CYBER SECURITY IN 2021 IN THE BANKING SECTOR AND FINANCIAL ORGANIZATIONS

KIBERBIZTONSÁG 2021-BEN A BANKSZEKTORBAN ÉS A PÉNZÜGYI SZERVEZETEKNÉL

GULYÁS Olivér[1], KISS Gábor [2]

Abstract

Every year marks another "worst year ever" for cyber-attacks. In 2021 cybersecurity was again in spotlight. The number of data breaches until September 30, 2021, has already exceeded the total number of events in 2020 by 17 percent [1]. The banking sector was disproportionately affected by the scale of the attacks. In the first half of 2021 blackmail virus attacks increased by 1318 percent on a y-o-y basis [2]. Therefore, in addition to taking advantage of the rapid development of information technology, the potential threat of the attack surface of the banking sector is increased and exposed to more sophisticated cyber threats. With the development of digital technology hackers are also improving their skills, building maximum protection against their malicious attacks is an increasing challenge for professionals. Day by day, more and more businesses are using the digital solutions offered by banks, which is why effective cybersecurity programs have become more important than any other-ever.

Keywords

hacker, banking sector, digital attacks, cyber threats

Absztrakt

A kiberbiztonsággal kapcsolatban minden évben azt gondoljuk, hogy ezt volt az eddigi legrosszabb év. 2021-ben a kiberbiztonság ismét nemvárt rivaldafénybe került. Az adathalász támadások 2021 szeptember 30-ig már 17 százalékkal meghaladták 2020 összes támadásának számát [1]. A bankszektort aránytalanul nagymértékben érintették a kibertámadások, 2021 első félévében 1318%-kal nőtt a zsarolóvírus-támadások száma év-per-év alapon [2]. Éppen ezért, a rohamos információ technológiai fejlődés mellett, a bankszektort érintő veszély potenciális támadási felülete is megnövekedett és napról napra kifinomultabb kiberfenyegetésnek vannak kitéve. A digitális technológia fejlődésével a hackerek is fejlesztik tudásukat, és a rosszindulatú támadásaik ellen maximális védelmet kiépíteni egyre nagyobb kihívást jelent a szakemberek számára. Napról napra egyre több vállalkozás használja a bankok által kínált digitális megoldásokat, éppen ezért a hatékony kiberbiztonsági programok minden eddiginél fontosabbá váltak.

Kulcsszavak

hacker, bankszektor, digitális támadások, kiberfenyegetések

[1] gulyaso@gmail.com | ORCID: 0000-0001-6945-2222 | doctoral candidate, Óbudai University | doktorandusz, Óbudai Egyetem

[2] kiss.gabor@bgk.uni-obuda.hu | ORCID: 0000-0002-0447-937 | associated professor, Óbudai University | egyetemi docens, Óbudai Egyetem

BEVEZETÉS

Mára már szinte minden bank bevezette a különböző mobil alkalmazásokat, amelyek új sebezhetőségi pontot kínálnak a kiberbűnözők számára, akik az ügyfelek banki adatait veszek leggyakrabban célba, hiszen a pénzügyi adatok óriási értékkel bírnak.

A banki alkalmazások két oldalról támadhatóak, egyrészt a kliens oldali alkalmazások révén, másrészt pedig szerver oldalról. Ezért a bankoknak biztosítaniuk kell az érzékeny adatok biztonságát az ügyfél eszközéről való hozzáféréskor, valamint a banki szervereken történő tároláskor. A pénzintézetek (is) sokszor külsős vállalkozást bíznak meg a szoftvereik programozásához és azok karbantartásához. A tapasztalatok alapján ők kevésbé tartják magukra nézve kötelezőnek a vállalati biztonsági szabályok betartását – így a hackerek rajtuk keresztül is indíthatnak támadást [3].

A pénzügyi szervezeteknek teljes mértékben át kell látniuk az információ technológiai ökoszisztéma sérülékenységét, és a támadások végrehajtásához használt különböző támadási vektorokat, ahhoz, hogy átfogó kiberbiztonsági programot tudjanak kidolgozni. Fontos, hogy a biztonsági rendszert kiépítők ne csak lépést tartsanak a folyamatosan fejlődő kiberbűnözőkkel, hanem egy lépéssel előttük járjanak.

A cikk célja bemutatni milyen kiberkockázatok merülnek fel a pénzintézeteknél, hogyan lehetne növelni a pénzintézetek hálózatainak biztonságát, ez által megakadályozva a veszteségeket. Ennek érdekében, adaptálhatóak-e a legújabb információ technológiai fejlesztések, azon belül a blokklánc technológia.

TÁMADÁSI VEKTOROK, TÁMADÁSI FELÜLETEK ÉS BIZTONSÁGI RÉSEK

A kiberkockázat kezelési program hatékony felépítéséhez meg kell ismernünk a támadási vektorok, a támadási felületek és a biztonsági rések közötti különbséget.

A támadási vektorok azok az eszközök vagy taktikák, amelyek segítségével a hackerek jogosulatlanul hozzáférhetnek egy hálózathoz.

A szervezet támadási felülete az összes olyan érintkezési pont, amelyeken keresztül a támadók hozzáférhetnek a hálózathoz, manipulálhatják azt, vagy érzékeny adatokat nyerhetnek ki. A támadási felületek lehetnek fizikaiak vagy digitálisak. A fizikai: hardver vagy fizikai eszközök, például számítógépek, táblagépek, útválasztók és szerverek; A digitális támadási felültek magukban foglalják például a szoftvereket, webes és asztali alkalmazásokat, hálózatokat és portokat.

A biztonsági rések digitális vagy fizikai hacker támadásnak adhatnak teret ezért különös figyelemmel szükséges kezelni őket. A legfontosabb azonban az emberi tényező, a csalódott vagy képzetlen, tájékozatlan alkalmazottak. Az emberek kezelik az információt, mint erőforrást, de rajtuk keresztül történhet az adatszivárgás is, melynek következtében illetéktelen felek hozzáférnek, ellopják vagy közzéteszik egy szervezet bizalmas vagy védett információit [3]. Ennek megelőzése érdekében fontos a jogosultsági szintek meghatározása: minden dolgozó csak azokhoz az adatokhoz és munkafolyamatokhoz férjen hozzá, amelyek a feladatköre ellátásához szükségesek. A dolgozókkal meg kell ismertetni a szervezet adatvédelmi és informatikai biztonság politikáját, fel kell hívni a figyelmüket a lehetséges veszélyekre.

TÁMADÁSOK OKAI

A kibertámadásoknak számos különböző oka van, de a leggyakoribb indíték a pénzbeli haszonszerzés. A második leggyakoribb támadás a személyazonosításra alkalmas adatokhoz való hozzáférés megszerzése, mivel ez által üzleti titkokhoz, szabadalmaztatott információkhoz juthatnak hozzá a hackerek. Szintén gyakori ok egy vállalat hírnevének szándékos csorbítása, vagy negatív üzleti pozícióba hozása, ez által ellehetetlenítése. Az információ típusa függvényében a támadók a megszerzett információ megosztásával, szenzitív adatok (cég vagy az adott személyre vonatkozó) világhálóra kerülésével is zsarolhatnak.

A kiberbűnözők két átfogó módon hajthatnak végre támadást. Az egyik a digitális támadás, a másik a fizikai támadás, amely során személyesen próbálnak bejutni egy irodaházba és ily módon adatokhoz jutni [4].

DIGITÁLIS TÁMADÁSOK TÍPUSAI

A leggyakoribb esetek a *ransomware*, azaz a zsarolóprogramok általi támadások, amelyek meggátolhatják a felhasználó hozzáférését az adataikhoz, zárolják a számítógépet, tulajdonképpen túszként tartják fogva a személyes fájljait. A támadók átveszik a számítógép feletti irányítást, és váltságdíjat követelnek a visszaállított hozzáférésért cserébe. A *ransomware* támadások elleni védekezés legfontosabb módja annak biztosítása, hogy minden eszköz és szoftvere folyamatosan naprakész és frissített legyen, folyamatosan készüljön biztonsági mentés, ne nyissanak meg a felhasználók automatikusan e-mail mellékleteket, valamint érdemes felhőszolgáltatásokat használni. A pénzintézetek fokozott veszélynek vannak kitéve e tekintetben, mivel a *ransomware* támadásokkal főleg olyan szervezeteket támadnak, akik érzékeny adatokat őriznek, és gyorsan tudnak váltságdíjat fizetni [5].

A *rootkit* eredetileg olyan eszközök gyűjtő elnevezése volt, amelyek lehetővé tették a rendszergazda szintű hozzáférést a számítógéphez vagy a hálózathoz. Manapság a *rootkit*-eket rosszindulatú szoftverekkel azonosítják, amelyek elrejtik a létezésüket az operációs rendszer és ezáltal a felhasználók elől. A támadó a *rootkit* telepítése után távolról képes lesz a gazdagépen a rendszerkonfigurációkat felülírni, valamint a fájlokon változásokat végrehajtani. Elsődleges céljuk az adathalászat [6].

Az adathalász támadások a támadási vektorok leggyakoribb típusai közé tartoznak, és ez lehet az egyik legnehezebben kezelhető támadási fajta, mivel az elsődleges célpont a képzetlen dolgozó, aki általában nem jártas az információ-technológiában. Az adathalász e-mailek legfőbb jellemzője, hogy pontosan úgy néznek ki, mintha ismert vagy megbízható cégtől érkeztek volna (például: banktól, vagy egy online áruháztól). Ezek az e-mailek azzal próbálnak a címzett bizalmába férkőzni, hogy valamilyen történetet mesélnek el, majd egy melléklet megnyitására, vagy egy linkre kattintásra biztatják a felhasználót. Előfordul, hogy azt állítják, a felhasználó adataival visszaélést vagy harmadik fél által bejelentkezési kísérletet észleletek, esetleg meg kell erősíteni személyes adatokat. Gyakori a nyereményhez jutás ígérete is [7].

Szolgáltatásmegtagadási támadások (*Distributed Denial of Service*, DDoS), az elosztott szolgáltatásmegtagadási támadások a webhely az informatikai rendszer kapacitásának határait feszegetik. Céljuk, hogy azok forgalmát megszakítsák a webhely túlterhelésével és működésképtelenné tételével. Ezeket a támadásokat jellemzően botnetek segítségével hajtják végre, amelyek arra szolgálnak, hogy a kérésekkel túlcsordulást hozzanak létre a webhelyen, melynek következtében a webhely leáll [8].

A gyenge vagy feltört felhasználónevek és jelszavak a biztonsági incidensek egyik fő okai, ezért a felhasználók számára egyértelmű útmutatásokra van szükség, mivel ők a vállalat leggyengébb láncszemei. 2018-ban fél milliárd személyes adatot sikerült hackereknek eltulajdonítania, ami az előző évhez képest 126 százalékkal több esetet jelentett [9]. Az elmúlt évtized öt legnagyobb adathalász eseménye (Yahoo, Alibaba, LinkedIn, Sina Weibo, Facebook) összesen közel 6 milliárd felhasználót érintett [10]. A probléma forrása az, hogy a felhasználóknak saját jelszavakat kell létrehozniuk, ezért nagy a valószínűsége, hogy nem fognak elég biztonságos jelszót kitalálni. Ennek oka az lehet, hogy a felhasználók könnyen megjegyezhető jelszót szeretnének, nem ismerik a bevált jelszóbiztonsági gyakorlatokat, vagy olyan mintákat használnak jelszavaik létrehozásához, mint például a nevüket és/vagy a születési dátumukat [9]. Látható, hogy az alapképzés sem készíti fel a hallgatókat a megfelelő jelszóhasználati szokások kialakítására, ezért mindenképp erre is hangsúlyt kell fektetni – már az oktatás során [11]. Az információbiztonsági oktatásnál is új didaktikai elemre van szükség a jelszóhasználati szokások megváltoztatására, például jelszófejtő programok használata által, ahol a résztvevők megtapasztalhatják a gyenge jelszavak feltörésén keresztül, mennyire rövid idő szükséges azok megfejtéséhez [12] [13].

A bennfentes fenyegetések többféle formában és mértékben fordulhatnak elő. Kiváltó oka lehet pusztán hanyagság, de eredhet bosszúból és rosszindulatból egyaránt. A gondatlanságra jó példa, amikor szenzitív adatokat küldenek véletlenül az arra jogosulatlan felhasználónak, míg rosszindulatú szándék amikor valaki szándékosan, károkozás céljából ad át információkat, vagy kifejezetten anyagi haszonszerzés céljából pénzért. Felmérések szerint a károk 62%-a származik a munkavállalók vagy beszállítók gondatlansága miatt. E támadások mérséklésének egyik módja az, hogy a pontos hozzáférési szinteket biztosítja a felhasználóknak, amelyre a feladatuk ellátásához szükségük van, semmivel sem többet [14].

Harmadik fél szállítók megbízott vállalkozások sok szervezet számára rugalmasságot és nagyobb termelékenységet tesznek lehetővé. De a külső beszállítók kiberbiztonsági helyzetét éppoly komolyan kell venni, mint a sajátot. Harmadik féltől származó adatvédelmi incidensek száma rohamosan növekszik, és mivel egy kutatás szerint a szervezetek több mint 36 százaléka azt állítja, hogy legalább egy harmadik fél által okozott adatvédelmi incidenst átélt, egyértelmű, hogy miért van szükség átfogó, harmadik fél kockázatkezelési programjára [15].

Megfelelő titkosítás nélkül a szervezetek támadások áldozataivá válhatnak, mivel az adatok különböző hálózatokon keresztül kerülnek továbbításra. Amikor a felhasználók kockázatnak kitett hálózatokhoz vagy alkalmazásokhoz csatlakoznak, megnő annak a valószínűsége, hogy az érzékeny információk nyilvánosságra kerülnek egy adatvédelmi incidens során. Proaktív és megelőző intézkedéseket kell hozni annak biztosítására, hogy minden adat biztonságban legyen a felhasználók és az alkalmazások közötti mozgás során. Az adatokat nem csak továbbítás közben, hanem nyugalmi állapotban (tárolás) és az adattal való munka (feldolgozás) közben is titkosítani kell.

A hibás konfiguráció könnyű lehetőségeket teremthet a hackerek számára a sebezhetőségek kihasználására. Az ez ellen való védekezés kulcsa, hogy folyamatosan figyelemmel kell kísérni a szervezet „kiber-higiéniáját", így biztosíthatja, hogy az alkalmazások és eszközök beállításai naprakészek legyenek az iparági szabványoknak és a legjobb gyakorlatoknak megfelelően [16].

FIZIKAI TÁMADÁSOK TÍPUSAI

A fizikai támadások alkalmával a támadó személyesen jelenik meg és avatkozik be az adatok megszerzésének érdekében. Ennél fogva igen komoly előzetes felkészülést, színjátszó képességet és nem utolsó sorban hidegvért igényel a támadó részéről.

Az első lépés ilyenkor, hogy a támadó tervet dolgoz ki az adott objektumba való észrevétlen bejutáshoz. A besurranáshoz felhasználhatja más dolgozó adatait, vagy megpróbálja elhitetni a biztonsági őrrel, hogy otthon hagyta a beléptető kártyáját, vagy keresi a táskája alján, miközben nagy csomagokkal egyensúlyoz. Az ilyen esetekben a segítség nyújtás iránti hajlandóságát igyekszik kihasználni. A bejutás másik bevett módszere, hogy karbantartó munkásként jelenik meg, vagy ilyen csoporthoz csatlakozva surran be munkásruhában. Ezek a módszerek *piggybacking* és *tailgating* néven váltak ismertté [17].

Előfordul olyan eset is, amikor a támadó öltönyben vendégként érkezik egy vállalathoz, és a dolgozók válla fölött átkukucskálva próbál megfigyelni felhasználó neveket és jelszavakat, ezt hívják *shoulder surfing*-nek [18].

Sok támadó kukabúvárként tevékenykedik, vagyis konkrétan a hulladékot nézi át. A szemét sok olyan kidobott levelet is tartalmazhat, amelyekből személyes információkhoz juthat a támadó. Ezért fontos az irodákban iratmegsemmisítőt használni, de mindemellett a dolgozókat is figyelmeztetni kell, az iratkezelési szabályzatok betartására, valamint otthonaikban se dobjanak ki olyan iratokat, számlákat, amelyekből profilt alkothat róluk egy kiberbűnöző [19].

COVID-19-CEL KAPCSOLATOS VÁLTOZÁSOK

A kibertámadások száma és intenzitása minden iparágban folyamatosan növekedett az elmúlt években. Bár egyes kutatók hangsúlyozzák, hogy 2020 óta a támadások növekedése még mindig csak az általános növekvő tendencia része, hajlamosak vagyunk elfogadni, hogy a globális világjárvány miatt a minta megváltozott. Tapasztalatunk és egyre több kutatás is azt bizonyítja, hogy a lezárások miatt a cégeknek át kellett térniük a távmunkára, ezáltal új támadási felületek nyíltak meg. A támadások száma és intenzitása az otthoni vagy távoli elérésű informatikai és internetes infrastruktúra gyengesége miatt tovább emelkedett. A Verizon jelentése szerint például az adathalász támadások gyakorisága 2021-ben 25 százalékról 36 százalékra nőtt, elsősorban a globális kijárási korlátozások miatt növekvő otthoni megrendelések miatt [20].

BLOCKCHAIN NYÚJTOTTA LEHETŐSÉGEK

A pénzügyi ágazat számára a legnagyobb kihívást a jelentős mértékű papírmunka, a veszélyes adatszivárgás és a redundáns folyamatok jelentik, ezek azok a kihívások, amelyek tovább növelik az amúgy is hatalmas működési költségeket és a növelik a fogyasztók bizalmának hiányát. A blokklánc alkalmazása a pénzügyi szolgáltatásokban sokat segíthetne ezeknek a problémáknak a kiküszöbölésében. A blokklánc eddig nem látott biztonságot és átláthatóságot hozhatna a pénzügyi szektorba. A technológia decentralizált, és egy-egy tranzakció hitelesítését több csomóponton végzik, ezért nem módosítható. Mivel minden csomóponton ugyanazok, az adatok fognak szerepelni, ez biztosítja, hogy az adatok visszakövethetőek, biztonságosak és hitelesek maradhatnak. Ugyanakkor adatvédelemi szempontból is megfelelő lehet, mivel a rendszer használatához egy nyilvános és egy privát

kulcsra van szükség a hálózathoz való hozzáférés biztonságának és az egyéni tranzakcióinak titkosságának megőrzése érdekében. Így a pénzintézetek az adatokhoz való hozzáférés nélkül is elvégezhetik a felhasználó-ellenőrzést az adat ellenőrzése el tud válni az adattól magától csökkentve ezzel a jogsértések esélyét [21].

Blokklánc segítségével hatékonyabban lehetne ellenőrizni a pénzügyi tranzakciókat. Mivel a blokkláncon lévő rekordok megváltoztathatatlanok, az auditorok ellenőrizhetik, hogy megfelelnek-e a valóságnak. Egy átlagos pénzügyi elszámolás több oda-vissza váltást foglal magában a bank *front-* és *back office*-a között. Az intelligens szerződések használatával elkerülhetőek ezek a lépések, megkönnyítik a P2P (*peer to peer*) tranzakciókat, és kihagyhatnak több lépcsőfokot a pénzügyi elszámolás felgyorsítása érdekében. A blokklánc közvetítők nélkül képes azonnali, határokon átnyúló fizetéseket is kezelni [21].

A Blockchain technológia használata segíthet a fenti kiberkockázatok egy részének csökkentésében. A legtöbb pénzintézet már vizsgálja a technológiában rejlő lehetőségeket. A technológia alapját adó funkciók, mint az elosztott főkönyvi technológia, nagyon jó kiindulási pont a kibertámadások elleni védekezésben. A különböző pénzügyi intézmények a blokklánc technológiát használják vagy tesztelik tőzsdei kereskedéshez, kereskedelem finanszírozáshoz, hűségprogramokhoz, ahogy korábban írtuk kísérleteznek a technológia felhasználásával a P2P kifizetések és a nemzetközi fizetések elszámolásában [22] [21] [23].

ÖSSZEFOGLALÁS

A cikkben bemutattuk a kritikus támadási pontokat és megnéztük a támadások okait. Összességében elmondhatjuk, hogy a gazdaság különböző szektorait, azon belül a pénzügyi szektort kiemelten, évről évre növekvő mértékben érintik a kibertámadások különböző módszerei. A digitális támadások mellett továbbra sem hanyagolhatjuk el a fizikai támadások jelentőségét. Azt is megállapítottuk, hogy az adatszivárgás kiemelkedő oka továbbra is az emberi tényező: a belső kolléga vagy külső beszállító gondatlansága, nem megfelelő jelszókezelése vagy szélsőséges esetben kifejezetten a rosszindulatú szándéka.

A cikkben vizsgált kibertámadások fő tanulságai összefoglalva:

1. Egyetlen szervezet vagy hálózat sem biztonságos: mérettől vagy az iparágtól függetlenül a cégek nincsenek biztonságban a kibertámadásoktól.
2. Üzletmenet folytonossági programokra, védelmi és biztonsági protokollokra vagy az ügyfélkommunikációra nagyon nagy hangsúlyt kell fektetni: a szervezeteknek elő kell készíteniük a megfelelő szabályzatokat. A szabályzatoknak harmadik feles szolgáltatókra és más szállítókra is vonatkozniuk kell.
3. Fizetni vagy nem fizetni: a szakemberek általában nem javasolják a váltságdíjak kifizetését. Precedenst teremt, felhívja a többi kiberbűnöző figyelmét, hogy az adott szervezet hajlandó fizetni
4. A támadások időzítettek és célzottak: az értékes felhasználói adatok, az áldozat fizetési potenciálja kulcsfontosságú tényezők. Sokszor egy támadást hónapokkal megelőzően már el lettek rejtve a jövőben támadáshoz a bejutást biztosító „trójai falovak”.
5. A kibertámadások akkor a legkártékonyabbak, ha hatással vannak az ügyfelekre: az üzleti működés elleni támadások akkor a leghatásosabbak, ha közvetlenül érintik, megzavarják az ügyfelek működését.

6. Az emberi tűzfal a védelem első vonala: az emberi hiba még mindig a legfontosabb kiberbiztonsági tényező [5] [8] [24] [25] [26].

A pénzügyi szektor esetében kiemelten fontos tényező, hogy a legtöbbször szenzitív adatokat kezelnek. Bár a blokklánc technológia tömeges elterjedése még várat magára, de megfelelő keretek között ez a technológia megoldást nyújthat a kibervédelem bizonyos kihívásaira. Jövőbeni új lehetőség lehet például a dolgok Internetje (*Internet of Things*, IoT) és a blokklánc technológia összekötésével a banki finanszírozás mögötti biztosítékok értékének valós idejű monitorozása is lehetővé válik.

FELHASZNÁLT IRODALOM

[1] M. Henriquez, „Security Magazine," 9 12 2021. [Online]. Available: https://www.securitymagazine.com/articles/96667-the-top-data-breaches-of-2021. [Hozzáférés dátuma: 16 12 2021].

[2] M. Henriquez, „Security Magazin," Reserved BNP Media, 20 10 2021. [Online]. Available: https://www.securitymagazine.com/articles/96128-banking-industry-sees-1318-increase-in-ransomware-attacks-in-2021. [Hozzáférés dátuma: 05 12 2021].

[3] P. Dr. Michelberger, Információ-, folyamat- és vállalatbiztonság, Budapest: ÓE-KGK-4086, ISBN 978-963-449-201-8, 2020.

[4] S. Scorecard, „Security Scorecard," Security Scorecard , 25 01 2021. [Online]. Available: https://securityscorecard.com/blog/what-is-an-attack-vector-common-examples. [Hozzáférés dátuma: 05 12 2021].

[5] A. G. Johansen, „Norton," NortonLifeLock, 23 11 2021. [Online]. Available: https://us.norton.com/internetsecurity-malware-ransomware-5-dos-and-donts.html. [Hozzáférés dátuma: 12 12 2021].

[6] Kaspersky, „What is Rootkit – Definition and Explanation," Kaspersky, na na 2021. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-rootkit. [Hozzáférés dátuma: 07 12 2021].

[7] KnowBe4, „Phishing," KnowBe4, [Online]. Available: https://www.phishing.org/what-is-phishing. [Hozzáférés dátuma: 12 12 2021].

[8] R. KARTCH, „Distributed Denial of Service Attacks: Four Best Practices for Prevention and Response," Carnegie Mellon University, 21 11 2016. [Online]. Available: https://insights.sei.cmu.edu/blog/distributed-denial-of-service-attacks-four-best-practices-for-prevention-and-response/. [Hozzáférés dátuma: 10 12 2021].

[9] C. D. Defense, „6 Password Security Risks and How to Avoid Them," Cypress Data Defense, 15 06 2020. [Online]. Available: https://www.cypressdatadefense.com/blog/password-security-risks/. [Hozzáférés dátuma: 08 12 2021].

[10] D. S. Michael Hill, „CSO, IDG Tech Media GmbH," 16 07 2021. [Online]. Available: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html. [Hozzáférés dátuma: 16 12 2021].

[11] G. Kiss, „The information security awareness of the Slovakian kindergarten teacher students at starting and finishing the study in higher education," SHS WEB OF CONFERENCES (2261-2424): 66 Paper 01042. 7 p., 2019.

[12] A. Szász, G. Kiss, „Jelszóvisszafejtő programok oktatási célú felhasználása és hatásuk az információbiztonsági tudatosságra," INFORMÁCIÓS TÁRSADALOM: TÁRSADALOMTUDOMÁNYI FOLYÓIRAT (1587-8694): 18 3-4 pp 82-104, 2018.

[13] A. Szász, G. Kiss, „Multimedia password retrieval programs in information security education," JOURNAL OF APPLIED MULTIMEDIA (1789-6967 1789-6967): 13 3 pp 87-96 Paper JAM.2018.3.002., 2018.
[14] Digitrend, „Kiberbiztonság: a leggyengébb láncszem a munkavállaló," Digitrend, 27 02 2020. [Online]. Available: https://digitrendi.hu/kiberbiztonsag-a-leggyengebb-lancszem-a-munkavallalo/. [Hozzáférés dátuma: 05 12 2021].
[15] E. global, „Building trust with your third parties in a technology-driven and disruptive world," EY third-party risk management, 2020. [Online]. Available: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-trpm-survey-2019-20-update-final.pdf. [Hozzáférés dátuma: 17 12 2021].
[16] C. Brook, „Digital Guardian," 6 10 2020. [Online]. Available: https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more. [Hozzáférés dátuma: 17 12 2021].
[17] K. T. P. Ltd., „Tailgating Attack: A Physical Social Engineering Crime," Kratikal Tech Pvt. Ltd., 20 04 2020. [Online]. Available: https://kratikal.medium.com/tailgating-attack-a-physical-social-engineering-crime-f63da4195536. [Hozzáférés dátuma: 10 12 2021].
[18] T. I. Team, „What is shoulder surfing?," Business Tech , 07 05 2021. [Online]. Available: https://www.businesstechweekly.com/cybersecurity/password-security/what-is-shoulder-surfing/. [Hozzáférés dátuma: 05 12 2021].
[19] G. Wright, „Tech Target," 04 2021. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/dumpster-diving. [Hozzáférés dátuma: 17 12 2021].
[20] Gabriel Bassett, C. David Hylender, Philippe Langlois, Alexandre Pinto, Suzanne Widup, 2021 Data Breach Investigations Report, Verizon, 2021.
[21] E. Learning, „Esme Learning," Esme Learning, 24 08 2021. [Online]. Available: https://esmelearning.com/blogs/news/blockchain-solving-financial-sector-problems. [Hozzáférés dátuma: 05 12 2021].
[22] D. Sinha, „Analytics Insight," 07 07 2021. [Online]. Available: https://www.analyticsinsight.net/blockchain-technology-disrupting-banking-sector-worldwide-in-2021/. [Hozzáférés dátuma: 22 02 2022].
[23] Mariano Belinky, Emmet Rennick, Andrew Veitch, „The Fintech 2.0 Paper: rebooting financial services," 2015. [Online]. Available: https://www.oliverwyman.com/our-expertise/insights/2015/jun/the-fintech-2-0-paper.html. [Hozzáférés dátuma: 01 02 2022].
[24] Ronald D. Lee, Michael A. Mancusi, Amber A. Hay, Anthony Raglani, „Arnold&Porter," 11 06 2021. [Online]. Available: https://www.arnoldporter.com/en/perspectives/publications/2021/06/lessons-learned-from-the-solarwinds-cyberattack. [Hozzáférés dátuma: 26 01 2022].
[25] J. p. M. Jr., „TechBeacon," 2020. [Online]. Available: https://techbeacon.com/security/8-lessons-garmin-ransomware-attack. [Hozzáférés dátuma: 26 01 2022].
[26] M. H. ("Heff"), „SecurityMetrics," [Online]. Available: https://www.securitymetrics.com/blog/garmin-ransomware-attack-soc-threat-analysis-and-10-lessons-learned. [Hozzáférés dátuma: 26 01 2022].