Kiberbűnözés és közösségi média

Bányász Péter[1]

Absztrakt:

Az infókommunikációs technológiák iránti függőségünk a bűnözés egy korábban soha nem tapasztalt formáját hozta létre a kibertérben. A kiberbűnözés sajátosságai új típusú kihívások elé állítják a felhasználókat és a bűnüldözőket. A tanulmány bemutatja azokat a kiberbűnözők által használt eszközöket és eljárásokat, amelyeket közvetetten vagy közvetlenül a közösségi média segítségével hajtanak végre az elkövetők.

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projektben működtetett Concha Győző Doktori Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Kulcsszavak: kiberbűnözés, közösségi média, terrorizmus, darknet, IOCTA

Abstract:

Our addiction of the information and communication technology created a special way of crime in the cyber space. The specialities of the cyber crime are particular challange for the users and for the persons who are responsible for the law enforcement. The study represents the tools and processes which are used by the cyber offenders. They make these actions directly or indirectly with social media.

The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance" in the Concha Doctoral Program.

Keywords: cybercrime, social media, terrorism, darknet, IOCTA

[1] Nemzeti Közszolgálati Egyetem Államtudományi és Közigazgatási Kar Elektronikus Közszolgálati Intézet, tanársegéd, ORCID azonosító: 0000-0002-7308-9304, elérhetőség: banyasz.peter@uni-nke.hu

Bevezetés

Napjainkban már- már közhelynek tekinthető a megállapítás, amely szerint az infókommunikációs technológiák elterjedése új típusú fenyegetettségek megjelenését hozta magával. Az okos mobil eszközök számának egyre nagyobb ütemű növekedése, a dolgok internetének kiterjedése várhatóan tovább növeli kitettségünket. Mindezek számos kockázatot hordoznak magukban, amelyek áttekintése még csak érintőlegesen sem férne bele e tanulmány terjedelmi korlátai közé. Ennél fogva az írás csupán a kiberbiztonság jelentette fenyegetést szándékozik bemutatni a szerző kutatási területére, a közösségi médiára fókuszálva, amelynek alapjául az Europol által évente kiadott, a szervezett bűnözés internetes fenyegetését vizsgáló jelentése szolgál.

Felületes olvasásra talán megdöbbenést kelthet, hogy a kiberbűnözést a közösségi médiával együtt említjük, hiszen alapvetően a különböző közösségi oldalakat barátainkkal, ismeretlenekkel való kapcsolattársra használjuk, milyen bajok származhatnak belőle. Rutinosabbak esetleg arra gondolnak, az általunk az oldalakon megosztott tartalmak, pl. mikor megyünk nyaralni jelenthetnek olyan információt, amelynek hatására betörnek otthonunkba, hiszen korábban egyébként az értékes televízió, festmény, egyebek előtt fényképezkedtünk, nem gondolva arra, hogy „értő szemeknek" a feltöltött képek teljesen másról árulkodnak, mint amit közölni szerettünk volna. Mint azonban látni fogjuk, sokkal komplexebb fenyegetéseket jelenthetnek a közösségi oldalak, legyen szó adatvédelmi kérdésekről, social engineeringről, pedofíliáról, terrorizmusról vagy éppen kiberhadviselés eszközéről. Való igaz, a közösségi oldalak alapvetően a barátainkkal, ismeretlenekkel való kapcsolattartásról szólnak, azonban annak függvényében, hogyan használjuk, igen eltérő veszélyeket hordanak magukban.

Napjainkban…

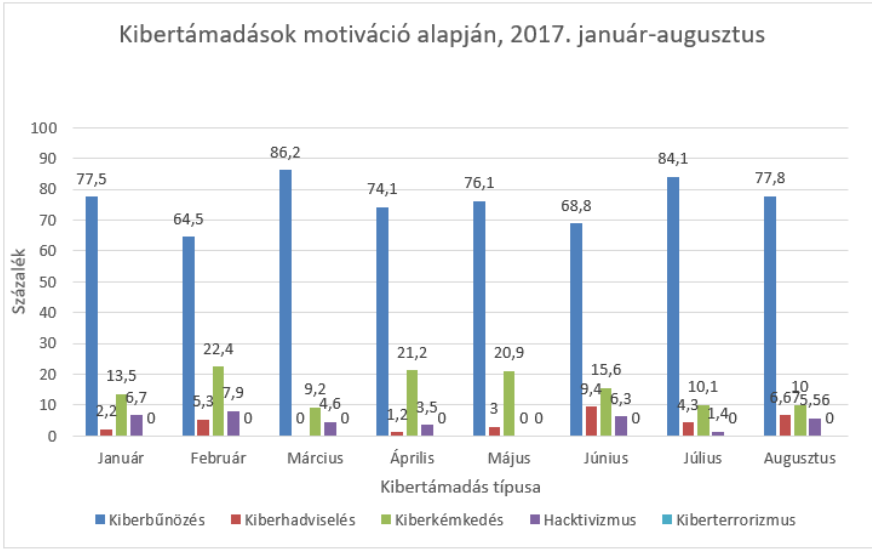
A kiberfenyegetéseket a szakirodalom alapvetően négy nagy csoportba sorolja.[2] A kiberbűnözés ez alapján az informatikai eszközök segítségével olyan illegális cselekmények elkövetése, amely a támadóknak anyagi haszonnal kecsegtet. A második nagy csoport a hacktivizmus és kiberterrorizmus, amelyek bár fogalmilag eltérő tevékenységet jelölnek, azonban bizonyos közös vonat kimutatható közöttük- mindkettő esetében kisebb, decentralizált csoportok működéséről beszélhetünk, amelyeknek célja a médiafigyelem elnyerése, hogy ezáltal hirdessék ideológiai céljaikat. A harmadik kategória a kiberkémkedés, amely az információs rendszerekben tárolt adatok megszerzésért végeznek állami és nem állami szereplők. Végül pedig negyedikként a kiberhadviselést kell említenünk,

[2] Krasznay Csaba: A polgárok védelme egy kiberkonfliktusban, In. Hadmérnök, 2012, VII:(4) pp. 142–151.

amely tevékenység az államok közti konfliktusokban jelenik meg, segítségével a szembenálló felek informatikai eszközöket alkalmaznak akár a konvencionális hadviselés támogatására, akár önálló tevékenység folytatására.

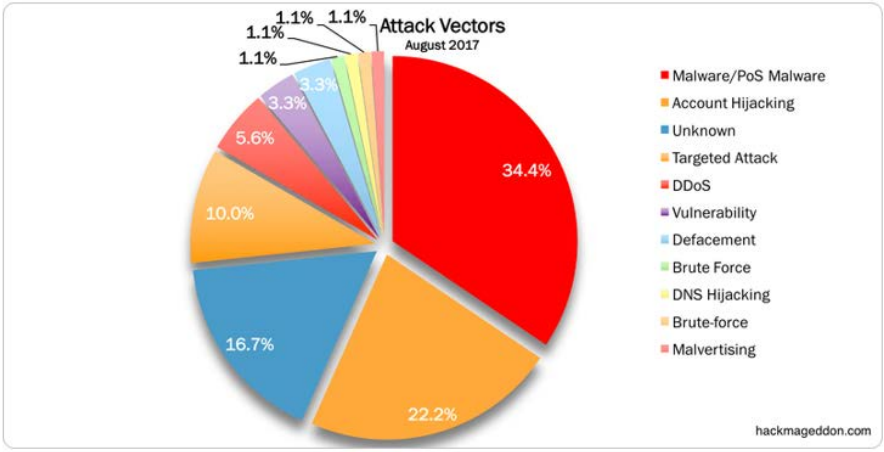
A kiberbűnözés azonban sajátságosnak tekinthető e négyes felosztásban. Ennek oka, hogy viszonylag korán egymásra találtak a szervezett bűnözői körök és hackerek, akik a minél nagyobb profit elérése érdekében az úgynevezett „Crime as a Service", vagyis „szolgáltatásszerű bűnözést" nyújtanak a vásárlóknak a Darkneten. Mindezt különösen professzionális keretek között, akár 0-24 órás help desket is fenntartva a megrendelői igényeknek megfelelően.

Mekkora fenyegetést jelent a kiberbűnözés? 2017 első öt hónapjának adatait alapul véve (lásd 1. számú ábra) megállapíthatjuk, hogy kiberbűnözés, februárt és júniust leszámítva, az összes támadás típus több mint két harmadáért felelt, márciusban kimagasló értéket olvashatunk le, az összes támadás 86,2%-a e kategóriába sorolható.



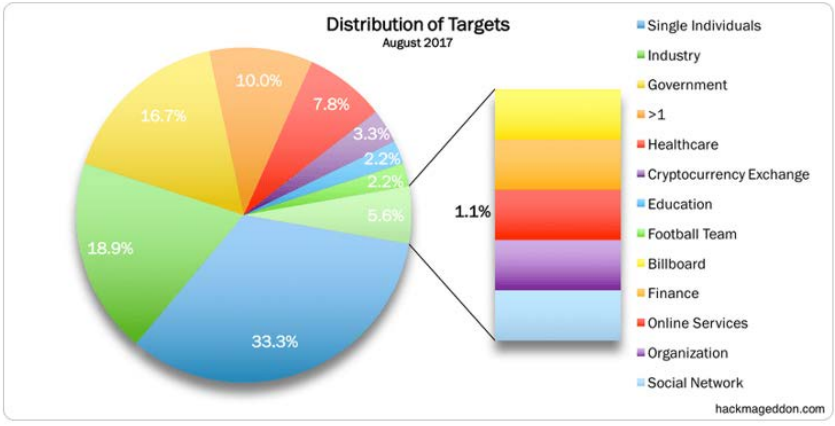
1. ábra Kibertámadások motivációk szerint 2017. január május (saját szerkesztés, forrás: http://www.hackmageddon.com)

Érdemes egy picit jobban megnézni, hogyan oszlanak meg a támadások az eszközök tekintetében. 2017 augusztusát alapul véve (2. számú ábra) elmondhatjuk, hogy leggyakrabban (34,4%) különböző rosszindulatú alkalmazások segítségével követtek el kibertámadásokat.



2. ábra Kibertámadások megoszlása eszközök szerint 2017. augusztus (forrás: http://www.hackmageddon.com)

Mindezt célpontokra vetítve azt tapasztaljuk (3. ábra), hogy az egyének (33,3%) mellett az ipari (18,9%) és kormányzati (16,7%) vannak a leginkább kitéve a támadásoknak.



3. ábra Kibertámadások megoszlása célpontok szerint 2017. augusztus (forrás: http://www.hackmageddon.com)

Ahogy egy közkedvelt toposz megfogalmazza, ami nincs fönt a Google-ben, az nem létezik. A WordWideWebSize oldal statisztikája szerint 2017. szeptember 24-éig több mint 4,55 milliárd weboldalt indexelnek a keresőszolgáltatások.[3] Figyelembevéve ezt az adatot, valóban könnyű elfogadni a mondás igazságtartalmát, hogy mindent megtalálunk az interneten. A teljes internet azonban nem ily módon áll össze. Az internet, amit mi használunk, és ennek fontos kritériumát jelenti, hogy valamilyen keresőszolgáltatás által indexelt honlap legyen, mindössze az internet körülbelül 5%-át teszi ki. A maradék 95% az úgynevezett Deep Webet, vagyis a láthatatlan internetet jelenti, amelyen a tartalmat nem indexeli semmilyen keresőszolgáltatás. Ide tartoznak többek között a felhők, a dolgok internete által generált adatforgalom is. Ennek a láthatatlan internetnek a része az úgynevezett Dark Net, vagyis sötét internet, amelynek keretében rendkívül könnyen és egyszerűen cserélnek gazdát illegális áruk és szolgáltatások.

A Dark Net népszerűségét elsősorban az adja, hogy az elérése olyan titkosítás alkalmazásával valósul meg, amely jelenlegi ismereteink szerint nem figyelhető meg, a titkosítást nem sikerült még feltörni, csupán a klasszikus felderítés eszközeit használhatják a bűnüldözők vagy a nemzetbiztonsági szolgálatok. Fontos azonban kiemelni a „jelenlegi ismereteink szerint" megfogalmazást. Mivel a Dark Neten pedofilok, terroristák, szervezett bűnözők igen jelentős ügyleteket bonyolítanak le, amelyek komoly fenyegetést jelentenek minden állam biztonságára, így vélelmezhetően az államok nemzetbiztonsági szolgálatai minden követ megmozgatnak, hogy sikerüljön feltörni azt a fajta titkosítást, amelynek segítségével a kommunikációs csatornákat védik az oldalak üzemeltetői.

A 2013-as Snowden ügy tanulságai[4] többek között arra is ráirányították a figyelmet, hogy az amerikai Nemzetbiztonsági Ügynökség (NSA) tudatosan gyengítette a kriptográfiai szabványokat, illetve beépült több titkosítással foglalkozó informatikai cégbe, amelyek szolgáltatásaiba később hátsókapukat nyitott. A Dark Net eléréséhez a TOR böngésző szükséges. A TOR[5] az US Navy egyik projektje volt, amit azzal a céllal alkottak meg, hogy a rendkívül kifinomult titkosítási eljárásnak köszönhetően szabad kommunikációs csatornát biztosítson a politikai

[3] WordWideWebSize, In. http://www.worldwidewebsize.com/ (Leöltve: 2017. szeptember 24.).

[4] Bányász Péter: Spies Act As A Spy: The Edward Snowden Case, In: Milan SOPÓCI, Mária PETRUFOVÁ, Miroslav ŠKOLNÍK, Viera FRIANOVÁ, Jaroslav NEKORANEC, Lubomír BELAN JIRÁSKOVÁ, Milota KUSTROVÁ, Stanislav MORONG (szerk.), Manažment - teória, výučba a prax 2014: zborník príspevkov z medzinárodnej vedecko-odbornej konferencie. 380 p.

[5] The Onion Router, magyarul: A Hagyma Elosztó. A neve a működési elvéből adódik, mivel az több szinten keresztül („mint egy hagyma rétegei") újabb titkosításokkal látja el a kezdeményező (initiator) csomagjait. A Tor hálózat minden tagja titkosítva kommunikál egymással 128 bites szimmetrikus kulcsolású kódokat használva, melyeket egy aszimmetrikus kulcsolású ún. handshake (kézfogás) után hoztak létre.

aktivistáknak, különösen olyan országokban, ahol a szabad véleménynyilvánítást nem feltétlenül tűrik meg vagy csak bizonyos korlátok között engedélyezik. Az interneten zajló kommunikáció megfigyelése nem újdonság, a nemzetbiztonsági szolgálatok számos eszközt és eljárást használhatnak erre. A már említett Snowden iratokból azt is tudjuk, hogy az internetes kommunikáció megfigyelésére valós időben, tömegesen is van lehetőség, így nem nehéz belátni az igényt arra vonatkozóan, hogy szabadon, mindenféle megfigyelés nélkül beszélhessünk ismerőseinkkel, barátainkkal, arról, amiről csak szeretnénk, ne kelljen öncenzúrát alkalmaznunk attól tartva, hogy egyébként valaki éppen figyeli a köztünk zajló kommunikációt. Természetesen a megfigyelésnek szigorú normatív szabályozásnak kell megfelelnie- elméletileg.

Az Edward Snowden által kiszivárogtatott információk egyik lényeges pontja volt, hogy az amerikai nemzetbiztonsági szolgálatok rendkívül kreatívan értelmezték az amerikai jogszabályokat, és nem egyszer megkerülték kiskapuk segítségével azokat. Ennek legjobb példája, amely szerint bírói felhatalmazás nélkül amerikai állampolgárokat nem figyelhettek volna meg- kivéve, ha kapcsolat állapítható meg egy megfigyelt külföldi állampolgárral. Az NSA viszont roppant megengedőnek bizonyult e kapcsolat felrajzolásában, nem érdekelte, hogy ez a „kapcsolat" egyébként több közbe ékelt személy hatására jött létre különböző országokból adott esetben, és a megfigyelt külföldi, illetve az amerikai állampolgár nem hogy nem ismerte egymást, de a másik létezéséről sem tudott.[6] A probléma az, hogy ezt az érthető, legitim igényt kielégítő alkalmazások rendkívül gyorsan terjednek el azok körében, akik valamilyen illegális cselekedet végrehajtásában használnák. Így vált többek között a titkosított kommunikációt biztosító Telegram Messenger az Iszlám Állam terroristáinak közkedvelt azonnali üzenetküldő alkalmazásává, amit maga az Iszlám Állam javasol használatra saját kiadású kézikönyvében,[7] a TOR böngésző pedig a kiberbűnözők felségterületévé.

Mielőtt elemeznénk a kiberbűnözés közösségi médiában való megjelenését, érdemes jobban megvizsgálni a kiberbűnözés fogalmát. Ahogy Simon Béla megfogalmazása szerint „korábban a számítógépes bűncselekmények a cybercrime fogalomkörébe tartoztak a biztonsági előírások megváltoztatásai, hobbi hackerek, honlap megváltoztatások, egyedi vírusok, szórványos támadások, egyfajta technikai érdeklődés az informatikai rendszerek biztonsági rései irányába. Leg-

[6] Dobák Imre: Technikai típusú információgyűjtés a változó biztonsági kihívások tükrében, In. Hadmérnök, XII. évfolyam 2. szám, 2017. június, pp. 235–249.

[7] Zetter, Kim: Security Manual Reveals the OPSEC Advice ISIS Gives Recruits, In: Wired, 2015. november 19., http://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/ (Letöltve: 2017. november 18.), a kiadványt magát lásd: Several cybersecurity to protect your account in the social networking http://www.wired.com/wp-content/uploads/2015/11/ISIS-OPSEC-Guide.pdf) (Letöltés dátuma: 2017. november 18.)

újabban azonban ezek kiegészültek a valóban kriminális szervezett bűnelkövetői csoportokkal, személyiség lopással, tervezett, irányított támadásokkal, kémkedéssel, szabotázzsal, felbérelhető profi hacker-ekkel, növekedő spam áradattal".

A szakirodalomban nem alakult ki egységes terminológia az ilyen típusú bűncselekményekre, van szerző, aki csúcstechnológiás bűnözésként, információ technológiai bűnözésként vagy számítógépes bűnözésként defininálja. A választott fogalom azért sem mindegy, mert például egy bankkártyával való visszaélés informatikai eszközök felhasználásával is történhet, de mégsem feltétlenül számítógépes bűnözés, ahogy mondjuk egy okos mobil eszközön egy kémprogram segítségével ellopott adatok sem számítógép segítségével valósulnak meg. E tanulmány során azért a kiberbűnözés fogalmát használom, mert megítélésem szerint a kibertér[8] egy olyan komplex fogalom, amely használt eszköz típusától függetlenül leírható.

Nem tekinthetünk el a kiberbűnözés lényegi sajátosságától, mi szerint a kibertér lebontja a klasszikus értelemben vett határokat, így az áldozat és az elkövető akár más országban, de akár más kontinensen belül tartózkodhat. Ebből következően a bűnüldözőknek nem csak a felderítés okoz nehézséget, hanem a felelősségre vonás is bonyolultabbá válik. Ennek érdekében különösen fontos, hogy olyan nemzetközi megállapodások szülessenek, amelyek lehetővé teszik a kiberbűnözés elleni fellépésben a jogharmonizációt. Ebben iránymutató a 2001-ben Budapesten megkötött Cybercrime Egyezmény, amely „*a számítástechnikai bűnözésről és az elektronikus bizonyítékokról szóló legfontosabb nemzetközi megállapodás marad, nemcsak a belföldi jogszabályok iránymutatásaként és a nemzetközi együttműködés alapjaként, hanem az együttműködési kapacitásépítés katalizátoraként.*"[9] Bár az Európai Unió jogharmonizációs tekintetben élen jár, azonban fontos, hogy az említett Cybercrime Egyezményt minél szélesebb körben ratifikálják.

[8] Haig Zsolt megállapítását kölcsönözve „egyértelműen kijelenthetjük, a kibertér fontos jellemzője, hogy abban az elektromágneses spektrumot felhasználva és/vagy vezetékes kapcsolaton keresztül hálózatba kötött infokommunikációs rendszerek működnek, amelyek különböző elektronikus információkezelési tevékenységeket (elektronikai úton végrehajtott adatszerzés, adatfeldolgozás, adattárolás, kommunikáció stb.) végeznek. A különböző hálózatba kapcsolt infokommunikációs rendszerek az információs környezet azon tartományát használják, amelyben e rendszerek működnek, léteznek (fizikai dimenzióban), a különböző elektronikus információkezelési folyamatok zajlanak (információs dimenzióban), valamint e rendszerek elleni tevékenység és védelem megvalósul (fizikai és információs dimenzióban). Ebből következően tehát, a kibertér az információs környezet fizikai és információs dimenziójában értelmezhető." In. Haig Zsolt: Információ- Társadalom- Biztonság, NKE Szolgáltató Kft., Budapest, 2015.

[9] Simon Béla: Bűnüldözés előtt álló digitális kihívások, In Magyar Rendészet (megjelenés alatt)

A kiberbűnözés mellett definiálni kell a közösségi médiát is. Mivel egy korábbi cikkemben, a Nemzetbiztonsági Szemlében ezt részletekbe menően elvégeztem,[10] így e tanulmány keretében csupán röviden határozom meg a fogalmat: a közösségi média olyan internetes alkalmazások és oldalak összessége, amelyekben a tartalmat a felhasználók állítják elő, a szolgáltató mindössze ennek a keretét biztosítja. Az előállított tartalom sokféle lehet (szöveg, videó, kép, hang), ami elméletben folyamatosan változhat, átalakulhat a közösség hatására.

Szeretjük vagy sem, a közösségi oldalak mindennapjaink részévé váltak: az otthonok, munkahelyek, iskolák, szabadidő megkerülhetetlen részesei. A 4. számú ábrán láthatjuk a népszerű közösségi oldalak látogatottságát.

4. ábra Közösségi oldalak látogatottsága, 2017. áprilisában (saját szerkesztés, Forrás: Statista.com)

A We are social nevű online marketingre szakosodott reklámügynökség globális felméréseit alapul véve megállapíthatjuk, hogy 2017. januári felmérése alapján[11] az aktív internet felhasználók száma meghaladja a 3,7 milliárd főt, ami

[10] Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe, In. Nemzetbiztonsági Szemle (Online) 2015., III:(2) pp. 21–36.

[11] KEMP, Simon: Digital in 2017- Global overview, We are social, 2017. január 24., https://wearesocial.com/special-reports/digital-in-2017-global-overview (Letöltés dátuma: 2017. szeptember 24.).

10%-os éves növekedést foglal magában. A közösségi média profilok száma több mint 2,7 milliárdra tehető, ami 21%-al magasabb, mint egy évvel korábban. Ebből a mobil eszközről való elérés több mint 2,5 milliárd felhasználói számot jelent, ez 30%-os éves növekedés (1. számú táblázat).

	Felhasználók száma (milliárd fő)	Penetráció aránya (%)	Éves növekedés aránya (millió fő)	Éves növekedés aránya (%)
Aktív internet felhasználók	3,773	50	354	10
Aktív közösségi média profilok	2,789	37	482	21
Egyéni mobil előfizetők	4,917	66	222	5
Aktív mobil közösségi média profilok	2,549	34	581	30

1. táblázat Internet és közösségi média használat globális szinten, 2016. (saját szerkesztés, forrás: We are social)

Az adatokból világosan leolvasható, a közösségi média használat olyan mértékű, hogy természetszerűen megjelennek benne azok az egyének, akik anyagi haszonszerzésre kívánják használni, nem elriadva adott esetben az illegális cselekményektől sem.

De mire használják a magyar internetezők a közösségi oldalakat? A Nemzeti Média és Hírközlési Hatóság témában elvégzett kutatását[12] alapul véve a 2. számú táblázaton olvashatóak le a leggyakoribb tevékenységek. Ez alapján nem túl meglepő, hogy a válaszadók több mint kétharmada (78%) a kapcsolattartást jelölte meg elsődleges szempontként. Érdemes megjegyezni, a válaszadók közel fele (49%) hírfogyasztás eszközeként tekint a közösségi oldalakra, ami beleillik a nemzetközi trendekbe.

Nem véletlen, hogy pár évvel ezelőtt a Facebook rendkívül sokat tett annak érdekében, hogy az online hírszolgáltatókat a felületére kényszerítsék, és így megkerülhetetlen, domináns szereplői legyenek a hírpiacnak. Amitől igazán pikánssá vált a helyzet, hogy a Facebook gyakorlatilag mindent tud a felhasználói preferanciáiról, és algoritmusa alapján megpróbálja a felhasználót leginkább

[12] NMHH: Lakossági internethasználat- Online piackutatás 2016., Ariosz Kft., NRC Kft., In. Nemzeti Média- és Hírközlő Hatóság, http://nmhh.hu/dokumentum/187704/lakossagi_internethasznalat_2016.pdf (Letöltve: 2017. szeptember 26.).

érdeklő hírt megjeleníteni neki. Ez azonban piaci szolgáltatásként is működik, ami a BREXIT és a Trump kampányban az álhírek terjesztésével új típusú, és annál jelentősebb fenyegetésekre hívta fel a figyelmet.

Használat célja	Százalék
kapcsolatot tartani barátokkal, családtagokkal, más, személyesen ismert emberekkel	78
kapcsolatot tartani olyan ismerősökkel, akikkel személyesen nem vagy nehezen tudok találkozni	54
érdekességekre rábukkanni	52
elolvasni, megtudni a friss híreket az ország-világ dolgairól	49
fotókat, videókat nézni	47
zenét hallgatni	45
kikapcsolódni, szórakozni	42
megtalálni olyan embereket, akikkel elvesztettem a kapcsolatot	26
fotókat, videókat megmutatni, megosztani	25
segítséget, tanácsot, információt kapni nekem fontos dolgokhoz, pl. iskolaválasztás, álláskeresés, gyereknevelés, magánélet	24
üzletek, szolgáltatók, vendéglátóhelyek, rendezvények profilját, saját magukról adott információit elolvasni	23
a tanuláshoz szükséges, hasznos	21
a munkámhoz szükséges, hasznos	19
hasonló érdeklődésű, gondolkodású emberek virtuális közösségéhez tartozni	18
ismerkedni, új embereket megismerni, barátokat szerezni	17
hírt adni saját magamról	13
megmutatni a tevékenységemet (pl. ahogy táncolok, zenélek vagy ha varrtam egy ruhát, készítettem egy tárgyat)	8
kapcsolatot tartani valamely hírességgel (pl. színésszel, zenekarral, politikussal)	5

2. táblázat A közösségi média használat okai százalékos megoszlás szerint (saját szerkesztés, forrás: NMHH)

Kockázatok és mellékhatások tekintetében

Ahogy a bevezetőben megfogalmaztam, az Europol Szervezett bűnözés internetes fenyegetettségét (IOCTA) vizsgáló éves jelentését veszem alapul e tanulmány során.[13]

A jelentés 12 területet foglal magába:

1. malwarekkel (pl. CryptoLocker, WannaCry. NonPetya stb.) való visszaélés.
2. gyerekek szexuális kizsákmányolása;
3. fizetőeszközzel elkövetett csalás;
4. social engineering;
5. adatok megszerzése, hálózatok támadása;
6. létfontosságú rendszerelemek ellen elkövetett támadások;
7. különböző pénzügyi tevékenységek (criminal-to-criminal payments, payment for legitimate services, victim payments);
8. online kommunikáció;
9. a kibertér és a terrorizmus összefonódása;
10. Darknet;
11. Internet of Things, Big Data, Clouds
12. internetirányítás.[14]

A 2016-os jelentés újdonsága, hogy megjelent benne két új terület, a kibertér és a terrorizmus összefonódása[15] és az internetirányítás. Szintén a bevezetőre kell visszautalnom, ahol azt írtam, elsőre nem is gondoljuk, hogy túl sok kapcsolat állapítható meg a kiberbűnözés és közösségi média között. Az Europol IOCTA jelentés 12 területéből mindössze két területtel, a különböző pénzügyi tevékenységekkel és az internetirányítással nem mutathatunk ki közvetett vagy közvetlen kapcsolatot.

Malwarekkel való visszaélés

Az angol malware kifejezés az angol malicious software (rosszindulatú szoftver, káros szoftver, kártékony szoftver) összevonásából kialakított mozaikszó. Ide

[13] Europol The Internet Organised Crime Threat Assesment 2016., Europol, Hága, 2016., https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 (Letöltve: 2017. szeptember 26.).

[14] Az internetirányítás fogalma azokat a globális megállapodásokat takarja, amelyek biztosítják az internet megfelelő működését és az internethez való hozzáférést. A legfontosabb kapcsolódó témák az internethez való hozzáférés, valamint az internet biztonsága

[15] Nem összekeverendő a kiberterrorizmussal!

tartoznak a vírusok, férgek (worm), kémprogramok (spyware), agresszív reklámprogramok (adware), a rendszerben láthatatlanul megbúvó, egy támadónak emelt jogokat biztosító eszközök (rootkit) és az egyre inkább globális méreteket öltő zsarolóvírusok (ransomware). Az informatikai eszközökre írt kártevő programok mennyisége folyamatosan növekszik, és időről időre új típusok terjednek el.

A közösségi médiában a malware-ek terjedése kiirthatatlan. Ahogy bizonyos időközönként újra és újra elterjednek bizonyos hoaxok (pl. Bill Gates szétosztja a vagyonát, oszd meg ezt, és te is kapsz belőle) és álhírek,[16] úgy terjednek rendszeresen különböző kártékony kódokat terjesztő alkalmazások, linkek. A közösségi oldalakon terjesztett malwarek alapvetően az üzenőfalunkon vagy személyes üzenetben érnek célt. Mindkettő esetében közös vonás, hogy a megfertőzött ismerősünk a tudta nélkül küldi ezeket a gyakran rövidített URL-be rejtett káros szoftvert. Akár személyes üzenetben kapjuk meg, akár üzenőfalunkon jelöl meg ismerősünk egy fertőzött URL-t, videót tartalmazó bejegyzésnél, rendkívül könnyű kiszűrni ezeket. Ennek ellenére igen eredményesen képesek tovább terjedni ezek a malwarek, mert az átlag felhasználó, sutba vetve minden gyanús jelt, mégis rákattint ezekre a fertőzött URL-ekre. Mik is ezek a jelek, amikre nem szoktak figyelni? Angol nyelven küld üzenetet az ismerősünk, aki egyébként nem beszél angolul, ahogy mi sem. A rövidített URL-el mindig gyanús kell hogy legyen, különösen olyan esetben, amikor a felhasználó, akitől kapjuk, vélhetően nem ismeri az URL rövidítésének eljárását. Gyakori továbbá, hogy híresség ekről szóló botrányt vagy rólunk szóló erotikus videót ígér a link.

A malware típusától függően a támadók számos célra használhatják a megfertőzött informatikai eszközt: megfigyelhetik az áldozatot, ellophatják az adatait, titkosíthatják filejait, amiért cserébe pénzt követelnek, botnet hálózat[17] részévé válhat az eszközünk.

[16] Pl. migránsok erőszakoltak meg a Bazilikánál egy fiatal nőt, a rendőrség és a média szigorúan titkolja az esetet. Az ilyen típusú álhírek, azért is érdekesek, mert hónapokkal később újra és újra feltámadnak, ugyanezzel a szöveggel, csak az időpontot datálva máskorra, és ugyanúgy nagy számú megosztást érnek el vele. In. Marinov: Migránstámadás a Bazilikánál? In. UrbanLegends, 2016. február, http://www.urbanlegends.hu/2016/02/migranstamadas-a-bazilikanal/ (Letöltés dátuma: 2017. november 18.)

[17] Botnet hálózat lényege, hogy a megfertőzött informatikai eszköz (legyen szó számítógépről, okos mobil eszközről, IoT eszközről) fölött átveszik a támadók, az irányítást, és annak erőforrásait a saját céljuk érdekében használják. Ez lehet spam küldő hálózat üzemeltetése, bitcoin bányászat vagy túlterheléses támadás elkövetése.

Gyerekek szexuális kizsákmányolása

A pedofil tartalmak mára alapvetően nem közösségi oldalakon keresztül terjednek (fórumok stb), hanem a Darkneten, azonban a közösségi oldalak igen komoly kockázatot jelentenek e területen.

Nem véletlenül több közösségi oldal tiltja, hogy 14 évesnél fiatalabb felhasználók regisztráljanak a felületén, ez azonban úgy vélem, önámítás. A regisztráció esetében nem kell igazolni a felhasználónak, hogy valóban annyi idős, mint amennyinek kiadja magát, innentől kezdve pedig olyan életkort állít be magának, amilyet szeretne. Ez történhet szülői közreműködéssel vagy anélkül- előbbi esetében egyfajta kontrollként, hogy lássuk gyermekeink online aktivitását, de úgy gondolom, ez is gyakran hamis biztonságérzetet adhat, amennyiben nem beszélünk rendszeresen a gyermekeinkkel az őket fenyegető veszélyekről, illetve nincs meg köztünk az a bizalmi viszony, aminek hatására elmondják az őket ért dolgokat. Az internetet, különösen a közösségi oldalakon nem mindenki az, akinek láttatja magát. Előfordulhat, hogy akiről gyermekünk azt hiszi, vele egykorú, az valójában egy nálánál jóval idősebb személy, aki így próbál meg erotikus képet, videót kicsalni tőle vagy rávenni szexuális tartalmú beszélgetésre vagy a későbbiekben valódi aktus lefolytatására.

Az által, hogy az okos mobil eszközök mára a beépített kamerájuk segítségével HD felbontásban képesek videót készíteni, továbbá elterjedtek az élő közvetítést lehetővé tévő szolgáltatások, (gondoljunk csak a Facebook Live vagy Youtube Live szolgáltatásaira), mindenféle komolyabb technológiai ismeret nélkül lehetséges online közvetíteni bármit. Az online stream pornószolgáltatások rendkívül nagy népszerűségnek örvendenek, óriási hasznot hajtanak. Természetesen ezeket nem Facebookon fogják az elkövetők végezni, azonban a gyermekek Facebookon és egyéb csatornákon történő behálózásával, adott esetben megzsarolásával, kényszerítésével dedikált csatornákon rendkívül könnyen képesek ezeket az üzelmeket végezni.

Gyermekeink még akkor is sokkal hiszékenyebbek, ha előzetesen átbeszéltük velük a veszélyeket és a biztonságos internethasználat szabályait,[18] így ezek ellenére is elkövetik naivan azokat a tiltott dolgokat, amik rendkívül veszélyesek lehetnek.

[18] Ezzel kapcsolatban érdemes az alábbi videót megtekinteni, amiben egy televízió stáb a szülőkkel előzetesen egyeztetve felvette a tinédzser lányokkal a kapcsolatot egy idősebb férfi személyében, és így csalták el őket akár egy furgonba, vagy vették rá őket könnyűszerrel, hogy a lányok otthonába hívja át a férfit, amikor egyedül volt otthon. A hét perces videó megtekinthető az alábbi linken https://www.youtube.com/watch?v=6jMhMVEjEQg vagy a YouTube keresőjébe a The Dangers Of Social Media (Girl Edition)! cím beírásával.

Fizetőeszközzel elkövetett csalás

A fizetőeszközökkel elkövetett csalások döntő többségében a bankkártyával összefüggő csalásokkal (visszaélés, hamisítás stb) kapcsolatosak, azonban az e-kereskedelem elterjedésével az egyéni vásárlók közötti (C2C) üzleti tevékenységek is rengeteg kockázatot jelentenek.[19] Ezek a felületek azonban a sikerük folytán integrálódásra kerültek a közösségi oldalakra is, ahogy például a Facebook Marketplace is mutatja.

Social engineering

A social engineering az emberi tényező kihasználhatóságára épülő támadási forma, olyan technológiák és eljárások összessége, amelyek segítségével a támadók egy védett rendszerhez a gyanútlan célszemély manipulálásával, megzsarolásával kívánnak hozzáférni.

A social engineering támadások esetében megkülönböztetünk humán[20] és IT[21] alapú támadásokat. Számos támadás esetében a közösségi média megkerülhetetlen. Az IT alapú támadásoknál említeni szükséges az adathalászatot, amely a malwarek fentebb említett alkalmazásával nyújt lehetőséget, a különböző alkalmazásengedélyek[22] megszerzését, amely az okos mobil eszközökre op-

[19] Krasznay Csaba- Simon Béla: Kiberbűncselekmények az online kereskedelemben, In. Hadmérnök,
XII. Évfolyam KÖFOP különszám - 2017.

[20] Deák Veronika: A social engineering humán alapú támadási technikái, In. Biztonságpolitika, 2017. április 10., http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-social-engineering-human-alapu-tamadasi-technikai

[21] Deák Veronika: A számítógép alapú social engineer támadási technikák, In. Biztonságpolitikai, 2017. április 28., http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-szamitogep-alapu-social-engineering-tamadasi-technikai

[22] Alkalmazások függvényében, rengeteg mindenhez hozzáférést engedélyezünk eszközeinken. A Facebook vagy a Google alkalmazás (amelyek sok esetben alapból telepítve vannak az eszközök, Androidos készülékről még csak le sem tudjuk törölni root, azaz rendszergazda jogosultság nélkül) közel 30 engedélyt kér a használatáért cserébe: minden üzenet tartalma, GPS alapú helymeghatározás, kamera és mikrofon vezérlés, az összes fileunk, kapcsolati hálónk stb. Ezek az alkalmazások azonban sok esetben kifejezetten adathalász céllal készültek el, és az óvatlan felhasználók ily módon gyűjtött adatait reklám célokra használják fel. Több esetben derült már ki, hogy több tíz millió felhasználó adatait adták el harmadik fél részére.

timalizált alkalmazások tekintetében jelentkezik vagy a WiFi hálózatokat.[23]

A humán alapú támadások esetében nem csupán a jelszavak kitalálására kell gondolnunk,[24] hanem a támadások kivitelezését megelőző információgyűjtésnek is kiváló eszközei a közösségi oldalai.

Nyílt forrásból rengeteg információ gyűjthető a célszemélyről, amelyeket később felhasználhatunk ellene. Minél régebb óta használ valaki egy közösségi oldalt, minél kevésbé figyel a biztonsági beállításokra, annál könnyebben tudunk róla használható információkat gyűjteni. Mindez ráadásul nem követeli meg, hogy órákat, napokat eltöltsünk az információgyűjtéssel, pár perc és néhány kattintás alatt megszerezhetjük az értékes információkat.

A social engineer addig fogja kutatni áldozatát, amíg meg nem találja azt a befolyásolható, adott esetben zsarolható személyt, akinek a felhasználáshoz hozzáfér a védett rendszerhez. Már pedig ezen oldalak segítségével rendkívül könnyen ismerhetik meg preferenciáinkat, életünk apró részleteit is, amelyek felhasználásával kiépíthet magának egy olyan legendát, amit felhasználva a közelünkbe férkőzik. Ha megtörtént a kapcsolatfelvétel, egy hamis Facebook profil segítségével, amellyel mondjuk előzőleg bejelölte több kollégánkat, akik ismeretlenül is visszaigazolták, tovább erősítheti a bizalmat. Ezt követően eljuttat hozzánk egy malwaret (egy fertőzött telefonalkalmazás vagy e-képeslap, vicces képeket tartalmazó ppt segítségével pl.), amit óvatlanul feltelepítünk, további információkhoz férhet hozzá.

Adatok megszerzése, hálózatok támadása

Az adatok megszerzése alapvetően az adathalászat segítségével valósul meg a közösségi oldalakon. Itt elsősorban nem a nyílt forrású információgyűjtésre kell gondolni, hanem egyrészt különböző adathalász alkalmazásokra, amelyek különösen népszerűek a közösségi oldalakon. Ezek az alkalmazások pár perc szórako-

[23] Még mindig rengetegen használnak nyílt WiFi hálózatokat, hiszen hozzá kell férni Facebookhoz, feltölteni egy kávézóban, étteremben megrendelt fogásokat Instagramra stb. Ezek pedig egyúttal magukban hordozzák azt a veszélyt, hogy a hálózat üzemeltetője monitorozza a hálózati forgalmat, és mindent lásson, amit a felhasználó végez. Fontos azonban kiemelni, attól, hogy egy nyílt WiFi hálózat jelszóval védett, még nem jelent nagyobb biztonságot, hiszen lehet, hogy ezzel akarják a támadók a bizalmat erősíteni a hálózattal kapcsolatban, továbbá amennyiben gyenge a WiFi hálózat védelme- ami az esetek jelentős többségében helytálló-, rendkívül könnyen fel lehet törni a hálózatot, és ezt követően figyelni az adatforgalmat.

[24] Sajnos továbbra is gyakori, hogy a jelszavak könnyen kitalálhatóak, nem kell a feltörésükhöz valamilyen algoritmust használni, a személyre utaló, értelmes szavak, amelyek a felhasználó több fiókjánál is ugyanazok. Így ha tudjuk mondjuk a Facebook jelszavát, sok egyéb fiókhoz is hozzáférhetünk, még több információt gyűjtve róla.

zást ígérnek a gyanútlan felhasználóknak, néhány kérdés megválaszolásáért cserébe megtudhatják, kik voltak előző életükben, kik lennének a Dallasból, vagy hogy mennyire intelligensek az olyan kérdések megválaszolásával, ami „a kitöltők 95%-a elront". Cserébe azonban hozzáférést engedünk a profilunkhoz és azon keresztül számos adatunkhoz. Ez különösen ott válik kockázatossá, amikor rendszeresen töltünk ki ilyen kvízeket, amelyek egy idő után nagyon hasznosak lehetnek az egyébként valójában profilozási céllal megalkotó fejlesztőknek- de erről bővebben a big data résznél. A hálózatok támadása itt malwarek esetében valósítható meg, amiről korábban már írtam.

Létfontosságú rendszerelemek ellen elkövetett támadások

A létfontosságú rendszerelemek elleni támadások a kiberhadviselés körébe tartoznak elsősorban. Azonban a szolgáltatásszerű bűnözés megjelenésével Darkneten a kiberbűnözők nyújtanak ilyen szolgáltatásokat.

Egy komplex kibertámadás végrehajtása óriási károkat okozhat, ami ellen védekezni mindig is hatványozottan drágább lesz, mint védekezni: egy lehetséges forgatókönyv adott.[25] A közösségi média ez esetben a nyílt forrású információgyűjtés, a social engineering, a malwarek elterjesztésében, a támadásra ráépülő dezinformáció kampány esetében használható, míg a védekezés szempontjából a kríziskommunikációban van óriási szerepe.[26]

Online kommunikáció

A Snowden iratokból tudjuk, hányféle kapcsolattartást tesz lehetővé a közösségi média, és mily módon figyelték meg az abban érintett nemzetbiztonsági szolgálatok ezeket a felületeket. Mégis, ezek ellenére továbbra is megmaradtak olyan eljárások, amelyeket nehezen tudnak megfigyelni, értékelni, elemezni az arra hivatott szolgálatok. Egy feltöltött képbe elrejtett üzenetek kiszűrésére megvan a technikai eszköz,[27] azonban ha a kommentekben elrejtett kódolt üzenetek, vagy egy feltöltött videóban szintén úgy összeállított tartalmakat használnak a konspi-

[25] Kovács László, Krasznay Csaba: A digital Mohács: a cyber attack scenario against Hungary
Nemzet És Biztonság: Biztonságpolitikai Szemle III:(Spec. Issue Winter) pp. 49-59. (2010)

[26] Bányász Péter, Orbók Ákos: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében, In. Hadtudomány: A Magyar Hadtudományi Társaság Folyóirata XXIII:(1 elektronikus) pp. 188-209. (2013)

[27] Bertók Zsófia: Szteganográfia,
http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2010/HF-reports/BertokZsofia.pdf

rált kapcsolattartásra, amelyek jelentését csak a beavatottak ismerik, nehéz kiszűrni.[28]

Ezen felül több olyan alkalmazást forgalmaznak, amelyek elméletileg titkosított (VoIP) kommunikációt tesznek lehetővé, pl. Signal, Telegram Messenger, de ilyen szolgáltatásokat ígér a Facebook, Google Hangouts, Viber is, de ez utóbbiakról eddig mindig kiderült, hogy az a titkosítás nem igazán több, mint marketingfogás.

A kibertér és a terrorizmus összefonódása;

A kibertér és terrorizmus összefonódására az Iszlám Állam tökéletes példával szolgál. Ez alapján, az alábbi területeken használhatják a közösségi médiát, mint ahogy többségüket az elmúlt években használták is:

- információgyűjtés,
- social engineering,
- kapcsolattartás,
- propaganda,
- új tagok toborzása,
- támogatók szerzése,
- pszichológiai és információs hadviselés,
- kibertámadás.

Szerencsére napjainkban még nincs meg a humán és technikai képességük a terroristáknak, hogy egy létfontosságú rendszerelem ellen kövessenek el kibertámadást, azonban a Darkneten kellő anyagi forrás meglétével megvásárolhatnak ilyen szolgáltatást.

Darknet

A gyermekek szexuális kizsákmányolását korábban említettük, a Darknet azoknak a pedofil tartalmaknak terjesztésére kiváló terepet nyújt akár képek, videók, akár online stream formájában. Amikor gyermekek szexuális kizsákmányolásáról beszélünk, tisztában kell lenni, hogy csecsemők sérelmére is követnek el ilyen bűncselekményeket. A Darkneten több olyan hálózatot lepleztek le, amelyek több százezer képet tartalmaztak, amik csecsemők megerőszakolását ábrázolták.

[28] Gondoljunk csak arra, hogy ha például egy sportesemény közvetítése alatt, olyan kommenteket helyeznek el, ami egyébként a sportesemény kontextusába illő, azonban a valódi tartalmat csak a pár beavatott ismeri. Hasonló a helyzet egy általunk feltöltött amatőr videó esetében is, amelyben pl. egy GoPro segítségével járjuk a múzeumokat, és bemutatjuk azokat az érdekes történelmi műtárgyakat. Kinek tűnik fel közben, hogy az őrök, kamerák elhelyezkedése is bele-bele esik mintegy véletlenül.

Ahogy a terrorizmus és létfontosságú rendszerelemek elleni támadás esetében említettük, itt vásárolhatnak olyan szolgáltatásokat a támadók, amelyet céljaik elérésére használhatóak, legyen szó botnet hálózatokról, a közösségi oldalak, okos mobil eszközökre írt alkalmazások által gyűjtött adatokról.

Internet of Things, Big Data, Clouds

Végezetül a big data-ról és a számítási felhőkről kell szólni. A big data megfelelő értékelésével és elemzésével rengeteg értékes információ nyerhető ki. Az adatok megszerzése esetében érintőlegesen már említettem a közösségi oldalakon népszerű kvízeket. Donald Trump kampányban nagy szerepe volt egy Cambridge Analytica nevű big data analízissel és lélektani műveletekkel foglalkozó cégnek, ami számos forrásból, többek között ilyen kvízekből gyűjtött adatokat a felhasználói szokásokról, s használta fel célzott politikai hirdetések megjelenítésére. A Facebook közel sok ezer szempont alapján gyűjti a felhasználókról az információt, s ez alapján óriási pontossággal meg tudja használni a felhasználó preferenciáit. Ezeket természetesen forgalmazza is. Ezeknek az információknak a megszerzése igen csak jövedelmező, különösen a Darkneten.

A felhők használata egyre nagyobb mértékben terjed el nem csak a magánéletben, de az üzleti szférában is. Ezek használatáról számos előny és hátrány sorolható fel, de ezek részletes nem ezen írás céljai. Sokszor nem is gondoljuk, hogy valójában felhőt használunk, azonban a Facebook, a Gmail és sok egyéb szolgáltatás gyakorlatilag felhőként funkcionál, azáltal, hogy képeinket feltöltjük, dokumentumokat küldünk rajtuk keresztül. Amikor a Google elindította Drive nevű felhőszolgáltatását, elég nagy botrányt okozott, hogy a felhasználási feltételekben az a kitétel szerepelt, hogy a felhasználó lemond a feltöltött fileokról, és a Google szabadon felhasználja céljaira. Természetesen a botrány hatására ezt kivették a felhasználási feltételek közül, elírásként hivatkozva rá. Azt gondolom, nem kell különösen magyarázni, milyen kockázatai vannak, ha valakik hozzájutnak a felhőben tárolt adatainkhoz- gondoljunk csak a jelszavak kezelésével kapcsolatos részre.

Összegzés

A tanulmány célja nem volt más, mint felhívni a figyelmet a közösségi média veszélyeire, amit a kiberbűnözés jelent. Bár számos területet érintettem, ez azonban még így is erős szűkítést jelent, különösen, hogy terjedelmi korlátok nem tették lehetővé egyes témák bővebb kifejtését (pl. a terrorizmus egy külön tanulmányt megérdemelne).

Az ismertetett területek ellen sok esetben védekezhetünk, és így sokkal kevésbé vagyunk kitéve a veszélyeknek. Ehhez azonban ismernünk kell azokat a kockázatokat, hogy megfelelő módon használjuk a közösségi oldalakat. Őszintén remélem, e tanulmány egy olyan gondolatébresztőként szolgál, amely biztonságosabb és tudatosabb internet és közösségi média használatra sarkalja a tisztelt Olvasót!

Felhasznált irodalom

- Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe, In. Nemzetbiztonsági Szemle (Online) 2015., III:(2) pp.
- Bányász Péter, Orbók Ákos: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében, In. Hadtudomány: A Magyar Hadtudományi Társaság Folyóirata XXIII:(1 elektronikus) (2013)
- Bányász Péter: Spies Act As A Spy: The Edward Snowden Case, In: Milan SOPÓCI, Mária PETRUFOVÁ, Miroslav ŠKOLNÍK, Viera FRIANOVÁ, Jaroslav NEKORANEC, Lubomír BELAN JIRÁSKOVÁ, Milota KUSTROVÁ, Stanislav MORONG (szerk.), Manažment - teória, výučba a prax 2014: zborník príspevkov z medzinárodnej vedecko-odbornej konferencie.
- Bertók Zsófia: Szteganográfia, http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2010/HF-reports/BertokZsofia.pdf
- Deák Veronika: A social engineering humán alapú támadási technikái, In. Biztonságpolitika, 2017. április 10., http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-social-engineering-human-alapu-tamadasi-technikai
- Deák Veronika: A számítógép alapú social engineer támadási technikák, In. Biztonságpolitikai, 2017. április 28., http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-szamitogep-alapu-social-engineering-tamadasi-technikai
- Dobák Imre: Technikai típusú információgyűjtés a változó biztonsági kihívások tükrében, In. Hadmérnök, XII. évfolyam 2. szám, 2017. június,
- Europol The Internet Organised Crime Threat Assesment 2016., Europol, Hága, 2016., https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016
  Gyaraki Réka: A nyomozóhatóság és a katasztrófavédelem feladata a kiberbűncselekmények vonatkozásában, In. Szakmai Szemle (megjelenés alatt)
- Gyaraki Réka, Simon Béla: Biztonsági események rendészeti szempontból – a kiberbűncselekmények kezelése, In. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2017, Nemzeti Közszolgálati Egyetem, Budapest, 2017.

- Haig Zsolt: Információ- Társadalom- Biztonság, NKE Szolgáltató Kft., Budapest, 2015.
- Kiss Tibor: Gyűlölet-bűncselekmények és szélsőséges csoportok az információs társadalomban, In. Prazsák Gergő (szerk.) Nemzeti szempont. Budapest: Apeiron Kiadó, 2014.
- Kiss Tibor, Parti Katalin: A mém vajon mi? Mémekért való felelősség megállapíthatóságának kérdései és lehetőségei, In. Infokommunikáció és Jog 2016/2, 2017
- Kiss Tibor, Parti Katalin: Informatikai bűnözés, In. Borbíró Andrea, Gönczöl Katalin, Kerezsi Klára, Lévay Miklós (szerk.) Kriminológia.. Budapest: Wolters Kluwer, 2016.
- KEMP, Simon: Digital in 2017- Global overview, We are social, 2017. január 24., https://wearesocial.com/special-reports/digital-in-2017-global-overview
- Kovács László, Krasznay Csaba: A digital Mohács: a cyber attack scenario against Hungary, In. Nemzet És Biztonság: Biztonságpolitikai Szemle III:(Spec. Issue Winter)
- Krasznay Csaba: A polgárok védelme egy kiberkonfliktusban, In. Hadmérnök, 2012, VII:(4)
- Krasznay Csaba- Simon Béla: Kiberbűncselekmények az online kereskedelemben, In. Hadmérnök XII. Évfolyam KÖFOP különszám - 2017.
- Marinov: Migránstámadás a Bazilikánál? In. UrbanLegends, 2016. február, http://www.urbanlegends.hu/2016/02/migranstamadas-a-bazilikanal/
- NMHH: Lakossági internethasználat- Online piackutatás 2016., Ariosz Kft., NRC Kft., In. Nemzeti Média- és Hírközlő Hatóság, http://nmhh.hu/dokumentum/187704/lakossagi_internethasznalat_2016.pdf
- Several cybersecurity to protect your account in the social networking http://www.wired.com/wp-content/uploads/2015/11/ISIS-OPSEC-Guide.pdf
- Simon Béla: Bűnüldözés előtt álló digitális kihívások, In Magyar Rendészet (megjelenés alatt)
- WordWideWebSize, In. http://www.worldwidewebsize.com/.
- Zetter, Kim: Security Manual Reveals the OPSEC Advice ISIS Gives Recruits, In: Wired, 2015. november 19., http://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/