EVENTS IN THE CYBERSPACE UNDER COVID-19

ESEMÉNYEK A KIBERTÉRBEN A COVID-19 JÁRVÁNY IDEJÉN

KUN Tamás[1]

Abstract

In the mists of the pandemic, hackers do not rest. A 'great' opportunity for them to exploit the uncertainty of these days and to sabotage national healthcare systems, that were in combat with the virus, so the protection of IT systems could be fall behind with the priorities, often remains on the theoretical basis, that is because of the criminal activities that happened recently. At the start of the year and the new decade, the Coronavirus Disease (COVID-19) created stressful circumstances all over the world, that took time even for the World Health Organization (WHO) to address that pandemic worldwide. The growth of cyber-attacks against medical institutions are showing ascending tendency, so the development and defense of these systems will be a determining issue for the following years. The successful defence sometimes not only technological issue, rather the quality of the human factor. In most cases, the attackers breaching over the loose ends of top secured systems, so the best practice should be controlling these at organizational level.

Keywords

IT security, cyber activities, pandemic, critical infrastructures

Absztrakt

A járványhelyzet idején a hackerek nem pihennek. Egy remek lehetőség számukra ugyanis, hogy a kiszámíthatatlan helyzetben, ami jellemzi a mindennapokat államok egészségügyi szervezeteinek működését szabotálják, amelyek éppen a vírus elleni küzdelemmel vannak nagyobb részben elfoglalva, így az informatikai rendszerek védelme nem feltétlenül prioritás, gyakran csak elméleti szinten valósul meg, mert ezt alátámasztják a megtörtént bűncselekmények, amelyek nemrégiben bekövetkeztek. Az új évtized kezdetén a COVID-19 nevet viselő új koronavírus meglehetősen stresszes körülményeket generált szerte a világban, még az Egészségügyi Világszervezet (WHO) is csak késlekedve minősítette világjárványnak azt. Az egészségügyi intézmények ellen elkövetett kibertámadások az utóbbi években növekvő tendenciát mutatnak, így ezeknek a rendszereknek a fejlesztése és védelmének javítása meghatározó témája lesz a következő éveknek. A sikeres védekezés viszont sokszor nem technológiai kérdés, hanem az emberi tényező minősége. A támadók az esetek döntő többségében a gyenge láncszemeken keresztül jutnak be a legvédettebb rendszerekbe, így a legjobb megoldás ezt szervezeti szinten kezelni.

Kulcsszavak

IT biztonság, kibertevékenységek, járványhelyzet, kritikus infrastruktúrák

[1] kun.tamas@phd.uni-obuda.hu | ORCID: 0000-0002-6620-7157 | PhD student/doktorandusz | Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Az elmúlt néhány évben egyre inkább közkedvelt célpontjaivá váltak a kritikus infrastruktúrák a kibertérben tevékenykedő szereplők számára, azonban maga a fogalom is vitatott, hogy mi számít kritikus infrastruktúrának. A magyar jogi szabályozás létfontosságú rendszerelemként is számon tartja ezeket az intézményeket, amelyeknek tartós kiesése a napi működésből beláthatatlan következményekkel járhat. Egy dolog azonban egészen bizonyos, a kórházak a társadalom kiemelt fontosságú rendszerelemei, azok részleges leállása is emberéletek kockán forgásával jár. Az egészségügyi adatok az Általános Adatvédelmi Rendelet (GDPR) alapján is érzékeny (sensitive) személyes adat [1] kategóriába tartoznak, azok védelme és kompromittálódásának elkerülése prioritást élvez az adatvédelem területén.

ANYAG ÉS MÓDSZER

A vizsgálat tárgyát képezik azok a kibertevékenységek és intézkedések, amelyek a COVID-19 világjárvánnyal kapcsolatosan vagy annak tematizálásával kerültek fókuszba. Ezek az események azért fontosak, mert világszerte nemzetközi forgalmi korlátozások, közösségi távolságtartásra vonatkozó szabályozások vannak érvényben, amelyeknek hatásait csak azok feloldását követően leszünk képesek értékelni, valamint mérni a hatásait. A jelenlegi helyzet alapvető sérülékenységi faktorát tekintve elmondható, hogy az esetek/próbálkozások számát tekintve jelentős potenciállal bír a járványhelyzet kihasználása a pszichológiai manipulációs technikák alkalmazását illetően. Ez a környezet továbbá lehetőséget nyújt arra is, hogy a potenciális áldozatok száma növekedjen, tekintettel a kilátástalan helyzetre, valamint az általános bizonytalanságra, amely jellemzi a mindennapokat. Világszerte a jogi eszközökkel és egyéb jogosítványokkal felhatalmazott kormányok és szervezetek igyekeznek az általános pánikhelyzet elkerülésére, valamint a lépcsőzetes lazításra és a folyamatos visszatérésre törekednek a megszokott életvitel felé. Azonban a kibertér szereplőit a támadói oldalon motiválja a zavart állapot, hiszen az emberi tényező ebben a szituációban újabb és újabb sérülékenységeket generál. Ilyen sérülékenységi pont lehet akár a távmunka általánossá válása is, az otthonról végzett munka esetében a belső hálózatok szigorú szabályrendszerével ellentétben külső hozzáférési pontokról csatlakoznak a munkavállalók, előfordulhat az is, hogy saját eszközökről, amelyek biztonsági szintje megkérdőjelezhető. Fő irányvonalként a járvány megjelenésének idejétől (2019 december) a közelmúltig (2020 április) terjedő időszakot tekintem, helyenként viszont korábbi évek trendjeire is utalok. A tanulmányban szereplő események a források megjelenési idejét alapul véve vannak időrendi sorrendben.

EREDMÉNYEK

Zsarolóvírusos támadások egészségügyi rendszerek ellen

2018-ban az egészségügyi szervezetek a negyedik legáltalánosabb célpontjai (7%) voltak a zsarolóvírusos (ransomware) támadásoknak az iparági megoszlás alapján, egy 2019-ben megjelent a Cylance kiberbiztonsági vállalat elemzésében [2]. “Néha a zsarolóvírus olyan, mint az influenza. Amint a kórházak megoldást találnak a védelemre, egy új és

kifinomultabb verzió üti fel a fejét.” 2019 decemberében Hackensack Meridian Health csoport, amely 17 korházat számlál New Jerseyben lévő székhellyel, megerősítette, hogy fizetett a zsarolóknak annak érdekében, hogy újra hozzáférjen az informatikai rendszereihez. Ebből az következett, hogy a rendszerek két napig nem voltak elérhetők, és az osztályokat nem kritikus folyamatainak újra szervezésére, papíralapú dokumentálásra kényszerítette az elektronikus megoldások helyett. [3] „Ne vessük el azonnal a váltságdíj kifizetésének lehetőségét.” mutat rá Robert Garrett, a Hackensack Meridian Health igazgatója. A továbbiakban leszögezi, hogy sok esetben nem áll módunkban alkudozni a támadókkal, mert nem vagyunk abban a luxusban, hogy újraépítsük a rendszereinket, az idő szorít bennünket. [4] Amit ebben az esetben megfigyelhetünk, az a teljes kiszolgáltatottság. Egy kórházigazgató szemszögéből nézve az álláspont helytálló, viszont védelmi szempontból a kapitulációval egyenlő. Sokszor hivatkoznak ilyen típusú esetekben a szakértők véleményére a döntéshozók, hogy mennyire helyes vagy sem váltságdíjat fizetni. Újra felmerül a kérdés, hogy a kibertevékenységek terrorista, adott esetben háborús cselekményeknek azonosíthatók e, viszont az elkövető személy/csoport jellemzően rejtve marad. A kibertámadásokkal kapcsolatban általában elmondható, hogy a visszakövetési folyamatban (IP-címek visszakövetése) csak országokig jutunk el, tehát annyit tudunk meghatározni, hogy melyik országból érkezhetett a támadás, a konkrét elkövető nemzetisége sem határozható meg sok esetben, ezért „casus belli” (háborús indok) sem fogalmazható meg.

Átfedések a koronavírus járvánnyal kapcsolatban

A Yoroi olasz hátterű kiberbiztonsággal foglalkozó vállalat szokásos vizsgálatai során egy „CoronaVirusSafetyMeasures_pdf” állományra figyelt fel, amelynek jobban utána jártak. Itt egy átlagos social engineering taktikáról, egy phishing típusú támadásról beszélhetünk, a fentebb említett állomány egy email csatolmányát képezhette, egy külön erre kialakított tesztkörnyezetben hajtották végre a feltárást. A fájl megnyitása után több művelet zajlik le, először egy TLS alapú védett kapcsolatot alakít ki, amely egy “share.]dmca.]gripe” elérési útvonalú fájlmegosztóra mutat, ezt a fájlból kinyert mintából is ki tudták olvasni. Ezután néhány script fut le, amelyek megalapozzák a fertőzést, kulcsok generálódnak a beállításjegyzékben (1. ábra), amelyek segítenek elkerülni a számítógép újraindításával kapcsolatos eljárásokat. Végeredményképpen a felállított kapcsolat alapján adathalászatra kiválóan alkalmas fertőzéses támadásról van szó. [5]

1. ábra: A malware sematikus fertőzési útvonala [5]

Amit ebben az esetben láthatunk az a szokásos eszköztár: tömeges vagy célzott célpont irányába elkészített levél és egy vagy több álcázott melléklet az aktuális téma alapján.

A COVID-19 keretei között éppen azért kiemelten veszélyesek ezek a próbálkozások, mert egy olyan világjárványról van szó, amellyel kapcsolatban minden egyes esemény egyenesen internetközpontú terjesztéssel is rendelkezik. A világ országaiban a meghatározó médiumok napi szinten számolnak be a „fejleményekről" idővel a társadalom teljesen elveszíti a napi rutinját a kitörést megelőző időkkel szemben. Felerősödik a „rugalmas" megoldások alkalmazása, széles körben terjednek el az internetalapú távoli hozzáférés útján történő munkavégzési megoldások, ezzel pedig újabb sebezhetőségek jelennek meg.

CISA ajánlás a COVID-19 keretében jelentkező kockázatkezelésben

A kibertevékenységek elemzése során célszerű nem csak a támadási eseményeket górcső alá venni, hanem annak fontos elemeit is, mint például a kritikus infrastruktúrák és az ellátási láncok, mert ezeknek a rendszereknek, intézményeknek, folyamatoknak a működtetése a rendkívüli helyzetben kiemelten fontos, valamint deklarálja azt a környezetet, ahol a támadók potenciális célpontjai találhatók.

Az Egyesült Államok Védelmi Minisztériuma (DHS) márciusban mind a járványhelyzettel, mind a kiberbiztonsági eljárásokkal kapcsolatban tesz javaslatokat, ahol több kulcsterületet határoz meg:

Infrastruktúra védelmi intézkedések (Kritikus Infrastruktúrák)

- Kijelölni a koordináló személyt és speciális felelősségi kört rendelni hozzá
- Kivitelezni egy hivatalos munkavállalói és munkahelyvédelmi stratégiát
- Képezni a munkavállalókat a személyes és munkahelyvédelmi stratégiákra
- Kiépíteni és tesztelni a rugalmas munkavégzés feltételeit és munkarendjének szabályozását
- Azonosítani a kritikus folyamatokat, javakat és szolgáltatásokat, amelyek elősegítik a szükséges működést
- Meghatározni, hogy mennyi ideig képes nélkülözni a szervezet a működéshez szükséges utánpótlásokat a csökkentett termelési kapacitások tekintetében
- Azonosítani és priorizálni a szükséges áruk és szolgáltatások beszállítóit
- Folyamatosan értékelni az aktív készültségi szintet a tervcélok elérése érdekében, vizsgálni azoknak hatásait, illetve az eseményeket, amelyek a megváltozott üzleti tevékenységből és társadalmi-gazdasági viszonyokból fakadnak
- Követni a szövetségi, állami, helyi, törzsi és területi COVID-19 tartalmú információs portálokat naprakész információért az enyhítéssel és társadalmi elszigeteléssel kapcsolatos stratégiákhoz [6]

Ellátási lánccal kapcsolatos intézkedések

- Mérlegelni a kieséseket az ellátási láncban a nemzetközi termelés és szállítás lassulásából fakadóan, ami a COVID-19 miatt jelentkezik
- Egyeztetni a szállítókkal bármely nehézség kapcsán, ami a helyzetből ered, illetve amire a jövőben számítani lehet
- Azonosítani az alternatív forrásokat a készletek, helyettesítő termékek és/vagy védelmi intézkedések területén, amelyek a zavarok enyhítését célozzák

Kapcsolatot létesíteni a törzsvásárlókkal, folyamatosan tájékoztatni az érdekükben tett enyhítésekkel kapcsolatos lépésekről [6]

Kiberbiztonsági intézkedések szervezetek számára

Biztosítani a rendszereket, amelyek távoli hozzáférést tesznek lehetővé

- Meggyőződni arról, hogy VPN kapcsolat van alkalmazásban, valamint a rendszerek naprakészek
- Fejleszteni a rendszerellenőrzést annak érdekében, hogy minél előbb információhoz jussunk szokatlan működés esetén
- Többlépcsős azonosítás alkalmazása
- Meggyőződni arról, hogy minden eszközön tűzfal és vírusírtó- és behatolás meggátló szoftver konfigurálva legyen
- Tesztelni a távoli hozzáférés kapacitásait
- Növelni a tudatos használat szintjét a távoli hozzáférést alkalmazók számára
- Frissíteni a reagálási terveket a megváltozott munkaerőszükséglet vonatkozásában [6]

Kiberbiztonsági intézkedések munkavállalók és ügyfelek számára

- Kerülni a kéretlen levelekben található linkek és azok csatolmányainak megnyitását
- Ne fedjünk fel személyes és pénzügyi adatot, valamint ne küldjünk választ kéretlen tartalomra
- Tekintsük meg a CISA útmutatását a pszichológiai manipuláció és adathalászati technikák felismeréhez a COVID-19 járvánnyal kapcsolatban
- Tekintsük meg a Szövetségi Kereskedelmi Bizottság által közzétett bejegyzést a koronavírus járvány során megismert csalási kísérletekkel kapcsolatban
- Használjunk megbízható forrásokat legitim kormányzati oldalakat, amelyek naprakész és hiteles információkkal szolgálnak a COVID-19 járvánnyal kapcsolatban [6]

A „FormBook” malware a koronavírus köntösében

A MalwareHunterTeam szakértői felfedtek egy kampányt, ami a COVID-19 kötelékében terjed. A támadók a WHO képviselőiként adják ki magukat, a kéretlen levélben egy .zip állományban van a FormBook elnevezésű információlopásra tervezett trójait letöltő futtatható program MyHealth.exe néven. Korábban kiberkémkedési céllal ezt a kártékony kódot alkalmazták már amerikai és dél-koreai célpontok ellen is. [7]

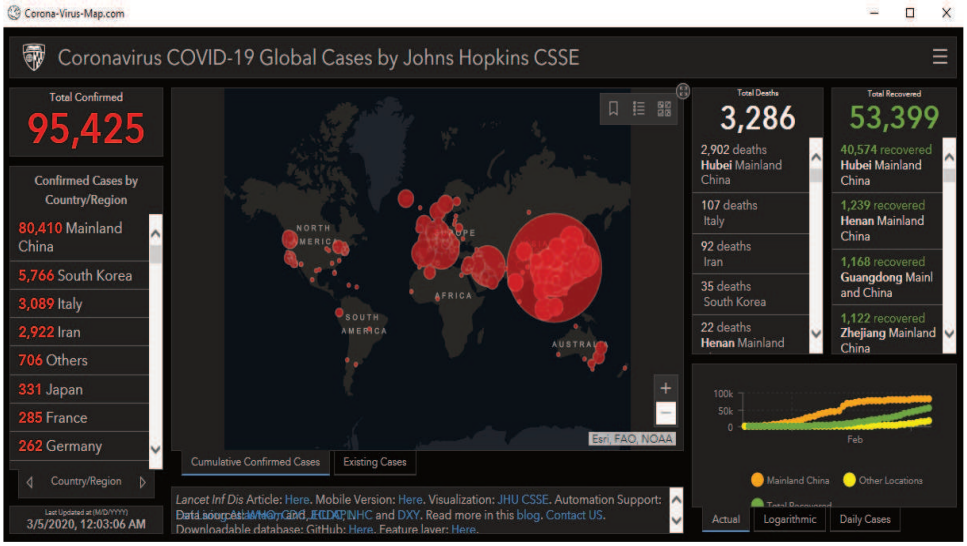
A FireEye elemzése alapján a kártékony kód helyi jelszavakat, sütibeállításokat, vágólapon szereplő tartalmakat, valamint adatokat lop el http időszakokból. A kód továbbá képes parancsokat is végrehajtani egy távoli vezérlőszerverről (C2) többek között: letölteni és futtatni fájlokat, folyamatokat elindítani, leállítani és újraindítani a számítógépet. [8]

A COVID-19 terjedésével foglalkozó térkép weboldalának hamisítványa

Egy grafikus felhasználói felület (Graphical User Interface) használatával a háttérben fut a rosszindulatú kód (malware) AZORult névvel fémjelezve. Ezt az információlopási technikát 2016-ban fedezték fel először, illegális orosz oldalakon közkedvelten árulták.

Böngészési előzmények, bejelentkezési adatok, sütibeállítások és kriptovaluták lopására alkalmazták, valamint az ellopott adatokat további értékesítésre bocsátásának a lehetősége is adott. A kód többszintes összeállításban fut, multi-sub-process (azaz párhuzamosan és egymásra épülő, könyvtárrendszeri szinten) annak érdekében, hogy egy vizsgálat lefolytatását nehezebbé tegye. Annak érdekében, hogy a futása tartós legyen, a feladatütemezőt használja az operációs rendszerben. [9]

A kártékony kódot tartalmazó GUI felület (2. ábra) az eredeti webes forrásból kapja az adatokat, így a gyanútlan szemlélőnek akár fel sem tűnik, hogy nem hivatalos helyről szerzi az információkat. Az emberi természetet és a kíváncsiságra való hajlamosságot használja ki a támadó, altatva a célpont biztonságérzetét.



2. ábra: A Corona-Virus-Map.com grafikus felülete [9]

Ransomware támadás egy cseh kórház ellen járvány közepén

Helyi idő szerint reggel 5 óra körül kibertámadás érte a Brno-i Egyetemi Kórházat 2020 március 14.-én a járvány közép-európai terjedésének sűrűjében. A kórház kénytelen volt leállítani informatikai struktúráját az incidens alatt, valamint érintette két alszervezetét is. A központi hangosbemondóban fél óránként elhangzott, hogy minden dolgozó állítsa le a számítógépét kibernetikai biztonsági okokból. Reggel 8 óra magasságában pedig újabb üzenet került bemondásra a hangosbemondóban, mely szerint az aznapi összes orvosi beavatkozás szünetel. [10] Egy nappal később túlterheléses támadás érte az Egyesült Államok egészségügyi és szociális minisztériumát is, melynek során nem történt behatolás, illetve negatív fejlemény. A támadás, ami a HHS szervereit érte nem bizonyult eredményesnek, mert számottevő lassulást nem sikerült elérnie. [11]

Iráni hátterű kibertámadások a WHO dolgozói ellen

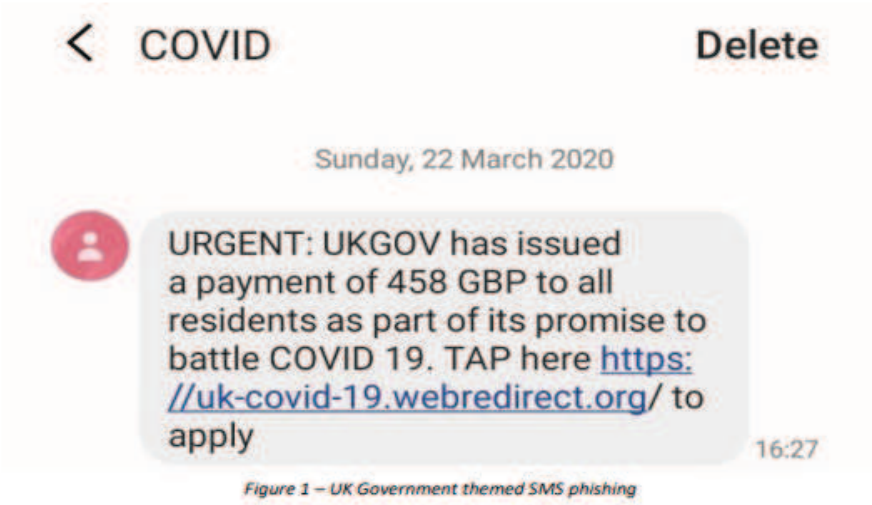
A Reuters márciusi közleménye alapján az ENSZ egészségügyi szervezetei és a hozzá kapcsolódó intézmények ellen elkövetett támadások megduplázódtak a COVID-19 járvány kezdete óta. A legutóbbi próbálkozás jelszavak ellopása volt a WHO dolgozóitól,

előre elkészített emaileket küldve személyes emailpostafiókjaikra, melyekben álcázott Google webes szolgáltatásokkal igyekezték megvezetni az áldozatokat. [12] A Foreign Policy beszámolója szerint, a mostani járványhelyzet miatt különösen fontos lenne, hogy globális szinten lévő magatartás legyen a kibertérben az egészségügyi szervezetek védelme érdekében. A lap továbbá beszámol arról, hogy a világ most végül kénytelen lépéseket tenni az egészségügyi infrastruktúra kiberbiztonsága végett.

A fenyegetettség azonban nem újkeletű, 2017-ben egy New York állam béli, Buffaloban lévő kórház, az Erie County Medical Center ellen elkövetett zsarolóvírusos támadás során a NotPetya vírus használatával 10 millió USA dollár értékben követeltek bitcoin kriptovalutát a támadók, a több, mint 6000 zárolás alatt álló számítógép feloldásáért cserébe. [13]

A National Cyber Security Centre tapasztalatai a COVID-19 kapcsán jelentkező kártékony szereplőkkel szemben

Az NCSC áprilisi kiadványában többek között szerepel egy SMS-alapú adathalászati kísérlet (3. ábra), ahol a támadó az Egyesült Királyság kormányának adja ki magát, és egy hivatalosnak tűnő szöveg mellett egy külső weboldalra mutató linket küld az áldozat számára. A kiadvány a továbbiakban kitér arra is, hogy a támadók nem csak email alapon jelentkezhetnek, WhatsApp és egyéb chatalkalmazásokat is előszeretettel használnak. Jellemzően bejelentkezési adatok ellopására törekednek, pénzügyi haszonszerzés céljával. De további példaként megemlítenek egy phishing kampányt is 2020 március 19.-i kezdettel, ahol Dr. Tedros Adhanom Ghebreyesus, feladótól a WHO főigazgatójának kiadva magukat az Agent Tesla nevű leütéskövető kémprogramot igyekeznek terjeszteni. Más kampányokban Excel fájlok is alkalmazásra kerülnek, amelyek megnyitása után egy makró fut le, ami aktiválja a rosszindulatú kód letöltését, erre példa a 'EMR Letter.xls.' nevű állomány, amelybe egy beágyazott dynamic-link library (DLL) telepíti a Get2 loader malware-t. Ez a kód pedig a GraceWire trójai programot telepíti a továbbiakban, ami a számítógép feletti irányítás átvételére hivatott. [14]



3. ábra: COVID-19 témájú SMS-alapú adathalászat [14]

Adatszivárgás a Beaumontnál, 112 000 érintett adatainak kiszivárgása

Az amerikai Michigan állam legnagyobb egészségügyi intézményében történt adatszivárgásról tett bejelentést 2020 április 17.-én a Beaumont Health Services, melynek során aktív és korábbi páciensek adatai kerültek illetéktelen kezekbe. A kikerült adatok természetét tekintve a páciensek neve, születési ideje, társadalombiztosítási azonosítója, egészségügyi állapotukra vonatkozó információ, valamint helyenként banki adatok, de még vezetői engedélyek adatai is kompromittálódtak. A kórház több, mint 1000 igazolt COVID-19 fertőzöttet kezelt ebben az időszakban. Ebben az évben ez a második eset, 2020 januárjában 1182 pácienst értesítettek, hogy egy munkavállaló jogosulatlan hozzáférése során kerültek ki adatok egy személyi sérülésekkel foglalkozó ügyvédi iroda számára. [15]

A pénzügyi érdek (financial gain) ahogyan általában megfigyelhető az információlopás szándékával elkövetett kibertevékenységek során itt is jól tetten érhető, hogy a járványhelyzetet kihasználva a támadó könnyűszerrel ragadta meg a lehetőséget. Egy negyedéven belül két támadás egészségügyi adatok megszerzése céljával pedig intő jel a társadalom számára.

KONKLÚZIÓ

Néhány hónap leforgása alatt eljutottunk oda, hogy valós veszélye van annak, hogy többtízezres nagyságrendben kerülhetnek adatok illetéktelen kezekbe, akár hivatalos ajánlások megjelenése után pár héttel. A támadások volumene a korábbi évekhez képest, főként az egészségügyi szektorban a járványhelyzettel kapcsolatban multiplikálódott, ez a jövőre tekintettel még inkább aggasztó, mert a támadások száma és a károkozások mértéke jelentős. A járványhelyzet nem csak a távoli hozzáférés és munkavégzés elméleti és gyakorlati megoldásaiban változtatott, de új irányokat is felvázol, abba az állapotba, ami előtte volt, visszatérni már nem fogunk tudni. Továbbra is azt állítom, hogy teljes mértékben biztonságos rendszer nem létezik, hiszen az ember/munkavállaló, mint tényező mindig jelen lesz a folyamatokban, hasonlóan egyéb csalási eseményekhez, a kiberbiztonság területén is törekedni kell a belső tájékoztatásra, ezzel hatékonyan tudjuk csökkenteni a fennálló kockázatokat és növelni tudjuk a szervezeti reagálóképességet egy lehetséges incidens esetére.

HIVATKOZÁSOK

[1] European Commission, „What personal data is considered sensitive?,” 18 12 2019. [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en. [Hozzáférés dátuma: 23 05 2020].

[2] Cylance, 25 02 2019. [Online]. Available: https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Cylance-2019-Threat-Report.pdf?_ga=2.194100014.207560192.1557408928-1034628078.1557241850. [Hozzáférés dátuma: 23 05 2020].

[3] J. K. Cohen, „Ransomware targeting health systems in more 'sophisticated' ways,” 24 01 2020. [Online]. Available: https://www.modernhealthcare.com/cybersecurity/ransomware-targeting-health-systems-more-sophisticated-ways. [Hozzáférés dátuma: 20 05 2020].

[4] R. Garrett, „Lessons learned from a targeted ransomware attack," 20 12 2019. [Online]. Available: https://www.modernhealthcare.com/opinion-editorial/lessons-learned-targeted-ransomware-attack. [Hozzáférés dátuma: 23 05 2020].
[5] Yoroi, „New Cyber Attack Campaign Leverages the COVID-19 Infodemic," 25 02 2020. [Online]. Available: https://yoroi.company/research/new-cyber-attack-campaign-leverages-the-covid-19-infodemic/. [Hozzáférés dátuma: 08 04 2020].
[6] CISA, „CISA INSIGHTS Risk Management for Novel Coronavirus (COVID-19)," 06 03 2020. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus.pdf. [Hozzáférés dátuma: 21 05 2020].
[7] Nemzeti Kibervédelmi Intézet, „VIGYÁZAT: ÚJABB KORONAVÍRUS MALSPAM KAMPÁNYOKAT FEDEZTEK FEL," 03 2020. [Online]. Available: https://nki.gov.hu/it-biztonsag/hirek/vigyazat-ujabb-koronavirus-malspam-kampanyokat-fedeztek-fel/. [Hozzáférés dátuma: 23 05 2020].
[8] P. Paganini, „New Coronavirus-themed malspam campaign delivers FormBook Malware," 08 03 2020. [Online]. Available: https://securityaffairs.co/wordpress/99156/cyber-crime/coronavirus-spam-campaign.html. [Hozzáférés dátuma: 14 05 2020].
[9] Reason Labs, „COVID-19, Info Stealer & the Map of Threats – Threat Analysis Report," 09 03 2020. [Online]. Available: https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/. [Hozzáférés dátuma: 13 03 2020].
[10] C. Cimpanu, „Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak," 13 03 2020. [Online]. Available: https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/?fbclid=IwAR3jE3mDkxTfKSL8UOeGlsqaXsgQ1wN_SekAn7t9EEMpYr5BW-fA9XX3p4M. [Hozzáférés dátuma: 20 03 2020].
[11] S. Stein és J. Jacobs, „Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak," 16 03 2020. [Online]. Available: https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response. [Hozzáférés dátuma: 29 05 2020].
[12] J. Menn, C. Bing, R. Satter és J. Stubbs, „Exclusive: Hackers linked to Iran target WHO staff emails during coronavirus - sources," 02 04 2020. [Online]. Available: https://www.reuters.com/article/us-health-coronavirus-cyber-iran-exclusi/exclusive-hackers-linked-to-iran-target-who-staff-emails-during-coronavirus-sources-idUSKBN21K1RC. [Hozzáférés dátuma: 29 05 2020].
[13] C. Ruhl, „Note to Nations: Stop Hacking Hospitals," 06 04 2020. [Online]. Available: https://foreignpolicy.com/2020/04/06/coronavirus-cyberattack-stop-hacking-hospitals-cyber-norms/. [Hozzáférés dátuma: 23 05 2020].
[14] National Cyber Security Centre, 08 04 2020. [Online]. Available: https://www.ncsc.gov.uk/files/Final%20Joint%20Advisory%20COVID-19%20exploited%20by%20malicious%20cyber%20actors%20v3.pdf. [Hozzáférés dátuma: 23 05 2020].

[15] D. Walsh, „Data breach at Beaumont exposes information of 112,000 patients,” 17 04 2020. [Online]. Available: https://www.crainsdetroit.com/health-care/data-breach-beaumont-exposes-information-112000-patients. [Hozzáférés dátuma: 26 04 2020].