HADMÉRNÖK
VÉDELEMINFORMATIKA

16. évfolyam (2021) 3. szám 173–187.
DOI: 10.32567/hm.2021.3.10

Dub Máté[1]

A social engineering támadások megelőzésének lehetőségei[2]

The Opportunities for Social Engineering Attacks Prevention

Társadalmunk rohamos technológiai fejlődésével párhuzamosan új típusú kihívások és fenyegetések jelentek meg, és nem pusztán a kibertérben, hanem mindennapi életünk folyamán, az offline térben is fenyegetettségként jelentkeznek. A támadások számában szignifikáns növekedést, a támadási technikák szempontjából pedig egyre nagyobb szofisztikáltságot tapasztalhatunk. Gyakran elhangzik, már-már közhelyként, hogy a kiberbiztonság leggyengébb láncszeme a humán tényező. Ez a gondolat akármennyire is régóta előfordul a kiberbiztonsággal kapcsolatos publikációkban, annak érvényessége a mai napig fennáll, ugyanis a támadók leggyakrabban a nem kellően biztonságtudatos felhasználókat veszik célba, és e személyek tevékenysége miatt a legkiválóbb szoftverek sem nyújthatnak megfelelő biztonságot abban az esetben, ha a kezelő nem rendelkezik a megfelelő kompetenciákkal.

A nem kellően biztonságtudatos emberek számára kifejezetten nagy veszélyt jelentenek az egyre kifinomultabb social engineering szintjén zajló támadások, így e technika támadási keretrendszereinek és támadási modelljeinek vizsgálatával a megelőzés és az elkerülés minél hatékonyabb működését érhetjük el. Természetesen e tekintetben a tudatosítás és az oktatásba történő bevezetés fontosságát sem szabad elhanyagolnunk.

Kutatásomban a cél a védettség prosperálási lehetőségeinek vizsgálata volt a fentebb részletezett kiberfenyegetettségekkel szemben. Empirikus kísérletek elemzésével, a social engineering szintjén zajló támadások megelőzésével kapcsolatban a fő kérdést úgy fogalmazhatjuk meg, hogy vajon az adat- és információbiztonság,

[1] Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar, hallgató, e-mail: mate.dub@protonmail.ch

[2] A kutatás és a publikáció az Innovációs és Technológiai Minisztérium ÚNKP-20-1-I-NKE-71 kódszámú Új Nemzeti Kiválóság Programjának szakmai támogatásával készült.

a biztonságtudatosság potenciálisan növelhető-e az érdeklődés felkeltése, a személyes, problémaorientált példák és az oktatásba való implementálás mentén?

Kulcsszavak: **social engineering, adat- és információbiztonság, biztonságtudatosság, adatvédelem, kiberbiztonság, közszolgálat**

In parallel with the rapid technological development of our society, new types of challenges and threats have emerged, and they are emerging as threats not only in the cyberspace, but also in our daily lives, in the offline space. There is a significant increase in the number of cyberattacks, while in terms of attack techniques we can see an increasing sophistication. It is often said, almost as a commonplace, that the weakest link in cybersecurity is the human factor. As often as this idea occurs in cybersecurity publications, it is still valid today, as attackers are most often targeted at users who are not sufficiently security-conscious, and even the best software cannot provide adequate security through the actions of these individuals if the user does not have the appropriate competencies.

People, who are not sufficiently security-conscious are especially at risk from increasingly sophisticated social engineering attacks, so by examining the attack frameworks and attack models of this technique, we can achieve the most effective prevention and avoidance. Of course, the importance of awareness raising and introduction into education should not be underestimated in this regard either.

The aim of my research was to investigate the possibilities of prosperity of protection against cyber threats, which have been detailed above. Regarding the analysis of empirical experiments and the prevention of social engineering attacks, the main question can be formulated as to whether data and information security, security awareness can potentially be increased along the lines of interest, personal, problem-oriented examples and implementation in education.

Keywords: **social engineering, data and information security, security awareness, data protection, cybersecurity, public service**

1. Bevezető

Az infokommunikációs technológiák rohamos terjedésével napjaink egyik legjelentősebb biztonsági kockázataként a kiberteret azonosíthatjuk. A nyilvánosságra kerülő, bejelentett kibertámadások száma drasztikusan növekszik, amely a trendek alapján várhatóan a privát, a vállalati és az állami szférában egyaránt jelentősen emelkedni fog. A támadók motivációi között szerepelhet többek között anyagi haszonszerzés, államok belpolitikai döntéshozatalának befolyásolása, kritikus infrastruktúrák elleni támadás, illetve a legkülönbözőbb bűncselekmények elkövetése.

A kibertámadásokkal szemben rendkívül nehéz védekezni, mivel annak költségei jelentősen magasabbak, mint a támadásoké. Az egyik legfontosabb és egyben legköltséghatékonyabb módja a védekezésnek a felhasználók kiberbiztonsági tudatosságának erősítése. Az internetezők adat- és információbiztonsági tudatosságának

szintje – függetlenül korosztálytól, nemtől, iskolai végzettségtől, beosztástól – nem nevezhető magasnak.

Ahogy a védelmi megoldások, úgy a támadások is egyre szofisztikáltabbak, komplexebbek, ezért a támadók elsősorban a rendszerek leggyengébb láncszemén, a nem kellően biztonságtudatos felhasználón keresztül igyekeznek hozzáférni a védett rendszerekhez. A szakirodalom az ilyen jellegű támadásokat social engineering támadásként definiálja. E támadási technikát egyaránt alkalmazzák a bűnözők, a terroristák és a hírszerzők céljaik elérése érdekében, ami rendkívül eltérő lehet, irányulhat információszerzésre, informatikai rendszer befolyásolására, dezinformálásra és számos egyéb tevékenységre.[3]

1.1. Social engineering

A social engineering fogalmának legjobb meghatározása Kevin Mitnick nevéhez köthető, amely szerint: „A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni."[4]

Egy social engineering támadás négy fázisból épül fel: információgyűjtés; kapcsolat kiépítése; kapcsolat kihasználása; támadás végrehajtása.[5]

A social engineering támadások alkalmával a támadó egy személy vagy szervezet azon információihoz akar hozzájutni, amelyek a számára nem elérhetők, és ezen információkhoz az út magán a személyen vagy a szervezet munkatársain át vezet. A támadó a támadás végrehajtása során a célpontról személyes információkat gyűjt, személyes kontaktusba elegyedik, beszélget, és bizalmat, neki kedvező hangulatot teremt. A támadó a célpont emberi magatartására támaszkodva (empátia, segítségnyújtás) kezd el tevékenykedni.[6]

A befolyásolás művészeteként is definiált social engineeringnek számos támadási modellt és módszertant tulajdoníthatunk.[7] A social engineering támadások keretrendszerének alapját a négyfázisú körciklus adja, míg a támadási keretrendszerek összehasonlításának az alapját a különböző támadási szcenáriók adják.[8]

A támadási modell tekintetében a támadók a kommunikációjuk jellegeként használhatnak direkt és indirekt modellt. A támadáshoz a social engineernek meg

[3] Bányász Péter – Bóta Bettina – Csaba Zágon: A Social Engineering jelentette veszélyek napjainkban. In Zsámbokiné Ficskovszky Ágnes (szerk.): *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében.* Budapest, Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 2019. 12–37.

[4] Kevin Mitnick – William L. Simon: *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker, Illustrated edition.* New York, Back Bay Books, 2012.

[5] Francois Mouton – Louise Leenen – H.S. Venter: Social Engineering Attack Examples, Templates and Scenarios. *Computers and Security,* 59. (2016), 186–209.

[6] Kevin D. Mitnick – William L. Simon: *The Art of Deception: Controlling the Human Element of Security.* John Wiley & Sons, 2003.

[7] Christopher Hadnagy: *Social Engineering: The Art of Human Hacking.* John Wiley & Sons, 2010.

[8] Katharina Krombholz et al.: Advanced Social Engineering Attacks. *Journal of Information Security and Applications,* 22. (2015), 113–122.

kell határoznia emellett a célpontot, a közeget, a célt, valamint a manipuláció alapját és technikáit, emellett el kell döntenie, hogy a támadás több lépcsőfokon keresztül valósuljon-e meg. Mindezek az alkalmazott modelltől függenek.[9]

1.2. Információbiztonság-tudatosság

Az információbiztonság és a social engineering kapcsolatáról elmondható, hogy a social engineer a célponttal – ideértendő a személy mint individuum, mint egy szervezet képviselője vagy mint egy csoport tagja – folytatott szociális interakciói során próbálja meg rábeszélni vagy megtéveszteni és végül meggyőzni az illetékes személyt, hogy egy konkrét kérést teljesítsen.

A kibertér mára információs társadalmunk integráns részét képezi.[10] Személyes és szakmai összefüggésben egyaránt a kibertér rendkívül hatékony eszközzé vált, és lehetővé teszi, hogy a legtöbb ember mindennapjait digitális tevékenységbe ültesse át. Elmondható azonban, hogy ez az életünkbe történő új behatás magával hozza az információbiztonság fontosságát is.[11]

A korszerű technológiákhoz való hozzáférés és használatuk széles körben elérhető bárkinek, ezért a kibertérben a tömegek megjelenésével együtt tapasztalhatjuk a humánalapú támadások szignifikáns növekedését is, azonban a kiberfenyegetések elleni védelemhez szükséges és már meglévő eszközök ismerete ennek ellenére hiányos.[12]

A kibertérben jelentkező veszélyek és kockázatok csökkentése szempontjából a legjelentősebb előrelépést akkor érhetnénk el, ha képzések, tanfolyamok, programok, szimulációk terén kezdenénk el felkészíteni az egyéneket. A megszerzett tudást a felhasználók hasznosíthatnák a mindennapi tevékenységük során és természetesen munkahelyi környezetükben.[13]

1.3. A potenciális veszélyekkel kapcsolatos tudatosság

Korunk új „olaja" az adat. Az adatokra napjainkra új iparágak épültek, amelyek azokat felhasználva teremtenek értékeket vagy profitot. Ugyan a cégek, vállalkozások a lehető legtöbb adatot próbálják begyűjteni a felhasználókról, hogy abból profilokat építsenek, azokat tovább értékesítsék, de Európában ez – a felhasználók javára – nem

[9] Bányász Péter: Social engineering and social media. *Nemzetbiztonsági Szemle,* 6. (2018), 1. 59–77.

[10] Tibor Farkas: Communication and Information Services – NATO Requirements, Part I. *Land Forces Academy Review,* 25. (2020), 4. 281–289; Tibor Farkas: Communication and Information Services – NATO Requirements, Part II. *Land Forces Academy Review,* 26. (2021), 1. 9–15.

[11] Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* 3. (2015), 2. 21–36.

[12] S. M. Furnell – P. Bryant – A. D. Phippen: Assessing the Security Perceptions of Personal Internet Users. *Computers & Security,* 26. (2007), 5. 410–417.

[13] Jemal Abawajy: User Preference of Cyber Security Awareness Delivery Methods. *Behaviour and Information Technology,* 33. (2014), 3. 237–248; Jemal Abawajy – Tai-hoon Kim: Performance Analysis of Cyber Security Awareness Delivery Methods. In Tai-hoon Kim et al. (szerk.): *Security Technology, Disaster Recovery and Business Continuity.* Berlin, Heidelberg, Springer, 2010. 142–148.

teljes mértékben triviális kérdés az évek óta hatályban lévő általános adatvédelmi rendeletnek (GDPR) köszönhetően.

Ahogy az infokommunikációs társadalmunkat egyre inkább behálózzák a különböző eszközök és technológiai vívmányok, úgy ezek teljesen új perspektívákat nyitnak a világ felé. Eszközeink segítségével szervezhetjük napjainkat, kapcsolatba léphetünk új vagy rég nem látott ismerőseinkkel, valamint teljesen új iparágak épülhetnek ki. Mindezek magukkal hozzák a magasabb szintű technológiához értő szakemberek képzésének szükségességét. Naivan úgy gondolhatjuk, hogy azáltal, hogy egyre többet használjuk ezeket a technológiákat és megfelelő szakembereket képzünk, alkalmazunk a cégeknél, az állami szektorban, legrosszabb esetben is autodidakta módon felismerjük – akár társadalmi szinten – a biztonságtudatosság hiányából fakadó kockázatokat és fenyegetettségeket. Ennek ellenére az emberek többsége továbbra is elszenvedője az imént felsorolt hiányosságoknak. E ránk leselkedő fenyegetések mértékének skálája a kis hatású adatvesztéstől egészen a katasztrofális gazdasági következményekig terjedhet. A kiindulópontot jelentheti például egy spam e-mail, amely egy kiberbűnözői csoporttól érkezett, és különböző kártékony kódokat alkalmazva lop el, korrumpál, vagy semmisít meg adatokat, akár jelentős mértékben.[14]

Az információbiztonság tekintetében a legjelentősebb tényező az emberek információbiztonság-tudatossága. E skálát meghatározhatjuk az alábbi szinteken:

- Alacsony szintű biztonságtudatosságú személyek: nem veszik figyelembe vagy közömbösen tekintenek a különböző biztonsági értesítésekre, valamint automatikusan elfogadnak minden feltételt az alkalmazások kezelésekor, weboldalak látogatásakor, illetve felcsatlakoznak az eszközeikről bármilyen nyílt hálózathoz titkosítás vagy anonimizálás nélkül (például WiFi-hez).
- Közepes szintű biztonságtudatosságú személyek: gondatlanságuk a technológia nem szakszerű alkalmazása mentén fejezhető ki.
- Magas szintű biztonságtudatosságú személyek: hasznosítják tudásukat a mindennapokban a kiberfenyegetettségek elkerülése érdekében, és képesek megelőző intézkedésekre az incidensek megelőzése céljából.

Az egyik legjelentősebb sérülékenységnek a különböző alkalmazások telepítésekor történő engedélymegadást, a webhelyeken történő információhozzáférés engedélyezését és a közösségimédia-oldalakon történő információmegosztást tekinthetjük.[15] A helyzetet az alacsony biztonságtudatossággal rendelkező személyek tekintetében tovább rontja, hogy a támadók leginkább ezt a csoportot veszik célba mint potenciális áldozatot, ugyanis ezek a hackerek ki tudják használni a különböző sérülékenységeket,

[14] Martti Lehto: Cyber Security Competencies – Cyber Security Education and Research in Finnish Universities. In Nasser Abouzakhar (szerk.): *14th European Conference on Information Warfare and Security, 2015.* Hatfield, The University of Hertfordshire, 2015. 179–188; Tóth András: Information-Sharing Challenges and Issues in Multinational Operations. *Land Forces Academy Review*, 25. (2020), 4. 307–316.

[15] R. S. Shaw et al.: The Impact of Information Richness on Information Security Awareness Training Effectiveness. *Computers & Education,* 52. (2009), 1. 92–100; Tóth András: International information security in hungary. In Ivan Majchút et al. (szerk.): *8. medzinárodná vedecká konferencia: National and International Security 2017.* Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2017. 548–557.

szoftveres hibákat és biztonsági hiányosságokat, amelyekről az ezen a szinten lévő felhasználók tudomást sem vesznek.[16]

A kibertérben történő jogsértések elszenvedői jelentős mértékben a biztonságtudatosság hiányából eredő személyekhez köthetők. Mára már elmondható, hogy a különböző vállalatok és az állami szektor széles körben folytat képzéseket és tudatosítási programokat, ám ezek közel sem nehezítik meg eléggé a kiberbűnözők tevékenységét, mindazonáltal a folyamatos tudatosítási kampányokkal az egyéni és szervezeti védettséget is növelhetjük. Az államigazgatás, a vállalati szereplők és a kibertérben tevékenykedő egyének tudatosításának legjobb módszere az, ha megmutatjuk, milyen módszerek alkalmazásával dolgoznak a támadók, és azoknak milyen következményei lehetnek, ezáltal fejlesztve a képességeket. A legfontosabb szempont e tekintetben az, hogy érthető legyen az átadni kívánt kompetencia a kiberbiztonság területén kevésbé jártas egyéneknek is.

2. A vizsgálat tárgya és a célkitűzések

A kutatás tudományos problémája a fentebb megfogalmazottakból ered, és alapjául két empirikus social engineering támadási kísérlet összevetése szolgál.

A kutatás célcsoportjának tagjai a magyar közszolgálat (a széles értelemben vett államigazgatás, Magyar Honvédség, Rendőrség, Katasztrófavédelem) iránt érdeklődő, vagy jelenleg e területeken a felsőoktatási képzésben részt vevők vagy jelenleg is ott dolgozók csoportja adta. Esetükben különösen fontos a megfelelő szintű biztonságtudatosság, hiszen a mindennapos munkavégzés során hozzáférnek – hozzáférhetnek majd – azokhoz a védett rendszerekhez, amelyekben a támadók számára értékes információk találhatók, vagy a döntéshozatalban való szerepük okán a befolyásolásuk értékes lehet. Ezek védelme és a munkatársak felkészítése az ország biztonságának érdekében is kiemelt fontosságú.[17]

Az empirikus kutatás kontrollcsoportjában az IT-biztonság, valamint az adat- és információbiztonság és social engineering iránt érdeklődő személyek szerepelnek.

A vizsgálat tárgyát a két csoport egy social engineering támadás esetén nyújtott viselkedésének elemzése adja.

A kutatás célkitűzése az volt, hogy tudományos vizsgálat során kimutatható-e összefüggés az adat- és információbiztonság, biztonságtudatosság és a social engineering támadások felismerése kapcsán a célcsoport és a kontrollcsoport teljesítménye között. Az érdeklődés felkeltése, a személyes, problémaorientált példák és az oktatásba történő bevezetés kapcsán vajon növelhető-e a személyek biztonságtudatossága?

[16] Tibor Farkas – András Tóth: Electronic warfare in full spectrum operation. In Milos Sotak – Mikulas Sostronek – Roman Beresik (szerk.): *Proceedings of the International Scientific Conference: New Trends in Signal Processing.* 2012. 181–188.

[17] Bányász Péter: A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében. *Szakmai Szemle,* 13. (2016), 1. 61–81; Tamás Szádeczky: Governmental Regulation of Cybersecurity in the EU and Hungary after 2000. *AARMS,* 19. (2020), 1. 83–93.

2.1. Kutatási hipotézisek

A kutatási téma feldolgozása során az alábbi hipotéziseket fogalmaztam meg:

H1. Az információbiztonsági tudatosságról alkotott önpercepció nem párosul valós biztonságtudatossággal kapcsolatos viselkedéssel.

H2. A célcsoportba tartozó személyek nagyobb valószínűséggel adják meg személyes adataikat, mint az adat- és információbiztonság iránt érdeklődő társaik.

H3. A kontrollcsoport tagjai kisebb eséllyel adják hozzájárulásukat olyan adatkezelési nyilatkozathoz, amelynek tartalma nem felel meg a törvényi előírásoknak.

2.2. Kutatási módszertan

A módszertan alapját a Tudás–Képesség–Viselkedés-modell és az információbiztonság humán aspektusa jelentette, emellett az elkészített kérdőíves felmérést tudományos statisztikai módszertannal (kereszttábla-elemzéssel) értékeltem ki, az SPSS Statistics szoftver segítségével. A kutatás során a felmérésekkor kitértem többek között az éberségen alapuló kísérletek elemzésére, valamint a social engineering támadási technika közvetlen, kétirányú kommunikációs modelljére

Fontos megjegyezni, hogy az itt felsorolt kutatási módszertanok mindegyike megfelel a hatályos jogszabályoknak. Vizsgálataim szigorúan az adatvédelmi elveknek megfelelő kutatásra korlátozódnak, amelynek célja az egyének és szervezetek védelmi képességeinek növelése.

A kutatási módszertan leírása egyaránt vonatkozik a célcsoportra, valamint a kontrollcsoportra.

3. Empirikus kutatások bemutatása

A célcsoport és a kontrollcsoport tekintetében is elmondható, hogy a social engineering támadási kísérletet azonos technikával, ám különböző eseményeken végeztem el. A rendezvények jellegéből adódóan különíthetjük el a két csoportot az adat- és információbiztonság, biztonságtudatosság kapcsán laikusokra (célcsoport) és érdeklődőkre (kontrollcsoport). Az alábbiakban részletezett felmérések összevetése által így megállapítható, hogy azonos körülmények között a csoportok tagjai milyen eredményeket mutattak fel.

3.1. Az empirikus kísérlet összeállítása

Mind a két esetben a social engineering támadási kísérlet hátterében egy ingyenes, ám feltételekhez kötött, kisebb-nagyobb értékű tárgyi nyereményeket kínáló sorsolás állt. A két empirikus kísérlet között a különbséget az jelentette, hogy a célcsoportnak több, a támadásra és a nyereményjáték valószerűtlenségére utaló jel állt rendelkezésére. Elmondható, hogy míg a kontrollcsoport az adatvédelmi nyilatkozatból tudta

kézzelfogható módon a támadást felismerni a támadó személyének – vagyis a kutatást végzőnek – attitűdjén, vagy az adatminimalizációs elvek figyelembevételének hiányán kívül, addig a célcsoportnak több lehetősége is volt felismerni a támadást, ezzel kompenzálva az esetleges szakmai hiányosságokat (ezek közé tartozott például az adatkezelési nyilatkozat szabadabb megfogalmazása).

Az alapvetően kérdőíven és kisebb, ezt követő interjúkon alapuló kísérlet magját egy négy részre osztható ív adta. Első oldalának felső részén a különböző rendezvényekkel kapcsolatos statisztikai jellegű kérdések, illetve egy, a kitöltő biztonságtudatossági önpercepciójára, valamint a jelszókezelésére vonatkozó kérdések szerepeltek. Az alsó felén volt található egy táblázat, amelybe a kitöltőnek különböző személyes adatait kellett/lehetett megadnia, egyéb kérdésekre kellett/lehetett válaszolnia, valamint itt szerepelt az adatvédelmi és hozzájáruló nyilatkozat is. A nyilatkozat a legkisebb mértékben sem volt a törvényi előírásokkal és az általános adatvédelmi rendelettel összhangban. Az aláírás alatt szereplő apróbetűs szöveg egyaránt vonatkozott a hozzájáruló személy nevében történő pénzfelvételre, csomagrendelésre és nyíltan tartalmazta a nyereményjáték valótlanságát is. Itt kell szót ejtenem arról, hogy személyes adatok valódi gyűjtésére nem került sor. A felső és az alsó részt egy preparált vonal választotta el, a támadási kísérlet befejezését követően pedig a hozzájáruló nyilatkozatot, valamint a személyes adatokat tartalmazó alsó részt a kitöltők minden esetben megkapták, míg a felső részen, ahol a statisztikai jellegű, jelszavakkal és biztonságtudatossági önpercepcióval kapcsolatos kérdések voltak, megtartottuk. Ezen felső laprész hátsó oldalán X-szel és pipával jelöltük azt, hogy az adott kitöltő mely kérdésekre válaszolt, mely személyes adatait adta meg, és hozzájárult-e a nyilatkozathoz aláírásával. A személyes adatok a két esetben vonatkoztak többek között a névre, életkorra, kapcsolati státuszra, e-mail-címre, telefonszámra, lakcímre és személyigazolvány-számra. A szenzitív jellegéből adódóan az elemzés tárgyát mindezek kapcsán utóbbi két személyes adat megadása, a biztonságtudatossági önpercepció, a jelszókezelési készségek és a nyilatkozat aláírása jelenti.

3.2. Módszertan szerinti elemzés

Ezen alfejezetekben részletezem a különböző módszertanok és modellek leírását, amelyek alapján a csoportokat vizsgáltam, és ismertetem azok eredményét. A leíró statisztika és a különböző kutatásmódszertani elemek mellett bemutatom az empirikus kutatások kereszttábla általi elemzését, amelyet SPSS Statistics szoftverrel készítettem. Meghatározom emellett a hipotézisek alátámasztására vagy megdöntésére vonatkozó eredményeket.

3.2.1. Éberségen alapuló kísérletek

A kísérlet elemzésének tekintetében beszélhetünk az úgynevezett éberségen alapuló kísérletről. Ennek lényege, hogy a kísérlet során arra vagyunk kíváncsiak, hogy a személyek mennyire képesek dinamikusan eloszlatni figyelmüket, a körülöttük zajló

dolgokat milyen valószínűséggel veszik észre, figyelnek-e a kontextusra, gyanakvásra okot adó dolgokra.[18]

Jelszavak és e-mailek

A célcsoport és a kontrollcsoport tagjainak is fel lett téve két különböző kérdés: mi az e-mail-címük és a számukra ideális jelszó.

Megvizsgáltam, hogy a különböző csoportokban a „Milyen az Ön számára a legideálisabb jelszó? Kérjük, mondjon rá példát!" kérdésre valóban adtak-e konkrét jelszópéldát.

Elmondható, hogy a kontrollcsoport tagjai közül 0%, azaz senki nem mondott konkrét jelszóra példát.

A célcsoportról elmondható, hogy a kitöltők közül több konkrét jelszóra érkező példa érkezett, vagyis a kitöltők több mint 33%-a megválaszolta azt. E kitöltők mindegyike megadta az e-mail-címét is, amely további biztonságtudatossági kérdéseket vethet fel a megadott ideális jelszópéldával együttesen.

Jelszóemlékeztető és e-mailek

A célcsoport körében szerepelt egy kérdés, amely arra vonatkozott, hogy rendelkeznek-e a kitöltők jogosítvánnyal, autóval, illetve ehhez kapcsolódóan arra, hogy milyen autón tanultak vezetni – mint egy tetszőlegesen választott tipikus jelszóemlékeztető kérdés.

Elmondható, hogy az összes kitöltő közül, aki rendelkezett jogosítvánnyal, mindenki válaszolt erre a kérdésre, és közülük mindenki megadta az e-mail-címét is kivétel nélkül, mikor pedig fel lett téve a kérdés, hogy asszociáltak-e a jelszóemlékeztetőre, arra senki nem válaszolt igennel. A kérdés feltevését követően viszont többen megerősítették, hogy találkoztak már ezzel a jelszóemlékeztető kérdéssel, és volt, hogy alkalmazták.

Hozzájárulás az adatvédelmi nyilatkozathoz

Ahogy korábban részleteztem, az adatvédelmi nyilatkozat nem a jogszabályi előírásoknak megfelelően volt megfogalmazva, és a két csoport között a nyilatkozat kapcsán alapvető különbség volt, hogy a célcsoportnak jóval szabadabban volt megfogalmazva az, több utaló jelet tartalmazva.

A célcsoportról ennek ellenére elmondható, hogy azok aránya, akik észrevették a hamis nyilatkozatot, mindössze a kitöltők 12%-át tette ki, két kitöltő viszont ennek ellenére is hozzájárult az adatai kezeléséhez, hogy a nyereményjátékon részt vehessen. Mivel mások nem olvasták el az adatvédelmi nyilatkozatot, így nincsenek arra vonatkozó információim, hogy elolvasás után is aláírták volna-e azt.

A kontrollcsoportról a hozzájárulás kapcsán elmondható, hogy a kitöltők mindössze 9%-a tagadta meg az adatvédelmi nyilatkozat aláírását, amely kevesebb a célcsoport eredményénél, viszont közülük három személy olvasta el az adatvédelmi nyilatkozatot, ami arányaiban nagyobb a célcsoport teljesítményénél. Elolvasás melletti aláírásra itt nem került sor.

[18] Matthew L. Jensen et al.: Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Journal of Management Information Systems,* 34. (2017), 2. 597–626.

3.2.2. Leíró statisztikák és attitűd

A leíró statisztikák által megállapíthatjuk, hogy a szenzitív adatok megadásának megtagadásában a kontrollcsoport jobban szerepelt. Személyigazolvány-számuk és lakcímük megadását 20%-kal nagyobb valószínűséggel tagadták meg, mint a célcsoport tagjai.

Ahogy az előző alfejezetben leírtam, a hozzájáruló nyilatkozatot arányaiban többen tagadták meg a célcsoport tagjai közül, viszont számukra több utaló jel állt rendelkezésre, valamint a mérleg nyelvét kiegyenlíti továbbá, hogy a kontrollcsoport tagjai közül arányaiban többen olvasták el a nyilatkozatot, illetve nem került sor a nyilatkozat elolvasását követő aláírásra, amely két esetben a célcsoportra jellemző volt.

Összességében tehát elmondható, hogy sem a célcsoport, sem a kontrollcsoport nem nyújtott kiemelkedő teljesítményt az információbiztonság terén, viszont levonhatjuk azt a konzekvenciát, hogy a kontrollcsoport attitűdjét vizsgálva jóval nehezebb a social engineer tevékenysége. Emellett fontos kiemelnünk, hogy nem adnak olyan nagymértékben visszaélési lehetőséget vagy kihasználható humánalapú sérülékenységet a támadóknak az elvégzett értékelések alapján, mint laikus társaik, ami a személyes kommunikáció során volt tapasztalható.

Ezen a ponton a H2. hipotézisemet alátámasztottam. Igazoltam, hogy az információbiztonsági szempontból laikus emberek legalább kétszer nagyobb valószínűséggel adják meg személyes adataikat, mint az információbiztonság iránt érdeklődő személyek.

A H3. hipotézisem az éberségen alapuló teszt elemzése során megdőlt, ugyanis az információbiztonság iránt érdeklődő személyek nagyobb valószínűséggel írják alá az adatvédelmi nyilatkozatot, mint az információbiztonság tekintetében laikus emberek, noha az utóbbi csoportba tartozók kisebb valószínűséggel is olvassák el annak tartalmát. (A hipotézisek értékelésekor természetesen nem hivatkozhatok a kommunikációra és az adatok kinyerésének nehézségére, amely a mérleget az érdeklődők felé döntené.)

3.2.3. A támadási kísérlet modellje

A korábban elméleti jelleggel bemutatott social engineering támadási modell gyakorlati megvalósítása az alábbiak szerint történt:

A célcsoporton, illetve a kontrollcsoporton is egyaránt direkt, kétirányú kommunikációs modellt alkalmaztunk.

A támadáshoz a social engineernek meg kell határoznia mindezek mellett a célpontot, a közeget, az elérendő célt, valamint a manipuláció alapját és a technikákat, emellett el kell döntenie, hogy a támadás több lépcsőfokon keresztül valósuljon-e meg.

Mind a két empirikus kutatásról elmondható, hogy:

- a social engineer személy;
- a célpont személy;
- a manipuláció alapját adja:
  - szimpátia: a rendezvények hangulata, a nyereményjáték és a személyes attitűd által;

  - elkötelezettség vagy következetesség: a nyereményjátékon való részvétel feltételeként volt szükséges megadni a kért adatokat, amelyek kompenzációja a nyeremény;
  - viszonosság/kölcsönösség: mind a két esetben átadtak kis értékű ajándékokat a rendezvényről, illetve a statisztikai felmérés eredménye lehetett a sorsoláson való részvétel;
- hatóság: részben beszélhetünk erről az empirikus kutatással kapcsolatban. Elmondható, hogy a kitöltők minden esetben azt hihették, hogy a szervezők által finanszírozott alkalmazottak vagy önkéntesek vagyunk az esemény javítását szolgáló feladatlapok kitöltésének tekintetében;
- technika szempontjából adathalászatról beszélhetünk. Megvalósult egyrészt az úgynevezett pretexting (ürügy, amely alapul szolgál a támadó számára értékes információk kiadásának igénylésére, ezúttal a személyes adatok elkérésére az áldozattól annak érdekében, hogy a sorsoláson be lehessen azonosítani). Másrészt beszélhetünk baitingről („beetetésről", vagyis hamis ígéretekkel lettek az emberek becsapva, az áldozatok mohóságát vagy kíváncsiságát kihasználva);
- cél a személyes adatok megszerzése és a hozzájáruló nyilatkozatnak az áldozat által történő aláírása volt;
- a közeg a személyes kapcsolatfelvétel volt;
- a támadás egy lépcsőfokban valósult meg.

3.3. Az empirikus kutatások elemzése

A kutatás elemzésének gerincét a két rendezvényen azonos módon felvett adatok összehasonlítása adja. Idetartozik a biztonságtudatossággal kapcsolatos önpercepció, az adatvédelmi nyilatkozathoz való hozzájárulás, illetve a személyes adatok megadása (személyigazolvány-szám, lakcím).

A leíró statisztikák alapján elmondható, hogy a célcsoport tagjai rosszabb eredményeket értek el a kontrollcsoportban szereplő társaikhoz képest. Amennyiben a szenzitív adatnak számító lakhelyet vagy személyigazolvány-számot tekintjük, úgy deklarálhatjuk a tényt, hogy a téma iránt érdeklődők jobban teljesítettek laikus társaiknál.

A kereszttábla-elemzés eredményeképpen a Khí-négyzet próba elemzésével szignifikáns összefüggéseket kutattam, majd amennyiben találtam összefüggést, a Cramer's V együttható vizsgálatának tekintetében, az asszociációs mérőszám által meghatároztam az összefüggés mértékét. Ezek gyakorlati magyarázatát és jelentőségét az első eredmény elemzésénél adom meg.

Kutatási célkitűzéseim tekintetében vizsgáltam azt, hogy az adott rendezvényen való részvétel összefüggésben van-e azzal, hogy az egyének milyen gyakorisággal adnak meg magukról információt.

Eredményként a rendezvényen történő megjelenés és a személyazonosító igazolvány megadására való hajlandóság között szignifikáns összefüggést véltem felfedezni. Khí-négyzetének (X^2) megfigyelt értéke 5,921, ahol a kétoldali szignifikanciaszintjének értéke 0,015, tehát megállapítom, hogy a két változó között az összefüggés

szignifikáns. A kapcsolat erősségét Cramer's V (C V) segítségével vizsgáltam, ugyanis ez tekinthető az egyik legmegbízhatóbb mutatónak. A C V egy asszociációs együttható, amely a két nominális változó közötti szorosságot mutatja meg. A C V értéke 0 és 1 közötti intervallumú, a 0-hoz való közelség függetlenséget, az 1-hez való közelség erős kapcsolatot jelent. Vizsgálatomban a Cramer's V mutató megfigyelt értke 0,214, kétoldali szignifikanciaszintjének értéke szintén 0,015. A 0,214-es érték azonban alacsony korrelációra utal a két változó esetében.

A rendezvényen történt megjelenés és a hozzájáruló nyilatkozat összefüggésében elmondhatom, hogy X^2 megfigyelt értéke 0,308, amelynek kétoldali szignifikanciaszintjének értéke 0,579, tehát megállapíthatom, hogy a két változó között nincs szignifikáns összefüggés.

A rendezvényen történt megjelenés és a lakhely megadása összefüggésében elmondhatom, hogy X^2 megfigyelt értéke 6,926, ennél a kétoldali szignifikanciaszintjének értéke 0,008, tehát megállapíthatom, hogy a két változó között az összefüggés szignifikáns. Vizsgálatomban a C V mutató megfigyelt értéke 0,236, kétoldali szignifikanciaszintjének értéke szintén 0,008. A 0,236-os érték azonban alacsony korrelációra utal a két változó esetében.

Ezen a ponton eredményeimmel szintén megerősítettem a H2. hipotézisemet, ugyanis elmondhatom, hogy a kontrollcsoport tagjai között jóval nagyobb az információbiztonság szintje, hiszen szenzitív (személyazonosító szám, lakhely) adataik kiadását jóval nagyobb mértékben tagadják meg.

Az információbiztonsági tudatosságról alkotott önpercepció mindkét eseményen történő vizsgálata és az adatvédelmi nyilatkozat aláírásának összefüggésében elmondhatom, hogy a X^2 megfigyelt értéke 2,909, amelynek kétoldali szignifikanciaszintjének értéke 0,088, tehát megállapíthatom, hogy a két változó között nincs szignifikáns összefüggés.

Ezen a ponton bizonyítottam a H1. hipotézisemet, vagyis azt, hogy az információbiztonsági tudatosságról alkotott önpercepció nem párosul valós biztonságtudatossággal kapcsolatos viselkedéssel.

4. A kutatás eredményei

A megfogalmazott hipotéziseimmel kapcsolatban az alábbi téziseket állapítom meg:

T1. Bizonyítottam, hogy a laikusok és az információbiztonság iránt érdeklődő személyek, bár biztonságtudatosnak gondolják magukat, a cselekedeteik alapján ez az önpercepció nem helytálló.

T2. Igazoltam, hogy az információbiztonsági szempontból laikus emberek legalább kétszer nagyobb valószínűséggel adják meg személyes adataikat, mint az információbiztonság iránt érdeklődő személyek.

T3. Bizonyítottam, hogy az információbiztonság tekintetében laikus személyek nagyobb valószínűséggel tagadják meg az adatvédelmi nyilatkozat aláírását, még akkor is, ha kisebb valószínűséggel is olvassák el annak tartalmát, ezzel megdöntve H3. hipotézisemet.

5. Összegzett következtetések

Kutatásom fontosságát az exponenciálisan növekvő, egyre fejlettebb humánalapú támadások adják, amelyek az államigazgatási szektor tisztségviselőire és a hivatásos szervek munkatársaira fokozottan érvényesek. A kutatás célja ezáltal az volt, hogy megállapítsam, a biztonságtudatosság növelhető-e az érdeklődés, a problémacentrikus, személyes érintettségen alapuló példák és kísérletek elvégzése által. Fontosnak találtam továbbá a támadási modellek, stratégiák, keretrendszerek és a felismerési lehetőségek ismertetését a védelmi képességek javítása érdekében.

Összegezve a két empirikus kutatást megállapítom, hogy az adat- és információbiztonság-tudatosság, valamint a kiberbiztonsággal kapcsolatos képességek növelhetők az érdeklődés megteremtését követően, ezzel elősegítve az esetleges sajátos, autodidakta elsajátításra történő buzdítást, vagy még jobb esetben az aktív oktatásban történő önkéntes fejlesztést.

Az empirikus kutatások kapcsán megállapítom, hogy az információbiztonság iránt érdeklődők az adataik védelmében sokkal tudatosabbak voltak. A célcsoportról pedig: a biztonságtudatosság optimumának tekinthető szintet nem érte el. A szubjektív, személyes tapasztalat és a leírt kutatási eredmények, valamint a személyek attitűdjének tekintetében elmondható, hogy a kontrollcsoport nagyságrendekkel biztonságtudatosabb.

Végső következtetésként megállapítom, hogy a biztonságtudatosság iránti érdeklődés megjelenésével párhuzamosan növelhetők az egyének képességei is.

Felhasznált irodalom

Abawajy, Jemal: User Preference of Cyber Security Awareness Delivery Methods. *Behaviour and Information Technology,* 33. (2014), 3. 237–248. Online: https://doi.org/10.1080/0144929X.2012.708787

Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* 3. (2015), 2. 21–36. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1974/1259

Bányász Péter: A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében. *Szakmai Szemle,* 13. (2016), 1. 61–81. Online: http://real.mtak.hu/47801/1/A_kozossegi_media_szerepe_a_lelektani_mu.pdf

Bányász Péter: Social engineering and social media. *Nemzetbiztonsági Szemle,* 6. (2018), 1. 59–77. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1511/829

Hadnagy, Christopher: *Social Engineering: The Art of Human Hacking.* John Wiley & Sons, 2010.

Bányász Péter – Bóta Bettina – Csaba Zágon: A Social Engineering jelentette veszélyek napjainkban. In Zsámbokiné Ficskovszky Ágnes (szerk.): *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében.* Budapest, Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 2019. 12–37. Online: https://doi.org/10.37372/mrttvpt.2019.1.1

Farkas, Tibor: Communication and Information Services – NATO Requirements, Part I. *Land Forces Academy Review,* 25. (2020), 4. 281–289. Online: https://doi.org/10.2478/raft-2020-0034

Farkas, Tibor: Communication and Information Services – NATO Requirements, Part II. *Land Forces Academy Review,* 26. (2021), 1. 9–15. Online: https://doi.org/10.2478/raft-2021-0002

Farkas, Tibor – András Tóth: Electronic warfare in full spectrum operation. In Milos Sotak – Mikulas Sostronek – Roman Beresik (szerk.): *Proceedings of the International Scientific Conference: New Trends in Signal Processing.* 2012. 181–188.

Furnell, S. M. – P. Bryant – A. D. Phippen: Assessing the Security Perceptions of Personal Internet Users. *Computers & Security,* 26. (2007), 5. 410–417. Online: https://doi.org/10.1016/j.cose.2007.03.001

Jemal Abawajy – Tai-hoon Kim: Performance Analysis of Cyber Security Awareness Delivery Methods. In Tai-hoon Kim – Wai-chi Fang – Muhammad Khurram Khan – Kirk P. Arnett – Heau-jo Kang – Dominik Ślęzak (szerk.): *Security Technology, Disaster Recovery and Business Continuity.* Berlin, Heidelberg, Springer, 2010. 142–148. Online: https://doi.org/10.1007/978-3-642-17610-4_16

Jensen, Matthew L. – Michael Dinger – Ryan T. Wright – Jason Bennett Thatcher: Training to Mitigate Phishing Attacks Using Mindfulness Techniques. *Journal of Management Information Systems,* 34. (2017), 2. 597–626. Online: https://doi.org/10.1080/07421222.2017.1334499

Krombholz, Katharina – Heidelinde Hobel – Markus Huber – Edgar Weippl: Advanced Social Engineering Attacks. *Journal of Information Security and Applications,* 22. (2015), 113–122. Online: https://doi.org/10.1016/j.jisa.2014.09.005

Lehto, Martti: Cyber Security Competencies – Cyber Security Education and Research in Finnish Universities. In Nasser Abouzakhar (szerk.): *14th European Conference on Information Warfare and Security, 2015.* Hatfield, The University of Hertfordshire, 2015. 179–188.

Mitnick, Kevin D. – William L. Simon: *The Art of Deception: Controlling the Human Element of Security.* John Wiley & Sons, 2003.

Mitnick, Kevin – William L. Simon: *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker.* Illustrated edition. New York, Back Bay Books, 2012.

Mouton, Francois – Louise Leenen – H.S. Venter: Social Engineering Attack Examples, Templates and Scenarios. *Computers and Security,* 59. (2016), 186–209. Online: https://doi.org/10.1016/j.cose.2016.03.004

Shaw, R. S. – Charlie C. Chen – Albert L. Harris – Hui-Jou Huang: The Impact of Information Richness on Information Security Awareness Training Effectiveness. *Computers & Education,* 52. 1. (2009), 92–100. Online: https://doi.org/10.1016/j.compedu.2008.06.011

Szádeczky, Tamás: Governmental Regulation of Cybersecurity in the EU and Hungary after 2000. *AARMS,* 19. (2020), 1. 83–93. Online: https://doi.org/10.32565/aarms.2020.1.7

Tóth András: *International information security in hungary.* In Ivan Majchút – Vladimír Andrassy – Štefan Ganoczy – Michal Hrnčiar – Ondrej Kredatus – Gabriela Kredatusová – Jakub Sasarák – Juraj Šimko – Jaroslav Varecha – Lubomír Belan – Stanislav

Morong (szerk.): *8. medzinárodná vedecká konferencia: National and International Security 2017.* Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2017. 548–557.

Tóth András: Information-Sharing Challenges and Issues in Multinational Operations. *Land Forces Academy Review,* 25. (2020), 4. 307–316. Online: https://doi.org/10.2478/raft-2020-0037