DOI:10.37372/mrttvpt.2019.1.1

Bányász Péter – Bóta Bettina – Csaba Zágon: A social engineering jelentette veszélyek napjainkban

Absztrakt

A social engineering angol nyelvterületről származó fogalom napjaink kiberbűnözéséhez köthető népszerű támadási forma. Ennek során a bűnözők az információbiztonságot nem, vagy csak nagyon kevéssé ismerő, vakon együttműködő személyektől szereznek információt. Ezek az értesülések később gyakran védett rendszerekhez történő hozzáférés kulcsaként szolgálnak, vagy csak egyszerűen megkönnyítik a jogtalan hozzáférést. A social engnineering jelensége nem egyszerűen a nemzeti büntetőtörvényekből indul ki, hanem inkább csak több elkövetési módszert, azaz modus operandit foglal magába. Ezek közös jellemzője, hogy a két mozzanatos cselekmény során az elkövetők főként megtévesztéssel, ritkán nyomás gyakorlásával (pszichikai erőszakkal), esetleg ezek kombinációjával, de sohasem fizikai erőszakkal először hozzájutnak a második mozzanat elkövetéséhez szükséges, vagy azt megkönnyítő információkhoz, majd ezeket a cselekmény második mozzanatánál alkalmazzák jogtalan előnyök megszerzése érdekében. A cikk szerzői tudománymetriai vizsgálat keretében elemzik a fogalom eredetét, annak tudományközi kapcsolatait, amelyeket elengedhetetlenül szükségesnek tartanak a mai értelmezéshez. Az ismertté vált esetek alapján felvázolható főbb trendek alapján a szerzők napjainkban megtörtént konkrét példán keresztül igyekeznek bemutatni a jelenséget és felhívni a figyelmet a veszélyekre, a megelőzés terén pedig és az adat- és információbiztonsági tudatosság jelentőségére. A tanulmány zárásaként megvizsgáljuk azokat a személyiséghez kapcsolódó tényezőket, amelyek befolyásolhatják az információbiztonsági tudatosságot.

Abstract

Social engineering, an English-language concept, become a very popular method of our days' cybercrime, where criminals obtain information from blindly cooperating individuals having no, or very little awareness of information security. This information often serves later as a key to protected systems or simply makes ease breaching into them. The phenomenon of social engineering is not purely based on national criminal laws, but rather includes several modi operandi. A common feature of these two-phase acts is that the perpetrators obtaining primary information necessary or facilitating the second act to receive illicit benefits, mainly by deception, rarely by pressure (psychological violence), or possibly by a combination of these, but never by physical violence. The authors examined the origin of the concept of social engineering and its interdisciplinary relationships in the context of a scientometric analysis, which is considered essential for a proper interpretation in our time. Based on the major trends outlined from the known cases, the authors present the phenomenon and raise awareness on the dangers through a current example, and the importance of information security awareness in the prevention. At the closure of this study, we examined personality-related factors that may influence information security awareness.

***

1. Bevezetés

A 21. században az internet elterjedése lebontotta a földrajzi határokat. Az internet az összes társadalmi alrendszerben paradigmaváltáshoz vezetett. Nem túlzás kijelenteni, hogy az internet hiányában a ma ismert társadalom fenntarthatatlanná válna. Ennek ellenére még mindig az internet forradalma előtt állunk, a „dolgok internetének" várható elterjedésével a kibertértől való kitettségünk jelentősen növekedni fog. Hamarosan minden fűszálnak IP címe[1] lesz, szokták mondani humorosan, de ez a megjegyzés rávilágít az okos város koncepciója[2] mögött felsejlő jövőképre. Az emberiség népességszámának növekedésével, illetve azok egyre inkább a rurális terekből a városokba történő mozgásával az emberi élet minőségének, a társadalom működésének megőrzése elkerülhetetlen cél lesz, amennyiben a városszervezés nem a lehető a leghatékonyabb megoldások alkalmazásával működik. Mindez a mindenütt megjelenő infokommunikációs technológiák, a nagy adattömegek elemzése, az ún. „big data", és a mesterséges intelligencia fejlődésével kihívások elé állítja a társadalmakat és azon belül az egyéneket is.

Az infokommunikációs technológiákkal szembeni kockázati kitettségünk napjainkban is rendkívüli problémának tűnik. Sokszor naponta értesülünk olyan típusú sérülékenységekről, támadásokról, amelyek alapvetően írják át a biztonságról alkotott ismereteinket. Elég csak a két paradigmaváltó támadásra gondolni, a 2013-ban az Edward Snowden által nyilvánosságra hozott dokumentumokra[3], amelyek többek között a magánszféra létével, minőségével kapcsolatban kérdőjelezett meg számos dolgot, vagy az iráni natanzi nukleáris létesítmény ellen elkövetett kibertámadásra a Stuxnet vírus segítségével, ami egyes szerzők[4] szerint évekkel vetette vissza az iráni nukleáris kutatásokat.[5]

A kibertámadások számával kapcsolatos trendek az utóbbi időszakban folyamatos emelkedést mutatnak, azonban fontos látni, hogy ezek sokkal nagyobb számban történnek meg, mint amiről egyáltalán ismeretekkel rendelkezünk. Ennek egyik oka, hogy maguk a támadások is egyre kifinomultabbak, például az említett Stuxnet vírus évekig rejtőzködött, mire sikerült azonosítani. Talán ennél is fontosabb azonban, hogy sokszor maguk a felhasználók nem is veszik észre, hogy támadás áldozatai. Ennek okaként elsősorban a biztonságtudatosság hiányát, a digitális írástudatlanságot azonosíthatjuk. Mint a későbbiekben látni fogjuk, az internetezőknek számtalan támadástípus ellen kell védekeznie, amelyek nagy részét kellő biztonságtudatossággal jelentős mértékben ki lehet szűrni. Ennek azonban feltétele, hogy a felhasználó ismerje azokat a kockázatokat, fenyegetettségeket, amelyek őt is érinthetik. Remélhetőleg, tanulmányunk ebben fontos szerepet tölt majd be.

---

[1] Az IP cím angol nyelvű Internet Protocol address rövidítésből elterjedt és ma általánosan alkalmazott fogalom, amely meghatározza egy internetes hálózatba kapcsolt számítógép (intelligens eszköz) eléréséhez szükséges digitális címet.

[2] SALLAI Gyula: *Az okos város koncepciója.* In: SALLAI Gyula (szerk.) Az okos város (Smart City). Dialóg Campus Kiadó, Bp., 2018. pp. 13-34.

[3] GREENWALD, Glenn: *A Snowden-ügy - Korunk legnagyobb nemzetbiztonsági botránya*. HVG Könyvek Kiadó, Bp., 2014.

[4] Lásd például GYURÁK Gábor: *Kritikus infrastruktúrák védelme hálózati behatolásjelző rendszerekkel.* Hadmérnök, 2015/2 szám, pp. 223-233. vagy CSERHÁTI András: A Stuxnet vírus és az iráni atomprogram. Fizikai Szemle 2011/5. pp. 150-155.

[5] SINGER, Peter W., FRIEDMAN, Allen: *Cybersecurity and Cyberwar - What Everyone Needs to Know.* Oxford University Press, Oxford, 2014. pp. 114-120.

2. Tudománymetriai vizsgálat

Tanulmányunk alapját a social engineering tudománymetriai vizsgálata jelenti. A social engineering egy olyan támadásforma, amely során a támadó először a kihasználható emberi tulajdonságokkal [6] él vissza, hogy ily módon férjen hozzá megtévesztéssel, zsarolással a védett információkhoz, illetve rendszerekhez. A téma ismert szakértője, Kevin David Mitnick szerint a social engineering a befolyásolás és rábeszélés eszközével operál. Megtéveszti az embereket, manipulálja vagy egyszerűen meggyőzi őket, hogy az alkalmazó szándéka tényleg az, mint aminek azt feltünteti. Ennek eredményeként pedig a „social engineer” vagyis maga az alkalmazó személy – információs technológiák használatával vagy akár anélkül – képes az embereket információszerzés érdekében kihasználni.[7]

A social engineeringnek, talán a fogalom komplexitásából is fakadóan, jelenleg nincs általánosan elfogadott magyar megfelelője. A leggyakrabban a pszichológiai manipulációként szokták fordítani, amely a fogalom társadalomtudományi eredetére utal. Jelen cikk korlátai nem teszik lehetővé, hogy a fogalmat a maga komplexitásában kielégítően elemezzük, ugyanis ez a szerzők megítélése szerint egy önálló tanulmányt igényel.

Kutatásunk első lépéseként megvizsgáltuk a social engineering keresőkifejezés megjelenését a releváns nemzetközi szakirodalomban. Ehhez az Elsevier gondozásában levő Scopus adatbázist hívtuk segítségül, ami a tudományos közlemények legnagyobb adatbázisa, ahol nem csak az ott indexált közleményeket, hanem azok metaadatait[8] is kereshettük. 2017-ben 69 millió rekordot, ezekhez mintegy 70 ezer hozzárendelt intézményt és 12 millió személyes szerzői profilt tartalmazott a Scopus. Az adatbázisban több, mint 5000 kiadó által gondozott közlemény lett indexálva, melyek közt 24 ezer folyóirat és 150 ezer könyv volt bejegyezve. Az adatbázisban kezelt rekordok száma évente folyamatosan növekszik.[9]

A social engineering kifejezést a keresés során idézőjelek között adtuk meg annak érdekében, hogy a keresőmotor értelmezze a két szó közti kapcsolatot. Ez alapján 1898 közleményt kaptunk, amit az összehasonlítás érdekében leszűkítettünk Magyarországra [10] is, ahol összesen csak 8 publikációra találtunk. Az adatbázisban 2020-ig terjedően szerepelnek közlemények. [11] A közlemények évek szerinti megjelenését az 1. számú ábra tartalmazza az utolsó teljes évig, azaz 2018-ig bezárólag.

---

[6] Naivitás, hiszékenység, segítségnyújtás, kíváncsiság, biztonságtudatosság hiánya, figyelmetlenség, szexualitás stb.

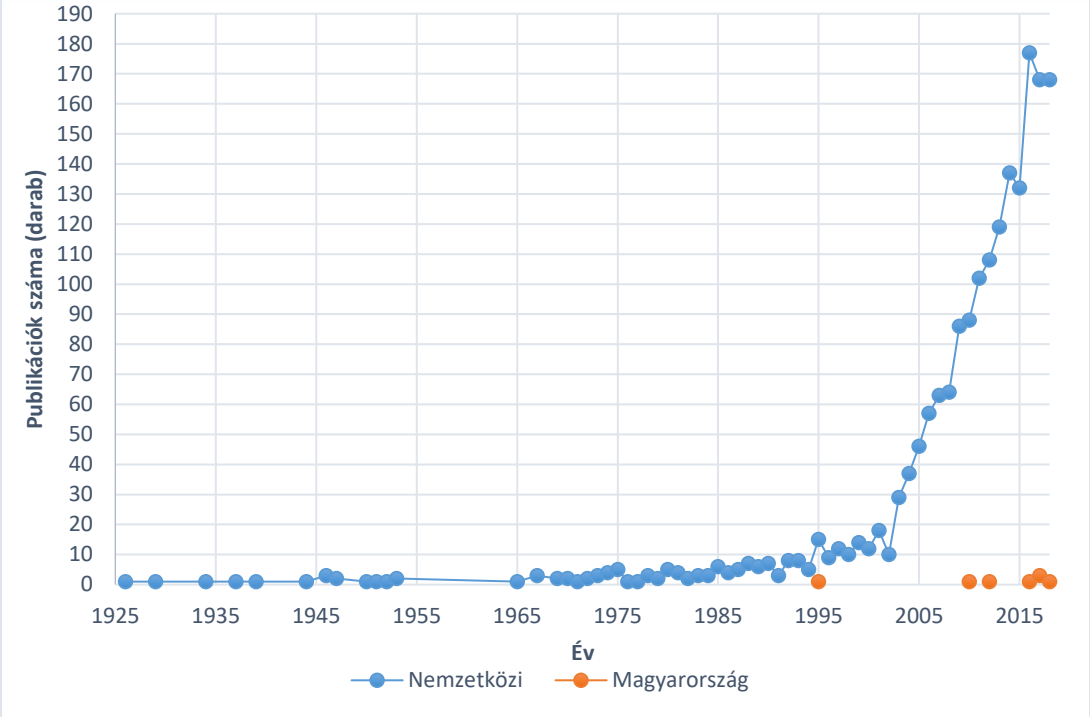
[7] MITNICK, Kevin David*: A legendás hacker - A megtévesztés művészete*. Perfact Kiadó, Bp., 2003. p. 1.

[8] A közlemények metaadatainak számít például a cím, a szerző, a szerző affiliációja, a közleményben hivatkozott publikációk, ezek száma stb.

[9] URBANOVICS Anna - SASVÁRI Péter: *A tudományos kutatás elixírje*. Working Paper, 2019. július, DOI: 10.13140/RG.2.2.26344.83204

[10] Ez alatt azt érjük, ha a szerző, a szerző intézménye, a tudományos kiadvány Magyarországhoz köthető.

[11] Ennek oka, hogy a még nem publikált, de közlésre befogadott közlemények is megjelennek.



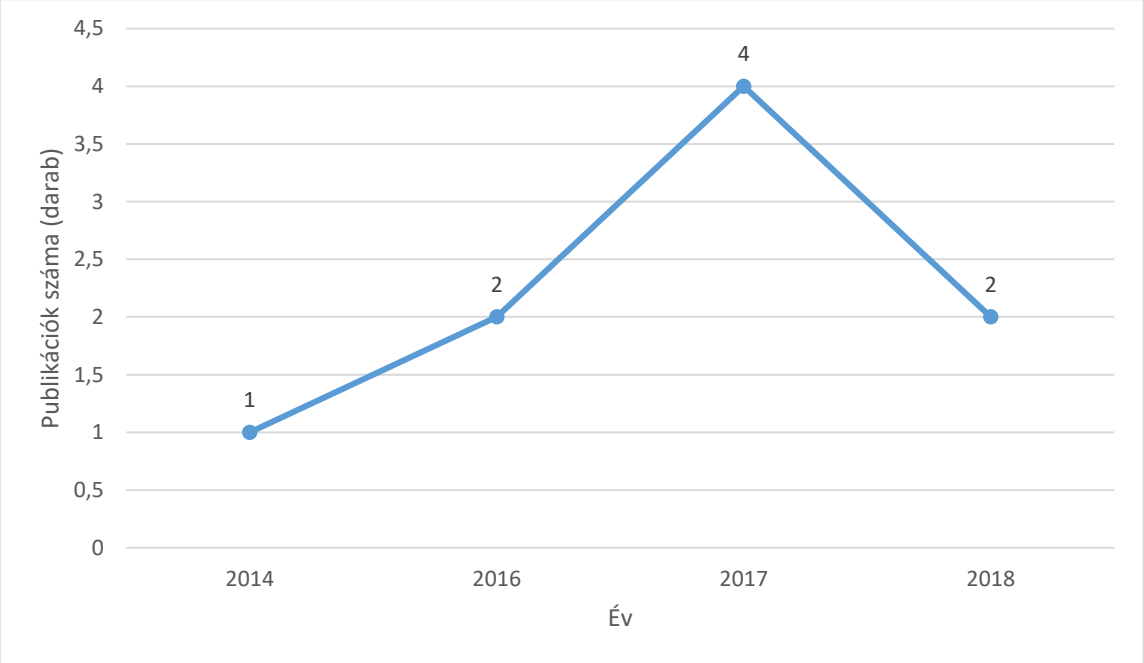
1. ábra: A „social engineering" keresőkifejezés megjelenése a nemzetközi tudományos publikációkban 1925-2018 között (Saját szerkesztés, forrás: Scopus)

Mint az ábrán is látható, a kifejezés először 1925-ben jelent meg Scopus által indexált nemzetközi szakirodalomban, azonban a kifejezés először 1842-ben tűnt fel John Gray brit közgazdász An Efficient Remedy for the Distress of Nations című könyvében.[12] A kifejezés szociológiai, később politológiai használata az emberek csoportjainak, vagy akár a társadalomnak tervszerű (előre eltervezett) megváltoztatási szándékára utal.[13] Ez alatt azt kell érteni, hogy bizonyos hatalmi csoportosulások, akik saját érdekeiknek megfelelően meg kívánják változtatni emberek közötti kapcsolatokat, számítaniuk kell azok ellenállására. Az ellenállás leküzdése érdekében tervszerűen tévesztik meg a kiválasztott célcsoportot. Az angol terminus technicus „engineering", azaz „mérnöki tevékenység"eleme ebből származik, azonban itt nem a klasszikus értelemben vett építőanyag felhasználásával terveznek, hanem a „social", vagyis a társadalom tagjai lesznek az „építőelemek". A fogalom társadalomtudományi értelmezésében a cél eléréséhez a megtévesztés mellett megengedett a fizikai erőszak alkalmazása is. A social engineeringnek ez a fajta megközelítése a hadtudomány területéről ismerős lélektani műveletek tartalmához hasonlít, azonban ez utóbbinál a fizikai erőszak még eshetőlegesség szintjén sem megengedett. A fogalom evolúciójából fakad, mint ahogy később látni fogjuk, hogy a social engineering egyre több tudományterületen nyer értelmezést. A fogalom értelmezése a társadalom befolyásolása mellett egyre nagyobb arányban az egyén befolyásolása jelenik meg célként, amely visszavezet a fentebb hivatkozott és Kevin David Mitnick által levezetett gondolatokhoz[14].

[12]HATFIELD, Joseph M.: *Social engineering in cybersecurity: The evolution of a concept.Computers & Security* 73, 2018. pp. 102-113. https://doi.org/10.1016/j.cose.2017.10.008
[13]ALEXANDER, Jon, SCHMIDT, Joachim K. H. W.: *Social engineering: Genealogy of a concept*. In. PODGÓRECKI, Adam et al. (eds.) Social Engineering. Carleton University Press, Ottawa, 1996. p. 1.
[14]MITNICK: i. m. 2003.

Megvizsgáltuk a fogalmat a Magyar Tudományos Művek Tárában (MTMT) is, ami a tudományos művek legfontosabb magyarországi gyűjteménye, hitelesnek tekinthető adatbázisa, ahová ellenőrzött módon tölthetők fel a részt vevő intézmények kutatóinak tudományos munkásságát és teljesítményét jellemző adatok. A tudományos közleményeket tartalmazó nemzeti bibliográfiai adatbázis kötelezően feltünteti a költségvetési szerveknél foglalkoztatottak jogviszonyuk keretén belül megalkotott és megjelentetett tudományos publikációinak, valamint azoknak a tudományos munkáknak a metaadatait (címét, első megjelenési helyét, a szerző és a tudományos közlemény felett rendelkezni jogosult nevét, illetve megjelenését), amelyek írásakor szerzőjük tudományos mű létrehozására irányuló, a költségvetésből származó támogatásban részesült.[15]

Az MTMT továbbfejlesztett változatában lehetőség nyílik a rögzített közlemények címében is keresni, amely során összesen 9 közleményt azonosítottunk 2014 és 2018 közötti időszakra vonatkozóan (ezek megoszlását lásd a 2. számú ábrán).



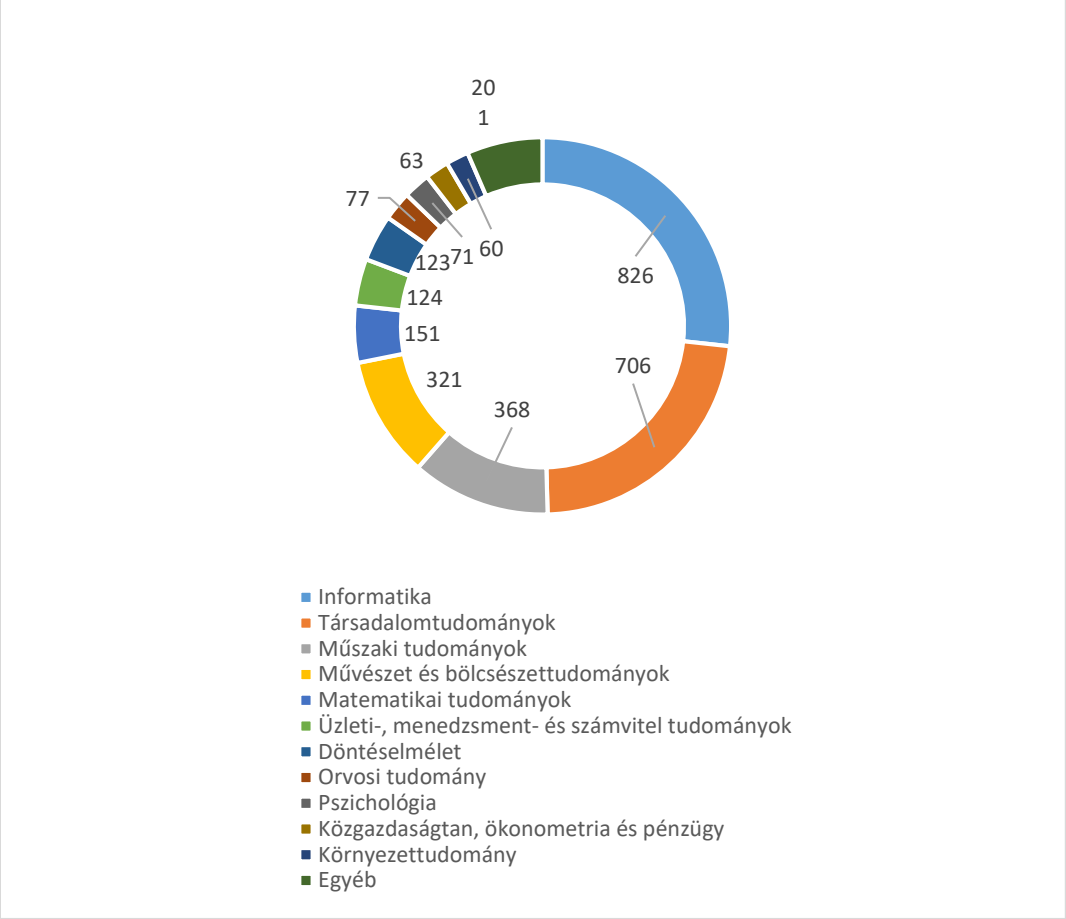
2. ábra: A "social engineering" keresőkifejezés előfordulása a Magyar Tudományos Művek Tára adatbázisban nyilvántartott tudományos közlemények címében (Saját szerkesztés, forrás: MTMT)

A 9 közlemény összesen 11 szerzőhöz köthető, amelyek esetében 3 szerző írt 2-2 közleményt, azonban ezek egyike sem Scopus által indexált. Ezek mindegyike az információbiztonsági, illetve a fogalom kriminalisztikai értelmezési köréhez kapcsolódnak.

A fogalom elterjedésével egyre több tudományterület esetében vált releváns kutatási témává (lásd 3. számú ábra). Fontos megjegyezni, hogy a közlemények egyszerre több tudományterületet is érinthetnek, ahogy erre a korábban idézett Hatfield tanulmány [16] is példával szolgál. A közlemény a Computer and Security nevű, mértékadó brit tudományos lapban jelent meg, amely az Informatika és

[15] 1994. évi XL. törvény a Magyar Tudományos Akadémiáról.
[16] HATFIELD: i. m. 2018.

Társadalomtudományok tudományterületeit érintő tudományos közlemények számára egyaránt relevánsnak tekinthető. Ez jól rávilágít a téma inter- és multidiszciplinaritására.

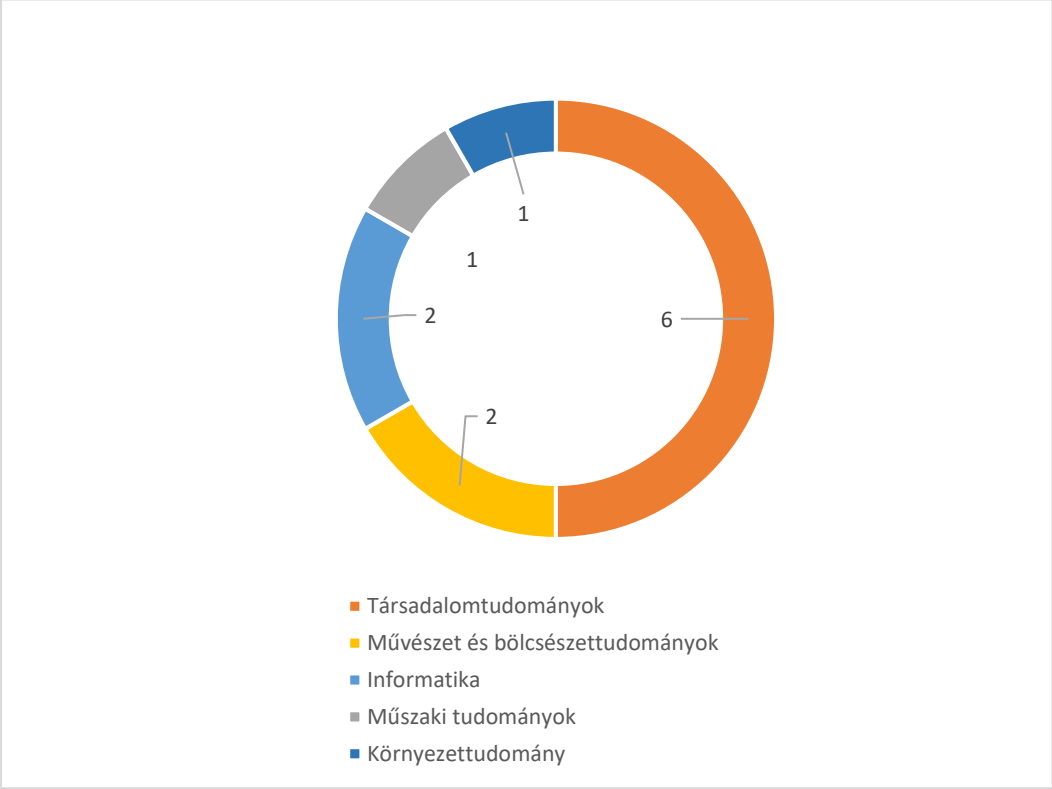


3. ábra: A "social engineering" keresőkifejezés megoszlása tudományterületenként (Saját szerkesztés, forrás: Scopus)

Az általunk vizsgált nemzetközi adatbázisban eltérés figyelhető meg a Magyar Tudományos Akadémia (MTA) által meghatározott tudományterületi nómenklatúrához képest. Míg a nemzetközi tudományos világban 27 tudományterületet azonosítanak, addig az MTA a 2016-ban felülvizsgálta az általa korábban alkalmazott tudományági besorolását, és egy hármas szintű osztályozást vezetett be, amelyben 3 tudományterületet határozott meg. Az elemzés során mi a nemzetközi nómenklatúrát vettük figyelembe, hogy elkerüljük az egyes területek átsorolásából, illetve egymásnak megfeleltetéséből következő módszertani kockázatokat. Ennek fontosságát talán a „Computer Science" szemlélteti leginkább, amely amíg a nemzetközi tudományos világban önálló tudományterületként jelenik meg, amelyhez 12 tudományág kötődik. Az MTA nómenklatúrájában viszont ugyanez leginkább a „Természettudományok és matematika" tudományterület „Műszaki tudományok" tudomány-részterületen belül található „Informatika" tudományághoz lehetne besorolni.

Az általunk vizsgált 1898 közlemény tartalma szerint összesen 3091 tudományterületre sorolható. A Pareto-eloszlást figyelembe véve megállapíthatjuk, hogy a releváns tudományterületek közül már az első hat kiteszi ezek 80%-át, ezért a közlemények tudománymetriai súlypontja az informatika (26,72%), a társadalomtudományok (22,84%), a műszaki tudományok (11,91%), a művészet és bölcsészettudományok (10,38%), a matematikai tudományok (4,89%) és az üzleti-, menedzsment- és számvitel tudományok (4,01%) lettek.

Érdemes megvizsgálni a Magyarországhoz köthető közlemények tudományterületi megoszlását is (lásd 4. számú ábra).



4. ábra: A "social engineering" keresőkifejezés megoszlása tudományterületenként Magyarországon (Saját szerkesztés, forrás: Scopus)

Bár ez esetben jelentősen kevesebb közleményt vizsgálhatunk, de látható, hogy a publikált közlemények illeszkednek a nemzetközi trendekbe. Itt is a társadalomtudományok, a művészet és bölcsészettudományok, illetve az informatika adja a közlemények súlypontját.

Megítélésünk szerint külön kutatást érdemel, hogy a social engineering fogalom evolúciója mely tudományterületekre helyez súlypontot, illetve hogyan változott a téma tudományos feldolgozása az egyes diszciplinákon belül.

Vizsgálatunk következő fázisában a SciValt adatbázist használtuk. Ez az Elsevier kutatást támogató programja keretében működik, és a Scopus citációs adatbázis valamint a ScienceDirect teljes szöveges adatbázis adatain alapul. A SciValt ezekre építi saját elemzési szolgáltatásait a Big Data és üzleti analitikai eszközök segítségével. Jelenleg több mint 10 ezer kutatási és felsőoktatási intézmény tudományos tevékenységeinek adatait, legfontosabb kutatási témáit, partneri viszonyait és kutatás támogatásait gyűjti össze[17] és teszi elemezhetővé az előfizetői számára. A SciVal segítségével sajnos nincs mód arra, hogy mind az 1898 közleményt vizsgáljuk, mert az csupán az elmúlt 10 év elemzését teszi lehetővé. Ily módon a 2009 és a 2018 közötti időszakra eső 1350 közleményt elemezhettük a leggyakrabban előforduló 50 kulcsszó alapján (lásd 5. számú ábra). Emögött az a feltételezésünk állt, hogy minél gyakrabban jelenik meg egy kulcsszó a közleményekben, ez annál meghatározóbb módon azonosítja a social engineering fogalom már ismert kutatási irányait.

[17] URBANOVICS – SASVÁRI: i. m. 2019.

5. ábra: A "social engineering" keresőkifejezéshez köthető leggyakoribb 50 kulcsszava (Forrás: SciVal)

Az 5. számú ábrán látható szófelhőben minél nagyobb betűmérettel szerepel egy kulcsszó, az annál gyakrabban jelenik meg az egyes közleményekben. A szófelhő lehetővé teszi azt is, hogy megadott időintervallumban vizsgáljuk, milyen trendek jellemezték az egyes kulcsszavak megjelenését. Az ábrán első ránézésre visszaköszönnek az informatika tudományterülethez sorolható, informatikai biztonsági kifejezések. Az eddigi elemzésből (3. számú ábra) nem volt azonban ilyen markánsan látható, hogy a fogalom értelmezései közt olyan kutatási szakterületek is megjelennek, amelyeket a bűnügyi tudományok területére sorolhatunk, függetlenül attól, hogy a nemzetközi nómenklatúrában elkülönítenek-e. A nemzetközi tudománymetriai elemzésünk által talált második leggyakoribb tudományterület a társadalomtudományok voltak. E kategórián belül található jogtudományok nyilvánvalóan jórészt lefedik azokat a témákat, amelyeket a bűnügyi tudományokhoz sorolhatók.

Vizsgálatunkat 2 kulcsszóra szűkítettük, „Crime", mint bűnözés, és „Computer Crime", mint számítógépes bűnözés. Ennek oka, hogy ez a két kulcsszó egyértelműen a bűnügyi tudományokhoz köthető.[18]

A két kulcsszó relevanciáját az 1. számú táblázatban ábrázoltuk, ahol 2009-et vettük bázisévnek.

1. táblázat: "Számítógépes bűnözés" és "Bűnözés" kulcsszavak relevanciája 2009-2018 között a nemzetközi tudományos közleményekben (Saját szerkesztés, forrás: SciVal)

Kulcsszó	Relevancia	Növekedés (%)
Számítógépes bűnözés	0,61	275
Bűnözés	0,33	175

A kulcsszó relevanciáját az előfordulás gyakorisága adja, amelynek maximális értéke 1,00 lehet. A növekedés a tudományos eredmény növekedésére vonatkozik, az értéke pedig azt jelzi, hogy 2009 és 2018 között hány százalékkal növekedett a kulcsszó előfordulásának gyakorisága a tudományos közleményekben.

[18] Természetesen a többi esetében is lehet kapcsolat a bűnügyi tudományokkal. A hálózatba való behatolás például bűncselekmény, de a kifejezésből nem egyértelmű, hogy azt bűnügyi megközelítésben használják.

2.1. A leggyengébb láncszem

A kibertérből érkező támadásokat a szakirodalom motivációk alapján öt csoportba sorolja.[19] Ez alapján beszélhetünk:

- kiberbűnözésről,
- hacktivizmusról,
- kiberterrorizmusról,
- kiberkémkedésről és
- kiberhadviseléről.

A kiberbűnözés célja – értelemszerűen – informatikai eszközök segítségével az anyagi haszonszerzés. A hacktivizmus internetes aktivizmust jelent, tehát valamilyen politikai cél megvalósítását. A hacktivisták célja az információhoz való szabad, egyenlő hozzáférés, még akkor is, ha az esetleg mások titokvédelmi céljai, gyakran nemzetbiztonsági érdekei ellen történik. A kiberterroristák célja, hogy az információs rendszerek megzavarásával, lerombolásával hatást gyakoroljanak szolgáltatások működésére, rontsák a lakosság biztonságérzetét és ezeken keresztül nagyobb láthatóságot biztosítsanak ügyüknek. Terrista szervezetek jelenleg nem rendelkeznek azzal a képességel, amellyel súlyos következményekkel járó kibertámadás elkövetésére lennének képesek, ettől függetlenül számtalan módon használják az internetet.[20] Kiberkémkedés alatt az államok, piaci szereplők, de akár magánszemélyek informatikai eszközök útján végzett hírszerző tevékenységét értük.[21] A kiberhadviselés pedig államok, állami szintet el nem érő entitások közti konfliktusokban jelenik meg, amelynek során a konvencionális hadviselés támogatására (vagy akár kiváltására) az ellenfél információs rendszereinek működésképtelenné tételére törekszenek.[22] A bejelentett támadásokról szóló jelentésekben a leggyakoribb támadás motivációk alapján a kiberbűnözés, általában az összes támadás kétharmada ide sorolható.[23]

Fontos látni, hogy az egyes motivációk között átjárás lehet. Az észak-koreai nukleáris program sikerében fontos szerepe volt az észak-koreai hackereknek, akik sok esetben kiberbűnözőként is tevékenykedtek. A 2016-os amerikai elnökválasztás esetében pedig orosz titkosszolgálati kötődésű hackercsoportok, mint a Cozy Bear és Fancy Bear, hatoltak be amerikai információs rendszerekbe. Az onnan szerzett információkat átadták a hacktivista Julien Assangenak, amelyek kiszivárogva, elemzők szerint fontos szerephez jutottak Donald Trump elnökké választásában.[24] Nem nehéz elképzelni olyan forgatókönyvet, ahol kiberbűnözésből származó pénzből vásárolnak szolgáltatásokat, illetve bizonyos képességet[25] a Darkneten, amelyeket végül terroristák

---

[19] KRASZNAY Csaba: *A polgárok védelme egy kiberkonfliktusban*.Hadmérnök, 2012/4. szám. pp. 142-151.

[20] Többek között propagandára, konspirált kapcsolattartásra, hírszerzésre stb. – Lásd például: RITECZ György: *A terrorizmus és a migráció viszonya a számok alapján.*Acta Humana, 2016/5. pp. 113-123:119.

[21] THOMSON, Jim R.: *Cyber Security, Cyber-attack and Cyber-espionage. In. High Integrity Systems and Safety Management in Hazardous Industries*. Elsevier B. V., Amsterdam, 2015. pp. 45-53.

[22] ROBINSON, Michael et al.: *Cyber warfare: Issues and challenges*. Computers & Security. 2015/49. pp. 70-94.

[23] Ezzel kapcsolatban a www.hackmageddon.com honlap statisztikái irányadóak.

[24] KOVÁCS László, KRASZNAY Csaba: *„Mert övék a hatalom”: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során*. In. SVKK elemzések, 2017/9. pp. 1-11.

[25] Az Europol Súlyos és Szervezett Bűnözés Fenyegetettség Értékelése 2017 című jelentés nyilvános változata beszámol a szakértő bűnözők jelenségéről. Ezek a személyek különleges szakismereteiket, technológiai képességeiket elsősorban a csúcstechnológiai bűnözés területére vonatkozóan, mint igénybe vehető szolgáltatást hirdetik. Szakértelmükre fizetőképes kereslet jelentkezése esetén kapcsolódnak

kritikus infrastruktúrát érintő támadáshoz használnak fel. Az említett példák felhívják a figyelmet az állami és nem állami célok közötti határok elmosódására, de épp így lehetséges a szervezett bűnözés és a terrorista csoportok közötti alkalomszerű, vagy folytatólagos együttműködésre is.

Fentieket figyelembe véve látható, hogy a kiberbiztonság egy rendkívül komplex, számos terület (köztük politikai, műszaki, gazdasági, jogi, oktatási stb.), illetve az állami és piaci szereplők állandó kooperációját megkívánó folyamat. Az informatikai biztonság egy informatikai rendszer olyan állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg.[26] Célja, hogy az információ megőrizze és fenntartsa a biztonsági tulajdonságait, az úgynevezett „CIA" hármasát, amiben alapján C, mint *confidentiality* a bizalmasságot, az I, mint *integrity* a sértetlenséget, valamint az A, mint *availability* a rendelkezésre állást jelenti. Ezzel szemben az információbiztonság egy folyamatot jelöl, aminek során megvédjük az információt a nem engedélyezett megzavarástól, hozzáféréstől, használattól, módosítástól, megsemmisítéstől, vagy kiszivárgástól. Az információbiztonságnak négy szintjét különböztetjük meg, ami a személyi, fizikai, adminisztratív és elektronikus információbiztonság.[27]

Mivel a szervezetek egyre fejlettebb fizikai, logikai védelmi megoldásokat alkalmaznak, így a támadóknak is változatos eljárásokat kell kidolgozniuk. Egy megfelelő fizikai, logikai védelemmel ellátott szervezet informatikai rendszerébe történő behatoláshoz fejlett informatikai tudásra, rengeteg időre van szükség, ha informatikai úton történik a támadás, ezért a támadók az esetek többségében úgynevezett social engineering támadásokhoz folyamodnak.[28]

2.2. A támadástípusok

A social engineering támadásokat e tanulmányban mi két csoportra bontjuk aszerint, hogy szemtől szemben vagy infokommunikációs technológia használatával történik-e a cselekmény megtévesztés mozzanata.[29] Az első kategóriát humán alapú támadásként azonosítjuk, amelyben számos eljárást, eszközt különböztethetünk meg. A humán alapú támadások esetében a támadóknak sokkal nehezebb dolga van, szemtől szemben kell megtévesztenie áldozatát, amire nem mindenki képes. Az infokommunikációs technológia (IT) alapú támadások esetében a támadók nem szemtől szemben tartják a kapcsolatot az áldozattal, itt viszont elengedhetetlen, hogy a támadó fejlett informatikai tudással rendelkezzen.[30]

---

különböző bűnszervezetekhez. [CaaS – Crime as a Service] vö. European Union Serious and Organised Crime Threat Assessment – Crime in the Age of Technology 2017. Public Version. Europol, The Hague, 2017. pp. 15., 28-29.

[26] MUNK Sándor: *Információbiztonság vs. informatikai biztonság*, Hadmérnök, 2007/különszám. pp. 1-21. http://hadmernok.hu/kulonszamok/robothadviseles7/munk_rw7.pdf

[27] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[28] SZÁDECZKY Tamás: *Risk Management of New Technologies.*Academic and Applied Research in Military and Public Management Science 15(3), 2016. pp. 279-290.

[29] Más szerzők más csoportosítási rendszert alkalmaznak, lásd például MOUTON, Francois et al.: *Social engineering attack examples, templates and scenarios*. Computers & Security, 2016/59. pp. 186-209.

[30] Természetesen kisebb támadások esetében használhatóak különböző eszközök és szolgáltatások, amelyeket fix összegért vásárolhat meg a gyengébb informatikai tudással rendelkező támadó, de ezek többségében korlátozottan működnek, például jelszavak feltörésére.

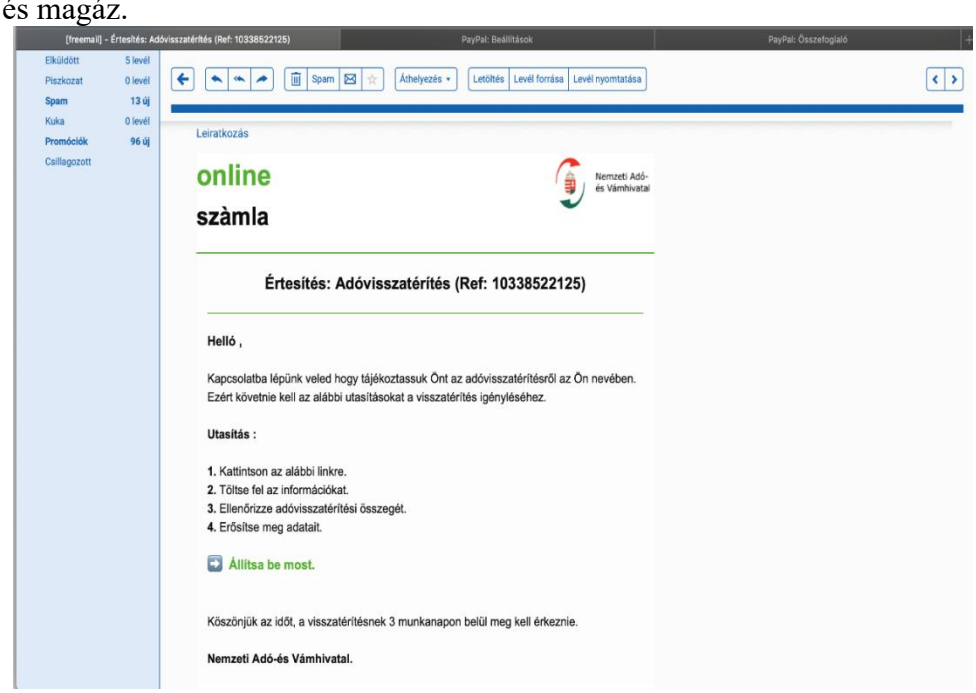
A humán alapú támadások körébe soroljuk többek között a(z):

- segítségkérést,
- segítségnyújtást,
- identitás lopást, álruhába bújást,
- épületbe való bejutást,
- „sírkő” lopást, amelynek során egy szervezetnél már nem dolgozó, de a jogosultságot továbbra sem megszüntetett személy bőrébe bújnak,
- jelszavak kitalálása,
- kukabúvárkodást, amikor a szervezet, magánszemély szemétjét vizsgálják át,
- „*shoulder sourfinget*”, amikor a célszemély mögül lesik ki a jelszavait, azonosítóit stb.

Az IT alapú támadásokat négy fő kategóriára oszthatjuk. Ezek a(z)

- adathalászat,
- kártékony programok,
- alkalmazásengedélyek,
- wi-fi alapú támadások.

Az adathalászat a trendek alapján az egyik legkedveltebb támadásforma. Számos módon történhet, köztük e-mailben, sms-ben, hamis weboldalak, alkalmazások, játékszoftverek stb. segítségével. Gyakran könnyű kiszűrni az ilyen jellegű támadásokat például a helytelen nyelvtan, szokatlan nyelvi fordulatok, rossz helyesírás, értelmetlen mondatok, rossz minőségű logók, nem megszokott URL cím segítségével (lásd 6. számú ábra). Mint az ábrán is látható, már maga a megszólítás és az első mondat teljes egészében helytelen, hiszen egy valódi hatóság formális, hivatali stílusban ír és magyar nyelven sohasem alkalmaz „Helló” megszólítást. „Kapcsolatba lépünk veled hogy tájékoztassuk Önt az adóvisszatéritésről az Ön nevében.” (Sic.) mondat amellett, hogy értelmetlen, központozási hibáktól hemzseg, továbbá egy mondaton belül egyszerre tegez és magáz.



6. ábra Adathalász e-mail a NAV nevében az adóbevallás időszakában (saját szerkesztés, forrás: a szerzők e-mail fiókjaiba spontán beérkező üzenetek)

Ennek ellenére gyakran sikeresek ezek a támadások, hiszen az alacsony biztonságtudatosságú felhasználók, az egyre gyakoribb hivatali tájékoztatások és tudatosságnövelő kampányok ellenére, nem mindig ismerik fel a fenti jeleket, és a bűnelkövetői oldal sikerességhez elegendő csak néhány megtévesztett személy is. Ebben rejlik az ilyen típusú támadások veszélyessége, hiszen nehéz hatékonyan védekezni ellenük. Az adathalászat egy kifinomult formáját jelentik az úgynevezett „pharming" típusú támadások, amiket eltérítéses adathalászatként fordíthatunk. Ennek a lényege, hogy a támadók a DNS kiszolgálókat támadják, és a valódi URL cím helyett egy általuk létrehozott hamis URL-re irányítják a gyanútlan felhasználót. Amennyiben a támadók pontosan lemásolják az adott oldal felületét, már pedig szofisztikált támadás esetén a fentebb írt jellemzőkre gondosan ügyelnek, rendkívül nehéz kiszűrni, hogy adathalász oldalon, vagy a keresett szolgáltatás valódi címén vagyunk-e.

A kártékony programok, a malwarek különböző módon próbálnak a felhasználók informatikai rendszerébe juttatni. Ilyen lehet például, amikor arról tájékoztat a rendszerünk, hogy vírus fertőzés áldozatai lettünk, de a felajánlott vírusírtó, frissítés telepítésével megszabadulhatunk a kockázattól. A frissítések telepítése létfontosságú a rendszerek védelmét illetően, így a támadók értelemszerűen ezeken keresztül igyekeznek hozzáférést szerezni azokhoz, többségében csak frissítésnek álcázva a kártékony kódot. A felhasználók itt legtöbbször a saját hiszékenységüknek esnek áldozatul és közreműködnek abban, hogy a kártékony program a gépükre települjön. 2017 júliusában, amikor Ukrajna logisztikai rendszerét, közvetetten pedig a globális árúszállítási láncot bénította meg a NotPetya nevű zsarolóvírus, a támadás alapjául egy Ukrajnában használt könyvelőszoftver biztonsági frissítésébe elrejtett kártékony kód szolgált. Hasonló biztonsági frissítéseken keresztül bárki támadhatóvá válhat. Várhatóan ez a módszer a jövőben még gyakoribbá válik. A kártékony kódok esetében szintén fontosak az üzenetekben küldött csatolmányok, amelyeket a levelezőprogram, vagy a gyanútlan felhasználó megnyit és ezen keresztül biztosít hozzáférést a támadók számára. Említeni szükséges az úgynevezett „*keylogger*" programokat, amelyek harmadik fél részére továbbítják a billentyűleütéseket. Népszerű támadásforma az úgynevezett „*baiting*" is, amikor a támadók fertőzött adathordozókat, például pendriveokat, dvd-ket „hagynak el", illetve „ajándékoznak" másoknak.

A szerzők szerint nagy kockázatot jelentenek az okos mobil eszközökre írt alkalmazások, ugyanis a használatért cserébe különböző hozzáféréseket kérnek a felhasználóktól. Ezek gyakorlatilag mindenhez hozzáférést engedhetnek az alkalmazás fejlesztőjének, az üzeneteink tartalmától kezdve a geolokációs helymeghatározáson, a tárolt fájljainkon keresztül a kameránk, mikrofonunk irányításán bezárólag. Az áldozatok sokszor nem is tudnak arról, hogy a hozzáférést ők maguk engedélyezték. A felhasználók sajnálatos módon nagyon kevés esetben olvassák el, hogy egy alkalmazás telepítésekor mihez adnak engedélyt. Egy okostelefonos zseblámpa alkalmazás esetén értelemszerűen szükség van a vaku irányításához. Az üzenetek olvasása, kamera, mikrofon tárhely vezérlése és egyebekhez való hozzáférés azonban teljességgel indokolatlan ehhez. Ha ilyen engedélyeket kér egy alkalmazás, akkor annak célja az adathalászat lesz, és nem az, mint aminek a program feltüntette magát.

Ennek ellenére rendszeresen derül kialkalmazásokról, amelyet több tízmillióan használtak, [31] hogy valójában adathalászatra írták azokat, és mégis hosszú ideig letölthetők a Google Play áruházból.[32]

A wi-fi alapú támadások esetében elmondható, hogy a hálózat üzemeltetője monitorozhatja az adott hálózaton zajló kommunikációt. A szerzők tapasztalata, hogy egyre többen vannak tisztában a nyílt wi-fi hálózat jelentette veszélyekkel, azonban ugyanezek a kockázatok érvényesek a jelszóval védett hálózatokra is. Támadóként nem nehéz egy jelszóval védett wi-fi hálózatot létrehozni, amihez aztán a bizalom kialakítása érdekében jelszavakat osztogatnak. Sajnálatos módon a felhasználók ritkán változtatják meg hozzáférési adataikat, ezért szinte gyerekjáték behatolni ezekbe a hálózatokba. A router megpingelésével megismerhető a router típusa, azt követően egy szimpla Google-ös kereséssel meghatározható az alapértelmezett jelszó és azonosító (lásd 7. számú ábra).

A Cisco routerek az egyik legnépszerűbbek a piacon, és mint az ábrán is látható, az alapértelmezett jelszavak mégsem túl bonyolultak. Természetesen több száz modell található forgalomban hasonlóan egyszerűen kideríthető alapbeállításokkal.

Cisco Default Passwords (Valid April 2019)

Default Password List			
Cisco Model	**Default Username**	**Default Password**	**Default IP Address**
ESW-520-24-K9	cisco	cisco	192.168.10.2
ESW-520-24P-K9	cisco	cisco	192.168.10.2
ESW-520-48-K9	cisco	cisco	192.168.10.2
ESW-520-48P-K9	cisco	cisco	192.168.10.2
ESW-520-8P-K9	cisco	cisco	192.168.10.2
ESW-540-24-K9	cisco	cisco	192.168.10.2
ESW-540-24P-K9	cisco	cisco	192.168.10.2
ESW-540-48-K9	cisco	cisco	192.168.10.2
ESW-540-8P-K9	cisco	cisco	192.168.10.2
RV016	admin	admin	192.168.1.1
RV042	admin	admin	192.168.1.1

7. ábra A Cisco routerek alapértelmezett jelszavai (saját képernyő mentés, forrás: https://www.lifewire.com/cisco-default-password-list-2619151)

[31] *Adatokat eltulajdonító androidos zseblámpa alkalmazás*, In. GovCERT, 2013. december 6., http://tech.cert-hungary.hu/tech-blog/131206/adatokat-eltulajdonito-androidos-zseblampa-alkalmazas (letöltve 2019. március 12-én.)

[32] Fontos látni, hogy az Androidos mobil eszközök jelentősen kitettebbek az ilyen jellegű támadásokkal szemben, ugyanis az Apple alkalmazásboltjába több körös, szigorú ellenőrzést követően kerülhetnek csupán fel alkalmazások.

2.3. Egy támadás felépítése

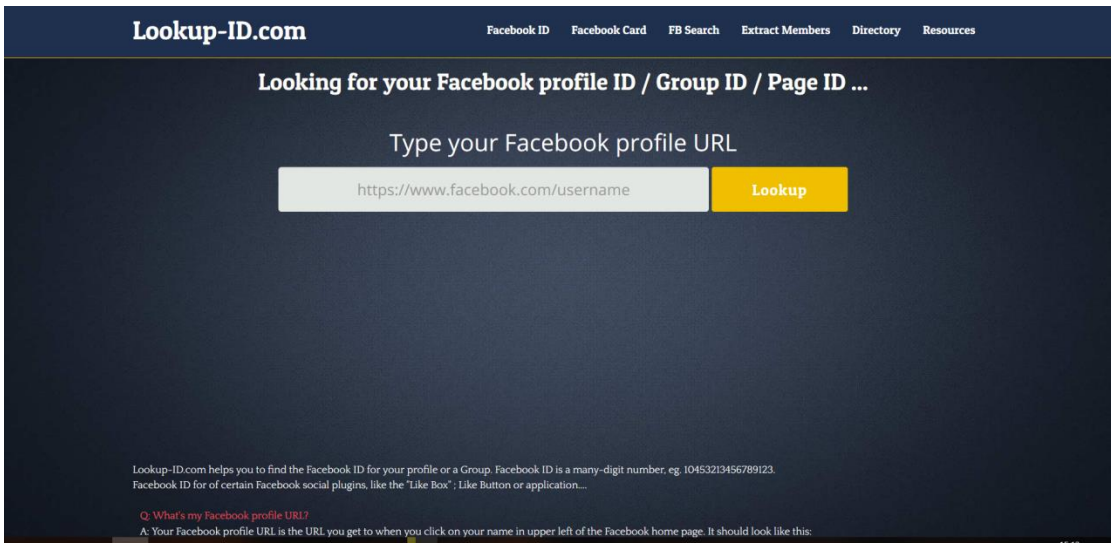
Ahogy a támadástípusok esetében a különböző szerzők eltérő csoportosítást alkalmaznak, úgy a támadások felépítésre is eltérő lehet a különböző szerzőknél.[33] Jelen cikkben mi az alábbi lépéseket tekintjük egy támadás felépítéséhez.

Egy social engineering támadás az információgyűjtéssel indul. A támadóknak erre a célra az internet és a közösségi oldalak széleskörű lehetőséget biztosítanak.[34] Egy egyszerű Google-ös keresés a „Facebook Open Source Intelligence" keresőszavak alkalmazásával több olyan oldalt is listáz, amelyek használatával percek alatt megszerezhetünk rengeteg nyilvánosan elérhető adatot a célszemélyünk Facebook aktivitásáról.[35] Ilyen oldal például a 8. számú ábrán látható (www.uk-osint.net).

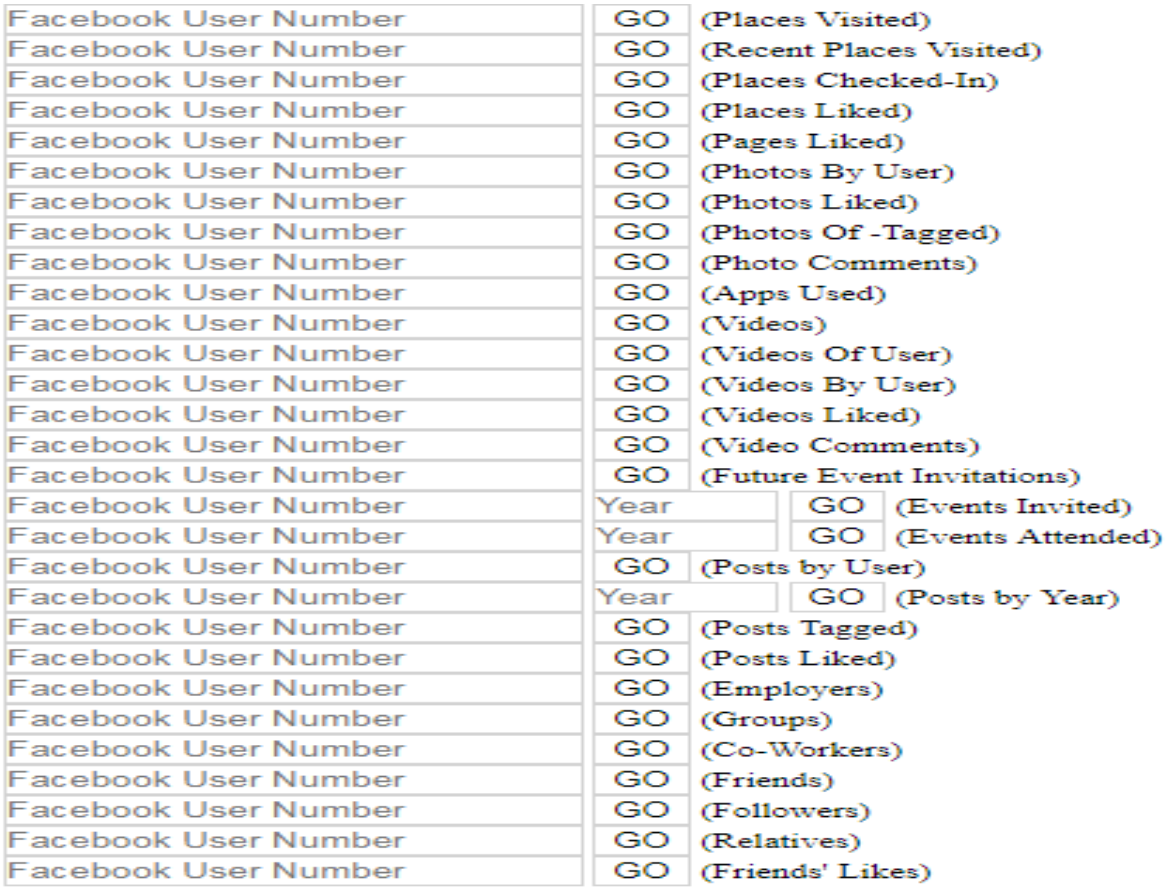
Az oldal használatához szükségünk van a célszemélyünk Facebook által használt azonosítójára (ID Number), az oldalon található több ID Number generáló oldal segítségével szerezhetünk meg (9. számú ábra). Ehhez be kell másoljuk a célszemély Facebook profiljának az URL-jét. Ezt követően az ID Numbert a számunkra érdekes részhez másoljuk, s meg is kaptuk az elérhető információkat (10. számú ábra). Természetesen csak a nyilvános információk érhetők el, tehát ha letiltották a láthatóságot, akkor azt nem látjuk. Ettől eltekintve kereshetünk minden egyéb nyilvános adat között: milyen oldalakat kedvel, honnan szokott bejelentkezni, milyen fényképeken jelölték meg, milyen kommenteket szokott írni, kik a munkatársai stb. Ezek jelentős része szintén letiltható, hogy látható legyen, de ha mondjuk olyan helyre kommentelünk, ahol az ismerősünk nem tiltotta le a láthatóságot, azt meg fogjuk találni.

[33] Lásd szintén Mouton és szerzőtársai által korábban hivatkozott tanulmányt. MOUTON et al.: i. m. 2016.
[34] BÁNYÁSZ Péter: *Social engineering és közösségi média*. In. Nemzetbiztonsági Szemle 5(1), 2018. pp. 59-77.
[35] Fontos megjegyezni, hogy a tanulmány megírása és lektorálása közötti időszakban a Facebook lekorlátozta az ilyen jellegű elemzéshez ingyenesen használható, külső oldalakra történő integrálását, ezért a cikkben említett példák használhatósága bizonytalan. Ettől függetlenül számos fizetős szolgáltatás foglalkozik ilyen keresési lehetőségek biztosításával.

8. ábra Nyílt forrású információgyűjtés pár kattintással a Facebookról (saját szerkesztés, forrás: www.uk-osint.net)



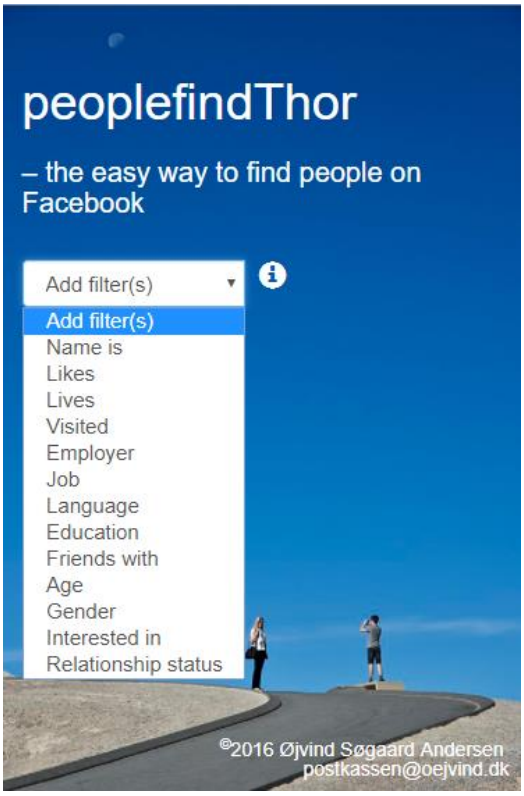
9. ábra Hogyan szerezzük meg a célszemély Facebook ID Numberét (saját szerkesztés, forrás: http://lookup-id.com/)



10. ábra Néhány példa, hogy milyen információkat szerezhetünk meg pár perc alatt (saját szerkesztés, forrás: https://inteltechniques.com/OSINT/facebook.html)

Értelemszerűen fentiek csak abban az esetben működnek, ha ismerjük a célszemélyt. Az ismertetett oldalon azonban egy másik hasznos oldalra is átnavigálhatunk, ami különböző, általunk megadott változók alapján végzi a keresést (lásd 11. számú ábra). Ezek lehetnek például a lakhely, nem, kor, oldalkedvelések, munkahely, iskola, kapcsolati státusz stb. Az információgyűjtés szürke zónáját jelenthetik az okos mobil eszközökre optimalizált alkalmazások, hiszen ahogy fentebb is látható volt, számos lehetőséget biztosítanak az információgyűjtésre, többek között legszemélyesebb üzeneteink olvasásával, kameránk, mikrofonunk aktiválásával.[36]

[36]BÁNYÁSZ Péter: *Rolle der sozialen Medien bei OSINT*. Mitteleuropaische Polizeiakademie Fachjournal, 2018/2. pp. 15-21.



11. ábra Nyílt forrású keresés különböző variásnok alapján (saját szerkesztés, forrás: https://www.peoplefindthor.dk/)

Az információszerzés fázisát a célszeméllyel való kapcsolat kiépítése jelenti, amelynek során a támadók a bizalmába férkőznek vagy éppen a róla gyűjtött információkkal történő megzsarolása követi, amelynek következtében végrehajtják a támadást. Minél értékesebb a célszemély, annál komolyabb nyomás alá helyezik az illetőt. Nem nehéz belátni, ha biztonságtudatos is az illető, de a gyerekén keresztül támadják, például hasonló nyílt forrású információgyűjtést követően a gyermek bizalmába férkőznek, és csalnak ki tőle érzékeny dolgokat (például erotikus képeket), nagyon nehéz nemet mondani a támadók kérésére, mondjuk egy fertőzött csatolmányt tartalmazó e-mail munkahelyen történő megnyitására.

3. Veszélyeket és kockázatokat befolyásoló tényezők az információbiztonsági tudatosság terén

3.1. Személyiségjegyek

Az információbiztonsági tudatosság (Information Security Awareness, továbbiakban ISA) arra összpontosít, hogy a munkavállaló mennyire érti az információbiztonsági politikák, szabályok és irányelvek jelentőségét és következményeit, valamint mennyire hajlandó ezeknek megfelelően cselekedni.[37] Ezzel összefüggésben az alkalmazottak ismereteinek növekedésével javul a hozzáállás, és

[37] KRUGER, Hennie A., KEARNEY, Wayne D.: *A prototype for assessing information security awareness.*Computers & security, 25(4), 2006. pp. 289-296.

ezzel együtt fejlődik az ISA és az elvárható viselkedés.[38] Az egyének közötti különbségek figyelembe vétele elengedhetetlen ahhoz, hogy megértsük az alapul szolgáló pszichológiai mechanizmusokat, amelyek befolyásolják a felhasználói tudatosságot.

Az ötfaktoros személyiségmodellt széles körben alkalmazzák számos tényező megértésére, és előrejelzésére különböző és összetett környezetekben. A „Big Five" modell a személyiség mérésének vezető elméleti modellje, amely a következő tényezőkből áll: neuroticizmus, extraverzió, nyitottság a tapasztalatra, barátságosság és lelkiismeretesség.[39] A neuroticizmus a pszichológiai stresszre való hajlamot jelenti, vagyis azt, hogy mennyire könnyen ragad el bennünket egy negatív érzelem, például a harag, a szorongás vagy a depresszió. Az extraverziót az impulzusok szabad kifejezése, a határozottság, a dominancia vagy a boldogság jellemzi leginkább. A tapasztalatra való nyitottság alatt a művészet, az érzelem, a kíváncsiság és a sokféle tapasztalat méltánylását értjük. A barátságosság azt mutatja meg, hogy a személy inkább együttérző és kooperatív, nem pedig gyanakvó és ellentmondásos másokkal szemben. A lelkiismeretesség a szervezettség és a megbízhatóság tendenciája, ide tartozik az önfegyelem, kötelességteljes cselekvés, ambíció és a tervezett viselkedés.

2001-ben szignifikáns fordított kapcsolatot találtak a lelkiismeretesség, a barátságosság, valamint a munkahelyi balesetek száma között.[40] Egy olyan tanulmányban, amely a személyiség és a webes biztonsági szoftverek elfogadására irányuló szándékot vizsgálta, megállapították, hogy a magas szintű nyitottság a biztonsági szoftverek tényleges használatára pozitív hatással van. Felvetették, hogy azok az egyének, akik magas pontszámot értek el a nyitottság tényezőben, aggódnak amiatt, hogy mások mit gondolnak róluk, és ennélfogva nagyobb valószínűséggel foglalkoznak a biztonsági kérdésekkel is. Ezeknél a személyeknél az olyan tulajdonságok, mint a szabálykövetés pozitívan társultak a lelkiismeretességgel és a nyitottsággal azokban az esetekben is, amikor nem tudták, hogy megfigyelik őket.[41] 2015-ben egy másik kutatás a meggondolatlan számítógépes viselkedést és az egyes egyéni tényezőket vizsgálta, beleértve a munkavállaló életkorát, az iskolázottsági szintet, a digitális kompetenciákat és a felhasználók személyiségé. Ez a kutatás megállapította, hogy a munkavállalók naiv magatartása valószínűleg kevésbé kockázatos, ha lelkiismeretesebbek, elfogadóbbak, kevésbé impulzívak, nyitottabbak és kevesebb ismeretük van a számítógép használat terén.[42]

A kutatók vizsgálták a kockázatvállalási hajlandóságot, aminek az eredményeként megállapították, hogy bár az különböző helyzetekben változik, az egyénnek az észlelt kockázathoz való kapcsolata hosszabb távon viszonylag stabil

---

[38] SIPONEN, Mikko T.: *A conceptual foundation for organizational information security awareness.* Information Management & Computer Security, 8(1), 2000. pp. 31-41.

[39] JOHN, Oliver P., SRIVASTAVA, Sanjay:*The Big Five trait taxonomy: History, measurement, and theoretical perspectives*. In: PERVIN, Lawrence A., JOHN, Oliver P. (eds.) *Handbook of personality: Theory and research*. Vol. 2, Guilford Press, New York, NY, USA, 1999. pp. 102-138.

[40] CELLAR, Douglas F. et al.: *The five-factor model and safety in the workplace: Investigating the relationships between personality and accident involvement.* Journal of Prevention & Intervention in the community, 22(1), 2001. pp. 43-52.

[41]SHROPSHIRE, Jordanet al.:*Personality and IT security: An application of the five-factor model.* AMCIS 2006 Proceedings, 2006. p. 415.

[42] PATTINSON, Malcolm et al.:*Factors that influence information security behavior: An Australian web-based study.* In International Conference on Human Aspects of Information Security, Privacy, and Trust. Springer, Cham, 2015. pp. 231-241.

marad.[43] A mindennapi kockázatvállalási magatartások rendszerint serdülőkorban, illetve a korai felnőttkorban jelentkeznek, majd fokozatosan csökkenek. Kutatások kimutatták, hogy az extraverzió és a nyitottság jellemzőit magasan magukban hordozó, és a barátságosság, a lelkiismeretesség és a neuroticizmus értékét alacsony szinten hordozó személyek magasabb kockázatvállalási hajlandósággal rendelkeznek.[44]

3.2. Kulturális háttér

A viselkedéses információbiztonsági megközelítésű kutatásának egyfajta korlátját jelenti, hogy a vizsgálatokat döntően a nyugati kultúrkörökben végezték, azonban szintén jelentős számban végeztek hasonló kutatásokat többek között Indiában, Dél- Afrikában, Kínában és Oroszországban is, ahogy ezt a SciValban történt elemzésünk megállapította. A világ többi területének nagy részét figyelmen kívül hagyták; keveset vizsgálták a kultúraközi különbségeket a témán belül. A jelenlegi tanulmányokat fontos lenne kiigazítani a kultúrák közötti különbségek figyelembevételével, mint például a bizonytalanság kerülés, az individualizmus-kollektivizmus és a hatalmi távolság, hiszen ezek a különbségek bizonyítottan hatással vannak más informatikai témákban is[45].

A bizonytalanságkerülés megmutatja, hogy egy nemzet mennyire várja el, hogy az általuk tapasztalt szituációk strukturáltak, koordináltak legyenek. A túl magas érték legtöbbször aggódó, az újtól tartó nemzetre utal, míg egy kisebb értékkel bíró inkább flexibilisebbnek tekinthető. A bizonytalanság elkerülése azt jelenti, hogy a kultúra tagjai mennyire érzik magukat fenyegetettnek bizonytalan, vagy ismeretlen helyzetekben. Dánia és Szingapúr az alacsony bizonytalanságkerülő nemzeti kultúrák példái, Japán a nagy bizonytalanságkerülésnek a példája. Tekintettel az erre való hajlandóságukra, feltételezhető, hogy egy japán felhasználó kevésbé válik adathalász-e-mailek áldozatává, mint a bizonytalanságra nyitottabb emberek.[46]

Az individualizmus olyan kultúrákat ír le, amelyekben laza az egyének közötti kapcsolatrendszer. A kollektivizmus pedig olyanokat, amelyekben az emberek erős, összetartó közösségekbe integrálódnak, amelyek megvédik az egyéneket cserébe a megkérdőjelezhetetlen lojalitásért. USA az individualista nemzeti kultúrának, míg Kína a kollektivista kultúrának a példája. Ezek a különbségek egyértelműen pozitív vagy negatív hatást gyakorolhatnak az információbiztonsági viselkedésére: a kollektivista egyének nagyobb hűségének köszönhetően erőteljesebben ragaszkodhatnak a biztonsági politikákhoz, de csak addig, amíg azok betartása hűségnek tekinthető. Az ilyen személy viszont kevésbé valószínű, hogy jogsértéseket jelentene azokról, akikhez lojális. Az individualisták sokkal inkább jelentik a magasabb pozíciójú szervezeti tagok által elkövetett jogsértéseket abban az esetben is, ha feléjük elkötelezettek.[47]

---

[43] WEBER, Elke U., MILLIMAN, Richard A.: *Perceived risk attitudes: Relating risk perception to risky choice*. Management science, 43(2), 1997. pp. 123-144.

[44] NICHOLSON, Nigel et al.: *Personality and domain-specific risk taking.* Journal of Risk Research, 8(2), 2005. pp. 157-176;

[45] CROSSLER, Robert E. et al.: *Future directions for behavioral information security research*. computers & security, 32, 2013. pp. 90-101.

[46] ZHANG, Dongsong, LOWRY, Paul B.: *Issues, limitations, and opportunities in cross-cultural research on collaborative software in information systems*. In E-Collaboration: Concepts, Methodologies, Tools, and Applications. IGI Global, 2009. pp. 553-585.

[47] ZHANG, Dongsong et al: *The impact of individualism—collectivism, social presence, and group diversity on group decision making under majority influence.* Journal of Management Information Systems, 23(4), 2007. pp. 53-80.

A hatalmi távolság megmutatja, hogy az országon belüli intézmények és szervezetek hierarchiájának alsó szintjén elhelyezkedő tagjai elfogadják-e, hogy a hatalom egyenlőtlenül oszlik meg, és elvárják-e az egyenlőtlenséget egy közösségen belül. Az alacsony hatalmi távolság és hozzávetőleg kis egyenlőtlenség jellemzi Kanadát, míg Kínára a nagy hatalmi távolság jellemző. Ez a faktor drámai hatást gyakorolhat a friss informatikai védelmi előírások és technológia alkalmazására és az új szabályok elfogadására. A nagy hatalmi távolságú kultúrákhoz tartozók inkább hajlandók betartani az informatikai biztonsági követelményeket, míg az alacsony hatalmi távolsági kultúrákból származók saját választásuk szerint igazodhatnak egy-egy előíráshoz.[48]

Egy más szemlélet, melyen keresztül vizsgálni lehet a kultúrát, a konfuciánus dinamizmus. Ez a kultúra időorientáltságát jelöli, melyet két pólusként hosszú távú és rövid távú orientációval jellemeznek. A rövid távú szemléletre USA vagy Kanada a megfelelő példa, míg a hosszú távú szemlélet, kitartás, státus központúság, szégyentudat, közösség méltóságának megőrzése jellemzi Kínát és Japánt. Az időorientáció komoly hatást gyakorolhat a szervezetek vezetőinek döntéseire, hiszen például Japánban hosszabb távú stratégiai szempontból fontolják meg biztonsági struktúrájukat.[49]

3.3. Az életkor és a nem

A nemek közötti különbségek a kor előrehaladtával elhatárolhatóbbak, pontosabban az idősebb munkavállalók körében jobb teljesítmény mérhető.[50] Számos tanulmány kimutatta, hogy a nemek kihatással vannak online térbeli elővigyázatosságra, amiben a nők bizonyulnak erősebbnek, hiszen a nőknél dominánsabb a megfelelés szándéka, mint a férfiaknál.[51] Az idősebb korosztály továbbá inkább kockázatkerülőbb a számítógépes viselkedésük tekintetében, mint a fiatalabbak. Azt is megállapították, hogy a 18 és 35 év közötti személyek érzékenyebbek, vagyis jobban kitettek az adathalász e-mailek által jelentett fenyegetésekre, mint az idősebbek. [52] A kockázatvállalási hajlam akár fiatal felnőttkortól is csökkenhet, de az életkor és a vizsgált viselkedés közötti kapcsolat szignifikáns marad a kockázatvállalási hajlandóságot figyelmen kívül hagyva is.

Egy adathalászatot vizsgáló tanulmányban kicsi különbségeket találtak a felhasználók viselkedése között nemek szerint. A tanulmány úgy találta, hogy a nők valamivel érzékenyebbek voltak az adathalász e-mailekre, mint a férfiak.[53]

Az olyan elméleteket, mint az egészséghit modell[54] és a védelmi motivációs elmélet[55], elsősorban a felhasználók biztonsági technológiák alkalmazására irányuló

---

[48] ZHANG, LOWRY: i. m. 2009.
[49] uo.
[50] MORRIS, Michael G. et al: *Gender and age differences in employee decisions about new technology: An extension to the theory of planned behavior*. IEEE transactions on engineering management, 52(1), 2005. pp. 69-84
[51] HERATH, Tejaswini, RAO, H. Raghav.:*Protection motivation and deterrence: a framework for security policy compliance in organisations.* European Journal of Information Systems, 18(2), 2009. pp. 106-125.
[52] SHENG, Steve et al.:*Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions.* In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2010. pp. 373-382.
[53] PATTINSON et al.: i. m. 2015.
[54] ROSENSTOCK, Irvin M.: *The health belief model and preventive health behavior*. Health education monographs, 2(4), 1974. pp. 354-386.

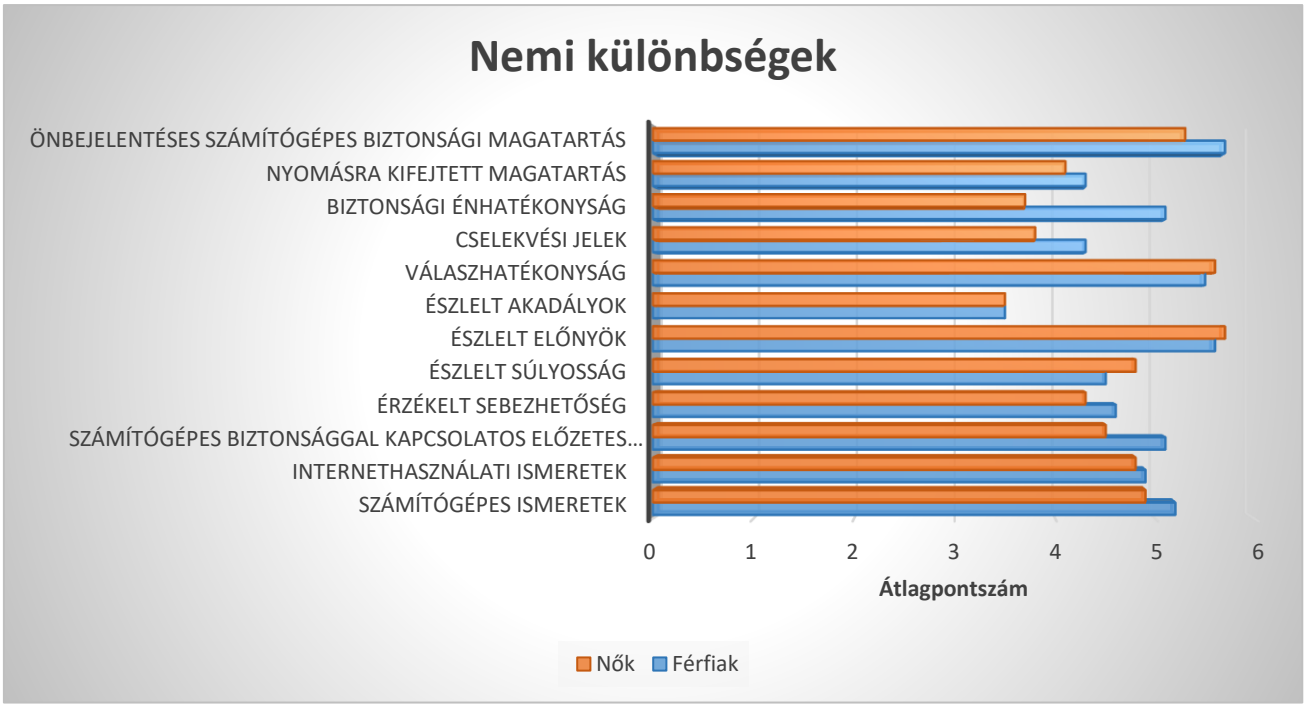
szándékának magyarázatára, valamint arra használták, hogy megfejtsék, hogyan és mikor alkalmaz az egyén adaptív, illetve maladaptív viselkedést, amikor fenyegetést észlel. Az egészséghit modell szerint három tényező járul hozzá a fenyegetés észleléséhez: az észlelt súlyosság (az állapot súlyosságával és következményeivel kapcsolatos vélekedések), az észlelt hajlamosság (veszélyeztetettség érzésének mértéke), valamint a cselekvésre felszólító ingerek. A védelmi motivációs elmélet tulajdonképp ennek a kiterjesztése és átdolgozása. Az elmélet az egyén védekezési szándékát veszi figyelembe, mint az egészséges viselkedés meghatározóját, ahol a szándék az észlelt hajlamtól, az észlelt súlyosságtól, az énhatékonyságtól és a válaszhatékonyságtól függ. Ezen elméletek alapján a közelmúltbeli tanulmányok az információbiztonságban is megállapították, hogy az észlelt hajlamosság, észlelt súlyosság, észlelt előnyök és az énhatékonyság a biztonsági viselkedésekkel összefüggésben áll.

Kutatások olyan pszichológiai tényezőket alkalmaztak, amelyek az egészséggel kapcsolatos viselkedésekkel magyarázták a kiberbiztonsági viselkedést. Egy 2017-es kutatás[56] a nemek és az ajánlott kiberbiztonsági viselkedésmodell összetevői közötti kapcsolatokat vizsgálta (lásd 12. számú ábra), amely a védelmi motivációs elméleten és az egészséghit modellen alapul. A kutatásban kérdőíves felmérést végeztek a nemek és a modell többi tényezői közötti összefüggések vizsgálata érdekében. Különböző amerikai szervezetek és cégek alkalmazottai töltötték ki a 87 elemes online Likert-skálás kérdőívet.

A felmérés kiberbiztonsági, információtechnológiai, pszichológiai és döntéshozatali perspektívákat mért. Az egészséghit modellhez és a védelmi motivációs elmélethez alkalmazkodva a következő konstrukciókat vizsgálták: biztonsági énhatékonyság, észlelt súlyosság, érzékelt sebezhetőség, észlelt előnyök, számítógépes ismeretek, internetes készségek, számítógépes biztonsággal kapcsolatos korábbi tapasztalatok, észlelt akadályok, válaszhatékonyság, cselekvésre utaló jelek, nyomás alatt kifejtett magatartás, és önbejelentéses számítógépes biztonsági magatartás.

[55]ROGERS, Ronald W.: *Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation.* In: CACIOPPO, John T., PETTY, Richard (eds.) Social psychophysiology: A sourcebook. Guilford Press, New York, NY, USA, 1983. pp. 153-176.

[56] ANWAR, Mohd et al: *Gender difference and employees' cybersecurity behaviors.* Computers in Human Behavior, 69, 2017. pp. 437-443.



12. ábra: a nemek és a kiberbiztonsági viselkedés összetevői közötti kapcsolatok (saját szerkesztés, forrás: Anwar, Mohd et al.: i. m. 2017:440.)

Az előzetes tanulmányok többsége azt mutatja, hogy a nők általában jobban aggódnak a magánéleti dolgok miatt (észlelt sebezhetőség) mint a férfiak, és nagyobb valószínűséggel alkalmazkodnak a biztonsági politikához, mint a férfiak, de az imént említett kutatás szerint a férfiak kibertérben való viselkedése egy fokkal biztonságorientáltabb. Mivel a nők énhatékonysága lényegesen alacsonyabb, mint a férfiaké, a női énhatékonyság célpontja lehet kiberbiztonsági tudatosságnövelő képzéseknek.

2005-ben tanulmányokat folytattak a technológia alkalmazásának és folyamatos használatának mérésére a munkahelyeken. A vizsgálatok azt mutatták, hogy a férfiak nagyobb befolyást gyakorolnak a technológiák használatára, mint a nők, míg a nőket inkább a szubjektív normák, a társadalmi szerepek és a viselkedéskontroll vezérli.[57] A nők továbbá érzékenyebbek a kockázatokkal szemben, míg a férfiak, akik nagyobb eséllyel hajlandók kockázatot vállalni. [58] A nők sokkal nagyobb jelentőséget tulajdonítanak az érzékelt kontroll és magánéleti kockázatoknak, amikor információkat osztanak meg a közösségi oldalakon.[59]

4. Összefoglalás

Tudománymetriai vizsgálat keretében vizsgáltuk a social engineering fogalom eredetét, az ezzel leírt jelenségek tudományközi kapcsolatait, amelyeket elengedhetetlenül szükségesnek tartottunk az értelmezéshez. Nagyszámú (N=1898) nemzetközi tudományos közlemény elemzése során megállapítottuk, hogy a social

[57] MORRIS et al.: i. m. 2005.
[58] DWYER, Peggy D. et al.: *Gender differences in revealed risk taking: evidence from mutual fund investors.* Economics Letters, 76(2), 2002. 151-158.
[59] HAJLI, Nick, LIN, Xiaolin: *Exploring the security of information sharing on social networking sites: The role of perceived control of information*. Journal of Business Ethics, 133(1), 2016. pp. 111-123.

engineering fogalma több, mint 177 évre tekint vissza, amely időszak alatt bizonyos fejlődésen ment keresztül, illetve megfigyelhető az is, hogy az eredetihez képest új jelenségek leírására is elterjedt a fogalom. A fogalom komplexitása mellett azonban megállapítható, hogy a social engineeringgel összefüggő tudományos kutatás, illetve ennek köszönhetően a publikációk száma külföldön a 2000-évek elején robbanásszerűen megnövekedett, amely egyértelműen a csúcstechnológiai bűnözéssel, illetve a kiberbiztonsággal összefüggő fogalom értelmezésnek köszönhető. Az említett felfutás a külföldiekhez képest néhány évvel később és számszerűen jelentősen kisebb mértékben, de a hazai tudományos kutatások terén is megfigyelhető. Vizsgálatunk megmutatta, hogy a kutatások között a multidiszciplináris megközelítés dominál. Az általunk vizsgált 1898 közlemény tartalma szerint összesen 3091 tudományterületre sorolható. A Pareto-eloszlást figyelembe véve megállapíthatjuk, hogy a releváns tudományterületek közül már az első hat kiteszi ezek 80%-át, ezért a közlemények tudománymetriai súlypontja az informatika (26,72%), a társadalomtudományok (22,84%), a műszaki tudományok (11,91%), a művészet és bölcsészettudományok (10,38%), a matematikai tudományok (4,89%) és az üzleti-, menedzsment- és számvitel tudományok (4,01%) lettek.

Szintén nagyszámú (N=1350) social engineeringgel foglalkozó közleményt elemezhettük a leggyakrabban előforduló 50 kulcsszó alapján, melynek során megállapítottuk, hogy a fogalom erősen kapcsolódik a bűnözéshez, ezen belül pedig a csúcstechnológiai bűnözéshez. Az utolsó teljes 10 év periódusban pedig megállapítottuk, hogy az általunk választott kulcsszó, illetve kulcs kifejezés gyakorisága szignifikánsan növekedett, ami arra utal, hogy a social engineering kutatások, illetve ezek következtében a tudományos közlemények száma a bűnügyi tudományok területén is felfutóban vannak.

A social engineering fogalom alá tartozó és a tanulmány írásakor már ismert támadási módszerek bemutatását, néhány fontosabb jellemzőit, illetve az ellenük való védekezés szempontjait ismertettük. Bemutattunk egy lehetséges forgatókönyv szerinti támadást és annak során felhasznált és az interneten bárki által hozzáférhető alkalmazásokat.

Vizsgálatunk során azonban arra a következtetésre jutottunk, hogy mára elengedhetetlenül szükségessé vált a fogalom magyar nyelvi és tudományos igényű megfeleltetése, amelyre e tanulmány keretein belül a szerzők nem vállalkoztak. Javaslataik megfogalmazását követően e célból egy másik vizsgálat elvégzését, illetve tanulmány elkészítését tartjuk indokoltnak, amely reményeink szerint a tudományos közösség képviselői közötti diskurzust is előmozdítja.

Az információbiztonsági tudatosság fejlesztése jelenleg, és várhatóan a jövőben is kulcskérdés marad a social engineering kategóriába tartozó támadások elleni védekezésben. Ennek oka főként az emberi tulajdonságok, gyengeségek kihasználására irányuló törekvésből fakad. A megelőzésben fontos kérdés, hogy kockázati megközelítést alkalmazzunk, amely tekintettel kell legyen a kockázatokkal szembeni kitettségre, érzékenységre, a támadások gyakoriságára és a sikeres támadások által okozott kárra. Tanulmányunkban bemutattuk az egyén social engineering kockázatokkal szembeni jellemzőit személyiségjegyek, kulturális háttér, az életkor és a nemek szerinti megoszlásban. A kockázatok elemzését azonban időszakonként szükséges megismételni és az esetlegesen tapasztalt változásokat a védekezés során figyelembe venni.

Felhasznált irodalom

[1] 1994. évi XL. törvény a Magyar Tudományos Akadémiáról

[2] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[3] *Adatokat eltulajdonító androidos zseblámpa alkalmazás*. In: GovCERT, 2013. december 6., http://tech.cert-hungary.hu/tech-blog/131206/adatokat-eltulajdonito-androidos-zseblampa-alkalmazas (letöltve: 2019. március 12.)

[4] ALEXANDER, Jon, SCHMIDT, Joachim K. H. W.: *Social engineering: Genealogy of a concept.* In. PODGÓRECKI, Adam et al. (eds.) Social Engineering. Carleton University Press, Ottawa, CA, 1996.

[5] ANWAR, Mohd et al: *Gender difference and employees' cybersecurity behaviors.* Computers in Human Behavior, 69, 2017. pp. 437-443.

[6] BÁNYÁSZ Péter: *Social engineering és közösségi média*. Nemzetbiztonsági Szemle 5(1), 2018. pp. 59-77.

[7] BÁNYÁSZ Péter: *Rolle der sozialen Medien bei OSINT.*Mitteleuropaische Polizeiakademie Fachjournal, 2018/2. pp. 15-21.

[8] CELLAR, Douglas F. et al.: *The five-factor model and safety in the workplace: Investigating the relationships between personality and accident involvement.* Journal of Prevention & Intervention in the community, 22(1), 2001. pp. 43-52.

[9] Cisco routerek alapértelmezett jelszavai. https://www.lifewire.com/cisco-default-password-list-2619151 (letöltve: 2019. március 12.)

[10] CROSSLER, Robert E. et al.: *Future directions for behavioral information security research.* computers & security, 32, 2013. pp. 90-101.

[11] CSERHÁTI András: *A Stuxnet vírus és az iráni atomprogram.*Fizikai Szemle, 2011/5. pp. 150-155.

[12] DWYER, Peggy D. et al.: *Gender differences in revealed risk taking: evidence from mutual fund investors.* Economics Letters, 76(2), 2002. 151-158.

[13] European Union Serious and Organised Crime Threat Assessment – Crime in the Age of Technology 2017. Public Version. Europol, The Hague, 2017.

[14] GREENWALD, Glenn: *A Snowden-ügy - Korunk legnagyobb nemzetbiztonsági botránya.* HVG Könyvek Kiadó, Bp., 2014.

[15] GYURÁK Gábor: *Kritikus infrastruktúrák védelme hálózati behatolásjelző rendszerekkel.*Hadmérnök, 2015/2 szám, pp. 223-233.

[16] HATFIELD, Joseph M.: *Social engineering in cybersecurity: The evolution of a concept.*Computers & Security 73, 2018. pp. 102-113. https://doi.org/10.1016/j.cose.2017.10.008

[17] HAJLI, Nick, LIN, Xiaolin: *Exploring the security of information sharing on social networking sites: The role of perceived control of information.*Journal of Business Ethics, 133(1), 2016. pp. 111-123.

[18] HERATH, T., RAO, H. R.:*Protection motivation and deterrence: a framework for security policy compliance in organisations*.European Journal of Information Systems, 18(2), 2009. pp. 106-125.

[19] JOHN, Oliver P., SRIVASTAVA, Sanjay:*The Big Five trait taxonomy: History, measurement, and theoretical perspectives.* In: PERVIN, Lawrence A., JOHN, Oliver P. (eds.) *Handbook of personality: Theory and research*, Vol. 2, Guilford Press, New York, NY, USA, 1999. pp. 102-138.

[20] KOVÁCS László, KRASZNAY Csaba: *„Mert övék a hatalom”: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során.*SVKK elemzések, 2017/9. pp. 1-11.

[21] KRASZNAY Csaba: *A polgárok védelme egy kiberkonfliktusban*. Hadmérnök, 2012/4. szám. pp. 142-151.
[22] KRUGER, Hennie A., KEARNEY, Wayne D.: *A prototype for assessing information security awareness.*Computers & security, 25(4), 2006. pp. 289-296.
[23] MITNICK, Kevin David*: A legendás hacker - A megtévesztés művészete*. Perfact Kiadó, Bp, 2003.
[24] MORRIS, Michael G. et al: *Gender and age differences in employee decisions about new technology: An extension to the theory of planned behavior.* IEEE transactions on engineering management, 52(1), 2005. pp. 69-84.
[25] MOUTON, Francois et al.: *Social engineering attack examples, templates and scenarios.* Computers & Security, 2016/59. pp. 186-209.
[26] MUNK Sándor: *Információbiztonság vs. informatikai biztonság.*Hadmérnök, 2008/különszám. pp. 1-21. URL.: http://hadmernok.hu/kulonszamok/robothadviseles7/munk_rw7.pdf
[27] NICHOLSON, Nigel et al.*: Personality and domain-specific risk taking*.Journal of Risk Research, 8(2), 2005. pp. 157-176.
[28] PATTINSON, Malcolm et al.:*Factors that influence information security behavior: An Australian web-based study.* In: International Conference on Human Aspects of Information Security, Privacy, and Trust. Springer, Cham, DE, 2015. pp. 231-241.
[29] RITECZ György: *A terrorizmus és a migráció viszonya a számok alapján.*Acta Humana, 2016/5. pp. 113-123.
[30] ROBINSON, Michael et al.: *Cyber warfare: Issues and challenges.*Computers & Security. 2015/49. pp. 70-94.
[31] ROSENSTOCK, Irvin M.: *The health belief model and preventive health behavior.* Health education monographs, 2(4), 1974. pp. 354-386.
[32] ROGERS, RONALD W.:*Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation.* In: CACIOPPO, J. T., PETTY, R. (eds.) *Social psychophysiology: A sourcebook.* Guilford Press, New York, NY, USA, 1983. pp. 153-176.
[33] SALLAI Gyula: *Az okos város koncepciója.* In: SALLAI Gy. (szerk.) *Az okos város* (Smart City). Dialóg Campus Kiadó, Bp., 2018. pp. 13-34.
[34] SHENG, Steve et al.:*Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions.* In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2010. pp. 373-382.
[35] SHROPSHIRE, Jordanet al.:*Personality and IT security: An application of the five-factor model.* AMCIS 2006 Proceedings, 2006. pp. 415.
[36] SINGER, Peter W., FRIEDMAN, Allen: *Cybersecurity and Cyberwar - What Everyone Needs to Know*. Oxford University Press, Oxford, 2014. pp. 114-120.
[37] SIPONEN, Mikko T.: *A conceptual foundation for organizational information security awareness*. Information Management & Computer Security, 8(1), 2000. pp. 31-41.
[38] SZÁDECZKY Tamás: *Risk Management of New Technologies*. *Academic and Applied Research in Military and Public Management Science* 15(3), 2016. pp. 279-290.
[39] THOMSON, Jim R.: *Cyber Security, Cyber-attack and Cyber-espionage.* In. High Integrity Systems and Safety Management in Hazardous Industries. Elsevier B. V., Amsterdam, 2015. pp. 45-53.
[40] URBANOVICS Anna, SASVÁRI Péter: *A tudományos kutatás elixírje*. Working Paper, 2019. július, DOI: 10.13140/RG.2.2.26344.83204

[41] WEBER, Elke U., MILLIMAN, Richard A.: *Perceived risk attitudes: Relating risk perception to risky choice*. Management science, 43(2), 1997. pp. 123-144.

[42] ZHANG, Dongsong et al.: *The impact of individualism—collectivism, social presence, and group diversity on group decision making under majority influence.* Journal of Management Information Systems, 23(4), 2007. pp. 53-80.

[43] ZHANG, Dongsong, LOWRY, Paul B.: *Issues, limitations, and opportunities in cross-cultural research on collaborative software in information systems*. In: E-Collaboration: Concepts, Methodologies, Tools, and Applications. IGI Global, 2009. pp. 553-585.

Lektorálta: Sasvári Péter Dr. PhD. egyetemi docens
Nemzeti Közszolgálati Egyetem
Államtudományi és Nemzetközi Tanulmányok Kar
Közszervezési és Infotechnológiai Tanszék
sasvari.peter@uni-nke.hu

›››››