Herendy Csilla–Bányász Péter

IX. DIGITÁLIS TÉR – SZERVEZETI KÖZÖSSÉGIMÉDIA-FUNKCIÓK (MÓDSZEREK, FUNKCIÓK, LEHETŐSÉGEK)

A FEJEZET CÉLKITŰZÉSE

Mindenféle online kommunikáció csak jó minőségű, felhasználói részvétellel fejlesztett, könnyen érthető, átlátható és hatékony webes felületek segítségével képzelhető el. Ezt a fajta külső szervezeti kommunikációt is csak az adott platform adta lehetőségek maximális figyelembevételével és optimális kihasználásával lehet hatékonyan végezni.

Az alábbi fejezetben röviden áttekintjük az online színtér fejlődését a web 1.0-tól a web 3.0-ig, mégpedig két markáns szereplő, a közigazgatási és a digitális turisztikai megoldások bemutatásával. Látni fogjuk, mennyire másként használják a felületeket az egyes szereplők, hogyan élnek a lehetőségekkel, mely szereplő a fejlődés motorja.

Ezt követően gyakorlati javaslatokat teszünk arra is, hogyan érdemes hiteles beszállítót választani többek között a települési kommunikációt, településmarketinget támogató appok, egyéb online megoldások, virtuális felületek készíttetésére. Ezen gyakorlati információk mindenki számára fontosak, aki valaha, valamilyen webes fejlesztés közelébe került, lehetősége és felelőssége lesz megfelelő beszállítót választani.

A fejezet a fentieken túl a közösségimédia-használat veszélyeire is felhívja a figyelmet, bemutatva azokat az adat- és információbiztonsági kockázatokat, amelyek a hivatali munka során valós fenyegetést jelenthetnek.

KÖZÖSSÉGIMÉDIA-HASZNÁLAT A KÖZIGAZGATÁSI SZERVEKNÉL – JELLEMZŐ GYAKORLATOK ÉS VESZÉLYEI

A közigazgatás intézményei világszerte, így Magyarországon is, fokozatosan nyitnak a közösségi média használata felé, felismerve annak sokféle kommunikációs, szolgáltatási és közösségépítő lehetőségét. A kormányzati és önkormányzati kommunikáció a 2010-es évek végére kilépett a statikus honlapok korából, és elérte a *web 2.0* logikáját követő, kétirányú, interaktív digitális jelenlétet.[1] A közösségi

[1] Mergel 2013.

ORCID: https://orcid.org/0000-0003-3824-0950 (H. Cs.)
https://orcid.org/0000-0002-7308-9304 (B. P.)
DOI: https://doi.org/10.36250/01334_09

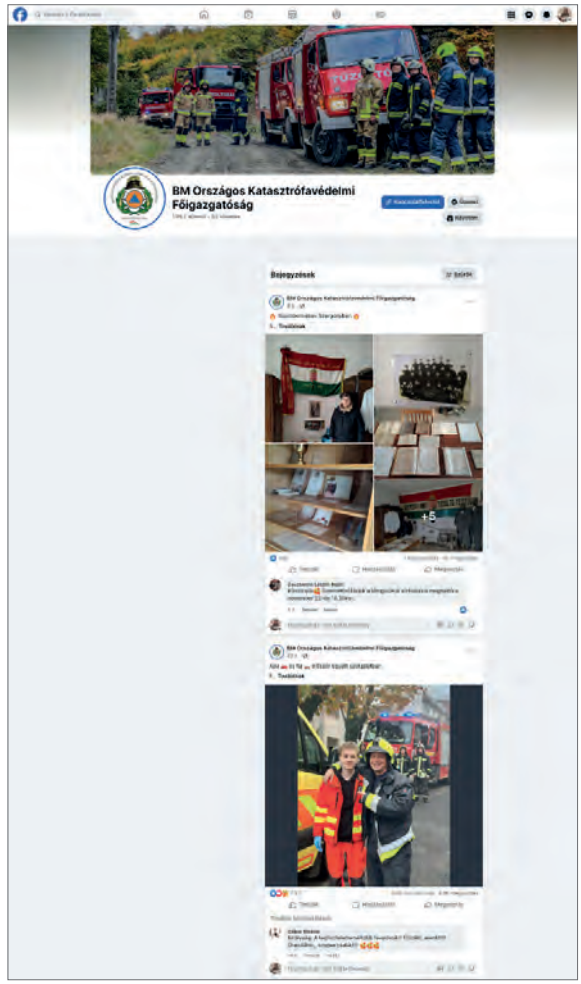
platformok – elsősorban a *Facebook, X (korábban Twitter), Instagram, LinkedIn* és újabban a *TikTok* – a közérdekű tájékoztatás, az állampolgári bevonás és a transzparencia fontos színtereivé váltak.[2]

A közösségi média mint a közigazgatás új kommunikációs tere

A közösségi média alkalmazása a közigazgatásban három alapfunkció köré szerveződik:[3]

1. *Tájékoztatás és információszolgáltatás.* Ez a legelterjedtebb gyakorlat: a minisztériumok, önkormányzatok és hivatalok a közérdekű információk (határidők, rendeletváltozások, események) gyors, vizuálisan vonzó kommunikációját valósítják meg. A magyar gyakorlatban például Budapest Főváros Önkormányzata, a XII. kerületben működő Hegyvidéki Önkormányzat, a Kormányzati Tájékoztatási Központ vagy a BM Országos Katasztrófavédelmi Főigazgatóság napi rendszerességgel használja a Facebookot és az Instagramot hivatalos tájékoztatásra.
2. *Állampolgári részvétel lehetőségei és közösségi bevonás.* Egyre több helyen jellemző a lakossági visszajelzések begyűjtésének kezdeményezése, online konzultációk vagy közösségi szavazások biztosítása, kérdőívek alkalmazása – például a *Decidim Barcelona* vagy a *Helsinki City App* mintájára –, ezek a részvételi demokrácia eszközei lehetnek. Magyar önkormányzati példák is megjelentek, például a *Debrecen Városi Mobilapp,* amely a helyi ügyintézést és közlekedési visszajelzéseket integrálja.
3. *Közösségépítés és identitáserősítés.* Sok önkormányzat a helyi kulturális események, sportprogramok és városi identitást erősítő kampányok kommunikációjára használja a közösségi médiát (például „Szeged 2030" stratégia). A közösségi médiában zajló beszélgetések segítenek emberközelivé tenni a közigazgatást, erősítve az állampolgári bizalmat.[4]

[2] Criado – Sandoval-Almazan – Gil-Garcia 2023.
[3] Bertot–Jaeger–Grimes 2020.
[4] Luna-Reyes – Gil-Garcia 2021.



9.1. ábra. *BM Országos Katasztrófavédelmi Főigazgatóság Facebook-oldala*
Forrás: Facebook, https://www.facebook.com/bmokf.hivatalos

Az új trendek: audiovizuális és MI-támogatott kommunikáció

A 2020-as évek közepére a közigazgatási kommunikációban is megjelentek a *rövid formátumú videók* (Reels, Shorts, TikTok), amelyek közérthetően mutatják be a hivatalos információkat vagy szolgáltatásokat. Magyarországon úttörő példának számít a Nemzeti Adó- és Vámhivatal (NAV) TikTok-csatornája, amely edukációs jellegű, fiatalokat megszólító tartalmakkal népszerűsíti a pénzügyi tudatosságot.

Ezzel párhuzamosan mutatkozott be az MI-támogatású tartalomkészítés: egyre több közigazgatási kommunikációs egység használ automatikus szöveg-, kép- vagy statisztikát generáló eszközöket (például ChatGPT, Canva AI, Hootsuite Insights). Az MI-támogatott elemzések lehetővé teszik a közösségi visszajelzések, sentiment-adatok és interakciók gyors feldolgozását, így az intézmények hatékonyabban reagálhatnak a lakossági igényekre.[5]

Kockázatok és etikai dilemmák

A közösségimédia-használat ugyanakkor jelentős *adatvédelmi, biztonsági és reputációs kockázatokat* hordoz.

Az *adatvédelem* terén kihívást jelent, hogy a használt platformok sok esetben amerikai vagy kínai tulajdonúak, így az ott megosztott információk külföldi adatkezelőkön keresztül jutnak el a felhasználókhoz. Az Európai Adatvédelmi Testület[6] iránymutatása kiemeli: a közintézményeknek akkor is felelősséget kell vállalniuk a személyes adatok védelméért, ha azok harmadik fél platformjain keletkeznek vagy haladnak át.

A *dezinformáció, álprofilok* és *kommentháborúk* szintén veszélyt jelentenek: a hamis hírek vagy manipulált *(deepfake)* videók alááshatják az intézményi hitelességet.[7] Emellett a közösségimédia-felületek 24/7-es működésük miatt folyamatos kommunikációs jelenlétet igényelnek, ez pedig humánerőforrás-terhet jelenthet az intézményeknek.

A közigazgatásban ezért egyre gyakoribb a *social media policy létrehozása,* azaz a közösségimédia-használatot szabályozó belső szabályzat kialakítása, alkalmazása. Ez a belső szabályzat a posztolás, moderálás, válságkommunikáció és etikai magatartás alapelveit fekteti le.[8] Ennek a belső szabályzatnak, *közösségimédia-kódexnek* a bevezetését több európai város javasolja, annak érdekében, hogy az online interakciók egységes elvek mentén történjenek.

A magyar közigazgatási szervek számára ezek a modellek azt mutatják, hogy a közösségi média nem csupán kommunikációs csatorna, hanem a *részvételi demokrácia digitális eszköze* is lehet. A jövő iránya az *integrált, biztonságos, MI-támogatott kommunikáció,* amely a közösségi térben is hiteles és átlátható közigazgatást képvisel.

5 United Nations 2024.
6 European Data Protection Board 2021.
7 Thurman–Flew–Kuntsman 2023.
8 OECD 2023.

KOCKÁZATOK ÉS MELLÉKHATÁSOK TEKINTETÉBEN…

A közösségi média használatának egy szervezet esetében – a korábbiakban ismertetett lehetőségei mellett – számos kockázata is van. A következőkben ezt vizsgáljuk az egyén és a szervezet aspektusából. Fontos látni, hogy az egyének, illetve a szervezetek esetében azonosítható kockázatok gyakran összemosódnak, és kölcsönösen hatnak egymásra. Ennek egyik okát a szabadidő és munkaidő összemosódásában találjuk meg, amit a BYOD[9]-politika tovább bonyolít. Napjainkban bizonyos munkakörök oly módon alakultak át, hogy elvégzésükhöz nem vagyunk szorosan a munkahelyünkhöz kötve. A 2020-as évet felforgató Covid–19-járvány erősítette az otthoni munkavégzés *(home office)* lehetőségeit, hiszen sok esetben derült ki, hogy ugyanolyan hatékonysággal, viszont alacsonyabb költségek mellett lehet dolgozni. Vélhetően ez a digitális nomadizmusra[10] is fejlesztő hatással lesz, aminek következtében még inkább el fog mosódni a szabadidő és munkaidő közti határ.

Mindez elvezetett egy olyan állapotba, ahol a munkaidőben is gyakran foglalkozunk magántermészetű dolgokkal – az esetleges tiltás ellenére is –, míg otthon vagy akár a közösségi közlekedés ideje alatt is foglalkozunk céges ügyekkel.

Adatok, adatok mindenhol!

Az egyének esetében az egyik legnagyobb biztonsági kockázatot a *social engineering* jelenti. A fogalommal részletesen e tankönyv következő, a *Biztonságtudatosság a digitális térben* című fejezetében foglalkozunk, így az ismétlés elkerülése érdekében itt csupán érintjük. A *social engineering* egy olyan támadási formát jelent, amely során a támadók egy vagy több, nem kellően biztonságtudatos alkalmazotton keresztül igyekeznek hozzáférni védett információs rendszerekhez, információkhoz. A social engineering támadástípusok sok eljárást kölcsönöznek a klasszikus hírszerzés repertoárjából.[11] Az első lépés minden esetben a szervezet, illetve az esetleges gyenge láncszem feltérképezése.

Jól ismert közhely, hogy ami nem található a Google-on, az nem létezik. Mégis, a Google (illetve más keresőszolgáltatások) által indexált weblapok a teljes internet

9 *Bring your own device,* vagyis használd a saját eszközöd.

10 Digitális nomádok alatt azokat a személyeket értjük, akik nem egy klasszikus irodában dolgoznak, ugyanis a munkavégzésük mobilinternettel és egy laptoppal bárhol megtörténhet, legyen szó egy kávézóról, egy pár napig bérelt irodáról vagy bármilyen egyéb helyszínről.

11 Ezek közül a közösségi oldalak számos esetben támadási felületként szolgálnak. Bővebben lásd Bányász 2018.

elenyésző részét jelentik: ez az úgynevezett *surface web,* vagyis a felszíni internet. A *deep web,* vagyis a mély internet, amely az internet hozzávetőlegesen 90%-át teszi ki, nem csupán az *internet of things,* vagyis a dolgok internete körébe tartozó eszközök adattovábbító részét jelenti, hanem azok a zárt fórumok, internetes oldalak, felhőszolgáltatások is idetartoznak, amelyekbe a keresőszolgáltatások nem látnak bele.[12]

Nem nehéz belátni, hogy az internetre felkerülő nagy mennyiségű adat, vagyis *big data* kiváló lehetőséget szolgáltat a célpontok feltérképezésére. Az úgynevezett nyílt forrású információgyűjtés, vagy közismert nevén OSINT,[13] az értő kezekben rendkívül hatékony lehet. Maga a nyílt forrású információgyűjtés legális, bárki által végezhető tevékenység. Mivel a felhasználók adat- és információbiztonsági tudatossága gyakran alacsony szintű, így rengeteg információ gyűjthető a célszemélyekről, és ezek akár zsarolásra, akár befolyásolásra is felhasználhatók. Természetesen számos szoftver,[14] eszköz[15] támogatja, hogy gyorsan, strukturált formában gyűjtsük be a szükséges információkat.

Mindebből látható, hogy a szervezetek weboldalai, közösségi oldalakon levő profiljaik számos információt rejtenek. Az aktív közösségi médiás jelenlét gyakran elvárásként fogalmazódik meg az ügyfelek részéről, amely nemcsak marketing, hanem a stratégiai kommunikáció része is lehet. Mindezek akaratlanul elárulhatnak olyan, a nagyközönség számára érdektelen, de egy támadó számára kifejezetten értékes információkat, amelyek megalapozhatnak egy támadást. Egy irodában, munka közben feltöltött kép, videó rengeteget elárulhat a munkakörnyezetről, esetleges védelmi megoldásokról, az ott dolgozók szokásairól, preferenciáiról. A díszítésként kitett képek, családunk fényképei, esetleg a monitorra *post it*-tel kiragasztott bejelentkezési adatok felbecsülhetetlen értéket képviselnek. Éppen ezért körültekintően kell eljárni minden esetben, amikor akár a szervezet, akár a saját nevünkben használjuk a közösségi oldalakat. A feltöltött képek a vizuális tartalmon kívül további metaadatokat[16] rejthetnek, mint például a geolokációs helymeghatározás. Fontos tehát, hogy körültekintően járjunk el az adatvédelmi beállításaink esetében, illetve rendszeresen ellenőrizzük azokat, hiszen a közösségi oldalak gyakran változtatják

12 Ennek vannak speciális eszközöket igénylő részei, amelyek az úgynevezett *dark web,* vagyis sötét web körébe tartoznak. Ezekkel jelen fejezetben nem foglalkozunk.

13 A mozaikszó az *open source intelligence* kifejezésből származik.

14 Például a Maltego nevű program.

15 Például a https://osintframework.com/ nevű oldalon több tucat eszközt használhatunk, amelyek különböző technológiai úton gyűjthető adat (többek között geolokációs helymeghatározás, hálózattal kapcsolatos információk) megszerzését is támogatják.

16 A metaadat: adat az adatról. Például amikor felkeresünk egy weboldalt, akkor ahhoz társul az IP-címünk, a használt eszközünk különböző jellemzői, mint a készülék, az operációs rendszer, böngésző típusa stb.

az általános szerződési feltételeiket, és ilyenkor többször is előfordult már, hogy átállítják a korábban megadott adatvédelmi beállításainkat, a nyilvánosság számára láthatóvá téve olyan tartalmakat, amelyeket korábban priváttá tettünk.

Mindebből belátható, hogy a közösségi oldalak alacsony adatvédelmi szempontból alacsony érzékenységű környezetként kezelendők.

Véleményem szerint…

A közösségi oldalak esetében régóta visszatérő vita, hogy minek minősülnek az egyes oldalak, hiszen annak függvényében merül fel a szabályozási igény. Mivel a hírfogyasztási szokásaink egyre inkább a közösségi oldalakra terelődnek (ami egyébként számos további kockázatot jelent – erről szintén a következő fejezetben ejtünk bővebben szót), felmerül, hogy a közösségi oldalak médiaszolgáltatóknak minősülnek-e, hiszen gyakran egy-egy felhasználó által megosztott tartalom válik virálissá, ami aztán a *mainstream* médiában is vezető hírré lehet. Ily módon nem mindegy, hogy a közösségi térben megfogalmazott véleményeink mekkora nyilvánosság előtt terjednek el, különösen, ha a szervezetünkkel kötnek össze.

Bár a véleménynyilvánítás szabadsága (akárcsak a lelkiismereti szabadság) alkotmányos alapjognak tekinthető, a közszolgálatban bizonyos alkotmányos szabadságjogaink korlátozhatók. Elég itt a fegyveres erők tagjaira gondolni, amivel kapcsolatban többek között a Magyar Honvédség esetében a 2012. évi CCV. törvény a honvédek jogállásáról[17] (Hjt.) tekinthető irányadónak. A Hjt. 5. §-a az „Általános magatartási követelmények" kapcsán érinti a honvédek szolgálatteljesítésen kívüli szabályait, ami rögzíti a Magyar Honvédség iránti közbizalom megóvásának kötelezettségét. A Hjt. rendelkezik egyes alapjogok gyakorlásának korlátozásáról, ami esetünkben például a gyülekezési jogra, párttagságra stb. vonatkozik (21–23. §). Tekintettel arra, hogy a nagy közösségi oldalak, mint például a Facebook is, a nyilvánosság színterei, még akkor is, ha ez a nyilvánosság korlátozott, és csak ismerőseink előtt valósul meg, lehetőséget teremtenek arra, hogy az idézett jogszabályi előírásokat a felhasználó megsértse. A kibertérben zajló interperszonális interakciók nem követelik meg, hogy például politikai tüntetésen vegyen részt a fizikai dimenzióban, a tüntetésre létrehozott eseményre adott reakcióval már megvalósulhat mindez. Nem ennyire egyértelmű a helyzet a 22. § esetén, hiszen attól eltekintve, hogy egy zárt Facebook-csoport nem tekinthető bejegyzett szervezetnek, a csoport működése, belső szabályai, céljai lehetnek hasonlók bejegyzett szervezetekéhez. Ezen belül pedig

[17] 2012. évi CCV. törvény a honvédek jogállásáról.

tanúsíthat a felhasználó olyan viselkedést, ami ellentétes a Hjt.-ben megfogalmazottakkal. Az egyik legizgalmasabb kérdés a 23. §, ugyanis a közösségi oldalon folytatott aktivitásunk, még ha nem is tudatosan, de – a megosztott hírek, vélemények akár kép, videó vagy írott szöveg formájában – alkalmas lehet pártpolitizálásra, a szolgálati fegyelmet sértő tartalmak megosztására stb. Nem nehéz belátni, hogy különböző álhírek megosztása, legyen szó a Honvédség állapotáról, olyan politikai tartalmakról, amelyek a Honvédség feladatkörébe tartoznak (például migráció, határőrizet stb.), igen komolyan sérthetik az előírásokat.

Értelemszerűen ennyire szigorú előírások nem vonatkoznak a civilekre, ettől függetlenül a 2012. évi I. törvény a munka törvénykönyvéről[18] (Mt.) általános magatartási követelmények részénél meghatározza,

> „a munkavállaló a munkaviszony fennállása alatt – kivéve, ha erre jogszabály feljogosítja – nem tanúsíthat olyan magatartást, amellyel munkáltatója jogos gazdasági érdekeit veszélyeztetné. A munkavállaló munkaidején kívül sem tanúsíthat olyan magatartást, amely – különösen a munkavállaló munkakörének jellege, a munkáltató szervezetében elfoglalt helye alapján – közvetlenül és ténylegesen alkalmas munkáltatója jó hírnevének, jogos gazdasági érdekének vagy a munkaviszony céljának veszélyeztetésére. A munkavállaló magatartása a 9. § (2) bekezdésében foglaltak szerint korlátozható. A korlátozásról a munkavállalót írásban előzetesen tájékoztatni kell."

Az Mt. 11. §-a az alábbiakat írja elő:

> „a munkáltató a munkavállalót csak a munkaviszonnyal összefüggő magatartása körében ellenőrizheti. A munkáltató ellenőrzése és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével. A munkavállaló magánélete nem ellenőrizhető. A munkáltató előzetesen tájékoztatja a munkavállalót azoknak a technikai eszközöknek az alkalmazásáról, amelyek a munkavállaló ellenőrzésére szolgálnak."

Megítélésünk szerint e kitételek rendkívül nehezen tarthatók a gyakorlatban, hiszen sok munkahelyen a munkatársak, beosztottak és elöljáróik ismerőseik egymásnak a közösségi oldalakon, ami ha nem is jelenthet szándékos ellenőrzést, okozhat hátrányt a munkahelyen.

[18] 2012. évi I. törvény a munka törvénykönyvéről.

Az 1992. évi XXXIII. törvény a közalkalmazottak jogállásáról[19] (Kjt.) esetében nem találunk a Hjt.-hez hasonló előírásokat, azonban a 2011. évi CXCIX. törvény a közszolgálati tisztviselőkről[20] (Kttv.) Általános magatartási követelmények résznél megtalálható az alábbi kitétel:

> „A közszolgálati tisztviselő a munkaidején kívül sem tanúsíthat olyan magatartást, amely – különösen munkakörének jellege, a munkáltató szervezetében elfoglalt helye alapján – közvetlenül és ténylegesen alkalmas munkáltatója helytelen megítélésére, az általa betöltött beosztás tekintélyének, a munkáltató jó hírnevének, a jó közigazgatásba vetett bizalomnak, valamint a közszolgálat céljának veszélyeztetésére."

A Kttv. 12. § értelmében

> „a munkáltató a közszolgálati tisztviselőt csak a közszolgálattal összefüggő magatartása körében ellenőrizheti. A munkáltató ellenőrzése és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével. A közszolgálati tisztviselő magánélete nem ellenőrizhető. A munkáltató előzetesen tájékoztatja a közszolgálati tisztviselőt azoknak a technikai eszközöknek az alkalmazásáról, amelyek a közszolgálati tisztviselő ellenőrzésére szolgálnak."

A közösségi média kockázatai szervezeti szempontból

Az állami szférában a közösségimédia-használat engedélyezése hivatásnemektől függően eltérő lehet, hiszen a szervezet által kezelt adatok esetében eltérő kockázatot jelent. A Kádár-korszak klasszikus kultúrpolitikájának volt jelszava a három T, vagyis a tilt, a tűr és a támogat, amely véleményünk szerint a közösségimédia-használat esetében is követendő. Ennek eldöntése kockázatelemzést kíván meg a szervezet részéről.

Természetesen látni kell, hogy a teljes tiltás nem kivitelezhető abban az esetben sem, ha a szervezet munkatársainak részére nem engedélyezzük a közösségi médiában való jelenlétet. Elég csak a nemzetbiztonsági szolgálatok munkatársaira gondolni, hiszen a 2013-as Snowden-iratokból tudjuk,[21] hogy az amerikai nemzetbiztonsági szolgálatok valós időben képesek monitorozni a nagy közösségi oldalakon zajló kommunikációt, ez pedig komoly kockázatot jelent más nemzetek különleges állami szolgálatban dolgozói esetében. Azonban, mint ahogy Mark Zuckerberg 2018-as

[19] 1992. évi XXXIII. törvény a közalkalmazottak jogállásáról.
[20] 2011. évi CXCIX. törvény a közszolgálati tisztviselőkről.
[21] Greenwald 2014.

kongresszusi meghallgatásán elismerte, a Facebook[22] azokról a személyekről is gyűjti az adatokat, akik sosem regisztráltak a közösségi oldalakra.[23] Nem beszélve az okos mobileszközökre előre telepített alkalmazásokról, amelyek rendszergazdai jogosultság híján nem törölhetők a készülékről, és folyamatosan gyűjtik a különböző adatokat.

Azt sem szabad elfelejteni, ha tiltjuk is például munkahelyen a közösségi oldalak használatát szoftveres úton, például korlátozzuk az oldalak elérhetőségét a belső hálózatról, a felhasználó saját eszközéről, mobilinternetről már nem tudjuk ezt megvalósítani. Az egyes generációk között éles ellentétek mutatkoznak azzal kapcsolatban, hogyan viszonyulnak a közösségimédia-használathoz. Az elmúlt években az is beigazolódott, hogy a nagy közösségi oldalak, alkalmazások szándékosan úgy fejlesztik termékeiket, hogy azok függőséget okozzanak. Ráadásul minden tiltás annyit ér, amennyire ellenőrizni tudjuk, mindez pedig mind a regisztráció, mind pedig a munkaidőben történő használat esetében nehézkes.[24]

A kockázatelemzésre számos módszertan áll rendelkezésre, például az úgynevezett a Cramm-modell, amely a brit Central Computer and Telecommunication Agency által kidolgozott kockázatelemzési és -kezelési módszertan (CCTA *risk analysis and management method*). A Cramm-modell alapvetően az információs rendszerekben kezelt adatok esetében segít kockázatelemzést végezni.[25] A Nemzeti Kibervédelmi Intézet Hatósága is javasol különböző kockázatelemzési módszertant. Bármelyiket is választjuk, a cél mindegyik esetben azonos: a lehetséges kockázatok, illetve azok hatásának felmérése, amelyekre valamilyen kockázatkezelési megoldást választunk. Mivel a közösségi média folyamatosan változik, egyre megújuló biztonsági kockázatok jelennek meg, ezért az általunk választott kockázatelemzési módszertannak erre reagálni szükséges, és azt adaptív módon kell alkalmazni.

Első lépésként fel kell mérnünk, hogy a védendő vagyonelemek közül melyeket érinthetik a közösségi hálózatok irányából származó fenyegetések. Először érdemes megvizsgálni, hogy a közösségi média hivatali használata milyen jellegű információkat érinthet. Ennek érdekében célszerű a 2011. évi CXII. törvény az információs

[22] Joggal feltételezhetjük, hogy más techcégek is hasonló elvet követnek.

[23] Ilyen gyakorlat például a különböző scriptek használata a weboldalakon, amelyek segítségével integrálhatunk megosztást támogató ikonokat. Ezek a scriptek, amellett, hogy egy kattintással megoszthatjuk a számunkra érdekes tartalmat, egyúttal nyomon követik például, milyen weboldalról érkeztünk, mennyi ideig tartózkodtunk az oldalon, onnan hová megyünk tovább stb. Ezek mellett jellemző, hogy úgynevezett adatbrókertől vásárolnak adatokat, amelyeket például az okos mobileszközökön begyűjtött adatok értékesítéséből szereznek be harmadik féltől.

[24] Ez utóbbi esetében nem mintha nem lenne műszaki megoldás, de a szervezet informatikai munkatársai nem minden esetben ismerik ennek a módját.

[25] Eloff–Labuschagne–Badenhorst 1993: 597–603.

önrendelkezési jogról és az információszabadságról[26] alapján a különböző adatokat típusuk szerint elkülöníteni. A közösségi média használata során ugyan fennállhat a veszélye minősített adatok kiszivárgásának, de ennek kockázati szintje igen alacsonynak tekinthető. A problémát a közösségi hálózatok által kezelt és gyűjtött nagy mennyiségű személyes és adott esetben különleges adathoz való illetéktelen hozzáférés és felhasználás jelentheti.

Mint korábban említettük, a közösségi médiát változatos módon, gyakran saját eszközökön keresztül lehet elérni, amelyek különböző kockázati tényezőket jelentenek. Ezért a közösségi hálózatokon megjelenő információkon túl célszerű a fizikai vagyonelemekre vonatkozó leltárral és nyilvántartással folytatni a lehetséges kockázatok felmérését. A közösségi hálózatok ugyanis bármilyen okos mobileszközről elérhetők, így, ha nem szabályozzuk ezek használatát, a szervezet fokozottan ki van téve a közösségi hálózatok eléréséből származó kockázatoknak, amit a BYOD-politika engedélyezése tovább fokoz.

Amennyiben a szervezet kényelmi vagy költségvetési okokból él ezzel a lehetőséggel, mindenképp számolni kell azzal, hogy a munkavállalók hozzáférhetnek a közösségi hálózatokhoz, aminek számos biztonsági fenyegetése lehet, mint például a fentiekben említett metaadatok gyűjtése. Emellett további kockázati tényezőt jelent, hogy az okoseszközök szoftveres és egyéb[27] sérülékenységeit kihasználva számos módon feltörhetők, amelyen keresztül kritikus információkhoz lehet hozzájutni. Ennek értelmében a szabályozásnak érintenie kell az eszközökön található alkalmazások hálózati hozzáférésének korlátozását, valamint meg kell valósítani az általuk generált hálózati forgalom fokozott ellenőrzését.

A vagyonelemek fizikai nyilvántartása mellett fontos továbbá az eszközök teljes körű felmérése, ami számba veszi a rajtuk tárolt információkat, alkalmazásokat – beleértve az operációs rendszert – és technikai paramétereket, amelyek külön-külön kockázati tényezőként jelenhetnek meg. Ennek értelmében elengedhetetlen a megfelelő stratégia és szabályozási környezet kialakítása, ugyanis az okoseszközök és közösségi hálózatok teljes kitiltására vonatkozó szervezeti politika kialakítása nehezen megvalósítható és kontraproduktív.

Amikor kialakítjuk a szervezetünk közösségimédia-használatának szabályzóit, figyelemmel kell lennünk a fentieken kívül az alábbi tényezőkre is. Egyrészt nem tudjuk felügyelni, hogy adatainkat milyen szervereken tárolják. A tanulmány írásának idején éppen az ír adatvédelmi hatóság és a Facebook között ezzel

[26] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

[27] Ilyennek számíthatnak többek között az okoseszközök által használt 4G LTE protokoll sérülékenységeit kihasználó támadások (Hussain et al. 2018).

kapcsolatban komoly vita bontakozott ki.[28] Ennek értelmében az Európai Unió állampolgárainak Facebook által kezelt adatait kötelezően az EU területén levő szervereken lenne köteles tárolni a közösségi oldal, így védve az adatokat attól, hogy az amerikai nemzetbiztonsági szolgálatok felügyelet nélkül hozzáférjenek azokhoz. A Facebook ezzel kapcsolatban az európai piacról történő kivonulással fenyegetőzik, de ez vélhetően nem fog bekövetkezni, hiszen nemcsak a második legnagyobb piaca az Európai Unió, de számos tagállam a világ legerősebb gazdaságai között van, polgárai komoly vásárlóerőt jelentenek.

Azt sem szabad elfelejteni, hogy a különböző közösségi oldalakon nehezen átlátható a jogosultságkezelés. A szervezeti oldalak esetében nem mindegy, hogy hányan, milyen jogosultsággal férnek hozzá az oldalhoz. A kezelők lehetnek a szervezet munkatársai vagy külső vállalkozók, utóbbi esetben fontos szempont a marketinges, politikai tanácsadó cég megbízhatósága, referenciái. A szerződéskötéskor célszerű meghatározni, az adott cég hány munkatársa fog hozzáférni az oldalhoz, azonosíthatók-e a kezelők egyénileg, vagy csoportosan használnak egy közös profilt. A Facebook-oldalak, -csoportok kezelését adminisztrátorok végzik. Az adminisztrátorok dönthetik el a követők, tagok részvételének mértékét. Tilthatják a felhasználók oldalon, csoportban való tartalomgyártását (nem engedélyezik például a kommentelhetőséget, linkek, bejegyzések közzétevését). Egy oldalnak, csoportnak lehet több adminisztrátora, ráadásul eltérő jogosultságot lehet kiosztani az egyes kezelőknek. Ahhoz, hogy valaki adminisztrátor legyen, szükséges, hogy birtokoljon személyes profilt, amin keresztül belép a Facebookra és hozzáfér a hivatalos oldal kezelőfelületéhez. Egy oldal az általa megosztott tartalmakat hirdetésként is közölheti, ebben az esetben az oldalhoz egy számla is tartozik.

Egy felhasználó egy közösségi oldalon belül akár több különböző hivatalos oldal kezelője lehet. Ez esetben különösen fontos az azonosságkezelés, hiszen ha egy korábbi adminisztrátor már nem tagja tovább egy adott szervezetnek, de megmarad a felhasználónak az oldalkezelési jogosultsága ezt követően, óriási károkat képes okozni, akár bosszúból, akár anyagi haszonszerzés céljából. Amennyiben a támadók szereznek hozzáférést a kezelő személyes profiljához, úgy a hivatalos oldal esetében két főbb támadási irányt azonosíthatunk. Az egyik az anyagi haszonszerzéshez kapcsolódik, hiszen az oldalak hirdetéseket adhatnak fel, ily módon a támadók átvehetik a hirdetéskezelést, és az oldalhoz hozzárendelt számláról hirdetéseket rendelhetnek meg, költségét az általuk létrehozott számlára utalhatják. A Facebook hirdetési rendszere olyan elven működik, hogy a hirdető által preferált

[28] Dömös 2020.

célcsoportnak a lehető legszemélyesebb hirdetést jelenít meg, és a hirdetésre történő kattintást számlázza fel, nem magát a megjelenést. Az elmúlt években Magyarországon is gyakori volt ez a támadási forma, amelynek segítségével akár több százezer forintos károkat is okoztak a támadók a szervezeteknek.

A másik fő támadási irány a szervezet hivatalos oldalán közzétett tartalmak befolyásolása. A rosszindulatú tartalmak közzététele nagyban ronthatja egy szervezet megítélését, azonban sokkal komolyabb kockázatot jelenthet egy komplex kibertámadás esetében pánikkeltésre használt álhírek terjesztése a hivatalos oldalaknál. Egy nagy volumenű kibertámadás, terrortámadás, de valamilyen természeti katasztrófa megvalósulása esetében növelheti a lakosság körében fellépő pánik mértékét, amennyiben a támadók, felhasználva a hivatalos oldalakba vetett közbizalmat, olyan híreket tesznek közzé, amelyek súlyosabb következményeket kommunikálnak vagy olyan intézkedéseket fogalmaznak meg, amelyek további emberéleteket veszélyeztetnek.

A 9.1. táblázatban a Bányász Péter és Fekete Csanád által azonosított szervezeti kockázatok típusait ábrázoltuk, amelyek eligazodást nyújtanak a kockázatelemzéshez.

9.1. táblázat. *A közösségi média fenyegetettségei*

Fenyegetések		
Fenyegetési kategória	**Fenyegetés**	**Fenyegetés leírása**
Technikai és eszközalapú fenyegetések	Sérülékenységek kihasználása	Szoftveres sérülékenységek kihasználása, amelyek lehetővé teszik az eszközök feltörését és az érzékeny adatokhoz való illetéktelen hozzáférést
A szervezet megítélését érintő fenyegetések	A szervezetet érintő hamis vagy rosszindulatú információk közzététele	A szervezetet lejárató információk nyilvánosságra hozása a közösségi hálózatokon. Ezeket gyakran valamilyen szervezett dezinformációs vagy propaganda-hadjárat részeként hajtják végre
	A szervezet közösségimédia-oldalainak eltérítése	A támadók valamilyen módszert felhasználva illetéktelen hozzáférést szereznek a szervezet közösségimédia-profiljaihoz, ahol olyan információkat tehetnek közzé, amelyek rombolják a társadalmi megítélést. Emellett a szervezet megítélését rombolhatják az álcsoportok nevében közzétett félrevezető információk, amelyek a gyanútlan felhasználókat megtéveszthetik és pánikot kelthetnek

Fenyegetések		
Fenyegetési kategória	**Fenyegetés**	**Fenyegetés leírása**
A munkavállalókat érintő fenyegetések	Social engineering támadások	A közösségi médián keresztül a támadók könnyen kapcsolatba tudnak lépni a munkavállalóval, a hiszékenységét kihasználva pedig különböző támadások valósíthatók meg. Ezek segítségével illetéktelen hozzáférést szereznek a munkavállalók közösségimédia-profiljaihoz, ahol érzékeny információkhoz férhetnek hozzá. Kiemelt figyelmet kell fordítani a különböző online levelezőkliensekre, amelyek gyakran össze vannak kötve a közösségimédiaprofilokkal
	OSINT-alapú információgyűjtés	A szervezetre vonatkozó információk összegyűjtése, az egyre bővülő OSINT-módszerekkel. A közösségi média jól használható a munkavállalók kilétének megállapítására és a rájuk, valamint a szervezetre vonatkozó információk összegyűjtésére
	A szervezetet érintő információk szándékos kiszivárogtatása	A munkavállaló által hozzáférhető érzékeny belső információk tudatos kiszivárogtatása a közösségi médiában, ami rombolhatja a szervezet jó hírnevét és társadalmi megítélését
A műveleti biztonságot érintő fenyegetések	Bejegyzések, képek és videók engedély nélküli közzététele a közösségi médiában	Az állomány tagjai előzetes engedély nélkül tesznek közzé információkat egy művelet végrehajtása során, és ezzel veszélyeztetik a műveleti biztonságot
	Geolokációs adatok nyomon követése	A bekapcsolt eszközökön futó közösségimédia-alkalmazások által gyűjtött geolokációs adatok nyomon követése. Mindez jelentősen kihathat a műveleti biztonságra

Forrás: Bányász Péter és Fekete Csanád szerkesztése

A kockázatelemzés egyik legalapvetőbb módja a SWOT-analízis, amely a szervezet erősségeit, gyengeségeit (mint belső tényezőket), illetve lehetőségeit és fenyegetéseit (mint külső tényezőket) veszi alapul. A 9.2. táblázatban egy lehetséges SWOT-analízist végeztünk a szervezet aktív közösségimédia-használatát vizsgálva.

9.2. táblázat. *SWOT-analízis az aktív szervezeti közösségimédia-használattal kapcsolatban*

Aktív közösségimédia-jelenlét		
SWOT	**Pozitív oldal**	**Negatív oldal**
Belső tényezők	**Erősségek** • Információk nyilvánosságra hozatalának ellenőrzött formája • Egységes arculat • Közvetlen és nyílt kommunikációs csatorna a társadalom felé	**Gyengeségek** • Információbiztonsági tudatosság alacsony szintje • A közösségi média használatát érintő megfelelő kontrollok hiánya
Külső tényezők	**Lehetőségek** • Társadalmi megítélés javítása • Félrevezető információk és álhírek hatásainak csökkentése • A társadalmi feszültség és pánik megelőzése	**Fenyegetések** • Kritikus információk kiszivárgása • Műveleti biztonság sérülése • Szervezet társadalmi megítélésének romlása

Forrás: Bányász Péter és Fekete Csanád szerkesztése

A fentiek elkerülése érdekében, összhangban a 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról rendelkezéseivel, szükséges a szervezeten belül az alapvető információbiztonsági tudatosító képzések szervezése, amelyeknek vonatkozni kell többek között az alábbiakra.

- Kétfaktoros hitelesítés használata: amennyiben a támadók megszerezték a profilunkhoz tartozó jelszavunkat, a belépéshez szükséges egy véletlenszerűen generált, rövid ideig élő számsor megadása is, amelyet a telefonunkra küldenek. Ez figyelmeztet, illetve segíthet kiszűrni az illetéktelen belépési kísérleteket.
- Azonosságkezelés: ez egyrészt az egyes adminisztrátorok esetében eltérő jogosultságok kezelését teszi lehetővé, másrészt a korábban már említett egykori alkalmazottak visszaélésével kapcsolatban érvényes figyelemmel függ össze.
- Jelszókezelés: a megfelelő jelszószabályok használata, illetve a jelszavak meghatározott időközönkénti változtatása. Különösen fontos lenne egy jelszómenedzser-program használata, amely véletlenszerűen generál erős jelszavakat, a védelmük pedig erős titkosítással biztosított.
- Privát eszközök fokozott védelme: a különböző informatikai eszközök eltérő biztonsági kockázatot jelentenek, ebből következően, ha például a munkahelyi informatikai eszközök magasabb szintű védelmi megoldásokat alkalmaznak is, az otthoni vagy saját mobileszközünk nem megfelelő védelme támadási felületet szolgáltat. Például, ha az otthoni operációs rendszerünk nem jogtiszta, hanem *crackelt* verziót használunk, magában hordozza azt a lehetőséget,

hogy a *crack* olyan kártékony kódot tartalmaz, amellyel hozzáférhetnek a rendszerünkhöz. Ehhez kapcsolódik az eszközökön használt programok, *driverek up-to-date*-en tartása.
- Az oldalak alapvető biztonsági beállításainak elsajátítása.
- Adatvédelem: ennek keretében nem csupán arra kell kihegyezni az oktatást, hogy milyen kockázatokat rejtenek a közösségi oldalak, az ily módon gyűjtött adatokat hogyan, milyen célból használhatják fel, de fontos részét kell képezze azoknak a gyakorlatoknak az ismertetése, amelyekkel növelhető a magánszféránk és csökkenthető a technológiai adatgyűjtés (például a privát szférát erősítő technológiák ismertetésével, *cookie-k [cross-site], trackerek, scriptek* tiltása, anonimizálók, VPN-használat).
- Social engineering: ezen belül különösen az adathalász technikákra, az ellenük való védekezés módjaira.

ÖSSZEFOGLALÁS

A közösségi média a közigazgatási kommunikáció új dimenzióját jelenti. Lehetőséget kínál a társadalmi párbeszédre, és így az állampolgári bizalom növelésére. Ugyanakkor ez a transzparencia csak akkor tartható fenn, ha az intézmények egyidejűleg biztosítják az *adatvédelem, etika és hitelesség* érvényesülését is. A tudatos stratégia, az etikus működés és az MI-eszközök felelős alkalmazása együttesen alapozhatja meg a jövő *digitálisan érett közigazgatását.*

FELHASZNÁLT IRODALOM

1992. évi XXXIII. törvény a közalkalmazottak jogállásáról. Online: https://njt.jog.gov.hu/jogszabaly/1992-33-00-00.67

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról. Online: https://njt.jog.gov.hu/jogszabaly/2011-112-00-00.2

2011. évi CXCIX. törvény a közszolgálati tisztviselőkről. Online: https://njt.jog.gov.hu/jogszabaly/2011-199-00-00.3

2012. évi I. törvény a munka törvénykönyvéről. Online: https://njt.jog.gov.hu/jogszabaly/2012-1-00-00.38

2012. évi CCV. törvény a honvédek jogállásáról. Online: https://njt.jog.gov.hu/jogszabaly/2012-205-00-00

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról. Online: https://njt.jog.gov.hu/jogszabaly/2013-50-00-00

Bányász Péter (2018): Social engineering és közösségi média. *Nemzetbiztonsági Szemle,* 5(1), 59–77.

Bertot, John Carlo – Jaeger, Paul T. – Grimes, Justin M. (2020): Promoting Transparency and Accountability Through ICTs, Social Media, and Collaborative E-government. *Government Information Quarterly,* 37(4), 101495.

Criado, J. Ignacio – Sandoval-Almazan, Rodrigo – Gil-Garcia, J. Ramon (2023): Social Media in Public Administration: Trends and Challenges. *Government Information Quarterly,* 40(2), 102–119.

Dömös Zsuzsanna (2020): A Facebook azzal fenyegetőzik, hogy kivonul Európából. *24.hu,* 2020. szeptember 26. Online: https://24.hu/tech/2020/09/23/facebook-kozossegi-media-europai-unio-adatvedelem-kivonulas/

Eloff, Jan H. P. – Labuschagne, Les – Badenhorst, Karin P. (1993): A Comparative Framework for Risk Analysis Methods. *Computers & Security,* 12(6), 597–603. Online: https://doi.org/10.1016/0167-4048(93)90056-B

European Data Protection Board (2021): *Guidelines 8/2020 on the Targeting of Social Media Users.* Online: https://www.edpb.europa.eu/system/files/documents/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf

Greenwald, Glenn (2014): *A Snowden-ügy.* Ford. Böszörményi Jenő, Nagy Marcell. Budapest: HVG.

Hussain, Syed Rafiul et al. (2018): *LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE.* Network and Distributed Systems Security (NDSS) Symposium, 2018. február 18. Online: http://dx.doi.org/10.14722/ndss.2018.23313

Luna-Reyes, Luis Felipe – Gil-Garcia, J. Ramon (2021): Digital Government and Public Value Creation. *Information Polity,* 26(1), 1–15.

Mergel, Ines (2013): *Social Media in the Public Sector: A Guide to Participation, Collaboration and Transparency.* San Francisco: Jossey-Bass.

OECD (2023): *Integrity in Digital Government.* Párizs: OECD Publishing.

Thurman, Niel – Flew, Terry – Kuntsman, Adi (2023): Social Media, Disinformation and Trust in Government Communication. *Digital Journalism,* 11(5), 627–643.

United Nations (2024): *E-Government Survey 2024. Digital Government in the Age of AI.* New York: United Nations Public Administration Network.