piacra. A különböző típusú eszközök, például részvények, kötvények, ingatlanok és alternatív befektetések kombinálása csökkentheti a portfóliónk kockázatát. A pénzügyi tervünk részeként érdemes kialakítani egy vésztartalékot is, amely segíthet váratlan kiadások vagy nehézségek esetén. Ez lehetővé teszi, hogy ne kelljen azonnal eladnunk befektetéseinket kedvezőtlen piaci környezetben. Emellett fontos rendszeresen felülvizsgálni és frissíteni a pénzügyi tervünket, figyelembe véve az élethelyzetünk változásait és a piaci feltételeket.

Az aktív pénzkezelés és az információk folyamatos követése is növelheti a vagyonvédelem hatékonyságát. Tartsuk szem előtt a gazdasági és piaci trendeket, és tájékozottan hozzunk befektetési döntéseket. Az oktatás és a pénzügyi ismeretek bővítése segíthet abban, hogy jobban megértsük a pénzügyi rendszert, és képesek legyünk az esetleges kockázatokat és lehetőségeket felismerni. A biztosítások használata is kulcsfontosságú a vagyonvédelem szempontjából. Az életbiztosítások, egészségbiztosítások és vagyongazdálkodási biztosítások segíthetnek abban, hogy váratlan események, betegségek vagy balesetek esetén ne kerüljünk pénzügyi nehézségekbe. Fontos azonban alaposan megismerni és értelmezni a biztosítási feltételeket, valamint időről időre felülvizsgálni a biztosítási tervünket az életkörülményeink változásaival összhangban.

Végül, az öröklési tervezés is része lehet a vagyonvédelemnek. Szakértői tanács és egy jól kidolgozott öröklési terv segíthet abban, hogy a vagyontárgyaink és befektetéseink a kívánt módon kerüljenek át az örököseinkre, minimalizálva az esetleges adóterheket és jogi problémákat.

Ezen intézkedések kombinációja lehetőséget teremt számunkra a vagyonunk hatékonyabb védelmére és növeli a pénzügyi biztonságunkat a hosszú távon.

Azt gondolom mindenképpen a polgárok tájékoztatása és tanítása lenne a legfontosabb. Ehhez egy hajlandóság is szükséges az emberek oldaláról, akarniuk kell megismerni a legfontosabb biztonsági tényezőket. Meggyőződésem, hogy a visszaélések csalások nagy része elkerülhető

lenne, azzal, ha a kiszemelt áldozat, már esetleg egy telefonszámból vagy a beszélgetésből el tudná dönteni, hogy valószínűleg megpróbálják átverni vagy ez egy valós megkeresés. Ez talán függ az adott személy korosztályától is, hiszen aki úgy nő fel, hogy ez már egy valós veszélyforrás, annak talán jobbat szemet szúr egy esetleges átverési próbálkozás. Mégis mindenképpen azt gondolom az az első, amit mindenki megteheti, hogy állandóan tájékozódik és próbálja edukálni magát kiberbiztonsági, illetve összeségében pénzbiztonsági téren.

Ámde nem csak a csalások, átverések jelentenek veszélyt pénzünkre, hanem olyan tényezők is mint az infláció, ez különösen igaz az elmúlt évben Magyarországon. Ugyanis ennek a pénzromlásnak köszönhetően, ha a pénzünket nem fektetjük be legalább egy az inflációval azonos szintű kamattal rendelkező értékpapírba, a pénzük veszít értékéből.

Jövőkép: pénzbiztonság és bankbiztonság a jövőben

A digitalizáció várható hatása a bank és pénzbiztonságra

Úgy gondolom a jövőben még hatalmas változásokat fog hozni a digitalizáció a bank és pénzbiztonság terén. Főképpen az innovatív technológiák beintegrálása, a pénzügyi szolgáltatások átalakulása, valamint rengeteg új adat és kiberbiztonsági kihívás várható az elkövetkezendő időkben. Az egyre nagyobb online jelenlét, egyre több digitális megoldás és új technológiák, rendszerek majd várhatóan növelik a támadási felületet. Tehát a bankoknak is folyamatosan fejleszteniük kell a kiberbiztonságot és reagálniuk kell az állandóan változó fenyegetésekre. Az adatvédelem továbbá is kritikus szerepet fog kapni a pénzügyi szektorban. Feltehetően a mostaninál sokkal szigorúbb szabályozás és jogi követelmények lépnek majd életbe. Ezenfelül az adatvédelem nem csak egy kötelesség lesz a vállalatok részéről, hanem az üzleti sikerességhez is elengedhetetlenné válik. Összeségében a cégeknek majd egy megfelelő hangsúly felállítására kell törekednie az innováció, a technológiák és biztonság között, hogy hatékonyan tudjanak működni.

Blockchain technológia és a kriptovaluták

„*A 21. század egyik legfontosabb találmányaként tartjuk számon a blokkláncrendszereket és a kriptovalutákat. Ezeknek a rendszereknek számtalan felhasználási lehetősége van, képesek a tulajdonosi lánc és az eredetiség igazolására, forradalmasíthatják a kereskedelmet az úgy nevezett okos szerződések segítségével, sőt egyes vélemény szerint akár teljesen megváltoztathatják a jelenleg ismert bankrendszer szükségességét. Ugyanakkor fontos tudnunk, hogy a blokkláncok legalább annyi veszélyt hordoznak, mint amennyi problémára megoldást kínálnak. Ezen kockázatok közé tartozik a terrorizmus finanszírozásának és a pénzmosásnak a veszélye is.*”[7]

Okos szerződések és azok szerepe

Az okos szerződések olyan számítógépes protokollok, amelyek megkönnyítik és ellenőrzik a szerződés megtárgyalását vagy végrehajtását. Blockchain technológia és az okos szerződések szinte bármilyen pénzügyi tranzakció megkönnyítésére használhatók. Ezeknek az okos szerződéseknek köszönhetően az osztalék elszámolást és a kamatfizetést automatizálni lehetne. Az okos szerződések potenciális célpontokká válhatnak a támadók számára, mert nagy összegű pénzt is tartalmazhatnak. Bár széles körben a blokklánc technológiát használják, a biztonságuk még messze nem tökéletes, ami aggodalmakra adhat okot. Bár a támadások listázva vannak, hiányoznak a biztonság javítására vonatkozó törekvések és javaslatok.[8]

---

[7] Kenéz Dávid: A blokklánc technológia a pénzmosással szemben [online]. Fókuszban a vállalati szabálykövetés 2. évfolyam, 4. szám 2023, DOI: 10.14267/VILPOL2023.04.07. Hozzáférés: https://drive.google.com/file/d/1lsFzoxUQ7eDR7WvSTAXRlrhBLkGp9h7x/view [megtekintve 2023.12.09.].

[8] Malaw Ndiaye, Karim Konate: Security Strengths and Weaknesses of Blockchain Smart Contract System: A Survey [online]. World Academy of Science, Engineering and Technology International Journal of Information and Communication Engineering Vol:16, No:5, 2022. Hozzáférés: https://www.researchgate.net/profile/Malaw-Ndiaye/publication/360624196_Security_Strengths_and_Weaknesses_of_Blockchain_Smart_Contract_System_A_Survey/links/62824c3590841d5155d7dbb7/Security-Strengths-and-Weaknesses-of-Blockchain-Smart-Contract-System-A-Survey.pdf [megtekintve 2023.12.09.].

Új technológiák a virtuális védelemben

Biometrikus azonosítás és más új technológiák

Biometrikus adatok, amelyek az emberek automatikus felismerésére utalnak sajátosságuk alapján anatómiai (pl. arc, ujjlenyomat, írisz, retina, kéz geometriája) és viselkedési (pl. aláírás, járás) jellemzői, a hatékony személyazonosítás elengedhetetlen elemévé válhatnak, mert a biometrikus adat az egyén testi identitása. A biometria olyan technológia, amely képes biztonságosabbá tenni társadalmunkat, csökkenteni a csalásokat és a felhasználó kényelmét szolgálja.

A biometrikus adatok használata az internetes banki szolgáltatásokban egyre kényelmesebb és lényegesen pontosabb, mint a jelenlegi módszerek (például jelszavak vagy PIN-kódok használata). Ez azért van, mert a biometrikus adatok egy adott személyhez kapcsolják az eseményt (jelszót vagy tokent használhat valaki más, nem csak a jogosult felhasználó), kényelmes (nincs semmi hordozható vagy emlékezni való), pontos, ellenőrzési nyomvonalat tud biztosítani, és egyre inkább társadalmilag elfogadható és olcsó.

A biometrikus adatok használata az emberi lények azonosítására az internetes banki szolgáltatásokban egyedülálló lehetőségeket kínál, a következő előnyökkel jár:

• A biometrikus adatok segítségével Ön azonosítható Önként.

• Tokenek, például intelligens kártyák, mágnescsíkos kártyák, fényképes igazolványok, fizikai kulcsok és így tovább, elveszhetnek, ellophatják, lemásolhatják vagy otthon hagyhatják.

• A jelszavak elfelejthetők, megoszthatók vagy megfigyelhetők. Ráadásul a mai rohanó világban arra kérik az embereket, hogy emlékezzenek sok jelszóra és személyes azonosító számokra (PIN-ek) internetes számlákhoz, banki ATM-ekhez, e-mail fiókokhoz, közösségi médiához, webhelyekhez és így tovább.

• A biometria gyors, könnyen használható, pontos, megbízható és olcsóbb megoldást ígér a többi hitelesítési lehetőségnél.

• Egy másik kulcsfontosságú szempont, hogy mennyire "felhasználóbarát" egy rendszer. A folyamatnak gyorsnak és egyszerű, például videokamerával fényképezve, mikrofonba beszélve, vagy ujjlenyomat-szkenner megérintésével, egyszerűen kell működnie.

• Ahogy a biometrikus technológiák kiforrnak és széles körű kereskedelmi felhasználásra kerülnek, a hitelesítés kevesebb terhet jelent majd a felhasználók számára.[9]

Mesterséges intelligencia alapú védelmi megoldások és annak előnyei

„A pénzügyi intézmények számára a mesterséges intelligencia lehetővé teszi, hogy felgyorsítsák és automatizálják a történelmileg manuális és időigényes feladatokat, például a piackutatást. A mesterséges intelligencia gyorsan képes nagy mennyiségű adatot elemezni a trendek azonosítása és a jövőbeli teljesítmény előrejelzésének segítése érdekében, többek között lehetővé téve a bankok számára a hitelezési potenciál növekedésének feltérképezését és a kockázatok értékelését. Az értékelés a biztosítások esetében is alkalmazható, ahol a személyes adatok összegyűjthetők és felhasználhatók a biztosítási fedezet és a díjak meghatározásához. A mesterséges intelligencia kiberbiztonsági célokra is használható, különösen a csalárd tranzakciók azonosítására. A vásárlási viselkedés szoros figyelemmel kísérésével és a korábbi adatokkal való összehasonlításával az AI képes jelezni a rendellenes tevékenységet, automatikusan figyelmeztetni az intézményt és az ügyfelet is, hogy valós időben ellenőrizze a vásárlást vagy átutalást, és ha szükséges, lépéseket tegyen annak megoldására. A banki ügyfelek számára az AI és az ML (Machine Learning – gépi tanulás) javíthatja az általános ügyfélélményt. Az online bankolás (azaz az érintésmentes bankolás) térhódítása minimalizálja a személyes interakciók szükségességét, de a virtuálisra való áttérés több végponton (pl. okostelefonok, asztali számítógépek és mobileszközök) jelenthet sérülékenységet. A mesterséges intelligencia számos alapvető banki tevékenységet, például a fizetéseket, befizetéseket, átutalásokat és ügyfélszolgálati kéréseket automatizálhatja. A mesterséges intelligencia képes kezelni a hitelkártyák és hitelek kérelmezési folyamatait, beleértve az elfogadást és az elutasítást is, szinte azonnali válaszokat adva.”[10]

---

[9] *Gunajit Sarma, Pranav Kumar Singh: Internet Banking: Risk Analysis and Applicability of Biometric Technology for Authentication [online]. Hozzáférés: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=3b100fe0af708daf4457c17de0ffcfcad4d07cc4 [megtekintve 2023.12.09.].*

[10] *Bagó Péter: A MESTERSÉGES INTELLIGENCIA LEHETŐSÉGEI A PÉNZÜGYEKBEN [online]. Hozzáférés: https://bankszovetseg.hu/Public/gep/2023/021-038%20Bago%20P.pdf [megtekintve 2023.12.09.].*

Jövőbeli kihívások és lehetőségek

Személyes adatok lopása és a személyazonosságlopás elleni küzdelem

A jövőben valószínűsíthető, hogy még kiemeltebben kell foglalkozni a bank és pénzügyi szektornak a személyes adatok védelmével. Ugyanis a digitális átmenettel és az adatok szélesebb körű felhasználásával együtt jár a növekvő fenyegetés a személyes adatokkal kapcsolatos kiberbűnözés terén. Nagy figyelmet kell majd fordítani a vállalatoknak arra, hogy megfeleljenek a várhatóan egyre szigorúbb és több mindenre kiterjedő jogszabályoknak, követelményeknek, amit akár az ügyfelek várnak el tőlük. Ahogy már fentebb olvasható volt, ebben a harcban nagy segítség lehet a mesterséges intelligencia, gépi tanulás és a biometrikus azonosítás is. Az utóbbi előretörése már tapasztalható a mai világba is, de valószínű, hogy ezt is sokkal pontosabbá és biztonságosabbá kell majd tenni, hogy a csalók, hackerek ne találjanak fogást rajta.

A kibertámadások és azok elleni védekezés

A jövőbeli banki kibertámadások elleni védekezés kiemelkedően fontos terület a pénzügyi szektor számára, ahogy a technológiai fejlődés és a digitalizáció továbbra is előre halad. A kiberbűnözők folyamatosan fejlesztik és alkalmazzák az új technikákat és eszközöket, hogy kijátszák a pénzintézetek védelmi rendszereit. A pénzügyi szervezeteknek proaktívan kell válaszolniuk e kihívásokra, és olyan kiberbiztonsági stratégiákat kell kialakítaniuk, amelyek hatékonyan azonosítják, megelőzik és ellensúlyozzák az esetleges támadásokat.Az adaptív és intelligens kiberbiztonsági megoldások bevezetése elengedhetetlen a folyamatosan változó fenyegetések elleni védekezéshez. A mesterséges intelligencia és gépi tanulás alkalmazása lehetővé teszi a rendszereknek, hogy tanuljanak a korábbi támadásokból, és gyorsan reagáljanak az új, ismeretlen fenyegetésekre. Az események valós idejű monitorozása és a szükséges intézkedések gyors végrehajtása kulcsfontosságú a kibertámadásokkal szembeni hatékony védekezésben.

A szektoron belüli együttműködés is nélkülözhetetlen. A bankoknak és pénzügyi szervezeteknek információkat kell megosztaniuk az esetleges fenyegetésekről, és közösen kell dolgozniuk az új kiberbiztonsági eszközök és módszerek kifejlesztésében. A jogszabályi keretek és szabványok szigorú betartása, valamint az ügyfelek kiberbiztonságra való tudatosságának növelése további fontos lépések a jövőbeli banki kibertámadások elleni hatékony védelem érdekében.

Összefoglalás

A bank- és pénzbiztonság témakörében végzett részletes elemzés alapján megállapítható, hogy az elmúlt évtizedekben a pénzügyi szektor jelentős változásokon ment keresztül a digitalizáció és a technológiai fejlődés hatására. A fizikai és virtuális biztonság összehasonlításakor kiderült, hogy mindkét területen kiemelt figyelmet kell fordítani a kockázatokra és a megfelelő védelmi intézkedésekre. A fizikai biztonság terén a bankfiókok, ATM-ek és tranzakciós helyszínek megfelelő védelmi protokolljai, az eszközök és az infrastruktúra biztonsága kulcsfontosságú az ügyfelek és a pénzintézetek számára egyaránt.

A digitalizáció hatásai rávilágítottak a pénzintézetek kibővített kiberbiztonsági kihívásaira. Az online és mobilbanki szolgáltatások térhódításával együtt nőtt az adatbiztonság és az ügyfélazonosítás jelentősége. A digitális tranzakciók és az online bankolás elterjedése új típusú kiberfenyegetéseket hozott létre, amelyekre a pénzintézeteknek innovatív és hatékony védekezési stratégiákat kell kidolgozniuk.

A fizikai és virtuális biztonság összehasonlítása után a hamisításának kérdéskörébe mélyültem el. Kiemeltem a hamisítás különböző formáit, beleértve a bankjegyek és dokumentumok hamisítását. Az új biztonsági intézkedések és az intelligens technológiák alkalmazása elengedhetetlen a pénzintézetek számára a hamisítás kockázatának minimalizálása érdekében.

Az adatvédelem és az online identitás védelmének kérdéseire kiterjesztve a szöveget, bemutattuk a személyes adatok védelmének fontosságát a digitális környezetben. A titkosítási és védelmi mechanizmusok részletes elemzése segített abban, hogy megértsük, hogyan működnek a modern technológiák az ügyfelek személyes adatainak védelmében, és miként járulnak hozzá a bankok online tranzakcióinak biztonságához.

Az okosszerződések és a blokklánc technológia vizsgálata azt mutatta, hogy ezek a technológiák forradalmasíthatják a pénzügyi szektor biztonságát. Az okosszerződések automatizált végrehajtása és a blokklánc állandósága új szintre emelheti a tranzakciók biztonságát és nyomon követését. Ugyanakkor azonban kiemeltem az esetleges kihívásokat, beleértve a kódhibákat és a jogi kérdéseket, amelyekkel a pénzintézeteknek számolniuk kell az új technológiák integrációjakor.

A végén hangsúlyoztam a pénzintézetek jövőbeli kihívásait és lehetőségeit a bank- és pénzbiztonság terén. A digitalizáció, a biometrikus azonosítás és más fejlett technológiák tovább formálják a pénzügyi szektort. A pénzintézeteknek alkalmazkodniuk kell a változó környezethez, hatékonyan kezelniük kell a kiberbiztonsági kihívásokat, miközben biztosítják az ügyfelek és az adatok biztonságát. Reményeim szerint átfogó képet nyújtottam arról, hogyan alakul a bank- és pénzbiztonság, és milyen stratégiákra van szükség a jövő kihívásaival való sikeres megbirkózáshoz.

Felhasznált Irodalom

Bagó Péter: A MESTERSÉGES INTELLIGENCIA LEHETŐSÉGEI A PÉNZÜGYEKBEN [online]. -in: Gazdaság és Pénzügy, 2023. - 10. évf. 1. sz., p. 21-38. – Hozzáférés: https://bankszovetseg.hu/Public/gep/2023/021-038%20Bago%20P.pdf [megtekintve 2023.12.09.].

Gunajit Sarma, Pranav Kumar Singh: Internet Banking: Risk Analysis and Applicability of Biometric Technology for Authentication [online]. -in: International Journal of Pure and Applied Sciences and Technology, 2010. – p. 67-78 Hozzáférés: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=3b100fe0af708daf4457c17de0ffcfcad4d07cc4 [megtekintve 2023.12.09.].

Kenéz Dávid: A blokklánc technológia a pénzmosással szemben [online]. -in: Fókuszban a vállalati szabálykövetés. 2023 2. évfolyam, 4. szám, Hozzáférés: https://drive.google.com/file/d/1lsFzoxUQ7eDR7WvSTAXRlrhBLkGp9h7x/view [megtekintve 2023.12.09.].

Magyar Nemzeti Bank: FORINTBANKJEGYEK BIZTONSÁGI ELEMEI [online]. Hozzáférés: https://www.mnb.hu/static/kpl/u5000/u5000.htm [megtekintve 2023.12.09.].

Magyar Nemzeti Bank: Intézményi biztonság [online]. Hozzáférés: https://www.mnb.hu/fogyasztovedelem/bankszamlak/elektronikus-banki-szolgaltatasok/intezmenyi-biztonsag [megtekintve 2023.12.09.].

Malaw Ndiaye, Karim Konate: Security Strengths and Weaknesses of Blockchain Smart Contract System: A Survey [online]. -in: World Academy of Science, Engineering and Technology International Journal of Information and Communication Engineering, 2022. Vol:16, No:5, Hozzáférés: https://www.researchgate.net/profile/Malaw-Ndiaye/publication/360624196_Security_Strengths_and_Weaknesses_of_Blockchain_Smart_Contract_System_A_Survey/links/62824c3590841d5155d7dbb7/Security-Strengths-and-Weaknesses-of-Blockchain-Smart-Contract-System-A-Survey.pdf [megtekintve 2023.12.09.].

ORIGO: Ennyi idő alatt törhetőek fel a jelszavak [online]. 2022.03.21. Hozzáférés: https://www.origo.hu/techbazis/20220321-eros-jelszo-feltoresi-ido.html [megtekintve 2023.12.09.].

OTP bank, Kibervédelmi Osztály: Többfaktoros azonosítás

Szatmári Ferenc: Az elektronikus banki csatornák biztonsági kérdései és a fejlődési irányok [online]. -in:BUDAPESTI GAZDASÁGI FŐISKOLA – MAGYAR TUDOMÁNY NAPJA, 2003. Hozzáférés: https://publikaciotar.uni-bge.hu/446/1/tek_2003_20.pdf [megtekintve 2023.12.09.].

Zsigrai bankbiztonsági és vagyonvédelmi KFT.: Bankbiztonság [online]. Hozzáférés: https://www.zsigraikft.hu/bankbiztonsag [megtekintve 2023.12.09.].

Ábrajegyzék

PANNON EGYETEM
GAZDÁLKODÁSI KAR ZALAEGERSZEG

SZERZŐI ÖSSZEFOGLALÁS

A dolgozat címe: Pénzbiztonság és bankbiztonság a fizikai és virtuális térben	
Hallgató neve: Mentes Dominik Attila	NEPTUN kód: HS52E6
Képzési szint: alapképzés	
Szak: Pénzügy és számvitel	Szakirány: Vállalkozások pénzügyei
Témavezető neve: Fejes Judit Katalin	Beosztása: mesteroktató
Tanszék: Pénzügy és Gazdálkodás tanszék	

Az elmúlt pár évben a világunk állandó, gyors változásnak és ezzel együtt fejlődésnek volt kitéve. Ez az életünk minden területére kihat, így természetesen a gazdaságra és még inkább a technológiára is. Az egyre felgyorsuló információcserének egyik nagy hozadéka az elektronikus pénzügyi ügyintézés. Az emberek egyre többször választják ezeket digitális megoldásokat a hagyományos lehetőségekkel szemben, főként gyorsasági és kényelmi szempontok miatt. Ezekhez a pénzintézetek és a bankok is partnerek, ugyanis egyre jobban ők is a digitalizálásra helyezik át a hangsúlyt, hiszen ez nekik is számos előnyt jelenthet. Ámde a pénzügyek digitalizálásának elterjedésével együtt számos új megoldandó probléma és kihívás elé állnak mind a bankok, mind az ügyfelek, különösen a biztonság terén. A pénzügyek biztonsága napjainkban az egyik legkritikusabb pontja a vállalatoknak és a magánembereknek is. A számos új technológiai fejlesztések, mint például az elektronikus fizetési rendszerek, a kriptovaluták vagy az online bankolás remek új pénzügyi lehetőségeket biztosítanak, de ahogy ez lenni szokott új lehetőségekhez általában új veszélyek, kockázatok is párosulnak és így van ez ebben ez esetben is. Főképp a pénzügyi és személyes adatok, illetve a tranzakciók digitális továbbítása, megőrzése és tárolása ad sok lehetőséget a kiberbűnözők, illetve csalók számára, akik számtalan módszerrel próbálnak hozzáférni ezekhez az adatokhoz, hogy utána vissza tudjanak élni azokkal. Ebben a szakdolgozatban a pénzintézetek, bankok és a pénz biztonságára szeretnék összpontosítani, cél a jelen korunk kihívásainak és veszélyeinek megállapítása, továbbá annak vizsgálata, hogy miként lehet minél biztonságosabbá tenni a pénzügyi környezetet mindenki számára. A dolgozatbank részletezni szándékozom a pénzügyi adatvédelmet, a kiberbiztonságot és bemutatom a legújabb technológiai megoldásokat, amelyek segítenek megőrizni a pénzügyi stabilitást és biztonságot a gazdaság digitalizációja után is. Továbbá kitérek majd a hagyományos, fizikai térben lévő gyakori veszélyekre és azok esetleges megoldásaira is.