HADMÉRNÖK
VÉDELEMINFORMATIKA

16. évfolyam (2021) 3. szám 203–218.
DOI: 10.32567/hm.2021.3.12

Katona Gergő[1]

A Covid-19 kiberbiztonsági kihívásai az első hullám idején[2]

The Cybersecurity Challenges of Covid-19 during the First Wave

2019 végén Kínában jelent meg, majd rövid időn belül az egész világon elterjedt egy újfajta vírus, amely az általunk ismert világ berendezkedését átformálta. Világszerte kijárási korlátozásokat vagy éppen tilalmat rendeltek el, amivel a köznyelvben koronavírusként ismert SARS-CoV-2 vírus terjedését próbálták, illetve a mai napig próbálják lassítani. A védelmi intézkedések az élet számos területére nagy hatást gyakoroltak, a gazdasági tevékenységek számos országban szinte teljesen leálltak, emberek milliói veszítették el az állásukat. Egyik napról a másikra egyes közigazgatási szerveknek és a gazdasági vállalatok nagy részének át kellett költözni az online térbe. Ezen átállás számos kiberbiztonsági kihívást rejtett magában. Jelen cikkben megvizsgálom és csoportosítom, hogy milyen támadások voltak jelen a kibertérben az első hullám idején. Illetve megvizsgálom, hogy a hazai kiberbiztonsági szakértők az egyes fenyegetéseket mennyire tartják kockázatosnak szervezetükre nézve.

Kulcsszavak: Covid-19, kiberbiztonság, kiberfenyegetések, világjárvány

At the end of 2019, a new type of virus appeared in China and then spread around the world in a short time, reshaping it to furnish the world we know. There have been worldwide restrictions or bans on trying to slow down the spread of the SARS-CoV-2 virus – commonly known as the coronavirus – to this day. Protection measures are having a major impact on many areas of life, economic activity has come to a complete halt in many countries, and millions of people have lost their jobs. In the fastest way possible, some public administration organisations and most businesses had to switch to teleworking. This switch included a number of cybersecurity challenges. In this article, I examine and group what attacks were present

[1] Puskás Tivadar Műszaki Szakkollégium, e-mail: katonagergo520@gmail.com
[2] A cikk az Innovációs és Technológiai Minisztérium ÚNKP-20-2-II-NKE-84 kódszámú Új Nemzeti Kiválóság Programjának szakmai támogatásával készült.

in cyberspace during the first wave. I also examine the opinions of cybersecurity experts for risks of different threats.

Keywords: **Covid-19, cybersecurity, cyber threats, pandemic**

1. Problémafelvetés

Ahogy a világ átállt az online működésmódra, egyre nagyobb kihívást kezdtek jelenteni azok a fenyegetések, amelyek a kibertérben jelen vannak. Az online vásárlások mértéke világszerte megnőtt, a munkavállalók nagy része, ha munkaköre engedte, otthonról dolgozott, illetve diákok milliói álltak át az online oktatásra általános iskolától kezdve egyetemig bezárólag. Ezen átállás nagy aránya számos kibertérből érkező fenyegetés kockázatának mértékét növelte. Jelen cikkben megnevezem és csoportosítom azokat a támadási típusokat, amelyek gyakoriak voltak a Covid-19 első hullámának idején. Ezt követően kérdőíves kiértékelésemben megnevezem azt, hogy hazai viszonylatban az egyes fenyegetéseket mennyire ítélik meg kockázatosnak a szakértők, és ezen megítélésüket befolyásolják-e egyéb tényezők.[3]

Így a következő hipotéziseket vizsgáltam kutatásom során:

H1: Az első hullám idején újfajta fenyegetések nem jelentek meg, azonban a meglévők számában növekedés mutatható ki, és megjelenésük szofisztikáltabb, mint eddig.

H2: Feltételezem, hogy azon szakértők, akik szerint a szervezetüknél dolgozók sűrűbben szegik meg a szabályokat, kockázatosabbnak tartják a kiberbiztonsági fenyegetéseket.

2. Kutatási módszer

Megvizsgáltam az egyes fenyegetéseket, amelyek jelen voltak az első hullám idején. Ezenfelül kiértékeltem azokat a támadási statisztikákat, amelyek az egyes támadások paramétereit vizsgálták a definiált időszakban.

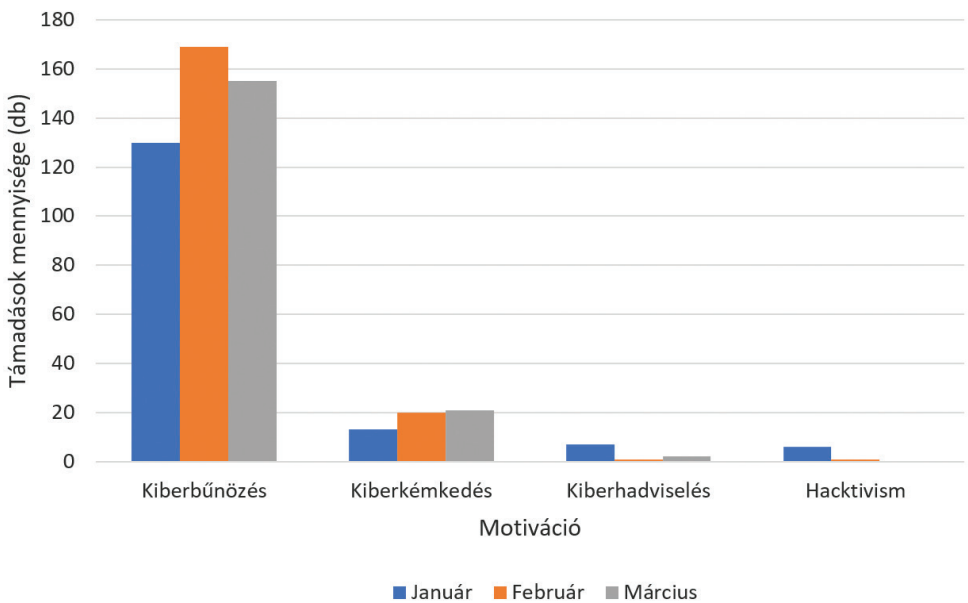
A kérdőívem célcsoportja a hazai kiberbiztonsági szakértők voltak. A kérdőívem kiértékelésére az IBM SPSS Statistics 25 programcsomagot használtam, amiben az eredményeim egy részét Kruskal–Wallis-próba alá vetettem. Ezt követően egyes kérdések kiértékelését osztályozással végeztem el. Kérdéseim egy csoportját kereszttáblás kiértékelés alá akartam vetni, azonban a Khi-négyzet próba azon feltétele nem teljesült, hogy az elvárt gyakoriság minden egyes cellában minimum 5 legyen. Ezért a Kruskal–Wallis-próbát használtam, amely egy típusa az olyan, összetett kontrollcsoportos vizsgálatnak, ahol kettőnél több részminta összehasonlítása történik ugyanazon változó alapján. Ekkor azt szeretnénk megtudni, hogy a részminták között van-e jelentős különbség ugyanazon változó alapján. A Kruskal–Wallis-próba segítségével tesztváltozót vizsgálunk egy csoportosító változóval. A tesztváltozónak és a csoportosító változónak is rangsorolt adatnak kell lennie. Fontosnak tartom kiemelni, hogy kutatásom során azért a Kruskal–Wallis-próbát használtam, nem pedig

[3] Megyeri Lajos – Farkas Tibor: Kockázatelemzés, tudomány vagy kuruzslás?. *Hadmérnök*, 12. (2017), 3. 198–209.

a Mann–Whitney U tesztet, mert a csoportosító változóban a rangsorolt értékek száma kettőnél több volt. A kívánt adatok betöltése és a próba lefuttatása után meg kell vizsgálni az eredményt. Ha az Asymp. Sig. változó, vagyis a szignifikancia nem haladja meg a 0,005-t ($p < 0{,}005$), akkor ki lehet jelenteni, hogy a részminták között jelentős különbség van a csoportosító változó függvényében. Ezután megvizsgáltam a rangátlagot, amely megmutatja a csoportosító változó értékeinek rangsorát a teszt-változó értékeinek függvényében.[4]

3. Eredmények

Ebben a részben bemutatom azokat a támadási formákat, amelyek elterjedtek voltak az agresszorok körében a koronavírus első hullámának idején. Azon adatokat, amelyek alapját adják a vizsgálatomnak, a *Hackmageddon* portál szolgáltatta. E portál adatait egy nemzetközileg elismert kiberbiztonsági szakember, Paolo Passeri gyűjti ki számos olyan forrásból, amelyek kibertámadásokat publikálnak. Látható, hogy motiváció szerint főleg kiberbűnözés volt fellelhető 2020 első negyedévében, továbbá megfigyelhető az is, hogy a támadások főbb célpontjai személyek voltak, de közigazgatás és egészségügy is eléggé nagy arányban állt a támadások középpontjában.

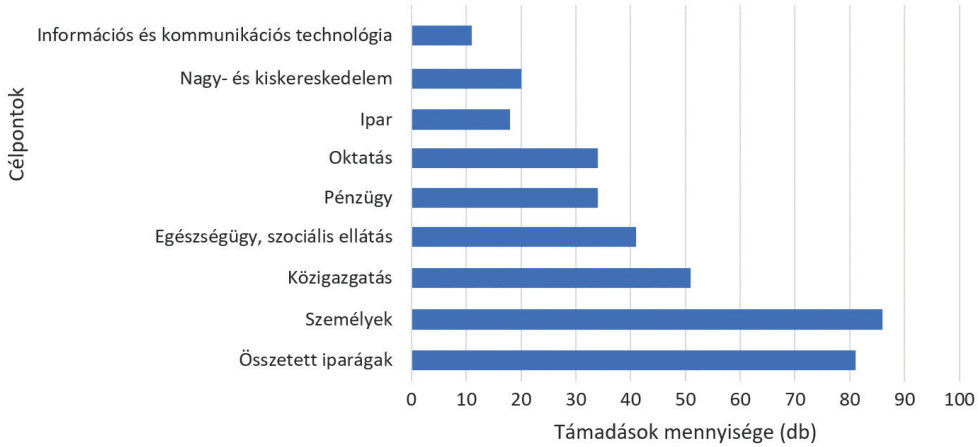


1. ábra

A motivációk havi elosztása 2020 Q1

Forrás: a szerző szerkesztése a *Hackmageddon* adatai alapján

[4] Sajtos László – Mitev Ariel: *SPSS. Kutatási és adatelemzési kézikönyv.* Budapest, Alinea, 2007.

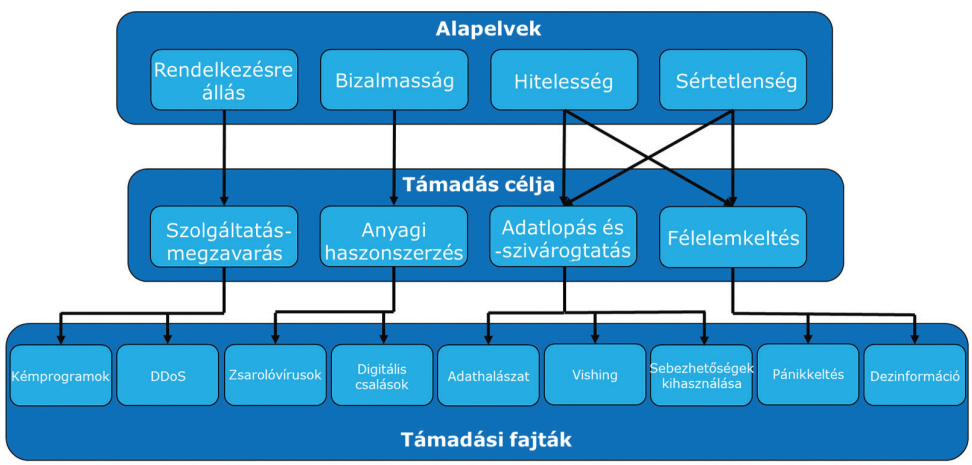


2. ábra

Támadások célpontjai 2020 Q1

Forrás: a szerző szerkesztése a *Hackameddon* adatai alapján

A továbbiakban elemzem, hogy a fenti ábrán látható célpontokat milyen célból, milyen eszközzel támadták az elkövetők, és hogy ezek a támadások mire irányultak. Illetve képet adok arról, hogy a támadók mely kiberbiztonsági fundamentum gyengítésével, megszüntetésével próbálták céljaikat elérni. Látni fogjuk azt, hogy egyes támadások között átfedés van, amely esetünkben azt jelenti, hogy egyes támadások végrehajtásához szükséges egy másik fenyegetés alkalmazása is.



3. ábra

A Covid-19 alatt megjelent támadások csoportosítása

Forrás: a szerző szerkesztése Saqib Hakak et al.: Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies. Access IEEE, 8. (2020), 124134–124144. alapján

Bizalmasság: „Az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról."[5]

Zsarolóvírusok: olyan rosszindulatú programok, amelyekkel a támadók a megfertőzött eszközt lezárják, ezzel elérhetetlenné téve az áldozat adatait. Céljuk a haszonszerzés, mivel váltságdíjat követelnek az adatok visszaállításáért, az úgynevezett visszafejtő kulcsért. Az e váltságdíj kifizetésére szabott határidő igen rövid, és legtöbbször a váltságdíjat valamely kriptodevizában kérik, azért, hogy ne lehessen visszakeresni a pénz útját. Ezek a támadók megtalálták a siker vektorát, amely magában foglalja az adatok kritikusságát és az információbiztonsági szegénységi küszöböt. Az információbiztonsági szegénységi küszöb egyensúlyt jelent egy szervezet biztonsági követelményei és a rendelkezésre álló költségvetés között. Egy szervezet a szegénységi küszöb alatt van, ha a biztonsági követelmények meghaladják a rendelkezésre álló költségvetést. A támadók rájöttek, hogy főleg az állami szektor szervezetei gyakran e szegénységi küszöb alá esnek, így ezek a szervezetek is a főbb célpontok között vannak. Bármely olyan szervezet, amely kritikus adatokat kezel elégtelen biztonsági költségvetéssel, tökéletes célpontja ezen anyagilag motivált kibertámadásnak. Az idő múlásával egyértelműen eltolódtak a támadási vektorok, ami bizonyítja a számítógépes bűnözés iparának opportunista tendenciáit. Elsődlegesen háromféle támadóvektor létezik a zsarolóvírus-fertőzés végrehajtására. A *social engineering* igen népszerű, és magában foglalja az adathalász taktikákat is, hogy megtévessze az áldozatot, aki rákattint egy linkre vagy rosszindulatú mellékletre. Más támadási vektorok is egyre népszerűbbek, mint például az ismert sebezhetőségek kihasználása. E vektor szerepe megnőtt a WannaCry segítségével, amely kihasználta a CVE-2017-0144 biztonsági résnek kitett hosztokat. Csak néhány hónappal később a NotPetya kihasználta ugyanezt a biztonsági rést, hangsúlyozva a rutinszerű és hatékony javításkezelés szükségességét. Végül a harmadik vektor a távoli bejelentkezési szolgáltatások kikényszerítése. A gyenge autentikációval rendelkező távoli asztaliprotokoll-szolgáltatásokat a támadók illetéktelen hozzáférésre és ransomware telepítésére kényszerítik.[6]

Online csalások: A tiltott pénzügyi nyereség megkönnyítésére tervezett Covid-19 témájú rosszindulatú programok mellett a koronavírus témájú marketingtevékenységek számának növekedése is megfigyelhető. Ilyenek például a személyes védőeszközök (PPE) vagy más, a Covid-19-hez kapcsolódó termékek csillagászati áron történő eladásának kísérletei. Vagy hamisított és nem jóváhagyott berendezések és termékek értékesítése. Az Interpol-felmérésre válaszoló tagországok körülbelül kétharmada számolt be arról, hogy a járvány kitörése óta a Covid-19-témát jelentős mértékben használják adathalászatra és más online csalásra. 2020 januárja óta az Interpol egyik magánpartnere, a Trend Micro 907 ezer üzenetet észlelt a Covid-19-hez kapcsolódóan, kihasználva a gazdasági visszaesést és az emberek szorongását a világjárvány idején. A kiberbűnözők fokozták social engineering taktikájukat azzal,

[5] Muha Lajos – Krasznay Csaba: Az elektronikus információs rendszerek biztonságáról vezetőknek. Budapest, Nemzeti Közszolgálati Egyetem, 2014. 9.

[6] Pranshu Bajpai – Richard J. Enbody: Attacking Key Management in Ransomware. *IT Professional,* 22. (2020), 2. 21–27.

hogy támadásaik alapjául a Covid-19-et használták.[7] A sértetlenségnél részletesebben kifejtem az adathalászmódszerek működését.[8]

Sértetlenség: „[A]z adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható."[9]

Hitelesség: a CIA-triász legújabb kiegészítése, amelyben a végső cél annak ellenőrzése, hogy a kapott üzenet vagy bármilyen adatcsere csak az eredeti forrásból származik-e. Ezt a célt gyakran statikus és dinamikus hitelesítési módszerekkel történő hitelesítéssel érik el. A járvány során számos rosszindulatú programot hoztak létre, hogy megkönnyítsék a felhasználói adatok és információk eltulajdonítását.[10]

Adathalászat: Fontosnak tartom megjegyezni, hogy a 3. ábrán maga az adathalászat és a Vishing külön szerepel. Ezen felosztás megtalálása azért volt számomra megfelelő, mert attól, hogy a telefonos adathalászat része a phishingnek, mégis olyan, merőben más technikai hátteret és folyamatot igényel, amely megkülönbözteti a többi adathalásztípustól. Az adathalászat szintén gyakori fenyegetés, amelyet a pandémiás helyzetben alkalmaznak a támadók. Az adathalászat alapja, hogy a támadók egy megbízható entitásnak adják ki magukat, mint például pénzintézet, közigazgatási szerv, munkáltató. A támadók meghamisítják az e-mail-címüket, így úgy tűnik, hogy valaki mástól származik. Hamis webhelyeket hoznak létre, és idegen karakterkészleteket használnak az URL-ek leplezéséhez. Különféle technikák léteznek, amelyek az adathalászat égisze alá tartoznak. A támadások kategóriákra bontására többféle módszer létezik. Az adathalász kampány általában két dolog egyikére próbálja rávenni az áldozatot:

- Érzékeny információk megszerzése: Ezeknek az üzeneteknek az a célja, hogy rávegyék a felhasználót a fontos adatok felfedésére, mint például felhasználónév és jelszó, amelyet a támadó felhasználhat a rendszer vagy a fiók megsértésére. A csalás klasszikus változata magában foglalja az e-mailek küldését, amit az emberek millióinak kiküldenek egy ismert bank nevében, így biztosítják, hogy a címzettek legalább egy része ennek a banknak az ügyfele legyen. Az áldozat rákattint az üzenetben található linkre, és egy rosszindulatú webhelyre kerül. Ezen oldalak többségében vagy egy feltört weboldalon helyezkednek el, vagy egy teljesen új domainnel lettek regisztrálva. Az egyik fő árulkodó jel az URL-cím lehet, amely ilyenkor teljesen más, mint az eredeti oldal esetében. Itt az áldozat megadja a belépési azonosítóját, amit már a támadó fel is tud használni.
- Rosszindulatú programok letöltése: A sok spamhez hasonlóan az ilyen típusú adathalász e-mailek célja, hogy az áldozat saját számítógépét megfertőzze rosszindulatú programokkal. Az üzenetek gyakran csalogató információkat ígérnek, mint például küldhető egy HR-munkatársnak olyan melléklet, amely állítólag

[7] Interpol: INTERPOL Report Shows Alarming Rate of Cyberattacks during COVID-19. (2020. augusztus 4.).
[8] Bányász Péter: Social engineering és közösségi média. *Nemzetbiztonsági Szemle,* 5. (2018), 1. 59–77.
[9] Muha–Krasznay (2014): i. m.
[10] William Stallings – Lawrie Brown: *Computer Security: Principles and Practice.* Boston, Pearson, 2012.

egy álláskereső önéletrajza lehet. Ezek a mellékletek gyakran.zip fájlok vagy rosszindulatú beágyazott kódot tartalmazó Microsoft Office dokumentumok. A rosszindulatú kódok leggyakoribb formája a ransomware – 2017-ben becslések szerint az adathalász e-mailek 93%-a tartalmazott zsarolóvírus-mellékleteket.[11]

Csoportosítani lehet az adathalász-támadásokat az elkövetés módja szerint is:

- Az első, amit meg lehet említeni, az SMS adathalászat, ahol a támadók egy hivatalosnak tűnő SMS-ben kérik az áldozatot, hogy a megadott linkre kattintva adja meg adatait. Számos adathalász-támadás központi eleme egy adathalászoldal, amely egy az egyben másolata azon szervezet oldalának, amelynek nevében az áldozatot felkeresték.
- A következő típus a Spear phishing célzott támadás, ahol a támadók az áldozatokról már tudnak egyes adatokat, mint például beosztás, e-mail-cím, telefonszám. Ezáltal egy személyre szólóbb és célozottabb támadást tudnak végrehajtani.
- A bálna-adathalászat a célzott adathalászat egyik formája, amely a nagyon nagy „halakra" – vezérigazgatókra vagy más fontos célpontokra – irányul. E csalások közül sokan a vállalati igazgatóság tagjait célozzák meg, akiket különösen kiszolgáltatottnak tartanak.

A RiskIQ beszámolt arról, hogy háromnapos időszak alatt (azaz 2020. április 11–13.) több mint 309 000 spam e-mailt fedeztek fel, amelyek vagy „korona", vagy „covid" kifejezést tartalmaztak.[12] Ezekben az e-mailekben a támadók az Egészségügyi Világszervezet tagjának (WHO) vagy egészségügyi szakembernek adták ki magukat, olyan előtagok használatával, mint a „Dr" és a „Professzor". Ezek az e-mailek gyakran tartalmaznak olyan témaköröket, mint a „Covid-19 frissítések", „A városod Covid-19 nyomkövetője", amelyek célja az áldozatok csalogatása a mellékletre való kattintásra, például „.rtf" kiterjesztésű fájlokra.[13]

- Vhishing (Telefonos adathalászat): A távoli ügyintézés (például Távegészségügy) mindennapossá vált a jelenlegi Covid-19-járványban, amelyben a szervezetek rugalmas munkamegállapodásokat kínálnak alkalmazottaiknak. Tekintettel arra, hogy ezek az alkalmazottak üzleti tevékenységük során nagymértékben támaszkodnak a telefonos és az internetes kommunikációra, egy ilyen kommunikációs csatornát a támadók könnyen ki tudnak használni. Például olyan támadásokról számoltak be, hogy az üzleti és személyes kommunikációt eltérítik hangalapú adathalászattal (azaz vishing), robocall-csalások és egyéb technikai támogatású csalások útján. Fény derül arra is, hogy ezek a támadók visszaélnek az IP- (Voice over IP, VoIP) szolgáltatásokkal, hogy becsapják az egyéneket a nem létező szolgáltatások kifizetéséért vagy személyes adataik (például bankszámlaadataik, társadalombiztosítási számaik) megszerzéséért.

[11] Maria Korolov: 93% of phishing emails are now ransomware. *CSO Online,* 2016. június 1.
[12] Hakak (2020): i. m.
[13] CISA. Cybersecurity and Infrastructure Security Agency: COVID-19 Exploited by Malicious Cyber Actors. (2020. április 8.).

- Kiszolgáltatottság kiaknázása: A meglévő társadalmi távolságtartási követelmények eredményeként szüneteltek az olyan szervezetek tevékenységei, mint az egyetemek, a kormányzati szervek ügyfélfogadása és más nem alapvető szolgáltatások. Ez a bezárás az online rendszerek és platformok, például az online tanuláskezelő rendszerek (*Learning Management System,* LMS) és a videokonferencia-alkalmazások és eszközök (például Zoom) jelentős használatát eredményezte. Számos olyan eseményről számoltak be – némelyike nagy nyilvánosságot is kapott –, amelyek során a számítógépes bűnözők azonosítják és kihasználják a fent említett rendszerek és platformok sebezhetőségét.
- Dezinformáció és pánikkeltés: Számos közösségimédia-kampányt figyeltek meg a népszerű közösségimédia-platformokon is, mint például a Facebook, a WhatsApp és a LinkedIn, ahol hamis vagy félrevezető információkat tettek közzé. Ilyen például, hogy egyes gyógyszerek hatékonyak a Covid-19 ellen, vagy a tehén vizeletének fogyasztása megakadályozhatja a vírus átadását. Bár semmilyen tudományos bizonyíték nem igazolja ezeket az állításokat, zavart keltettek a nyilvánosság körében, és egyes esetekben halálesetekhez vagy sérülésekhez vezettek. A közösségi média platformjain keresztül számos cikket és videót osztottak meg, amelyek megtanítják, hogyan hozzanak létre házi készítésű kézfertőtlenítő-szereket és más kapcsolódó termékeket. Természetesen ezeken a felületeken is felmerültek olyan állítások, miszerint a Covid-19 nem valós, és az állampolgároknak figyelmen kívül kell hagyniuk a társadalmi távolságtartás követelményeit és a maszkhasználatot. Az ilyen dezinformálás könnyen vezethet gyorsabban növekedő esetszámokhoz és ezáltal több halálesethez.[14]

Rendelkezésre állás: „annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek."[15]

- DDoS-támadások: A számos létező fenyegetés között az elosztott szolgáltatásmegtagadással járó támadás (*Distributed Denial of Service,* DDoS) viszonylag egyszerű, de nagyon hatásos technika az intranet és az internetes erőforrások megtámadására. Ebben a támadásban a jogosultsággal rendelkező felhasználókat általában nagy mennyiségű gépi erőforrás akadályozza a webalapú szolgáltatások használatában. A DDoS-támadásokat hálózati, szállítási és alkalmazási rétegekben lehet megvalósítani különböző protokollok, például TCP, UDP, ICMP és HTTP használatával. Az Europol a pandémiás helyzetben a DDoS-támadások folyamatos növekedéséről számolt be. Ezeknek a támadásoknak jelentős gyakorlati következményei vannak, mert többek között a társadalmi távolságtartás, az otthoni munkavégzés és az online oktatási tevékenységek miatt is nő az internetezők száma. Ezért alapból az egyes szolgáltatások így nagyobb terhelést kapnak, mint amekkora a vírus előtt megszokott volt.[16]

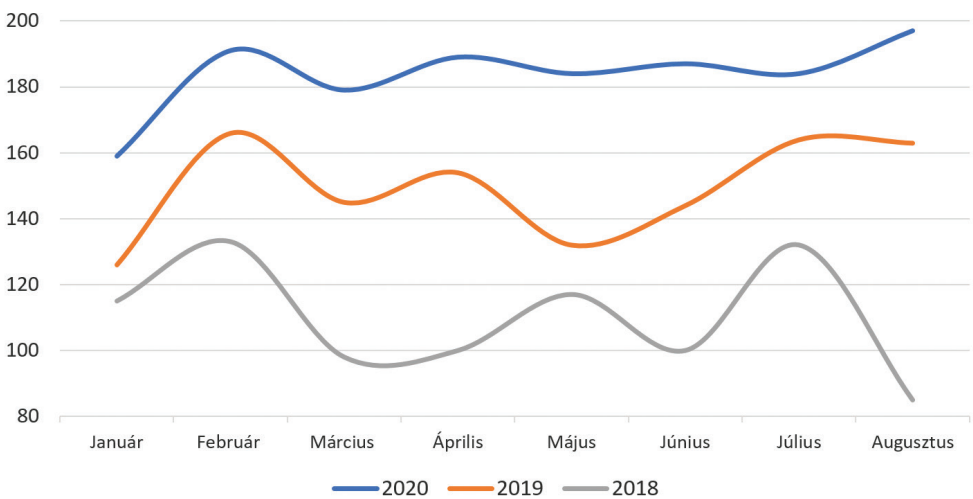
[14] Hakak (2020): i. m.; Bányász Péter: A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében. *Szakmai Szemle,* 13. (2016), 1. 61–81.

[15] Muha–Krasznay (2014): i. m.

[16] Iman Sharafaldin et al.: Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. *International Carnahan Conference on Security Technology.* 2019. 1–8; András Tóth: Information-Sharing Challenges and Issues in Multinational Operations Part 1. *Land Forces Academy Review,* 25. (2020), 4. 307–316.

- Kémprogram-támadások: A kémprogram egy olyan, rosszindulatú szoftver, amelyet rendszerek titkos információinak megszerzésére használnak. Például a COVID-19-hez kapcsolódó nyomkövető-alapú alkalmazásokat állítólag kémprogram-alapú applikációkba ágyazták a felhasználók tevékenységének nyomon követésére. Az ilyen nyomkövető és kontaktkutató alkalmazások különböző kapcsolati típusokat használnak, az adott eszköz és környezete azonosításához, ilyen a GPS, Bluetooth kapcsolat. A GPS alapon működő alkalmazások helymeghatározó adatokat küldenek a központi hatóságoknak időbélyegekkel. Ha kiderült az adott illetőről, hogy fertőzött, ezeket az adatokat össze tudják vetni a más eszközök által küldött adatokkal. Ezáltal értesíteni tudják azon személyeket, akik azonos időben a fertőzött, személy közelében voltak. A Bluetooth technológia képes egyszerre több kapcsolatot létrehozni, és ezeket fenntartani. Ennek a technológiának a megfelelő alkalmazása segítségével szintén beazonosíthatók azon eszközök felhasználói, akik fertőzött személy közelében tartózkodtak és esetleg maguk is megfertőződtek. [17]

A 4. ábrán látható, hogy a kibertámadások számában növekedés mutatható ki az előző évekhez képest, amely növekedésben közrejátszik természetesen a koronavírus megjelenése. Ezen kijelentésemet többek között mind az Interpol-, mind a RiskIQ-források alátámasztják. Azonban azt is ki kell jelenteni, hogy a vírus előtt is folyamatos növekedő tendencia volt jelen e támadások esetében.



4. ábra

A kibertámadások számának alakulása 2018–2020

Forrás: a szerző szerkesztése a *Hackameddon* adatai alapján

[17] Németh Attila – Magyar Sándor: An investigation of data used to support contact tracing to curb the spread of COVID-19 pandemic from the aspect of possible national security application (part 1). *National Security Review,* 6. (2020), 2. 52–64.

A fenti adatok alapján a támadásokat összegezve a T1-es tézisem az lett, hogy az első hullám idején nem jelentek meg új fenyegetések, viszont a már eddig jelen lévők számában növekedés mutatható ki, és e támadások egy részének témája a koronavírus lett. Így a H1 hipotézisem helytállónak bizonyult.

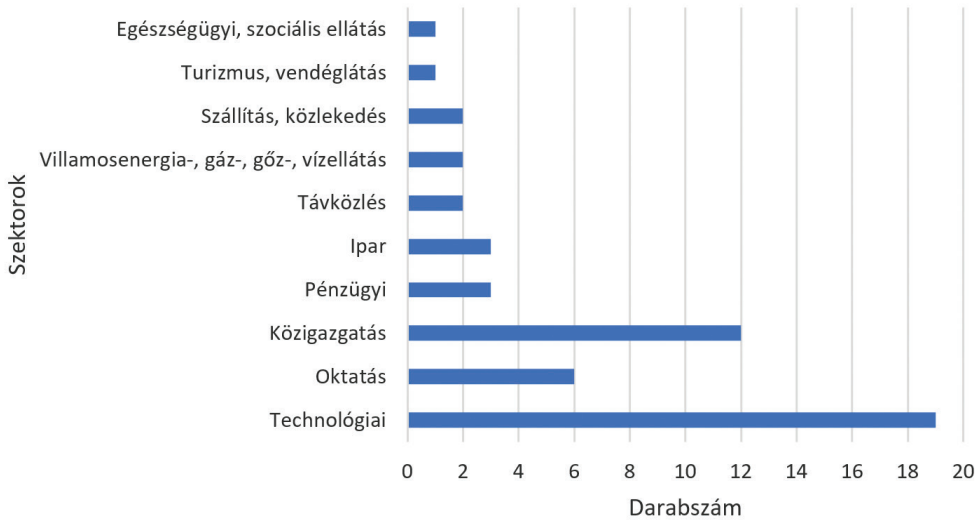
3.1. Kérdőíves felmérés eredménye

Empirikus kutatásom gerincét a kérdőívem jelentette, amelyet hazai információbiztonságban dolgozó személyek körében töltettem ki. A kérdőívem kialakításához több nemzetközi tanulmányt vizsgáltam meg a kérdéskörben.[18] Végül Ulrik Franke és szerzőtársa, Joakim Wernberg által írt *A survey of cyber security in the Swedish manufacturing industry* cikk kérdőívét vettem alapul, és témaspecifikusan reprodukáltam. Kérdőívemben rákérdeztem a távoli munkavégzés megjelenésére, illetve megkérdeztem szakembereket, hogy az egyes fenyegetési típusokat mennyire tartják kockázatosnak saját szervezetükre nézve. A kérdőív két fő részből áll, az első rész általános információkra kérdez rá: itt olyan kérdések találhatók meg, amelyek magára a kitöltő személyre vonatkoznak (például melyik szektorban dolgozik; milyen végezettséggel rendelkezik; milyen beosztásban dolgozik; mióta dolgozik a kiberbiztonságban). A második részben főleg a támadási típusok és a távmunka kérdésköre, illetve a szervezetben dolgozó személyi kör szabályzatkövetési hajlandósága volt a téma (például távmunka volt-e engedélyezve; tettek-e külön intézkedést távmunka kapcsán; milyen típusú fenyegetést mennyire kockázatosnak ítélnek meg a szervezetre nézve; a munkavállalók szabálykövetők-e). A kérdőívem természetesen anonim volt, mivel olyan adatot nem kértem, amivel ki lehet deríteni a kérdőív kitöltőjének személyazonosságát, így megfelel a 2011. évi CXII. törvénynek, és ezáltal az Általános Adatvédelmi Rendeletnek (*General Data Protection Regulation,* GDPR).

Kérdőívemet 51 szakértő töltötte ki, jellegét tekintve nem reprezentatív a felmérés. A legtöbben a technológiai szektorból töltötték ki, szám szerint 19 személy; ezt követte a közigazgatási szektor 12 kitöltővel; majd az oktatás 6; pénzügyi szektor és az ipar 3; és a szállítás, közlekedés; villamosenergia-, gáz-, gőz-, vízellátás; távközlés 2 fő kitöltést kapott. A turizmus, vendéglátást; egészségügyi, szociális ellátást 1-1 ember választotta. A kitöltők 47%-a elektronikus információbiztonsági vezetői képzéssel rendelkezik; 21,6%-nak Certified Information Systems Auditor (CISA-) bizonyítványa van; 17,6%-a rendelkezik Certified Information Security Manager (CISM-) képesítéssel; 5,9% nyilatkozott arról, hogy Certified Information Systems Security Professional (CISSP-) végzetsége van; 11,8% Certified in Risk and Information Systems Control (CRISC-) bizonyítványa van; ISO lead auditor képesítéssel a válaszadók 27,5%-a rendelkezik; ISO internal auditor 11,8%-a megkérdezettek közül; egyéb

[18] Mark Rodbert: Why organisational readiness is vital in the fight against insider threats. *Network Security,* (2020), 8. 7–9; Mohamed Amine Ferrag – Messaoud Babaghayou – Mehmet Akif Yazici: Cyber security for fog-based smart grid SCADA systems: Solutions and challenges. *Journal of Information Security and Applications,* 52. (2020), 102500; Ulrik Franke – Joakim Wernberg: A survey of cyber security in the Swedish manufacturing industry. *International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2020.* 1–8; Hakak (2020): i. m.

információbiztonsági képesítéssel a kitöltők 23,5%-a rendelkezik és további 43,1% rendelkezik egyéb nem információbiztonsághoz kötődő végzettséggel. Fontosnak tartom kiemelni, hogy a kitöltők itt több válaszlehetőséget is választhattak, mivel az egyik végzettség nem zár ki más végzettségeket.



5. ábra

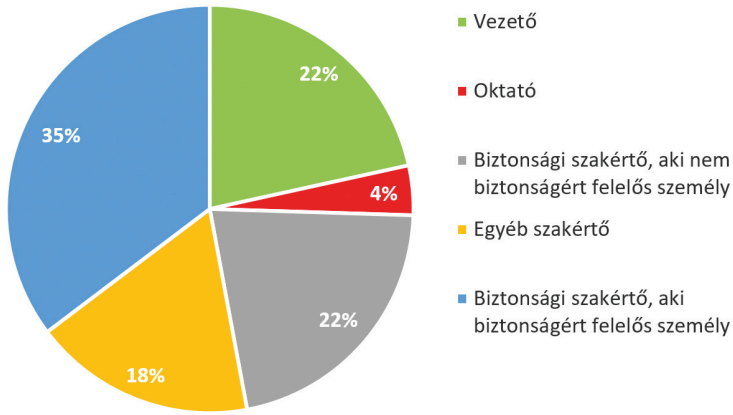
Kitöltők szektorbeli megoszlásai (fő)

Forrás: a szerző szerkesztése

Következő kérdésem arra irányult, hogy milyen beosztásban dolgoznak, ami egy nyitott kérdés volt. Így a kapott válaszokon osztályozó kiértékelést végeztem el. Öt külön osztályt hoztam létre, amelyek a következők voltak:

- vezető (gyakori válaszok: CEO, ügyvezető igazgató, vezető);
- oktató (gyakori válaszok: oktató, oktatás);
- biztonsági szakértő, aki nem biztonságért felelős személy (gyakori válaszok: tanácsadó; IT-biztonsági tanácsadó, IT-biztonsági elemző);
- egyéb szakértő (gyakori válaszok: termékfelelős rendszermérnök, sales, informatikus);
- biztonsági szakértő, aki biztonságért felelős személy (gyakori válaszok: IBF, információbiztonsági felelős, CISO, DPO).

Azt láthatjuk, hogy a kitöltők 22%-a vezető beosztásban dolgozik; 4%-a oktató; 22%-a biztonsági szakértő, aki nem biztonságért felelős személy; 18%-a egyéb szakértő és 35%-a biztonsági szakértő, aki biztonságért felelős személy.



6. ábra

Beosztás szerinti megoszlás (%)

Forrás: a szerző szerkesztése

A kérdőívemben megkérdeztem a szakembereket, hogy mekkora kockázati értéket adnának a következő támadásoknak a következő 1 évre:

- Az üzletmenet-folytonosság megszakításával járó támadás;
- Olyan támadás, amely az adatok megsértésével jár, és nyilvánossá válnak ezen adatok;
- Adatmegsértéssel járó támadás, ahol az adatokat a támadó megtartja magának (például ipari kémkedés);
- Nem szándékos esemény, amely üzletmenet-folytonosság megszakításával jár;
- Távoli munkavégzést kihasználó támadások.

A választási lehetőségek a következők voltak:

- Elhanyagolható kockázat;
- Alacsony kockázat;
- Közepes kockázat;
- Magas kockázat;
- Nagyon magas kockázat;
- Nem tudom.

A szakértők legnagyobb számban közepes kockázati szintet jelöltek meg a támadásoknál (szám szerint 84), ezt követi 69-cel az alacsony kockázati besorolás; majd 54-gyel az elhanyagolható szintű besorolás; az utolsó előtti összmennyiségben a magas kockázat 39-cel; és utolsó 3 db-bal a nagyon magas kockázat. Ebből látható, hogy a szakértők nagy része felkészültnek tartja a szervezeteiket e támadásokra. Ezenfelül az is látható az 1. táblázatból, hogy a magas és a nagyon magas kockázati szint összege a távoli munkavégzést kihasználó támadásoknál a legmagasabb. Ez azt jelenti, hogy a felsorolt támadási típusokból a kitöltők legnagyobb része a távoli munkavégzés kihívásaitól tart legjobban.

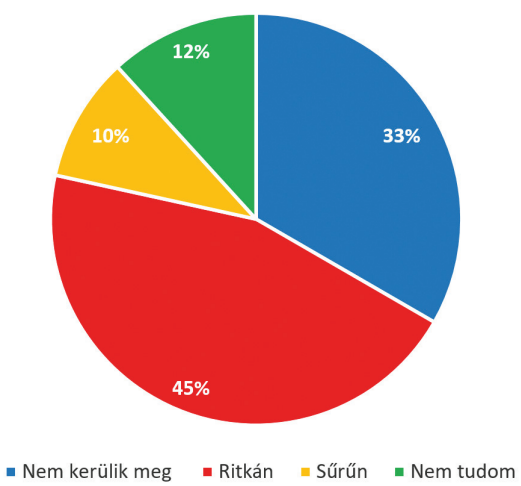
1. táblázat

Egyes fenyegetések bekövetkezési valószínűségének kockázatai a szakértők véleménye szerint (db)

Forrás: a szerző szerkesztése a kérdőív alapján

Mennyire tartja valószínűnek, hogy az Ön szervezete a következő 12 hónapban az alábbi incidensek valamelyikét elszenvedi						
	Az üzletmenet-folytonosság megszakításával járó támadás	**Olyan támadás, amely az adatok megsértésével jár, és nyilvánossá válnak ezen adatok**	**Adatmegsértéssel járó támadás, ahol az adatokat a támadó megtartja magának (például ipari kémkedés)**	**Nem szándékos esemény, amely üzletmenet-folytonosság megszakításával jár**	**Távoli munkavégzést kihasználó támadások**	**Válaszok megoszlása kockázati szintenként**
Elhanyagolható kockázat	13	8	15	9	9	54
Alacsony kockázat	14	18	16	13	8	69
Közepes kockázat	19	18	10	18	19	84
Magas kockázat	3	6	9	8	13	39
Nagyon magas kockázat	0	0	0	2	1	3
Nem tudom	1	0	0	0	0	1

Kérdőívemben kitértem arra is, hogy a szakértők szerint a szervezetükben megszegik-e a szabályokat, és ha igen, akkor ezt milyen sűrűn teszik. A 7. ábrán is látható, hogy a válaszadók 33%-a szerint a szervezetben dolgozó munkavállók nem kerülik meg a szabályokat; 45% gondolja úgy, hogy ritkán, de megkerülik a dolgozók a szabályokat; 10% az az arány a kitöltők esetében, akik azt mondják, hogy a munkavállalók sűrűn megkerülik a szabályokat és 12% nem tudta eldönteni ezt saját szervezetére nézve.



7. ábra

Szabálymegkerülési gyakoriság (%)

Forrás: a szerző szerkesztése

Mind a támadások kockázatára, mind a szabályszegés sűrűségére adott válaszokat megtisztítottam úgy, hogy kikerüljenek azon személyek válaszai, akik valamely kérdésnél a nem tudom opciót választották, így marad 44 válasz, amit külön Kruskal–Wallis-próba alá vetettem. Kíváncsi voltam, hogy van-e összefüggés a megadott fenyegetésekre adott kockázati szint, illetve a szabálykerülés sűrűségének szintje között. A próba lefuttatásában a csoportosító változó a szabálymegkerülési sűrűség és a tesztváltozók az egyes támadások kockázatának mértéke volt. A 2. táblázatból jól lehet látni azt, hogy a szignifikancia értéke egyedül az „Adatmegsértéssel járó támadás, ahol az adatokat a támadó megtartja magának (például ipari kémkedés)" csoportban haladja meg 0,005-t. Ez azt jelenti, hogy a másik 4 csoportban jelentős különbség mutatható ki a kockázati megítélésben a szabálymegkerülés függvényében.

2. táblázat

Kruskal–Wallis-próba szignfikanciaeredménye

Forrás: a szerző szerkesztése az SPSS alapján

	Nem szándékos esemény, amely üzletmenet-folytonosság megszakításával jár	**Távoli munkavégzést kihasználó támadások**	**Adatmegsértéssel járó támadás, ahol az adatokat a támadó megtartja magának (például ipari kémkedés)**	**Olyan támadás, amely az adatok megsértésével jár, és nyilvánossá válnak ezen adatok**	**Az üzletmenet-folytonosság megszakításával járó támadás**
Kruskal–Wallis H	11,566	13,756	4,766	15,140	11,541
df	2	2	2	2	2
Asymp. Sig.	,003	,001	,092	,001	,003

Ezt követően megvizsgáltam azt, hogy a rangátlag ebben a 4 csoportban miként oszlik meg. Ez a rangátlag mutatja meg a csoportosító változó értékeinek rangsorát (milyen sűrűn kerülik meg a szabályokat a szervezetben dolgozók) a tesztváltozó értékeinek (egyes fenyegetésre adott kockázati érték) függvényében. Ennek eredménye a 3. táblázatban látható.

Mind a 4 tesztváltozó esetében azt lehet megfigyelni, hogy a legmagasabb rangátlagot a sűrű szabálymegkerülés kapta, ezt követte a ritka megkerülés, és végül legkisebb rangátlagot a nem kerülik meg csoportosító változó kapta. Ezáltal kijelenthető az, hogy a kitöltésben részt vevő szakértők nagyobb kockázati értéket adtak, ha úgy vélték, hogy a szervezetben dolgozók megszegik a szabályokat. Így azon T2 tézisem született, miszerint azok a szakértők, akik szerint a szervezetüknél a szabálymegkerülés sűrűn fordul elő, nagyobb kockázati értéket adnak az egyes fenyegetéseknek, ezzel alátámasztottam a H2 hipotézisemet.

3. táblázat
A csoportosító értékek rangátlaga a tesztváltozók függvényében
Forrás: a szerző szerkesztése az SPSS alapján

	Nem kerülik meg a szabályokat rangátlaga	Ritkán kerülik meg a szabályokat rangátlaga	Sűrűn kerülik meg a szabályokat rangátlaga
Nem szándékos esemény, amely üzletmenet-folytonosság megszakításával jár	14,53	27,05	29,60
Olyan támadás, amely az adatok megsértésével jár, és nyilvánossá válnak ezen adatok	13,50	27,63	30,50
Az üzletmenet-folytonosság megszakításával járó támadás	14,71	26,77	30,20
Távoli munkavégzést kihasználó támadások	13,85	27,55	29,70

4. Összegzés

Az első hullám idején látható, hogy a legtöbb kibertérből érkező támadás hátterében mint motiváció a kiberbűnözés állt, amely főleg személyeket, közigazgatást és összetett iparágakat célzott meg. Ezen támadások között új nem jelent meg, ami azt jelenti, hogy olyan támadásokat használtak az elkövetők, amelyek 2020 januárja előtt is elérhetők voltak, viszont számukban növekedés mutatható ki, illetve egyes támadások központi témája a koronavírus lett. Hazai viszonylatban az mondható el, hogy a kitöltésben részt vevő szakértők egyes fenyegetéseket illető kockázati besorolására nagy befolyást gyakorol a szervezet szabálykövetése. Ezen eredmény azért lehet figyelemre méltó, mert a kitöltésben részt vevő szakértők végzik nagy eséllyel a szervezetükben a kockázatelemzést, amely alapján priorizálják a kockázatcsökkentő lépéseket. E priorizálás útján tervezik meg a fejlesztéseket és allokálják az egyes erőforrásokat a kockázatcsökkentő lépésekre.

Felhasznált irodalom

Amine Ferrag, Mohamed – Messaoud Babaghayou – Mehmet Akif Yazici: Cyber security for fog-based smart grid SCADA systems: Solutions and challenges. *Journal of Information Security and Applications,* 52. (2020), 102500. Online: https://doi.org/10.1016/j.jisa.2020.102500

Bajpai, Pranshu – Richard J. Enbody: Attacking Key Management in Ransomware. *IT Professional,* 22. (2020), 2. 21–27. Online: https://doi.org/10.1109/MITP.2020.2977285

Bányász Péter: Social engineering és közösségi média. *Nemzetbiztonsági Szemle,* 5. (2018), 1. 59–77.
Bányász Péter: A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében. *Szakmai Szemle,* 13. (2016), 1. 61–81.
CISA. Cybersecurity and Infrastructure Security Agency: *COVID-19 Exploited by Malicious Cyber Actors.* (2020. április 8.). Online: https://us-cert.cisa.gov/ncas/alerts/aa20-099a
Franke, Ulrik – Joakim Wernberg: A survey of cyber security in the Swedish manufacturing industry. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*. 2020. 1–8. Online: https://doi.org/10.1109/CyberSA49311.2020.9139673
Hakak, Saqib – Wazir Zada Khan – Muhammad Imran – Kim-Kwang Raymond Choo –Muhammad Shoaib: Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies. *Access IEEE,* 8. (2020), 124134–124144. Online: https://doi.org/10.1109/ACCESS.2020.3006172
Interpol: INTERPOL Report Shows Alarming Rate of Cyberattacks during COVID-19. (2020. augusztus 4.). Online: www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
Korolov, Maria: 93% of phishing emails are now ransomware. *CSO Online,* 2016. június 1. Online: www.csoonline.com/article/3077434/93-of-phishing-emails-are-now-ransomware.html
Megyeri Lajos – Farkas Tibor: Kockázatelemzés, tudomány vagy kuruzslás?. *Hadmérnök,* 12. (2017), 3. 198–209. Online: www.hadmernok.hu/173_18_megyeri.pdf
Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságáról vezetőknek.* Budapest, Nemzeti Közszolgálati Egyetem, 2014. Online: https://opac.uni-nke.hu/webview?infile=&sobj=9695&source=webvd&cgimime=application%2Fpdf
Németh Attila – Magyar Sándor: An investigation of data used to support contact tracing to curb the spread of COVID-19 pandemic from the aspect of possible national security application (part 1). *National Security Review,* 6. (2020), 2. 52–64.
Rodbert, Mark: Why organisational readiness is vital in the fight against insider threats. *Network Security,* (2020), 8. 7–9. Online: https://doi.org/10.1016/S1353-4858(20)30092-1
Sajtos László – Mitev Ariel: *SPSS. Kutatási és adatelemzési kézikönyv.* Budapest, Alinea, 2007.
Sharafaldin, Iman – Arash Habibi Lashkari – Saqib Hakak – Ali A. Ghorbani: Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. *2019 International Carnahan Conference on Security Technology,* 2019. 1–8. Online: https://doi.org/10.1109/CCST.2019.8888419
Stallings, William – Lawrie Brown: *Computer Security: Principles and Practice.* Boston, Pearson, 2012.
Tóth András: Information-Sharing Challenges and Issues in Multinational Operations Part 1. *Land Forces Academy Review,* 25. (2020), 4. 307–316. Online: https://doi.org/10.2478/raft-2020-0037