SZABÓ HEDVIG

KIBERBIZTONSÁG A KORONAVÍRUS-JÁRVÁNY IDEJÉN
A COVID-19 NEMZETBIZTONSÁGI ASPEKTUSAI

Nemzetbiztonsági Szakszolgálat, főigazgató

Absztrakt

A tanulmány a koronavírus járvány kiberbiztonsági és nemzetbiztonsági tapasztalatairól ad áttekintést. Összefoglalja a COVID-19 vírussal kapcsolatos applikációkat, így a kontaktkutató, a telemedicina, valamint a karantén alkalmazásokat. Foglalkozik a koronavírus alatti informatikai támadásokkal, továbbá az álhírek terjedésével. A tanulmány kitér a távmunka és a kapcsolattartás biztonsági kérdéseire is, majd egy olyan összegzéssel zárul, amely megmutatja, hogy a pandémiás tapasztalatokból milyen tanulságok szűrhetők le, és hogyan kell felkészülni egy esetleges, új, ismeretlen kihívásra.

Kulcsszavak: pandémia, kiberbiztonság, nemzetbiztonság, informatikai támadások

CYBER SECURITY DURING THE CORONAVIRUS EPIDEMIC - NATIONAL SECURITY ASPECTS OF COVID-19

Abstract

The study deals with the question of cyber security and national security during the pandemic. The analysis sums the apps regarding the coronavirus like the apps about curfews, telemedicine and contact tracks. The cyberattacks and the spreading of fake news are issues in it. The document writes about the security challenges of the home office and the remote education. The study finally concludes the information and communication technology consequences of the experiences during the pandemic and how we can prepare for new, unknown uncertain challenges.

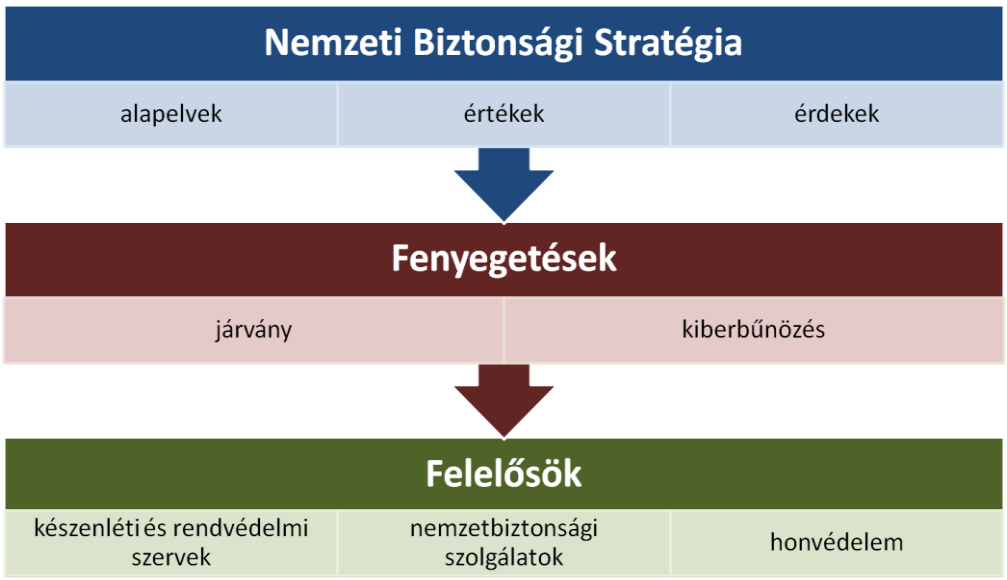
Keywords: pandemic, cyber security, national security, cyberattacks

Bevezetés

2020-ban a SARS-CoV-2[13] vírustörzs okozta COVID-19 betegség megjelenése miatt Magyarországon a veszélyhelyzet kihirdetéséről szóló 40/2020. (III. 11.) Korm. rendelettel március 11-től kihirdették az egészségügyi veszélyhelyzetet, amelynek eredményeként a távolságtartás, az otthoni munkavégzés válik alapértelmezett munkavégzési és viselkedési móddá. Ezzel egyidejűleg az információs és kommunikációs eszközök használata még elterjedtebbé, egyes feladatokban kizárólagossá vált, amely már önmagában növelte az állampolgárok, a gazdasági társaságok, az állami szervek kibertámadásokkal szembeni kitettségét. Ennek fényében érdemes vizsgálni, hogy a nemzetbiztonsági alapdokumentumok mennyire azonosították azokat a problémákat, melyek 2020 első negyedévében jelentkeztek.

A veszélyhelyzet kihirdetésénél még a 2012-ben Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozattal elfogadtatott Stratégia volt hatályban, amely már Magyarországot érintő biztonsági fenyegetések, kihívások között tartja számon a kiberbiztonság megteremtését, és már a járványok elleni védekezést célzó közegészségügyi felkészülést is beemelte a végrehajtandó feladatok közé. A kiberbiztonság biztosításának keretében elsődleges feladat a kibertérben ténylegesen jelentkező vagy potenciális fenyegetések és kockázatok rendszeres felmérése, valamint priorizálása. (1. ábra)

[13] SARS-CoV-2: severe acute respiratory syndrome coronavirus 2 - súlyos akut légzőszervi szindróma - koronavírus 2



1. ábra: Kiberbiztonság - nemzetbiztonság

Forrás: Saját szerkesztés

Az új – a 163/2020. (IV. 21.) Korm. határozattal kihirdetett – Nemzeti Biztonsági Stratégia már bőven a pandémia ideje alatt jelenik meg 2020 áprilisában, amely az elmúlt időszak változását lekövetve kiemelt biztonsági kockázatnak tekinti az információs és kommunikációs technológiából, a digitalizációból eredő fenyegetettségeket és kihívásokat, valamint a járványos betegségek magyarországi megjelenését és gyors terjedését.

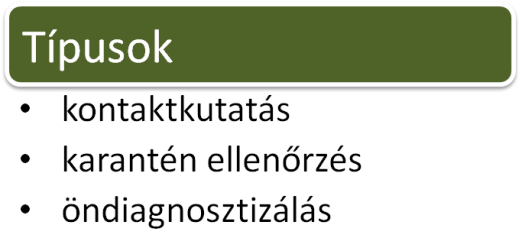
A veszélyhelyzet ideje alatt a két kiemelt kockázat, az egészségügyi veszélyhelyzet és a kiberbiztonságot veszélyeztető események egymásra gyakorolt hatásáról tapasztalatot szereztünk, melyből már tanulságok is levonhatók.

Koronavírus és kiberbiztonság / COVID-19 applikációk

A veszélyhelyzet kihirdetésével az állampolgároknak, a kormányzati szerveknek és a gazdasági társaságoknak is újra kellett gondolni a mindennapi működési célokat. Ezek közül a legfontosabbá az élet és az egészség védelme vált, de a működőképesség fenntartása is kiemelt fontosságot élvezett.

Az informatikai szakma a koronavírus-járvány idején azonnal reagált az ágazatra jellemző gyorsasággal és rugalmassággal. Ennek eredményeként számos olyan informatikai alkalmazás született, amely segítette a fő prioritást élvező, az élet és az egészség védelmével kapcsolatos feladatokat, infokommunikációs eszközökkel és technológiával megtámogatva.

Az élet, a testi épség megőrzése érdekében három irányra fókuszáltak a fejlesztések és kutatások, úgymint a kontaktkutatást elősegítő alkalmazások, a karantén ellenőrzés támogató fejlesztések, valamint az öndiagnosztizálást lehetővé tevő kutatások. (2. ábra)



2. ábra: COVID-19 applikációk

Forrás: Saját szerkesztés

Az öndiagnosztizálást segítő alkalmazásokkal kapcsolatos kutatások, fejlesztések nem a koronavírus járvány alatt kezdődtek. Az infokommunikációs szolgáltatások fejlődése az egészségügyi ágazatot sem kerülte el, számos rendszer került kialakításra, amely a diagnosztizálást és a terápiás kezelések támogatását célozta.

A telemedicina[14] részét képező távfelügyeleti, távkonzílium eljárások alkalmazását a koronavírus járvány alatt az illetékes minisztérium szabályozta a veszélyhelyzet ideje alatt az egészségügyi szolgáltatások nyújtásához szükséges szakmai minimumfeltételekről szóló 60/2003. (X. 20.) ESZCSM rendelettel, így a rendelet szerint az egészségügyi szolgáltatás nyújtásának és finanszírozási elszámolásának nem feltétele a beteg személyes jelenléte, ha az ellátás sajátosságai és orvosszakmai megítélése ezt lehetővé teszik.

2020-ban az általános telemedicina fejlesztések mellett megjelentek speciálisan már a Sars-CoV-2 vírusra reagáló, diagnosztikát segítő alkalmazások. A legismertebb ilyen kutatást a Massachusetts Institute of Technology (MIT)[15] végezte el. A fejlesztés mesterséges intelligencia modellt alkalmazva tudja megállapítani a tünetmentes COVID fertőzés lehetőségét mobiltelefonnal rögzített erőltetett köhögési minták alapján. Ebben az esetben a kutatók nem a nulláról indultak, mert már a járvány előtt is foglalkoztak azzal a megoldandó feladattal, hogy hogyan lehetséges köhögésmintából azonosítani betegségeket. A kutatók

[14] „A telemedicina tehát olyan infó-kommunikációs eszközzel támogatott diagnosztikus vagy terápiás-, távfelügyeleti eljárás, amelyben az egészségügyi szakszemélyzet szükségszerű beteg melletti jelenlétét on line elektronikus kapcsolaton keresztül távolról pótolják.” Egészségügyi Fogalomtár. https://fogalomtar.aeek.hu/index.php/Telemedicina [Letöltve: 2021.01.23.]

[15] IEEE Journal of Engineering in Medicine and Biology COVID-19 Artificial Intelligence Diagnosis using only Cough Recordings Authors: Jordi Laguarta, Ferran Hueto, Brian Subirana [Letöltve: 2021.01.25.]

összegyűjtöttek több mint 70.000 rögzített mintát, amely 200.000 köhögést tartalmazott. Az eredményeket követően a MIT kutatói egy céggel együttműködve folytatták a közös munkát, annak érdekében, hogy hogyan lehet beépíteni a kutatás eredményét egy egyszerűen kezelhető alkalmazásba.

A pandémia járványhatósági intézkedései indították a fejlesztések egy másik típusát, amelyek a karantén szabályok betartásával kapcsolatos applikációk megjelenését hozták magukkal.

A járványügyi védekezés egyik alapja, hogy a fertőzöttek és a velük szoros kontaktba kerülők ne tudják továbbadni a vírust egészséges embereknek. Az állam feladata ebben az esetben az, hogy ezt biztosítsa, melynek ellenőrzése két módon valósítható meg, úgymint rendőrségi személyes, helyszíni ellenőrzéssel vagy infokommunikációs eszközök (ICT) támogatásával.

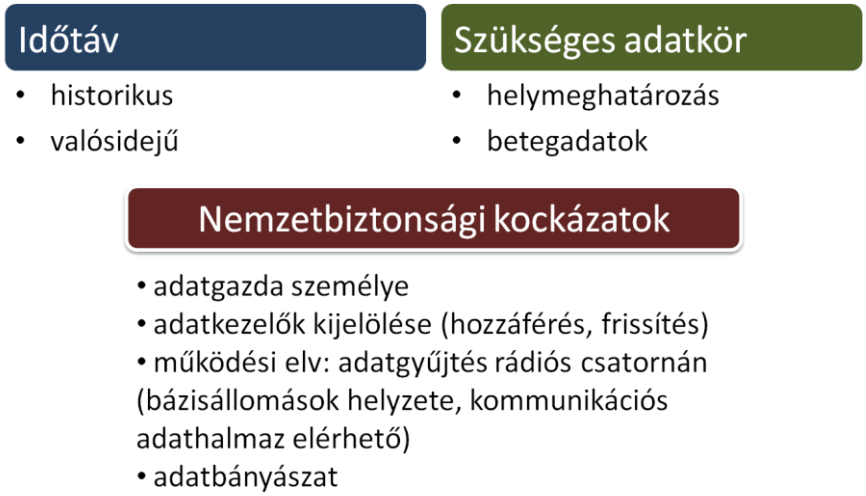
Számos alkalmazás jelent meg különböző országokban, így Magyarországon is. A Házi Karantén Rendszer (HKR)[16] olyan alkalmazás, amely segít ellenőrizni a COVID-19 fertőzés miatt hatósági házi karanténba rendelt személyek esetében a karantén szabályainak betartását, és lehetővé teszi a karanténra kötelezett betegek nyilvántartását, illetve felügyeletét. A szabályok értelmében, amennyiben a technikai feltételek adottak, a rendszer használata kötelező, ezzel biztosítva az érintettnek egy ICT megoldást a karantén szabályainak betartására. Ezzel az alkalmazással megelőzhető, hogy a rendvédelmi szervek fő feladatává váljon a karantén ellenőrzése. A HKR okostelefonra tölthető le, alkalmazás áruházakból (Google Play, AppStore). A karantén ideje alatt a HKR rendszer véletlenszerűen generált időpontokban távellenőrzési kéréseket küld a felhasználónak rövid szöveges üzenet (sms) útján, melyeket a felhasználó mobilkészüléke használatával egyszerűen teljesíthet. Távellenőrzési kérés esetén annak beérkezését követő 15 percen belül szükséges a HKR alkalmazás elindítása a mobil készüléken, majd a távellenőrzési kérés teljesítése. A rendszer automatikusan több képet készít a felhasználóról, ami alapján igazolja a személyazonosságát, illetve tartózkodási helyét, amit összevet a regisztráció során megadott házi karantén címével.

Mielőtt rátérek a COVID-19 applikációk harmadik nagyobb csoportjára, foglalkoznunk kell a megjelent alkalmazások biztonsági kérdéseivel is.

[16] https://hazikaranten.hu/ [Letöltve: 2021.01.25.]

A járvánnyal összefüggő fejlesztések – valamennyi fejlesztés – a biztonsági kérdéseken túl azért érdemelnek kiemelt figyelmet, mert ezek a fejlesztések érzékeny egészségügyi adatokról szólnak.

A koronavírus elleni küzdelmet támogató informatikai alkalmazások közül a kontaktkutató alkalmazások vetették fel a legtöbb nemzetbiztonsági kérdést. (3. ábra)



3. ábra: Kontaktkutatás – adatvédelem vs. nemzetbiztonsági érdek

Forrás: Saját szerkesztés

A pandémia első hullámában a fertőzött ember kontaktjainak megtalálása jelentette az egyik legnagyobb kihívást, mert nem állt elég járványügyi szakember rendelkezésre, hogy el lehessen végezni rövid idő alatt a kontaktkutatást. Erre a feladatra az ICT eszközök, technológiák alkalmazása ésszerű megoldásnak tűnt. Jelentős számú fejlesztéseket indítottak el az államok azzal a módszertannal, hogy az embereknél lévő mobiltelefonok nyújtsanak segítséget a kontaktkutatásban. Ennek az lett az eredménye, hogy 71 ország 120 alkalmazása érhető el kontaktkutatásra. Az applikációkból az Egyesült Államokban alkalmazzák a legtöbbet, szám szerint 23-t.[17]

A kontaktkutató alkalmazások működése általában három féle elv szerint, vagy azok kombinációján alapult, úgymint a bluetooth (kis hatótávolságú rádiós kapcsolatot lehetővé tevő szabvány), a GPS (globális helymeghatározó rendszer), valamint a Google és Apple-s API (alkalmazásprogramozási felület) technológiában lévő lehetőségeket használták ki. A kontaktkutató appok kifejlesztése mögött az a cél állt, hogy a járvány terjedését akadályozzák.

[17] https://www.top10vpn.com/ [Letöltve: 2021.01.26.]

A tényleges eredmény eléréséhez azonban szükségessé vált az egyes embereknél, valamint az emberek tömegénél megismerni legalább a helyadatokat (hol jár, kivel találkozik), valamint a betegségre vonatkozó adatokat (fertőzött, nem fertőzött). Így a cél érdekében alkalmazott módszer az adott ember szintjén felveti a személyhez fűződő adatok védelmének kérdését (mellyel ez a tanulmány nem foglalkozik), továbbá az emberek tömegéről történő adatgyűjtés esetén már az alkalmazás biztonságának nemzetbiztonsági vetületét is.

A kontaktkutató applikációk esetén nemzetbiztonsági kockázat elemzést igénylő kérdésként merülnek fel az alábbi témák:

- csak az egyes ember kap értesítést a saját fertőzött kontaktjairól (és már nem lát rá az adatokra) vagy
- központi helyen is tárolásra kerülnek a keletkezett tömeges adatok,
- ez hol van tárolva (külföldön, Magyarországon),
- ez megbízható módon személytelenítve van-e,
- a hely adat meghatározás esetén ki fér hozzá a hírközlési szolgáltatóknál rendelkezésre álló torony adatokhoz, cella adatokhoz,
- mennyire egyediesíthető a személy mozgási térképe,
- az adatok esetén ki az adatgazda, ki vesz részt az adatkezelésben, az adatfeldolgozásban.

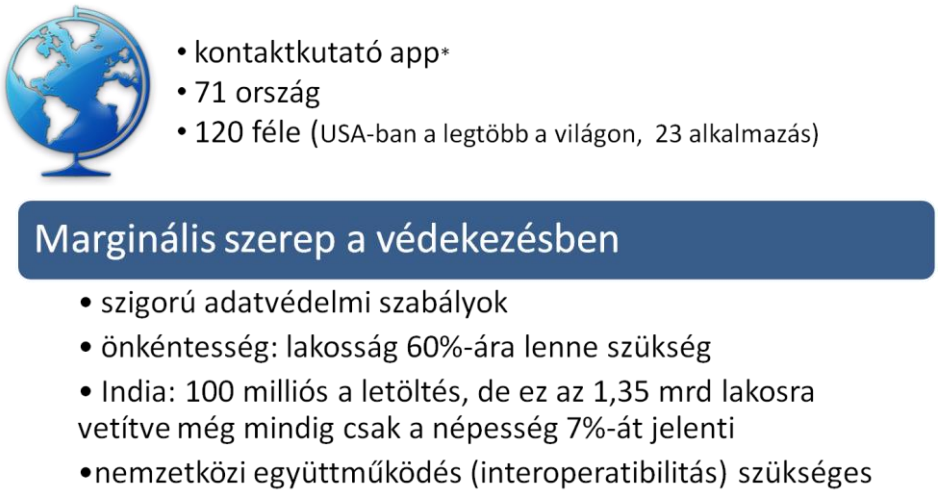
A kockázat elemzés alapján a kontaktkutató appok nemzetbiztonsági kitettségét az adott országban úgy lehetett csökkenteni, hogy a fejlesztéssel foglalkozó szervezetek, az adatgazdai jogokat gyakorlók, az adatfeldolgozásban részt vevő személyek, gazdasági társaságok nemzetbiztonsági kockázatot nem jelentő körből kerülhettek ki, az adatfeldolgozás és adatkezelés, adattárolás csak az adott ország jogszabályainak megfelelően történhetett. A hírközlési szolgáltatók adatokat csak a hírközlési jogszabályoknak megfelelően adhatták át.

A koronavírus applikációk megjelenésével egyidejűleg a nemzetbiztonsági problémák mellett kibervédelmi támadások is azonosításra kerültek. Legismertebb példa a Domaintools[18], a kiberbiztonsági kutatóintézet által azonosított coronavirusapp elnevezésű weboldal, mely támogatta a Covidlock zsarolóvírus letöltését. A honlap azt hirdette látogatóinak, hogy töltsenek le egy androidos applikációt a koronavírus terjedésével összefüggésben, és amikor a letöltés megtörtént, az alkalmazás zárolta a képernyőt. Mindez

[18] https://www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware [Letöltve: 2021.01.26.]

egy olyan honlapról történt, mely feltüntetett az oldalán egy igazolást az Egészségügyi Világszervezettől (World Health Organization) és a Járványügyi Megelőző Központtól, ennek ellenére a gyanútlan felhasználók egy képernyő zárolást használó zsarolóvírushoz jutottak a letöltéssel, de koronavírussal kapcsolatos információhoz nem.

A biztonsági problémák mellett érdemes vizsgálni, hogy a kontaktkutató appok milyen hatékonysággal tudtak működni, mennyire bizonyultak hatékony eszköznek a járvány elleni küzdelemben. Az Oxfordi Egyetem kutatói által publikált matematikai modell[19] szerint a kontaktkutató alkalmazások akkor tudtak volna segíteni megállítani a fertőzés terjedését, ha a lakosság megközelítőleg 60%-a töltötte volna le és használta volna a kontaktkutatást segítő alkalmazást. Bár a letöltések számában volt kontaktkutató app, mely rekordot döntött, az Aarogya Setu által fejlesztett app Indiában 13 nap alatt 50 millió letöltést ért el, mellyel megelőzte az addigi rekorder Pokémon GO-t is, és jelenleg 100 milliós letöltésnél jár, de a matematikai modell számítása szerint ez még így is jelentősen alatta van a teljes lakosság 60%-ának (India lakossága 1.35 Milliárd fő). Hogy hogyan lehetett volna megközelíteni az ideális értéket, azt nehéz megválaszolni. Tényként azonban megállapítható, hogy a legtöbb országban az alkalmazások letöltése önkéntes alapon történt adatvédelmi okok miatt, amely az egyik terjedési korlátot jelentette. A példában említett Indiában ugyan kötelező volt letölteni az alkalmazást, ennek ellenére jóval alatta volt a fertőzés terjedésének megakadályozásához szükséges letöltésszámnak. (4. ábra)



4. ábra: Koronavírus elleni küzdelmet támogató alkalmazások

Forrás: Saját szerkesztés

[19] https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown [Letöltve: 2021.01.25.]

Koronavírus és nemzetbiztonság / Álhírek

Általánosságban elmondható, hogy az álhírek az olyan hamis információkat tartalmazó hírek, amelyeket úgy tesznek közzé és hirdetnek, mintha azok valódiak lennének. A járvánnyal kapcsolatosan is számos hír látott napvilágot, mely a vírus eredetét, terjedését, gyógymódját, emberekre gyakorolt hatását (továbbá még számos egyéb, járvánnyal összefüggő kérdést), a hivatalos és tudományos álláspontól eltérő tényezőkkel hozta összefüggésbe. Ezeknek a híreknek azonban kétséges a valóságalapja, és általában semmilyen tényszerű bizonyítékot sem találni rájuk. Az álhírek mind nemzetbiztonsági, mind kiberbiztonsági szempontból veszélyt jelenthetnek. (5. ábra) A koronavírus járvány alatt számos adathalász kampány is álhíreket tartalmazott (ilyenek voltak pl. az egészségügyi intézmények nevében kiküldött tájékoztatók – melyben felhívást intéztek cégekhez, jelezzék, ha egészségügyi maszkot kérnek, mert rendelkezésre áll, ehhez adják meg az adathalászok által megszerezni kívánt adatokat). Továbbá figyelmet érdemel az is, hogy az álhírek – tartalmuktól függően – alkalmasak lehetnek akár a közrend megzavarására, titkosszolgálati befolyásoló műveletek támogatására.

5. ábra: Az álhírterjesztés céljai

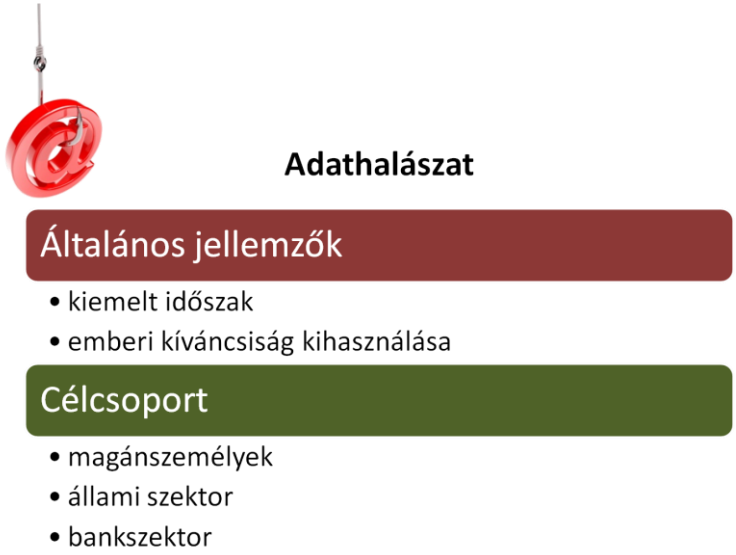
Forrás: Saját szerkesztés

Koronavírus és kiberbiztonság / kibertámadások

A koronavírus járvány idején a nemzet- és kiberbiztonsági kihívások nemcsak az erre a célra fejlesztett applikációkkal összefüggésben jelentkeztek, hanem a megváltozott

körülmények is teremtettek számos olyan lehetőséget, amelyek a kiberbűnözők előtt újabb távlatokat nyitottak.

A vírushelyzet ismeretlen volta miatt az emberek fokozott érdeklődést mutattak minden olyan információ, ismeret után, ami a koronavírusra vonatkozott. Számos hír, statisztika, tematikus honlap és közösségi (social) média bejegyzés foglalkozott a témával. Az emberek minden információra „ugrottak", hogy az ismeretlentől való félelmük enyhülni tudjon. Ezt a félelmet használták ki a hackerek. A koronavírus-járvány terjedésével arányos növekedést mutatott a pandémiával összefüggő adathalász incidensek száma, amelyeket jellemzően az adathalász e-mail-ek rosszindulatú csatolmányaival juttattak el az áldozatokhoz. (6. ábra) Ezek sok esetben nemzetközi szervezetek, egészségügyi intézmények (pl. a WHO, Magyarországon: EMMI, NNK) nevében íródott levelek, amelyek érzékeny személyes adatok megszerzésére irányuló káros programokat terjesztettek. Továbbá a csalók – a pandémiát és az emberek kíváncsiságát kihasználva – már célzott adathalász módszerekkel is igyekeztek rávenni az áldozatokat pénzátutalások indítására vagy szenzitív – például banki – adatok megadására.

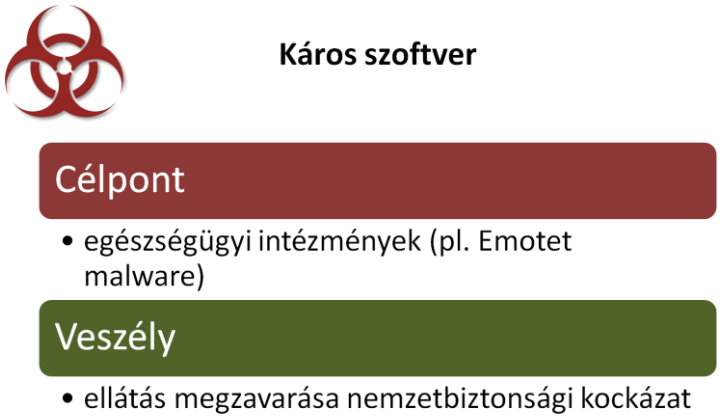


6. ábra: Az adathalászat jellemzői, célcsoportjai

Forrás: Saját szerkesztés

A koronavírus-járványt nem csak az adathalászok használták ki, hanem a káros szoftverek (malware-k) terjesztői is lehetőséget kaptak. (7. ábra) Egy ilyen tipikus példa az Emotet malware, mely alig néhány év alatt egy egyszerű banki adatlopásra szakosodott trójaiból (egy olyan rosszindulati program, mely mást tesz a háttérben, mint amit a felhasználónak mutat), egy kiváló rejtőzködési lehetőségekkel bíró, komplex károkozó

szoftverré nőtte ki magát, amelyet a gazdasági társaságokra nézve egyik legnagyobb veszélyt jelentő kiberfenyegetésnek tartottak 2019-ben. Az Emotet már a koronavírus járvány előtt is emberek, cégek és kormányzati szervek ellen indított támadásokkal próbált pénzügyi/banki és személyes adatokat megszerezni. Az Emotet alkalmazói a járvány előtt is általában a nagy érdeklődésre számot tartó lehetőségeket használták ki, így pl. az Edward Snowden könyv world[20] változatát ígérték Spam kampányként, a pandémia alatt vírussal kapcsolatos információkat ígértek kéretlen levelekkel. Magyarország is az Emotet malware terjesztői célpontjává vált, és beazonosítottan[21] az Állami Egészségügyi Ellátó Központ, illetve a Szabolcs-Szatmár-Bereg Megyei Kórházak és Egyetemi Oktatókórház nevében kerültek kiküldésre olyan e-mail-ek, melyek csatolmányai megnyitás után futtatták az Emotet malware-t. Az egészségügyi intézmények nevében kiküldött e-mail-ekre általában jellemző volt, hogy a COVID-19 járvánnyal kapcsolatos teendőkre hivatkoztak, a levéltörzsben pedig valódinak tűnő, korábbi levelezésre való hivatkozással próbálták elérni a csatolmány megnyitását, továbbá a levelek aláírásmezőjének tartalma szintén teljesen valósághűnek tűnt.



7. ábra: A káros szoftver

Forrás: Saját szerkesztés

Ahogy az Emotet-es példából is látszik, a pandémia alatt előtérbe kerültek az egészségügyi vonatkozású támadások. A támadások azon része, mely magát az egészségügyi intézményt célozza, külön figyelmet érdemel, mert az egészségügyi intézmények létfontosságú intézmények, feladatellátásuk zavarmentessége a veszélyhelyzet, a járvány nélkül is alapvető érdek. A kórházak, egészségügyi intézmények ellen irányuló támadások

[20] https://blog.malwarebytes.com/botnets/2019/09/emotet-malspam-campaign-uses-snowdens-new-book-as-lure/ [Letöltve:2021.01.26.]

[21] https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-egeszsegugyi-intezmenyeket-erinto-emotet-terjesztesi-kampannyal-kapcsolatban/ [Letöltve: 2021.01.26.]

nemzetbiztonsági kockázatot jelentenek, mert az ellátó rendszerek kiesését okozhatják, közvetlen életveszélyt teremtve. A kiberbűnözöket azonban ez sem tartja vissza általában vagyoni haszonban megjelenő céljaik elérése érdekében. A legismertebb nagyobb volumenű támadás célpontja a Universal Health Services (UHS) volt. Az UHS az Egyesült Államokban és az Egyesült Királyságban évente 3,5 millió beteget lát el, és a kibertámadás következtében több mint 400 kórház és egészségügyi intézménynél állt le az informatikai rendszer a világjárvány időszakában. Az incidens következtében az érintett kórházak a sürgősségi ellátást felfüggesztették, és a betegeket más kórházakba irányították át. Hogy ez a páciensek szempontjából milyen egészségügyi következménnyel járt, arra nincs adat. De az adatok ismerete nélkül is bátran kijelenthető, hogy a támadás mértéke már nemzetbiztonsági szempontból is értékelendő esemény volt.

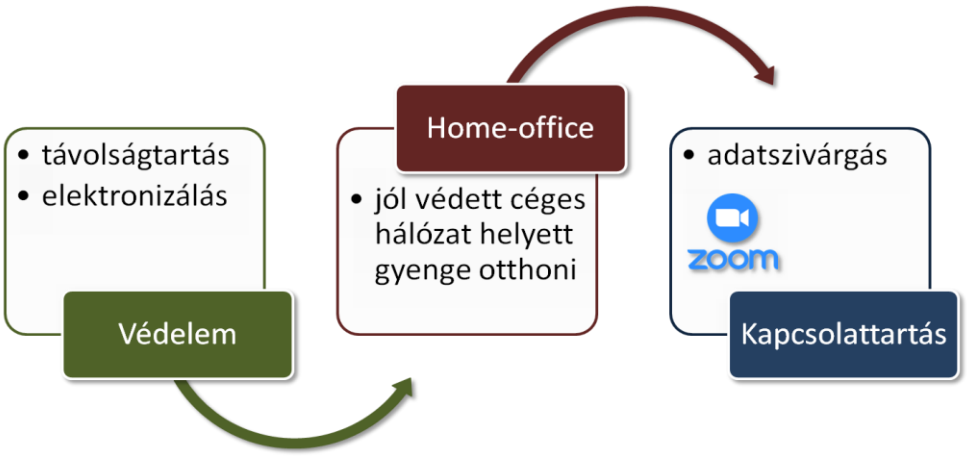
A tanulmány írásának idején tette közé az Europol[22], hogy 2021. január 27-én széleskörű rendvédelmi és ügyészségi összefogással sikerült semlegesíteni az elmúlt évtized legkártékonyabb botnet hálózatát, az Emotet-et úgy, hogy a nyomozóhatóságok átvették az irányítást az Emotet terjesztésében közreműködő IT infrastruktúra felett, nemzetközi akció keretében. A művelet egy egyedülállóan új megközelítést alkalmazott, mivel a rendvédelem a kiberbűnözés elleni harcban eddig még nem alkalmazta azt a módszert, hogy ténylegesen megsemmisítsék az Emotet működését támogató infrastruktúrát.

Koronavírus és kiberbiztonság / otthoni munkavégzés

A koronavírus járvány egyik első intézkedése az volt, hogy a nemzeti kormányok azt javasolták mindenkinek, hogy aki megteheti, az dolgozzon home office-ban. Hogy ezt ténylegesen meg lehessen tenni, ahhoz a cégeknek/munkáltatóknak komoly intézkedéseket kellett tenni az IT rendszerek átalakítása érdekében. (8. ábra) Elsődleges feladat volt megfelelő számú eszköz biztosítása – átcsoportosítással, vásárlással, bérléssel – az otthoni munkavégzéshez. Emellett szükséges volt a megfelelő szoftverkörnyezet kialakítása, a belépések, hitelesítések, jogosultságok szabályozása, a munkavégzés ellenőrzése, valamint az ehhez szükséges adatvédelmi szabályozás elkészítése, illetve a dolgozók számára szükséges oktatások megtartása. Ezek a teendők, amelyek a működés fenntartásához szükségesek voltak, nagyjából le is kötötték a rendelkezésre álló IT szakértők teljes kapacitását, és az olyan

[22] https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action [Letöltve: 2021.01.26.]

feladatokra, mint a biztonság igen kevés idő és energia maradt. Így jellemzővé vált, hogy az informatikai tevékenység jelentős része áttevődött a jól védett, céges hálózatokról a gyenge védettséggel rendelkező, otthoni rendszerekre. A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézetének IT szakértői[23] meghatározták, hogy milyen paramétereket kell figyelembe venni, ha kiberbiztonsági szempontból biztonságossá akarjuk tenni az otthoni munkavégzés IT támogatását. A teljesség igénye nélkül, a következő felsorolás tartalmazza, hogy mire kell figyelmet fordítani, ha az otthoni munkavégzés IT minimum biztonsági követelményeit meg akarjuk teremteni. Ezek a következők: az ellenőrzött eszközök alkalmazására, az eszközökhöz való hozzáférések kezelésére/korlátozására, a távoli bejelentkezésekhez kétfaktoros azonosítás használatára, védelmi megoldások alkalmazására, egy megfelelő feladatkiosztó program használatára, a távoli munkavégzéshez szükséges együttműködési eszközök használatára (videokonferencia, chat, konferenciahívás), az internetkapcsolatok szabályozására (Wifi), külső eszközök használatának szabályozására/korlátozására, mentések készítésére, helpdesk szolgáltatás biztosítására, az adatok védelmére, megfelelő szintű jelszavas védelem alkalmazására. Ha ezek a biztonsági megoldások alkalmazásra kerültek, akkor már csak egy kiemelt tényezőre kellett figyelmet fordítani, a munkavállalóra. Arra, hogy az IT biztonság szempontjából az egyik leglényegesebb elem is megkapja azt a tudást, képzést, hogy ne saját maga veszélyeztesse az információbiztonságot.



8. ábra: Az otthoni munkavégzés miatti veszélyek

Forrás: Saját szerkesztés

[23] https://nki.gov.hu/it-biztonsag/hirek/biztonsagos-home-office/ [Letöltve: 2021.01.26.]

Koronavírus és kiberbiztonság / kapcsolattartás

Az otthoni munkavégzés, a kijárási tilalom, a távolságtartás, a digitális oktatás megkövetelte, hogy a kapcsolattartás formái és eszközei is megújuljanak. Értelemszerűen itt is a már meglévő infokommunikációs lehetőségek kerültek alkalmazásra. A kiválasztás szempontja a funkcionalitás volt és nem a platform biztonsága.

A legelterjedtebbek alkalmazások közé tartozott a Zoom, a Google Meet, a Microsoft Teams, a Cisco Webex, a Skype, a Jitsi Meet, a WhatsApp és a Signal. Ezek a platformok nemcsak a felhasználók közötti hang és kép továbbítására alkalmasak, hanem általában lekezelik a csoportmunkát, a képernyőmegosztást, a felvétel készítést és a rögzítést. Hogy melyik alkalmazást, mikor lehet használni, milyen biztonsági elvárásoknak kell megfelelnie, az nagyban függ a résztvevőktől (feladatuktól, beosztásuktól), illetve a tárgyalt téma érzékenységétől, esetleg minősített voltától. Számos IT biztonsággal foglalkozó szervezet – az Európai Unió Kiberbiztonsági Ügynöksége (ENISA), valamint az Egyesült Államok Nemzetbiztonsági Ügynöksége (NSA), továbbá a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézete – tette közé, hogy milyen szempontokat kell mérlegelni, amikor videokonferencia alkalmazást választunk.

Egy, talán a legismertebb (de biztonsági szempontból mindenképp a leghírhedtebb) videokonferencia alkalmazás, a Zoom biztonsági helyzetét érdemes elemezni. 2019 decemberében az egynapi felhasználók száma 10 millió fő volt, mely 2020 márciusában már 200 millióra emelkedett. A felhasználók között maga Boris Johnson, az Egyesült Királyság miniszterelnöke is megtalálható volt, aki 2020. március 24-én tweetelte, hogyan csatlakozik az első videokonferenciás kormányüléshez.

A Zoom problémái[24] között elsőként az adatmegosztással kapcsolatosak vetődtek fel, így egy Kaliforniában indított per irataiból derült ki, hogy a vállalat iOS-es alkalmazása külső felekkel, többek között közösségi média szolgáltatókkal is megosztotta felhasználóinak adatait, azok megfelelő tájékoztatása nélkül. Másik súlyos probléma a végponttól végpontig terjedő (az end to end) titkosítás kapcsán merült fel. A cég weboldalán azt állította, az online meetingek végpontok közötti titkosítással biztosíthatók, valójában azonban szó sem volt hasonló védelemről (ez azóta javításra került). Úgyszintén megkérdőjeleződtek az adatvédelmi szabályok, mikor nyilvánosságra került, hogy a vállalati felhasználóknak nyújtott

[24] https://blog.zoom.us/ [Letöltve: 2021.01.26.]

megoldással az adminisztrátorok jelzést kaphatnak, ha egy-egy felhasználónál a Zoom alkalmazás fél percnél hosszabb időre kerül háttérbe - és az is követhető vele, hogy épp milyen programok futnak a számítógépen (ez a probléma is javításra került azóta). Egy Zoomos biztonsági probléma még önálló nevet is kapott, ez a Zoombombing, amelynél egy-egy video beszélgetésbe idegenek hívatlanul be tudtak csatlakozni, kameraképükön pedig obszcén tartalmakat jeleníthettek meg. Ezt az tette lehetővé, hogy a rendszer minden híváshoz egy 9, 10 vagy 11 jegyű, véletlenszerűen generált ID-t hoz létre, amelynek birtokában csatlakozni lehet az adott beszélgetéshez, a belépéshez pedig az alkalmazás alapértelmezetten nem kér jelszót. Így a tréfás kedvű felhasználók néhány tetszőleges karaktersort végigpróbálgatva random videokonferenciákban köthetnek ki, amelyeket aztán oda nem illő tartalmakkal áraszthatnak el - a hatékonyabbak akár brute force megoldásokkal is végigpróbálgathatják a lehetséges azonosítókat. (Az oktatási intézményeknél módosította a Zoom az alapbeállításokat, miután az FBI riasztást adott ki az iskoláknak.)

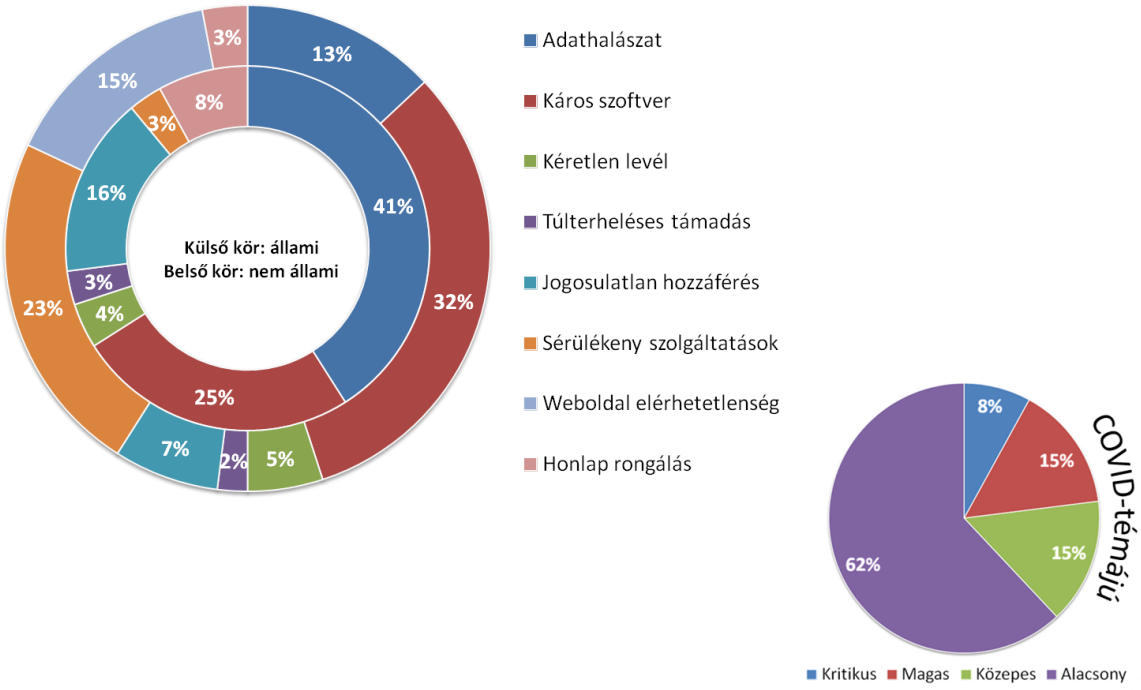
Ahogy a Zoom példája is mutatta, az idő előrehaladásával a videokonferencia alkalmazások biztonság szempontjából is jelentős fejlődésen mentek keresztül.

A járvány kiberbiztonsági tanulságai

Becslések szerint a kibertámadások – járvány nélkül is – éves szinten 400 milliárd eurós veszteséget okoznak a globális gazdaságban. Ha a Google adatait vizsgáljuk[25] azt látjuk, hogy 2020 április második hetében naponta 18 millió olyan rosszindulatú e-mail-t azonosítottak, amelyek küldői kifejezetten a COVID-19 okozta nehézségeket igyekeztek kihasználni. Továbbá, 240 millió spam üzenetet küldtek, amely szintén a járványról szóló tartalommal bombázta a felhasználókat, valamint 18 millió elektronikus levél kifejezetten bizalmas információk megszerzését célzó, rosszindulatú fájlokat vagy hivatkozásokat tartalmazott.

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézete (NKI) a koronavírus járvány alatt is nyomon követte az informatikai incidenseket Magyarországon. Az IT kihívások volumene jelentősen növekedett, továbbá a támadások típusa is követte az előző évek tendenciáit, de megjelentek a COVID-19 tematikájú támadások. (9. ábra)

[25] https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond [Letöltve: 2021.01.26]



9. ábra: 2020. I. félévben rögzített incidensek
Forrás: Nemzeti Kibervédelmi Intézet

A biztonsági problémák ellenére a pandémia megmutatta, hogy veszélyhelyzetben valódi kihívások felmerülése esetén a kreativitás és innováció alkalmazásával gyorsan megoldhatóvá vált a távmunka, a távoktatás és a kapcsolattartás. A tapasztalatok azonban azt is megmutatták, hogy a biztonság egy olyan terület, amelyre előre is fel lehet készülni. Fő feladat, hogy minden szervezetnek (gazdasági társaságnak, kormányzati szervnek) fel kell készülnie egy újabb, hasonló helyzet kezelésére, ahol mind a szükséges infokommunikációs eszközök biztosítása, mind a biztonság szempontjainak való megfelelés kulcsfontosságú lesz.

Technológiai oldalról kiemelt fontosságú a jól kiválasztott, megbízható infrastruktúrák és alkalmazások használata, a jogosultságok, hitelesítések, biztonságos kapcsolatok (például VPN) kialakítása, a rendszeres mentések rendje. Nem lehet elfeledkezni a megfelelő vírusvédelemről, mind a szerverek, mind a végpontvédelemre kiterjedve.

Humán oldalról a felkészüléshez szükséges a kollégák rendszeres IT biztonsági képzése, továbbá a home office alatti időszakban azoknak a felelősöknek a kijelölése, akik a felmerülő üzemeltetési és biztonsági kihívásokat azonnal kezelik, a hibákat a legrövidebb idő alatt kijavítják, szükség esetén távsegítséget nyújtanak.

Végül, de nem utolsósorban nélkülözhetetlen a biztonságtudatos hozzáállás, mert ne feledjük, hogy a kiberbiztonság közös érdekünk!

Irodalomjegyzék

Laguarta, J., Hueto, F., Subriana, B. (2020) COVID-19 Artificial Intelligence Diagnosis using only Cough Recordings. *IEEE Open Journal of Engineering in Medicine and Biology*, Vol. 1. pp. 275-281. ISSN: 2644-1276. DOI: 10.1109/OJEMB.2020.3026928 https://ieeexplore.ieee.org/document/9208795/metrics#metrics [Letöltve: 2021.01.25.].

Internetes források

Biztonságos home office. Nemzeti Kibervédelmi Intézet, weboldal. https://nki.gov.hu/it-biztonsag/hirek/biztonsagos-home-office/ [Letöltve:2021.01.26.].

Digital contact tracing can slow or even stop coronavirus transmission and ease us out of lockdown. University of Oxford/Our Research/Coronavirus Research. https://www.research.ox.ac.uk/Article/2020-04-16-digital-contact-tracing-can-slow-or-even-stop-coronavirus-transmission-and-ease-us-out-of-lockdown [Letöltve: 2021.01.26.].

Kumaran, N., Lugani, S. (2020) *Protecting businesses against cyber threats during COVID-19 and beyond*. Blog, Identity and Security. https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond [Letöltve: 2021.01.26].

Riasztás egészségügyi intézményeket érintő Emotet terjesztési kampánnyal kapcsolatban. Nemzeti Kibervédelmi Intézet, weboldal. https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-egeszsegugyi-intezmenyeket-erinto-emotet-terjesztesi-kampannyal-kapcsolatban/ [Letöltve: 2021.01.26.].

Saleh, T. (2020) *CovidLock: Mobile Coronavirus Tracking App Coughs Up Ransomware.* Blog, Domaintools Research. https://www.domaintools.com/resources/blog/covidlock-mobile-coronavirus-tracking-app-coughs-up-ransomware [Letöltve: 2021.01.26.].

Telemedicina. Egészségügyi Fogalomtár. https://fogalomtar.aeek.hu/index.php/Telemedicina [Letöltve: 2021.01.23.].

Threat Intelligence Team (2020) *Emotet malspam campaign uses Snowden's new book as lure.* Blog. https://blog.malwarebytes.com/botnets/2019/09/emotet-malspam-campaign-uses-snowdens-new-book-as-lure/ [Letöltve: 2021.01.26.].

World's most dangerous malware Emotet disrupted through global action. Europol, weboldal. https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action [Letöltve: 2021.01.26.].

https://blog.zoom.us/ [Letöltve: 2021.01.26.].

https://hazikaranten.hu/ [Letöltve: 2021.01.25.].

https://www.top10vpn.com/ [Letöltve: 2021.01.26.].