SZIGETSZENTMIKLÓSI TANKERÜLETI KÖZPONT

A videókonferencia rendszerek biztonsági kérdései

I. Néhány szó a Zoom alkalmazásról

Március 30-án az Indexen cikk jelent meg *„Az otthonról dolgozókra is rászálltak a kiberbűnözők”* címmel. A cikkben az alábbiak olvashatóak:
„Vigyázat! A csalók most a Zoom nevű vállalati videókonferencia alkalmazásra hivatkozva próbálják meg átverni a távmunkában dolgozó felhasználókat” – figyelmeztet hétfői Facebook-posztjában a Nemzeti Kibervédelmi Intézet.
Februárban az Index is beszámolt róla, hogy a kiberbűnözők az emberek félelmeire alapozó emailekkel kezdtek el adatokat kicsalni, illetve vírusokat terjeszteni, az NKI legfrissebb tájékoztatása pedig egy újabb csalásra figyelmeztet…”

A Nemzeti Kibervédelmi Intézet (a továbbiakban: NKI) tájékoztatása teljes terjedelmében az alábbi linken olvasható:
https://nki.gov.hu/it-biztonsag/tanacsok/biztonsagi-megfontolasok-a-videokonferencia-szolgaltatasok-kapcsan/

Az NKI a fenti link alatt biztonsági ajánlásokat fogalmaz meg általánosságban a videokonferencia szolgáltatásokkal kapcsolatban.

Az NKI ajánlásai mellett a Zoom digitális platformról az alábbi tájékoztatást szeretném adni:

A több, mint 74 000 ügyféllel és 13 millió aktív felhasználóval a Zoom az egyik legpopulárisabb felhőalapú vállalati kommunikációs platform, amelynek népszerűsége az elmúlt hetekben még inkább megugrott.
A szolgáltatás kapcsán azonban az elmúlt években több súlyos sérülékenység is felmerült, illetve nemrég az internetes polgárjogi szervezet, az EFF (Electronic Frontier Foundation) adatvédelmi aggályokat is megfogalmazott. A Check Point jelentése szerint – ahogy az várható volt – a kiberbűnözők is meglátták a potenciált a távmunkában, ugyanis **egyre több hamis, Zoomra hasonlító megtévesztő domaint regisztrálnak és egyre gyakrabban jelenik meg káros kód is a platformmal összefüggésben**. A szakértők azt javasolják, minden alkalommal, amikor valakitől egy Zoom linket kapunk, legyünk különösen óvatosak.
A hivatalos Zoom domain: https://zoom.us.
Amennyiben nem https:// kezdetű vagy nem .us végződésű, esetleg nem zoom.us domain-t tartalmazó linket kapott arra ne kattintson rá és az emailt is lehetőleg törölje!
Amennyiben **a Zoom mobil kliensét használjuk, mindig frissítsük az alkalmazást a legutóbbi verzióra.**

További probléma, hogy a Motherboard elemzése szerint a Zoom iOS-alkalmazása (ez az operációs rendszer fut az Apple iPhone és iPad eszközökön) adatvédelmi szempontból aggályos lehet.

Kiderült többek között, hogy az alkalmazás az emberek beleegyezése nélkül továbbított adatokat a Facebooknak akkor is, ha illető nem is tagja a közösségi portálnak. Az ilyen jellegű adattovábbítás egyébként nem szokatlan, számos fejlesztő használja a Facebook szoftverfejlesztő csomagját azért, hogy információkat és adatokat juttasson el a közösségi oldalnak. Általában erre a programok adatvédelmi irányelveiben felhívják a felhasználók figyelmét.

A Zoom esetében a Google Ads és a Google Analytics ugyan szerepel a külső partnerek között, de a Facebook nem. A kapcsolat ráadásul már a kliensalkalmazás első megnyitásakor létrejön és a továbbított információk között vannak a használt mobileszköz típusa, modellszáma, az adott időzóna és város, ahol a szoftvert elindították.

Electronic Frontier Foundation (EFF) rávilágított, hogy a felhasználók valós idejű tevékenységei, tartózkodási helyei, operációs rendszerei és IP-címei szintén ismertté válnak a Zoom fejlesztői és a Facebook előtt. Sőt, ha valaki egy hívást rögzít a Zoom segítségével, akkor a felvételhez hozzá lehet férni, legyen szó videóról, audioanyagról vagy chatfájlról.

A **Zoom fejlesztői a kritikák hatására tájékoztatták a felhasználókat, hogy az iOS-szoftverüket frissítették és az új változat már nem küld titokban információkat a Facebooknak, ezért javasoljuk a applikáció mielőbbi frissítését**.
A Zoom helyett alternatíva lehet egyébként a Jitsi, amely nyílt forráskódú és akár saját szerverre is telepíthető, ráadásul titkosított video- és audiokapcsolatokat alkalmaz.

A digitális platformokon és az interneten 100 %-os biztonság nincsen, azonban a tudatos internethasználattal és óvatos felhasználói magatartással a kockázatok csökkenthetőek.

A Zoom használata során a felhasználók számára ajánlott

- kép- és hangfelvétel csak indokolt esetben készüljön,
- kép- és hangfelvételt rögzíteni online óráról akkor lehet, ha erről minden felhasználót előzetesen tájékoztatták. Amennyiben oktatási célú az online óra *rögzítése*, akkor az a közfeladat ellátás „része", így adatkezelési hozzájárulás nem szükséges. Amennyiben magáncélból kíván valaki az online óráról felvételt készíteni, akkor ehhez minden esetben az összes érintett hozzájárulása szükséges (tehát, akinek a hangja hallható vagy a képmása látható). A felvételeket közösségi oldalakon vagy bárhol nyilvánosan megosztani kizárólag akkor lehet, ha ehhez mindenki hozzájárult. Ha valaki utólagosan visszavonja a hozzájárulását, akkor a tartalmat törölnie kell haladéktalanul a közzétevőnek.
- a webkamera csak abban az esetben legyen bekapcsolva, illetve felfedve, ha a használata szükséges (pl. vers felmondása),
- a webkamera használata során figyelni kell arra, hogy a kamera látószögében a lakással, családdal, egyénnel kapcsolatos információk ne legyenek megismerhetőek (pl. a berendezések értékére és ez alapján a vagyoni helyzet),
- amennyiben nagyobb terjedelmű kép- vagy hanganyagot youtube csatornán kell a pedagógus számára rögzíteni, akkor minden esetben figyelni kell a beállításokra. A helyes beállítás a „nem publikus". Ebben az esetben kizárólag a youtube csatorna tulajdonosa fér a kép- és hangfelvételhez, továbbá az a személy, akivel a felvétel linkje megosztásra kerül, jelen esetben a feladat elvégzését értékelő pedagógussal. Általános szabály, hogy a felvételek csak abból a célból kezelhetőek, amely célból létrejöttek, ettől eltérő felhasználás jogszerűségéről egyeztetni kell az adatvédelmi tisztviselővel.

II. Néhány alapvető ajánlás a digitális eszközök használatával és védelmével kapcsolatban:

A távoktatásra használt különféle plattfarmokon fontos, hogy a **gyerekek regisztrációja** ne "kamu" profilokkal történjen, hanem ahol ez lehetséges a valós adataik megadásával. Ennek felügyeletére a platformok többféle családi beállítást kínálnak fel, pl. a Google platformon a Google Family Linkjén keresztül javasolt létrehozni a gyerekfiókot és abban dolgozni. A Facebook esetében a 13 év feletti gyerekeknél azért fontos, hogy a valós életkorukat adjuk meg, mert ebben az esetben a Facebook automatikusan a legszigorúbb adatvédelmi beállításokat teszi alapértelmezetté.

Nagyon fontos, hogy a használt eszköz, legyen az asztali számítógép, laptop, tablet vagy okostelefon, rendelkezzen **naprakész vírusvédelmi megoldással**, mert a megnövekedett adatforgalommal a kockázat is megnövekedett a káros kódok összeszedésére. Van, ahol az operációs rendszer tartalmaz ilyen védelmi funkciót (pl Windows Defender), de **sok ingyenes és jól alkalmazható program is elérhető.**

Veszélyhelyzetben különösen fontos, hogy meg tudjuk különböztetni a valós és az álhíreket egymástól. Próbáljunk meg hiteles forrásból származó híreket olvasni. A közösségi médiában terjedő hírek gyakran nem valósak, csak pánikkeltésre alkalmasak.

Ugyancsak fontos, hogy a veszélyhelyzet kapcsán megnövekedett a helyzetet kihasználni akaró, az **emberek félelemérzetére ható adathalász, csaló és egyéb email támadások és átverések** száma. Fontos, hogy jelen körülmények között legyünk még körültekintőbbek például a személyes vagy bankszámlához kapcsolódó adatokat kérő e-mailekkel kapcsolatban. Gyanús, ha az e-mail írója sürgeti vagy nyomás alá helyezi a címzettet. A hatóságok, pénzintézetek és egyéb szervek soha nem kérnek ilyen jellegű adatokat e-mailen!

A fentiek mellett a járványt kihasználva **károkozó kódot tartalmazó csatolmánnyal ellátott e-mailek** is érkezhetnek, amik sok esetben hivatalosnak látszó, jól megszerkesztett formában készültek, esetleg valamelyik nemzetközi szervezet (pl. WHO) nevében íródtak. Ne kattintsanak az ilyen e-mailekben szereplő hivatkozásokra, és ne töltsék le a mellékletben szereplő jellemzően Microsoft Word, Excel, PDF vagy MP4 formátumú fájlokat!

Hasznos tartalmak:

IT Biztonság közérthetően:
https://njszt.hu/hu/news/2019-09-30/it-biztonsag-kozerthetoen-elso-kiberbiztonsag

Magyar álhírterjesztő oldalak listája:
https://www.urbanlegends.hu/2020/01/megteveszto-magyar-hiroldalak-listaja-2020/?fbclid=IwAR1Konn-vI6o9FvJ6m6M53jjeOYhdHbpSVzJc3oh0YcT8guTgVYxpoXQEeU

Ingyenes antivírus programok (Windows, Mac, Android):
https://www.antivirussoftwareguide.com/best-free-antivirus

Safer Internet Program:
Tippek gyerekeknek: http://saferinternet.hu/tippek-videok/gyerekeknek
Tippek fiataloknak: http://saferinternet.hu/tippek-videok/fiataloknak
Tippek szülőknek/pedagógusoknak: http://saferinternet.hu/tippek-videok/szuloknek-pedagogusoknak

Szigetszentmiklós, 2020. március 31.

dr. Pálos Annamária s.k.
tankerületi igazgató