Kiberbiztonság a koronavírus idején – a COVID–19 nemzetbiztonsági aspektusai

Palicz Tamás[1]*, Bencsik Balázs[2], Szócska Miklós[1]

[1]Semmelweis Egyetem, Egészségügyi Közszolgálati Kar, Egészségügyi Menedzserképző Központ, Budapest, Magyarország
[2]Nemzetbiztonsági Szakszolgálat, Nemzeti Kibervédelmi Intézet, Budapest, Magyarország

Beérkezett: 2021. április 27.; Elfogadva: 2021. május 7.

Összefoglalás

A COVID–19 pandémia az információbiztonság területén új kihívásokat jelentett. A távolról végzett munka különböző formái jelentős mértékben növelték az online tér biztonsági kockázatát. Nőtt a hálózatok nagysága, az adatforgalom, és azon felhasználók száma, akiknek nem volt érdemi tapasztalatuk az online térben. A járvány ideje alatt a kibertérből érkező támadások szektoronként és időszakonként eltérő intenzitásúak voltak, a támadások típusa a phishingtől a malwareken keresztül az információs zavarkeltésig széles spektrumban változott. Számos jelenségnek nemzetbiztonsági vonatkozásai is voltak. Összefoglaló cikkünkben a fenti jelenségek nemzetközi és hazai tapasztalatait összegezzük, különös figyelmet szentelve az egészségügyi rendszernek, illetve a vakcinafejlesztés kibertérből érkező fenyegetéseinek.

Kulcsszavak: kiberbiztonság, kiber fenyegetések, egészségügy, vakcináció, zsarolóvírus

Cyber Security in the Time of the Coronavirus – National Security Aspects of COVID-19

Tamás Palicz[1], Balázs Bencsik[2], Miklós Szócska[1]

[1]Semmelweis University, Faculty of Public Health Services, Health Services Management Training Centre, Budapest, Hungary
[2]Special Services for National Security, National Cyber Security Center, Budapest, Hungary

Summary

During the COVID-19 pandemic, new challenges emerged in the field of information security and cyber security. Home office, home schooling and distance learning, or even telemedicine hit some organizations unprepared. Security risks in online space have increased significantly: the number of network endpoints and the number of computers, laptops and mobile devices have increased with network data traffic as well as the number of users who had no significant experience in online space. They appeared as a significant risk factor. This has been exacerbated, especially in healthcare, by the extremely high workload, which has made systems highly vulnerable. During the epidemic, attacks from cyberspace varied in intensity from sector to sector and period to period. Statistics from international and national organizations have shown that from the end of the first quarter of 2020, the number of cyber security incidents jumped sharply and then remained high even after a small decline. The types of attacks had an extremely wide range: from phishing through malware to misinformation, almost all types of attacks occurred. Many phenomena also had national security implications. Ransomware virus attacks on health have affected almost all health systems and reached high levels by the end of 2020 in particular. It was during the first period that, in an emergency case, there is thought to be an association between a ransomware virus attack and the death of a patient who was not admitted because of the attack.

In addition to distance measures and the associated increase in cyber threats, the emerging threats related to vaccination, which is central to the fight against the epidemic, should also be highlighted. This period has shed light on

how many vulnerabilities there are, from vaccine development through drug trials to delivery to vaccines and the organization of vaccines, that cybercriminals are able to attack. In order to prevent and combat these threats and attacks, and to respond appropriately, complex, multidisciplinary collaborations are needed in which security science has a privileged place. In our review article, we summarize the international and national experiences of the above phenomena, paying special attention to the health care system and the threats coming from cyberspace in vaccine development.

Keywords: cybersecurity, cyberthreats, healthcare, vaccination, ransomware

Bevezetés

A koronavírus-járvány 2019-es indulása, majd 2020-as világjárvánnyá válása sok tekintetben megváltoztatta a korábbi életünket: számos azonnali intézkedés került bevezetésre Magyarországon is már az első járványhullám megjelenésekor *(Szerencsés et al. 2021)*. A járványkezelés sikeressége szempontjából az egyik kritikus döntés a kontaktusszám csökkentése volt. Ennek lépései közé tartozott az otthonról végzett munka (home office) lehetővé tétele, az otthoni tanulás (home schooling) azonnali bevezetése a közoktatásban, de említhetjük az egészségügy területén megjelent, főként az alapellátásban és a járóbeteg szakellátásban lehetőségként megjelenő távegészségügyi (telehealth, telemedicina) megoldásokat is *(Wosik et al. 2020)*, illetve a járvány miatti szükségszerűen átszervezett egészségügyi kapacitásokat.

Ezek, a járványkezelés érdekében különösebb előkészület nélkül (technológiai és humánfelkészülés) bevezetett eljárások még a modern, fejlett államok számára is jelentős kihívást, időnként komoly megterhelést jelentettek, elég ha csak a távoktatás széles körű elrendelésére utalunk *(Bansak–Starr 2021)*.

Ezzel párhuzamosan az online térben megnövekedett a jelenléte és az aktivitása azoknak a rosszindulatú szereplőknek is, akik – ugyan eltérő szándékkal, de mégis – a kibertér és az ott megjelenők biztonságát veszélyeztették.

A helyzetet egyfajta ambivalencia jellemezte és jellemzi napjainkban is: az online térben megfigyelhető fokozott aktivitás folyamatos terhelés alatt tartja a rendszereket, miközben ez a terhelés ráirányította a figyelmet a kiberbiztonságra mint témára, ez pedig érezhetően növeli a biztonságtudatosság iránti igényt.

Így bátran mondhatjuk, hogy ebben a hirtelen megváltozott környezetben, ahol az online megoldások felértékelődtek, a személyes és a nemzetbiztonság egyik kulcstényezője lett a kibertér biztonságos használatának biztosítása, segítése.

Ezek a tényezők nemcsak a kiberbiztonság vagy a járványkezelés szempontjából fontosak, hanem ebben a rendkívül érzékeny pszichológiai helyzetben alkalmasak az emberek bizonytalanságának fokozására, ezáltal rendszerek destabilizálása révén politikai válságot, valamint személyes és nemzetbiztonsági problémát vagy válságot is képesek előidézni.

Összefoglaló cikkünk célja, hogy áttekintsük a COVID–19 járványidőszak alatti főbb változásokat, tendenciákat, valamint külön kiemeljük azokat a szempontokat, amelyek különös figyelmet kaptak a 2020-as évben. Az egészségügyi vonatkozásokkal, tekintettel a járvány leküzdésében betöltött kulcsfontosságú szerepére, külön részekben foglalkozunk. A fentiek mellett külön utalunk néhány, kifejezetten nemzetbiztonsági vonatkozású megfontolásra is, illetve kiemeljük a lényegesebb hazai mutatókat és történéseket is.

2020 és a COVID–19-járvány az éves beszámolókban

A 2020-as év során folyamatosan jelentek meg elemzések, amelyek próbálták érzékeltetni és bemutatni, hogy hogyan befolyásolja a járvány a kiberbiztonsági helyzetet.

Az Interpol a 2020. augusztusi kiadványában összefoglalta a COVID–19-járványhoz köthető legjellegzetesebb kibereseményeket, bűncselekményeket *(Interpol 2020b)*. Öt típust különböztettek meg, amelyek mindegyikében megdöbbentően alakultak a számok.

1. Online átverés és phishing

   Nem véletlen, hogy ezt a kategóriát említi először az Interpol összefoglalója. Szinte valamennyi megjelent összefoglaló, beszámoló az első helyen említi ezeket a kiberbűnözői tevékenységeket. Az átverések és a phishing kampányok számának növekedéséről mind az Interpol, mind az ENISA (European Union Agency for Cybersecurity – ENISA) nagyon hasonló számokat közölt.

   A 2020 októberében megjelent ENISA-jelentés, amely a 2019. január és 2020. április közötti adatokat dolgozza fel, azt emeli ki, hogy a COVID–19-pandémia egy hónapja alatt a phishing-aktivitás 667%-kal nőtt *(ENISA 2020)*.

   Hasonló tendenciát, de nem ilyen erőteljes növekedést mutatnak az Anti Phishing Munkacsoport (Anti-Phishing WorkGroup – APWG) adatai is, itt a növekedés kb. négyszeres *(APWG 2020)*, és az a tevékenység 2020 márciusától kezd majdnem egyenletesen növekedni.

   A másfél milliárd e-mail-használóval rendelkező Google 2020. április közepén jelezte, hogy a phishing e-mailek száma „felrobbant", és az ő rendszerük naponta 100 millió káros tartalmú e-mailt szűr ki a rendszerben *(BBC News 2020a)*.

Az Interpol jelentése szerint a phishing-kampányok az alábbi főbb témák körül csoportosultak:

a. e-mail valamilyen globális vagy helyi egészségügyi hatóságtól,
b. kormányzati utasítás,
c. pénzügyi támogatás kezdeményezése,
d. pénzügyi teljesítés kérése, fizetés,
e. vakcina vagy a járvánnyal kapcsolatos gyógyászati anyag vagy eszköz ajánlata,
f. COVID–19 mobil nyomkövető,
g. befektetések,
h. COVID–19-hez kapcsolható jótékonysági tevékenység.

A helyi hatóságoktól érkező e-mail phishing-kampányra vonatkozóan Magyarországon is volt példa. 2020 júniusában kiterjedt e-mail-kampányban próbálták a bűnözők a járvány kapcsán az Országos Tisztifőorvos által kialakított általános bizalmat kihasználni *(1. ábra)*.

2. Diszruptív malware-ek használata (zsarolóvírusok és DDoS)

A zsarolóvírus fertőzések a COVID–19 járványidőszak kiemelt kiberbiztonsági történései, ezért erről egy külön bekezdésben részletesen írunk. Itt talán annyit elég megemlíteni, hogy ennek az időszaknak a legnépszerűbb ransomware-jei a CERBER, NetWalker és a Ryuk voltak, feltételezések szerint erőteljes orosz háttérrel. Mindhárom zsarolóvírus esetében az RaaS (Ransomware-as-a-Service) üzleti modell működik, amely nagymértékben hozzájárult ahhoz, hogy az elmúlt 2 év alatt ezzel a három zsarolóvírussal kb. 250 millió USD (~75 Mrd Ft) bevételt generáltak.

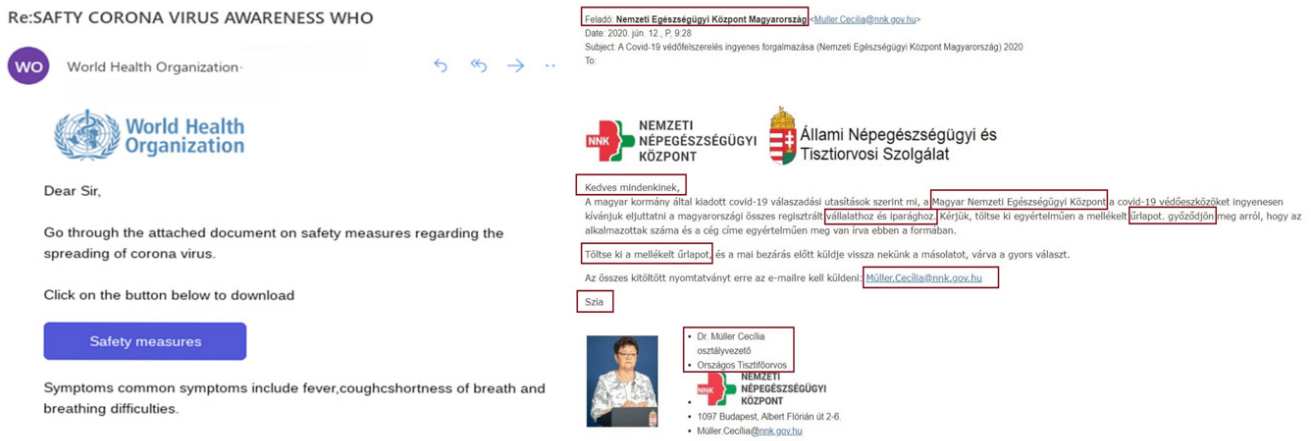
A vakcinaregisztrációt biztosító magyar informatikai rendszer 2021. februári DDoS támadásáról a cikk későbbi részében írunk.

3. Rosszindulatú domainek

A „corona” vagy „COVID” kulcsszavakkal regisztrált domainek száma 2020-ban ugrásszerűen megnövekedett. Az Interpol 2020. március végéig több mint 116 000 ilyen domaint azonosított, amelyek közül 2022 kifejezetten rosszindulatú volt, míg több mint 40 000-t magas rizikójúnak detektált. 2020 júniusára ez a szám 200 000-re növekedett. Az ilyen típusú domaineket leginkább malware terjesztésére, phishing-kampányokhoz, kriptovaluta-bányászathoz, illetve hivatalos weboldalak (pl. hatóságok, egészségügyi szolgáltatók, adóhivatal, bankok, kormányzati oldalak stb.) hasonmásainak előállításához használták és használják. A megnövekedett regisztrációt magyarázza az is, hogy az internetes kereskedés mértéke extrém mértékben nőtt, ez pedig együtt járt a járványhoz kapcsolódó, hamisított áruk (maszkok, egyéni védőeszközök, diagnosztikai kitek, higiénés eszközök, gyógyszerek, vakcinák stb.) kereskedésével, vagy egyszerű csalásra használt weboldalak létrehozásával is.

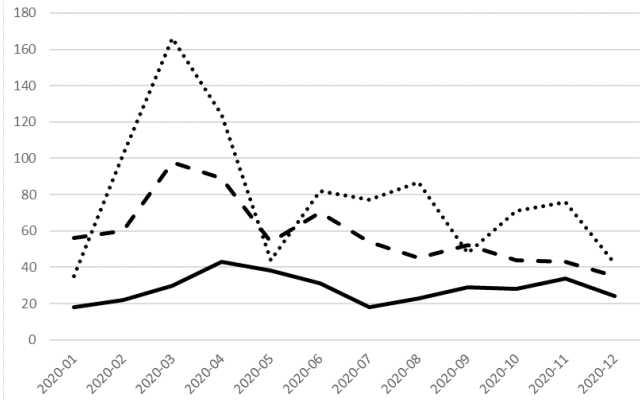
4. Adatgyűjtő malware-ek

Ebben a kategóriában az Emotet-et és a TrickBot-ot említi meg a jelentés. Az előbbi egy rendkívül „jó képességű” moduláris trójai, amelyet pdf, docx és mp4 fájlokhoz csatolva terjesztettek leggyakrabban. 2020 elején a legelterjedtebb adatgyűjtő malware volt, egyes statisztikák szerint a malware közel egyharmadát ez adta. Az Emotet Magyarországon is megjelent az egészségügyi intézményekben, ami miatt a Nemzeti Kibervédelmi Intézet (NKI) 2020 őszén riasztást is kiadott *(NKI 2020)*. 2021 januárjában több ország együttműködésével az európai hatóságok lekapcsolták az Emotet hálózatát, ami remélhetőleg jelentősen csökkenti ezeket a kockázatokat *(The Hacker News 2021)*.



1. ábra Példa globális szervezettől és helyi hatóságtól érkező phishing e-mailre (Nemzeti Kibervédelmi Intézet saját gyűjtése)

A magyar példa kapcsán feltüntettük azokat a sajátosságokat, amelyek figyelmes megtekintése segíti annak eldöntését, hogy ez nem valós e-mail, pl. szövegezés, az intézmény nevére hasonlító, de azzal nem egyező név, fénykép becsatolása a hivatalos e-mailbe stb. (Nemzeti Kibervédelmi Intézet saját gyűjtése)



2. ábra A Nemzeti Kibervédelmi Intézet által észlelt események számának alakulása típus szerint 2020. január 1. – 2020. december 31. között (észlelés: folytonos vonal, jelzés: szaggatott vonal, bejelentés: pontozott vonal) (Nemzeti Kibervédelmi Intézet saját adatai)

Az ábrából látható, hogy a nemzetközi adatoknak megfelelően a 2020. évben a március–áprilisi időszak volt a kiberbiztonsági események szempontjából a legaktívabb.

A másik fontosabb adatgyűjtő malware a TrickBot volt, amely leggyakrabban phishing-kampányok részeként vagy nonprofit szervezetek adománygyűjtő e-mailjének csatolmányaként került be a rendszerekbe.

5. Megtévesztés (miszinformáció), fake news

Talán ez az a terület, ahol szinte végtelen mennyiségű esetet, történést lehetne bemutatni, mind a nemzetközi, mind a hazai események alapján. Azt fontosnak tartjuk kiemelni, hogy a hazai szabályozás lehetővé tette és teszi, hogy azok a szereplők, akik ilyen lépést tesznek, álhíreket terjesztenek, eljárás alá vonhatók. Az álhírek veszélyére már a járvány kezdetén, 2020 februárjában felhívta a figyelmet a WHO *(WHO 2020)*, és a jelentősebb tudományos folyóiratok, a nagy technológiai cégek csatlakoztak az álhírek elleni harchoz *(Zarocostas 2020; Vraga–Bode 2020)*. Így a kialakított mesterségesintelligencia-eljárásokkal a közösségimédia-platformokról jó eredményességgel távolítják el a félelmet és bizonytalanságot keltő híreket. A küzdelembe beszállt az Európai Bizottság is, és elérte, hogy több mint 3,4 millió gyanús Twitter-felhasználó ellen eljárjanak; hogy 100 000 YouTube-videót eltávolítsanak, illetve hogy a Microsoft naponta 96 millió felhasználót elérjen a koronavírussal foglalkozó online platformján keresztül *(Privátbankár.hu 2020)*.

A magyarországi események kapcsán a Nemzetbiztonsági Szakszolgálat alá tartozó Nemzeti Kibervédelmi Intézet adatait tekintjük át. Az intézet – a hatályos jogszabályok alapján – 2019. január 1-től látja el a létfontosságú információs rendszerek és rendszerelemek, valamint az online piactér, internetes keresőszolgáltatás, és felhőszolgáltatások esetében az eseménykezelési feladatokat.

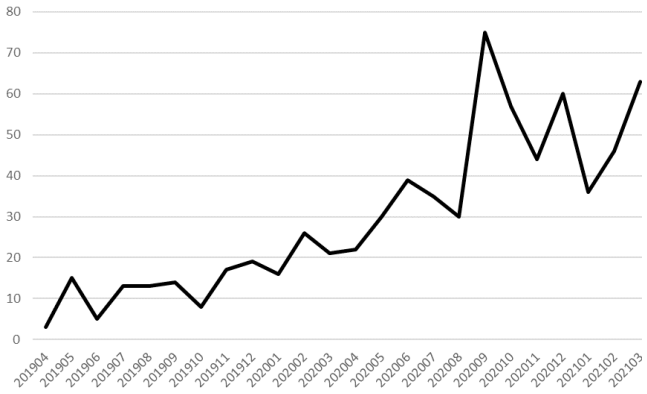
A hazai adatok azt mutatják, hogy 2020 március–áprilisában voltak jelentősebb számban események, majd azt követően csökkent az események száma, és kisebb időszakos változások voltak *(2. ábra)*.

Amennyiben ezen események szektoriális megoszlását vizsgáljuk, akkor egyértelműen látszik, hogy az állami és önkormányzati szervezetek esetében fordultak elő legnagyobb számban események. Ki kell emelni, hogy az oktatási intézmények is milyen „előkelő" helyen végeztek: az online oktatás bevezetése a 2020-as évben nagyon nagy lehetőséget teremtett a kiberbűnözők számára *(3. ábra)*.

A Nemzeti Kibervédelmi Intézet számára nemcsak szakmai, eljárásrendi kihívást jelentett és jelent a járvány, hanem a folyamatosan felmerülő kiberbiztonsági és védelmi kérdések miatt erőteljes kommunikációra is

3. ábra A Nemzeti Kibervédelmi Intézetnél a 2020-as évben regisztrált események megoszlása intézménytípusonként (Nemzeti Kibervédelmi Intézet saját adatai)

Az állami és önkormányzati szervek esetében közelíti az ezret az éves eseményszám. Az oktatási intézményeknél észlelt magasabb szám az online oktatás 2020. márciusi bevezetésével is magyarázható.



4. ábra A 2019. április 1. – 2021. március 31. között az USA Egészségügyi Minisztériuma felé kiberbiztonsági eseményt jelentő egészségügyi szolgáltatást nyújtó intézmények számának alakulása *(HHS 2021a)*

Jól látható, hogy a pandémia előretörésével folyamatosan nőtt a támadott intézmények száma, amely 2020 szeptemberében ért a csúcsra. Ennek következménye volt a CISA által 2020 októberében kiadott riasztás (CISA, 2020).

szükség van. 2020. október végéig a COVID–19-cel összefüggésben 2 riasztást, 3 közleményt, 5 információbiztonsági tippet és 17 cikket publikált az Intézet. Emellett a közösségi médiában 19 poszt és több mint 30 szereplés volt a járványhoz köthető.

Az egészségügy tekintetében érdemes kiemelni az USA egészségügyi kormányzata alatt működő központ adatait (Department of Health and Human Services – HHS) *(HHS 2021a)*, ahol 2010-től folyamatosan regisztrálják az egészségügyi intézmények eseményeit (ez nemcsak egészségügyi szolgáltatókat jelent, hanem egészségbiztosítókat, illetve egészségszervezéssel foglalkozókat, és minden, legalább 500 ügyfelet érintő eseményt jelezni kell). A 2020-as év adatai egyértelműen növekedést mutatnak az egészségügyi szolgáltatók esetében. Itt a növekedés már 2019 végétől megindult, és folyamatos. Érdemes kiemelni a 2020. szeptember–decemberi kiugrásokat. Azonban az adatok alapján úgy tűnik, hogy továbbra is magas az észlelt események száma *(4. ábra)*.

Egészségügy és nemzetbiztonság = egészségbiztonság?

Magyarország 2020-ban, a 1163/2020. (IV. 21.) Kormányhatározattal elfogadott Nemzeti Biztonsági Stratégiája kiemelten foglalkozik az egészségbiztonsággal is. A 169. pontban megfogalmazott megállapítás szerint „kiemelt figyelmet kell fordítani az egészségbiztonságra, amely a magas szintű egészségügyi ellátás mellett magában foglalja a természeti vagy civilizációs eredetű közegészségügyi és járványügyi kihívásokkal szembeni operatív és hatósági reagáló képességet is. Szélsőséges esetben készen kell állni a haderő alkalmazására járványügyi válsághelyzet elhárítása érdekében (kitelepítésben és karantén fenntartásában történő részvétel, személyi mozgások ellenőrzése, migrációs és bűnözési hullám megfékezésében történő részvétel, katonai kórházak működtetése stb.).” Az egészségbiztonsági kérdések azonban a XXI. században túlmutatnak a járványügyön, illetve nem értelmezhetők kizárólag az egészségügyi ellátás folyamatának biztonságaként. Szócska és Joó 2018-as tanulmányában mutatta be, hogy a folyamatok komplexitása, az egymással összefüggő rendszerek azt mutatják, hogy amikor egészségbiztonságról beszélünk, akkor ma már figyelembe kell venni olyan tényezőket és szempontokat is, mint például a környezeti tényezők, az egészségre károsan ható szerek kereskedelme (pl. dohányáruk), az elérhető információs anyagok megbízhatósága (social media és fake news jelentősége) vagy éppen az egészségügy által is használt kibertér biztonsága *(Szócska–Joó 2018)*.

Az egészségügynek van néhány jellemzője, amely kiberbiztonsági, és részben nemzetbiztonsági szempontból különleges helyzetet jelent az ágazat számára. A XXI. század elejére az egészségügy lett az az egyik ágazat, ahol a digitálisan keletkező adatok különleges jelentőséggel rendelkeznek. Az egészségügyi adatok keletkezésének napjainkra szinte végtelen forrása és lehetősége van, és az adat- és információtárolás és a számolási képességek növelése az egészségügyi adathasznosítás új perspektíváit nyitották meg. Ezek a kihívások és lehetőségek nemcsak az ágazaton belül dolgozók részéről kívánnak erőfeszítéseket, hanem olyan társtudományokkal és határterületekkel történő együttműködést is megkívánnak, mint a biztonságtudomány, az információbiztonság, vagy kifejezetten a kiberbiztonság *(Palicz–Joó 2020)*. Ki kell emelni, hogy az itteni adatvisszaélések hátterét az adatvezérelt egészségügyi megoldások előretörése, piacképessége adja, vagyis az itt keletkezett adat jelentős kutatás-fejlesztési és innovációs (KFI) potenciállal rendelkezik. Emellett fontos az is, hogy az adat nemcsak a KFI tevékenységet tudja támogatni, hanem az azonnali orvosi döntések alapja, illetve olyan érzékeny adat, amely a betegek számára érzékeny lehet (pl. pszichiátriai kezelés adatai), illetve akár az azonosításukra is alkalmas (biometrikus adatok). Ezt használják ki például a zsarolóvírus-támadás során, amikor az egészségügyi informatikai adatokat hozzáférhetetlenné téve kényszerítik ki, hogy a megtámadott fizessen.

Az emberi tényező

A kibertér biztonsága szempontjából mindig érdemes az emberi tényezőt az elsők között kiemelni. Egy 2020 májusában megjelent magyar tanulmány szerint számos olyan emberi tulajdonság van, amely a járvány kezdetétől növelte a pszichológiai manipuláció (social engineering) esélyét *(Oroszi 2021)*. Ezek közül a cikk kiemeli a következőket: félelem megléte, kíváncsiság, információéhség és tudásvágy, ismerethiány, figyelmetlenség és kapkodás, unalom. Emellett érdemes kiemelni, hogy ugyan a fenti publikáció nem egészségügy-specifikus, azonban számos

olyan vonatkozást és megállapítást tartalmaz, amely az egészségügyben dolgozókra is érthető. Kiemeljük ezek közül, hogy a social engineering típusú sérülékenységet fokozza az egészségügyi dolgozók alapattitűdje (segítőkészség), a járvány alatti munkaszervezési helyzetek (átvezénylések, új munkatársak megjelenése, gyors problémamegoldás, ismeretlenekkel való együttműködés szükségessége, új típusú feladatok megjelenése a szervezetben), valamint az aktuális munkaterhelésből adódó tényezők (fáradtság, túlterheltség, sietség és kapkodás, szabadság).

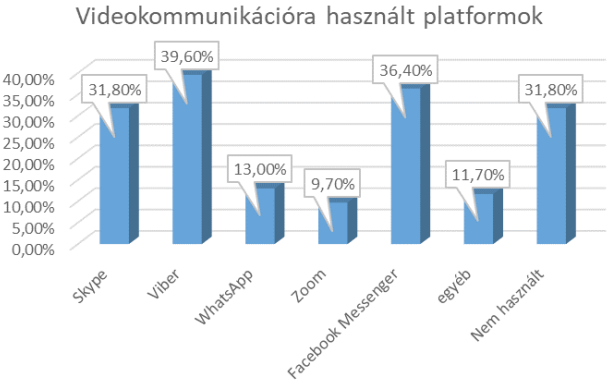
A fentieket erősíti az a 2020 elején végzett tanulmány is, amely kórházi dolgozók esetében kimutatta, hogy a munkaterhelés és a káros csatolmányra történő kattintás között szignifikáns összefüggés van, így a COVID–19 alatti extrém körülmények közötti betegellátás jelentősen megnövelheti a sikeres támadások esélyét, hiszen a maszkban, speciális öltözékben szinte megállás nélkül dolgozó egészségügyi munkatársak sokkal könnyebben kattinthattak egy-egy phishing e-mail csatolmányára a kimerítő nap során vagy nap végén *(Jalali et al. 2020)*.

A fentieket figyelembe véve a pszichológiai megtévesztésre (social engineering) alapuló támadásokra a COVID–19 járványidőszak alatt nagy esély van, és magas sikerrátával járhatnak, ezért a védelmi intézkedések kapcsán kiemelt figyelmet érdemelnek.

Telemedicina alkalmazások használata

Mint azt a bevezetőben is említettük, a mostani járványidőszaknak az egyik legfontosabb története kiberbiztonsági szempontból az volt, hogy a kontaktusszám csökkentése érdekében az online tér lehetőségeit a politikai és gazdasági döntéshozók a legszélesebb körben fel kívánták használni a járvány elleni küzdelemben. A távmunka és az otthoni oktatás olyan számban növelte meg a kibertérbe felkészületlenül érkezőket, hogy ez értelemszerűen eredményezte a kiberbűnözői aktivitás növekedését. Egy 2020 szeptemberében, információbiztonsági cégek által végzett kutatás alapján kiberbiztonsági szempontból a telehealth jelenti a legnagyobb fenyegetést az egészségügyre. Ezen belül az alkalmazások biztonsága, a végponti (készülék) biztonság, a hálózati biztonság és a frissítések kapcsán szükséges jelentős lépéseket tenni a biztonság növelése érdekében *(SecurityScorecard 2020)*.

Itt külön kell szót ejtenünk arról, hogy számos egészségügyi intézmény is biztosította a távolról történő munkavégzés lehetőségét. Ugyan bizonyos szakterületek esetében ez már régóta bevett szokás, hogy bizonyos munkafázisokat (pl. a képalkotó eljárások esetén a távdiagnosztizálás, leletezés) távolról végeznek, azonban ez 2020-ban általánossá vált. Emellett ki kell azt is emelni, hogy az orvos-beteg és az orvos-orvos kapcsolattartás is átterelődött az online térbe, amelynek jogszabályi kereteit a magyar kormány a 157/2020. (IV. 29.) Kormányrendelettel is biztosította már a járvány első hulláma során.



5. ábra Magyar háziorvosok által videokommunikációra használt platformok megoszlási gyakorisága 2020 augusztusában (válaszadók száma: 145) *(Hadi 2020)*

A 2020 augusztusában végzett felmérésben az alapellátásban dolgozó orvosok 68%-a már használt valamilyen videokommunikációs platformot.

A hazai alapellátásban dolgozók között 2020 augusztusában végzett saját kutatásunk (5383 bevont háziorvos, 145 kitöltés, online kérdőíves felmérés) jól mutatja *(5. ábra)*, hogy milyen széles körű az itt használt online kapcsolattartó platformok választéka *(Hadi 2020)*. A válaszadók 68%-a használt, vagy használ ma is ilyen videokommunikációs eszközöket az ellátás során, amelyek közül a Viber, a Facebook Messenger és a Skype volt a legnépszerűbb. A válaszadók közel 32%-a ugyanakkor nem használt még ilyen rendszert a munkája során *(5. ábra)*. A kutatás arra is rámutatott, hogy az alapellátásban dolgozók a választáskor nem tartották szem előtt az információbiztonsági és kiberbiztonsági szempontokat, elsősorban egy platform ismerete, és kényelmi szolgáltatások befolyásolták a döntést. A nem használóknak azt a további kérdést tettük fel, hogy amennyiben lenne egy országosan elérhető, speciálisan orvosok számára, kapcsolattartásra kifejlesztett videokommunikációs rendszer, szívesen használnák-e azt. Erre a kérdésre a 75%-uk (37 kitöltő) igennel válaszolt, amely azt jelezheti, hogy egy biztonságos, az egészségügyi folyamatokat figyelembe vevő, a magyar Elekronikus Egészségügyi Szolgáltatási Térhez kapcsolódó állami szolgáltatás esetén még kiterjedtebben lehetne alkalmazni ezt a korszerű ellátási formát.

Az orvosok és szolgáltatók által használt alkalmazások kockázatai miatt az amerikai kormány egészségügyi minisztériuma 2020 tavaszán ki is adott egy ajánlást, amelyben meghatározta azokat a szolgáltatásokat, amelyeket javasol az egészségügyi kapcsolattartásra, és amelyeket kifejezetten nem javasol (pl. TikTok, Facebook Live stb.) *(HHS 2021b)*.

Zsarolóvírus-támadások

Az elmúlt években az egészségügyi létesítmények esetében az egyik jellegzetes támadástípus a zsarolóvírus-támadás lett. Ennek hátterében támadói oldalról a gyors

megtérülés lehetősége áll, hiszen a mára már szolgáltatásként is igénybe vehető lehetőség (Ransomware-as-a-Service, RaaS) viszonylag kis pénzügyi ráfordítással elérhető, és gyors megtérüléssel kecsegtet, amellett hogy a támadó számára lehetőséget jelent az adatok másodlagos hasznosítására is *(Palicz et al. 2020)*. A COVID–19-járvány alatt lett egyre általánosabb a zsarolóvírusok azon képességének kihasználása, amely az adatokhoz történő hozzáférés révén lehetőséget teremt a támadónak arra, hogy akár érzékeny adatokat is közzétegyen, ezzel is kényszerítve a megtámadott intézményt a fizetési hajlandóság növelésére. Érdemes két esetet kiemelni. Az egyik eset az USA-ban történt, ahol a járóbeteg-ellátásban végzett béltükrözéses vizsgálatok eredményeit tették közzé, míg a másik esetben finnországi pszichiátriai gondozóintézet betegeinek adatait tették nyilvánossá. Ez utóbbi esetben a finn kormány rendkívüli összehívására is sor került a részletek tisztázása és a további teendők meghatározása érdekében *(BBC News 2020b)*.

A 2020-as évet és a járványidőszakot az egészségügyi zsarolóvírusok tekintetében azonban más ok miatt érdemes megjegyezni. Az egészségügyi szolgáltatók mint kritikus infrastruktúra-elemek, kiemelt szerepet játszanak az ellátásban, illetve gyakran az ellátás szervezésében is. Két eseményt emelünk ki: egyrészt 2020 őszén történt az első olyan halálozással járó eset, amelyet közvetlenül összefüggésbe hoztak egy zsarolóvírus-támadással, másrészt ekkor zajlott az USA kórházait érintő legnagyobb támadás, amelyek közül egy nagy országos hálózatot is érintett az egyik eset.

Az első olyan dokumentált klinikai ellátási esemény, amely halálos kimenetellel járt, és közvetlen összefüggésbe hozható egy zsarolóvírus-támadással, Németországban történt 2020 szeptemberében. A Düsseldorfi Egyetemi Kórházat egy DoppelPaymer zsarolóvírussal támadták meg. A ransomware-t használó, nem egészségügyi szektorra specializálódott kiberbűnözői csoport – amely egyébként a járvány elején deklarálta, hogy nem fogja támadni a járványkezelésben részt vevő egészségügyi szolgáltatókat – eredetileg az Egyetemet szándékozott megtámadni, azonban „félrement" a támadás, emiatt állt le az egyetemi kórház sürgősségi osztálya 2020. szeptember 11-én. A beérkező kritikus állapotú beteget a leállás miatt a 32 km-re levő wuppertali kórházba kellett volna szállítani, ami az azonnali ellátást egy órával késleltette, ezt a beteg már nem élte túl. A haláleset miatt ismeretlen tettes ellen nyomozást indítottak a német hatóságok *(Wired UK 2020)*.

2020 szeptemberében egy másik jelentős zsarolóvírus-támadás hívta fel a figyelmet arra, hogy az egészségügyi intézmények milyen mértékben vannak kitéve ezeknek a támadásoknak. Szeptember 27-én, egy vasárnapi nap reggelére az amerikai kontinensen több száz egészségügyi szolgáltatóval rendelkező Universal Health Services (UHS) rendszerében jelentős lassulásokat, indokolatlan leállásokat és a kommunikációs rendszer leállását tapasztalták. Ezt követően azonosították, hogy a Ryuk zsarolóvírus-támadás áldozatai lettek, és több napon keresztül kénytelenek voltak mellőzni az informatikai szolgáltatásokat: az orvosok és az egészségügyi személyzet a hagyományos papír-ceruza alapú dokumentációt voltak kénytelenek használni, és számos diagnosztikai és terápiás szolgáltatást nem tudtak teljesértékűen igénybe venni. A UHS rendszere az USA egyik legnagyobb egészségügyi szolgáltatója, körülbelül 400 egységgel, közel 90 000 munkavállalóval, és éves szinten 11,4 Mrd USD (3300 Mrd Ft) árbevétellel. Ezek az adatok nagyságrendileg hasonlóak a magyarországi egészségügyi rendszer főbb paramétereihez (~120 000 munkavállaló, éves egészségügyi kiadások kb. 2900 Mrd Ft).

Az egészségügyi intézmények, főként kórházak elleni fenyegetések a járvány első hullámától jelen voltak, amelyre a nemzetközi szervezetek a járvány kezdetétől *figyelmeztettek (Interpol 2020a)*. 2020. második felére olyan mértékűvé vált ez a fenyegetettség, hogy 2020. október végén az amerikai egyesült államokbeli nemzetbiztonsági szervezetek közös figyelemfelhívást tettek közzé az egészségügyi létesítményekkel kapcsolatos támadásokkal kapcsolatban *(CISA 2020)*.

Tesztelés, tesztelés, tesztelés? – a genetikai vizsgálatok biztonsági jelentősége

A járvány valamennyi időszakában, a kezdetektől a most zajló harmadik hullámban is, az egyik fontos szakmai kérdés az, hogy milyen mértékben érdemes a fertőzöttséget kimutató tesztvizsgálatokat elvégezni. A WHO ajánlása szerint az elvégzett tesztek száma, és azon belül a pozitív esetek aránya a járvány kontrollálásának egyik fontos mutatója. A tesztek hátterében többféle laboratóriumi módszer is létezik, azonban a legáltalánosabban elterjedt és a legmegbízhatóbb eljárás a genetikai vizsgálaton alapuló PCR (polymerase chain reaction – polimeráz láncreakció) vizsgálat. Ennek során a fertőzésgyanús személyből levett mintában próbálják kimutatni a vírusra specifikus genetikai szakaszt. A mintavétel kapcsán azonban a fertőzésgyanús személyből is kerülnek be olyan testnedvek, vagy akár hámszövetrészlet, amelyek akár az egyén genetikai vizsgálatára is alkalmasak lehetnek. A személy genetikai vizsgálata során feltárt gének lehetővé teszik azt, hogy valakit megváltoztathatatlanul azonosítsunk, vagy egy genetikai sorrend alapján meghatározzuk, hogy milyen betegségre van esélye, ez alapján specifikus terápia adható. A terápia azonban a meghatározott ponton ható gyógyszer mennyiségének növelésével méreggé válhat, így már nem gyógyít, hanem öl. Az eredmények nemcsak személyre szabottan, hanem egy-egy populáció, népcsoport, nemzet esetében is felhasználható bizonyos betegségek előfordulásának meghatározására. A kutatásokkal és a genetikai vizsgálatokkal kapcsolatos kockázatokra már 2020 májusában felhívta az FBI a figyelmet *(FBI 2021)*, amelyet 2021 februárjában a Nemzeti Kémelhárítási és Biztonsági Központ (National Counterintelligence and Security Center – NCSC) meg-

erősített *(NCSC 2021)*. A felhívásban rámutattak arra, hogy a kínai gyártók által uralt géntechnológiai piacon jelen levő készülékek lehetővé teszik, hogy nagy mennyiségű genetikai adat kerüljön át más nemzethez, ezzel személyes és nemzetbiztonsági kockázatot is előidézhetnek ezekkel a vizsgálatokkal. A felhívás természetesen nem a genetikai vizsgálatok szükségességét kérdőjelezi meg, hanem arra hívja fel a figyelmet, hogy a géntechnológiai vizsgálatok elvégzéséhez szükséges műszerek kiválasztásánál gondosan kell figyelni azok gyártójára, és a készülékek biztonságosságára, elsősorban arra, hogy milyen adatok kerülhetnek ki az adott vizsgálat elvégzése során.

Itt érdemes megemlíteni azt is, hogy a 2020-as év során több olyan kibertámadás is történt, amely kifejezetten kutatással foglalkozó akadémiai intézeteket, intézményeket támadott meg világszerte, így az ott végzett kutatások eredményeit felhasználva, vagy azokat módosítva befolyásolhatják a kutatás-fejlesztés innovációs potenciálját egy adott országnak vagy szektornak.

Kiberfenyegetések a vakcinációs folyamatra

A COVID-19-járvány leküzdésének leghatásosabb, és máig egyetlen eszköze a vírus ellen kifejlesztett vakcina. Ennek a leggyorsabb és legbiztonságosabb eljuttatása a fejlesztéstől a gyártón keresztül az oltási pontokig, a járvány elleni küzdelem egyik kritikus sikertényezője. Ezzel elérhető, hogy a veszélyeztetett csoportok számára megfelelően szervezett oltással a közösségek a leghamarabb elérjék a nyájimmunitás kialakulásához szükséges átoltottsági szintet. A fejlesztéstől a betegekig történő eljuttatás, és annak a dokumentálása során számos olyan „beavatkozási" pont létezik, amely a kiberbűnözői csoportok számára lehetőséget teremtenek rosszindulatú tevékenység kifejtésére.

Szinte a vakcinafejlesztés első pillanatától megjelent a fenyegetettség. 2020 júliusában jelezte az egyesült királyságbeli Nemzeti Kiberbiztonsági Központ (National Cyber Security Centre), hogy az orosz hátterű APT29 csoport megtámadta a vakcinafejlesztésben részt vevő szervezeteket *(National Cyber Security Centre 2020a)*. Az egyik ilyen egyesült királyságbeli gyógyszervállalat az AstraZeneca, amely az Oxfordi Egyetemmel közösen fejlesztett ki egy vektorvírus vakcinát, és a fejlesztésben sokáig elöl járt. Ezt a támadást a kanadai és USA-beli kibervédelmi kormányzati szervek is megerősítették. A jelentés nagyon óvatosan fogalmaz a szellemi tulajdonra vonatkozóan („highly likely with the intention of stealing information and intellectual property relating to the development and testing of COVID-19 vaccines"), és az ok-okozati összefüggés nehezen bizonyítható. Az azonban tény, hogy Oroszország 2020. augusztus elején az elsők között jelentette be a Szputnyik-V vakcina kifejlesztését, amely ugyanarra a technológiára épül, mint az AstraZeneca által kifejlesztett. 2020 végén az AstraZenecát ismételten kibertámadás érte, ezúttal észak-koreai államilag támogatott csoportot sejtettek a háttérben *(National Cyber Security Centre 2020b)*.

A vakcinafejlesztést követően a termékfejlesztési lánc következő lépésénél az egyik klinikai kipróbálást szervező nagy cégnél (IQVIA) 2020 októberében észleltek zsarolóvírus-támadást, amely több hétig lelassította a cég működését, azáltal a klinikai tesztelések folyamatát is. Érdemes megemlíteni, hogy a cég nemcsak a vakcinák klinikai kipróbálását szervezte (pl. az AstraZeneca vakcináét), hanem a Bristol Myers Squibb által gyártott COVID-19 diagnosztikai gyorstesztek kipróbálását is ők végezték. A Pfizer és a Johnson&Johnson vakcinája nem volt érintve ebben a támadásban. A támadók ebben az esetben teljesen ismeretlenek maradtak, még gyanú sem volt arra vonatkozóan, hogy honnan érkezhetett a zsarolóvírus *(CPO Magazine 2020)*.

A gyógyszerek engedélyezési folyamata sem maradt érintetlen kiberbiztonsági szempontból. 2020 decemberében jelezte az Európai Gyógyszerügynökség (European Medicine Agency – EMA), hogy támadás érte, és megkezdte a kivizsgálást *(EMA 2020)*. Ennek során derült fény arra, hogy nemcsak adatokat lophattak, hanem az adatintegritás is sérülhetett, ezzel befolyásolva a vakcinafejlesztés és az ehhez kapcsolódó hatósági értékelési folyamatok sebességét, illetve a kiszivárgott belső bizalmas levelezések módosítása alkalmassá válhatott a vakcinákba és az eljárásokba vetett bizalom megingatására *(HIPAA Journal 2021)*.

Ha a teljes ellátási láncot tekintjük, akkor a különleges gyártási, tárolási és szállítási körülmények is számos ponton jelentenek biztonsági kockázatot. Ennek veszélyére hívja fel a figyelmet a napokban megjelent USA-beli tanulmány, amely hangsúlyozza, hogy a logisztikai területet is egyre gyakrabban támadják zsarolóvírussal, amely nagymértékben veszélyezteti a vakcinák biztonságos eljuttatását az oltást végzőkhöz *(BlueVoyant 2021)*. Emellett az oltópontokon meglevő infrastruktúra és a betegek szervezésének szempontjai miatt további olyan lehetőségek vannak, amelyek jelentősen növelik a vakcinációs folyamat sérülékenységét.

Az aktualitása miatt érdemes kiemelni, hogy a lakossági oltás szervezéséhez szükséges informatikai infrastruktúra támadása, az adatok sértetlenségének módosítása, és az álhírek megjelenése több esetben is előfordult, ezzel okozva zavart az oltási folyamatban, lassítva azt, és részben csökkentve a lakosság bizalmát a kormányzati szervek munkájában. 2020 februárjában a magyar kormány által üzemeltetett, az oltásra jelentkezők regisztrációját biztosító koronavirus.gov.hu oldalt is megosztott terheléses támadás (DDoS) érte, amelyet sikeresen elhárítottak az állami szervek *(Magyar Kormány 2021)*.

A vakcináció kapcsán érdemes utalni a korábban már részletesebben kifejtett dezinformációs, „fake news" jelenségre is, amely komoly nemzetbiztonsági kockázatot jelent a jelenlegi COVID–19 vírushelyzetben.

Összegzés

A COVID–19-járvány mind nemzetközileg, mind a hazai környezetben kiberbiztonsági szempontból ambivalens helyzetet teremtett: miközben a folyamatos, magas szintű terhelés rávilágított a kiberbiztonsági Achilles-pontokra, ezzel együtt az események napvilágra kerülése, a hatóságok proaktív lépése jelentősen növelték a laikusok számára a téma ismertségét, amely kedvezően befolyásolta az együttműködést, és ezáltal a biztonságtudatosságot. A járvány ugyanakkor segítette bizonyos fogalmak és a párhuzamos értelmezések révén a kiberbiztonsági intézkedések egyszerűbb értelmezhetőségét, megértését. Gondoljunk csak arra, hogy mennyivel könnyebb elmagyarázni ebben a környezetben a számítógépes vírus fogalmát, vagy éppen a kézmosással kapcsolatosan a kézhigiéné fogalmából sokkal könnyebben értelmezhetővé válik a kiberhigéné fogalma, és az ehhez kapcsolódó tennivalók.

A hazai és a nemzetközi adatok alapján a 2020-as év kibervédelmi szempontból sok új területre is ráirányította a figyelmet. Itt nemcsak az egészségügyre mint a járvány alatt a kritikus infrastruktúrák egyik központi elemére gondolunk, hanem olyan új területek is középpontba kerültek, mint az online oktatás, vagy éppen a genetikai vizsgálatok nemzetbiztonsági jelentősége, vagy a nemzeti szinten jelentős kutatás-fejlesztési innovációs potenciállal rendelkező gyógyszerfejlesztés sérülékenysége. Ezek a területek új, speciális megközelítéseket igényelhetnek, és szoros együttműködés szükséges a különböző szereplők és a kapcsolódó tudományterületek között.

Irodalomjegyzék

1163/2020. (IV. 21.) Korm. határozat – Nemzeti Jogszabálytár (2020) https://njt.hu/jogszabaly/2020-1163-30-22.2 [Letöltve: 2021. 04. 22.]

157/2020. (IV. 29.) Korm. rendelet a veszélyhelyzet során elrendelt egyes egészségügyi intézkedésekről (2020) https://www.hbcs.hu/uploads/jogszabaly/3123/fajlok/157_feld.pdf [Letöltve: 2021. 04. 22.]

APWG (2020) *APWG Q3 Report: Four Out of Five Criminals Prefer HTTPS.* https://info.phishlabs.com/blog/apwg-q3-report-four-out-of-five-criminals-prefer-https

Bansak, C. & Starr, M. (2021) Covid-19 shocks to education supply: how 200,000 U.S. households dealt with the sudden shift to distance learning. *Review of Economics of the Household*, Vol. 19. pp. 63–90. https://doi.org/10.1007/s11150-020-09540-9

BBC News (2020a) *Google blocking 18m coronavirus scam emails every day.* https://www.bbc.com/news/technology-52319093 [Letöltve: 2021. 04. 22.]

BBC News (2020b) *Therapy patients blackmailed for cash after clinic data breach.* https://www.bbc.com/news/technology-54692120 [Letöltve: 2021. 04. 22.]

BlueVoyant (2021) *Cyber Security & Attacks in the Logistics Industry* | BlueVoyant. https://www.bluevoyant.com/resources/gated-resource/cyber-security-and-attacks-in-logistics/ [Letöltve: 2021. 04. 22.]

CISA (2020) *Ransomware Activity Targeting the Healthcare and Public Health Sector* | CISA. https://us-cert.cisa.gov/ncas/alerts/aa20-302a [Letöltve: 2021. 04. 22.]

CPO Magazine (2020) *Ransomware Attack on a Major Health Tech Firm Slows Down Several COVID-19 Clinical Trials.* CPO Magazine. https://www.cpomagazine.com/cyber-security/ransomware-attack-on-a-major-health-tech-firm-slows-down-several-covid-19-clinical-trials/ [Letöltve: 2021. 04. 24.]

EMA (2020) *Cyberattack on the European Medicines Agency* | European Medicines Agency. https://www.ema.europa.eu/en/news/cyberattack-european-medicines-agency [Letöltve: 2021. 04. 24.]

ENISA (2020) *ENISA Threat Landscape 2020 - Phishing.* ENISA. https://www.enisa.europa.eu/publications/phishing [Letöltve: 2021. 04. 22.]

FBI (2021) *People's Republic of China (PRC) Targeting of COVID-19 Research Organizations.* FBI. https://www.fbi.gov/news/press-rel/press-releases/peoples-republic-of-china-prc-targeting-of-covid-19-research-organizations [Letöltve: 2021. 04. 22.]

Hadi K. (2020) *A telemedicina alkalmazása a COVID-19 pandémia magyarországi kezelésében, különös tekintettel a kiberbiztonságra.* Szakdolgozat, Semmelweis Egyetem

HHS (2021a) U.S. Department of Health and Human Services Office for Civil Rights, Breach Portal, Cases Under Unvestigation https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf [Letöltve: 2021. 04. 22.]

HHS (2021b) *Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency* | HHS.gov. https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html [Letöltve: 2021. 04. 22.]

HIPAA Journal (2021) *Hackers Leak Data Stolen in European Medicines Agency Cyberattack.* https://www.hipaajournal.com/hackers-leak-data-stolen-in-european-medicines-agency-cyberattack/ [Letöltve: 2021. 04. 24.]

Interpol (2020a) *Cybercriminals targeting critical healthcare institutions with ransomware.* https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware [Letöltve: 2021. 04. 22.]

Interpol (2020b) INTERPOL report shows alarming rate of cyberattacks during COVID-19. https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 [Letöltve: 2021. 04. 22.]

Jalali, M. S., Bruckes, M., Westmattelmann, D., & Schewe, G. (2020) Why employees (still) click on phishing links: Investigation in hospitals. *Journal of Medical Internet Research,* Vol. 22. No. 1. e16775. https://doi.org/10.2196/16775

Magyar Kormány (2021) *Összehangolt kibertámadás indult a kormányzati oldalak ellen.* https://kormany.hu/hirek/osszehangolt-kibertamadas-indult-a-kormanyzati-oldalak-ellen?fbclid=IwAR2yvVAm3BohhS_08mXo8HdY9Xs8gcoaqcSSTY9Y3daWJE10Uzc886fWPxo [Letöltve: 2021. 04. 22.]

National Cyber Security Center (2020a) *Advisory: APT29 targets COVID-19 vaccine development.* NCSC.GOV.UK. https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development [Letöltve: 2021. 04. 22.]

National Cyber Security Center (2020b) *NCSC response to speculation about cyber attacks.* NCSC.GOV.UK. https://www.ncsc.gov.uk/news/ncsc-response-to-speculation-about-cyber-attacks-on-uk-coronavirus-research [Letöltve: 2021. 04. 22.]

NCSC (2021) *China's collection of genomic and other healthcare data from America: risks to privacy and U.S. economic and national security.* https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021.pdf [Letöltve: 2021. 04. 22.]

NKI (2020) *Riasztás egészségügyi intézményeket érintő Emotet terjesztési kampánnyal kapcsolatban.* Nemzeti Kibervédelmi Intézet. https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-egeszsegugyi-intezmenyeket-erinto-emotet-terjesztesi-kampannyal-kapcsolatban/ [Letöltve: 2021. 04. 22.]

Oroszi, E. D. (2021) *Social Engineering a koronavírus tükrében, avagy a rendkívüli helyzetet kihasználó támadási technikák és megelőzésük*. Dunakavics, Vol. VIII, No. V, pp. 5–20.

Palicz, T. & Joó, T. (2020) Az infrastruktúra-védelem és az információbiztonság kapcsolata. In: Deák V. (ed.) *Az IBTV. gyakorlata*. Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, 2020, pp. 21–31. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15923/Az%20Ibtv.%20gyakorlata%20Eves%20tovabbkepzes%20felelos%20vezeto.pdf?sequence=3

Palicz, T., Sas, T., Tisóczki, J., Bencsik, B. & Joó, T. (2020) „Pénzt vagy életet!" – Zsarolóvírusok az egészségügyi informatikai rendszerekben ["Your money or your life!" – Ransomwares in healthcare information systems]. *Orvosi Hetilap,* Vol. 161. No. 36. pp. 1498–1505. https://doi.org/10.1556/650.2020.31788

Privátbankár.hu (2020) 900 százalékkal nőtt a koronavírus-álhírek száma. https://privatbankar.hu/cikkek/makro/5-osszeeskuves-elmelet-a-koronavirusrol.html [Letöltve: 2021. 04. 23.]

SecurityScorecard (2020) Listening to Patient Data Security: Healthcare Industry and Telehealth Cybersecurity Risks. https://securityscorecard.com/resources/healthcare-industry-telehealth-cybersecurity-risks-report [Letöltve: 2021. 04. 24.]

Szerencsés, V., Palicz, T., Joó, T., Lám, J., Demeter-Fülöp, V. & Ugrin, I. (2021) A Covid19 járvány során hozott egészségügyi intézkedések és hatásaik Magyarországon és Ausztriában. *Belügyi Szemle,* Vol. 69. No. 1. pp. 123–142. https://doi.org/10.38146/BSZ.2021.1.6

Szócska, M. & Joó, T. (2018) Health Security Issues. In: Finszter G. & Sabjanics I. (eds) *Security Challanges in the 21st Century*. pp. 335–347. Dialóg Campus, 2018, https://www.bm-tt.hu/assets/letolt/secchal21.pdf.

The Hacker News (2021) *European Authorities Disrupt Emotet – World's Most Dangerous Malware*. https://thehackernews.com/2021/01/european-authorities-disrupt-emotet.html [Letöltve: 2021. 04. 22.]

Vraga, E. K. & Bode, L. (2020) Defining Misinformation and Understanding its Bounded Nature: Using Expertise and Evidence for Describing Misinformation. *Political Communication,* Vol. 37. No. 1. pp. 136–144. https://doi.org/10.1080/10584609.2020.1716500

WHO (2020) *Situation Report-13.* 20200202-sitrep-13-ncov-v3.pdf (who.int) [Letöltve: 2021. 04. 22.]

Wired UK (2020) *The untold story of a cyberattack, a hospital and a dying woman* | WIRED UK. https://www.wired.co.uk/article/ransomware-hospital-death-germany [Letöltve: 2021. 04. 22.]

Wosik, J., Fudim, M., Cameron, B., Gellad, Z. F., Cho, A., Phinney, D. & Tcheng, J. (2020, June 1). Telehealth transformation: COVID-19 and the rise of virtual care. *Journal of the American Medical Informatics Association,* Vol. 27. No. 6. pp. 957–962. https://doi.org/10.1093/jamia/ocaa067

Zarocostas, J. (2020) How to fight an infodemic. *Lancet,* Vol. 395. No. 10225. pp. 676. https://doi.org/10.1016/S0140-6736(20)30461-X