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 minden ember számára fontosak, aki valaha, valamilyen webes fejlesztés közelébe kerül, és lehetősége-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.

Web 0, web 1.0, web 2.0, web 3.0 – rövid áttekintés

A web 3.0 előzménye a web 2.0, annak pedig a web 1.0, sőt: a web 0.

Részben történeti, részben pedig minőségi előzményekről beszélünk, hiszen az egyes szakaszokat többféle, így funkcionális szempontok szerint is elkülöníthetjük egymástól. Egymásból következő fejlődési útról beszélünk tehát, így a web 3.0 sem egy újfajta web, hanem a meglévő egyfajta „kiterjesztése", lehetséges fejlődési útja.[1]

A web 1.0 alatt a net 1990, web 2.0 alatt pedig a 2001 utáni időszakát szokták érteni.

Néha beszélnek web 0-ról is, vagyis az előtti időkről, amikor 1990-ben az ARPANET befejezte a tevékenységét. Addigra már létezett – a középkorú és az idősebb generáció számára ismerős – Internet Relay Chat (IRC), az amerikai egyetemek e-mailben kommunikáltak egymással, Németország és Kína között pedig e-mailes kapcsolat létezett, és az egykori katonai szegmenset (amely az egykori ARPANET főszereplője volt) is leválasztották a hálóról.

Erre az időszakra (1989–1990) tehető a weblapok és böngészők létrejötte is. Ez azért fontos fejlemény, mert a világháló leggyakrabban használt szolgáltatása a mai napig a weblapok közötti

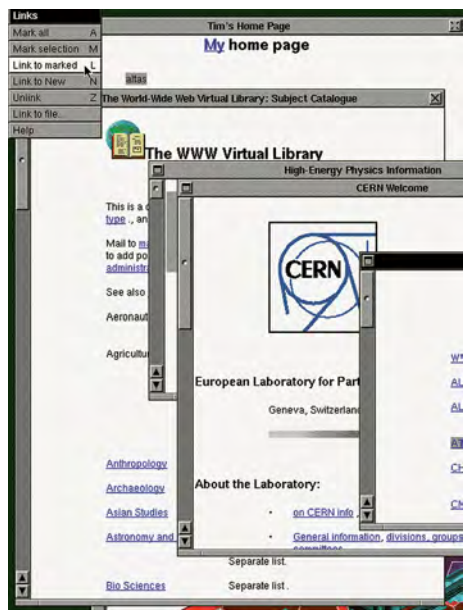
[1] Herendy Csilla: A kereső, a dokumentumok és a user. Budapest, Médiakutató, 2010.

https://doi.org/10.36250/00977_09

böngészés lehetősége. Ennek alapjait (vagyis a HTTP protokollt) egy európai kutató, Tim Berners-Lee, a CERN (Európai Nukleáris Kutatási Szervezet) fizikusa hozta létre.

9.1. ábra: Tim Berners-Lee saját számítógépe előtt a CERN-ben.
Forrás: © 1994–2018 CERN. *Vanityfair.com.*

Tim Berners-Lee a világháló alapötletén túl elkészítette az első böngészőprogramot is.



9.2. ábra: A világ első keresőmotorja, az Archie
Forrás: Informatikai jegyzetek és feladatok

9.1. táblázat: Internetstatisztika 1991–2018

Év	Weboldalak száma	Változás	Internethasználók száma	Átlagos felhasználók száma / weboldal	Legismertebb felületek
2018	1 630 322 579	–8%	–	–	–
2017	1 766 926 408	69%	–	–	–
2016	1 045 534 808	21%	–	–	–
2015	863 105 652	–11%	3 185 996 155*	3,7	–
2014	968 882 453	44%	2 925 249 355	3,0	–
2013	672 985 183	–3%	2 756 198 420	4,1	–
2012	697 089 489	101%	2 518 453 530	3,6	–
2011	346 004 403	67%	2 282 955 130	6,6	–
2010	206 956 723	–13%	2 045 865 660	9,9	Pinterest, Instagram
2009	238 027 855	38%	1 766 206 240	7,4	–
2008	172 338 726	41%	1 571 601 630	9,1	Dropbox
2007	121 892 559	43%	1 373 327 790	11,3	Tumblr
2006	85 507 314	32%	1 160 335 280	13,6	Twtter
2005	64 780 617	26%	1 027 580 990	16	YouTube, Reddit
2004	51 611 646	26%	910 060 180	18	Facebook, Flickr
2003	40 912 332	6%	778 555 680	19	WordPress, LinkedIn
2002	38 760 373	32%	662 663 600	17	–
2001	29 254 370	71%	500 609 240	17	Wikipédia
2000	17 087 182	438%	413 425 190	24	Baidu
1999	3 177 453	32%	280 866 670	88	PayPal
1998	2 410 067	116%	188 023 930	78	Google
1997	1 117 255	334%	120 758 310	108	Yandex, Netflix
1996	257 601	996%	77 433 860	301	–
1995	23 500	758%	44 838 900	1 908	Altavista, Amazon, AuctionWeb
1994	2 738	2006%	25 454 590	9 297	Yahoo
1993	130	1200%	14 161 570	108 935	–
1992	10	900%	–	–	–
Aug. 1991	1		–	–	World Wide Web Project

Forrás: NetCraft and Internet Live Stats (elaboration of data by *Matthew Gray of MIT and Hobbes' Internet Timeline and Pingdom)*

Web 1.0

A web 1.0, a „hőskor" – a web 2.0 szemszögéből (is) nézve – nem szólt másról, mint az online jelenlétről, a megmutatkozásról, cégek esetében a prospektus jellegű (ritkán frissülő) weboldalakról, egyes személyek esetében pedig a portfólió- és egyéb bemutatkozó oldalakról. Szólt még különböző híroldalakról, vagyis összességében a papírvilág egyfajta online leképezéséről, ahol a visszajelzés magától értetődő formája a telefon vagy a fax. E-mailes elérhetőség is szerepelt olykor a weboldalakon, de általában nemigen bízhattunk a gyors e-mailes válaszadásban (sem).

Hasonló módon képeztük le az 1990-es évek során a papírvilágot online felületen, mint ahogyan Gutenberg első nyomtatott, 42 soros Bibliája a kézírást igyekezett a sorokba szedett ólombetűk segítségével megjeleníteni az 1450-es években. Ugyanazt a vizuális felületet tettük át egy merőben más platformra. Kézzel írt bibliát nyomtatottra, szórólapokat online felületre.

Web 2.0

Amíg a web 1.0 az online jelenlétről és a közzétett információról, addig a web 2.0 (többek között) a felhasználók által generált tartalomról és a közösségekről, a közösségi cselekvésről szól.

A web 2.0-ról a 2001-es dotcomválság után kezdtek el beszélni, és az első, a témával kapcsolatos konferenciát – amelynek célja az volt, hogy a dotcomválság után megpróbálják helyreállítani a piac bizalmát, és feltárják, hogy bizonyos vállalatok miért élték túl a válságot – 2004-ben tartották. A web 2.0 kifejezés ezután, valamint Tim O'Reillynek köszönhetően vált ismertté. Akkoriban a web 2.0-t úgy igyekeztek meghatározni, hogy számba vették a web 1.0 és web 2.0 közötti különbségeket, például Britannica Online (a web 1.0 esetében) → Wikipédia (a web 2.0 esetében), publishing (a web 1.0 esetében) → participation (a web 2.0 esetében), personal websites (a web 1.0 esetében) → blogging (a web 2.0 esetében). (Az összehasonlítást lásd bővebben a 9.2 táblázatban.) A konferenciát követően az összehasonlítás ábra formájában a neten szélsebesen terjedt, O'Reilly később néhány pontján korrigálta, pontosította.[2]

9.2. táblázat: Web 1.0 és a web 2.0 összehasonlítása

Web 1.0		Web 2.0
DoubleClick	→	Google AdSense
Ofoto	→	Flickr
Akamai	→	BitTorrent
mp3.com	→	Napster
Britannica Online	→	Wikipédia
personal websites	→	blogging
evite	→	upcoming.org and EVDB
domain name speculation	→	search engine optimization
page views	→	cost per click
screen scraping	→	web services
publishing	→	participation
content management systems	→	wikis
directories (taxonomy)	→	tagging („folksonomy")
stickiness	→	syndication

Forrás: Tim O'Reilly: What Is Web 2.0. *Oreilly.com,* 2005.

[2] Tim O'Reilly: What Is Web 2.0. *Oreilly.com,* 2005.

További frappáns összehasonlítások a blogszférából:

Web 1.0: You and I
Web 2.0: Us

Web 1.0: Bring the web into our lives
Web 2.0: Bring our lives into the web

Web 1.0: „Under construction”
Web 2.0: „Beta”

9.3. ábra: Web 1.0: Under construction, legtöbbször mint under-construction.gif volt látható.
Forrás: OMG Standards Development Organization, *Omgwiki.org.*

9.4. ábra: Web 2.0: „Beta”
Forrás: Hashem Almakrami, almakramih.wordpress.com.

Tim O’Reilly a web 2.0-t a „kollektív intelligencia felhasználásaként” határozta meg, azonban a web 2.0 fogalmát illetően (természetesen) nincsen olyan definíció, amely *mindenki* számára elfogadható lenne. Sokan a közösségek erejét látják benne, mások „jelentés nélküli marketing buzzwordnek” gondolják,[3] egyesek pedig a web 2.0-ról beszélve kritikus jelleggel megemlítik, hogy a fogalom az üzletemberek számára a business 2.0-t, míg a szkeptikusok számára inkább dotcom 2.0-t jelenti.

Abban azonban többnyire egyetértés van, hogy a web 2.0 a közösen létrehozott tudásról, összeadott értékekről, közösségi hálózatokról szól, így jó példája a Wikipédia, a Flickr vagy a Facebook.

[3] O’Reilly (2005): i. m.

9.5. ábra: A szófelhő (tipikus webkettes megoldás) saját magát mutatja be
Forrás: Web 2.0. .Wikipedia.org.

Az általunk manapság leggyakrabban és leginkább használt felületek: Facebook, LinkedIn, Snapchat, Instagram vagy a Twitter, de ezeknél sokkal több *tool* érhető el (lásd a következő ábrát).

9.6. ábra: Webkettes megoldások témák szerint csoportosítva
Forrás: Project Handsonict

Web 3.0

Sokakban merül fel a kérdés: és mi lesz a web 2.0 után? Milyen lesz majd a web 3.0? Szemantikus (semantic) web? Érzékelő/érző (sentient) web? Esetleg szociális (social) web? Vagy talán mobil (mobile) web? Esetleg a virtuális valóság valamely formája? „Mindezek egyszerre, de még annál is több."[4]

O'Reilly–Battelle 2009-es elmélkedéséhez képest 2020-ra körvonalazódni látszik a helyzet, amit a 9.3 összefoglaló táblázat szemléltet. Effélékből számos elérhető online, különböző területekre vetítve. Látható, hogy az egyénre, a felhasználói viselkedésre és a gondoskodásra helyeződik a hangsúly.

9.3. táblázat: A fejlettségi szintek összehasonlítása

	Web 1.0	Web 2.0	Web 3.0
Kommunikáció	Egyoldalú	Interaktív	Elkötelezett / Befektetett
Információ	Statikus / Csak olvasható	Dinamikus	Hordozható & személyes
Fókusz	Szervezet	Közösség	Személy
Tartalom	Tulajdonosé	Megosztott	Felügyelt
Interakció	Webes adatlapok	Webes applikációk	Okosapplikációk
Keresés	Könyvtárak	Kulcsszavak / Tagek	Tartalom / Tárgyhoz tartozó
Mérés	Letöltött oldalak száma	Klikkenkénti költség	Felhasználói elköteleződés
Hirdetés	Bannerek	Interaktív	Viselkedés
Kutatás	Britannica Online	Wikipédia	Szemantikus web
Technológia	HTML / FTP	Flash / Java / XML	RDF / RDFS / OWL

Forrás: Aashish Sharma, 2018

A lehetőségek egyike a *szemantikus web elgondolás,* amely Tim Berners-Leetől[5] származik, 1998-ból. A szemantikus web víziójáról úgy szokás beszélni, mint az „értő" vagy „intelligens" webről, ahol az információk rendezettek, a keresés magától értetődően könnyű és precíz, ahol minden felhasználó egyszerűen és gyorsan megtalálja *egészen pontosan* azt az információt, amelyre szüksége van. Ideája tehát a „tökéletes keresés" és az „értő web", amely elérése érdekében többen többféle megoldást javasolnak, és a keresés tökéletesítésére is sokféle fejlesztés van folyamatban.

A webkettő üzleti vállalkozásaival szemben (AirBnB, Uber, Facebook) a web 3.0 *decentralizált tárhelyekről, kriptovalutáról*[6] is szól. Ennek egyik előnye, hogy nincsenek központok, se közvetítők, hanem a blokkláncok nyújtanak megbízható plaformot, titkosított adatokkal és feltörhetetlen szabályokkal. Ebben az elképzelésben még a legnagyobb vállalatok sem ellenőrizhetik a felhasználói adatokat, és egyetlen kormány sem állíthat vagy tilthat le weboldalakat, online szolgáltatásokat (Medium.com).

Merre tovább?

[4] Tim O'Reilly – John Battelle: Web Squared: Web 2.0 Five Years On. *Kimchristen.com.* 2009.
[5] Tim Berners-Lee: Semantic Web Road Map. *W3.org,* 1998.
[6] Werner Vermaak: Crypto Basics. What Is Web 3.0? *Coinmarketcap.com,* 2021.

Web 4.0 – „Mobil web”

A következő lépés valójában nem a web új verziója lesz, hanem egy alternatív változata annak, ami már megvan. A webnek alkalmazkodnia kell a mobil környezetéhez. A jelen lévő elképzelések egyike szerint a web 4.0 valós időben köti össze a valós és a virtuális világ összes eszközét. Kiváló példa erre a 2022-ben már elérhető okosotthon bármelyik megoldása[7], például amikor fizikai kontaktus nélkül, közelségérzékeléssel *(proximity sensing)* automatikusan elindulhatnak/leállhatnak a lakásban a dolgok, bekapcsolódnak a lámpák vagy beindul a fűtés. A Samsung Galaxy A52-es telefonban például a Bixby rutinok aszerint állítgatják a hangerőt, hogy hol van a telefon tulajdonosa, vagy a beállított alvásidő elején bekapcsolják, végén pedig kikapcsolják a repülőgép-üzemmódot.

Web 5.0 – Nyílt, összekapcsolt és intelligens web

Tim Berners-Lee igencsak magával ragadó TED-beszédet tartott 2009-ben, az új Open and Linked Web eseményen. Az előadásában mesélt arról, hogyan fogadta még 1990 előtt az akkori világ, kollégái és a főnöke az általa bemutatott *hypertext* elképzelést. Felvázolta azt az elképzelését is, miszerint bár a web 5.0 egyelőre fejlődő módban, a valódi formája is még kialakulóban van, a fejlődés első jelei már most körvonalazhatók. Eszerint a web 5.0 várhatóan egy olyan, összekapcsolt hálóról fog szólni, amely úgy kommunikál velünk, mint ahogyan mi kommunikálnánk egymással, vagy például egy személyes asszisztenssel.

A web 5.0 várhatóan az emberek és a számítógépek közötti (érzelmi) interakcióról fog szólni. Jelenleg a web „érzelmileg” semleges, ami azt jelenti, hogy a web nem érzékeli a felhasználók érzését és érzelmeit. Ez fog megváltozni a web 5.0 (azaz az érzelmi vagy érző web) használatával. Ennek egyik lehetséges példája a We Feel Fine applikáció,[8] amely feltérképezi az emberek érzelmeit. A felhasználók az app segítségével, fülhallgatón keresztül olyan tartalommal találkoznak, amely hat az érzemeikre és így az arckifejezésükre is.

Területek, esettanulmányok

A webes fejlődés az online kommunikáció világában, amióta az mint kommunikációs színtér létezik, többféle szférában, területen, más-más intenzitással van jelen. A különböző szféráknak különböző megjelenési jellegzetességeik, tulajdonságaik, sajátos problémáik, előnyeik és könnyebbségeik vannak, így nem egyféleképpen fejlődnek és vannak jelen.

Általános tapasztalat, hogy a fejlődésben rendre *élenjárók* a turizmussal, digitális turizmussal foglalkozó appok és weboldalak, szemben a települési site-okkal és a közigazgatási és e-közigazgatási megoldásokkal. Így volt ez a web 1.0-s időszaktól kezdve, és így van ez napjainkban is. Kérdés, mi lehet ennek az oka azon kívül, hogy a két szféra másképpen, más fókuszokkal, szakemberekkel, tudásokkal és szabályokkal működik. Az egyik szférában van igény a felhasz-

[7] Kiváló példák itt: www.reviewgeek.com/111275/smart-home-essentials-the-stuff-thats-actually-useful/

[8] We Feel Fine. *Number27.org.*

nálók rendszeres és aktív bevonására, jellemző például a felület előzetes tesztelése, a másikban pedig kevéssé vagy egyáltalán nincs erre igény, vagy pedig jellemzően kisebb-nagyobb hibákkal végzik azt.

Kérdés, mi lehet ennek az oka azonkívül, hogy a két szféra másképpen, más fókuszokkal, szakemberekkel, tudásokkal működik, és még inkább az: mit tanulhatnak egymástól az egyes területek? A következő fejezetben e két terület egymásmellettiségét is bemutatva röviden[9] összefoglaljuk a két szegmens online jelenlétét, és javaslatokat adunk a közigazgatási szféra aktuális és leendő képviselőinek arra, hogy ha bármilyen, például akár egy egyszerűbb applikációt, webes felületet, web vagy 3.0-s megoldást, települési kommunikációt, településmarketinget támogató *augmented reality*, illetve *immersive* videók megrendelését, készíttetését tervezik, hogyan válaszszanak maguknak megbízható és hiteles beszállítót. Nem kevéssé fontos résztvevői a folyamatnak a felhasználók is: szempontjaikkal a *XIV. Az ergonómia és az UX (User eXperience) elmélete és gyakorlata* című fejezet foglalkozik.

Feladat
Rendeződjenek párokba! Gondolja át, és írja le saját magának, aztán egyeztesse párjával, milyen mobilwebes megoldásokkal találkoznak a mindennapjaikban? Melyiknek milyen előnyei – hátrányai annak?

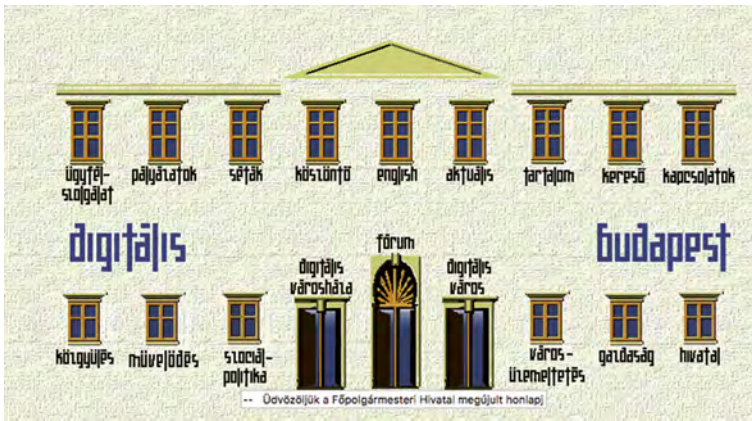
Turisztikai és települési weboldalak a web 1.0 és a web 2.0 idején

Már az internet viszonylag korai, web 1.0-s szakaszában látványos felületeket és megoldásokat produkált a digitális turizmus utazásszervezés, utazási információk és tippek tekintetében (lásd például az induló Lonley Planet vagy Travelweb oldalakat, 1994-ben). A digitális turizmus úgy definiálható, mint a turizmus online támogatása utazás előtt, alatt és után is.[10]

1996-ban a „Book through your local travel agent" szlogent felváltotta a „Book on our website" ajánlat. Vagyis lehetőség nyílott az oldalak (például Expedia) segítségével teljes utazást megszervezni, online jegyeket foglalni és szállást intézni. Ezzel egy időben a hazai városok online jelenléte még igazán web 1.0-s jellegű volt, ha egyáltalán jelen voltak az online térben. Brosúra típusú felépítés (lásd a Budapest.hu-t bemutató ábrát) jellemezte ezeket a felületeket, ahol jellemző kapcsolatfelvételi mód volt a telefon és a fax, e-mail-cím pedig elvétve volt megtalálható – nem is vártuk, hogy e-mailes kapcsolatfelvételünkre bárki rövid időn belül reagál.

[9] Ennek bővebb bemutatására jelen keretek között nincsen mód.

[10] David Benyon – Aaron Quigley – Brian O'Keefe – Giuseppe Riva: Presence and Digital Tourism. *AI & Society,* 29. (2013), 4. 521–529.



9.7. ábra: Budapest.hu, 1998.
Forrás: webarchive.com

Ebben az időszakban a legtöbb önkormányzat, település, sőt a közigazgatási szféra összességében még nem fedezte fel magának a webes kommunikációban rejlő hatalmas lehetőségeket, inkább óvatos hozzáállás volt tapasztalható a részükről. Idővel azonban a piaci szféra fejlődése és az állampolgári-turisztikai igények mintegy kikényszerítették a települések online jelenlétét is. Ennélfogva egyre kevésbé engedhették meg maguknak, hogy ne rendelkezzenek saját weboldallal. Ezek formátuma egy darabig még mindig inkább web 1.0-s jellegű volt (sőt, kisebb települések esetében még mindig az), és a főoldal terjedelmes vagy legfontosabb részét sokáig tipikusan a polgármesteri köszöntő foglalta el – és van, ahol elfoglalja napjainkban is, lásd például Hejőpapi weboldalát –, miközben az önkormányzati weboldalak felületén a legtöbbet keresett tartalom az óvodai jelentkezés, építésiengedély-ügyintézés volt, és manapság is az.

9.8. ábra: Hejőpapi weboldala, 2019. április
Forrás: Hejőpapi weboldala [képernyőkép], a szerző szerkesztése

A *web 2.0-s* időszakban olyan oldalak jelentek meg az online felületeken, mint például: LinkedIn (2003), Facebook (2004), YouTube (2005), Twitter (2006), Dropbox (2008) vagy a Pinterest (2010). Jellemző volt az online közösségek létrejötte, a közösségi akciók szerveződése, és olyan fogalmakkal ismerkedtünk meg az online térben, mint a lájkolás, közösségi jelenlét, megosztás. Gyarapodtak a Wiki-oldalak, a kommunikáció legjellemzőbb formái pedig a kommentek és a láj-

kok voltak. A felhasználók generálta tartalom lassanként elkezdte megelőzni, majd a webkettes időszak közepére már bőven megelőzte a tulajdonosok által közzétettet. A turisztikai szféra számára a jelenlét egyértelmű volt, komplett kampányok épültek YouTube-os videókra, és események teljesedtek ki azok segítségével.

Az ezeken a felületeken való jelenlét azonban egyre kevésbé elhanyagolható tényező. Arra, hogy mennyivel gyorsabb és hatékonyabb (ugyanakkor részben ellenőrizetlenebb is) a web 2.0-s média, emlékezetes példa a 2013-as bostoni maraton. A sporteseményen történt lövöldözésről még a klasszikus média is a Twitteren elérhető képeket és információkat használta, sőt, mi több: a rendőrség is a Twitter segítségével keresett képeket és felvételeket a történtekről.[11] Ugyancsak példa erre a 2022 márciusában zajló ukrán–orosz konfliktus: a webkettes megoldásoknak köszönhetően például szinte élőben követhetők egyes harci cselekmények és figyelhetők meg éles bevetésen a haditechnikai eszközök. Gyakorlatilag a szemünk előtt zajlik a háború a Facebook, a Twitter vagy a 9gag oldalain.

9.9. ábra: #mit fotója az esemény utáni estéről
Forrás:@smfrogers: The Boston Bombing How Journalists Used Twitter to Tell the Story. [Blogbejegyzés]. *Twitter Blog,* 2013. július 10.

Napjainkban egyre inkább természetesnek számít (vagy kellene hogy számítson), hogy a települések jelen vannak a webkettes felületeken, leginkább a Facebookon. Azonban az, hogy a települések vagy a különböző közigazgatási szervek mennyire összetetten vannak jelen a digitális térben, digitális jelenlétük és identitásuk mennyire kiforrott, szervenként és településenként változó.

A webkettes, közösségi médiabeli jelenlét egyértelmű volt a turisztikai szférának, de kihívásokat hozott a hazai közigazgatás számára. Sok településnek nagyon sokáig nem volt például saját Facebook-oldala, és az egyéb webkettes felületekre (Wikipedia, YouTube, Snapchat, Instagram, Twitter, tematikus weboldalak – linkgyűjtemények) is változó mértékben koncentráltak. 2022-ben néhány városnévre rákeresve (Érd, Tapolca, Zalaegerszeg), a Facebook által

[11] Erről bővebben:@smfrogers (2013): i. m.

automatikusan összeállított felülettel találkozunk csak. Sok település attól tart, hogy ha létrehoz egy Facebook-oldalt, azon majd elszabadulnak a posztok és a kommentek: ez azonban megfelelő kommunikációs aktivitással, külső-belső szabályokkal, beállításokkal megelőzhető, karban tartható. A Facebook-oldal hiánya turisztikai szempontból és egyéb kommunikációs aktivitásra tekintettel is kihagyott lehetőség.

Ugyancsak eltér településenként, hogy a weboldaluk esetében mennyire vannak tekintettel a keresőoptimalizálásra (SEO). Ezt és a webkettes, közösségi kommunikáció adta lehetőségeket is érdemes kihasználni: feltételük, hogy az adott szerv, település nyitott legyen a részvételre.

Ugyanilyen kihívást hoz a közigazgatási szféra számára a turisztikai oldalakon mára már megszokottnak számító kényelmes és gyors szállásfoglalás, egyszerű és gyors online fizetés, repülőjegy-foglalás, programtervezés, tehát gyakorlatilag a teljes ügyintézés. A hazai közigazgatás online felületei és az elektronikus közigazgatás gyors fejlesztése egyre inkább igyekszik ezeknek az igényeknek megfelelni.

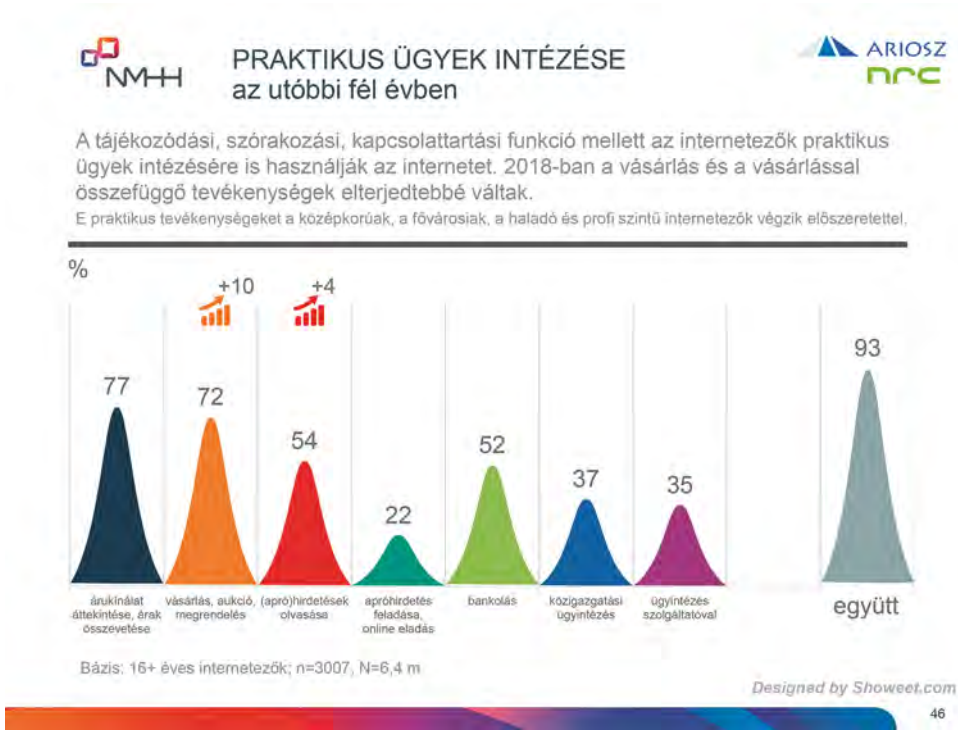
Míg az említett utazási oldalakat kizárólag hosszú és körültekintő tervezés, felhasználói tesztelés mellett fejlesztik és tartják fenn, addig ezek a tesztelések a hazai közigazgatási szféra oldalainak esetében vagy elmaradnak, vagy kevésbé szerencsés módszertannal végzik őket.[12] Például felhasználói tesztnek tekintik azt, amikor az informatikus ellenőrzi, hogy rendben átkattinthatók-e az oldalak (ami nagyon fontos feladat, de ez a tevékenység nem felhasználói, hanem programozói teszt). Más esetekben tesztelnek ugyan, de hibásan kiválasztott felhasználókkal, jellemzően a közigazgatás szerv alkalmazottaival. Ezzel az a probléma, hogy a készülő oldalnak a felhasználói gondolkodást lenne érdemes hangsúlyosabban figyelembe vennie, és nem a hivatalét, de ha hivatali alkalmazottakkal tesztelik az oldalt, akkor nem sokat tudnak meg arról, hogy érthetők-e annak funkciói a helyi lakosok számára.

Az állampolgároknak pedig éppen azért nehéz eligazodniuk ezeken a webes felületeken, mert azok a hivatal gondolkodását (mentális modelljét[13]) tükrözik, és nem veszik kellőképpen figyelembe az övékét. Ugyanezen felhasználók azonban időközben máshol már megszokták, hogy az oldal tulajdonosa tekintettel van rájuk, igyekszik könnyen és egyszerűen használható felületet létrehozni. Szívesebben is használják azokat: az NMHH 2022-ben legfrissebbnek számító, 2018-as évről szóló internethasználati felmérése[14] szerint a 16 évesnél idősebb internetezők 77%-a már online tájékozódik, 72%-a online vásárol is, 52%-uk online bankol, és csak 37%-uk használja az online közigazgatási ügyintézési lehetőségeket. Ezt az adatot torzítja (emeli) az a tény, hogy a vállalkozások kötelesek az online ügyintézést választani.

[12] Erről bővebben lásd: Herendy Csilla: Online kommunikációs kihívások a közigazgatásban. In Magyar Turisztikai Társaság: *Városi válaszok a globális gazdasági kihívásokra és technológiai trendekre különös tekintettel az intelligens városok modelljére.* Budapest, CITY GLOBE konferencia, 2015. 142–147.

[13] Erről bővebben lásd: Herendy Csilla: Miért fontos a user experience, a mentális modellek kutatása, és mi közük van a közigazgatáshoz? In Tózsa István (szerk.): *E-government tanulmányok 2019.* Budapest, Nemzeti Közszolgálati Egyetem Közszervezési és Közigazgatástani Intézet, 2019. 101–110.

[14] NMHH: Lakossági internethasználat online piackutatás, 2018. *NMHH.hu.*



9.10. ábra: 2018-as NMHH-felmérés, részlet
Forrás: NMHH: Lakossági internethasználat online piackutatás, 2018

Valószínűsíthető tehát, hogy nem azért nem terjed sokkal jobban és gyorsabban az e-közigazgatás, mert nem kellőképp érett a felhasználói nethasználat, vagy mert alacsony a lakosság digitális írástudása. Ugyanúgy terjedne, mint ahogy az online bankolás és az online repülőjegy-foglalás is. Vélhetően azért élünk ezzel a lehetőséggel ritkábban és nehézkesebben, mert a közigazgatási felületek jellemzően kevésbé jól használhatók és nehezebben érthetők,[15] régi megfogalmazással élve: kevésbé felhasználóbarátak. Igazi kihívásnak tűnik ez a közigazgatás számára, bár jó megoldások már most is láthatók. A közigazgatás webes jelenlétével, beleértve az eParticipációt, több írás is foglalkozik,[16] és több helyen a szerzők hangsúlyozzák a felhasználók igényeinek és érdekeinek figyelembevételét a webes fejlesztés során.[17]

[15] NMHH: Lakossági internethasználat online piackutatás, 2018. *NMHH.hu.*
[16] Lásd például: Alexander Schellong – Philipp Girrger: *Government 2.0 in der Betaphase January 2011.* CSC Public Sector Study Series, CSC, 2011.
[17] Stuart J. Barnes – Richard Vidgen: *Electronic Government, an International Journal,* 1. (2004), 2. 213–228.

Az alábbiakban azt tekintjük át röviden, hogy többek között milyen megoldásokkal rukkol elő a digitális turizmus az országok, városok kommunikációja területén. Míg a web 2.0-s időszakban kedvcsináló klipeket láthattunk, a web 3.0 idejére kitalálták a táj 360 fokos megtekintését is lehetővé tevő videókat. Olyan *augmented reality* megoldásokat kezdtek el alkalmazni, amelyek izgalmasabbá és érdekesebbé teszik az utazás előkészítését, magát az ottlétet és annak emlékeit is. A Sygic map pedig Google-térképszerűen teszi kereshetővé a helyi nevezetességeket.

Az *immersive videók* különlegessége, hogy már utazás előtt lehetővé teszik, hogy a turista odaképzelje magát, ahová majd utazni fog. Elindítva a videót, a bal felső sarokban elhelyezett nyilakkal körbe is tekinthet az adott város egyes részletein, a tájon.

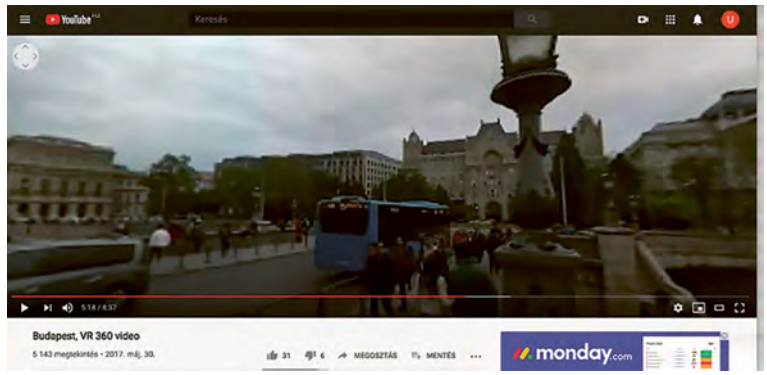
Amszterdam jól ismert korábbi kommunikációs kampányairól,[18] online megoldásairól, például web 2.0-s marketingvideóiról. Nem meglepő tehát, hogy az *immersive videók* tekintetében is újítónak számít, számos nagyvárossal együtt. Amszterdam immersive, a várossal előzetes ismerkedést lehetővé tevő, kedvcsináló mozgóképe a YouTube-on érhető el. A videóban (lásd 9.11. ábra) egy kedves lány mutatja meg nekünk a legfontosabb városi nevezetességeket, miközben a bal felső sarokban lévő nyilacskák segítségével körbe is tekinthetünk ott, amerre épp járunk. Az amszterdami életmódhoz csinál kedvet azzal, hogy búcsúzás után biciklire pattan, és elteker.

9.11. ábra: Amszterdam, immersive videó, YouTube
Forrás: YouTube

Ilyen videó Budapestről szintén elérhető a YouTube-on.[19] Ez nem történetmesélős videó, hanem inkább a 360 fokos szögben mozgatható kamerákkal lehet rajta nézelődni.

[18] Mihalis Kavaratzis – Gregory J. Ashworth: *Changing the Tide: the Campaign to Re-Brand Amsterdam*. Conference Paper. 46th Congress of the European Regional Science Association: „Enlargement, Southern Europe and the Mediterranean", August 30th – September 3rd, 2006. Volos, Greece Provided in Cooperation with: European Regional Science Association (ERSA). 2006.

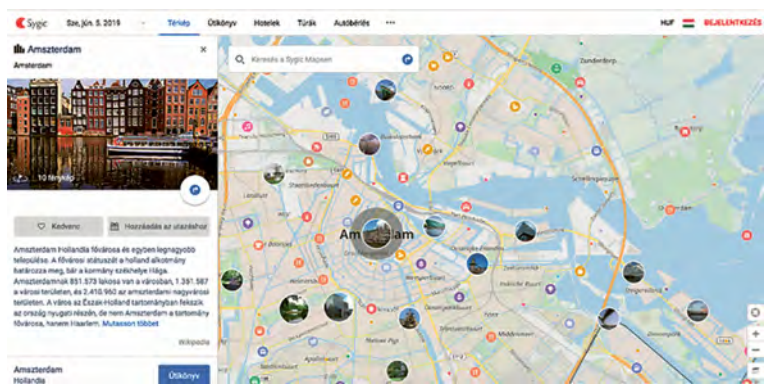
[19] Budapest, VR 360 videó. *Youtube*. 2017. május 30.



9.12. ábra: Budapest, 360 fokos videó
Forrás: YouTube

De segítőkész a YouTube akkor is, ha Koppenhágába[20] vagy épp Szentpétervárra[21] tervezünk utazni, és már szeretnénk előzetesen megismerkedni a várossal.

A *Sygic map* (lásd: 9.13 ábra) megoldás ugyancsak az utazás előzetes megtervezését, az ottlétet és az utazás felidézését támogatja. A felületen az adott város fontosabb nevezetességei láthatók. Segítségével hotelt is foglalhatunk, autót bérelhetünk, túrákat tervezhetünk. A Sygic map szintén elérhető más városok esetében is.



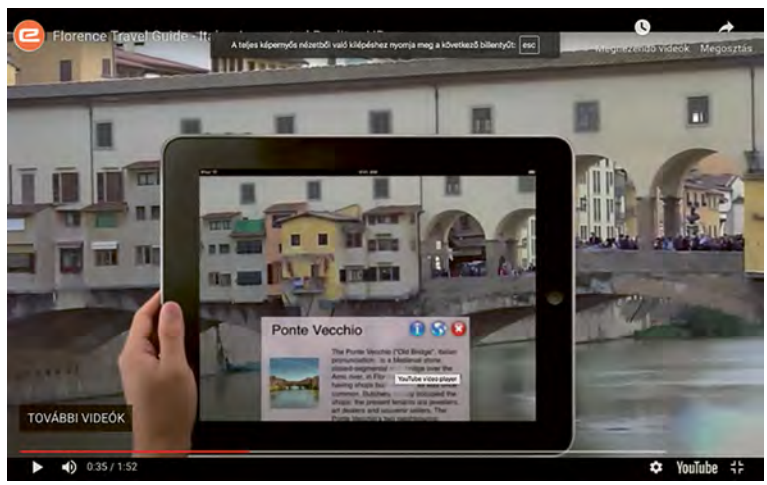
9.13. ábra: Sygic map, Amszterdam
Forrás: Sygic

A fentiekhez hasonlóképpen a digitális turizmus megoldásai közé tartoznak az *augmented reality* (kiterjesztett valóság) érzést kínáló, kifejezetten mobileszközökre (tabletre vagy mobiltelefonra) letölthető appok. Készíthetnek ilyeneket a múzeumok, támogatva ezzel a műalkotások megtekintésének élményét, városok (lásd 9.15. ábra), de készíttethetnek önkormányzatok is akár

[20] One day in Copenhagen: 360° Virtual Tour with Voice Over. *Youtube.* 2018. február 8.
[21] 360°, Church of the Savior on Blood, Saint Petersburg, Russia. *Youtube.* 2017. április 24.

(lásd 9.16 ábra), hogy egy tervezett beruházás látványát még az építési tervek jóváhagyása előtt ellenőrizhessék.

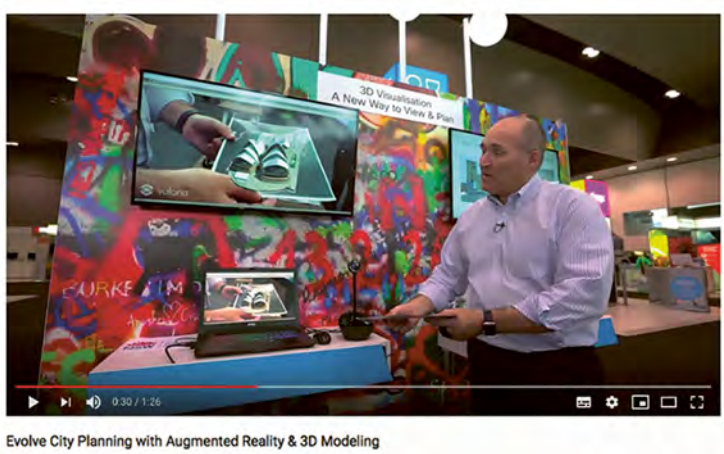
9.14. ábra: Amszterdam, augmented reality app: segítségével bárhová odatehetjük a város logóját, és fotót is készíthetünk róla
Forrás: Google Play webáruház



9.15. ábra: Firenze, Ponte Vecchio
Forrás: Revfine

Számos egyéb, nagyszerű ötlet és megoldás érhető el például arra is, hogy a mobiltelefonunkat egy-egy nevezetesség felé fordítva megtekinthessük annak adatait, történetét, vagy akár egy városrészletet 100 évvel azelőtt, vagy a világháború után. A települések számára hasznos, turizmus szempontjából egyre értékesebb megoldási lehetőségek ezek, sőt, még az oktatásban is kiválóan lehet őket használni, amikor azt szeretnénk a diákoknak megmutatni, hogyan nézett ki egy történelmi helyszín a második világháború előtt, alatt vagy után.

Azt, hogy korábban hogyan nézett ki egy komplett városrész, a virtuális valóság tudja nekünk megmutatni: ilyen megoldás segítségével tehetünk körutazást például a középkori Luxembourg utcáin.



9.16. ábra: Az augmented reality és a LEGO használata a várostervezésben
Forrás: YouTube

9.17. ábra: Augmented reality Luxembourg utcáin
Forrás: Urban Time Travel

9.18. ábra: Bal oldalon a virtuális valóság, jobbra a reality. Történelmi körutazás Luxembourg utcán
Forrás: YouTube

Hatalmas lehetőség az oktatásban, turizmusban, kihagyhatatlan megoldás a várostervezésben, már csak egy megbízható beszállítóra és elérhető költségkeretre lesz szükségünk. De hogyan válasszunk beszállítót? Erről szól a következő alfejezet.

Következtetések és javaslatok: a hiteles beszállítóválasztás szempontjai

Mindezek a megoldások tehát nagyszerű turistacsalogató webkettes, illetve webhármas lehetőségek, és nem véletlen, hogy egyre több település kap kedvet hasonlók fejlesztéséhez.

Milyen szempontokat vegyenek figyelembe a helyi önkormányzatok, turizmussal foglalkozó vállalkozások, múzeumok, ha *valóban* jó *augmented reality* (és egyéb, web 3.0-s) megoldást szeretnének fejlesztetni? Mire figyeljenek oda, ha *valóban* igény az, hogy a felület a felhasználóknak kedvezzen, netán szeressék is azt, és ajánlják másoknak is?

Általánosságban elmondható, hogy ha online app készül, érdemes ellenőrizni, hogy:

- Az ajánlatadó egyéb megoldásai letölthetők-e a Google Play áruházból?
- Ajánlják azok, akik korábban használták?
- Hogyan értékelik az appot a meglévő felhasználók?
- Ha építő jellegű vagy bármilyen kritikát fogalmaztak meg, érkezett-e arra válasz a felületen?

Egy konkrét alkalmazás megrendelése esetén tarthatunk önvizsgálatot is:

- Ha odamennék, használnám? Hasznos is a megoldás, vagy csak szép?
- Innen tájékozódnék vajon, amikor a nevezetességeket nézem majd? Legutóbb, amikor utaztam, használtam ilyen megoldást? Vagyis: az előttem látható látványra-élményre figyeltem elsősorban, vagy útikönyvet olvasgattam/appot néztem a látvány mellett?
- Nem épp a város élvezetében és a turisztikai élményemben zavarna egy ilyen applikáció?
- Elegendő a rajta keresztül elérhető információ, vagy szükséges még tovább keresgélni más felületeken?

Legyünk kritikusak:

- Működik élőben a megoldás, vagy csak a demóverziója látványos és szép?
- Látszódnak-e igazi vevői elégedettségek, valódi észrevételek?
- Van-e tényleges visszajelzés?
- Milyenek a vállalkozó korábbi megbízásai? Az készült el, amire szerződött?
- A webáruházban megfogalmazott kritikára reagál-e a fejlesztő vagy a tulajdonos?

Beszélgessünk a célcsoport tagjaival!

- Természetesen, mint minden UX (felhasználói élmény) kutatásra, úgy erre is igaz: az a legbiztosabb, ha a fejlesztést megelőzően beszélgetünk a célcsoport tagjaival. Ők hogyan szoktak az utazásuk előtt-során városi sétákat tervezni? Hogyan szeretnek a látottakról bővebb információhoz jutni? Legutóbb hogyan tették?
- Megoldás lehet az interjúalanyokkal a legutóbbi utazásaikról (mint konkrét példa) beszélgetni: hogyan tervezték az utazásukat, hol (milyen felületen) és hogyan (laptopon, mappában, képernyőn megtekintve vagy fotóalbumba rendezve?) tárolják az emlékeiket? Mire voltak kíváncsiak egy-egy nevezetességgel kapcsolatban, és hogyan szerezték meg a keresett információkat? Milyen egyéb információ volt hasznos, például kávézó-fagyizó a közelben, ajándékboltok, egyebek?

Kutatni nem kizárólag a tervezés előzetes fázisaiban érdemes, hanem végigkísérve a teljes fejlesztési folyamatot is.

Feladat
Rendeződjenek párokba. Gondoljanak ki és tervezzenek meg egy turisztikai és/vagy közigazgatási applikációt a fenti szempontok figyelembevételével!

Kockázatok és mellékhatások tekintetében…

A közösségimédia-használatnak 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-politika[22] – vagyis használd a saját eszközöd – tovább bonyolít. Napjainkban bizonyos munkakörök oly módon alakultak át, hogy betöltésükhöz nem vagyunk szorosan a munkahelyünkhöz kötve. A 2020-as évet felforgató Covid–19-járvány a *home office* esetében erősítette az otthoni munkavégzés lehetőségeit, hiszen sok esetben derült ki, hogy ugyanolyan hatékonysággal, viszont alacsonyabb költségek mellett lehet dolgozni. Vélhetően ez a digitális nomadizmusra[23] is fejlesztő hatással lesz, aminek következtében még inkább el fog mosódni a szabadidő és a munkaidő közti határ.

[22] Bring Your Own Device.

[23] 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.

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" címet viselő fejezetében részletesen foglalkozunk, így az ismétlés elkerülése érdekében itt csupán érintjük. A *social engineering* 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.[24] Az első lépés minden esetben a szervezet, illetve az esetleges gyenge láncszem feltérképezése.

Jól ismert közhely, hogy ami nincs fent a Google-ben, az nem létezik. Mégis, a Google (illetve más keresőszolgáltatások) által indexált weblapok csupán a teljes internet 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" (IoT), 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.[25]

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[26] az értő kezekben rendkívül hatékony információszerzést biztosít. Maga a nyílt forrású információgyűjtés legális, bárki által végezhető tevékenység. Mivel a felhasználók adat- és információbiztonsági tudatossága gyakran alacsony szintű, rengeteg olyan információt gyűjthetünk a célszemélyekről, amelyet zsarolásra vagy befolyásolásra használhatunk fel. Természetesen számos szoftver,[27] *tool*[28] 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 közösségimédia-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,

[24] Ezek közül a közösségi oldalak számos esetben támadási felületként szolgálnak. Bővebben lásd: Bányász Péter: Social engineering és közösségi média. *Nemzetbiztonsági Szemle,* 5. (2018), 1. 59–77.

[25] Ennek vannak speciális eszközöket igénylő részei, amelyek az úgynevezett „dark web", vagyis sötét web körébe tartoznak. Ezekkel jelen fejezetben nem foglalkozunk.

[26] A mozaikszó az Open Source Intelligence kifejezésből származik.

[27] Például a Maltego nevű program.

[28] Például az OSINT Framework nevű oldalon több tucat eszközt használhatunk, amelyek különböző technológiai úton gyűjthető adatok (többek között geolokációs helymeghatározás, hálózattal kapcsolatos információk) megszerzését is támogatják.

az esetleges védelmi megoldásokról, az ott dolgozók szokásairól, preferenciáiról. Díszítésként kitett képek, családunk fényképei, a monitorra post-ittel 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[29] rejthetnek, mint például geolokációs helymeghatározást. Fontos tehát, hogy körültekintően járjunk el az adatvédelmi beállításaink esetében, illetve rendszeresen ellenőrizzük azokat, hiszen a közösségi oldalak gyakran változtatják az általános szerződési feltételeiket – és ahogy többször is előfordult már –, átállítják a korábban megadott adatvédelmi beállításainkat, a nyilvánosság számára láthatóvá téve olyan tartalmakat, amelyeket korábban priváttá tettünk.

Mindebből belátható, hogy a közösségi oldalak alacsony *privacy*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 a kérdés, hogy médiaszolgáltatóknak minősülnek-e? Hiszen gyakran egy-egy felhasználó által megosztott tartalom válik virálissá, amely később a *mainstream* médiában is vezető hírré avanzsálhat. 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, akikkel kapcsolatban többek között a Magyar Honvédség esetében a a honvédek jogállásáról szóló 2012. évi CCV. törvény[30] (Hjt.) tekinthető irányadónak. A Hjt. 5. §-a az „Általános magatartási követelmények" kapcsán érinti a honvédek szolgálatteljesítésen kívüli szabályait, rögzíti a Magyar Honvédség iránti közbizalom megóvásának kötelezettségét. A Hjt. rendelkezik egyes alapjogok gyakorlásának korlátozásáról, ami 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 valaki 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 hasonlóak. Ezen belül pedig tanúsíthat a felhasználó olyan viselkedést, amely 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,

[29] 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, a böngésző típusa stb.

[30] 2012. évi CCV. törvény a honvédek jogállásáról (Hjt.).

vélemények akár kép, videó vagy írott szöveg formájában – alkalmas lehet pártpolitizálásra, a szolgálati fegyelmet sértő tartalmak megosztására stb. Nem nehéz belátni, hogy különböző álhírek megosztásával, 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[31] (Mt.) általános magatartási követelmények részénél meghatározza, hogy „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, elöljárók ismerőseik egymásnak a közösségi oldalakon. Ez nem feltétlenül jelent szándékos ellenőrzést, de okozhat hátrányt a munkahelyen.

Az 1992. évi XXXIII. törvény a közalkalmazottak jogállásáról[32] (Kjt.) esetében nem találunk a Hjt.-hez hasonló előírásokat, azonban a közszolgálati tisztviselőkről szóló 2011. évi CXCIX. törvényben (Kttv.) már igen. Az 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 „(2) 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. (3) A munkáltató előzetesen tájékoztatja a közszolgálati tisztviselőt azoknak a technikai eszközöknek az alkalmazásáról, amelyek a közszolgálati tisztviselő ellenőrzésére szolgálnak."

[31] 2012. évi I. törvény a munka törvénykönyvéről (Mt.).

[32] 1992. évi XXXIII. törvény a közalkalmazottak jogállásáról (Kjt.).

A közösségi média kockázatai a szervezet részéről

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–Tűr–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,[33] 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 dolgozó személyei esetében. Azonban, mint ahogy Mark Zuckerberg 2018-as kongresszusi meghallgatásán elismerte, a Facebook[34] azokról a személyekről is gyűjti az adatokat, akik sosem regisztráltak a közösségi oldalakra.[35] Nem beszélve az okosmobileszközökre előre telepített alkalmazásokról, amelyek rendszergazdai jogosultság híján nem törölhetők a készülékről, és folyamatosan gyűjtik a különböző adatokat.

Azt sem szabad elfelejteni, hogy ha tiltjuk is munkahelyen a közösségi oldalak használatát szoftveres úton, például korlátozzuk az oldalak elérhetőségét a belső hálózatról, a felhasználó saját eszköze, mobilinternete tekintetében már nem tudjuk ezt megvalósítani. Az egyes generációk között éles ellentétek mutatkoznak azzal kapcsolatban, hogyan viszonyulnak a közösségimédia-használathoz. Az elmúlt években az is igazolást nyert, 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.[36]

A kockázatelemzésre számos módszertan áll rendelkezésre, például az úgynevezett Cramm-modell, amely a brit Central Computer and Telecommunications 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.[37] A Nemzeti Kibervédelmi Intézet Hatósága is javasol különböző kockázatelemzési módszertanokat. Bármelyiket is válasszuk, a cél mindegyik esetben azonos: a lehetséges kockázatok, illetve azok hatásának felmérése, amelyekre valamilyen kockázatkezelési megoldást választunk. Mivel a közösségi média folyamatosan változik, egyre

[33] Glenn Greenwald: *A Snowden-ügy.* Budapest, HVG Kiadó Zrt., 2014.

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

[35] Ilyen gyakorlat például a különböző *script*ek használata a weboldalakon, amelyek segítségével integrálhatunk megosztást támogató ikonokat. Ezek a *script*ek, amellett, hogy segítségükkel 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 okosmobileszközökön begyűjtött adatok értékesítéséből szereznek be harmadik féltől.

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

[37] Jan H. P. Eloff – Les Labuschagne – Karin P. Badenhorst: A Comparative Framework for Risk Analysis Methods. *Computers & Security,* 12. (1993), 6. 597–603.

megújuló biztonsági kockázatok jelennek meg, ezért az általunk választott kockázatelemzési módszertannak szükséges ezekre reagálnia és adaptív módon kell alkalmazni.

Első lépésként fel kell mérnünk, hogy a védendő vagyonelemek közül melyek azok, amelyeket 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 önrendelkezési jogról és az információszabadságról[38] 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 okosmobileszközről 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 okokól él ezzel a lehetőséggel, mindenképp számolni kell azzal, hogy a munkavállalók hozzáférhetnek a közösségi hálózatokhoz, amelyek számos biztonsági fenyegetést jelenthetnek, mint például a fentiekben említett metaadatok gyűjtése. Emellett további kockázati tényezőt jelent, hogy az okoseszközök szoftveres és egyéb[39] sérülékenységeiket kihasználva számos módon feltörhetők, rajtuk 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, amelynek során számba kell venni 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 komoly vita bontakozott ki az ír adatvédelmi hatóság és a Facebook között ezzel kapcsolatban.[40] Ennek értelmében az Európai Unió állampolgárai Facebook által kezelt adatait kötelezően az EU területén levő szervereken lenne köteles tárolni a közösségi oldal, így védve az adatokat attól, hogy az ame-

[38] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról.

[39] Ilyennek számíthatnak többek között az okoseszközök által használt 4G LTE protokoll sérülékenységeit kihasználó támadások Syed Rafiul Hussain – Omar Chowdhury – Shagufta Mehnaz – Shagufta Mehnaz: LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE. *Network and Distributed Systems Security (NDSS) Symposium 2018*.

[40] Dömös Zsuzsanna: A Facebook azzal fenyegetőzik, hogy kivonul Európából. *24.hu*. 2020. szeptember 26.

rikai nemzetbiztonsági szolgálatok felügyelet nélkül hozzáférjenek azokhoz. A Facebook ezzel kapcsolatban az európai piacról történő kivonulással fenyegetőzik, de ez vélhetően nem fog bekövetkezni, hiszen nem csak 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 oldalak esetében nehezen átlátható a jogosultságkezelés. A szervezeti oldalak esetében nem mindegy, hogy hányan, milyen jogosultsággal férnek 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, linket, bejegyzések közzétevését). Egy oldalnak, csoportnak lehet több adminisztrátora, ráadásul eltérő jogosultságokat lehet kiosztani az egyes kezelőknek. Ahhoz, hogy valaki adminisztrátor legyen, szükséges, hogy birtokoljon személyes profilt, amelyen 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 is lehet. Ez esetben különösen fontos az azonosságkezelés, hiszen ha egy korábbi adminisztrátor már nem tagja tovább egy adott szervezetnek, de megmarad 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 olyan hirdetéseket rendelhetnek meg, amelyek költségét az általuk létrehozott számlára utalhatják. A Facebook hirdetési rendszere olyan elven működik, hogy a hirdető által preferált 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 komolyan kockázatot jelenthet egy komplex kibertámadás esetében pánikkeltésre használt álhírek terjesztése a hivatalos oldalak esetében. Ez egy nagy volumenű kibertámadás, terrortámadás, 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 9.4. táblázatban a Bányász Péter és Fekete Csanád által azonosított szervezeti kockázatok típusait ábrázoltuk, amelyek eligazodást nyújtanak a kockázatelemzéshez.

9.4. táblázat: A közösségi média fenyegetettségei

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 lejáratő információk nyilvánosságra hozása a közösségi hálózatokon. Ezeket gyakran valamilyen szervezett dezinformációs vagy propagandahadjárat 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.
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 közösségimédia-profilokkal.
	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 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, amivel 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 9.5. táblázatban egy lehetséges SWOT-analízist végeztünk a szervezet aktív közösségimédia-használatát vizsgálva.

9.5. táblázat: SWOT-analízis az aktív szervezeti közösségimédia-használattal kapcsolatban

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[41] rendelkezéseivel szükséges a szervezeten belül az alapvető információbiztonsági tudatosító képzések szervezése, amelyeknek vonatkozniuk kell többek között:

– A kétfaktoros hitelesítés használatára: 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.
– Azonosságkezelésre: ez egyrészt az egyes adminisztrátorok esetében eltérő jogosultságok kezelését teszi lehetővé, másrészt a korábban már említett egykori alkalmazottak visszaélésével kapcsolatban érvényes figyelemmel függ össze.
– Jelszókezelésre: a megfelelő jelszószabályok használatára, amelyeket meghatározott időközönként változtatni szükséges. Különösen fontos lenne egy jelszómenedzser-program használata, amely véletlenszerűen generál erős jelszavakat, a védelmük pedig erős titkosítással biztosított.
– Privát eszközök fokozott védelmére: 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 *crack*elt verziót használunk, az magában hordozza azt a lehetőséget, hogy a *crack* olyan kártékony kódot tartalmaz, amellyel

[41] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

hozzáférhetnek a rendszerünkhöz. Ehhez kapcsolódik az eszközökön használt programok, *driverek up to date*-en tartása.
– Az oldalak alapvető biztonsági beállításainak elsajátítására.
– Adatvédelemre, amelynek 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 emellett fontos részét kell képezze azoknak a gyakorlatoknak az ismertetése is, amelyekkel növelhető a magánszféránk, és csökkenthető a technológiai adatgyűjtés (például a privát szférát erősítő technológiák ismertetésével, *cookie-k, [cross-site] trackerek, scriptek* tiltásával, anonimizálók, VPN használatával).
– *Social engineeringre:* ezen belül különösen az adathalász technikákra, az ellenük való védekezés módjaira.

Összefoglalás, feladatok

Jelen fejezet arra vállalkozott, hogy a közigazgatási szféra számára fogalmazzon meg olyan ajánlásokat, amelyek abban segíthetik az önkormányzatokat, illetve településeket, vagy akár általánosságban a közigazgatási, államigazgatási szerveket is, hogy valóban jó, szerethető és jól használható web 3.0-s, *augmented reality* megoldásokat rendeljenek meg és fizessenek ki. A digitális turizmus, sőt az e-közigazgatás fejlődése is csak jó minőségű, felhasználói részvétellel fejlesztett felületekkel képzelhető el.

Feladat
Gondoljanak ki 2-3 fős csoportokban egy webkettes, webhármas települési kampányt! Mi lenne a kampány fő üzenete, és hogyan épülne fel? Kiket bíznának meg a különböző appok, online felületek elkészítésével? Hogyan választanák őket ki? Tegyenek részletes javaslatokat! (Külön papíron dolgozzanak.)

Főbb fogalmak

- adatbiztonság
- adatszivárgás
- adatvédelem
- anonimizálás
- befolyásolás
- BYOD
- fake news
- incidens
- jogosultságkezelés
- kockázatelemzés
- nyílt forrású információgyűjtés
- nyomkövető
- sérülékenység
- SWOT-analízis

Áttekintő kérdések

1. Engedélyezné-e a nemzetbiztonsági szolgálatok munkatársainak a közösségimédia-használatot? Válaszát indokolja!
2. Engedélyezné-e a minisztériumok munkatársainak a közösségimédia-használatot? Válaszát indokolja!
3. Ön egy önkormányzat információbiztonsági felelőse. Milyen szabályokat alkotna az önkormányzat Facebook-oldala kezelőjének?
4. Ön egy önkormányzat információbiztonsági felelőse. Milyen oktatást tartana a munkatársainak a közösségimédia-használatot illetően?

Felhasznált irodalom

@smfrogers: The Boston Bombing How Journalists Used Twitter to Tell the Story. [Blogbejegyzés]. *Twitter Blog.* Online: https://bit.ly/3s1fx77

1992. évi XXXIII. törvény a közalkalmazottak jogállásáról (Kjt.).

2011. évi CXCIX. törvény a közszolgálati tisztviselőkről (Kttv.).

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv.).

2012. évi CCV. törvény a honvédek jogállásáról (Hjt.).

2012. évi I. törvény a munka törvénykönyvéről (Mt.).

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

Benyon, David – Aaron Quigley – Brian O'Keefe – Giuseppe Riva: Presence and Digital Tourism. *AI & Society,* 29. (2013), 4. 521–529. Online: https://bit.ly/3I1JMQO

Berners-Lee, Tim: The Next Web of Open, Linked Data. *YouTube,* 2009. Online: www.youtube.com/watch?v=OM6XIICm_qo

Berners-Lee, Tim: Semantic Web Road Map. *W3.org,* 1998. Online: www.w3.org/DesignIssues/Semantic.html

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

Barnes, Stuart J. – Richard Vidgen: Interactive e-Government Services: Modelling User Perceptions with eQual. *Electronic Government, an International Journal,* 1. (2004), 2. 213–228. DOI: 10.1504/EG.2004.005179

Dömös Zsuzsanna: A Facebook azzal fenyegetőzik, hogy kivonul Európából. *24.hu.* 2020. szeptember 26. Online: https://bit.ly/3LKYxtC

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

Greenwald, Glenn: *A Snowden-ügy.* Budapest, HVG Kiadó Zrt., 2014

Herendy Csilla: *A kereső, a dokumentumok és a user.* Budapest, Médiakutató, 2010. Online: https://bit.ly/3sMumJW

Herendy Csilla: Miért fontos a user experience, a mentális modellek kutatása, és mi közük van a közigazgatáshoz? In Tózsa István (szerk.): *E-government tanulmányok 2019.* Budapest, Nemzeti Közszolgálati Egyetem Közszervezési és Közigazgatástani Intézet, 2019. 101–110. Online: https://bit.ly/3BtoKIi

NMHH: Lakossági internethasználat online piackutatás, 2018. *NMHH.hu.* Online: https://bit.ly/37A6vWS

Herendy Csilla: *Online kommunikációs kihívások a közigazgatásban.* In Salamin Géza (szerk.): *Városi válaszok a globális gazdasági kihívásokra és technológiai trendekre különös tekintettel az intelligens városok modelljére.* Budapest, CITY GLOBE konferencia, 2015. Online: https://bit.ly/3rZud6I

Herendy Csilla: *Tekintetkövetéses vizsgálat és online fókuszcsoportos pilot-kutatás a magyarorszag.hu oldalon*. Jel-kép, Budapest, 2018.

Hussain, Syed Rafiul – Omar Chowdhury – Shagufta Mehnaz – Shagufta Mehnaz: LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE. *Network and Distributed Systems Security (NDSS) Symposium 2018.* Online: https://bit.ly/35bYAhm

Kavaratzis, Mihalis – Gregory J. Ashworth: *Changing the Tide: the Campaign to Re-Brand Amsterdam.* Conference Paper. 46th Congress of the European Regional Science Association: „Enlargement, Southern Europe and the Mediterranean", August 30th – September 3rd, 2006. Volos, Greece Provided in Cooperation with: European Regional Science Association (ERSA). 2006. Online: https://bit.ly/350RdZT

Lu, Tan – Neng Wang: Future internet: The Internet of Things. In *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE).* IEEE, 2010. 5:V5-376-V5-380. Online: https://doi.org/10.1109/ICACTE.2010.5579543

O'Reilly, Tim – John Battelle: *Web Squared: Web 2.0 Five Years On.* 2009. Online: www.kimchristen.com/wp-content/uploads/2015/07/web2009_websquared-whitepaper.pdf

O'Reilly, Tim: *What Is Web 2.0.* 2005. Online: https://bit.ly/34NN7Vf

Schellong, Alexander – Philipp Girrger: *Government 2.0 in der Betaphase January 2011.* CSC Public Sector Study Series, CSC, 2011. Online: https://bit.ly/3sWqy94

Vermaak, Werner: Crypto Basics. What Is Web 3.0? Coinmarketcap.com, 2021. Online: https://bit.ly/3MTQhI6

Ajánlott irodalom

Essential1: *Why the Web 3.0 Matters and You Should Know About It.* Online: https://bit.ly/36nPz5j

Informatikai jegyzetek és feladatok, internet történet. Online: https://bit.ly/3gUqPU7

Szűts Zoltán: *Online. Az internetes kommunikáció és média története, elmélete és jelenségei.* Budapest, Wolters Kluwer, 2018.

Web 1.0 vs Web 2.0 vs Web 3.0 vs Web 4.0 vs Web 5.0 – A Bird's Eye on the Evolution and Definition. 2011. Online: https://bit.ly/3By055f