

D I P L O M A M U N K A

Katona Gergő
2022



**Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok Kar
Köszervezési és Infotechnológiai Tanszék
Kiberbiztonsági mesterképzési szak**

A home office kiberbiztonsági kihívásai a COVID-19 tükrében

A konzulens:

Dr. Bányász Péter, adjunktus

Szakfelelős:

Dr. Krasznay Csaba, egyetemi docens

Készítette:

Katona Gergő

**Budapest
2022**



Tartalomjegyzék

Bevezetés	3
<i>A téma aktualitása.....</i>	<i>3</i>
<i>A tudományos probléma.....</i>	<i>4</i>
<i>Módszertan.....</i>	<i>4</i>
<i>Kutatási hipotézisek</i>	<i>4</i>
<i>Kutatási célkitűzések</i>	<i>5</i>
1. fejezet- SARS-CoV-2 vírus, megjelenése és az ismert világ átrendeződése	6
1.1. <i>A világjárvány társadalmi hatása</i>	<i>6</i>
1.2. <i>A világjárvány gazdasági és politikai hatása.....</i>	<i>11</i>
1.3. <i>A világjárvány technológiai hatása</i>	<i>15</i>
1.4. <i>Következtetés.....</i>	<i>17</i>
2. fejezet- A távoli munkavégzés szabályozásának és az interneten való megjelenésnek vizsgálata.....	19
2.1. <i>Távoli munkavégzés hazai szabályozása és annak változása.....</i>	<i>19</i>
2.2. <i>Távoli munkavégzés nemzetközi szabályozása</i>	<i>22</i>
2.2.1. <i>Európai Unió szabályozása</i>	<i>24</i>
2.2.2. <i>Európai szabályozás kiberbiztonsági aspektusa</i>	<i>26</i>
2.2.3. <i>Egyesült Államok szabályozása</i>	<i>26</i>
2.2.4. <i>Amerikai szabályozás kiberbiztonsági aspektusa.....</i>	<i>28</i>
2.2.5. <i>Finnország törvényi szabályozása</i>	<i>29</i>
2.2.6. <i>A finn szabályozás kiberbiztonsági aspektusa</i>	<i>30</i>
2.3. <i>A „Home office” kifejezés megjelenése az interneten.....</i>	<i>31</i>
2.4. <i>Következtetés.....</i>	<i>35</i>
3. fejezet- Távoli munkavégzés információ- és kiberbiztonsági kihívásai.....	37
3.1. <i>Főbb támadási formák, amelyek népszerűek voltak a Covid-19 első hulláma idején</i>	<i>37</i>
3.2. <i>Kockázatkezelés</i>	<i>45</i>
3.3. <i>Lehetséges kockázat csökkentő lépések bemutatása</i>	<i>50</i>
3.4. <i>Következtetés.....</i>	<i>58</i>
4. fejezet- Kérdőív.....	59
4.1. <i>Kérdőív bemutatása, észrevételek leírása</i>	<i>59</i>
4.2. <i>Fenyegetettségek, és a távmunka</i>	<i>62</i>
4.3. <i>Következtetés.....</i>	<i>66</i>
Összegzés	67
<i>Eredmények.....</i>	<i>68</i>
Felhasznált irodalom	68

Mellékletek.....	72
1. számú melléklet (ábra jegyzék).....	72
2. számú melléklet (táblázat jegyzék)	73
3. számú melléklet (Kérdőív)	74
4. számú melléklet (Kérdőív kielemezése)	79
5. számú melléklet (Rövidítések jegyzéke)	82
Függelékek	84
Annotáció	84

BEVEZETÉS¹

A téma aktualitása

2019 végén Kínában megjelent, 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 köznyelven koronavírusként ismert SARS-CoV-2- vírus terjedését próbálták, illetve és 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 kellett átállni távoli munkavégzésre. Ebben a legnagyobb problémát, az idő rövidsége jelentette, ami alatt az egyes vállalatoknak biztosítaniuk kellett a távoli munkavégzéssel üzletmenet folytonosságukat. Az ipari korszak kezdete óta Európa munkarendje nagyrészt olyan munkanapokból állt, amely 9 órákor kezdődött, 5 órákor ért véget és két hektikus ingázásból áll. A COVID-19 teljesen megváltoztatta ezt a hagyományt. A Microsoft, Boston Consulting Group és a KRC Research készített egy nemzetközi tanulmányt², amiben több ezer munkavállalót és vezetőt kérdeztek meg Európa-szerte, a távmunkával kapcsolatos tapasztalataikról, valamint a jövőre vonatkozó elvárásaikról. A jelentés egyik legvilágosabb megállapítása az a felszabadulás, amelyet az emberek éreznek, hogy mentesek az irodai szabályok alól. Szeretnek kényelmesen öltözködni, személyre szabni a munkaterületüket, és azt akarják, hogy házikedvencük mellettük üljön, amikor dolgoznak. A vezetők a belátható jövőben másfajta munkamódszert várnak el. Tavaly a vállalatoknak csak kis hányada (15%) rendelkezett távmunka szabályzattal. Ez a szám ma már sokkal nagyobb (76%). A vezető tisztségviselők látták, hogy a távolimunkavégzési formában dolgozó csapatok rendkívül produktívak lehetnek, 82%-uk szerint a termelékenység szintje vagy stabil, vagy növekszik, amikor az emberek távmunkára váltanak, míg az üzletmenet folytonossága és a termelékenység nagyjából változatlan maradt. Az üzleti vezetők az alapvető termékek és szolgáltatások körüli innováció csökkenéséről számolnak be. Ez azért lehet mert a dolgozók távolabb tartják magukat a vállalati kultúrától, kevésbé szorosan kötődnek a csapatokhoz és kevésbé együttműködők.

¹ A dolgozatot az Innovációs és Technológiai Minisztérium ÚNKP-20-2-II-NKE-84 kódszámú Új Nemzeti Kiválóság Programjának szakami támogatásával készült.

² Microsoft reporter, „Flexible Ways of Working Are Here to Stay, Finds New European Research – with Leaders Focused on Maintaining Culture and Innovation”, Microsoft News Centre Europe, 2020. október 15., Letöltés dátuma: 2020. október 17., <https://news.microsoft.com/europe/features/flexible-ways-of-working-are-here-to-stay-finds-new-european-research-with-leaders-focused-on-maintaining-culture-and-innovation/>.

Amikor az emberek fizikailag együtt vannak a hét öt napján, könnyű összekapcsolódni - legyen szó akár viccmegosztásáról, akár alkalmi csapatebédről. Mindezek a látszólag apróságok összeadódnak, és nagy hatással vannak az üzleti életre és a csapatkultúrára.

A tudományos probléma

Jelen kutatásban arra szeretnék rávilágítani, hogy milyen nehézséget jelentett hazánkban és világon ez a tömeges átállás a távoli munkavégzésre. A hangsúly ez esetben a tömegesen van, mivel hazánkban 2020 előtt nem volt annyira elterjedt ezen munkavégzési forma. A tömeges és gyors átállás számos problémát okozott a szervezeteknek, amely probléma kiberbiztonsági kockázatokkal is járhat. Ilyen probléma volt például, hogy a munkavállalóknak nem biztos, hogy tudtak elegendő eszközt biztosítani a távmunkához, így saját eszközüket kellett használni. Ilyen probléma lehet továbbá a fizikai biztonság alapvető biztosítása is, mivel munkavállalónként eltérő azok a megoldások, amelyekkel a munkához szükséges eszközök fizikai biztonságát biztosítják (például: valamelyik munkavállaló rendelkezik riasztóval, kamera rendszerrel és külön zárható szekrénnel a vállalati eszközei számára, más munkavállaló pedig nem rendelkezik ilyen eszközökkel).

Módszertan

Szakirodalom feldolgozással megvizsgáltam, hogy milyen fenyegetések jelentek meg a koronavírus idején, továbbá keresek jó gyakorlatokat, illetve nemzetközi sztemderdeket ezen fenyegetések kockázatainak csökkentésére. Jogszabály elemzéssel megvizsgáltam a hazai, nemzetközi és más nemzetek szabályozását távmunka kapcsán. Szentiment analízist végeztem, melyben megvizsgáltam, hogy az interneten a távmunkával kapcsolatos szavak hol és milyen formában jelennek meg. Kérdőíves felmérést végeztem hazai kiberbiztonsági szektorban dolgozó személyek körében, amelynek egy részét osztályozó kiértékeléssel értékelem, másik részét pedig Kruskal-Wallis-próba alá vetem.

Kutatási hipotézisek

A kutatási téma feldolgozása során az alábbi hipotéziseket fogalmaztam meg:

H1: Feltételezem, hogy a távmunkával kapcsolatos hazai normatív szabályozás nem reflektál a kiberbiztonsági kihívásokra.

H2: Feltételezem, hogy a vírus hatására új fajta fenyegetések nem jelentek meg, azonban a meglévők számában növekedés mutatható ki, és megjelenésük szofisztikáltabb, mint eddig.

H3: Home office kifejezés megjelenése az interneten a második hullám idején is legalább akkora mértékű, mint az első hullám alatt.

H4: Azon országokban, ahol a távolimunkavégzés aránya magasabb, részletesebb a normatív szabályozás a témában.

H5: Feltételezem, hogy azon szakértők, akik szerint a szervezetükben dolgozók sűrűbben szegik meg a szabályokat kockázatosabbnak tartják a távmunkát, mint munkavégzési formát.

Kutatási célkitűzések

A fentiek okán kutatásom célkitűzése volt kivizsgálni a távolimunkavégzés megjelenését és tömeges elterjedését a vírus kirobbanását követően. Feltárom azon kockázatokat, amelyek a távoli munkavégzés során a különböző szervezeteket fenyegetik. Megvizsgáltam azon lehetőségeket, amelyekkel a kutatásom által feltárt és rendszerezett fenyegetéseket csökkenteni, illetve megszüntetni lehet. Megvizsgáltam a hazai és nemzetközi normatív szabályozást a távmunkát illetően. Külön vizsgáltam azon országokat, ahol a távoli munkavégzés aránya kimagasló. Kivizsgáltam, hogy ebben az évben miként jelent meg a távmunka kifejezése az interneten, többek között olyan tulajdonságokat vizsgálva, mint mely platformokon jelent meg a kifejezések, szentiment analízissel vizsgáltam, hogy miként beszéltek ezekről az emberek. Kérdőíves kutatási módszertannal megvizsgálom azt, hogy hazánkban, mind a köz és mind a magánszektorban miként ment végbe a távoli munkavégzésre való tömeges átállás a vírus megjelenésének idején.

1. FEJEZET- SARS-COV-2 VÍRUS, MEGJELENÉSE ÉS AZ ISMERT VILÁG ÁTRENDÉZŐDÉSE

1.1. A világjárvány társadalmi hatása

A járvány társadalmi hatásában vannak azonos tényezők világszerte, mint például az idős és beteg emberek külön védelme. Jelenlegi tapasztalatok szerint a pandémiára a legmegfelelőbb kormányzati válasz a szélesebb körű társadalmi távolságtartás elrendelése, és ezáltal a vírus terjedésének lelassítása, amely elegendő időt biztosít az egészségügyi szolgálatok számára kapacitásuk növeléséhez, valamint a laboratóriumok számára hatékony oltások kifejlesztéséhez.³ A kormányzati válasz szigorúsága csak egy változó, amely befolyásolja a vírus terjedését, míg a lakosság reakciója az intézkedésekre egy másik igen jelentős része ennek. Mind az intézkedések és mind a válasz reakciók országonként eltérők voltak. Ebben az eltérésben számos tényező játszott szerepet, ezek részletes értékelését Kapitány-Fövény és Sulyok szerzőpáros kutatásának eredményét⁴ ábrázoltam 1-4. számú táblázatban. Fontosnak tartom megjegyezni, hogy jelen elemzés 2020 január 23. és március 27. időintervallumot foglal magában. Tehát főleg világjárvány megjelenése és terjedése jelenik meg, és ezekre adott akkori válaszügy, amelyek lehetnek egyes országokban már eltérőek mostanra. Azonban kutatásom középpontjában a távoli munkavégzés tömeges elterjedése áll, amely 2020 tavaszára vált világméretű tendenciává, ezért megfelelő számomra a kutatásban használt idő intervallum.

1. táblázat A társadalmi klaszterek kialakításának szempont rendszere- Leíró célok az országszintű klaszterprofilok részletezéséhez- Saját szerkesztés, Forrás: Kapitány-Fövény, M., Sulyok, M.

Leíró célok az országszintű klaszterprofilok részletezéséhez	
Vizsgált változó neve	A változó leírása
Kormányzati szigorúsági index	A következő mutatókon alapul: iskolák és munkahelyek bezárása, nyilvános rendezvények lemondása, tömegközlekedés korlátozása, nyilvános információs kampányok, a belső mozgás korlátozása, nemzetközi utazási ellenőrzések, fiskális és monetáris intézkedések, beruházások az egészségügybe és az oltásokba.
Tesztek millió emberre	Az elvégzett tesztek összesített száma, vagyis a tesztelt emberek száma millió emberre vetítve.

³ Roy Anderson és mtsai., „Comment How will country-based mitigation measures influence the course of the COVID-19 epidemic?”, *The Lancet* 395 (2020. március 6.), [https://doi.org/10.1016/S0140-6736\(20\)30567-5](https://doi.org/10.1016/S0140-6736(20)30567-5).

⁴ Máté Kapitány-Fövény és Mihály Sulyok, „Social Markers of a Pandemic: Modeling the Association between Cultural Norms and COVID-19 Spread Data”, *Humanities and Social Sciences Communications* 7, sz. 1 (2020. szeptember 16.): 1–9, <https://doi.org/10.1057/s41599-020-00590-z>.

Leíró célok az országszintű klaszterprofilok részletezéséhez	
Vizsgált változó neve	A változó leírása
V74 — Schwartz értékelem	Ez a változó méri annak érzékelt fontosságát, hogy valamit tegyünk a társadalom érdekében (társadalmi hasznosság).
V77 — Schwartz értékelem	Ez a változó a megfelelő viselkedés érzékelt fontosságát méri (megfelelőség).
V115 - Bizalom elem	Ez a változó azt méri, hogy az állampolgárok mennyire bíznak a kormányban (bizalom).
V138 - A demokrácia, mint elem alapvető jellemzői	Ez a változó azt méri, hogy az állampolgárok mennyire tekintik vezetőinek való engedelmséget a demokrácia alapvető jellemzőjének (megfelelés).

2. táblázat A társadalmi klaszterek kialakításának szempont rendszere- Klaszterezés és prediktív célok leírása- Saját szerkesztés, Forrás: Kapitány-Fővény, M., Sulyok, M.

Klaszterezés és prediktív célok: ezek a változók képezik az országszintű klaszterek alapját, és előre jelzik a COVID-19 megduplázódási idejét	
Vizsgált változó neve	A változó leírása
A kormány hatékonysága (a kormányzás része)	A kormány hatékonysága meghatározza a közegészségügyi ellátás minőségét, a tisztviselők kompetenciáját és a bürokrácia minőségét (mutatói például A politikai koordináció, a kormányzat minősége és hitelessége, a kormányzati kiadások hatékonysága stb.).
Ügynökség (a személyes szabadság része)	Az ügynökség meghatározza, hogy az állampolgárok milyen mértékben mentesek a korlátozásoktól és mennyire mozoghatnak szabadon, jelezve az önálló cselekvés szabadságának és a szabad döntések tapasztalatait (mutatói például a személyes autonómia és az egyéni jogok, a mozgás szabadság, a szabadsággal való elégedettség stb.).
Gyülekezési és egyesülési szabadság (a személyes szabadság része)	A gyülekezés és az egyesülés szabadsága meghatározza, hogy az állampolgárok mennyire szabadon gyülekezhetnek másokkal a nyilvános tereken.
Közösségi hálózat (a társadalmi tőke része)	A közösségi hálózat meghatározza az egyén és a tágabb társadalmi hálózat közötti kapcsolatok erősségét és lehetőségeit, ideértve a társadalmi támogatást is (mutatói például tisztelet, barátkozási lehetőség vagy mások segítése).
Személyes és családi kapcsolatok (a társadalmi tőke része)	A személyes és családi kapcsolatok meghatározzák a legszorosabb személyes kapcsolatok és családi kapcsolatok erősségét, formálva az egyén érzelmi, szellemi és pénzügyi támogatását (mutatói például család és barátok megsegítése baj esetén, vagy a család által nyújtott pozitív energia).
Polgári és társadalmi részvétel (a társadalmi tőke része)	Az állampolgári és társadalmi részvétel határozza meg azt az eredményt, amely azt mutatja, hogy az állampolgárok

	miként vesznek részt a társadalomban, felosztva a polgári és a társadalmi szférára (mutatói például jótékonyági célokra felajánlott pénz, önkéntesség, közhivatalnokoknak adott vélemény stb.).
Megelőző beavatkozások (az egészség része)	A megelőző beavatkozások meghatározzák, hogy az egészségügyi rendszer milyen mértékben akadályozza meg a betegségek és más orvosi szövődmények előfordulását (mutatói például a nemzeti szűrési programok megléte, vagy a diphtheria, kanyaró, hepatitis immunizálás stb.).

3. táblázat A társadalmi klaszterek kialakításának szempont rendszere- Éghajlat mint befolyásoló tényező
- Saját szerkesztés, Forrás: Kapitány-Fővény, M., Sulyok, M.

Éghajlat, mint befolyásoló tényező: Ez a változó segítségével szolgált a COVID-19 megduplázódási idejének előrejelzésében	
Vizsgált változó neve	A változó leírása
A osztály - trópusi éghajlat	Az egyik legmelegebb, földrajzi régiókat foglalja magában trópusi monszunokkal, esőerdőkkel vagy szavannákkal. Állandóan magas hőmérséklet, aminek az egész éves átlaga 18 ° C (64,4 ° F) vagy magasabb.
B osztály - száraz és fél száraz éghajlat	A B osztályú éghajlati zónába tartoznak a forró vagy hideg sivatagokkal vagy fél száraz éghajlattal rendelkező régiók, amelyekre a leeső csapadékot meghaladó párolgás a jellemző. Az alacsony szélességi fokú éghajlat átlagos éves hőmérséklete 18 ° C (64,4 ° F) felett van, míg középső szélességű éghajlat esetén az átlagos éves hőmérséklet 18 ° C (64,4 ° F) alatt van.
C osztály - mérsékelt (mezotermikus) éghajlat	A C osztályú éghajlati zónába szubtrópusi, mediterrán és óceáni éghajlatú régiók tartoznak. A tavaszi / nyári hónapokban a havi átlaghőmérséklet átlagosan 10 ° C (50 ° F) vagy annál magasabb, míg az őszi / téli hónapokban az átlagos havi hőmérséklet meghaladja a -3 ° C (27 ° F) fokot.
D osztály - kontinentális (mikrotermikus) éghajlat	A D osztályú éghajlati zónába kontinentális és szubarktikus éghajlatú régiók tartoznak. A legmelegebb hónapokban az átlagos hőmérséklet 10 ° C (50 ° F) fölött figyelhető meg, míg a leghidegebb hónapokban a havi átlag -3 ° C (27 ° F) alatt van.

4. táblázat A társadalmi klaszterek kialakításának szempont rendszere- Az országok társadalmi és gazdasági helyzete - Saját szerkesztés, Forrás: Kapitány-Fővény, M., Sulyok, M.

Az országok társadalmi és gazdasági helyzete: Ezek a változók képezik az országszintű klaszterek alapját, és megjósolják a COVID-19 megduplázódási idejét.	
Vizsgált változó neve	A változó leírása
Az egészségügyi ellátás hozzáférése és minőségének (HAQ) indexe 2015	A HAQ index - egy összefoglaló mutató a 0–100 skálán - az olyan országos halálozási arányokon alapul, amelyek olyan okokból származnak, amik nem lehetnek halálosak hatékony orvosi ellátás jelenlétében.
Egy főre jutó GDP	Az egy főre eső GDP a bruttó hazai termék osztva az év közepi népességgel.
Az utazás és az idegenforgalom közvetlen hozzájárulása a GDP-hez 2018-ban	Ez az index azt jelzi, hogy az utazási és turisztikai ipar milyen mértékben járult hozzá közvetlenül a bruttó hazai nyereséghez.
Népesség és népsűrűség	A népesség nagyságának és a területegységre jutó népesség országos mutatói.

4 Fő klaszter került kialakításra, értékelve a fenti változókat világszerte. Ezek a klaszterek a következők:

- 1. klaszter - fenntartott társadalmak: Az 1. klaszter jellemzően magas népességű országokból állt, alacsonyabb népsűrűséggel, alacsony kormányzati hatékonysággal, továbbá alacsonyabb egy főre jutó GDP-vel és HAQ indexel. Az egymillió lakosra elvégzett tesztek viszonylag alacsonyak voltak ebben a klaszterben, a kormány szigorúsági mutatója magasabb volt, mint a 3. klaszterben, de alacsonyabb, mint a 2. és 4. klaszterben. Jellemzően alacsony mértékű volt az ügynöki tevékenység és a gyülekezési és egyesülési szabadság mértéke, valamint a családi és személyes kapcsolatok mértékei is alacsony volt. Ezek a jellemzően száraz, és fél száraz éghajlati országok. A klaszter országai például Irán, Pakisztán, Egyiptom, Algéria, Kazahsztán és Mexikó voltak. Úgy tűnik, hogy ezekre a társadalmakra a társadalmi távolságtartás és a személyes autonómia vagy a mozgás szabadságának viszonylag alacsony igénye jellemző. Ezeknek a társadalmaknak a polgárai kevésbé érdeklődtek az iránt, hogy valamit tegyenek a társadalom érdekében, és kevésbé tartották fontosnak a megfelelő viselkedést. Másrészt nagyobb bizalommal voltak kormányaik iránt, mint a 2. és 3. klaszter országainak állampolgárai, valamint úgy vélték, hogy a vezetőknek való engedelmesség a demokrácia fontos jellemzője.

- 2. klaszter - sodródó társadalmak: A 2. klaszter országaiban (pl. Csehország, Görögország, Olaszország, Magyarország, Szlovénia, Szlovákia, Peru, Észtország, Lengyelország) jellemzően mérsékelt éghajlat, alacsony népesség szám és népsűrűség a jellemző ezekre az országokra, továbbá magasabb kormányzati hatékonyság, mérsékelt gyülekezési és egyesülési szabadság is jellemző ezekre az államokra. A családi és személyes kapcsolatok szintje alacsonyabb, ahogy alacsonyabb társadalmi részvétel is, alacsonyabb GDP és HAQ index is. Az egymillió lakosra elvégzett tesztek alacsonyabbak voltak, mint a 3. és 4. klaszterben, de magasabbak, mint az 1. klaszterben. A kormány szigorúsági mutatója magas volt. Ezeket a társadalmakat a határozott vezetés, a társadalmi felelősség megtagadására való hajlam és a szoros kapcsolatok előnyben részesítése jellemző. Ezeknek az országoknak a polgárai nem tartották igazán fontosnak, hogy tegyenek valamit a társadalom érdekében, vagy hogy megfelelően viselkedjenek, miközben csökkent bizalmukat mutatták kormányuk iránt.
- 3. klaszter - Asszertív társadalmak: A 3. klaszter országai Ausztrália, USA, Egyesült Királyság, Németország, Svédország, Spanyolország, Svájc és Franciaország. Ezen államok mérsékelt éghajlattal, magasabb kormányzati hatékonysággal, erősebb társadalmi hálózatokkal, jelentősebb személyes és családi kapcsolatokkal, illetve jelentősebb gyülekezési és egyesülési szabadsággal rendelkeznek. Emellett magasabb az egy főre jutó GDP, és magas HAQ index is ezen államok esetében. Az egymillió lakosra elvégzett tesztek száma magasak voltak, a kormány szigorúsági mutatója az összes klaszter közül a legalacsonyabb volt. Ezeket a társadalmakat a személyes autonómia és függetlenség, a társadalmi részvétel és a kiterjedt hálózatépítés iránti erős igény jellemzi. Ezen államokban fontos az egyéneknek, hogy tegyenek valamit a társadalom érdekében, és megfelelően viselkedjenek.
- 4. klaszter - Megfelelő társadalmak: A 4. klaszter országaiban jellemzően száraz az éghajlat, magas a népsűrűség és alacsonyabb pontszámokkal rendelkeznek a közösségi hálózatok, személyes és családi kapcsolatok terén, továbbá alacsonyabb a gyülekezési és egyesülési szabadság is. A HAQ pontszám és az egy főre eső GDP itt magasabb volt, de nem volt olyan magas, mint a 3. klaszterben. Az egymillió lakosra elvégzett tesztek aránya itt volt a legmagasabb az összes klaszter között. E klaszter országai például Dél-Korea, Kína, Egyesült

Arab Emírségek, Izrael, Szingapúr voltak. Ehhez a csoporthoz a legmagasabb duplázási idő társult (ezt követte az 1. klaszter). Ezek a társadalmak nem kezelhetik központi elemként a személyes autonómia, a cselekvés vagy a gyülekezés szabadságának fontosságát. Itt fontosabb, hogy ezek az állampolgárok tegyenek valamit a társadalom érdekében, és megfelelően viselkedjenek, mint az 1. és 2. klaszter országai esetében. A 4. klaszter országai mutatták a legmagasabb meggyőződést abban, hogy kormányaik uralják a helyzetet. Az alapvető különbség a 4. és 1. klaszter társadalma között az, hogy a 4. klaszter országainak lakói nemcsak a kormányaikkal, hanem más egyénekekkel szemben is nagyobb összhangot mutatnak.⁵

Mind ezen eredmények azt mutatják, hogy vannak egyes tényezők, amelyek szerint be lehet az egyes társadalmakat sorolni, a járványhoz és annak következményeihez való hozzáállásuk szerint.

1.2. A világjárvány gazdasági és politikai hatása

A járványból való gazdasági felépülésének a sebességét és jellegét mind a kínálati, mind keresleti tényezők befolyásolják. A kínálati oldalon sok gyártó a nemzetközi ellátási lánctól függ. Azok a nemzetek, amelyek készek voltak folytatni az első hullám után az árucikkek gyártását (de termelésük során a nemzetközi ellátási láncokra támaszkodnak), azt tapasztalhatják, hogy korlátozottan tudták elkezdni a termelést, mert nemzetközi beszállítóik a folyamatos bezárások miatt vagy a csökkentett árumennyiségek miatt nem tudják kielégíteni igényeiket. A nemzetközi szállítási szolgáltatások korlátozása lehet akadálya a szállítási lánc működésének is, például a légi szolgáltatások megszakadása. A közelmúltban Kína nagyfokú függőséget mutatott az áruk gyártása során felhasznált importált alapanyagok irány,⁶ ezért meglehetősen ki volt téve a kínálati oldali zavaroknak. Ez az exporttól való nagy függőségével együtt komoly gazdasági kihívásokat jelentett a kínai kormány számára a COVID-19-re adott válasza, ami a kijárási tilalom volt, nem beszélve a Trump Kínával folytatott „kereskedelmi háborúja” által létrehozott problémákról.⁷

⁵ i.m.Kapitány-Fővény és Sulyok.

⁶ Clement Tisdell, „Economic and Business Relations Between China and Australia: Insights Into China’s Global Economic Footprint” (Brisbane: Australian Academic, 2007), 11–24.

⁷ Clem Tisdell, „Economic Reform and Openness in China: China’s Development Policies in the Last 30 Years”, *Economic Analysis and Policy* 39, sz. 2 (2009. szeptember 1.): 271–94, [https://doi.org/10.1016/S0313-5926\(09\)50021-5](https://doi.org/10.1016/S0313-5926(09)50021-5).

Valószínűleg csak lassan áll helyre a kereslet azoknak az iparágaknak az árucikkei iránt, amelyek korlátlan árucikkeket értékesítenek, és amelyekért vásárlóik fokozott kockázatnak vannak kitéve a COVID-19 fertőzéssel kapcsolatban. Következésképpen egyes iparágak gazdasági fellendülését mindkét tényező korlátozni fogja, vagyis a diszkrecionális vásárlás csökkentése és kockázatkerülés az áruk vásárlásakor.

Sok nemzet protekcionista politikát kezdett el alkalmazni a COVID-19 járvány által kiváltott gazdasági aktivitás és foglalkoztatás szintjének növelése érdekében. Ez késleltetheti a globális gazdasági fellendülést. Hátrányos helyzetbe hozza azokat az országokat (például Ausztráliát és Németországot), amelyek gazdasági tevékenységük és foglalkoztatásuk szintjének megteremtésében nagymértékben függenek az exporttól.⁸

Ahogy Weder di Mauro nemzetközi közgazdász professzor fogalmazta: *"A gazdasági kár nagysága és tartóssága attól függ, hogy a kormányok hogyan kezelik ezt a hirtelen szoros találkozást a természettel és a félelemmel."*

Az egyes államok gazdaságának helyreállítását, illetve magának annak a tényét, hogy mekkora kár éri a gazdaságot, számos tényező befolyásolja, mint például egy gazdaság mérete, illetve annak nyitottsága.

Az egyes paraméterek jelentése:

- Egy adott ország gazdaságának mérete azt mutatja meg, hogy gazdasági helyzete, illetve gazdasági döntései mennyire befolyásolják számottevően a nemzetközi helyzetet.
- Egy adott ország gazdasági nyitottsága azt mutatja, meg hogy mennyire része a globális piacnak ezen állam. Egy zárt gazdaságban az import és export aránya a GDP-ben nem nagy mértékű, míg egy nyitott gazdaságban eléggé számottevő ez az arány.

Hazánk például egy kis nyitott gazdaság, ami tehát azt jelenti, hogy a nemzetközi gazdasági helyzetre nem vagyunk nagy hatással, viszont az import és export aránya a GDP-ben jelentős, így a nemzetközi gazdaság alakulása nagyban befolyásolja hazánk gazdaságát is. Tehát hazánk gazdasági helyzete akkor fog javulni, ha ez nemzetközi szinten elkezdődik.

A Weder di Mauro nemzetközi közgazdász kifejti, hogy a két forgatókönyv elképzelhető a járvány miatt. Az elsőben globális dimenziójú gazdasági válság és a globalizáció hosszú távú megállása és esetleges visszafordulása várhat minket. Míg a másik oldalon, a politikai

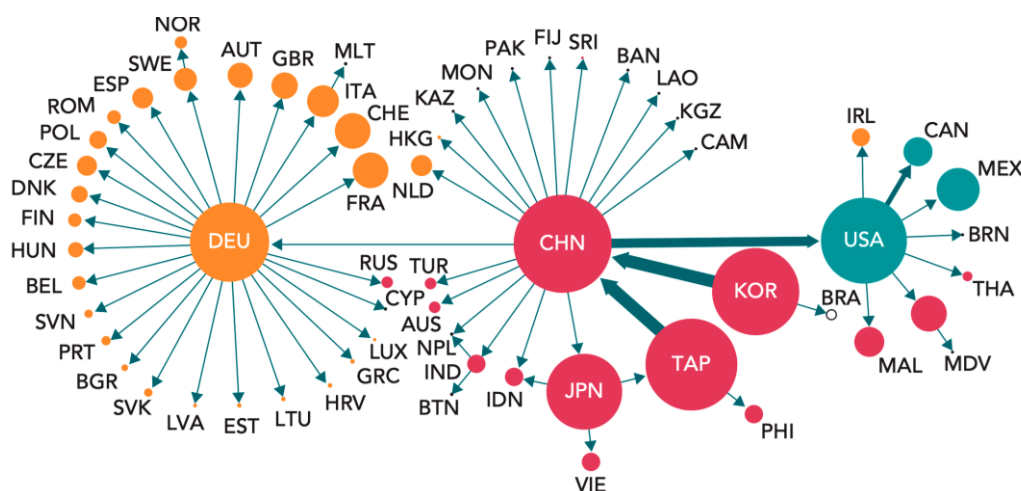
⁸ Clement A. Tisdell, „Economic, Social and Political Issues Raised by the COVID-19 Pandemic”, *Economic Analysis and Policy* 68 (2020. 0 1.): 17–28, <https://doi.org/10.1016/j.eap.2020.08.002>.

döntéshozók közös válságkezelésbe kezdenek a így globalizációt fenntartva. Sőt sikerül helyreállítaniuk a bizalmat, és olyan együttműködési szellemet hozhatnak létre, amely segíti az emberiséget más közös problémák kezelésében, mint a klímaváltozás.⁹

Mit tehetnek a kormányok a gazdasági fájdalom csökkentése érdekében?

A kedvezőtlen forgatókönyvek esetén makroszinten erőteljes szakpolitikai válaszra lesz szükség a károk visszaszorítására.

- Mind monetáris, mind fiskális politikai fellépésre is szükség lesz, és egyértelműen a leghatékonyabb fellépés egy nemzetközileg összehangolt fellépés lenne. A főbb központi bankok közös megközelítései és bejelentései nagyobb hatékonyságot mutatnának, mint a külön álló sürgősségi intézkedések.



1. ábra Csomópontok a világ információs és kommunikációs technológiai áruk ellátási láncában (Forrás: Világ Bank)

A nemzetközi fellépés fontosságát az 1. ábra is mutatja, ami az információs és kommunikációs technológiai (továbbiakban IKT) áruk ellátási láncát írja le. Az ábrán a buborék nagysága tükrözi az ország méretét (ez az ország kereskedelmi értéke), az összekötő vonalak vastagsága pedig az áramlások relatív jelentőségét mutatja. Ebből azt lehet látni, hogy az ellátási láncok összefonódnak az egész világon keresztül, és láthatjuk, hogy Kína milyen központi szerepet tölt be ebben a szektorban, már érthető is, hogy amikor itt év elején megállt az élet, miért volt az IKT szektorban hiány.

⁹ „INTERPOL Report Shows Alarming Rate of Cyberattacks during COVID-19”, Letöltés dátuma 2020. szeptember 19., 15-29, <https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>.

- A sokk jellegét figyelembe véve a kis- és középvállalkozások lehetnek a leginkább kitettek a likviditási problémáknak, ezért megfelelő lehetőségnek mutatkoznak a kisvállalkozásoknak nyújtott hitelek. Kína, Hong Kong és Szingapúr jelentős pénzügyi intézkedésekről döntött a kereslet élénkítése és a bizalom növelése érdekében (Szingapúr esetében ez a GDP majdnem 2% -a).
- A karantén és a jövedelemhiány által sújtott emberek számára célzott segítségként gyorsan alkalmazhatók a fiskális intézkedések - amint ezt Olaszországban már megtették. Cochrane katasztrofális víziójában drasztikusabb fellépésre lenne szükség, ahol pénzügyi válságtervet javasol, hogy „pénzzel áraszák el az országot a megfelelő helyeken”, megfontoltan célzott mentőeszközökkel, amelyek segítenek megakadályozni a vállalkozások és az emberek csődjét.

Következőkben olyan szakpolitikai intézkedések bemutatása következik, amelyeket az elsőhullám idején főleg az elején hoztak ezért dominál főleg Ázsia és Olaszország a lépésekben.

célzott intézkedések az egészségügy bizalom építésének irányába:

- bónusz az egészségügyi dolgozók számára (Szingapúr);
- a politikai vezetés szolidaritásból felajánlotta egyhavi fizetését (Szingapúr);
- biztosítson kis mennyiségű arcmaszkot az összes háztartás számára (Szingapúr).

célzott fiskális intézkedések a háztartások irányába:

- Készpénz kifizetése minden 18 éven felüli polgárnak, 1000 USD felett (Hong Kong);
- A villamos energetikai számlák kifizetéseinek felfüggesztése az érintett területeken (Olaszország);
- A szövetségi kormány fizeti az összes vizsgálati és orvosi számlát, beleértve az intenzív osztályokban történő drága tartózkodást is azoknak az amerikaiaknak, akiknek nincs egészségbiztosításuk (USA).

célzott intézkedések vállalatok irányába:

- Támogatott rövid távú foglalkoztatási rendszerek (Németország);
- Ágazatspecifikus pénzügyi támogatás az idegenforgalom, szálloda ipar és légitársaságok számára (Szingapúr);

- Széles körű pénzügyi segítség a vállalkozások számára, beleértve a munkavállalók távolléteinek fokozott támogatását (Szingapúr);
- A nyereségadó csökkentése és az alacsony kamatozású hitelek biztosítása a kis- és középvállalkozások számára (Hong Kong).

célzott intézkedések a Monetáris / banki tevékenység irányában:

- Célzott banki likviditási finanszírozás, amely a kicsi bankok hitelezéséhez kötött (EKB, TLTRO-k);
- Likviditási támogatás a bankoknak.

Átfogó, a G20 / EU szintjén összehangolt fiskális ösztönző csomag

- Sürgősségi adócsökkentések;
- A társadalombiztosítási kifizetések felfüggesztése;
- Enyhítés az EU-ban érintett országok költségvetési kritériumain.

globális / regionális katasztrófavédelem / sürgősségi finanszírozás:

- 50 milliárd USD sürgősségi hitelezés (IMF);
- Az International Finance Corporation (IFC), European Bank for Reconstruction and Development (EBRD) a vírus által érintett országok magánszektorának finanszírozására;
- Az EU Szolidaritási Alapjának kiterjesztése az egészséggel kapcsolatos katasztrófák bevonására.¹⁰

1.3. A világjárvány technológiai hatása

Az egyre növekvő válság miatt a vállalatok és kutatók a világ minden táján keresik a vírus okozta kihívások kezelésének módjait, a betegség terjedésének enyhítését és a gyógy mód fejlesztését. Ebben a csatában a tudomány és a technológia létfontosságú szerepet játszik. Például a járvány korai szakaszában, amikor Kína intézkedéseket vezetett be a vírus ellen a mesterséges intelligenciára (továbbiakban AI) összpontosított. Felhasználata az arcfelismerő

¹⁰ Richard Baldwin és Beatrice Weder di Mauro, *Economics in the Time of COVID-19: A New EBook* (CEPR, 2020), <https://voxeu.org/article/economics-time-covid-19-new-ebook>.

kamerákat az utazási előzmények felkutatására a fertőzött betegek nyomon követése során, az élelmiszerek és gyógyszerek szállítására szolgáló robotokat vetett be, továbbá a nyilvános helyek fertőtlenítésére szolgáló drónokat kezdett használni.¹¹ Az AI-t széles körben alkalmazzák új molekulák felfedezéséhez a COVID-19 elleni formula megtalálásában. Számos kutató használja az AI-t új gyógyszerek megtalálására a gyógyítás mellett, az orvosok a fertőző betegek észlelésére is összpontosítanak orvosi képfeldolgozással, például röntgennel és CT-vel.¹² Ezentúl olyan nyomkövető szoftvereket és hardvereket is fejlesztenek, mint a megfigyelő karkötők vagy megfigyelő applikációk, amelyek segítenek a karantén szabályt sértő emberek felderítésében. Okostelefonokat és mesterséges intelligenciával továbbfejlesztett hőkamerákat is használnak a láz és a fertőzött emberek felderítésére.¹³ Hazánkban is megtalálható egy okostelefonra letölthető alkalmazás, amely a VírusRadar nevet viseli. Ez az alkalmazás bluetooth kapcsolat segítségével vizsgálja, hogy mely más telefonok voltak a közelben az elmúlt 2 hétben. Így a fertőzött személy kontaktuskutatása igen fel tud gyorsulni, továbbá fel tudják keresni a kontaktokat, akik lehetséges vírus hordozóvá váltak. Azonban a technológiai fejlettséget nem csak a COVID 19 elleni küzdelemben használják, számos szolgáltató iránti kereslet megnőtt a vírus hatására. 2020 első negyedében nőtt az Apple bevétele olyan szolgáltatásból mint, például iCloud-tárolás, zenei előfizetések és AppleCare-garanciák. Hasonlóképpen, az Amazon Prime előfizetési bevétele is nőtt 28 %-al 2020 első negyedében a 2019 első negyedéhez viszonyítva, továbbá a Netflix 2020 első negyedében 15,77 millió új előfizető jelent meg a platformon a korábbi, 7,2 milliós előre jelzéshez képest.¹⁴¹⁵

Az Amazon Prime előfizetési bevétele 28% os növekedése a pandémia miatt bezárt kiskereskedelmi vállalkozásokból származó ügyfelek átvándorlásából adódott össze¹⁶. Az

¹¹ Ruiz Estrada és Mario Arturo, „The Uses of Drones in Case of Massive Epidemics Contagious Diseases Relief Humanitarian Aid: Wuhan-COVID-19 Crisis”, SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 2020. február 29.), <https://doi.org/10.2139/ssrn.3546547>.

¹² Thanh Nguyen, *Artificial Intelligence in the Battle against Coronavirus (COVID-19): A Survey and Future Research Directions*, 2020, <https://doi.org/10.13140/RG.2.2.36491.23846/1>.

¹³ Halgurd Maghdid és mtsai., „A Novel AI-enabled Framework to Diagnose Coronavirus COVID-19 using Smartphone Embedded Sensors: Design Study”, in *2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI)* (Las Vegas, NV, USA: IEEE, 2020), 180–87.

¹⁴ Shoshanna Delventhal, „Apple’s 5 Most Profitable Lines of Business”, Investopedia, 2020.március 10., Letöltés dátuma: 2020. szeptember 14., <https://www.investopedia.com/apple-s-5-most-profitable-lines-of-business-4684130>.

¹⁵ Ciara Linnane, „Netflix Stock Price Target Raised by Imperial on Expectations It Will Continue to Benefit during Pandemic”, MarketWatch, 2020.április 23, Letöltés dátuma: 2020. szeptember 10., <https://www.marketwatch.com/story/netflix-stock-price-target-raised-by-imperial-on-expectations-it-will-continue-to-benefit-during-pandemic-2020-04-23>.

¹⁶ Karen Ho, „Propelled by Covid-19, Amazon’s Prime Subscriptions Grow to \$5.6 Billion”, Quartz, 2020.március 10., Letöltés dátuma: 2020. szeptember 19., <https://qz.com/1849803/amazons-quarterly-subscription-sales-top-5-6-billion/>.

olyan platformok, mint a Facebook, a Google és a Twitter használata drámai módon megnőtt. Például 2020 áprilisában a Facebook üzenetküldő szolgáltatásainak a használata 50% -kal nőtt ebben videó küldés több mint 100% -kal emelkedett a vírus előtti szinthez képest.¹⁷ A videokonferencia-platformok használata a munka és társadalmi tevékenységek kibertérbe való átköltözése miatt az egekbe szökött, ami erős versenyhez vezetett az ágazatban. A Zoom videokonferencia népszerűsége kiváltotta a tech óriások, például a Facebook lépését. Áprilisban a Facebook bejelentette a csoportos videocsevegési funkciót, a Messenger Rooms-ot. Mondhatni, hogy a videokonferencia-platformok piaca felrobbant.¹⁸

Természetesen világszinten megnövekedett internet felhasználás a támadók figyelmét is felkeltették, ezáltal a támadások mennyisége is megnőtt a kibertérben. Kutatásom későbbi fejezetében bővebben foglalkozok a támadásokkal. Elemzem és kiértékelem, hogy a koronavírus során milyen támadások terjedtek el és ezek ellen milyen védekezési formák léteznek.

1.4.Következtetés

A világjárvány az élet összes területén kifejtette a hatását. Ebben a fejezetben megvizsgáltam a COVID 19 társadalmi, gazdasági, politikai és technológiai hatását. Ami először észrevehető volt, hogy ezek a kategóriák igen szorosan összefonódnak és hatással vannak egymásra. Ha csak a társadalmi aspektust vizsgáljuk, ott a felhasznált kutatás az egyes társadalmakat egy olyan szempont rendszer szerint osztályozta, aminek része volt a gazdasági mutatók és a politikai döntések elemzése is. Itt 4 különböző csoportot alkottak a világ számos országai, olyan szempontok szerint, mint például egy főre jutó GDP aránya vagy a kormányzati döntések szigorának mértéke, társadalom szabálykövetésre való hajlandósága.

A gazdasági és politikai aspektust azért egy fejezeten belül vizsgáltam, mivel meglátásom szerint ezek még nagyobb összefüggésben vannak, hiszen minden olyan szakpolitikai intézkedés, amely a vírus terjedését lassítja nagyban kihatással van a gazdaságra. Például a beutazási korlátozások, illetve a vendéglátóhelyek nyitvatartásának korlátozása csökkenti az esélyét annak, hogy emberek csoportosulni tudjanak, illetve külföldről fertőzött személy

¹⁷ Jon Swartz, „Facebook Has Weathered Many Storms, but the Latest Are Coming for Its Core”, MarketWatch, 2020.április 06., Letöltés dátuma: 2020. október 10., <https://www.marketwatch.com/story/facebook-in-the-age-of-covid-19-users-are-online-but-will-advertisers-pay-to-get-to-them-2020-04-06>.

¹⁸ Alison DeNisco Rayome, „Messenger Rooms: How to Use Facebook’s Free New Video Chat Feature Now”, CNET, 2020. május 19., Letöltés dátuma: 2020. szeptember 17., <https://www.cnet.com/how-to/messenger-rooms-heres-how-to-use-facebooks-free-new-video-chat-feature/>.

érkezzen. Azonban ezek a lépések a turizmust és vendéglátást rövidtávon megrengeneti hosszútávon ellehetetleníti azt. Ezenkívül a már kialakult helyzetre is lépni kell politikai szinten, különböző fiskális és monetáris lépésekkel. Itt összegyűjtöttem pár olyan lépést, amelyet az egyes országok vagy szervezetek hoztak meg a válság enyhítésére. Azonban, ki kell hangsúlyozni, hogy nem lehet egy univerzálisan mindenhol működő döntést kialakítani, mivel az egyes országok eltérő gazdasági tulajdonsággal rendelkeznek, amelyek nagyban befolyásolják egyes lépések hatását. Többek között azért próbáltam a világ különböző részeiről szakpolitikai lépéseket gyűjteni.

Technológiai értelemben látjuk azt, hogy a COVID 19 hatására jobban függünk az információs és informatikai rendszerektől, mint valaha. Láthattuk, hogy számos online szolgáltatás iránti kereslet mértéke megugrott, mind a hétköznapi életben (például Netflix vagy Zoom előfizetés), mind a járvány elleni intézkedésekben (például: gyógyszerek keresése, kontakt kutatás online lábnyomok alapján, távoli munkavégzés tömeges bevezetése).

2. FEJEZET- A TÁVOLI MUNKAVÉGZÉS SZABÁLYOZÁSÁNAK ÉS AZ INTERNETEN VALÓ MEGJELENÉSNEK VIZSGÁLATA

2.1. Távoli munkavégzés hazai szabályozása és annak változása

Magyarországon a távoli munkavégzésről a 2012. évi I. törvény a munka törvénykönyvéről tartalmaz szabályozást, amely a távmunkavégzés kifejezést használja. Pontosan a következő képpen definiálja: „*Távmunkavégzés a munkáltató telephelyétől elkülönült helyen rendszeresen folytatott olyan tevékenység, amelyet számítástechnikai eszközzel végeznek és eredményét elektronikusan továbbítják.*”¹⁹ Ha megvizsgáljuk a jogi szabályozást láthatjuk, hogy a távmunkavégzést és a home office-t nem használhatjuk szinonima ként. A különbség a rendszerességben van, mivel a home office-t a munkáltató csak ad hoc jelleggel engedélyezi, így ezt nem feltétlenül kell a munkaszerződésben megjelölni. Azonban mihamarabb a heti 1 napot, vagy csak kéthetente 1 napot a munkavállaló otthonról dolgozik, akkor már beszélhetünk távmunkáról, mert megjelenik a rendszeresség kritériuma.²⁰ Következő fontos pont, hogy számítástechnikai eszközzel végezzék, és elektronikusan lehessen az eredmény továbbítani. Ha ez nem teljesül akkor inkább bedolgozói munkaviszonyról beszélünk.

Távmunka vizsgált részei:

- Munkavégzés helye: jogszabály nem kötelezi kötelező elemként meghatározni a munkaszerződésben, de ezt a jogászok szokták javasolni. Fontos, hogy ennek el kell különülnie a munkáltató telephelyétől, azonban a munkáltatónak biztosítania kell, hogy a munkavállaló beléphessen a telephelyére.
- Munkaidő: alaphoz a törvény kötetlen munkarendet ír elő a távmunka során, amitől a felek elérhetnek és hagyományos úton megszabhatják az időbeosztást ebben az esetben ugyanakkor a munkáltatónak ellenőriznie kell majd a munkarend betartását.
- Eszközök: a munkáltató biztosítja a munkaeszközt, és előírhatja, hogy a munkavállaló azt csak munkára használhatja, de engedélyezheti a magán célból történő használatot is.
- Tájékoztatás: a munkáltató köteles az általános tájékoztatási kötelezettségén túlmenően tájékoztatni a munkavállalót az általa tartott ellenőrzés, a számítástechnikai vagy elektronikus eszközhasználat korlátozásának szabályairól.

¹⁹ „2012. évi I. törvény a munka törvénykönyvéről” (é. n.).

²⁰ Bihary Ákos és Pulay Flóra, „Home office vagy távmunka?”, Jogadó Blog, 2019. július 18., Letöltés dátuma: 2020.szeptember 01., <https://www.jogado.hu/home-office-vagy-tavmunka/>.

- Utasítás: a munkáltató csak a távmunka által ellátott feladatban utasíthatja a munkavállalót, ha a munkaszerződésben máshogy nem rendelkeznek.

2020 tavaszán hazánkban is megjelent a vírus, amely a megváltoztatta az akkori szabályozást. A kormány a 47/2020. (III. 18.) Korm. rendeltettel reagált a helyzetre, amely 2020. március 20-tól lehetővé tette a veszélyhelyzet időtartamára, és az azt követő 90 napra a munkáltató otthoni munkavégzést rendeljen el egyoldalúan. Ez kettő dologban könnyítette meg a mihamarabbi átállást. Első körben az eseti jelleget szüntették, ami azt jelenít, hogy folyamatosan tud a munkavállaló úgy otthonról munkát végezni, hogy csak vezetői utasítást kap rá, nem szükséges munkaszerződést módosítani. A másik változtatás, hogy a munkaidő beosztás a napi munkaidő kezdetét megelőzően kilencvenhat órán belül is módosítható a munkáltató részéről, ha olyan körülmény mutatkozik, amely a gazdálkodást vagy a működést befolyásolja, és előre nem volt látható.

Ez a rendelkezés már hatályát veszítette, de dolgoznak a Munka törvénykönyvének módosításán, amely nagyobb hangsúlyt fektet a távmunka szabályozására. Ebben fontos részt fog képezni az, hogy a távmunkavégzésre mind a két fél szándékozik átállni, ha csak az egyik fél mutat ár hajlandóságot, akkor a törvényjavaslat nem engedélyezné. Ezenfelül a másik fontos kérdésre próbál választ adni a javaslat, hogy ki viselje az otthoni munkavégzés költségeit. A mostani szabályozás ezt a munkáltatónak írja elő, ha távmunkában foglalkoztatja a munkavállalót. A törvényjavaslatban kidolgozásra kerülne egy havi átalány összeg, ami legfeljebb a mindenkor minimálbér 10 százaléka lehetne. A munkáltatói támogatás tehát idén 16 100 forint lehetne, amely a rezsinek azon részét fedezné, amelyet a munkavállaló munkába fektet.²¹

2020. október 15-én részt vettem a Women in IT Security (WITSEC) szervezet WITSEC Pro Day 2020 konferenciáján, ahol Kállai László, a Magyar Nemzeti Bank Senior Superviora adott elő a távmunka biztonsági követelményeit magába foglaló de még nem publikált MNB ajánlásról. Maga az MNB ajánlás pontos meghatározása a következő: „*A Pénzügyi Stabilitási Tanács által kiadott ajánlások a Magyar Nemzeti Bankról (MNB) szóló 2013. évi CXXXIX. törvény 13. § (2) bekezdés i) pontjának megfelelően kiadott, kötelező erővel nem bíró jogalkalmazást ismertető eszközök.*”²² Előadásának központi eleme a Magyar Nemzeti Bank

²¹ „Formálódnak az új home office szabályai, új részletek derültek ki”, 24.hu (blog), 2020. szeptember 7., Letöltés dátuma: 2020. szeptember 21., <https://24.hu/fn/gazdasag/2020/09/07/formalodnak-az-uj-home-office-szabalyai-uj-reszletek-derultek-ki/>.

²² „Ajánlások”, Magyar Nemzeti Bank, Letöltés dátuma: 2020. október 16., <https://www.mnb.hu/felugyelet/szabalyozas/felugyeleti-szabalyozo-eszkozok/ajanlasok>.

elkészült, de jelenleg még nyilvánosan nem elérhető ajánlása, amely a távmunka információbiztonságát vizsgálja és ad útmutatást a biztonságos távmunka kialakításához. Az ajánlás kitér arra, hogy szabályozni szükséges az távmunka elrendelésének és visszavonásának módját, továbbá szabályzatban meg kell jelölni azon eszközök körét, amely ezen atipikus munkaformában elérhetőek a munkavállalók számára, illetve külön meg kell határozni a távmunka elvégzéséhez szükséges eszközök listáját. Rendelkezni kell azon munkavállalók köréről, akik esetében lehet ezt a típusú munkavégzést alkalmazni. Szabályzatba kell foglalni az IT biztonsági követelményeket külön erre a munkaformára. Elhangzott még, hogy a születendő ajánlás a kockázatelemzésre is nagy hangsúlyt fektet, amely alkalmazásakor az adott szervezeteknek meg kell határozniuk azon kockázati tényezőket, amelyet csökkenteni vagy elfogadni szükséges. A távmunka infrastruktúrájának meghatározása is része lesz az ajánlásnak. Az ajánlás tartalmazza, hogy miként lehet a meglévő infrastruktúrát bővíteni úgy, hogy az megfeleljen az intézményi és jogszabályi követelményeknek. Az előadás következő pontja az eszköz osztályozása volt, amelyben 3 fő osztály lett elkülönítve. Ezen csoportok az intézményi eszközök, személyi eszközök és harmadik fél tulajdonában levő eszközök. Mindegyik csoport más és más kockázatokkal rendelkezik, amelyeket külön vizsgálni szükséges a kockázatfelmérésnél. Ha belegondolunk, hogy például egy intézményi laptop esetében a szervezet pontosan tisztában van azzal, hogy milyen szoftverek vannak az adott eszközön, és az adott felhasználó milyen jogosultságokkal rendelkezik. Azonban, ha a munkavállaló saját eszközét használja a távoli munkavégzés során, a szervezet ez esetben nincs tisztában, hogy az adott eszközön milyen szoftverek vannak telepítve, rendelkezik-e a munkavállaló bármilyen vírusvédelmi eszközzel. Ez mind olyan kockázat lehet, amellyel egy adott szervezetnek számolni kell. A leendő ajánlás a helyszíni biztonságra is hangsúlyt fektet, aminek keretén belül leír egy minimális biztonsági követelmény szintet. Ebben kitér a fizikai, adminisztratív és hálózati védelemre. Erre azért van nagy szükség, mert például a munkavállaló egy kávéházban végezné a munkáját, körülötte lévő személyek láthatják, illetve hallhatják, hogy mivel foglalkozik, továbbá ilyen helyeken eléggé alacsony védelemmel rendelkező hálózati hozzáférési pontokat telepítenek, amelyen keresztül könnyű a forgalmat figyelni és értékes adatokhoz jutni. Fontos és egyben nem egyszerű a minimális biztonsági szint meghatározása, mivel a munkáltató telephelyén mindenki számára egységes feltételek vannak biztosítva biztonság szempontjából, mint például beléptető rendszer, portaszolgálat, kamera rendszer. Azonban a munkavállalók otthonai eltérőek, valahol van riasztó valahol nincs, egyik helyszín kertes ház a másik panellakás, az egyik munkavállaló egyedül él, a másik egy kollégiumban. Az oktatás is fontos szempontja az ajánlásnak, hogy a munkavállalók folyamatosan a lehető

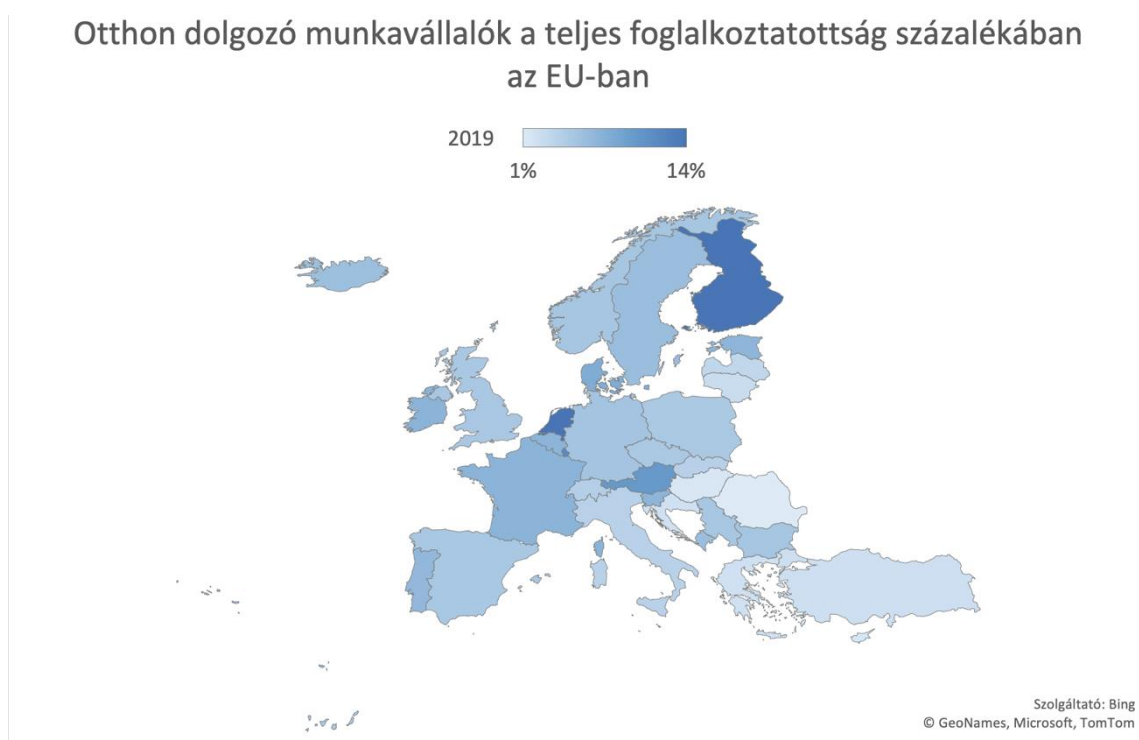
legmagasabb információbiztonsági tudatosság szintjén helyezkedjenek el. Az online konferencia is a távoli munkavégzés szervezés részét képezi, és természetesen az ajánlásban is helyet fog kapni. Ebben a titkosítás fontossága külön részt fog kapni, hogy csak olyan alkalmazások használata legyen engedélyezve, amely titkosított kapcsolatot biztosít a felek között. Fontos az ilyen online konferenciák részvételéhez szükséges hitelesítési folyamat kialakítása, amelynek egységesen mindenki alkalmazhatónak kell lennie. Kiemelt jelentőséggel bír, hogy az ilyen konferenciák során külön védeni szükséges a nem publikus adatokat. A szervezeteknek egy ellenőrzési rendszert kell alkalmazni a távoli hozzáférés monitorozására. A szervezetnek információval kell rendelkezni arról, hogy melyik rendszerében ki mikor és hogyan lépett be. Ezt naplózni szükséges, és ezen naplóállományokat esetleges incidens esetén kielemezhetőnek kell lennie. Ezek voltak azok a főbb pontok, amelyet a Magyar Nemzeti Bank szakembere ismertetett az előadása során. Ezen ajánlás főleg pénzügyintézeteknek szól, azonban könnyen implementálható lesz más ágazatokban is, és nagy segítséget nyújthat a hazai vállalkozásoknak egy biztonságos távmunkavégzés kialakításában.

Az elemzéséből látni lehet, hogy a magyar szabályozás egy keretrendszert ad meg a távmunkavégzéssel kapcsolatban, amely számos részletszabályozást átenged a feleknek, akik ezen szabályokat a munkaszerződésben fektethetik le. Kötelező érvényű szabályozás a közeljövőben nem terveznek kialakítani a távoli munkavégzés kiberbiztonságával kapcsolatban. Viszont lassan megjelenik egy Magyar Nemzeti Bank által kiadott ajánlás, amely nem kötelező érvényű, de legalább a szervezetek rendelkeznek majd egy olyan dokumentummal, ami szerint ki tudják alakítani a biztonságos távmunka végzés rendszerét. Így az a T1 tézisem született, hogy a magyar jogi szabályozások nem térnek külön ki a kiberbiztonságra a távmunka tükrében, tehát a H1 hipotézisem miszerint, feltételezem, hogy a távmunkával kapcsolatos hazai normatív szabályozás nem reflektál a kiberbiztonsági kihívásokra helyt állt.

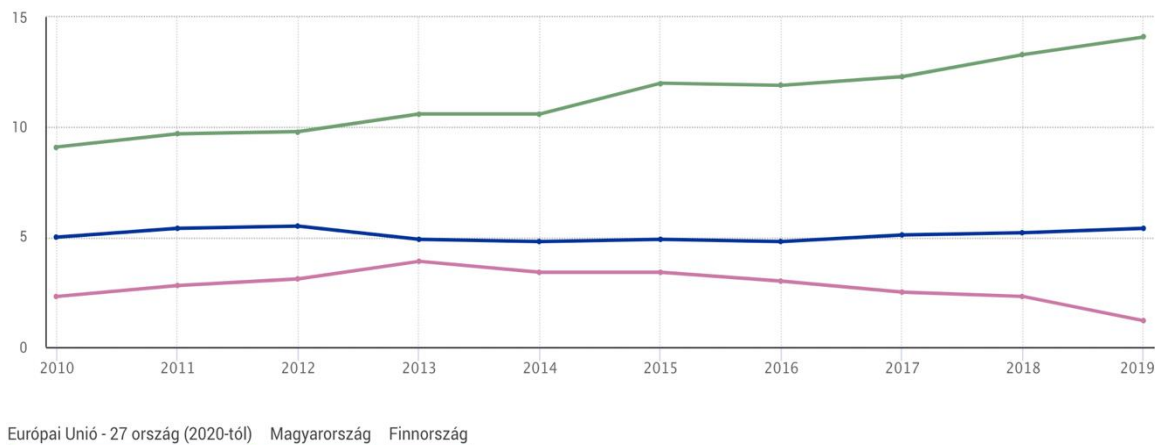
2.2. Távoli munkavégzés nemzetközi szabályozása

Az Eurostat 2019. évi felmérésében láthatjuk, hogy hazánk az otthoni munkavégzés tükrében az utolsók között mozgott 1,2%-al, míg például Finnország volt a vezető 14%-al. Jelen részben az európai uniós jogi háttérrel vizsgálom meg, hogy milyen irányelvek vonatkoznak a tagországokra a távmunka kapcsán. Részletesen az Amerikai Egyesült Államokat, mint Európán kívüli államot vizsgálom meg, ahol magasnak mondható a távoli munkavégzés aránya,

ezt követően pedig Finnországot vizsgálom meg, hogy jogilag hogyan szabályozza a távmunkavégzést, illetve milyen lépéseket eszközölt a koronavírus első hulláma során.



2. ábra Otthon dolgozó munkavállalók a teljes foglalkoztatottság százalékában az EU-ban(2019)(sajátszerkesztés forrás: Eurostat)



3. ábra Otthoni munkavégzés aránya 2010-2019-ig az vizsgált országokban (forrás: Eurostat)

2.2.1. Európai Unió szabályozása

A távmunkáról szóló európai keretmegállapodást 2002-ben fogadták el. A megállapodás általános európai keretet biztosít a távmunkát végző emberek számára, amelyet a nemzeti eljárásoknak és gyakorlatoknak megfelelően kell végrehajtani. Ebben a megállapodásban a távmunkát a következőképpen határozzák meg. A távmunka a munka megszervezésének és / vagy elvégzésének egy formája, az informatika alkalmazásával, egy munkaszerződés / jogviszony keretében, ahol a munkát, amelyet a munkáltató telephelyén is el lehetne végezni, a telephelytől távol, rendszeresen végzik. Az EU-tagállamok többsége végrehajtotta a távmunkáról szóló európai keretmegállapodást. Írország és az Egyesült Királyság bevezették ezt, mint útmutatót és helyes gyakorlatot. Néhány más ország, például Magyarország átültette a megállapodást nemzeti jogrendszerébe. A távmunkáról szóló európai keretmegállapodás a következő elemeket tartalmazza:

- a távmunka önkéntes jellegű mind az érintett munkavállaló, mind az érintett munkáltató számára;
- annak garantálása, hogy a távmunkát végzők ugyanazon jogokat élvezzék a foglalkoztatási feltételek tekintetében, mint a munkáltató telephelyén dolgozó hasonló munkavállalók;
- a munkáltató által meghozandó intézkedések annak biztosítására, hogy a távmunkát végző által használt és feldolgozott adatokra megfelelő adatvédelmi előírások vonatkoznak, és hogy a távmunkát végző magánéletének tiszteletben tartása megtörténjen;

- a távmunkához szükséges berendezések telepítésének és karbantartásának biztosítása, amely a munkaadók felelőssége, kivéve, ha a távmunkát végző a saját eszközének használatát választja;
- a távmunkát végző munkahelyi egészségének és biztonságának védelme, amelyért a munkáltató felelős az alkalmazandó uniós és nemzeti jogszabályokkal, valamint a kollektív szerződésekkel összhangban;
- a távmunkát végző irányítja saját munka idejének megszervezését az alkalmazandó jogszabályok, kollektív szerződések és a vállalati szabályok keretein belül, és a munkáltató telephelyén hasonló munkavállalókra alkalmazandó egyenértékű munkaterhelésre és teljesítményre vonatkozó normákat is alkalmaz;
- intézkedések annak megakadályozására, hogy a távmunkát végző elkülönüljön a vállalat többi munkaközösségétől;
- képzéshez és karrierfejlesztési lehetőségekhez való hozzáférés, amelynek meg kell egyeznie a munkáltató telephelyén dolgozó hasonló munkavállalókkal;
- a távmunkát végzők kollektív jogai, amelyeknek meg kell egyezniük a munkáltató telephelyén dolgozó munkavállalókéval;
- végrehajtás és nyomon követés.

A távmunka előfordulása nemcsak a különböző országok technológiai fejlődésével, hanem a meglévő gazdasági struktúrákkal és munkakultúrákkal is összefügg. Jenleg magas távmunka arányú országok között szerepel Finnország, Hollandia, Svédország. Összességében a távmunka előfordulása jelentősen változik, a munkavállalók 2% és 40% között, attól függően, hogy melyik országban, milyen foglalkozással, melyik ágazatban és milyen gyakorisággal végeznek ilyen típusú munkát a munkavállalók. Az EU-28 egész területén az alkalmazottak átlagosan 17%-a dolgozik ezen atipikus munkavégzési formában. A legtöbb országban a munkavállalók nagyobb hányada alkalmanként, nem pedig rendszeresen végez távmunkát. A távmunka gyakoribb a szakemberek és a menedzserek körében, de jelentős az irodai támogatást nyújtó és az értékesítési szektorban dolgozók körében is. A nemek vonatkozásában általában a férfiak mutatnak nagyobb hajlandóságot a távmunkára. A nők azonban rendszeresebben végeznek otthoni munkát, mint a férfiak. Ez arra utal, hogy az országspecifikus nemi szerepek, valamint a munka és a családi élet modelljei is szerepet játszanak a távmunka kialakításában. Ami a távmunka pozitív hatásait illeti, a munkavállalók az ingázási idő csökkenéséről, a munkaidő nagyobb autonómiájáról számolnak be, ami nagyobb rugalmasságot eredményez a

munkaidő-szervezés terén, jobb a munka és a magánélet közötti egyensúly és a termelékenység javulása mutatkozik. A vállalatok profitálnak a munka és a magánélet egyensúlyának javulásából, ami fokozott motivációhoz, valamint fokozott termelékenységhez és hatékonysághoz vezethet, valamint csökkenhet az irodahelyiség iránti igény és a kapcsolódó költségek. A távmunka hátránya az a tendencia, hogy hosszabb munkaidőhöz vezet, átfedést hoz létre a fizetett munka és a magánélet között (munka - otthon interferencia), és a munka intenzívebbé válását eredményezi. Úgy tűnik, hogy a távmunka részleges és alkalmi formái pozitívabb végeredményt mutatnak az előnyök és hátrányok tükrében. Nemi szempontból a távmunkát végző nők általában rövidebb ideig dolgoznak ilyen atipikus munkaszervezésben, mint a férfiak, és úgy tűnik, hogy a nők valamivel jobb munka- és magánélet egyensúlyi hatásokat érnek el. A távmunkáról szóló európai keretmegállapodás (2002) bizonyos mértékben foglalkozik a távmunka lehetséges nyereségeivel és kockázataival az EU tagállamaiban ²³

2.2.2. Európai szabályozás kiberbiztonsági aspektusa

Az európai keretmegállapodás nem tér ki az távoli munkavégzés információ- és kiberbiztonsági aspektusára, amely több ok miatt lehet. Először is ezen keretmegállapodás a fő irányvonalat határozta meg a tagországoknak, nem tartalmaz részletszabályozásokat, továbbá 2002-ben a kiberbiztonság még nem volt ennyire központi szempont, mint ma a világban. Tehát kijelenthető, hogy ezen megállapodástól nem is volt elvárható, hogy reflektáljon a kiberbiztonsági kihívásokra.

2.2.3. Egyesült Államok szabályozása

A távmunka aránya egyre növekszik az Egyesült Államokban a közigazgatáson kívül is. A telephelyen kívüli munkavégzéssel töltött órák száma, valamint a munkavállalók száma, akik távmunkában dolgoznak növekszik. 2012-ben a Gallup adatai azt mutatták, hogy az alkalmazottak 39% -a távolról dolgozott valamilyen minőségben, vagyis idejük legalább egy részét munkatársaiktól távol töltötték. 2016-ban ez a szám négy százalékponttal nőtt 43% -ra.

²³ Jon Messenger és mtsai., *Working Anytime, Anywhere: The Effects on the World of Work* (Geneva: International Labour Organization and the European Foundation for the Improvement of Living and Working Conditions, 2017), http://www.ilo.org/global/publications/books/WCMS_544138/lang--en/index.htm.

Azonban 2012 és 2016 között nem csak a személyek szám nőtt, hanem az időintervallum aránya is, amelyben a munkavállalók távmunkában dolgoztak.²⁴

2000 óta az amerikai szövetségi törvény előírja, hogy minden egyes amerikai kormány alkalmazottja a lehető legnagyobb mértékben tudjon otthonról dolgozni. Az eredeti motiváció a kormány leállásától való félelem volt a madárinfluenza-járvány miatt. Azóta a terrorcselekmények, a szélsőséges időjárási események és más járványos fenyegetések többször emlékeztették a kormány vezetőit a távmunka szükségességére. 2010-ben Obama elnök, szorgalmazta a szövetségi távmunkára vonatkozó jogszabályok elfogadását. 2010 decemberében a távmunka-fejlesztési törvény (Telework Enhancement Act továbbiakban: TEA) kétpárti támogatással elfogadta a kongresszus mindkét háza, és az elnök törvénybe foglalta. Ez a törvény arra kötelezte az Egyesült Államok szövetségi ügynökségeit, hogy:

- olyan politikát alakítsanak ki, amely alapján a jogosult munkavállalók távmunkát folytathatnak;
- jelöljenek ki egy távmunka-irányító tisztet;
- határozzák meg az alkalmazottak jogosultsági körét és értesítsék őket jogosultsági állapotukról;
- ki kell jelölniük egy felső vezetőt, hogy koordinálja az egyes ügynökségek távmunkaprogramját;
- írásbeli megállapodást igényel az ügynökség vezetője és a távmunkára felhatalmazott munkavállalói között;
- távmunka-képzési programok kidolgozása és végrehajtása a vezetők és alkalmazottak számára;
- gondoskodjanak arról, hogy interaktív képzést nyújtsanak a jogosult munkavállalóknak és menedzsereiknek, és hogy a képzés sikeresen lezáruljon a távmunka-megállapodás megkötése előtt;
- elfogadják a távmunkát az ügynökség folytatólagos működési tervének részeként.²⁵

²⁴ Inc Gallup, „Is Working Remotely Effective? Gallup Research Says Yes”, Gallup.com, 2020. január 24., Letöltés dátuma: 2020. október 01., <https://www.gallup.com/workplace/283985/working-remotely-effective-gallup-research-says-yes.aspx>.

²⁵ „H.R.1722 - 111th Congress-Telework Enhancement Act of 2010” (2010), <https://www.congress.gov/bill/111th-congress/house-bill/1722/text>.

2.2.4. Amerikai szabályozás kiberbiztonsági aspektusa

Office of Management and Budget, és az Office of Management and Budget igazgatójának, a Department of Homeland Security és a National Institute of Standards and Technology együttműködésével iránymutatást kellett kiadniuk, legkésőbb 2011. június 7-ig, a 65. fejezet elfogadását követően annak biztosítása érdekében, hogy a távmunka során használt információs rendszerek információ- és kiberbiztonsági védelme megfelelő legyen. Az iránymutatásnak tartalmazniuk kell legalább az alábbi szükséges követelményeket:

- az ügynökség információihoz és információs rendszereihez való hozzáférés ellenőrzése;
- az ügynökségi információk (beleértve a személyazonosításra alkalmas információkat) és az információs rendszerek védelme;
- korlátozása a sebezhetőségek lehetőségeinek;
- az ügynökség ellenőrzése alatt nem álló, távmunkára használt információs rendszerek védelme;
- a távmunkához használt vezeték nélküli és egyéb telekommunikációs eszközök használatának biztosítása;
- és a pornográfia, beleértve a gyermekpornográfiát is, megtekintésének, letöltésének vagy cseréjének megakadályozása, továbbá megakadályozása a hivatali idő vagy erőforrások nem megfelelő felhasználásának. A törvény előírja, hogy az Office of Management and Budget igazgatója politikai iránymutatást adjon ki, amely előírja a végrehajtó ügynökségek számára, hogy számítógépes rendszerek vásárlásakor olyan számítógépes rendszereket szerezzenek be, amelyek lehetővé teszik és támogatják a távmunkát, hacsak az ügynökség vezetője nem állapítja meg, hogy küldetés-specifikus oka van annak, hogy ezt ne tegye.

Míg a TEA és az Egyesült Államok Személyzeti Menedzsment Irodája útmutatást kínált a szövetségi kormányzati szervek számára távmunka-programjaik kidolgozásához, mindegyik ügynökség feladata a saját szabályzatának, képzésének és eljárásainak kidolgozása. A TEA aláírása óta a rendszeres távmunka engedélyezése a szövetségi kormány alkalmazottainak 2011-es 4% -ról 2014-re 14% -ra nőtt.²⁶

²⁶ i.m. Messenger és mtsai., *Working Anytime, Anywhere*.

Viszont fontosnak tartom azt is kiemelni, hogy ezen részletes szabályozás csak a közigazgatásra vonatkozik. Az Egyesült Államokban nincs meghatározva egy szövetségi törvény, amely rendelkezik a távmunkáról, ezen szabályozások államonként igen eltérő.

Az USA példáján láthatjuk, hogy egy olyan átgondolt távmunkavégzési stratégiával rendelkeznek, amely tudja biztosítani a biztonságos távmunkavégzést. Ha megnézzük távmunka-fejlesztési törvényt külön felelőst biztosít az állami szerveken belül a távmunkavégzésre, illetve külön információ- és kiberbiztonsági szabályokat is előír.

2.2.5. *Finnország törvényi szabályozása*

A 3. ábrán jól látható, hogy Finnország vezet az távmunka végzés terén az Európai Unióban. Ez azért lehet, mert a rugalmas munkavégzés - amelyet néhány országban még mindig inkább kiváltáságnak, mint jognak tekintenek - több mint két évtizede beágyazódott Finnország munkakultúrájába.

Ez nagyrészt az 1996-ban elfogadott munkaidő-törvénynek köszönhető, amely a legtöbb munkavállaló számára megadja a jogot arra, hogy a napi óráit legfeljebb három órával korábban vagy később kezdje.

A magas távoli munkavégzés, illetve rugalmas munkavégzés aránya a finn bizalmi kultúrából is eredhet, hiszen az ötből négy finn azt mondja, hogy bízik honfitárásában, így a finnek bizalma nagyobb a polgártársaikban, mint bárhol máshol Európában.²⁷

A Grant Thornton globális könyvelőiroda tanulmánya szerint 2011-re Finnország a legrugalmasabb munkaidő-beosztást kínálta a bolygón, és a vállalatok 92% -a lehetővé tette a munkavállalók számára, hogy munkaidőt módosíthassák, míg az Egyesült Királyságban és az Egyesült Államokban ez az arány 76%, Oroszországban és Japánban csak 18% volt.²⁸

Azóta világszerte intenzívebbé váltak a rugalmas munkavégzés előnyeiről szóló viták, a nemzeti jogszabályok megjelenése a témában, amelyek célja az agilisabb munka előmozdítása. De úgy tűnik, Finnország az új munkaidő-törvénynek köszönhetően az élmezőny tagja marad továbbra is a témában.

²⁷ Maddy Savage, „Why Finland Leads the World in Flexible Work”, BBC, 2019. augusztus 7., Letöltés dátuma: 2020. október 21., <https://www.bbc.com/worklife/article/20190807-why-finland-leads-the-world-in-flexible-work>.

²⁸ Laura Walter, „Finland, Sweden, Australia Offer Most Flexible Work Schedules | EHS Today”, 2011. június 6., Letöltés dátuma: 2020. szeptember 02., <https://www.ehstoday.com/archive/article/21904410/finland-sweden-australia-offer-most-flexible-work-schedules>.

A finn parlament 2019. március 13-án fogadta el az új finn munkaidőről szóló törvényt. A törvény 2020. január 1-jén lépett hatályba. A törvény a munkaidő-irányelv követelményeit és annak értelmezéseit szolgálja. Az új törvény célja, hogy reagáljon a mai munka világában támasztott igényekre azáltal, hogy megkönnyíti a rugalmas munkaidő-megállapodást, és javítja az alkalmazottak lehetőségeit a munka és a magánélet összeegyeztetésére.

Munkaidőről szóló új törvény a következő változtatásokat foglalja megában:

- A régi munkaidőtörvénnyel ellentétben az új törvény viszonylag semleges a munka helyével kapcsolatban. Mivel számos iparágban a munka már nem kötődik egy adott helyhez vagy időhöz, az új törvény alkalmazása nem követeli meg, hogy a munkát egy bizonyos helyen végezzék. A fentieket figyelembe véve az új törvény a távmunkára is vonatkozik.
- A törvény a rugalmas munkaidő új koncepcióját vezeti be. A munkaadó és a munkavállaló megállapodhat a rugalmas munkaidőről, ha a munkavállaló feladatai olyan jellegűek, hogy a munkavállaló önállóan dönthet arról, hogyan osztja el teljes munka idejének legalább felét, valamint dönthet a munka helyéről. A munkavállaló fennmaradó munka idejét továbbra is a munkáltató ütemezheti. A rugalmas munkaidő kiválóan alkalmas szakemberi munkára, ahol a konkrét célok és az általános menetredek fontosabbak, mint egy adott időben történő munka.
- Jelenleg a túlórák maximális összege naptári évenként 250 óra, lehetőséget biztosítva a naptári évenként 80 órás túlórák megkötésére. A túlórák azonban négy hónapon belül nem haladhatják meg a 138 órát. Az új törvény rendelkezései már nem szabályozzák külön a túlórák maximális összegét, ehelyett a teljes munkaidő korlátját tartalmazza. A maximális munkaidő, a túlórával együtt, átlagosan heti 48 óra lesz négy hónapos időtartam alatt, és nincs lehetőség megállapodni a további túlórákról.²⁹

2.2.6. A finn szabályozás kiberbiztonsági aspektusa

A jogszabályi elemzésből látható, hogy a távoli munkavégzés információ- és kiberbiztonsági aspektusa nem jelenik meg normatív szabályozásban. Viszont kijelenthető, hogy részletesebb szabályokat tartalmaz a finn jogi szabályozás az atipikus munkavégzésre, mint a magyar jogi környezet. Azonban itt is mint a magyar szabályozásnál is hiányoznak azok a biztonsági

²⁹ Nevalainen Petri és Toivonen Sofia, „Finland’s Updated Working Hours Act Takes Effect 1 January 2020”, Ally Law, 2019. október 25., Letöltés dátuma: 2020. augusztus 28., <https://ally-law.com/finlands-updated-working-hours-act-takes-effect-1-january-2020/>.

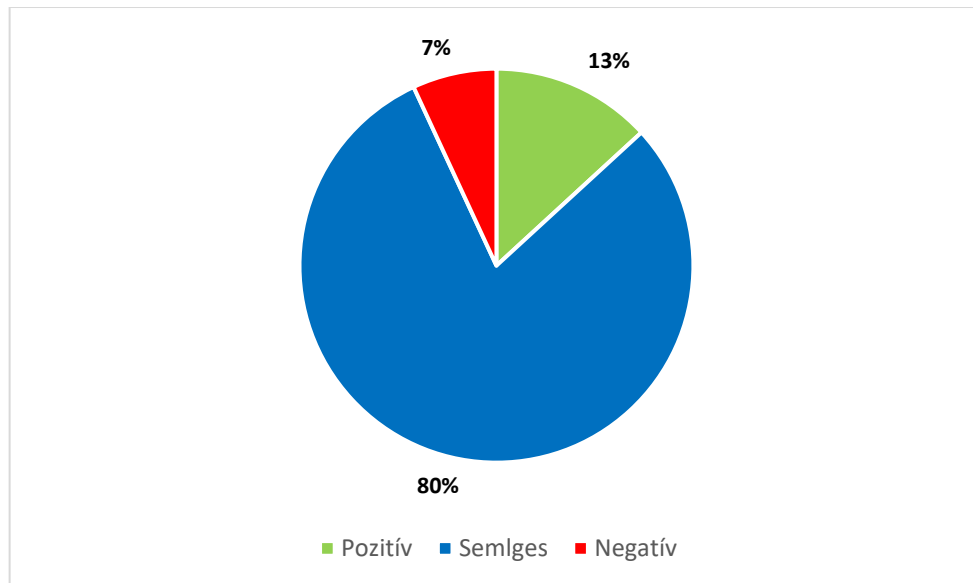
szabályok, amelyek biztosítanának egy olyan keretrendszert, amit a munkáltatónak, illetve munkáltatónak biztosítani kell.

Összegezve a hazai, illetve nemzetközi normatív szabályozás vizsgálatát a témában azt a T4 tézist lehet felállítani, hogy azon országok rendelkeznek részletes szabályozással, ahol a távoli munkavégzés nagyobb arányban megtalálható. Így H4 hipotézisem miszerint azon országokban, ahol a távolimunkavégzés aránya magasabb, részletesebb a normatív szabályozás a témában, helyt állt. Hiszen láthatjuk, hogy hazánk tipikusan egy olyan ország, ahol ez elmúlt években igen alacsony volt a távmunka aránya és az erre vonatkozó szabályozás is inkább csak egy keretrendszer, amitől több ponton elérhet a munkáltató és munkavállaló közös megállapodással. Láthatjuk, hogy a magyar szabályozás átemelte a központi elemeket a távmunkáról szóló európai keretmegállapodásból. Míg, ha megvizsgáljuk a finn szabályozást, sokkal több részletszabályozást tartalmaz az atipikus munkavégzésre, mint a magyar. Illetve az Egyesült Államokbeli szövetségi szabályozás sokkalta részletesebb a hazai, illetve a finn normánál is. Ez az egyetlen jogszabály, ami tartalmaz utasítást például információbiztonság szempontjából.

2.3.A „Home office” kifejezés megjelenése az interneten

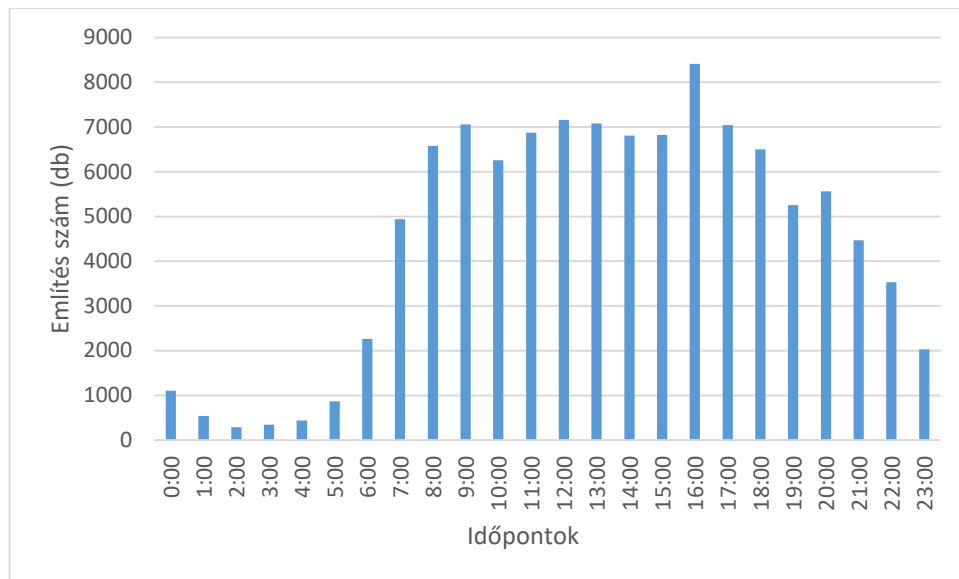
Ebben a részben azt vizsgálom meg, hogy a távoli munkavégzés miként jelenik meg az interneten. Ehhez a SentiOne (www.sentione.hu) weboldalt használtam, ami teljes világot lefedő, 30 nyelvet feldolgozó és webes szöveganalitikán alapuló social listening szoftver. Ami kulcsszavas keresés alapján, valós időben vagy akár 3 évre visszamenően figyeli, indexálja és elemezi az internetes fórumokon, blogokon, weboldalakon és közösségi média csatornákon közzétett publikus szöveges tartalmak minden típusát, melyek önmagukban vagy kontextusukban tartalmazzák a felhasználó által már előre definiált és a platformra felvitt kulcskifejezések bármelyikét. A releváns tartalmakat, kvantitatív kutatás céljából és ezt megkönnyítendő, különböző fókuszpontok és kutatási paraméterek mentén rendezi össze, melyeket interaktív grafikonokon ábrázol. A kvalitatív mélyelemzéseket is támogató módszertani, technológiai felépítés pedig biztosítja a kutatáshoz kapcsolódó összes indexált tartalom, poszt, komment, cikk és említés egyenként történő elemzésének és kategorizálásának lehetőségét is.

A vizsgált időtartam 2020. január 01.-től 2020. október 17.-ig terjedt, ahol a „home office”, „remote work”, „otthoni munkavégzés”, „távoli munkavégzés” kifejezésekre kerestem rá, ezen kifejezéseket angol, illetve magyar nyelven vizsgálta az algoritmus. Az látható, hogy összesen ez alatt az idő alatt 1 177 912 találat született, amelynek a szentiment analízis szerint 79,91%-a semleges megjegyzése volt közel 7%-a negatív és 13,18%-a pozitív. A SentiOne algoritmus mind magyar mind angol nyelven megvizsgálta a tartalmakat, hogy milyen szövegezéssel írták azt, negatív, pozitív vagy semleges.



4. ábra Kifejezések megjelenése érzelmek szerint (saját szerkesztés, forrás: SentiOne)

Ez az eredmény azért jöhetett ki, mert van olyan megosztás, amiben nem írnak semmit az adott tartalomról, amiben a kulcsszavak szerepelnek, így az algoritmus nem tudja a megosztó látásmódját vizsgálni. Azonban ezen magas arány azzal is magyarázható, hogy megosztások nagy része informatív jellegűnek voltak, vagyis a megosztó személy vagy oldal információt akart megosztani a témában nem pedig véleményét kifejteni. Ezenfelül lehet látni azt hazai tekintetben, hogy főleg a normál munkaidőben jelennek meg tartalmak (8:00-18:00) ezen keresőszavakkal, amit a lenti árba is jól mutat.

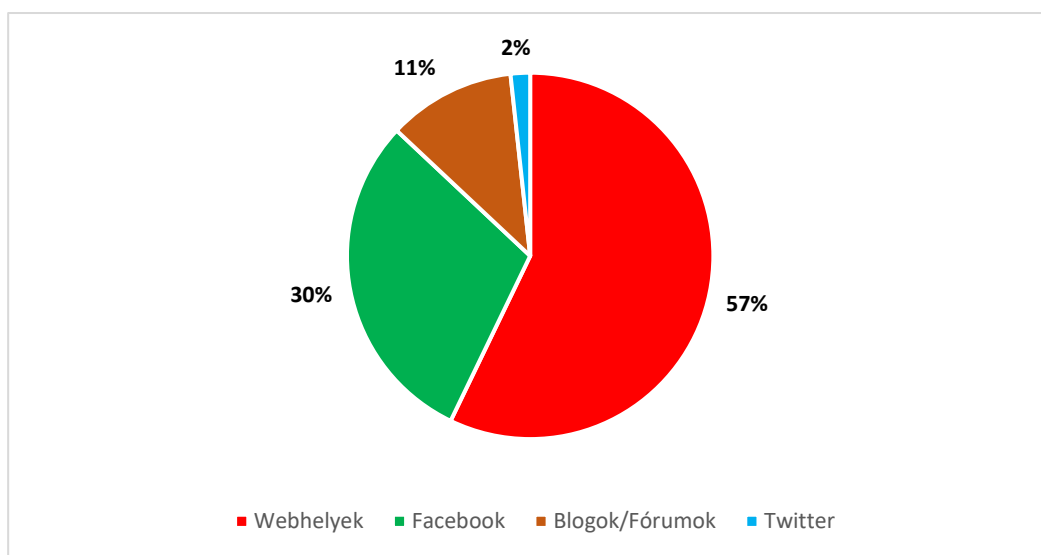


5. ábra Kifejezések hazai megjelenésének napi aránya,(saját szerkesztés, forrás: SenitOne)

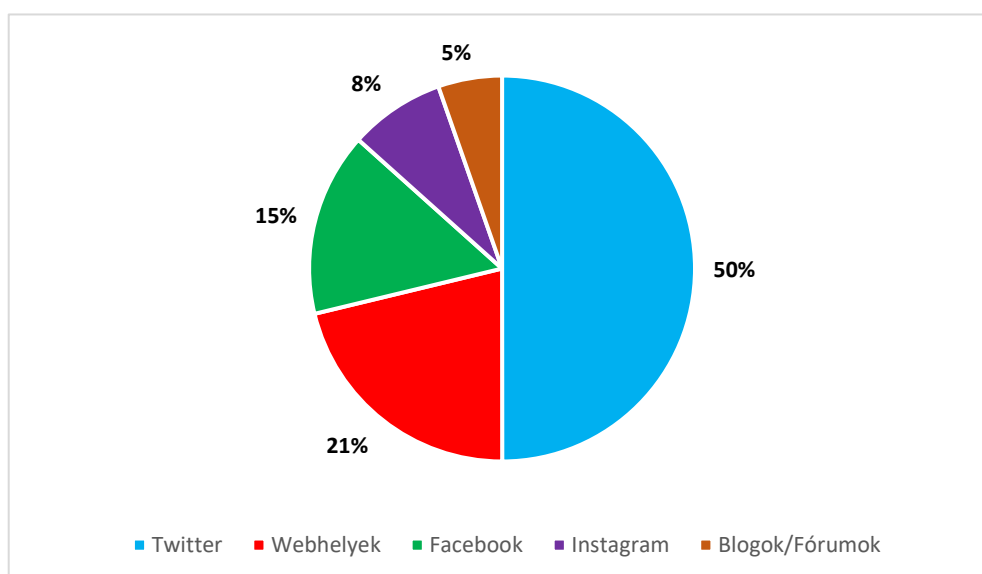
Megvizsgáltam a keresőszavak miként jelennek meg az egyes platformokon hazai és nemzetközi szinten. Kutatásom rámutatott arra, hogy míg nemzetközi szinten főleg a közösségi hálózati oldalakon jelentek meg a vizsgált kifejezések, addig Magyarországon nagyrészt weboldalakon voltak fellelhetők ezek a szavak, amit a lenti 4. és 5. ábra is szemléltet. Itt ki szeretném emelni, hogy a közösségi hálózati oldalak megfogalmazásomban nem egyenlő a közösségi médiával. A közösségi hálózati oldalak egy alcsoportja a közösségi médiának, ahol a hangsúly a hálózat építésén és a kommunikáción van főleg, és csak másodlagos a tartalom megosztás. Ebbe a csoportba tartozik a Twitter, Facebook, Instagram.³⁰ Igaz, hazánkban nem volt alacsony a Facebook platformon a megjelenés mértéke, de a Twitterrel együtt is csak 32%, ami a webhelyek 57%-hoz képest sokkal kevesebb. Azt lehet látni, hogy nemzetközi szinten a témáról az emberek, a közösségi hálózatokon nagyobb arányban osztanak meg tartalmat.

³⁰ Andreas Kaplan és Michael Haenlein, „Users of the World, Unite! The Challenges and Opportunities of Social Media”, *Business Horizons* 53 (2010. 0 28.): 59–68, <https://doi.org/10.1016/j.bushor.2009.09.003>.

Végül megvizsgáltam, hogy a home office tömeges megjelenésének hatására ebben az évben a kulcsszavak gyakorisága hogyan változott. Látható, hogy az első hullám idején márciusban volt a téma megemlézése a csúcson, majd folyamatos csökkentésnek indult, ezután még nyáron volt egy nagyobb növekedése, de azóta folyamatos és gyors csökkenést mutat. Ezek alapján az a T3 tézist állítható fel, hogy a második hullám idején nagy arányú csökkenés matatható ki a kulcsszavak tekintetében, így kijelenthetjük, hogy a H3 hipotézisem miszerint a home office kifejezés megjelenése az interneten a második hullám idején is legalább akkora mértékű, mint az első hullám alatt, megdőlt. Enne az egyik oka az lehet, hogy tavasszal vált világméretűvé a járvány és ekkor kellett a vállalatoknak tömeges szinten átállniuk távoli munkavégzésre.

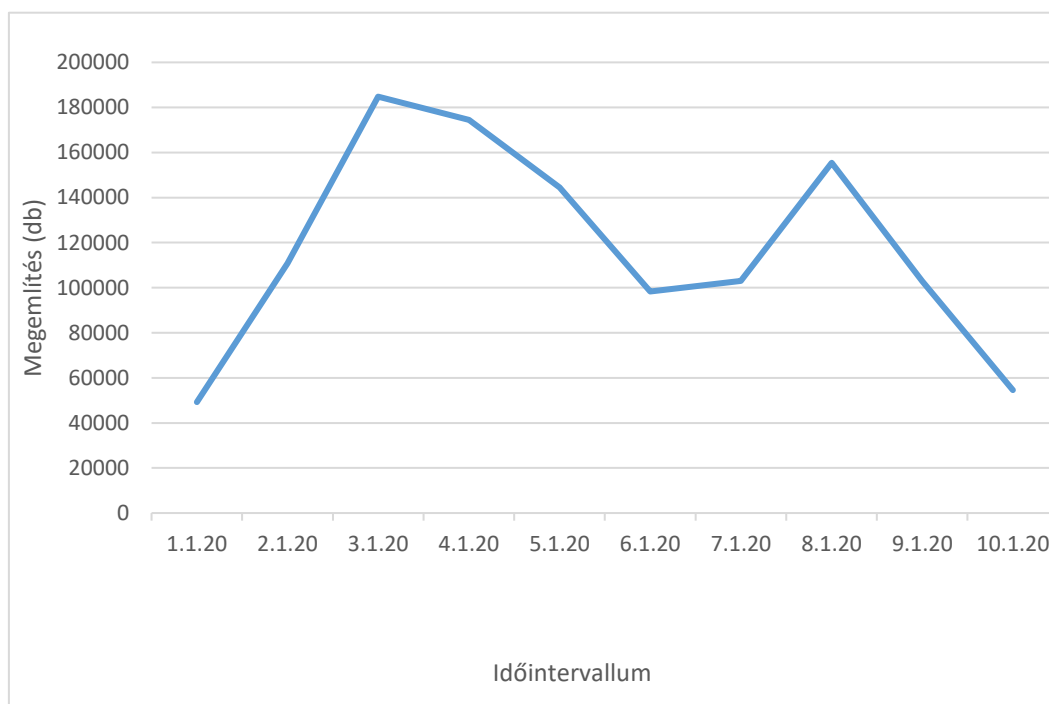


6. ábra Megemlékések platform szerinti megoszlása (Hazai), saját szerkesztés (forrás: SentiOne)



7. ábra Megemlékések platform szerinti megoszlása (Nemzetközi) (saját szerkesztés, forrás: SentiOne)

Mostanra a második hullám idejére a társadalom nagy része megszokta a COVID-19 jelenlétét és a távoli munkavégzést. Ez azt jelenti, hogy ezen munkaforma ugyan úgy nagyobb arányban van jelen, mint a vírus előtt azonban, mivel nem újdonság nem beszélnek róla annyit az emberek.



8. ábra Kulcsszavak időbeli megoszlása (saját szerkesztés forrás: SentiOne)

2.4. Következtetés

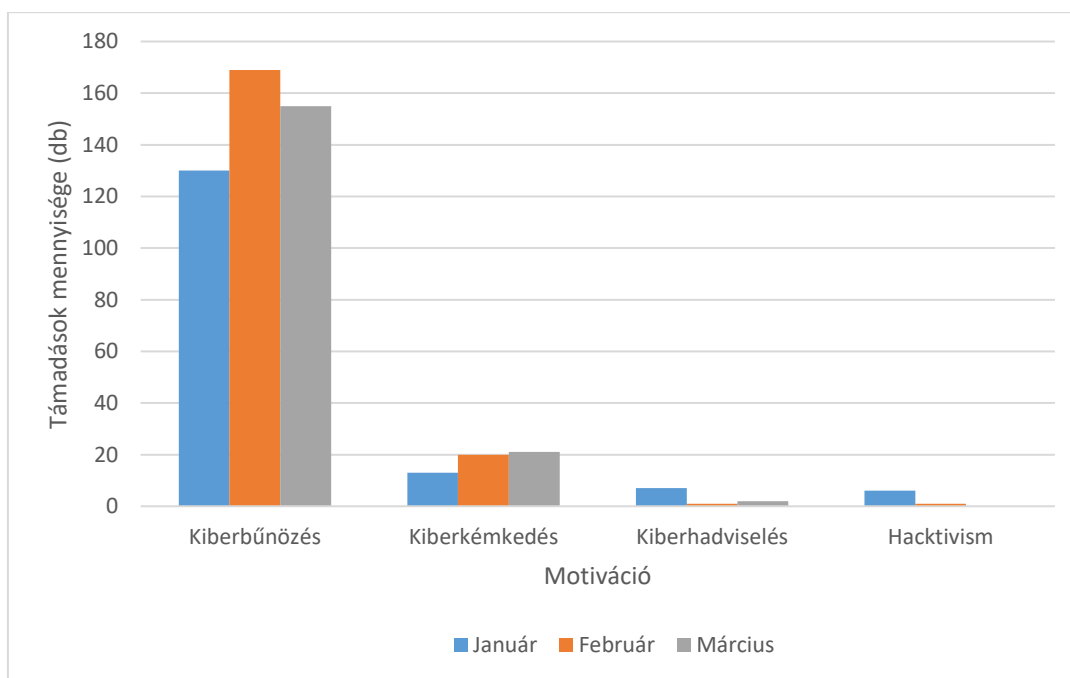
Összegezve az kijelenthető, hogy a távoli munkavégzés aránya a koronavírus előtt, igen sok tényezőtől függött. Hazánkban egy keretrendszer található meg, amely azon pontokon tartalmaz konkrét kikötéseket, ahol az európai keretmegállapodás is tartalmaz. Viszont a vizsgált államok közül mind az Egyesült Államok, mind Finnország tekintetében, részletesebb jogi szabályozás van hatályban. Ezen államokban a távmunka aránya a koronavírust megelőzően is magas volt, ezért a H4-es hipotézisem beigazolódott, miszerint azon államokban, ahol magasabb a távmunkavégzés aránya részletesebb jogszabályi rendelkezések vannak hatályban. Ezt követően megvizsgáltam, hogy a jogi szabályozáson kívül miként jelenik meg a távmunka kifejezés hazai, illetve nemzetközi szinten az interneten. Itt főleg az volt látható, hogy a platformok típusában eltérés mutatkozik hazai és nemzetközi említés kapcsán. Míg Magyarországon a témában főleg webhelyen találunk tartalmakat, addig nemzetközi szinten inkább a közösségi média hálózatokon jelennek meg témában anyagok. Ezenfelül a H3-as

hipotézisem megdőlt, miszerint a home office kifejezés megjelenése az interneten a második hullám idején is legalább akkora mértékű, mint az első hullám alatt.

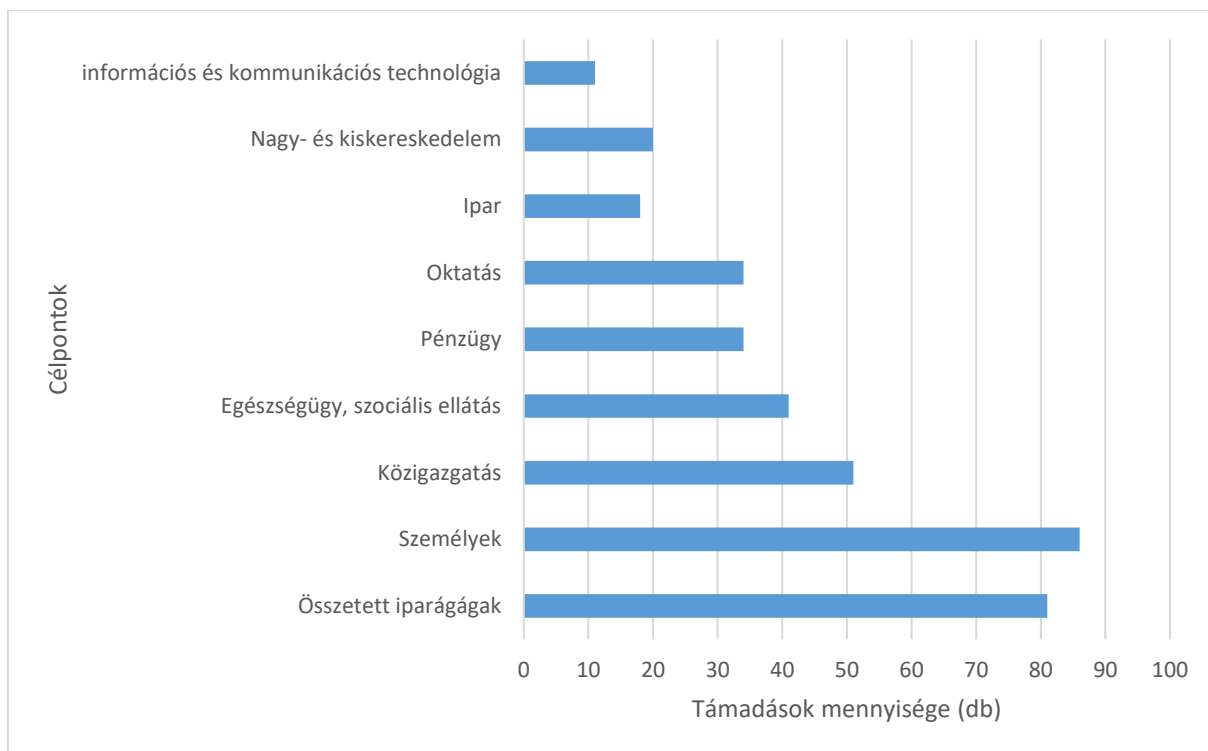
3. FEJEZET- TÁVOLI MUNKAVÉGZÉS INFORMÁCIÓ- ÉS KIBERBIZTONSÁGI KIHÍVÁSAI

3.1.Főbb támadási formák, amelyek népszerűek voltak a Covid-19 első hulláma idején

Ebben a részben rendszerezve kerül bemutatásra azok a támadások, amelyek népszerűek voltak a támadók körében a koronavírus első hullámának idején. Látható, hogy motiváció szerint főleg kiberbűnözés volt fellelhető 2020 elsőnegyedében, továbbá megfigyelhető az is, hogy a támadások főbb célpontjai személyek voltak, de közigazgatás és egészségügyi is eléggé nagy arányban volt a támadások középpontja.



9. ábra A motivációk havi eloszlása 2020 Q1 (sajátszerkesztés, forrás: Hackmageddon)



10. ábra Támadások célpontjai 2020 Q1 (sajátszerkesztés, forrás: Hackameddon)

A továbbiakban képet kapunk arról, hogy mely támadások, mire irányultak, és hogy mely kiberbiztonsági fundamentumot támadta. Látni fogjuk azt, hogy egyes támadások között átfedés van, amely esetünkben azt jelenti, hogy egyes támadások végrehajtásához szükséges egy másik fenyegetés alkalmazása is.

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.”³¹

- Zsarolóvírusok: olyan rosszindulatú programok, amivel a támadók a megfertőzött eszközt lezárják, ezzel elérhetetlenné téve az áldozat adatai. Céljuk a haszonszerzés, mivel váltságdíjat követelnek az adatok visszaállításáért, az úgy nevezett visszafejtő kulcsért. Ezen határidő igen rövid és legtöbbször a váltságdíjat valamely kripto devizában kérik azért, hogy ne lehessen visszakeresni azt. Ezek a támadók megtalálták a siker vektorát, amely magában foglalja az adatok kritikusságát és az

³¹ Muha Lajos és Krasznay Csaba, *Az elektronikus információs rendszerek biztonságáról vezetőknél* (Budapest: Nemzeti Közszerológati Egyetem, 2014): 9.

információbiztonsági szegénységi küszöböt. A biztonsági 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 most célpontok. Bármely olyan szervezet, amely kritikus adatokat kezel elégtelen biztonsági költségvetéssel, tökéletes célpontja ezeknek az anyagilag motivált kibertámadásnak. Az idő múlásával egyértelműen eltolódtak a támadási vektorok, ami bizonyítja a számítógépes bűnözés iparának opportunistá tendenciáit. Elsődlegesen háromféle támadóvektor létezik a kezdeti ransomware fertőzés véghezvitelre. 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. Ezen 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 kényszerítése. A gyenge autentikációval rendelkező távoli asztali protokoll szolgáltatásokat a támadók illetéktelen hozzáférésre és ransomware telepítésre kényszerítik.³²

- Online csalások: A tiltott pénzügyi nyereség megkönnyítésére tervezett COVID-19 témájú rosszindulatú programok mellett a COVID-19 témájú marketing tevékenységek 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 témákat jelentős mértékben használják az adathalászatra és más online csalásra. 2020 januárja óta az INTERPOL egyik magánpartnere, a Trend Micro 907 000 üzenetet észlelt a COVID-19-hez kapcsolódóan. Kihasználva a gazdasági visszaesést és az emberek szorongását a világjárvány idején. A kiberbűnözők fokozták socila engineering taktikájukat azzal,

³² Pranshu Bajpai és R.J. Enbody, „Attacking Key Management in Ransomware”, *IT Professional* 22 (2020. március 1.): 21–27, <https://doi.org/10.1109/MITP.2020.2977285>.

hogy támadásaik alapjául a COVID-19-et használták.³³ A sértetlenségnél részletesebben kifejezem az adathalász módszerek, működését.

Sértetlenség: „*az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvártnal 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.*”³⁴

Eredetiség: 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.³⁵

- Adathalászat: Fontosnak tartom megjegyezni, hogy a 9. számú ábrán maga az adathalászat és a Vishing külön szerepel. Ez a felosztást mikor megtaláltam azért volt számomra megfelelő, mert attól, hogy a telefonos adathalászat része az adathalászatnak, mégis olyan merőben más technikai háttérrel és folyamatot igényel, amely megkülönbözteti az többi adathalász típustól. Az adathalászat szintén gyakori fenyegetés, amelyet a COVID-19 pandémiás helyzetben alkalmaznak a támadók. Az adathalászat alapja, hogy a támadók egy megbízható entitásnak adják ki magukat, mint például pénzügyintézet, közigazgatási szerv, munkáltató. A támadók meghamisítják az e-mail címüket, így úgy tűnik, hogy valaki mástól származik. Hamis webhelyeket hoztak létre, és idegen karakterkészleteket használnak az URL-ek leplezéséhez. Különböző 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 becsapják a felhasználót a fontos adatok felfedezésére, mint például felhasználónév és jelszó, amelyet a támadó felhasználhat a rendszer vagy a fiók megsértésére. A csalás klasszikus változata magában foglalja az e-mailek

³³ i.m. „INTERPOL Report Shows Alarming Rate of Cyberattacks during COVID-19”.

³⁴ i.m. Muha és Krasznay, *Az elektronikus információs rendszerek biztonságáról vezetőknél: 9.*

³⁵ William Stallings és Lawrie Brown, *Computer Security: Principles and Practice* (Boston: Pearson, 2012).

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 domainel lettek regisztrálva. Az egyik fő árkódó jel az URL cím lehet, amely ilyenkor teljesen más, mint az eredeti oldal estében. 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 például küldhető egy HR-munkatársnak egy olyan melléklet, amely állítólag 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 ransomware mellékleteket.³⁶

Csoportosítani lehet az adathalász támadásokat az elkövetés módja szerint is:

- Az első, amit meglehet 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 adathalász oldal, 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 ezáltal célzottabb támadást tudnak végrehajtani.
- A bálna-adathalászat a célzott adathalászat egyik formája, amely a nagyon nagy „halakra” - vezérigazgatókra vagy más nagy értékű célpontokra - irányul. E

³⁶ Maria Korolov, „93% of Phishing Emails Are Now Ransomware”, CSO Online, 2016. június 1., Letöltés dátuma: 2020. szeptember 25. <https://www.csoonline.com/article/3077434/93-of-phishing-emails-are-now-ransomware.html>.

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.³⁷ Ezekben az e-mailekben a támadók az Egészségügyi Világszervezet tagjának (WHO) vagy egészségügyi szakembernek kiadva hivatkoznak magukra, 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 a például ".rtf" kiterjesztésű fájlokra.³⁸

- Vishing (Telefonos adathalászat): A távoliügyintézés (például Távegészségügy) normává válik 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 támogatási csalások útján. Fény derül arra is, hogy ezen támadók visszaélnek az IP (Voice over IP, VoIP) szolgáltatásokkal, hogy átverjék az egyéneket a nem létező szolgáltatások kifizetéséért vagy személyes adataik (például bankszámladataik, társadalombiztosítási számaik) megszerzéséért.
- Kiszolgáltatottság kiaknázása: A meglévő társadalmi távolságtartási követelmények eredményeként szüneteltek az olyan szervezetek, 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 továbbiakban 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

³⁷ Saqib Hakak és mtsai., „Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies”, *IEEE Access* PP (2020. június 30.): 1–1, <https://doi.org/10.1109/ACCESS.2020.3006172>.

³⁸ Cybersecurity and Infrastructure Security Agency, „COVID-19 Exploited by Malicious Cyber Actors | CISA”, 2020. április 8., <https://us-cert.cisa.gov/ncas/alerts/aa20-099a>.

bűnözők azonosítják és kihasználják a fent említett rendszerek és platformok sebezhetőségét.

- Dezinformáció és pánikkeltés: Számos közösségi média kampányt figyeltek meg a népszerű közösségi média platformokon is, mint például a Facebook, a WhatsApp és a LinkedIn, ahol hamis vagy félrevezető információkat tettek közzé. Ilyen például egyes gyógyszerek hatékonyságát a COVID-19 ellen, vagy a tehén vizeletének fogyasztása megakadályozhatja a COVID-19 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 készítsenek 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 maszk használatot. Az ilyen dezinformálás könnyen vezethet gyorsabban növekedő esetszámokhoz és ezáltal növekvő halálesetekhez.³⁹

Rendelkezésre állás: *„annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.”*⁴⁰

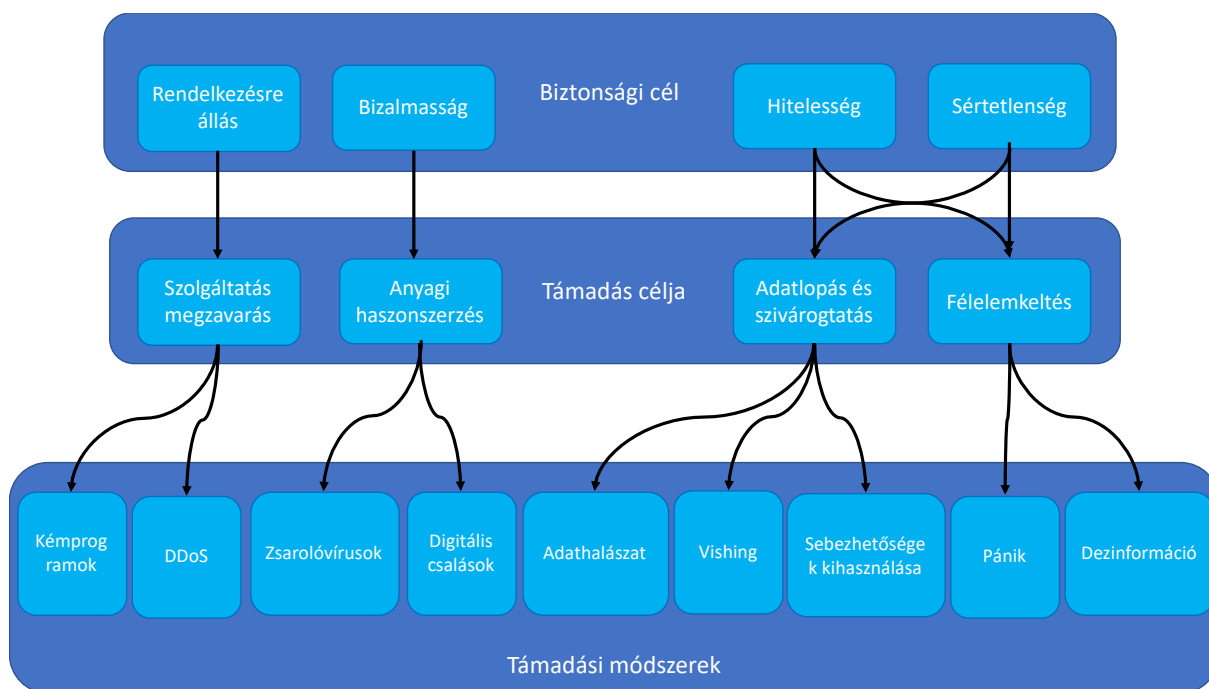
- DDoS támadások: a számos létező fenyegetés között a Distributed Denial of Service (DDoS) támadás viszonylag egyszerű, de nagyon erőteljes technika az intranet és az internetes erőforrások megtámadására. Ebben a támadásban a törvényes felhasználókat általában nagymennyiségű gépi erőforrás akadályoz 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.

³⁹ i.m. Hakak és mtsai., „Have You Been a Victim of COVID-19-Related Cyber Incidents?”

⁴⁰ i.m. Muha és Krasznay, *Az elektronikus információs rendszerek biztonságáról vezetőknak.*: 9.

Ezért alából ez egyes szolgáltatások így nagyobb terhelést kapnak mint, ami vírus előtt megszokott volt.⁴¹

- Kémprogram-támadások: A kémprogram egy olyan rosszindulatú program, amelyet más rendszerek titkos információinak megszerzésére használnak. Például a COVID-19-hez kapcsolódó nyomkövető-alapú alkalmazásokat állítólag kémprogram-alapú applikációkba ágyazták a felhasználók tevékenységének nyomon követésére.



11. ábra A COVID-19 alatt megjelent támadások csoportosítása (sajátszerkesztés, forrás: Saqib Hakak és mtsai.)

A fenti adatok alapján a támadásokat összegezve, a T2-es hipotézisem, hogy a koronavírus megjelenésével, nem jelentek meg teljesen új fenyegetések, viszont a már eddig jelenlévőket, sokkal szofisztikáltabban használják a támadók. Így a H2 hipotézisem miszerint „Feltételezem, hogy a vírus hatására új fajta fenyegetések nem jelentek meg, azonban a meglévők számában növekedés mutatható ki, és megjelenésük szofisztikáltabb, mint eddig.” helyt áll.

⁴¹ Iman Sharafaldin és mtsai., in *Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy* (International Carnahan Conference on Security Technology, 2019), 8, <https://doi.org/10.1109/CCST.2019.8888419>.

3.2.Kockázatkezelés

Egy szervezet működése során számos különböző fajta kockázatokkal néz szemben. A kockázatok csoportosításában Megyeri Lajos és Farkas Tibor osztályozását vettem alapul, amely a hatás szerint 2 csoportja osztja a kockázatokat:

- egyszerű (tiszt, pure) kockázatok, amelyek lehetséges kimenetelei a következők lehetnek:
 - kár, veszteség következik be;
 - vagy nem következik be semmilyen változás.
- összetett (speculative) kockázatról akkor beszélünk, ha következő három értéket veheti fel:
 - kár, veszteség következik be;
 - nem történik változás;
 - nyereség, gyarapodás az eredmény. ⁴²

Maga a kockázat értékelésére, illetve kezelésére számos módszertan létezik, teljesség igénye nélkül például Consultative, Objective & Bifunctional Risk Analysis (COBRA), Cost-of-Risk Analysis (CORA), Central Computer and Telecommunications Agency (CCTA) Risk Analysis and Management Methodology (CRAMM), Information Security Risk Analysis Method (ISRAM), ISO 3100.⁴³

ISO 3100

A felsorolt módszertanok az ISO 3100 szabvány nemzetközileg igen elismert és használatos a magán- és közszektorban egyaránt. A vizsgálatomban használt pontos szabvány az MSZ ISO 31000:2018. A szabvány 3 fő pilléren nyugszik, az első maga az értékrendszer, amelyet a szabvány képvisel és elvár. Ezen értékeket a szervezeten belül meg kell teremteni és védeni szükséges. Ezen értékeken alapszik a keretrendszer, amely létrehozásának célja a kockázatmenedzsment beillesztésének elősegítése a szervezet jelentős tevékenységeibe és funkcióiba. Illetve értékeken alapszik maga a folyamat is, amely a politikák, az eljárások és a

⁴² MEGYERI Lajos és FARKAS Tibor, „Kockázatkezelés, tudomány vagy kuruzslás”, *Hadmérnök* 12, sz. 3 (2017. szeptember 25.): 198–209.

⁴³ Ming-Chang Lee, „Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method”, *International Journal of computer science and information technology* 6 (2014. március 1.): 29–45, <https://doi.org/10.5121/ijcsit.2014.6103>.

gyakorlatok módszeres alkalmazását foglalja magában a következő területeken: kommunikáció és konzultáció, a környezet kialakítása, a kockázatok felmérése, kezelése, figyelemmel kísérése, átvizsgálása, feljegyzése és jelentéskészítése.⁴⁴ Látható a lenti ábrán, hogy az alapelvek mind a folyamatot, mind a keretrendszert befolyásolják, viszont ezen kettő rész kölcsönösen hatással van egymásra.

Alapelvek a következők, amelyeken ezen módszertan nyugszik:

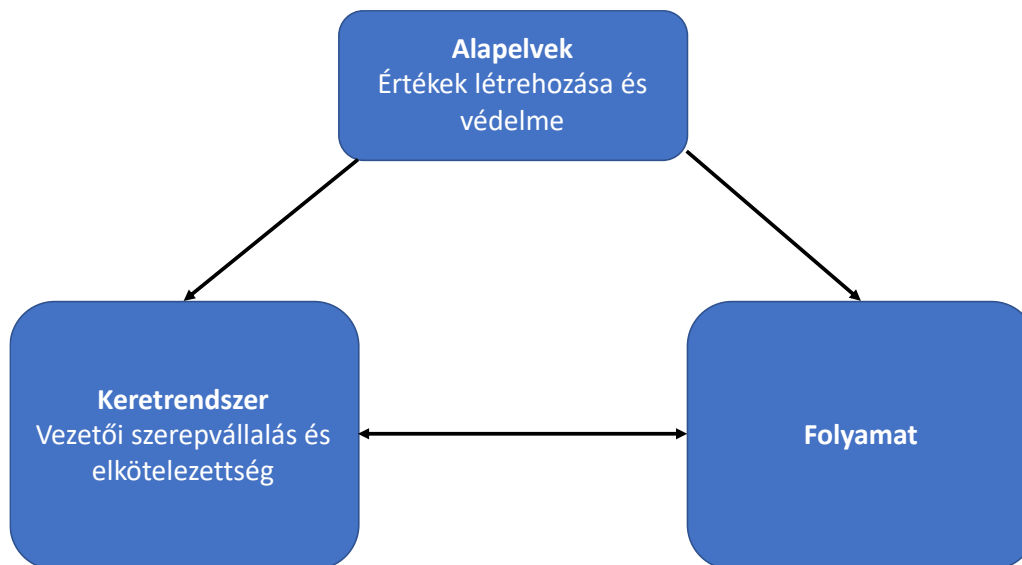
- integrálás;
- strukturáltság;
- testre szabottság;
- minden területre kiterjedtség;
- dinamikusság;
- legjobb elérhető információk;
- emberi és kulturális tényezők;
- folyamatos fejlesztés.

Ezek alapján a következő fő lépéseket lehet azonosítani kockázatkezelés során:

1. A kontextus létrehozása a vállalati célok meghatározásával.
2. Kockázat azonosítása, nevezetesen minden olyan kockázat azonosítása, amely befolyásolhatja az adott szervezet céljának elérését
3. Kockázatelemzés, az azonosított kockázatok lehetőségeinek és hatásainak elemzése.
4. A kockázatértékelés célja a kockázatelemzés eredményeinek összehasonlítása a kockázati kritériumokkal annak meghatározása érdekében, hogy a kockázatkezelést hogyan alkalmazzák.
5. Kockázatkezelés a szervezet által végzett folyamat a kockázat megszüntetése vagy a kockázat mérséklése érdekében. Amely során a kockázat lehetőségét vagy hatását csökkenteni lehet, a kockázatot harmadik felekre át lehet ruházni és a kockázatot el lehet fogadni.
6. A kommunikáció és a konzultáció olyan folyamat, amelyet úgy hajtanak végre, hogy a kockázatkezelési folyamat megfeleljen a szervezet által kitűzött céloknak.⁴⁵

⁴⁴ „MSZ ISO 3100:2019” (MAGYAR SZABVÁNYÜGYI TESTÜLET, é. n.).

⁴⁵ L.Y. Banowosari és B.A. Gifari, „System Analysis and Design Using Secure Software Development Life Cycle Based On ISO 31000 and STRIDE. Case Study Mutiara Ban Workshop”, 2019, <https://doi.org/10.1109/ICIC47613.2019.8985938>.



12. ábra Alapelvek, keretrendszer és folyamat viszonya az ISO 3100 keretrendszerben (sajátszerkesztés, forrás: ISO 3100)

CRAMM:

A CRAMM egy kvalitatív kockázatelemzési és -kezelési eszköz, amelyet az Egyesült Királyság kormányának Központi Számítógép- és Távközlési Ügynöksége fejlesztett ki 1985-ben annak érdekében, hogy a kormányzati részlegeknek módszert biztosítson az információs rendszerek biztonsági felülvizsgálatához. Az eszközt, amely mára már jelentősen átdolgozott, később kereskedelmi forgalomba hozták, és most egy brit vállalat „CRAMM Manager” néven értékesíti. Körülbelül 500 példány van használatban 20 országban, beleértve a kereskedelmi szervezeteket is. A CRAMM mindenféle szervezetben használható a következőre:

- Az információs rendszerek és hálózatok biztonsági vagy vészhelyzeti beruházásainak igazolására a vezetői szintű fellépés szükségességének kimutatására, számszerűsíthető eredményekkel, és a szervezet-specifikus kockázatelemzésből származó ellenintézkedések alapján, vagy;
- a ISO 27001 szabvány alkalmazásának bizonyítása a tanúsítási folyamat során. Ugyancsak referenciaértéknek tekinthető a szervezetek számára a kockázat- és készenléti menedzsment szempontjából. A CRAMM felülvizsgálatát három szakaszra lehet bontani:
 - eszközök azonosítása és értékelése;
 - fenyegetések és sérülékenységek azonosítása, kockázatok kiszámítása;

- az ellenintézkedések meghatározása és rangsorolása.

1. szakasz

A biztonság célkitűzéseinek meghatározása a következők révén:

- határ definiálása a kockázatértékelés vizsgálatához;
- a rendszer részét képező fizikai eszközök azonosítása és értékelése;
- a felhasználók által birtokolt adatok „értékének” meghatározása a nem elérhetőségből, megsemmisítésből, nyilvánosságra hozatalból vagy módosításból eredő lehetséges üzleti hatások;
- a rendszer részét képező szoftvereszközök azonosítása és értékelése.

2. szakasz

A javasolt rendszer kockázatainak értékelése a biztonságra vonatkozó követelmények szerint:

- a rendszert érintő fenyegetések típusainak és szintjeinek meghatározása és értékelése;
- a rendszer kiszolgáltatottságának felmérése az azonosított fenyegetésekkel szemben;
- a fenyegetés- és sebezhetőségértékelések, továbbá az eszközértékek kombinálása a kockázatok mértékének kiszámításához.

3. szakasz

Azon ellenintézkedések meghatározása és kiválasztása, amelyek arányosak a 2. szakaszban kiszámított kockázatok mértékével. A CRAMM egy nagyon nagy ellenintézkedési-könyvtárat tartalmaz, amely több mint 3000 részletes ellenintézkedést tartalmaz, több mint hetven logikai csoportosításba rendezve.⁴⁶

ISRAM

Az ISRAM célja az információbiztonsági problémák okozta kockázat felmérése. E cél elérése érdekében az ISRAM-ot a problémával kapcsolatos közvéleménykutatással hajtják végre. A felmérés az információbiztonsági problémával kapcsolatos kérdésekből áll. A felmérés kérdéseinek megválaszolására vezető, technikai személyek és általános felhasználók jelentkezhetnek. A felmérés célja az információbiztonsági probléma rendszerre vagy

⁴⁶ Yazar Zeki, „A Qualitative Risk Analysis and Management Tool - CRAMM” (SANS Institute, 2002), <https://www.sans.org/reading-room/whitepapers/auditing/paper/83>.

szervezetre gyakorolt hatásának megértése. Az ISRAM strukturált állapot-elemzést készít az információbiztonsági probléma okozta kockázat felmérésére.

Az ISRAM hét fő lépésből áll. Ebből a hét lépésből az első négy lépés a felmérés előkészítési szakaszába tartozik, az ötödik a felmérés lebonyolítása, az utolsó két lépés pedig az eredmények összegyűjtésének és értékelésének fázisa. Az ISRAM felmérés-előkészítési szakaszában meghatározzák a kérdéseket, a kérdések számát, a kérdések súlyértékét, a válaszváltások számát és a választások számértékeit. Végül elkészítik a kockázati táblázatokat.

Az első lépésben az információbiztonsági probléma fennállását észlelik. Az első lépés után az ISRAM folyamat két párhuzamos részfolyamatra oszlik. Ezen alfolyamatok egyikét a biztonsági rés paraméter előfordulásának valószínűségének vizsgálatára, a másikat a biztonsági rés paraméter bekövetkezésének következményeinek vizsgálatára hajtják végre.

A második lépésben felsorolásra kerülnek azok a tényezők, amelyek befolyásolhatják a biztonsági incidensek előfordulásának valószínűségét. A kockázati paraméter összes lehetséges tényezőjének felsorolása után a súlyértékeket kijelölik a tényezőkhoz. Az egyik tényező nagyobb hatással lehet az előfordulás valószínűségére, mint a másik, ezért vannak meghatározva a tényezők súlyértékei.

A harmadik lépésben a tényezőket felmérési kérdésekké konvertálják, és minden kérdésre meghatározzák a válaszváltási lehetőségeket. Minden kérdésnek különböző számú választási lehetősége lehet. A választások számát a kockázatelemzőnek kell meghatároznia a kérdések és az elemzett eset szerint. A válaszok meghatározása után numerikus értékeket rendelnek ezekhez.

A negyedik lépésben két kockázati táblázatot készítenek az előfordulási és bekövetkezési táblázatot. A kockázati táblák létfontosságúak a felmérés eredményeinek kvantitatív elemzéséhez. A kockázati táblázat a tömeges felmérés eredményét értelmes, kvantitatív és skálázott értékekké konvertálja. Ehhez egy kockázati táblázat tartalmazza az összes lehetséges felmérés eredményét, amely egyetlen felmérésből elérhető. A kockázati táblázatok a fő referenciapontok a felmérés eredményeinek értékeléséhez. Megakadályozzák a zavarokat, miközben kvantitatívan értékelik a felmérés eredményeit. A kockázati táblázat összekapcsolja a felmérés eredményét és a vizsgált kockázati paraméter mennyiségi értékét.

A felmérést a kockázati táblázatok elkészítésének befejezése után végzik, ez az ISRAM ötödik lépése. Két kockázati paraméter kérdését fel lehet adni egy felmérésben, vagy lehetőség van

külön felmérések elvégzésére két kockázati paraméterre vonatkozóan. Ebben az esetben a résztvevők száma két felmérésnél eltérő lehet.

A hatodik lépésben az ISRAM képletét alkalmazzák, hogy a megválaszolt felmérésekből egyetlen mennyiségi kockázati eredményt kapjanak.

A hetedik lépés az ISRAM értékelési szakasza. Az értékelési szakaszban nemcsak a hatodik lépésben kapott numerikus felmérés eredményét értékeli, hanem a felmérés kérdéseire adott válaszokat is elemzi.⁴⁷

3.3. Lehetséges kockázat csökkentő lépések bemutatása

Jelen fejezet arra próbál választ adni, hogy ezeknek a fenyegetéseknek a kockázatát hogyan lehet csökkenteni konkrét lépésekkel. A fejezetben külön kitérek a távolimunkavégzés biztonságosabbá tételére is.

Lehetséges általános, irányelvi megoldások:

- Információforrás validálása: A ransomware támadások enyhítésének egyik lehetséges megközelítése az, hogy harmadik féltől származó alkalmazásokat megvizsgáljuk és oktatjuk a felhasználókat, ezáltal lehetővé téve számukra megbízható források azonosítását. Az alkalmazásértékelések szintén jelezhetik az alkalmazások megbízhatóságát.
- Vishing felismerése és blokkolása: a VoIP-szolgáltatók hatékony szerepet játszhatnak az átveréses hívás fenyegetések mérséklésében, például segítséget nyújtanak a felhasználók tudatosságának növelésében, valamint a potenciálisan csaló hívók aktív azonosításában és blokkolásában is segít (például red flag indikátoron alapuló jelzés robóhívások alapján). Mivel, hogy nem minden felhasználónak van meg a kellő biztonságtudatossága, a járványok során fokozni lehet az ingyenes oktatási kampányokat, amelyek irányulhatnak például a személyes adatok megosztásának veszélyeire telefonhívások útján és a túl jó online ajánlatok figyelmen kívül hagyására is (például ingyenes orvosi vizsgálatok és oltások). A másik lehetséges enyhítési stratégia magában foglalja a AI alapuló anti-spam detektorok tervezését és fejlesztését.

⁴⁷ Bilge Karabacak és Ibrahim Sogukpinar, „ISRAM: Information Security Risk Analysis Method”, *Computers & Security* 24, sz. 2 (2005. március 1.): 147–59, <https://doi.org/10.1016/j.cose.2004.07.004>.

A korábbi járványok adatainak felhasználásával AI-alapú botot lehet fejleszteni a hívások fogadására (a felhasználók helyett) és annak ellenőrzésére, hogy a bejövő hívás spam-e vagy sem.

- Nagyfokú nemzetközi együttműködés: nyilvánvalóan különböző országok és kormányok kollektív erőfeszítéseire van szükségünk a járványok idején, például a jelenlegi COVID-19 vészhelyzet esetén. A világjárvány-témájú számítógépes fenyegetések leküzdése érdekében erőfeszítésekre és ellenintézkedésekre van szükség a nemzetközi közösség részéről, ideértve egy nemzetközi munkacsoport felállítását is, amely megkönnyíti a jelenlegi kiberfenyegetésről szóló híradások (pl. fenyegetésvektorok és technikák) megosztását. A pénzügyi támogatás fontosságát nem lehet lebecsülni a nemzetközi együttműködési tevékenységekben (pl. kiberhigiénia oktatás). Az enyhítési kezdeményezések finanszírozásához a közösség és a nemzetközi szervezetek támogatására kell törekedni. Például olyan szervezetek pénzügyi támogatása, mint a Nemzetközi Valutaalap (IMF), a felhasználható eszközök és készségek fejlesztésére a kiberfenyegetések mérsékléséhez.
- Álhírek visszaszorítása: fontos egy erős kollaborációban a közösségi média platformokkal egységben fellépni az álhírek ellen, ami ebben a vírusos helyzetben sok nehézséget okozhat, mivel az egyes hírekről, ami például a vírus tulajdonságáról szól eldönteni, hogy valós-e vagy sem elég nehéz. Viszont ezért kellene egy közös munkacsoportban több területen dolgozó szakembereknek együttműködni (például: orvos, biztonsági szakértő, szociológus).
- Biztonságos és frissített rendszerek: tekintettel arra, hogy a szociális távolságtartó intézkedések miatt a házakban egyre növekszik az egyes informatikai rendszerek használata, erőfeszítéseket kell tenni az otthoni rendszerek naprakészen tartására és biztonságának biztosítására. A biztonsági szervezetek is szerepet játszhatnak, például azzal, hogy a járványok idején nem számolnak fel előfizetési díjakat az erre rászorulóknak esetében a biztonsági termékeikért (például Rosszindulatú szoftverek ellen).
- Megfelelő kockázatkezelési keretrendszer kialakítása: a kockázatkezelési keretrendszer hatékony módszer a fenyegetéssel kapcsolatos kockázatok elérésére, mérséklésére és értékelésére. A COVID-19 járványnak megfelelően egy olyan, keretet kell kialakítani, amely rövid időn belül megvalósítható. Egy ilyen keretrendszernek robusztusnak, skálázhatónak, időhatékonynak és pontosnak kell lennie, amelyet technikai / nem

technikai számítógépes szakemberek könnyen követhetnek, akár otthoni, akár irodai környezetben.⁴⁸

A következőkben az Ausztráliai Kiberbiztonsági Központ által kialakított ajánlás alapján rendszerezett követelések kerülnek részletezésre⁴⁹, amelyek segítséget tudnak nyújtani egy szervezetnek, abban, hogyan is lehetne egy biztonságos távoli munkavégzési környeztetett kialakítani.

A következő 4 táblázatban különböző aspektus szerinti lépések szerepelnek, amelyek 3 téma alapján értékelésre kerültek. A következő értékelési szempontok jelennek meg:

A „Felhasználói ellenállás a stratégiával szemben” azt mutatja meg, hogy a felhasználók milyen szívesen fogadnák azt a lépést, az „Előzetes költségek mértéke (személyzet, szoftver és hardver)”, „Folyamatos karbantartási költség mértéke” a szükséges költség szinteket mutatja meg. Az utóbbi 3 vektor a következő értékeket vehetik fel: „Alacsony”, „Közepes”, „Magas”, „Nagyon magas”.

⁴⁸ i.m. Hakak és mtsai., „Have You Been a Victim of COVID-19-Related Cyber Incidents?”

⁴⁹ „Strategies to Mitigate Cyber Security Incidents | Cyber.gov.au”, 2017. február 1., Letöltés dátuma: 2020. október 21., <https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents>.

5. táblázat Stratégiák a kiberbiztonsági események enyhítésére - Enyhítő stratégiák a rosszindulatú programok célba érésének és feladatának végrehajtásának megakadályozására (sajátszerkesztés, forrás: Australian Cybersecurity Center)

Enyhítő stratégiák a rosszindulatú programok célba érésének és feladatának végrehajtásának megakadályozására			
Enyhítési stratégia	Felhasználói ellenállás a stratégiával szemben	Előzetes költségek mértéke (személyzet, szoftver és hardver)	Folyamatos karbantartási költség mértéke
Alkalmazásvezérlés a nem jóváhagyott / rosszindulatú programok, (beleértve az .exe, a DLL, a szkriptek és a telepítők) futtatásának megakadályozására.	Közepes	Magas	Közepes
Alkalmazások javítása (pl. Flash, webböngészők, Microsoft Office, Java és PDF nézők) Javítsa / enyhítse a „rendkívüli kockázatú” biztonsági résekkel rendelkező eszközöket 48 órán belül. Használja az alkalmazások legújabb verzióját.	Alacsony	Magas	Magas
Microsoft Office makróbeállításainak konfigurálása Blokkolja a makrókat az internetről, és csak ellenőrzött makrókat engedélyezhet korlátozott írási hozzáféréssel vagy megbízható tanúsítvánnyal digitálisan aláírva.	Közepes	Közepes	Közepes
Felhasználói alkalmazások megerősítése Konfigurálja a webböngészőket a Flash-t (ideális esetben távolítsa el), a hirdetések letiltása a böngészőkben. Tiltsa le a Microsoft Office, a webböngészők és a PDF-nézők szükségtelen szolgáltatásait.	Közepes	Közepes	Közepes
A sandboxban futó e-mailek és webtartalmak automatizált dinamikus elemzése Blokkolja, ha gyanús magatartást (pl. Hálózati forgalmat, új vagy módosított fájlokat vagy más rendszerkonfigurációs változásokat) észlelnek.	Alacsony	Magas	Közepes
Webtartalom szűrése Csak jóváhagyott típusú webtartalmakat és jó reputációval rendelkező webhelyeket engedélyezhet. Blokkolja a rosszindulatú domainekhez és IP-címekhez, hirdetésekhez és ingyenes domainekhez való hozzáférést.	Közepes	Közepes	Közepes
Az operációs rendszer általános kihasználásnak csökkentése pl. Az adatfuttatás megelőzése (DEP).	Alacsony	Alacsony	Alacsony

Enyhítő stratégiák a rosszindulatú programok célba érésének és feladatának végrehajtásának megakadályozására			
Enyhítési stratégia	Felhasználói ellenállás a stratégiával szemben	Előzetes költségek mértéke (személyzet, szoftver és hardver)	Folyamatos karbantartási költség mértéke
Szerver alkalmazások megerősítése, különösen az interneten elérhető webalkalmazások és adatbázisok esetében, valamint olyan alkalmazásoknál is, amelyek fontos (érzékeny / magas rendelkezésre állású) adatokhoz férnek hozzá.	Alacsony	Közepes	Közepes
Az operációs rendszer megerősítése (beleértve a hálózati eszközöket is) szabványos működési környezet alapján, kikapcsolva a szükségtelen funkciókat (pl. RDP, AutoRun, LanMan,).	Közepes	Közepes	Alacsony
Jó hírnévvel rendelkező víruskereső szoftver használata A fájl fontosságának és digitális aláírásának ellenőrzése a végrehajtás előtt. Az átjárókhoz és a számítógépekhez különböző gyártók víruskereső szoftvereit használja.	Alacsony	Alacsony	Alacsony
E-mail tartalom szűrése Csak jóváhagyott mellékletfájlokat engedélyezhet (beleértve az archívumokat és a beágyazott archívumokat is). A hiperhivatkozások, a PDF és a Microsoft Office mellékletek elemzése / megtisztítása. Karanténba helyezi a Microsoft Office makrókat.	Közepes	Közepes	Közepes
Kontrollálja a cserélhető adathordozókat és a csatlakoztatott eszközöket Blokkolja a nem jóváhagyott CD / DVD / USB adathordozókat. Blokkolja a kapcsolatot jóváhagyatlan okostelefonokkal, táblagépekkel és Bluetooth / Wi-Fi / 3G / 4G / 5G eszközökkel.	Magas	Magas	Közepes
Blokkolja a hamis e-maileket A beérkező e-mailek ellenőrzéséhez használja a Sender Policy Framework (SPF) vagy a Sender ID elemet. Használjon „hard fail” SPF TXT és DMARC DNS rekordokat a szervezet domainjét hamisító e-mailek enyhítésére.	Alacsony	Alacsony	Alacsony
Felhasználói oktatás Kerülje az adathalász e-maileket (pl. Hamis weboldalakra történő bejelentkezés linkje), a gyenge jelszavakat, a jelszavak újrafelhasználását, valamint a nem jóváhagyott: cserélhető adathordozókat, csatlakoztatott eszközöket és felhőszolgáltatásokat.	Közepes	Magas	Közepes

Enyhítő stratégiák a rosszindulatú programok célba érésének és feladatának végrehajtásának megakadályozására			
Enyhítési stratégia	Felhasználói ellenállás a stratégiával szemben	Előzetes költségek mértéke (személyzet, szoftver és hardver)	Folyamatos karbantartási költség mértéke
Víruskereső szoftver naprakészen tartása a rosszindulatú programok azonosítására, egy olyan gyártótól, amely gyorsan frissítést ad az új rosszindulatú programokhoz.	Alacsony	Alacsony	Alacsony
TLS-titkosítás az e-mail szerverek között, hogyan megakadályozza az e-mailek lehallgatását és későbbi socila engineering célú felhasználását.	Alacsony	Alacsony	Alacsony

6. táblázat Stratégiák a kiberbiztonsági események enyhítésére - A kiberbiztonsági incidensek mértékének korlátozására szolgáló enyhítési stratégiák (sajátszerkesztés, forrás: Australian Cybersecurity Center)

A kiberbiztonsági incidensek mértékének korlátozására szolgáló enyhítési stratégiák			
Enyhítési stratégia	Felhasználói ellenállás a stratégiával szemben	Előzetes költségek mértéke (személyzet, szoftver és hardver)	Folyamatos karbantartási költség mértéke
Jogosultság kezelés A felhasználói feladatok alapján korlátozza az adminisztrációs jogosultságokat az operációs rendszerekre és alkalmazásokra. Rendszeresen vizsgálja felül a jogosultságok szükségességét.	Közepes	Magas	Közepes
Patch az operációs rendszerekre Frissítse a „rendkívüli kockázatú” biztonsági réseket tartalmazó számítógépeket (beleértve a hálózati eszközöket is) 48 órán belül. Használja a legújabb operációs rendszer verziót. Ne használjon nem támogatott verziókat.	Alacsony	Közepes	Közepes
Többfaktoros hitelesítés, beleértve a VPN-eket, az RDP-t, az SSH-t és az egyéb távoli hozzáféréseket, valamint az összes felhasználó számára, ha privilegizált művelet hajtanak végre, vagy hozzáférnek egy fontos (érzékeny / magas rendelkezésre állású) adattárhoz.	Közepes	Magas	Közepes
Tiltsa le a helyi rendszergazdai fiókokat, vagy rendeljen véletlenszerű és egyedi jelszavakat az egyes számítógépek helyi rendszergazdai fiókjaihoz, hogy megakadályozza a megosztott helyi rendszergazdai hitelesítő adatok használatát.	Alacsony	Közepes	Alacsony

A kiberbiztonsági incidensek mértékének korlátozására szolgáló enyhítési stratégiák			
Enyhítési stratégia	Felhasználói ellenállás a stratégiával szemben	Előzetes költségek mértéke (személyzet, szoftver és hardver)	Folyamatos karbantartási költség mértéke
Hálózati szegmentálás Ha csak nem szükséges, tagadja meg a számítógépek közötti forgalmat. A felhasználói feladatok alapján korlátozza a hálózati meghajtókhoz és az adattárakhoz való hozzáférést.	Alacsony	Magas	Közepes
Védje a hitelesítési adatokat Alapértelmezett jelszavak módosítása. Hosszú, összetett jelszavakat igénylése.	Közepes	Közepes	Alacsony
Nem állandó virtualizált sandbox környezet, amely megtagadja a hozzáférést a fontos (érzékeny / magas rendelkezésre állású) adatokhoz, kockázatos tevékenységekhez (pl. Webböngészés, valamint a nem megbízható Microsoft Office és PDF fájlok megtekintése).	Közepes	Közepes	Közepes
Szerver alkalmazások megerősítése, különösen az interneten elérhető webalkalmazások és adatbázisok esetében, valamint olyan alkalmazásoknál is, amelyek fontos (érzékeny / magas rendelkezésre állású) adatokhoz férnek hozzá.	Alacsony	Közepes	Közepes
Szoftver alapú tűzfal, blokkolja a bejövő, rosszindulatú / jogosulatlan hálózati forgalmat, és alapértelmezés szerint megtagadja a hálózati forgalmat (pl. Szükségtelen / jogosulatlan RDP és SMB / NetBIOS forgalom).	Alacsony	Közepes	Közepes
Kimenő webes és e-mailes adatvesztés megelőzése Blokkolja a nem jóváhagyott felhőszolgáltatásokat. Biztonsági szavakkal vagy adatmintákkal blokkolja és naplózza az e-maileket.	Közepes	Közepes	Közepes

7. táblázat Stratégiák a kiberbiztonsági események enyhítésére - A kiberbiztonsági események észlelésének és a reagálás mérséklési stratégiái (sajátszerkesztés, forrás: Australian Cybersecurity Center)

A kiberbiztonsági események észlelésének és a reagálás mérséklési stratégiái			
Enyhítési stratégia	Felhasználói ellenállás a stratégiával szemben	Előzetes költségek mértéke (személyzet, szoftver és hardver)	Folyamatos karbantartási költség mértéke
Folyamatos eseményfelismerés és reagálás az engedélyezett és megtagadott számítógépes események, hitelesítés, fájlhozzáférés és hálózati tevékenység központsított, idővel szinkronizált naplóinak automatizált azonnali elemzésével.	Alacsony	Nagyon magas	Nagyon magas
Gépalapú behatolás-észlelő / -megelőző rendszer a rendellenes viselkedés azonosítására a program futtatása során.	Alacsony	Közepes	Közepes
Végpont-észlelő és reagáló szoftver minden számítógépen központilag naplózza a rendszer viselkedését és megkönnyíti az események reagálását. A Microsoft ingyenes SysMon eszköze belépő szintű opció.	Alacsony	Közepes	Közepes
Hálózati alapú behatolás-észlelő / -megelőző rendszer, amely aláírásokat alkalmaz a rendellenes forgalom azonosítására mind belsőleg, mind a hálózati határokat átlépésével.	Alacsony	Magas	Közepes
Rögzítse a hálózati forgalmat Rögzítse a hálózati forgalmat a fontos adatokat tároló vagy kritikus fontosságú eszköznek számító vállalati számítógépekre és onnan, valamint a hálózati határokon áthaladó hálózati forgalmat az események észlelése és elemzése céljából.	Alacsony	Magas	Közepes

8. táblázat Stratégiák a kiberbiztonsági események enyhítésére - Az adatok és a rendszer rendelkezésre állásának helyreállítására szolgáló enyhítési stratégiák (sajátszerkesztés, forrás: Australian Cybersecurity Center)

Az adatok és a rendszer rendelkezésre állásának helyreállítására szolgáló enyhítési stratégiák			
Enyhítési stratégia	Felhasználói ellenállás a stratégiával szemben	Előzetes költségek mértéke (személyzet, szoftver és hardver)	Folyamatos karbantartási költség mértéke
Biztonsági mentés készítése Naponta készít biztonsági mentést a fontos új / megváltozott adatokról, szoftvekről és	Alacsony	Magas	Magas

Az adatok és a rendszer rendelkezésre állásának helyreállítására szolgáló enyhítési stratégiák			
Enyhítési stratégia	Felhasználói ellenállás a stratégiával szemben	Előzetes költségek mértéke (személyzet, szoftver és hardver)	Folyamatos karbantartási költség mértéke
konfigurációs beállításokról. Tesztelje a helyreállítást évente és az informatikai infrastruktúra változásakor			
Üzletmenet-folytonossági és katasztrófa utáni helyreállítási tervek, amelyeket tesztelnek, dokumentálnak és rendelkeznek ezekből nyomtatott példánnyal és offline tárolt elektronikus másolattal. Összpontosítson a legmagasabb prioritású rendszerekre és a helyreállítandó adatokra.	Alacsony	Magas	Közepes
Rendszer-helyreállítási képességek, virtualizálás snapshot biztonsági másolatokkal, az operációs rendszerek és alkalmazások távoli telepítése számítógépekre, jóváhagyott vállalati mobilitás és helyszíni gyártói támogatási szerződések.	Alacsony	Magas	Közepes

9. táblázat Stratégiák a kiberbiztonsági események enyhítésére - A rosszindulatú belső személyek megelőzésére vonatkozó mérséklési stratégia (sajátszerkesztés, forrás: Australian Cybersecurity Center)

A rosszindulatú belső személyek megelőzésére vonatkozó mérséklési stratégia			
Enyhítési stratégia	Felhasználói ellenállás a stratégiával szemben	Előzetes költségek mértéke (személyzet, szoftver és hardver)	Folyamatos karbantartási költség mértéke
Személyzeti menedzsment, pl. Folyamatos kivizsgálás, különösen a kiváltságos hozzáféréssel rendelkező felhasználók számára, azonnali letiltás a távozó felhasználók összes fiókja tekintetében, és emlékeztetés alkalmazása a felhasználók körében a biztonsági kötelezettségeikről és esetleges büntetési tényezőkről.	Magas	Magas	Magas

3.4. Következtetés

Összegezve azt lehet mondani, hogy a koronavírus első hulláma idején felütötte a fejét az összes nagy támadási forma, amely kifejezetten szofisztikáltan kerültek kialakításra, így bebizonyosodott a H2 hipotézisem ezáltal. Azt lehet mondani a fejezetben megjelent adatokból,

hogy a támadók igen gyorsan és nagy számban használták ki a koronavírus adottságait, továbbá, hogy a védekezésben olyan többszintű feladatok szerepelnek, amelyeknek kialakítása nagy humán és pénzügyi tőkét igényel. Pont ez az egyik legnagyobb kockázat, mivel az első fejezet rámutatott arra, hogy a gazdaság válságban van, ami azt jelenti, hogy a vállalatok nem tudnak vagy nem akarnak nagy befektetéseket eszközölni annak érdekében, hogy a biztonsági lemaradását behozza, illetve egy biztonságos távoli munkavégzést tudjon kialakítani a munkavállalói számára.

4. FEJEZET- KÉRDŐÍV

4.1. Kérdőív bemutatása, észrevételek leírása

Empirikus kutatásom gerincét a kérdőívem jelentette, amelyet hazai információbiztonságban dolgozó személyek körében töltettem ki. A kérdőívem kialakításához több nemzetközi tanulmányt vizsgáltam meg a kérdéskörben.^{50 51 52 53} 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, amelyen belül kitértem arra is, hogy milyen típusú fenyegetések jelentek meg a szervezeten belül, illetve a megkérdezett szakemberek az egyes fenyegetési típusokat mennyire tartják kockázatosnak saját szervezetükre nézve. A kérdőív 2 fő részből áll, az első rész általános információkra kérdez rá: itt olyan kérdések találhatók meg, amelyek magára a kitöltő személyre vonatkoznak (melyik szektorban dolgozik; milyen végzettséggel 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 szabályzat követési hajlandósága volt a téma (távmunka volt-e engedélyezve; tettek-e külön intézkedést távmunka kapcsán; milyen típusú fenyegetést milyen kockázatosan kitélnék meg szervezetre nézve; a munkavállalók szabálykövetők-e). A kérdéseket teljes egészében megtalálható 3. számú mellékletben. A

⁵⁰ M. Rodbert, „Why organisational readiness is vital in the fight against insider threats”, *Network Security* 2020, sz. 8 (2020): 7–9, [https://doi.org/10.1016/S1353-4858\(20\)30092-1](https://doi.org/10.1016/S1353-4858(20)30092-1).

⁵¹ M.A. Ferrag, M. Babaghayou, és M.A. Yazici, „Cyber security for fog-based smart grid SCADA systems: Solutions and challenges”, *Journal of Information Security and Applications* 52 (2020), <https://doi.org/10.1016/j.jisa.2020.102500>.

⁵² U. Franke és J. Wernberg, „A survey of cyber security in the Swedish manufacturing industry”, in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 2020, 1–8, <https://doi.org/10.1109/CyberSA49311.2020.9139673>.

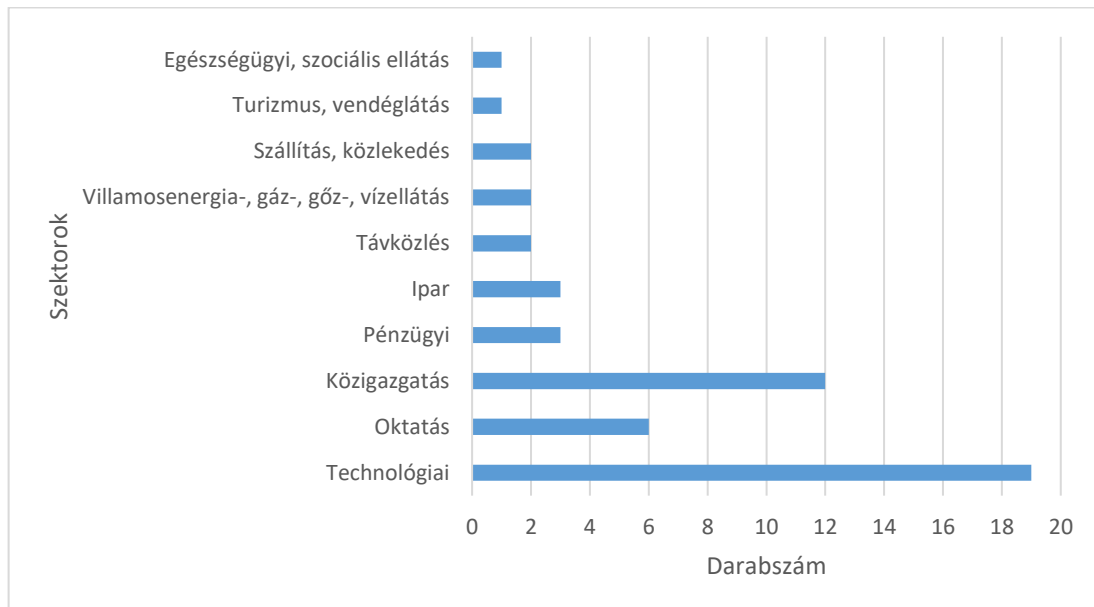
⁵³ i.m. Hakak és mtsai., „Have You Been a Victim of COVID-19-Related Cyber Incidents?”

kérdőívem természetesen anonim volt, mivel olyan adatot nem kértem, amivel ki lehet mutatni a kérdőív kitöltőjének személyazonosságát, így megfelel a 2011. évi CXII. törvénynek, és ezáltal az Általános Adatvédelmi Rendeletnek (General Data Protection Regulation GDPR).

A kérdőívem kiértékelésre az IBM SPSS Statistics 25 programcsomagot használtam, amiben az eredményeim egyrészét Kruskal-Wallis-próba alá vettem, továbbá egyes kérdések kiértékelést osztályozással végeztem el. Egyes kérdéseim keresztábrás kiértékelés alá akartam vetni, azonban khi négyzet próba azon feltétele nem teljesült, hogy az elvárt gyakoriság minden egyes cellában minimum 5 legyen. Kruskal-Wallis-próba egy típusa az 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 alatt egy tesztváltozót vizsgálunk, egy csoportosító változóval. A tesztváltozónak, és a csoportosító változónak is rangsorolt adatnak kell lenni. Fontosnak tartom kiemelni, hogy kutatásom során azért a Kruskal-Wallis próbát használtam nem pedig 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 a Asymp. Sig. változó vagy is 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 megvizsgáljuk a rangátlagot, amely megmutatja, a csoportosító változó értékeinek rangsorát a tesztváltozó értékeinek függvényében.

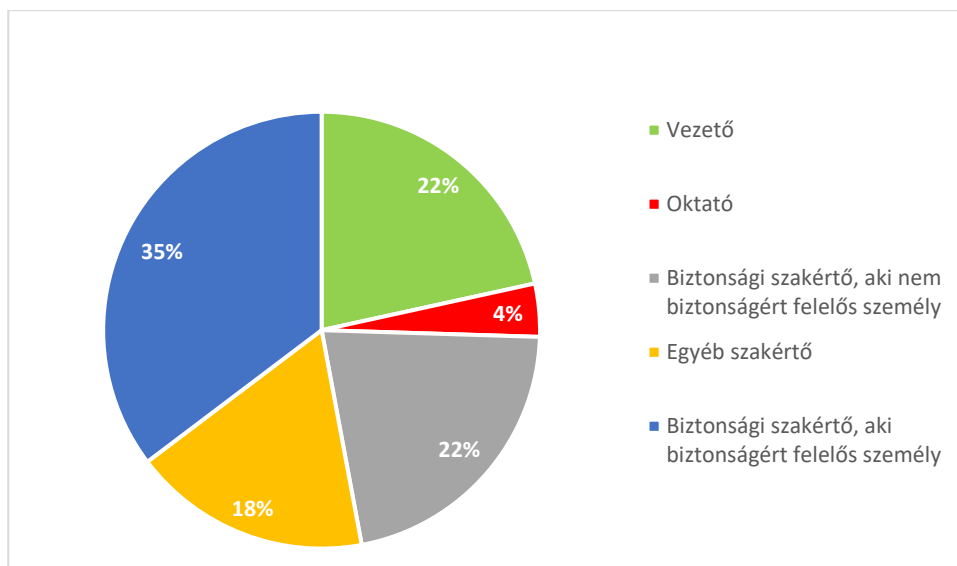
Kérdőívemet 51-en szakértő töltötte ki, jellegét tekintve nem reprezentatív a felmérés. A kitöltők legnagyobb számban a technológiai szektorból töltötték ki szám szerint 19 személy; ezt követte a közigazgatási szektor 12 kitöltővel; majd az oktatás 6; pénzügyi szektor és az ipar 3; és a szállítás, közlekedés; villamosenergia-, gáz-, gőz-, vízellátás; távközlés; 2 db 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) végzettsége 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 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.



13. ábra Kitöltők szektorbeli megoszlásai (db) (saját szerkesztés)

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, amely 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, Információ Biztonsági 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 18%-a Biztonsági szakértő, aki biztonságért felelős személy.



14. ábra Beosztás szerinti megoszlás (%) (sajátszerkesztés)

4.2. Fenyégetettségek, és a távmunka

A kérdőívemben megkérdeztem a szakembereket, hogy mekkora kockázati értéket adnának a következő támadások bekövetkezésére a következő 1 évben:

- 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 választás lehetőségek a következők voltak:

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

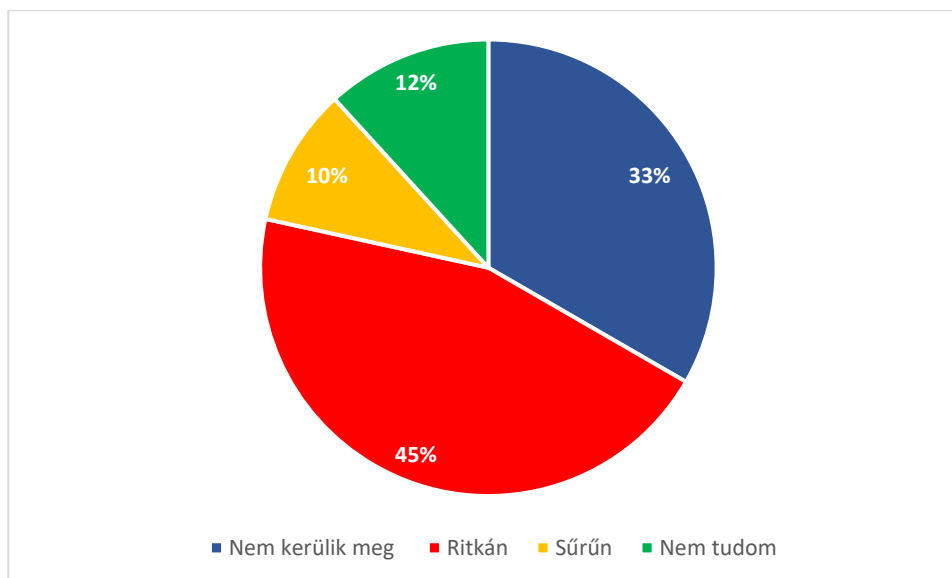
A szakértők legnagyobb számban közepes kockázati szintet jelöltek meg a támadásoknál szám szerint 84 szer; ezt követi 69-el az alacsony kockázati besorolás; majd 54-el az elhanyagolható

szintű besorolás; az utolsó előtti össz mennyiségben a magas kockázat 39-el és utolsó 3 darabban a nagyon magas kockázat. Egyetlen egy személy nem tudta valamely fenyegetést besorolni. Ebből látható, hogy a szakértők felkészültnek tartják szervezeteiket ezen támadásokra. Ezenfelül az is látható a 10. táblázatból, hogy összesen 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.

10. táblázat Egyes fenyegetések bekövetkezési valószínűségének kockázatai a szakértők véleménye szerint (db) (sajátszerkesztés forrás: kérdőív)

Mennyire tartja valószínűnek, hogy az Ön szervezete a következő 12 hónapban az alábbi incidensek valamelyikét elszenvedí						
	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 megsejgik-e a szabályokat, és ha igen akkor ezt milyen sűrűn teszik. A 12. ábrán is látható, hogy a válaszadók 33%-a szerint a szervezetben dolgozó munkavállalók nem kerülnek meg a szabályokat; 45% gondolja úgy, hogy ritkán, de megkerülnek a dolgozók a szabályokat; 10% az az arány a kitöltők esetében, akik azt mondják, hogy a szervezet munkatársai sűrűn megkerülnek a szabályokat és 12% nem tudta eldönteni ezt saját szervezetére nézve.



15. ábra Szabálmegkerülési gyakoriság (%) (sajátszerkesztés)

Mind a támadások kockázatára, mind a szabályszegés sűrűségére adott válaszokat megtisztítottam úgy, hogy kikerüljenek azon személyek válaszai, akik valamely kérdésnél nem tudom opciót választották, így marad 44 válsz, amit külön Kruskal-Wallis-próba alá vetettem. Kíváncsi voltam, hogy van-e összefüggés a megadott fenyegetéskere adott kockázati szint, illetve a szabálmegkerülés sűrűségének szintje között. A próba lefuttatását követően, ahol a csoportosító változó a szabálmegkerülési sűrűség, és a tesztváltozók az egyes támadások kockázatának mértéke volt, a 4. számú mellékletben megtalálható a tesztek részletes adatai. A 13. 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 szabálmegkerülés függvényében.

16. ábra Kruskal-Wallis-próba signfikanica eredménye (sajátszerkesztés, forrás: SPSS)

	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. Az látható, hogy a „Nem szándékos esemény, amely üzletmenet folytonosság megszakításával jár” változónál a legnagyobb rangátlagot a sűrű szabálmegkerülés kapta 29,60-as értékkel; ezt követte a ritka szabálmegkerülés 27,05-tel; majd a nem megkerülés 14,53-mal. Tehát ki lehet jelenti, hogy azon szakértők, akik szervezeténél a szabálmegkerülés sűrűn fordul elő nagyobb kockázati értéket adnak olyan nem szándékos esemény létrejöttére, amely az üzletfolytonosság megzavarását eredményezi.

Következő csoport az „Olyan támadás, amely az adatok megsértésével jár, és nyilvánossá válnak ezen adatok” volt. Itt is a legnagyobb rangátlaggal a sűrű szabálmegszegés áll 30,50-el; ezt követi a ritka 27,63-mal; majd 13,50-el a zárja a sort nem kerülnek meg csoport. Így itt is ki lehet jelteni, hogy azon szakértők, akik szervezeténél a szabálmegkerülés sűrűn fordul elő nagyobb kockázati értéket adnak olyan támadásokra, amelyek az adatok megsértésével jár és ezen adatok nyilvánosságra kerülhetnek.

„Az üzletmenet folytonosság megszakításával járó támadás” csoport estében is ugyan ez mondható el. Itt is a legnagyobb rangátlaggal a sűrű szabálmegszegés áll 30,20-el; ezt követi a ritka kategória 26,77-tel; és végül a nem kerülnek meg kategória 14,71-gyel. Tehát itt is kijelenthető ugyan az, hogy azon szakértők, akik szervezeténél a szabálmegkerülés sűrűn fordul elő nagyobb kockázati értéket adnak olyan támadásokra, amelyek az üzletmenet folytonosság megszakításával járnak.

Megvizsgáltam ugyan ezen rangátlagokat a „Távoli munkavégzést kihasználó támadások” csoportra. Ebben a vizsgálatban is ugyan ezen rangsort kaptam a következő értékekkel, sűrű 29,70; ritka 27,55; nem kerülnek meg 13,85. Így azon T5 tézisem született miszerint azon szakértők, akik szervezeténél a szabálmegkerülés sűrűn fordul elő nagyobb kockázati értéket adnak olyan támadásokra, amelyek a távoli munkavégzés során előfordulhatnak. Ezzel alátámasztottam a H5 hipotézisem: Feltételezem, hogy azon szakértők, akik szerint a szerevetükben dolgozók sűrűbben szegik meg a szabályokat kockázatosabbnak tartják a távmunkát, mint munkavégzési formát.



17. ábra Támadásonkénti rangátlag megoszlás (sajátszerkesztés forrás: SPSS)

4.3. Következtetés

Kérdőívem kiértékelését összegezve elmondható, hogy a kitöltők megfelelő képzettséggel rendelkeztek ahhoz, hogy pontosan meg tudják ítélni azt, hogy szerveztük, illetve szektoruk, milyen fenyegetésekkel néz szembe, és ezen fenyegetések milyen szintű kockázattal járnak. Legtöbben a technológiai szektorból töltötték ki, ezt követte a közigazgatás. Látható az is, hogy ezen szakértők legnagyobb részben a távmunka kiberbiztonsági kihívásai miatt aggódnak, és ezen aggodalmuk mértéke összefügg a szervezetben dolgozó személyek szabálykövetésével. Ki lehet azt is jelenti, hogy azon szakértők, akik szerint a szervezetükben dolgozók sűrűbben szegik meg a szabályokat kockázatosabbnak tartják a távmunkát, mint munkavégzési formát.

ÖSSZEGZÉS

Dolgozatom összegzéseként kijelenthető, hogy a koronavírus életünk minden területén nagy változást hozott. Ezen változások nem csak egyéni szinten jelentek meg, hanem társadalmi szinten is. Az első hullám idején nem volt egy egységes nemzetközi álláspont a pandémia kezelésére, minden állam saját területén próbálta megoldani a vírushelyzetet. Tavasszal sok állam szigorú intézkedéseket vezetett be, mint például kijárási korlátozás, amely a gazdaság visszaesését eredményezte. Ezen gazdasági visszaesés hatásának mértéke államonként elétert, viszont visszaesés a legtöbb helyen tapasztalható. A vírus terjedésének lassításában nagy szerepet játszott a távoli munkavégzésre való átállás. Dolgozatomban elemeztem a hazai, európai, egyesült államokbeli, és finn jogszabályokat. Az látható, hogy a hazai jogforrás csak keretszabályokat fogalmaz meg, főleg a munkavállalóra, illetve a munkáltatóra bízva a részletszabályozás kialakítását. A keretrendszeri szabályozás azért is volt kielégítő eddig Magyarországon mert a szervezetek 2019-ig igen kis számban alkalmazták a távmunkát. Európa 2002-óta szabályozási szinten rendelkezik a távoli munkavégzés követelményeiről, igaz itt is a szabályozás csak kereteket ad. Az látható, hogy hazánk ezen szabályozást vette át és ültette a hazai jogszabályba. Az Egyesül Államok szövetségi szinten csak a közigazgatásra alkalmazott távmunka szabályozással rendelkezik, a munkavállalókra és munkáltatókra vonatkozó szabályok tagállami szinten vannak meghatározva, amely jogszabályok igen eltérő tartalommal bírnak tagállamonként. Viszont a szövetségi szabályozás kifejezetten részletes, külön szervezetrendszert és dedikált személyt követel meg az egyes szervektől a távmunkavégzés kezelésére. Egyedülálló módon ezen szabályozás információ- és kiberbiztonsági szabályokat is tartalmaz, amely a többi vizsgált szabályozási környezetben nem található meg. Végül Finnországot vizsgáltam meg, mivel Európában itt volt 2019-ben a legnagyobb a távmunka aránya. Itt az volt látható, hogy részletesebb szabályokat alkalmaznak, azonban ezen szabályozások nem reflektálnak a kiberbiztonsági fenyegetésekre. Így kijelenthető, hogy ahol nagyobb volt a távmunka aránya ott a normatív szabályozás is részletesebb volt, azonban csak az USA estében reflektált a kiberbiztonsági kihívásokra. A koronavírus első hulláma alatt megnöttek az egyes kiberbiztonsági támadások, amelyek főleg COVID-19 témát használták fel. Azonban az is kijelenthető, hogy újfajta támadás nem jelent meg. Végül a hazai szakemberekkel folytatott kérdőíves felméréséből az látszik, hogy legnagyobb kockázatot az elkövetkezendő 1 évben a távoli munkavégzést kihasználó fenyegetésekben látják, továbbá azon szakemberek a megjelölt fenyegetésekben nagyobb

kockázatot látnak, akik a szervezeten belül azt tapasztalják, hogy a munkavállalók sűrűn kerülnek meg a szabályzatokat.

Eredmények

A kutatási téma feldolgozása során az alábbi eredményeket értem el:

T1: A távmunkával kapcsolatos hazai normatív szabályozás nem reflektál a kiberbiztonsági kihívásokra.

T2: A vírus első hulláma alatt új fajta fenyegetések nem jelentek meg, azonban a meglévők számában növekedés mutatható ki, és megjelenésük szofisztikáltabb volt, mint eddig.

T3: Home office kifejezés megjelenése az interneten a második hullám idején folyamatos csökkenő tendenciát mutat.

T4: A megvizsgált országok esetében, ahol a távolimunkavégzés aránya magasabb volt a koronavírus előtt, részletesebb a normatív szabályozás a témában.

T5: Kérdőíves kiértékelésből kiderül, hogy azon szakértők, akik szerint a szerevetükben dolgozók sűrűbben szegik meg a szabályokat kockázatosabbnak tartják a távmunkát, mint munkavégzési formát.

FELHASZNÁLT IRODALOM

2012. évi I. törvény a munka törvénykönyvéről (é. n.).

Magyar Nemzeti Bank. „Ajánlások”. Elérés 2020. október 16. <https://www.mnb.hu/felugyelet/szabalyozas/felugyeleti-szabalyozo-eszkozok/ajanlasok>.

Anderson, Roy, J.A.P. Heesterbeek, DonDon Klinkenberg, és T. Hollingsworth. „Comment How will country-based mitigation measures influence the course of the COVID-19 epidemic?” *The Lancet* 395 (2020. március 6.). [https://doi.org/10.1016/S0140-6736\(20\)30567-5](https://doi.org/10.1016/S0140-6736(20)30567-5).

Bajpai, Pranshu, és R.J. Enbody. „Attacking Key Management in Ransomware”. *IT Professional* 22 (2020. március 1.): 21–27. <https://doi.org/10.1109/MITP.2020.2977285>.

Baldwin, Richard, és Beatrice Weder di Mauro. *Economics in the Time of COVID-19: A New EBook*. CEPR, 2020. <https://voxeu.org/article/economics-time-covid-19-new-ebook>.

Banowosari, L.Y., és B.A. Gifari. „System Analysis and Design Using Secure Software Development Life Cycle Based On ISO 31000 and STRIDE. Case Study Mutiara Ban Workshop”, 2019. <https://doi.org/10.1109/ICIC47613.2019.8985938>.

Bihary Ákos, és Pulay Flóra. „Home office vagy távmunka?” Jogadó Blog, 2019. július 18.

Letöltés dátuma: 2020.szeptember 1., <https://www.jogado.hu/home-office-vagy-tavmunka/>.

Cybersecurity and Infrastructure Security Agency. „COVID-19 Exploited by Malicious Cyber Actors | CISA”, 2020. április 8. <https://us-cert.cisa.gov/ncas/alerts/aa20-099a>.

Delventhal, Shoshanna. „Apple’s 5 Most Profitable Lines of Business”. Investopedia, 2020. március 10. Letöltés dátuma: 2020. szeptember 14., <https://www.investopedia.com/apple-s-5-most-profitable-lines-of-business-4684130>.

Estrada, Ruiz, és Mario Arturo. „The Uses of Drones in Case of Massive Epidemics Contagious Diseases Relief Humanitarian Aid: Wuhan-COVID-19 Crisis”. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 2020. február 29. <https://doi.org/10.2139/ssrn.3546547>.

Ferrag, M.A., M. Babaghayou, és M.A. Yazici. „Cyber security for fog-based smart grid SCADA systems: Solutions and challenges”. *Journal of Information Security and Applications* 52 (2020). <https://doi.org/10.1016/j.jisa.2020.102500>.

24.hu. „Formálódnak az új home office szabályai, új részletek derültek ki”, 2020. szeptember 7., Letöltés dátuma: 2020. szeptember 21., <https://24.hu/fn/gazdasag/2020/09/07/formalodnak-az-uj-home-office-szabalyai-uj-reszletek-derultek-ki/>.

Franke, U., és J. Wernberg. „A survey of cyber security in the Swedish manufacturing industry”. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1–8, 2020. <https://doi.org/10.1109/CyberSA49311.2020.9139673>.

Hakak, Saqib, Wazir Khan, Muhammad Imran, Kim-Kwang Raymond Choo, és Muhammad Shoaib. „Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies”. *IEEE Access* PP (2020. június 30.): 1–1. <https://doi.org/10.1109/ACCESS.2020.3006172>.

Ho, Karen. „Propelled by Covid-19, Amazon’s Prime Subscriptions Grow to \$5.6 Billion”. Quartz. 2020.március 10., Letöltés dátuma: 2020. szeptember 19., <https://qz.com/1849803/amazons-quarterly-subscription-sales-top-5-6-billion/>.

H.R.1722 - 111th Congress-Telework Enhancement Act of 2010 (2010). <https://www.congress.gov/bill/111th-congress/house-bill/1722/text>.

Inc Gallup. „Is Working Remotely Effective? Gallup Research Says Yes”. Gallup.com, 2020. január 24., Letöltés dátuma: 2020. október 01., <https://www.gallup.com/workplace/283985/working-remotely-effective-gallup-research-says-yes.aspx>.

„INTERPOL Report Shows Alarming Rate of Cyberattacks during COVID-19”. Letöltés dátuma: 2020. szeptember 19., <https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>.

Kapitány-Fövény, Máté, és Mihály Sulyok. „Social Markers of a Pandemic: Modeling the Association between Cultural Norms and COVID-19 Spread Data”. *Humanities and Social Sciences Communications* 7, sz. 1 (2020. szeptember 16.): 1–9. <https://doi.org/10.1057/s41599-020-00590-z>.

Kaplan, Andreas, és Michael Haenlein. „Users of the World, Unite! The Challenges and Opportunities of Social Media”. *Business Horizons* 53 (2010. 0 28.): 59–68. <https://doi.org/10.1016/j.bushor.2009.09.003>.

Karabacak, Bilge, és Ibrahim Sogukpinar. „ISRAM: Information Security Risk Analysis Method”. *Computers & Security* 24, sz. 2 (2005. március 1.): 147–59. <https://doi.org/10.1016/j.cose.2004.07.004>.

Korolov, Maria. „93% of Phishing Emails Are Now Ransomware”. CSO Online, 2016. június 1., Letöltés dátuma: 2020. szeptember 25., <https://www.csoonline.com/article/3077434/93-of-phishing-emails-are-now-ransomware.html>.

Lee, Ming-Chang. „Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method”. *International Journal of computer science and information technology* 6 (2014. március 1.): 29–45. <https://doi.org/10.5121/ijcsit.2014.6103>.

Linnane, Ciara. „Netflix Stock Price Target Raised by Imperial on Expectations It Will Continue to Benefit during Pandemic”. MarketWatch, 2020. április 23., Letöltés dátuma: 2020. szeptember 10., <https://www.marketwatch.com/story/netflix-stock-price-target-raised-by-imperial-on-expectations-it-will-continue-to-benefit-during-pandemic-2020-04-23>.

Maghdid, Halgurd, Kayhan Ghafoor, Ali Sadiq, Kevin Curran, és Khaled Rabie. „A Novel AI-enabled Framework to Diagnose Coronavirus COVID-19 using Smartphone Embedded Sensors: Design Study”. In *2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI)*, 180–87. Las Vegas, NV, USA: IEEE, 2020.

MEGYERI Lajos, és FARKAS Tibor. „Kockázatkezelés, tudomány vagy kuruzslás”. *Hadmérnök* 12, sz. 3 (2017. szeptember 25.): 198–209.

Messenger, Jon, Oscar Vargas Llave, Lutz Gschwind, Simon Boehmer, Greet Vermeylen, és Mathijn Wilkens. *Working Anytime, Anywhere: The Effects on the World of Work*. Geneva: International Labour Organization and the European Foundation for the Improvement of Living and Working Conditions, 2017. http://www.ilo.org/global/publications/books/WCMS_544138/lang--en/index.htm.

Microsoft reporter. „Flexible Ways of Working Are Here to Stay, Finds New European Research – with Leaders Focused on Maintaining Culture and Innovation”. Microsoft News Centre Europe, 2020. október 15., Letöltés dátum: 2020. október 17., <https://news.microsoft.com/europe/features/flexible-ways-of-working-are-here-to-stay-finds-new-european-research-with-leaders-focused-on-maintaining-culture-and-innovation/>.

„MSZ ISO 3100:2019”. MAGYAR SZABVÁNYÜGYI TESTÜLET, é. n.

Muha Lajos, és Krasznay Csaba. *Az elektronikus információs rendszerek biztonságáról vezetőknék*. Budapest: Nemzeti Közszerológati Egyetem, 2014.

Nevalainen Petri, és Toivonen Sofia. „Finland’s Updated Working Hours Act Takes Effect 1 January 2020”. Ally Law, 2019. október 25., Letöltés dátuma: 2020. augusztus 28., <https://ally-law.com/finlands-updated-working-hours-act-takes-effect-1-january-2020/>.

Nguyen, Thanh. *Artificial Intelligence in the Battle against Coronavirus (COVID-19): A Survey and Future Research Directions*, 2020. <https://doi.org/10.13140/RG.2.2.36491.23846/1>.

Rayome, Alison DeNisco. „Messenger Rooms: How to Use Facebook’s Free New Video Chat Feature Now”. CNET., 2020. május 9., Letöltés dátuma: 2020. szeptember 17., <https://www.cnet.com/how-to/messenger-rooms-heres-how-to-use-facebooks-free-new-video-chat-feature/>.

Rodbert, M. „Why organisational readiness is vital in the fight against insider threats”. *Network Security* 2020, sz. 8 (2020): 7–9. [https://doi.org/10.1016/S1353-4858\(20\)30092-1](https://doi.org/10.1016/S1353-4858(20)30092-1).

Savage, Maddy. „Why Finland Leads the World in Flexible Work”. BBC., 2019. augusztus 7., Letöltés dátuma: 2020. október 21., <https://www.bbc.com/worklife/article/20190807-why-finland-leads-the-world-in-flexible-work>.

Sharafaldin, Iman, Arash Habibi Lashkari, Saqib Hakak, és Ali Ghorbani. In *Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy*, 8. International Carnahan Conference on Security Technology, 2019. <https://doi.org/10.1109/CCST.2019.8888419>.

„Strategies to Mitigate Cyber Security Incidents | Cyber.gov.au”, 2017. február 1., Letöltés dátuma: 2020. október 21., <https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents>.

Swartz, Jon. „Facebook Has Weathered Many Storms, but the Latest Are Coming for Its Core”. MarketWatch. 2020.április 06., Letöltés dátuma: 2020. október 10., <https://www.marketwatch.com/story/facebook-in-the-age-of-covid-19-users-are-online-but-will-advertisers-pay-to-get-to-them-2020-04-06>.

Tisdell, Clem. „Economic Reform and Openness in China: China’s Development Policies in the Last 30 Years”. *Economic Analysis and Policy* 39, sz. 2 (2009. szeptember 1.): 271–94. [https://doi.org/10.1016/S0313-5926\(09\)50021-5](https://doi.org/10.1016/S0313-5926(09)50021-5).

Tisdell, Clement. „Economic and Business Relations Between China and Australia: Insights Into China’s Global Economic Footprint”, 11–24. Brisbane: Australian Academic, 2007.

Tisdell, Clement A. „Economic, Social and Political Issues Raised by the COVID-19 Pandemic”. *Economic Analysis and Policy* 68 (2020. 0 1.): 17–28. <https://doi.org/10.1016/j.eap.2020.08.002>.

Walter, Laura. „Finland, Sweden, Australia Offer Most Flexible Work Schedules | EHS Today”. Ehstoday, 2011. június 6. Letöltés dátuma: 2020. szeptember 02., <https://www.ehstoday.com/archive/article/21904410/finland-sweden-australia-offer-most-flexible-work-schedules>.

William Stallings, és Lawrie Brown. *Computer Security: Principles and Practice*. Boston: Pearson, 2012.

Zeki, Yazar. „A Qualitative Risk Analysis and Management Tool - CRAMM”. SANS Institute, 2002. <https://www.sans.org/reading-room/whitepapers/auditing/paper/83>.

MELLÉKLETEK

1. számú melléklet (ábra jegyzék)

1. ábra Csomópontok a világ információs és kommunikációs technológiai áruk ellátási láncában (Forrás: Világ Bank).....	13
2. ábra Otthon dolgozó munkavállalók a teljes foglalkoztatottság százalékában az EU-ban(2019)(sajátszerkesztés forrás: Eurostat).....	23
3. ábra Otthoni munkavégzés aránya 2010-2019-ig az vizsgált országokban (forrás: Eurostat).....	24
4. ábra Kifejezések megjelenése érzelmek szerint (saját szerkesztés, forrás: SentiOne).32	
5. ábra Kifejezések hazai megjelenésének napi aránya,(saját szerkesztés, forrás: SenitOne).....	33
6. ábra Megemlékések platform szerinti megoszlása (Hazai), saját szerkesztés (forrás: SentiOne).....	34
7. ábra Megemlékések platform szerinti megoszlása (Nemzetközi) (saját szerkesztés, forrás: SenitOne)	34
8. ábra Kulcsszavak időbeli megoszlása (saját szerkesztés forrás: SentiOne).....	35
9. ábra A motivációk havi elosztása 2020 Q1 (sajátszerkesztés, forrás: Hackmageddon)	37
10. ábra Támadások célpontjai 2020 Q1 (sajátszerkesztés, forrás: Hackameddon).....	38
11. ábra A COVID-19 alatt megjelent támadások csoportosítása (sajátszerkesztés, forrás: Saqib Hakak és mtsai.).....	44
12. ábra Alapelvek, keretrendszer és folyamat viszonya az ISO 3100 keretrendszerben (sajátszerkesztés, forrás: ISO 3100).....	47
13. ábra Kitöltők szektorbeli megoszlásai (db) (saját szerkesztés)	61
14. ábra Beosztás szerinti megoszlás (%) (sajátszerkesztés)	62
15. ábra Szabálmegkerülési gyakoriság (%) (sajátszerkesztés)	64
16. ábra Kruskal-Wallis-próba signifikancia eredménye (sajátszerkesztés, forrás: SPSS)	64
17. ábra Támadásonkénti rangátlag megoszlás (sajátszerkesztés forrás: SPSS)	66

2. számú melléklet (táblázat jegyzék)

1. táblázat A társadalmi klaszterek kialakításának szempont rendszere- Leíró célok az országszintű klaszterprofilok részletezéséhez- Saját szerkesztés, Forrás: Kapitány-Fövény, M., Sulyok, M.	6
2. táblázat A társadalmi klaszterek kialakításának szempont rendszere- Klaszterezés és prediktív célok leírása- Saját szerkesztés, Forrás: Kapitány-Fövény, M., Sulyok, M.....	7
3. táblázat A társadalmi klaszterek kialakításának szempont rendszere- Éghajlat mint befolyásoló tényező - Saját szerkesztés, Forrás: Kapitány-Fövény, M., Sulyok, M.....	8
4. táblázat A társadalmi klaszterek kialakításának szempont rendszere- Az országok társadalmi és gazdasági helyzete - Saját szerkesztés, Forrás: Kapitány-Fövény, M., Sulyok, M.....	9
5. táblázat Stratégiák a kiberbiztonsági események enyhítésére - Enyhítő stratégiák a rosszindulatú programok célba érésének és feladatának végrehajtásának megakadályozására (sajátszerkesztés, forrás: Australian Cybersecurity Center).....	53
6. táblázat Stratégiák a kiberbiztonsági események enyhítésére - A kiberbiztonsági incidensek mértékének korlátozására szolgáló enyhítési stratégiák (sajátszerkesztés, forrás: Australian Cybersecurity Center).....	55
7. táblázat Stratégiák a kiberbiztonsági események enyhítésére - A kiberbiztonsági események észlelésének és a reagálás mérséklési stratégiái (sajátszerkesztés, forrás: Australian Cybersecurity Center).....	57
8. táblázat Stratégiák a kiberbiztonsági események enyhítésére - Az adatok és a rendszer rendelkezésre állásának helyreállítására szolgáló enyhítési stratégiák (sajátszerkesztés, forrás: Australian Cybersecurity Center).....	57
9. táblázat Stratégiák a kiberbiztonsági események enyhítésére - A rosszindulatú belső személyek megelőzésére vonatkozó mérséklési stratégia (sajátszerkesztés, forrás: Australian Cybersecurity Center).....	58
10. táblázat Egyes fenyegetések bekövetkezési valószínűségének kockázatai a szakértők véleménye szerint (db) (sajátszerkesztés forrás: kérdőív).....	63

3. számú melléklet (Kérdőív)

1) Melyik iparágban dolgozik?

- Pénzügyi
- Turizmus, vendéglátás
- Közigazgatás
- Egészségügyi, szociális ellátás
- Távközlés
- Ipar
- Építő ipar
- Szállítás, közlekedés
- Kereskedelmi
- Technológiai
- Egyéb közösségi, személyi szolgáltatás
- Oktatás
- Ingatlanügyletek
- Villamosenergia-, gáz-, gőz-, vízellátás
- Egyéb

2) Ha az egyebet választotta, kérem írja le mely iparágban dolgozik.

3) Milyen végzettséggel rendelkezik kiberbiztonsági területen? (több választ is megjelölhet)

- Elektronikus Infomációbiztonsági vezető
- Infomációbiztonsági Szakjogász
- CISA
- CISM
- CISSP
- CRISC
- ISO Lead Auditor
- ISO Internal Auditor
- Egyéb információbiztonsági végzettség
- Egyéb nem információbiztonsági végzettség

- 4) Ha egyéb információbiztonsági végzettséget vagy egyéb nem információbiztonsági végzettséget választotta, kérem írja le végzettségét.
- 5) Milyen beosztásban dolgozik? (szabad szöveg)
- 6) Mióta dolgozik a kiberbiztonsági területen?
- 0-3 év
 - 4-6 év
 - 7-9 év
 - 10-12 év
 - 13-15 év
 - 15+ év
- 7) Mennyire igaz a következő állítás az ön iparágára?
- Az iparágamban működő vállalatok általában tisztában vannak a kiberbiztonsági kockázatokkal, és hogy ezek az események vagy támadások befolyásolhatják az üzletmenet folytonosságot.
 - 1 teljes mértékben nem igaz; 5 teljes mértékben igaz
- 8) Mennyire tartja valószínűnek, hogy az Ön szervezete a következő 12 hónapban az alábbi incidensek valamelyikét elszenvedti:
- 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

Kockázati szint:

- Elhanyagolható kockázat
 - Alacsony kockázat
 - Közepes kockázat
 - Magas kockázat
 - Nagyon magas kockázat
- 9) Tapasztalt-e az Ön szervezete valamilyen kiberbiztonsági incidenst az elmúlt 12 hónapban? (több választ is megjelölhet)

- Az üzletmenet folytonosság megszakításával járó támadás
- Olyan támadás, amely az adatok megsértésével jár és nyilvánossá váltak ezen adatok
- Adatmegsértéssel járó támadás, ahol az adatokat a támadó megtartja magának (ipari kémkedés)
- Nem szándékos esemény, amely üzletmenet folytonosság megszakításával jár
- Nem szándékos esemény, amely adatmegsértést von maga után
- Távoli munkavégzést kihasználó támadások
- Nem tapasztaltunk

10) Az Ön szervezete kapcsán kiberbiztonság melyik terület esetében játszik különösen fontos szerepet? (több választ is megjelölhet)

- Adminisztráció
- Ügyfélszolgálat (beleértve az ügyfelek panaszait, visszaküldéseket, garanciákat, pótalkatrészeket és javításokat)
- Döntéshozatal és döntéstámogatás
- Termelés
- Marketing és értékesítés
- Beszerzés
- Logisztika és szállítás
- Egyéb
- Nem tudom

11) Milyen intézkedéseket hajtott végre szervezete a kiberbiztonság javítása érdekében? (több választ is megjelölhet)

- A szervezet kiberbiztonsági stratégiával rendelkezik, külön dokumentumként vagy egy másik stratégia részeként.
- A vállalat folytonossági tervvel rendelkezik olyan események kezelésére, amelyek üzleti megszakítással vagy adatmegsértéssel járnak.
- Az alkalmazottak az elmúlt évben képzést kaptak a adat- és/vagy információbiztonsággal kapcsolatban.
- Kötelező rendszabályokat és folyamatokat vezettünk be az alkalmazottak számára, például a jelszó előállításával, a magántárhely vagy a digitális magánszolgáltatások használatával, a biztonsági mentésekkel és a hálózati hozzáféréssel kapcsolatban.

- Alkalmazunk olyan technikai megoldásokat, mint például szoftverfrissítések, biztonsági mentések készítése, kommunikáció titkosítása és a hálózati hozzáférésre vonatkozó szabályok alkalmazása.
- A vállalat tanúsított például: Az ISO27000 sorozat szerint.
- A társaság rendelkezik a kiberbiztosítás valamilyen formájával (ideértve a számítógépes bűnözéssel vagy az adatvédelemmel kapcsolatos biztosításokat), amely lefedi például az üzleti tevékenység megszakítását, az adatok megsértését és az eseménykezelés támogatását.
- A társaság kiberbiztonsági eseménykezelési gyakorlatokat végzett balesetek és / vagy támadások kapcsán.
- A vállalat kiberbiztonsági eseménykezelési protokolljait évente legalább egyszer frissítik.
- Nem történt ilyen jellegű intézkedés.

12) Az Önök szervezeténél engedélyezve volt-e a távolimunkavégzés a Vírus első hullámában?

- Igen
- Nem

13) A COVID-19 járványhelyzet tapasztalatai alapján tettek-e külön lépéseket annak érdekében, hogy a távoli munkavégzés biztonságosabb legyen a jövőben?

- Nem volt távoli munkavégzésre lehetőség
- Igen
- Nem
- Folyamatban van
- Nem tudom

14) Az alkalmazottak mennyire követik a rendszabályokat?

- Követik
- Nem követik

15) Ha nem követik, akkor miért nem?

- Követik
- Nem követik ismeret hiány miatt
- Nem követik kényelem miatt

16) Milyen gyakran kerülnek meg?

- Nem kerülnek meg

- Ritkán
- Sűrűn
- Nem tudom

4. számú melléklet (Kérdőív kiértékelése)

Descriptive Statistics

	N	Mean	Std. Deviation	Minimum	Maximum
8) Mennyire tartja valószínűnek, hogy az Ön szervezete a következő 12 hónapban az alábbi incidensek valamelyikét elszenvedi: [Nem szándékos esemény, amely üzletmenet folytonosság megszakításával jár]	44	2,55	1,130	1	5
8) Mennyire tartja valószínűnek, hogy az Ön szervezete a következő 12 hónapban az alábbi incidensek valamelyikét elszenvedi: [Távoli munkavégzést kihasználó támadások]	44	2,77	1,138	1	5
8) Mennyire tartja valószínűnek, hogy az Ön szervezete a következő 12 hónapban az alábbi incidensek valamelyikét elszenvedi: [Adatmegsértéssel járó támadás, ahol az adatokat a támadó megtartja magának (például: ipari kémkedés)]	44	2,25	1,123	1	4
8) Mennyire tartja valószínűnek, hogy az Ön szervezete a következő 12 hónapban az alábbi incidensek valamelyikét elszenvedi: [Olyan támadás, amely az adatok megsértésével jár, és nyilvánossá válnak ezen adatok]	44	2,41	,948	1	4

8) Mennyire tartja valószínűnek, hogy az Ön szervezete a következő 12 hónapban az alábbi incidensek valamelyikét elszenvedi: [Az üzletmenet folytonosság megszakításával járó támadás]	44	2,18	,947	1	4
16) Milyen gyakran kerülük meg?	44	1,73	,660	1	3

Test Statistics^{a,b}

	8) Mennyire tartja valószínűnek, hogy az Ön szervezete a következő 12 hónapban az alábbi incidensek valamelyikét elszenvedi: [Nem szándékos esemény, amely üzletmenet folytonosság megszakításával jár]	8) Mennyire tartja valószínűnek, hogy az Ön szervezete a következő 12 hónapban az alábbi incidensek valamelyikét elszenvedi: [Távoli munkavégzést kihasználó támadások]	8) Mennyire tartja valószínűnek, hogy az Ön szervezete a következő 12 hónapban az alábbi incidensek valamelyikét elszenvedi: [Adatmegsértéssel járó támadás, ahol az adatokat a támadó megtartja magának (például: ipari kémkedés)]	8) Mennyire tartja valószínűnek, hogy az Ön szervezete a következő 12 hónapban az alábbi incidensek valamelyikét elszenvedi: [Olyan támadás, amely az adatok megsértésével jár, és nyilvánossá válnak ezen adatok]	8) Mennyire tartja valószínűnek, hogy az Ön szervezete a következő 12 hónapban az alábbi incidensek valamelyikét elszenvedi: [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

a. Kruskal Wallis Test

b. Grouping Variable: 16) Milyen gyakran kerülük meg?

Ranks

	16) Milyen gyakran kerülük meg?	N	Mean Rank
8) Mennyire tartja valószínűnek, hogy az Ön szervezete a következő 12 hónapban az	Nem kerülük meg	17	14,53
	Ritkán	22	27,05
	Sűrűn	5	29,60

alábbi incidensek valamelyikét elszenvedi: [Nem szándékos esemény, amely üzletmenet folytonosság megszakításával jár]	Total	44	
8) Mennyire tartja valószínűnek, hogy az Ön szervezete a	Nem kerülik meg	17	13,85
következő 12 hónapban az	Ritkán	22	27,55
alábbi incidensek valamelyikét elszenvedi: [Távoli munkavégzést kihasználó támadások]	Sűrűn	5	29,70
8) Mennyire tartja valószínűnek, hogy az Ön szervezete a	Total	44	
következő 12 hónapban az	Ritkán	22	17,71
alábbi incidensek valamelyikét elszenvedi: [Adatmegsértéssel járó támadás, ahol az adatokat a támadó megtartja magának (például: ipari kémkedés)]	Sűrűn	5	26,39
8) Mennyire tartja valószínűnek, hogy az Ön szervezete a	Total	44	21,70
következő 12 hónapban az	Ritkán	22	13,50
alábbi incidensek valamelyikét elszenvedi: [Olyan támadás, amely az adatok megsértésével jár, és nyilvánossá válnak ezen adatok]	Sűrűn	5	27,64
8) Mennyire tartja valószínűnek, hogy az Ön szervezete a	Total	44	30,50
következő 12 hónapban az	Ritkán	22	14,71
alábbi incidensek valamelyikét elszenvedi: [Az üzletmenet folytonosság megszakításával járó támadás]	Sűrűn	5	26,77
	Total	44	30,20

5. számú melléklet (Rövidítések jegyzéke)

Rövidítés	Magyar jelentés	Idegen nyelvű jelentés
AI	-	Intelligent Artifacts
CCTA	-	Central Computer and Telecommunion Agency
CEO	-	Chief Executive Officer
CISA	-	Certified Information Systems Auditor
CISM	-	Certified Information Security Manager
CISO	-	Chief Information Security Officer
CISSP	-	Certified Information Systems Security Professional
COBRA	-	Consultative, Objective & Bifunctional Risk Analysis
CORA	-	Cost-of-Risk Analysis
CRAMM	-	CCTA Risk Analysis and Management Methodology
CRISC	-	Certified in Risk and Information Systems Control
DDoS	-	Distributed Denial of Service
DPO	-	Data Protection Officer
EBRD	-	European Bank for Reconstruction and Development
EKB	Európai Központi Bank	-
GDP		Gross Domestic Product
HAQ	-	Health Assessment Questionnaire
HTTP	-	HyperText Transfer Protocol
IBF	Információbiztonsági Felelős	-
ICMP	-	Internet Control Message Protocol
IFC	-	International Finance Corporation
IKT	Információs és Kommunikációs Technológia	-

Rövidítés	Magyar jelentés	Idegen nyelvű jelentés
IMF	-	International Monetary Fund
ISO	-	International Organization for Standardization
ISRAM	-	Information Security Risk Analysis Method
LMS	-	Learning Module System
MNB	Magyar Nemzeti Bank	-
MSZ	Magyar Szabvány	-
RDP	-	Remote Desktop
SCADA	-	Supervisory Control And Data Acquisition
SMB	-	Server Message Block
SSH	-	Secure Shell
TCP	-	Transmission Control Protocol
TEA	-	Telework Enhancement Act
TLTRO	-	Targeted Longer-Term Refinancing Operations
UDP	-	User Datagram Protocol
VOIP	-	Voice over IP
VPN	-	Virtual Private Network
WHO	-	World Health Organization

FÜGGELÉKEK

Annotáció

2019 végén Kínában megjelent, majd rövid időn belül az egész világon elterjedt egy újfajta vírus, amely az általunk ismert világ berendezkedését átformálta. Számos olyan területen jelent meg az online munkavégzés, ahol eddig nehezen megvalósíthatónak tűnt mint például a közigazgatás, banki konzultáció. Ez a gyors átállás számos biztonsági kihívást rejtett magában. Többek között nem volt elegendő eszköz, amivel lehetett volna távolról biztonságosan munkavégzést folytatni. Sok esetben a munkavállalóknak saját eszközükön kellett dolgozniuk, amelyeken nem volt biztosítva többek között a megfelelő végpont védelem. A kiberbiztonsági fenyegetések vizsgálata során az volt kimutatható, hogy a koronavírus hatására új típusú támadás nem jelent meg, inkább a meglévő támadást használták fel az elkövetők újra tematizálva azokat. Ezen felül az is látható, hogy a jogi szabályozása a távoli munkavégzésnek nemzetenként igen eltérő szintű volt. Ezen felül a közösségi média elemzésből többek között az derült ki, hogy a home office kifejezés megjelenése az interneten a második hullám idején folyamatos csökkenő tendenciát mutat. A megvizsgált országok esetében, ahol a távolimunkavégzés aránya magasabb volt a koronavírus előtt, részletesebb a normatív szabályozás a témában. Ezt követően kérdőíves felmérést végeztem a hazai kiberbiztonsági szakértők körében, ahol kiderül, hogy azon szakértők, akik szerint a szerevetükben dolgozók sűrűbben szegik meg a szabályokat kockázatosabbnak tartják a távmunkát, mint munkavégzési formát. Ez arra enged következtetni, hogy a kockázatelemzésekben megadott kockázati szintre hatással van a szakértők véleménye az egyes szervezeti tulajdonságokról. Ez azért lehet probléma mert a kockázatok súlyosság szerint kerül meghatározásra a kockázatok kezelési terve. Ezen kezelési terv határozza meg, hogy az információbiztonságra alokált forrás, miként is kerül pontosan felhasználásra. Ha a kockázatok hatása és valószínűsége nincs megfelelő módon felmérve, akkor a kezelési stratégia is hibás lesz, ami a meglévő kockázatokat tovább erősítheti, vagy újakat hívhat életre.