ACTA HUMANA • 2022/4. 19–34. • DOI: 10.32566/ah.2022.4.2

A videókonferencia-alkalmazások biztonsági kockázatai[1]

BÁNYÁSZ PÉTER[2] – TÓTH ANDRÁS[3] – MAGYAR SÁNDOR[4] – KOLLER MARCO[5]

Az új típusú koronavírus számos területen gyorsította fel a digitalizációt. A globális pandémia egyik jellegzetes képe az online értekezletekhez köthető. Az állami és piaci szervezeteknek, az oktatási intézményeknek szinte egyik napról a másikra kellett átállni távoli munkavégzésre, digitális oktatásra, ami a különböző videókonferencia-alkalmazások használatának megugrásával járt együtt. A Covid–19 azonban nem csupán a társadalmi funkciók fenntartásában okozott komoly kihívásokat; a kierőltetett digitalizáció emergens fenyegetettségeket is okozott a kibertérben. A videókonferencia-alkalmazások a fentiekből következően számos biztonsági kockázatot rejtenek magukban adatvédelmi és információbiztonsági aspektusból. Jelen tanulmány ezeket a kockázatokat kívánja bemutatni a technológia, illetve a humán tényező szempontjából, valamint a jó gyakorlatok elvét követve megoldási javaslatokat is felvázol.

Kulcsszavak: kiberbiztonság, videókonferencia-alkalmazások, infokommunikációs technológia, koronavírus, adatvédelem, információbiztonság

Security Risks of Video Conferencing Applications

A new type of coronavirus has accelerated digitisation in many areas. A common image of the global pandemic relates to online meetings. Government and business organisations and educational institutions had to adopt distance working and digital education from one day to the next,

1 A cikket támogatta a Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar Választás és Képviselet Kutatóműhelye.

2 Adjunktus, Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar; a Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar Választás és Képviselet Kutatóműhely tagja; kutató, Eötvös József Kutatóközpont Kiberbiztonsági Kutatóintézet, e-mail: Banyasz.Peter@uni-nke.hu

3 Egyetemi docens, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Híradó Tanszék, e-mail: toth.hir.andras@uni-nke.hu

4 Adjunktus, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Nemzetbiztonsági Intézet, e-mail: magyar.sandor@uni-nke.hu

5 Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: marcoakoller@gmail.com

accompanied by a boom in the use of various video conferencing applications. However, Covid-19 created serious problems in maintaining social functions, and the forced digitalisation also created emergent cyber threats. Consequently, video conferencing applications raise several security risks from a privacy and information security perspective. This paper aims to present these risks from a technology and human factor perspective and to outline possible solutions based on best practices.

Keywords: cybersecurity, video conferencing applications, infocommunication technology, coronavirus, privacy, information security

Bevezetés

Tanulmányunk megszületésének oka a Nemzeti Közszolgálati Egyetemen működő Választás és Képviselet Kutatóműhelyben folytatott munkánk, amelynek keretében az elektronikus választás magyarországi adoptálásának lehetőségeit vizsgáljuk kiberbiztonsági aspektusból. Ma Magyarországon nem lehet élni az e-választás lehetőségével, nincs erre kialakított funkció a digitális állam folyamataiban, továbbá a jogszabályok sem teszik lehetővé a választási folyamat teljesen digitális megvalósítását. A Kutatóműhelyben tudományos módszertani alapokon vizsgáljuk, hogy milyen digitális megoldásai vannak ezeknek az eljárási cselekményeknek, azoknak milyen biztonsági kockázatai vannak (választások hitelessége), és hogy más országok tapasztalatai mit mutatnak ezen a téren az elmúlt időszakban. A kutatás további célja a műszaki és logikai szempontok elemzésével annak összetett vizsgálata, hogy Magyarországon bármely választási folyamatnak (beleértve a népszavazásokat) mely lépései és milyen módon lehetnének lebonyolíthatók teljes mértékben elektronikusan. A lépések vizsgálata alatt a teljes választási eljárást, a választás lebonyolítását, az ehhez kapcsolódó igazgatási, szervezési, illetve pénzügyi feladatok műszaki-technológiai vetületeit is megvizsgáljuk. A kutatás során tekintettel kell lennünk az egyes területek által igényelt eltérő követelményekre (például amíg az anonimitás biztosítása fontos követelmény a „szavazatszámlálás" kapcsán, addig a „népszavazásra javasolt kérdés benyújtása" és az „aláírásgyűjtés", „jelöltajánlás" az állampolgárok egyértelmű beazonosíthatóságát írja elő). Célunk egy átfogó koncepció és javaslat megalkotása az online participáció értelmezésére és kiterjesztésére, illetve a magyar választási eljárás digitális megújítására, megfelelő helyenként szabályozási alternatívák kidolgozásával együtt.

Jelen közlemény a kutatási téma egy részterülete, amelynek alapját az adja, hogy a választási eljárásról szóló 2013. évi XXXVI. törvény (a továbbiakban: Ve.) 2021. január 21-től előírta, hogy a Nemzeti Választási Bizottság (a továbbiakban: NVB) ülése az elnök döntése alapján elektronikus úton is megtartható.[6] Az új típusú koronaví-

6 Kurunczi–Téglási 2022a: 40.

rus (Covid–19) ugyanis a választási szerveket is online működésre kényszerítette. Kurunczi Gábor és Téglási András rámutat arra, hogy bár a választási bizottságok online ülésezésének lehetőségét még csak néhány EU-s országban biztosítják, a koronavírus-járvány rávilágított arra, hogy nemcsak a választási eljárásban, hanem az egyes választási szervek ülésezési gyakorlatában is nyitni kell az online tér irányába.[7] A szerzők nem tartják elképzelhetetlennek, hogy a teljes választási folyamatot (beleértve az otthonról történő online szavazást is) digitalizálják, ahogy az Észtországban is történik.[8] Ehhez azonban még – véleményünk szerint – az egyes országoknak növelniük kell a választópolgárok digitalizációba vetett bizalmát, ugyanis a mai választópolgárok nem bíznak maradéktalanul a digitális eszközökben.[9]

Célunk a téma szélesebb kontextusba ágyazása, hiszen hiába adott a lehetőség és a jogi keret, amelyek alapján az online értekezleteket meg lehet tartani, ezeknek – mint ahogy tanulmányunkban is látható lesz – számos komoly biztonsági kockázata van.

A Covid–19-járvány ideje a globális statisztikákban a kibertámadások drasztikus számának növekedését mutatta. Az élet számos területén találkoztunk azokkal a kiberbiztonsági fenyegetésekkel, amelyek a Covid–19 következtében árasztották el az embereket.[10] Állami és piaci szereplőknek egyik napról a másikra kellett átállni az online munkavégzésre, az oktatási intézményeknek a digitális oktatásra,[11] ami a szervezetek jelentős részét felkészületlenül érte.[12] A felkészületlenség egyik fő okaként az adat- és információbiztonsági terület relevanciájának alulértékelését azonosíthatjuk.[13]

Ennek egyik igazolására a szervezetek üzletmenet-folytonossági tervének (a továbbiakban: BCP) hiánya szolgál.[14] E dokumentum lényege, hogy segítségével felkészüljünk a kritikus üzleti folyamatok sérülés vagy leállás utáni visszaállítására, lehetőleg a legkisebb kieséssel. Az üzletmenet-folytonosság tervezése rendkívül komoly adminisztratív tevékenység, ami egyúttal magyarázza, miért is mellőzik a szervezetek annak elkészítését. A BCP lényegében kockázatelemzést követően azonosítja a kritikus üzleti folyamatokat annak érdekében, hogy fel lehessen készülni az esetleges kiesésre, és megfelelő, előre eltervezett stratégiákat alkalmazva mérsékelni lehessen a kiesés mértékét.[15] Ennek érdekében elengedhetetlen a megfelelő tervezés, tesztelés, oktatás és karbantartás. A BCP céljait többek között az alábbiak szerint fogalmazhatjuk meg:

- azonnali és megfelelő választ ad a vészhelyzetekre;
- megkönnyíti a visszaállást a normál üzleti működésre, miközben a kritikus üzleti funkciókat tervezetten lehet újraindítani;

7 Kurunczi–Téglási 2022b.
8 Kurunczi–Téglási 2022a: 48.
9 Kurunczi–Téglási 2022b.
10 Bányász 2022: 241.
11 Krasznay–Koczka 2021.
12 László–Szakos 2021.
13 Mezei–Krasznay 2022.
14 Phillips–Landahl 2021.
15 Megyeri–Farkas 2017.

- csökkenti a kár mértékét;
- listázza azokat az eljárásokat és erőforrásokat, amelyeket a visszaállításhoz felhasználhatunk;
- azonosítja azokat a partnereket, akik bevonása indokolt lehet a visszaállítás érdekében;
- segíti a zavar elkerülését a világos útmutatók, tesztelés, dolgozók oktatásának segítségével.

Fontos emellett az is, hogy ahogy az egyének, úgy a szervezetek sem érzik komoly kockázatnak a kibertér jelentette fenyegetéseket. Gyakori toposz az átlagos adat- és információbiztonsági tudatossággal jellemezhető felhasználók részéről az „Én miért lennék célpont?" vagy „Az én nem vagyok eléggé fontos". A Covid–19 újfent igazolta, hogy ezönbecsapás. A kiberbűnözők szokásuk szerint rendkívül gyorsan alkalmazkodtak a jelenséghez, és támadásaikhoz adoptálták a koronavírus tematikáját. A sikeres támadásokhoz nagyban hozzájárult továbbá, hogy az átlagfelhasználók alacsony kiberhigiéniai képességekkel rendelkeznek, ami sok esetben szintén alacsony digitális kompetenciával társul. Ez a párosítás azért is különösen veszélyes, mivel ha a felhasználó nem tudja megfelelő magabiztossággal kezelni az általa használt információs technológiai eszközöket, úgy értelemszerűen nem lesz képes felismerni az esetleges informatikai támadásokat sem. Nem szabad elfelejteni azt sem, hogy a járvány olyan mentális állapotba helyezte az embereket, amely sokaknál a vírus, a létbizonytalanság miatti szorongáshoz, a lezárások okozta stressz fokozódásához, az esetleges függőségek felerősödéséhez vezetett.

Fentiek – a támadók szempontjából legalábbis – tökéletes egyveleget szolgáltattak a kiberbiztonsági incidensek bekövetkezéséhez, hiszen rengetegen kényszerültek arra, hogy otthonról dolgozzanak megterhelt mentális állapotban, gyengén védett informatikai eszközökről megfelelő eljárásrendek kidolgozásának hiányában, alacsony digitális kompetenciával, illetve kiberhigiéniai képességgel. Fontos látni, hogy a leggyakoribb támadások nem jelentettek újdonságot, bekövetkezésük nagy mértékben csökkenthető lett volna az általam korábban megfogalmazott tényezők „hiányában". Egyáltalán nem nevezhető újdonságnak az üzletmenet-folytonosság tervezése, mint ahogy több évtizedes múltra tekintenek vissza az adathalászattal, kártékony kódokkal kapcsolatos támadások, amelyek a pandémia kiberbűnözéssel kapcsolatos statisztikáiban a legnagyobb számban megjelentek.

Részben érvényes e megállapítás a tanulmány tárgyául szolgáló videókonferencia-alkalmazások használatára is. Bár használatuk szintén hosszú időre vezethető vissza, a koronavírus okozta távoli munkavégzés tömegessé tette alkalmazásukat, ami miatt jelentős fejlesztéseken estek át az egyes szoftverek. A hírekben leggyakrabban a Zoom online videókonferencia-program volt hallható különböző botrányok okán, pedig mind kríziskommunikáció, mind biztonsági fejlesztések tekintetében a fejlesztők példásan vizsgáztak.

Nem szabad elfelejteni, hogy a Zoom elképesztően gyorsan vált a lezárások alatt a legnépszerűbb platformmá, komoly konkurenciát jelentve a hasonló szolgáltatást nyújtó nagy techcégeknek (Facebook, Microsoft). A hírekbe kerülő, a céget érintő botrányok az esetek nagy részében nem a platform hibájából, hanem a felhasználók alacsony adat- és információbiztonsági tudatosságából fakadtak, a nagy elérést kapó beszámolók mégis inkább a Zoomot tették felelőssé. E sorok írói nem lennének meglepettek, ha valamikor a jövőben bizonyítékok látnának napvilágot arra vonatkozóan, hogy szervezett sajtóhadjárat zajlott a konkurensek részéről, hogy csökkentsék a platform iránti bizalmat.

De mely kockázatok fakadnak a videókonferencia-szolgáltatásokból? E vizsgálat során érdemes különválasztani a technológiából, illetve a humán aspektusból származó kockázatokat. Szintén tisztázni szükséges a biztonsághoz kapcsolódó fogalmi eltéréseket, ugyanis azok függvényében eltérő védelmi megoldásokat kell alkalmazni.

A kiberbiztonság a köznyelvben gyakran az informatikai, illetve információbiztonság szinonimájaként jelenik meg, azonban három eltérő fogalomról beszélhetünk. Segítségül hívva a 2013. évi L. törvényt az állami és önkormányzati szervek elektronikus információbiztonságáról[16] (a továbbiakban: Ibtv.), az informatikai biztonság egy informatikai rendszer olyan állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg.[17] Célja, hogy az információ megőrizze és fenntartsa a biztonsági tulajdonságait, vagyis az adatok sértetlenségét, bizalmasságát és rendelkezésre állását.

Ennek érdekében különféle hardveres és szoftveres biztonságtechnikai eszközöket alkalmaznak az illetéktelen hozzáférések és károkozás megelőzésére (például tűzfalak, vírusírtók, hozzáférés-szabályozás) továbbá biztonsági szabályzatokat, előírásokat (jelszóhasználat, biztonsági mentés) is létrehoznak. Ilyen védelmi megoldások:

- az adminisztratív védelem;
- a fizikai védelem;
- a logikai védelem.

Ez vezet el bennünket a kiberbiztonság fogalmához, az Ibtv. alapján „kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi,[18] gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez". Ebből következően a kibervédelem „a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését".

16 2013. évi L. törvény.

17 Munk 2008.

18 A jogi aspektust tovább bonyolítja a kibertér határon túli mivolta, ami alapján a vonatkozó nemzetközi jogi szabályzók különösen fontosak. Bővebben lásd e témában: Kasper–Krasznay 2019.

A megfelelő szintű informatikai és információbiztonság kialakítása minden szervezet számára létfontosságú. A védelem költségei rendkívül magasak lehetnek, és a szervezet által kezelt adatok függvényében változhatnak. Az Ibtv. hatálya alá tartozó szervezetek tekintetében kockázatelemzést kell végezni, amelynek alapját a kezelt adatok jelentik. A 41/2015. (VII. 15.) BM rendelet[19] meghatározza, hogy az egyes szervezeteket egy 1-től 5-ig terjedő skálán hányas biztonsági szintbe, illetve az általuk használt elektronikus információs rendszert szintén 1-től 5-ig terjedő skálán hányas biztonsági osztályba szükséges sorolni. A biztonsági osztályba és szintbe sorolás eredményének függvényében az Ibtv. és végrehajtási rendelete meghatározza, milyen típusú védelmi megoldásokat kell alkalmaznia a szervezetnek. Picit előre szaladva a feldolgozandó témában, ennek jelentősége a videókonferencia-programok kiválasztásánál fontos szempont, hiszen a szervezetek tekintetében nem mindegy, hogy az adott program milyen titkosítási protokollokat használ, az adatokat milyen szervereken tárolja. A korábban említett Zoom esetében komoly – és jogos – kritika, illetve aggály volt, hogy egyes esetekben az adatokat kínai szervereken tárolta.

Technológiából fakadó kockázatok

Az előző bekezdésben már említettük a titkosítás kérdését. Az adatátvitel titkosítása megfelelő protokollon keresztül történik. Ennek legismertebb módja az SSL- *(secure socket layer)* tanúsítvány, amely arra szolgál, hogy az informatikai eszközünk, illetve a felkeresett weboldalt tároló szerver között biztonságos, titkosított csatorna létesüljön. A https:// előtag jelenti az URL-ben, hogy egy tanúsítvánnyal hitelesített weboldalt készülünk felkeresni. Az előtagban szereplő s betű a biztonságot *(hypertext transfer protocol secure)* jelöli, amennyiben egy URL nem tartalmazza az s betűt a http:// után, az azt jelenti, hogy illetéktelenek is kifürkészhetik az adatátvitel tartalmát. Különösen fontos ez például online vásárlásnál, ahol a megadott bankkártyaadatok harmadik fél részére is láthatóak lehetnek. Természetesen rengeteg adathalászoldal, amely megpróbálja lemásolni egy létező oldal, szolgáltatás megjelenését, az URL-ben elhagyja az eredeti oldalban szereplő https://-t, és csak http:// jelölés lesz látható. Az ilyen oldalak gyakran egyéb eltéréseket is alkalmaznak a látogatók megtévesztésére. Állami szervezetek weboldalait másoló adathalászoldalaknál gyakori például, hogy a gov.hu részt qov.hu-ra cserélik, ugyanis sokszor felületesen olvassuk csak az elénk kerülő tartalmakat, a g betű pedig – különösen hosszú linkek esetében – megtévesztően hasonlít a q betűre. Videókonferencia-beszélgetések kapcsán így tehát kettős kockázatot is jelenthet a titkosított adatátvitel hiánya, hiszen ha nem titkosított csatornát biztosító alkalmazáson keresztül jelentkezünk be, mások is megszerezhetik az online megbeszélés tartalmát, illetve az adathalászat eszköze is lehet egy kártékony kódot tartalmazó, hamis URL. Ha például küldenek számunkra egy Zoom-hivatkozást (https://zoom.com/…), azonban a megkapott URL http://zoome.com/…, a felületes

19 41/2015. (VII. 15.) BM rendelet.

szemlélőt, különösen azt, aki a gyenge kiberhigiéniai készségei okán nem ismeri fel az adathalászat technikáit, sok kellemetlenség érhet. A kártékony kódot tartalmazó weboldalak nem csupán a látogatók adatait lophatják el (például a bejelentkezéshez Google fiókjának adatait kérhetik, amivel megadja e-mail-címét és a hozzá tartozó jelszavát[20]), de olyan kártékony kód telepítésére is rávehetik,[21] amivel az informatikai eszköz különböző támadásokat készíthet elő. Ilyen lehet többek között:

- kémprogramok telepítése, amellyel harmadik fél megfigyelheti a fertőzött eszközt;
- zsarolóvírus telepítése, amellyel titkosíthatják az áldozat eszközén szereplő adatokat (egyúttal el is lophatják őket), az újbóli hozzáférésért cserébe pedig váltságdíjat követelnek;[22]
- hátsókapu nyitása az eszközön, amelyen keresztül a támadók hozzáférhetnek a rajta tárolt adatokhoz rejtett módon.

Ahogy fentebb utaltunk már rá, a támadók folyamatosan újabbnál újabb technikákat találnak ki. Egy 2022 tavaszán megjelent támadási formában például a fertőzött URL-en „rajzolt" felugró ablak jelenik meg, amelyben a címsor nem kattintható, csupán egy ábra, ahol az URL https://-ként szerepel. Első ránézésre megbízható weboldalra utal, a valóságban azonban rendkívül szofisztikált támadás áldozataivá válhatunk. Célszerű ilyen esetben ellenőrizni, hogy az SSL-tanúsítványt ki akkreditálta. Ha az eredeti oldalon rákattintunk a tanúsítást jelző lakat ikonra, akkor megjelennek a validáló szervezet információi, a hamis felugró ablakban azonban nem tudunk kattintani, hiszen csupán egy kép próbálja utánozni az adott weboldalt.

A Zoomot érintő jogos aggályok esetében föntebb már utaltunk arra, hogy kiemelten fontos az adatok tárolására használt szerverek lokalizációja, hiszen az adott állam területén elhelyezkedő szerverparkok eltérő jogi védelem alá esnek. A 2013-ban kitört Snowden-ügy egyik tanulsága az volt,[23] hogy az amerikai nemzetbiztonsági szolgálatok hozzáférést szereztek az amerikai szervereken tárolt adatokhoz is, ami nem csupán az amerikai állampolgárok esetében következett be, hanem a világ bármelyik állampolgára esetében, ha amerikai szerverek által nyújtott szolgáltatást vett igénybe.

20 Bonyolítja ennek kockázatát, ha a felhasználó minden egyéb fiókjához ugyanazt a jelszót használja.

21 Fontos látni, hogy egy fertőzött URL-re való kattintásból még nem következik, hogy megfertőztük az eszközünket. Ahhoz, hogy telepítsük a kártékony kódot, további felhasználói tevékenységek szükségesek. Például felugrik egy hibaüzenet, miszerint frissítenünk szükséges a megnyitni kívánt szoftvert. Maradva a Zoom esetében, ilyenkor feldobhat egy olyan telepítőprogramot, amely a Zoom frissítésének álcázza magát, valójában azonban ebbe rejtették el azt a kártékony kódot, amelyet a két-három engedélyező kattintással telepítünk.

22 Amit fizetés után vagy feloldanak, vagy sem. A neves zsarolóvírus-csoportok számára presztízskérdés, hogy a titkosított állományokat feloldják, azonban a Darkneten is megvehető zsarolóvírusokhoz nem feltétlenül jár a feloldó kulcs, így semmi garancia nincs, hogy fizetést követően visszakapjuk adatainkat. Ebből következően nem javasolt fizetni a bűnözőknek.

23 Greenwald 2014.

Az egyes államok nemzetbiztonsági célú internetes megfigyelése nem új keletű dolog, számos ország él ezzel. A Zoom az említett botrányig kínai szervereken is tárolt adatokat, ami a kínai nemzetbiztonsági szolgálatok azokhoz való hozzáférésének lehetőségét teremtette meg. Nem nehéz belátni, szenzitív adatok esetében ez mennyire komoly kockázatot jelent. Mindebből következik, hogy egy platform választása során körültekintőnek kell lenni egy szolgáltatás adatvédelmi policyjával kapcsolatban. Nem könnyű azonban ez nem európai székhelyű szolgáltatók esetében: hogy az általuk alkalmazott adatvédelmi elvek mennyire vannak összhangban az Európai Unió Általános Adatvédelmi Rendeletével.[24]

A titkosítás tekintetében említeni szükséges a végpontok közötti titkosítást (end-to-end, E2EE), amely egy fontos védelmi mechanizmus.[25] A gyakorlatban ez azt jelenti, hogy a küldő (egyik végpont) és a fogadó (másik végpont) között titkosítva valósul meg az adatátvitel, a tartalmát még a csevegőalkalmazást működtető vállalat sem látja.[26]. A Covid–19 miatt a legtöbb nagy videókonferencia-szolgáltatást kínáló vállalat bevezette a végpontok közötti titkosítást – a Zoom például az őt ért támadások hatására.[27] Az E2EE kifürkészésére a támadók sok esetben nem a titkosítás feltörésével próbálkoznak, hanem az eszköz kémprogrammal történő megfertőzésével, amely még a titkosítás bekövetkezte előtt próbálja megszerezni az információt. Egyre népszerűbb, végpontok közötti titkosítást kínáló, üzenetküldésre, audio- és videóhívásra alkalmas program a Signal. A nagy port kavart izraeli kémprogram, a Pegazus is úgy próbálta megkerülni a Signal titkosítását, hogy üzenetküldés esetén képernyőmentést készített titokban a készülékről, és azt küldte el harmadik fél részére. A hívások esetében pedig a mikrofonhoz való hozzáféréssel hallgatta le a beszélgetéseket, mielőtt azok titkosításra kerültek volna.

A mikrofonhoz való hozzáférés vezet el bennünket a következő kockázathoz, a használt informatikai eszköz sérülékenységéhez. A videókonferencia-programok jellemzően multiplatformok, nem csupán PC-n, laptopon, hanem okos mobil eszközökön is elérhetőek, egyszerre akár több platformról is bejelentkezünk. A biztonságtudatosság legelső lépése, hogy az általunk használt eszközöket mindig naprakészen tartsuk. Rengeteg sérülékenység lát napvilágot, amit a támadók kihasználva hozzáférhetnek eszközeinkhez.[28] A tapasztalat azt mutatja, nagyon sok támadás azért következik be, mert a felhasználók nem frissítették az ismert sérülékenységekre kiadott javításokat. Egy ismert sérülékenység meglétét gyakran mesterséges intelli-

24 2016/679 (EU) európai parlamenti és tanácsi rendelet.

25 Beiter et al. 2014.

26 Szádeczky 2016; Szádeczky 2018.

27 Bár nem tartozik szorosan a videókonferencia-programok kérdéséhez, azonban fontos megérteni, az E2EE csak akkor működik, ha minden érintett azonos alkalmazást használ. Népszerű e-mail-szolgáltató a Protonmail, ami E2EE titkosítást használ az üzenetek küldése során, de ez csak addig jelent valódi védelmet, míg protonmailes címről protonmailes címre küldünk üzenetet, ellenkező esetben a fogadó végpontnál sebezhetőek lehetünk, hiszen ott nem alkalmazzák azt az elvárt titkosítást, és ha a támadók hozzáférnek a fogadó e-mail-fiókjához, olvashatják az üzenetet.

28 Paráda–Farkas 2020; Horváth–Erdősi 2016a; Horváth–Erdősi 2016b.

gencia segítségével tömegesen szkennelik a támadók. A sérülékenységek minősített esetét jelentik az úgynevezett nulladik napi sérülékenységek, amelyek egy hardver vagy szoftver olyan még a fejlesztő, gyártó által sem ismert sebezhetőségét jelentik, amelyen keresztül a támadók hozzáférhetnek az eszközhöz.[29] Ezeket a sérülékenységeket jellemzően államilag támogatott hackercsoportok fedezik fel, és az államokhoz köthető hírszerzés fontos eljárásai.[30] Egy átlagos felhasználó esetében ez kevésbé tekinthető reális kockázatnak, azonban az informatikai eszközök használata megkerülhetetlen az államigazgatásban is. Márpedig a korábban említett biztonsági osztályba és szintbe sorolás itt válik igazán relevánssá, hiszen minél értékesebb adatokat tárolnak egy elektronikus információs rendszerben, a támadók (és itt nagy valószínűséggel államokhoz köthető hackereket kell érteni) mindent el fognak követni, hogy hozzáférést szerezzenek.

A Covid–19, illetve a BCP-k hiánya is rávilágított újfent arra az alapelvre, hogy lehet bármilyen jól védett a rendszerünk, az annyira magas szintű, mint a leggyengébben védett eszközünk. Hiába volt jól védett nagyon sok szervezet vállalati eszköze, megfelelve azoknak a biztonsági mechanizmusoknak, amelyek a kockázatokkal arányos védelem kitételét is teljesítették, a hirtelen jött távoli munkavégzés nem tette lehetővé, hogy azonnal átálljanak védett otthoni munkavégzésre. Sok esetben a munkavállalók otthoni, alig védett eszközökről kényszerültek dolgozni, csatlakozni a belső, védett munkahelyi hálózathoz, megnyitva az utat az esetleges támadások előtt.

A multiplatform jellemzőből fakadó kockázatok az adathalászat esetében is érvényesek. Az általunk használt okos mobil eszközök rengeteg adat- és információbiztonsági fenyegetést jelentenek,[31] ami esetünkben az alkalmazások engedélykérésére vezethető vissza. Egy alkalmazás telepítésekor a program engedélyt kér a felhasználótól különböző hozzáférési jogosultságokhoz. Ezek az engedélyek alkalmazás függvényében reálisak, hiszen például egy videókonferencia-alkalmazás használatához szükséges a mikrofonhoz, kamerához való hozzáférés, elvégre ezek nélkül nem tudjuk rendeltetésszerűen használni a programot. Egy zsebláma-alkalmazás esetében azonban indokolatlan a mikrofonhoz, kamerához való hozzáférés igénye, mint ahogy egyéb engedélykérések is, mint például a geolokációs helymeghatározás, az üzeneteink tartalma stb. A kiberbűnözéssel foglalkozó statisztikák azt mutatják, hogy egyrészt a felhasználók jelentős része úgy telepíti mobil eszközére a programokat, hogy nem olvassa el az engedélykéréseket, és automatikusan mindenhez is jogosultságot ad, másrészt elképesztő számban kerülnek fel kifejezetten adathalászcélra írt programok az alkalmazásboltokba.[32]

29 Singh–Joshi–Kanellopoulos 2019.

30 „Pulse Zero-Day Exploited by APT Groups" 2021: 2–3; Kovács–Krasznay 2010.

31 Bővebben lásd Bányász 2018.

32 Az adathalászprogramok tekintetében aszimmetria figyelhető meg az androidos és iOS-es eszközök esetében, ugyanis az Apple sokkal komolyabban veszi az adatvédelmet, illetve a biztonsági

A technikai kockázatoknál szükséges említeni a belépéssel kapcsolatos lehetőségeket. Volt szó fentebb az adathalászatról és a jelszavak megszerzéséről, ami különösen nagy kockázat, ha valaki mindenhová ugyanazt a jelszót használja. A biztonságos jelszóhasználat alapelvei közé sorolhatjuk a meghatározott számú, vegyes karakterekből, nem értelmes kifejezésekből álló jelszavakat, amelyeket rendszeresen változtatunk. Ellenkező esetben nagy esély van arra, hogy korábban kiszivárgott valamilyen adatbázisból a jelszavunk, amelynek ismeretével a nevünkben be tudnak lépni a fiókjainkba. Mindez nem feltételez komoly informatikai ismereteket, egyszerű nyílt forrású információgyűjtéssel könnyen megvalósítható, egyszerű Google-keresésekkel (megfelelő operátorok használatával, mint például adatbázisokra keresni jelszóval – filetype:env „DB_PASSWORD" vagy adatszivárgással kapcsolatos adatokra – filetype:txt intext:"@gmail.com" site:anonfiles.com), a https://haveibeenpwned.com/ weboldalon való ellenőrzéssel,[33] az adott e-mail-cím más oldalakon való regisztrálásának ellenőrzésével könnyen beléphetünk más személyek fiókjaiba. Ezzel már önmagában bűncselekményt követünk el, így természetesen nem javasoljuk az olvasónak, de a támadókat értelemszerűen kevésbé fogják megkötni ezek az etikai kérdések. A megfelelő jelszópolicy mellett rendkívül fontos a multifaktoros azonosítás használata, ami egy esetleges jelszószivárgás esetén is védelmet jelenthet. A multifaktoros azonosítás lényege, hogy a jelszavunk mellett a belépéshez egyéb azonosítás szükséges (például egyszer használatos, rövid ideig érvényes kód küldése SMS-ben[34] vagy autentikációs alkalmazás használata). A multifaktoros azonosítás használatát a nagyobb videókonferencia-programok lehetővé teszik, de nem csak ezek esetében tanácsos bekapcsolni.

A multifaktoros azonosítás egyik lehetősége a biometrikus azonosítás,[35] amely videókonferencia programok esetében jellemzően arcképes azonosítást jelent. A technológia fejlődésével azonban egyre növekvő kockázatot okoz az úgynevezett deepfake

kérdéseket, így programok csak szigorúbb, több körös ellenőrzést követően kerülhetnek az általa üzemeltetett alkalmazásboltba. Ezek az alkalmazások nem csupán az engedélykérésekkel okozhatnak problémát, ugyanúgy lehetséges kártékony kód telepítése is. Persze a kreatív támadók a szigorú ellenőrzés kivédésére megtalálták a megoldást, a telepítendő alkalmazás „tiszta", csupán egy harmadik vagy későbbi frissítésbe rejtik el a kártékony kódot.

33 Az oldal érdekes szeglete a nyílt forrású információgyűjtésnek, egyúttal a GDPR szabályozásának furcsaságait is mutatja. Bár nyílt forrásból elképesztően sok információ gyűjthető be, tekinthető meg a célszemélyekről, azonban ha a személyes adatait letöltjük, onnantól kezdve adatkezelővé válunk. Csakhogy a személyes adat fogalma megítélésem szerint a technológiai adatok következtében jelentősen kibővült, hiszen egy IP-cím, e-mail-cím személyes adat lehet, ugyanis egyértelműben azonosítható belőle a természetes személy. Speciális esetben akár a gépelési habitusunk is ide sorolható, ugyanis piacon elterjedt programok segítségével biometrikus azonosításra is alkalmas. Az oldalon tárolt e-mail-címekre való kereséssel még nem leszünk adatkezelők, azonban ha a hozzájuk tartozó jelszavakra is kíváncsiak vagyunk, torrentről le kell töltenünk az azokat is tartalmazó adatbázisokat. Ezzel viszont adatkezelőkké válunk, hiába érhetőek el az adatok nyilvánosan.

34 Ez kevésbé biztonságos a korábban említett telefonos adathalász-technikák miatt, hiszen ha hozzáférnek az üzeneteinkhez, ezt a kódot is képesek olvasni a támadók.

35 E-közigazgatásban Magyarországon például az Ügyfélkapura történő belépéshez is használható. Erdősi 2017.

jelenség,[36] amely azt jelenti, hogy a nagy számban elérhető hang- és képanyag felhasználásával a mesterséges intelligencia képessé válik arra, hogy akár valós időben hangunkat, arcunkat reprodukálja, és videókonferenciákon ellopják személyünket. A Covid–19 alatt az ilyen jellegű támadások elsősorban a vezetőkkel kapcsolatos csalások esetében következtek be, de várhatóan ezek szofisztikáltsága növekedni fog.

A videókonferenciák esetében – bár jelentős többletköltséggel jár – javasolt saját videókonferencia-infrastruktúrát használni a felhő alapú rendszerek helyett. Ebben az esetben a szervezet adatközpontjában kerül telepítésre a videókonferencia-szerverszolgáltatás, amelyhez a végpontok csatlakoznak. Itt is számos biztonsági aggály merülhet fel, azonban a konferenciák központi mentése, naplózása szervezeten belül marad.

A videókonferenciák biztonsága esetében nem elhanyagolandó aspektus a hálózat sem, amelyhez csatlakozunk. Egy hálózat üzemeltetője monitorozhatja a hálózaton zajló adatforgalmat, így a beszélgetéseinket – különösen a szenzitív témában folytatottakat – célszerű megbízható hálózatokon keresztül lebonyolítani. 2022-re talán már sokaknak riasztóan hat egy nyílt wifi használata, azonban nem feltétlenül értik ennek okát. Azt kell megérteni, nem attól veszélyes egy wifihálózat, hogy a csatlakozáshoz nem szükséges jelszó, hanem azért, mert nem ismert az üzemeltető személye. Egy nyílt wifin keresztül is internetezhetünk biztonságosan, ha nem adunk meg semmilyen jelszót rajta keresztül (érvényes ez a bankszámlaadatainktól kezdve minden egyéb adatunkra), illetve ha valamilyen VPN-szolgáltatást használunk.[37] Egy jelszóval védett hálózat ugyanúgy lehet kockázatos, hiszen a támadók a bizalom kialakítása érdekében létrehozhatnak jelszóval védett wifihálózatot, amelyhez osztogatják a kreált jelszót. Ennél nagyobb probléma az otthoni hálózatok gyakran elégtelen védelme. Nyílt forrású információgyűjtéssel könnyen kideríthető a felhasználók által használt router típusa: egyszerű Google-kereséssel összeköthető a router típusának alapértelmezett jelszava és azonosítója, aminek ismeretében már be is lehet lépni az illető hálózatába. A statisztikák ismételten azt mutatják, rendkívül kis számban változtatják meg az emberek a routereik (vagy bármilyen internetre csatlakoztatható informatikai eszközük[38]) alapértelmezett jelszavát, azonosítóját.

Azt sem szabad elfelejteni, hogy az egyes alkalmazások kiterjedt nyomkövetést alkalmaznak. A nagy techcégek, amelyek fő bevételi forrása a minél pontosabban targetált hirdetések megjelenítése, a Covid–19 alatt piacra léptek videókonferencia-programokkal, amelyek az adatgyűjtésnek plusz csatornáit jelentették. Azok a nyomkövető sütik, amelyek bizonyos esetekben a kényelmes használatot hivatottak szolgálni, gyakran a megfigyelésünket növelik. A programok megfigyelhetik az egerünk mozgását, a leütött billentyűket, még ha nem is a program felületén írunk, hanem egy másik alkalmazásban. Azáltal, hogy jóhiszeműen figyelmeztet bennünket a program,

36 Mustak et al. 2023.

37 A VPN virtuális magánhálózatot jelent, amely az adatátvitelt titkosítja, így a hálózat üzemeltetője nem képes monitorozni a kommunikációt.

38 Egy wifis webkamera esetében ez további kockázatokat jelent, hiszen azon keresztül nemcsak a videókonferencia idején figyelhető meg az ember, hanem folyamatos működéssel is akár.

hogy lenémítva maradt a mikrofonunk, és nem hallják a többiek, amit mondani szeretnénk, a gyakorlatban azt jelenti, hogy az alkalmazás hall mindent a mikrofon lenémításának ellenére is. Humán kockázat oldaláról itt szükséges jelezni a tudatos kamera- és mikrofonhasználatot, figyelni azok kikapcsolására, amennyiben nem szükséges, különösen, ha mások prezentálnak. Rendkívül kellemetlen perceket tud okozni, ha oda nem illő megjegyzéseket fűzünk, gondolva, hogy senki nem hall bennünket. Ha mindezt rögzítik is, további problémák is adódhatnak.

A technológiai kihívások kapcsán utolsóként a csatolmányok küldését kell megemlíteni, hiszen a platformok a kép- és hangátvitel mellett fájlok továbbítását is lehetővé teszik, amelyek adott esetben kártékony kódokat is tartalmazhatnak. Korlátozhatjuk bizonyos fájltípusok küldését (érdemes ezt megtenni a futtatható fájlok, például a .exe kiterjesztés esetében).

A humán aspektus kockázatai

Mint fentebb már megfogalmaztuk, a videókonferenciákhoz köthető botrányok többsége a felhasználók viselkedéséből fakadt, amelyek megfelelő biztonsági beállítások alkalmazásával megelőzhetők lettek volna. Bár a technológiai kockázatok esetében is több olyan tényezőt azonosíthatunk, amelyekhez a nem tudatos felhasználói viselkedés szükséges (például az adathalászat), ebben az alfejezetben a klasszikus viselkedésből eredő fenyegetéseket vesszük górcső alá.

Elsőnek mindenképpen a videókonferencia résztvevőinek szűrését szükséges említeni. A biztonságos videókonferenciázás módját sokan fájó esetek kapcsán tanulták meg, ami a nem körültekintő résztvevői körből fakadt.[39] A bejelentkezéshez célszerű letiltani, hogy Facebook- vagy egyéb közösségimédia-profilból jelentkezünk be. Érdemes megjegyezni, hogy az elektronikus aláírás működik fájlok és videóstream esetében is.[40] Rengeteg probléma megelőzhető, ha az online megbeszéléseket jelszóval védett, privát értekezleten keresztül hirdetjük meg. Arra is figyelni kell, hogy ezeket az adatokat csak a meghívandók kapják meg, ne hozzuk nyilvánosságra. A tanulási folyamat emlékezetes példája volt Boris Johnson, az Egyesült Királyság miniszterelnöke, aki az első online kabinetülésről megosztott egy képernyőmentést Twitteren, és nem takarta ki a megbeszélés azonosító számát. Ennek ismeretében akár idegenek is csatlakozhattak volna az online értekezlethez. A jogosultságkezelésnek nemcsak a fentiekre érdemes kiterjednie, hanem a chat és egyéb funkciók elérésének korlátozására is.

Célszerű várószobát is létrehozni akadályozandó az automatikus csatlakozást, illetve az értekezlet gazdája dönthet arról, hogy a csatlakozni vágyó felhasználót beengedi-e az értekezletbe.

39 Ennek fokozatai szimplán illetéktelenek részvételétől kezdve az emlékezetes ELTE ÁJK diákköri konferencián botrányt okozó szatír jelenlétéig terjedhetnek. Ez utóbbi azonban sajnos a körültekintő biztonsági beállítások mellett sem szűrhető ki a nyilvánosság előtt zajló eseményeknél.

40 Erdősi 2019.

Videókonferenciához történő csatlakozás előtt érdemes ellenőrizni a kameraképet, hogy abból milyen következtetéseket vonhatnak le velünk kapcsolatban. Sok esetben olyan árulkodó apróságokat szúrhatnak ki az éles szemű résztvevők, amelyek később károsak lehetnek. Nem csupán kellemetlen dolgok lehetnek a háttérben, hanem olyan információk is, amelyek egy későbbi támadás megalapozására szolgálhatnak (kiragasztott jelszó stb.). Ezek megelőzésére lehetnek hasznosak a hátterek alkalmazásai, amelyek elhomályosítják vagy elfedik a mögöttünk levő teret.

A jogosultságkezelés egyes aspektusait már említettük a résztvevői kör beállításai kapcsán, azonban végezetül kettő pontra szükséges felhívni a figyelmet. Az egyik a képernyőmegosztás alapértelmezett tiltása, amivel megakadályozható, hogy illetéktelenek nem kívánatos tartalmakat osszanak meg. Képernyőmegosztáskor kizárólag a megmutatni szándékozott programot válasszuk, ne a teljes képernyőt, ugyanis ezzel véletlenül számos plusz, akár kompromittáló információt oszthatunk meg magunkról. A multiplatform jellegből fakadóan olyan kockázatok is felmerülhetnek, mint például IOS-mobil esetében, ha átváltunk egy másik alkalmazásba az értekezlet során, képernyőképet készít rólunk az alkalmazás, és ez érzékeny adatot is rögzíthet.

Ennél fontosabb azonban a rögzítés engedélyezése, illetve tiltása. Az, hogy egy értekezletet illetéktelenek is rögzíthetnek, úgy véljük, komoly adat- és információbiztonsági kockázatot jelent. Természetesen abból, hogy egy értekezlet során korlátozzuk, ki készíthet felvételt, nem következik az, hogy külső programmal nem rögzíthetik a résztvevők titokban az elhangzottakat. Az említett kockázat azonban nemcsak azért következhet be, mert esetlegesen az értekezlet minden résztvevője felveheti a videókonferenciát, hanem a rögzített felvétel megosztásából is. A különböző platformok folyamatosan változtatják szolgáltatásaikat, és korábbi beállítások egyik percről a másikra átalakulnak. Emiatt célszerű minden értekezlet előtt bizonyos beállításokat újra és újra ellenőrizni. Korábban a Microsoft Teams a rögzített értekezletet a host OneDrive fiókjába töltötte fel, és csak ő férhetett hozzá. Egy frissítést követően azonban a felhő mellett az értekezlet chatfelületében is elérhetővé váltak a rögzített felvételek, amelyek bárki által letölthetőek voltak. A felvételek rosszhiszemű összevágása, módosítása pedig jelentős reputációs károkat okozhat a szervezetek számára.

Összegzés

Összességében megállapíthatjuk, hogy a videókonferenciák a maguk egyszerűségében számos igen komoly biztonsági kockázatot jelentenek. Ez természetesen nem jelenti azt, hogy mellőzni kell őket, csupán a megfelelő platformot kell választani. Ennek bevezetése, különösen szenzitív adatok kezelésével foglalkozó szervezetek esetében, komoly kockázatelemzés elvégzését illetően célszerű. Emellett fontos szempont a platform kiválasztásánál, hogy az milyen technikai támogatást nyújt a felhasználók számára, illetve milyen jogorvoslati lehetőségeink vannak az adott vállalattal szemben.

A Freedom of the Press Foundation (FPF) nevű nonprofit szervezet foglalta összse a legnépszerűbb platformokat biztonsági szempontból, amelyeket az alábbi,

1. táblázatban gyűjtöttünk össze segítendő a szervezet számára legmegfelelőbb alkalmazás kiválasztását.

1. táblázat: Melyik videóchat-alkalmazást válasszuk?

Platform	Támogatja az E2E titkosítást?	Támogatja a saját hosztolást?	Az értekezlethez csatlakozás regisztrációhoz kötött?	Értekezlet kapacitása (ingyenes verzió esetén)
Zoom	Igen (Beállításoknál engedélyezett)	Igen (Kivéve a hívás metaadatai)	Nem (URL-lel való meghívás esetén)	100 fő (fizetős verzió 1000 fő)
BigBlueButton	Nem	Nem	Nem	150 (legalacsonyabb beállítással)
Google Meet	Nem	Nem	Nem	100 fő (fizetős verzió 500 fő)
Skype	Nem	Nem	Nem	100
Microsoft Teams	Nagyjából (2 személynél)	Nem	Nem	100 fő (fizetős verzió 1000 fő)
Slack	Nem	Nem	Igen	15
Webex	Igen (opcionális)	Nem (fokozatosan kivezetik)	Nem	100 fő (fizetős verzió 200 fő)
Jitsi Meet	Nagyjából (2 személynél)	Igen	Nem	75
Whereby	Nagyjából (2 személynél)	Nem	Nem	12 (100 fő kizárólag hanggal)
FaceTime	Igen	Nem	Igen (Kivéve iPhone)	32 (Kizárólag, ha Apple felhasználó a hoszt)
Signal	Igen	Nem	Igen	40
WhatsApp	Igen	Nem	Igen	8
Wire	Igen	Igen	Nem	2

Forrás: a szerzők szerkesztése FPF 2023 alapján

Bármilyen program használata mellett is döntsön a szervezet, kiemelten fontos, hogy a munkavállalókat alapos adat- és információbiztonsági képzésben részesítsék, olyan segédanyagok elérhetővé tételével, amelyek a lehető legbiztonságosabb kezelést teszik lehetővé.

Irodalomjegyzék

Bányász Péter (2018): Az okos mobil eszközök biztonsága. *Hadmérnök,* 13(2), 360–377. Online: http://real.mtak.hu/94336/1/182_25_banyasz.pdf

Bányász Péter (2022): Kiberbiztonság az FMCG-szektorban és a kiskereskedelemben. In Sikos T. Tamás – Molnár Dóra (szerk.): A *Covid–19-világjárvány hatása a kiskereskedelemre*. Budapest, Ludovika, 241. Online: https://m2.mtmt.hu/api/publication/33286733.

Beiter, Michael et al. (2014): End-to-End Policy Based Encryption Techniques for Multi-Party Data Management. *Computer Standards & Interfaces,* 36(4), 689–703. Online: https://doi.org/10.1016/j.csi.2013.12.004

Erdősi Péter Máté (2017): Fokozott biztonságú biometrikus aláírások alkalmazhatósági és szabályozási kérdései a közigazgatásban. In Polgár Miklós (szerk.): *A társadalom szolgálatában – felkészülés és felkészítés a katasztrófavédelmi kihívások tükrében.* Pécs: Baranya Megyei Katasztrófavédelmi Igazgatóság, 63–68.

Erdősi Péter Máté (2019): Az elektronikus aláírás fogalmának megjelenése és változása. *Információs Társadalom: Társadalomtudományi Folyóirat,* 19, 66–91. Online: https://doi.org/10.22503/inftars.XIX.2019.1.3

Freedom of the Press (2023): *Choosing the Right Video Conferencing Tool for the Job*. Online: https://freedom.press/training/blog/videoconferencing-tools/

Greenwald, Glenn (2014): *A Snowden-ügy*. Budapest: HVG.

Horváth Attila – Erdősi Péter Máté (2016a): Rosszindulatú számítógépes fertőződés vizsgálatának lehetséges kérdései és indokai a közigazgatásban. In *IT és Hálózati Sérülékenységek Társadalmi-Gazdasági Hatásai.* Budapest: Információs Társadalomért Alapítvány, INFOTA Kutatóintézet, 31–48.

Horváth Attila – Erdősi Péter Máté (2016b): Sérülékenységek hatásának vizsgálata a biztonsági követelmények aspektusából. In *IT és Hálózati Sérülékenységek Társadalmi-Gazdasági Hatásai.* Budapest: Információs Társadalomért Alapítvány, INFOTA Kutatóintézet, 49–58.

Kasper, Agnes – Krasznay, Csaba (2019): Towards Pollution-Control in Cyberspace: Problem Structure and Institutional Design in International Cybersecurity. *International and Comparative Law Review,* 19(2), 76–96. Online: https://doi.org/10.2478/iclr-2019-0015

Kovács László – Krasznay Csaba (2010): Digitális Mohács. *Nemzet és Biztonság: Biztonságpolitikai Szemle,* Különszám, 44–56. Online: www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf

Krasznay Csaba – Koczka Ferenc (2021): A távolléti oktatás jelentette kiberbiztonsági és adatvédelmi kihívások. In Koltay András – Török Bernát (szerk.): *Járvány sújtotta társadalom.* Budapest: Ludovika, 213–230. Online: https://m2.mtmt.hu/api/publication/32092423.

Kurunczi, Gábor – Téglási, András (2022a): Solutions and Challenges for Online Meetings of Electoral Bodies. *Krytyka Prawa,* 14(3). Online: https://doi.org/10.7206/kp.2080-1084.539

Kurunczi Gábor – Téglási András (2022b): A választási szervek online ülésezésének megoldásai és kihívásai. *Acta Humana,* 10(4), 35–46. Online: https://doi.org/10.32566/ah.2022.4.3

László, Gábor – Judit Szakos (2021): How Open Source Tools Could Help Remote Learning during the First Lockdown in Hungary? – Case Study of University of Public Service. In *Central and Eastern European e|Dem and e|Gov Days 2021.* 187–194. Online: https://doi.org/10.24989/ocg.v341.13

Megyeri Lajos – Farkas Tibor (2017): Kockázatkezelés, tudomány vagy kuruzslás? *Hadmérnök,* 12(3), 198–209. Online: http://real.mtak.hu/64731/1/1.Farkas_Hadm%C3%A9rn%C3%B6k2017.pdf

Mezei, Kitti – Krasznay, Csaba (2022): Cybersecurity and Cybercrime in Hungary During the COVID-19 Pandemic. In Chałubińska-Jentkiewicz, Katarzyna (szerk.): *The Role of Cybersecurity in the Public Sphere – The European Dimension*, 191–207. Online: https://m2.mtmt.hu/api/publication/33118087

Munk Sándor (2008): Információbiztonság vs. informatikai biztonság. *Hadmérnök,* Különszám, 1–21. Online: https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/31

Mustak, Mekhail et al. (2023): Deepfakes: Deceptions, Mitigations, and Opportunities. *Journal of Business Research,* 154, 113368. Online: https://doi.org/10.1016/j.jbusres.2022.113368

Paráda István – Farkas Tibor (2020): Felderítés és analízis a penetrációs tesztben – 1. Információgyűjtési technikák. *Hadmérnök,* 15(1), 159–182. Online: https://doi.org/10.32567/hm.2020.1.11

Phillips, Brenda D. – Landahl, Mark (2021): Chapter 1 – What Is Business Continuity Planning? In Phillips, Brenda – Landahl, Mark: *Business Continuity Planning.* Oxford: Butterworth-Heinemann, 1–24. Online: https://doi.org/10.1016/B978-0-12-813844-1.00009-9

„Pulse Zero-Day Exploited by APT Groups" (2021). *Network Security* 2021(5), 2–3. Online: https://doi.org/10.1016/S1353-4858(21)00045-3

Singh, Umesh Kumar – Joshi, Chanchala – Kanellopoulos, Dimitris: A Framework for Zero-Day Vulnerabilities Detection and Prioritization. *Journal of Information Security and Applications,* 46, 164–72. Online: https://doi.org/10.1016/j.jisa.2019.03.011

Szádeczky Tamás (2016): Kriptográfiai protokollok megfelelősége. *Hadmérnök,* 11(4), 178–83. Online: http://real.mtak.hu/id/eprint/49982

Szádeczky, Tamás (2018) Security of E-Government Website Encryption in Germany and Hungary. *AARMS,* 17(3), 127–138. Online: https://doi.org/10.32565/aarms.2018.2.9

Jogi források

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT vonatkozású szöveg)