DOI: 10.38146/BSZ.2023.1.6

21. századi social engineering támadások, védekezés és szervezeti hatások Európában

21st century social engineering attacks, defence and organisational impacts in Europe

Jagodics Ibolya
menedzser
Ebner Stolz Mönning Bachem Partnerschaft mbB
jagodicsibolya@gmail.com

Kollár Csaba
Dr. PhD, tudományos főmunkatárs, műhelyvezető
Óbudai Egyetem,
Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar,
Mesterséges Intelligencia Műhely
kollar.csaba@uni-obuda.hu

Absztrakt

Cél: Napjainkra megkérdőjelezhetetlenné vált, hogy a siker és túlélés záloga az idő és az információ. Különösen igaz ez az Európában működő szervezetekre, melyek célpontjai a social engineering támadásoknak. Kutatásunk tényfeltáró jellegéből adódóan a következő három területre fókuszálunk: 1) Milyen területeket és milyen mértékben érintettek a social engineering támadások? 2) Milyen tapasztalatokat szereztek a megtámadott szervezetek, hogyan védekeztek, és miként csökkentették a veszteségeket? 3) Megfigyelhető-e hasonlóság a szervezetek védekezési és felkészülési technikáiban?

Módszertan: E kérdések alapján állítottuk össze kérdőívünket, melyet online környezetben 561 válaszadó töltött ki.

Megközelítések: A tanulmány elméleti fejezetében áttekintjük a releváns szakirodalmat, továbbá a vizsgálatban szereplő modern technikákat, eszközöket, és az ezekkel elérhető social engineering támadásokat. A kutatási fejezetekben bemutatjuk a felmérés körülményeit, az elemzési módszert és a feldolgozás során feltárt eredményeket.

Érték: Mindezek alapján összegzés és következtetés útján javaslatokat fogalmazunk meg a szervezetek információbiztonságának fejlesztésével kapcsolatban.

Kulcsszavak: szervezetek, hatások, biztonság, támadás, védekezés, social engineering

Abstract
Aim: For today, it has become unquestionable that time and information are the key to success and survival. Especially in case of organisations operating in Europe, which are the target of social engineering attacks. As our research is a fact-finding nature we focus on the following 3 areas; 1) What fields and to what extent are social engineering attacks affected? 2) What experiences did the attacked organizations gain, how did they defend themselves, and how did they reduce losses? 3) Can there be similarities in the defense and preparation techniques of organizations? Which sectors have been affected by social engineering attacks?
Methodology: Based on these questions we generated our questionnaire, that was filled out by 561 respondents.
Findings: In the theoretical chapter of the study, we will review the relevant literature. Furthermore, the modern techniques, tools, and social engineering attacks available with them are included in the study. In the research chapters, we present the circumstances of the survey, the method of analysis and the results revealed during processing.
Value: On this basis, we make recommendations for improving the information security of organizations by summary and conclusion.

Keywords: organizations, impacts, security, attack, defense, social engineering

Bevezetés

A 21. században felértékelődött az információk megszerzése, s erre újabbnál újabb technikák látnak napvilágot. Ezek közül a social engineering módszereket helyeztük jelen tanulmány fókuszába, annak köszönhetően, hogy ezek során a támadók az elérhető szakirodalom által megfogalmazott emberi tényező gyengeségét, illetve a technológia használatát helyezik célkeresztbe. A social engineering egy információ megszerzésére irányuló technika, mely az egyének kihasználásán, megtévesztésén, manipulálásán alapul. Mitnick könyvében az alábbiak szerint fogalmazta meg a social engineeringet: „*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*.” (Mitnick & Simon, 2002). Jelen tanulmányunkban erre a definícióra támaszkodunk.

A social engineer emberi tulajdonságokkal él vissza – mint például a jószándék, a hiszékenység, a naivitás, a sebezhetőség, a fáradtság, a segítőkészség stb. – technikai eszközök és manipulációs, valamint befolyásoló technikák segítségével (Deák, 2019a). A támadások célja az információk megszerzése, módosítása, törlése, a rendszerek sebezhető pontjainak feltérképezése, jogosulatlan hozzáférések alkalmazása vagy komplex esetekben későbbi kibertámadások előkészítése is lehet. Fontos megjegyezni, hogy az információszerzés alapvetően irányulhat visszaélések megvalósítására, ugyanakkor saját információk védelmére is (Haig, 2018). A social engineering módszerek etikus hackerek esetében gyakorta alkalmazásra kerülnek a szervezetek esetében annak érdekében, hogy próbára tegyék működésüket, alkalmazottjaikat, ezekkel megállapíthassák a szervezet sérülékeny pontjait, kockázatokat azonosíthassanak, majd valós támadás esetén ezekre reagálva csökkenteni tudják a várható veszteségeket. A social engineer módszerei pszichológiai és műszaki vonatkozásúak is lehetnek, hiszen a social engineer az emberi természet kihasználását veszi alapul azért, mert a fejlett informatikai rendszereket végtére is emberek használják, kezelik, a hozzáférésüket aktiválják (Dub, 2021). A támadó ilyen jellegű stratégiája összetett (Bányász, Bóta & Csaba, 2019), mivel a támadáshoz szükséges információt szerezni az informatikai rendszerről, a célpontról, a működésről, illetve folyamatokról, meg kell tervezni és szervezni. Tehát a támadó időt, energiát, tudást fektet minden megkezdett akciójába, tájékozott és jól informált. Ebből kiderül egyben az is, hogy nem feltétlen szükséges, hogy magas szintű IT tudással, vagy akár programozói képességekkel rendelkezzen. Így intelligenciája és emberismerete által egy IT fejlesztői tudással már eredményesen tevékenykedhet felkészültsége révén. A szervezetek számára sajnos a megelőző intézkedések, a védekezés költségesebb, mint az esetleges elszenvedett károk realizálása. Összegezve megállapítható, hogy az adat és információbiztonság gyakran nem a technikai berendezések színvonalától, hanem a humán tényezőktől, a munkavállalók adat- és információbiztonság-tudatosságától függ (Kollár, 2018).

A korszerű technológiáknak köszönhetően az információs társadalom tagjai egyre több felületen, és egyre gyorsabb ütemben élik életüket a kényelem és az elérhetőség érdekében. Előfordulhat az is, hogy az áldozatok nincsenek tisztában azzal, hogy részesei voltak, hozzájárultak egyes akciókhoz, hiszen néhány technikai információszerző tevékenység nem okoz nyilvánvaló károkat, csupán egy rejtett program keretében figyeli a szervezet vagy áldozat aktivitását, különböző adatokat gyűjt, megfigyelést végez, viselkedést elemez. Ilyenek lehetnek a kártékony programok vagy „malware”-ek is, amelyek típustól függően lassíthatják a hálózati és belső rendszert, kárt okozhatnak tevékenységük során.

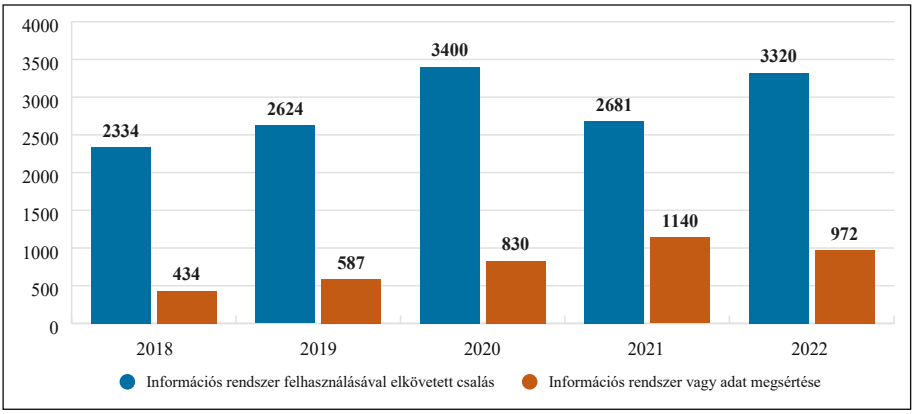
Az esetek túlnyomó többségében ezek a programok a felhasználók tudta vagy engedélye nélkül aktiválódnak a rendszerekben, ezek lehetnek többek között trójai programok, vírusok, kémprogramok, zsarolóvírusok, billentyűzet naplózók stb. Az adathalászat vagy phishing módszer arra alapul, hogy a támadó a felhasználókat valamilyen elektronikus csatornán keresztül, például e-mailben, szalagcímhirdetésekben látszólag valósnak tűnő, de hamis weboldalra irányítja, ahol célja bizonyos információk kicsalogatása (Deák, 2019b).

Az erőteljes technológiai fejlődés eredményeként a www.wearesocial.com weboldalon[1] elérhető 2022 februárjában (2022. 02. 15.) készült globális riport szerint Magyarországon a 9,62 milliós népességből 8,56 millió, a magyar lakosság 89%-a internetfelhasználó jelenleg, amely az egy évvel korábbi elemzés adataihoz mérten 265 000 felhasználóval, tehát 3,2%-kal emelkedett meg. Ugyanez a riport a leglátogatottabb közösségi oldalak között a www.google.com-ot első helyezettként mutatja 142 millió, a www.facebook.com-ot másodikként, 78,9 millió, a www.youtube.com-ot harmadikként, 43,4 millió látogatóval. Ez alapján érdekes tény, hogy a www.informationisbeautiful.com weboldalon elérhető a világ legnagyobb adatokkal való visszaélései és hackelései között ezen szolgáltatók kifejezetten magas számú felhasználóinak adataival kapcsolatos visszaélésekben érintettek. A következőkben a fentebb említett adatforrásokra hivatkozva ezek közül néhány releváns példát mutatunk be. 2021 márciusában a Facebook – sokadik alkalommal – 533 millió felhasználójának adatait szivárogtatta ki. A T-Mobile 2021 augusztusában szenvedett el magasan szofisztikált hacker támadást, melynek következtében ügyfeleinek 40 millió személyes adatát lopták el. A Microsoft 250 millió ügyféladatát tették közzé jelszóvédelem nélkül 2020 januárjában, mely akció 2005 és 2019 között történt (Winder, 2020). A Google+ – szintén sokadik alkalommal – 2018 decemberében 52,5 millió felhasználójának adatait veszítette el, melynek eredményeképpen véglegesen le is állították a felhasználói kiadást.

Ennek nyomán a Belügyi Statisztikai Rendszer online elérhető statisztikái szerint (bsr.bm.hu) a Büntető Törvénykönyv megfelelő paragrafusai szerinti besorolás alapján a 2018. július és 2022. április közötti időszakra Magyarország területén az „információs rendszer vagy adat megsértése” tétel esetén összesen 10 702 db bűncselekményt regisztrált.

1 Az oldal a közösségi média teljes körű elemzését végzi, mely az online média és közösségi magatartás vizsgálatát követi világszerte az érdeklődő magánszemélyek és vállalkozások számára.

1. számú ábra: *Regisztrált visszaélések száma 2018–2022*



Forrás: Bűnügyi Statisztikai Rendszer adatai alapján a szerzők saját szerkesztése.

Az ábra szerkesztése során a Bűnügyi Statisztika Rendszer által rendelkezésre bocsátott adatokon korrekciót hajtottunk végre és arányosítottuk annak érdekében, hogy a 2018. július előtti és a 2022. február utáni időszak elemzését egyszerűbbé tehessük. Ehhez a 2018. július 1-től december 31-ig tartó időszakra regisztrált 2334 darab esetszámát az információs rendszer felhasználásával elkövetett csalás, illetőleg a 217 darab esetszám az információs rendszer vagy adat megsértése paragrafusok alá sorolt adatokat kettővel felszoroztuk, feltételezve, hogy a 2018. év júliusáig is hasonló számú visszaélések zárulhattak le. Ugyanígy a 2022. március 1-jéig elérhető 830 darab esetszámot az információs rendszer felhasználásával elkövetett csalások esetében, illetve a 243 darab számú esetet az információs rendszer vagy adat megsértése esetében a teljes évre vetítve négyszer szoroztuk fel. Mivel a Bűnügyi Statisztikai Rendszer a lezárt esetek számát jelöli, így felhívjuk a kedves olvasó figyelmét a statisztika, illetve a kimutatás utánkövető jellegére.

Az Interpol honlapján (www.interpol.int) elérhető nyilvános jelentések kiemelik a pénzügyi bűnözésre mutató adatok között, hogy az üzleti elektronikus levelezésen keresztül elkövetett visszaélések globálisan már 2017-ben 676 millió, majd 2018-ra már 1,25 milliárd dollár értékű csalást tettek ki (Interpol, 2022).

Társadalmi környezet

Napjaink információs társadalmában már közhelynek mutatkozik a tény, hogy minden területen veszély leselkedik ránk magánszemélyként, illetve a különböző

szervezetekre (egyéni és társas vállalkozásokra, nonprofit szervezetekre, állami és kormányzati intézményekre), amellyel kapcsolatban állunk akár alkalmazottként, akár ügyfélként. A dinamikus technológiai fejlődés nemcsak az innovációval ajándékozott meg bennünket, hanem – mint minden érem két oldalaként – az újítások számos hátrányt is magukkal hoztak. Az említett fejlődés robbanásszerűen érte el a gazdasági, társadalmi rétegeket, melyre a felkészültség hiányosnak volt mondható ilyen ütemű változások mellett (Dyson, 1998). Rövid idő alatt ismertük meg az internetet, majd vált a mindennapi életünk részévé, ahol mára már a kapcsolattartás, ügyintézés, munkavégzés, vásárlás a legtermészetesebb események. Ez a hirtelen megnövekvő felhasználói igény mind technikai, mind humán oldalról megközelítve ismertette meg velünk például a „big data" vagy „felhő" fogalmát, a jelszavak létjogosultságát különböző általunk használt online felületeken, közösségi oldalakon (Haig, 2018). Lassan beláttuk, hogy az információ és idő párosa felbecsülhetetlen értéket képvisel, mi több elengedhetetlen feltétele a mindennapi életben való boldogulásnak. Majd ráébredtünk, hogy az adataink – közöttük a legszemélyesebb információkkal – az online világba kerültek. Az általunk használt közösségi oldalakon bármely rég elfeledett ismerősünkkel megvalósult ismét a kapcsolattartás, megosztottuk életünk részleteit akár a beszélgetések, akár a megosztott fényképek által (Jóri, 2012). Eltűntek a korábban ismert fizikai határok, korlátok és a távolságok. Ezzel együtt kezdtük megtapasztalni azt is, hogy a korábban ismert visszaélési formák és technikák igazodtak a technológiai változásokhoz, és egyre inkább találkoztunk online visszaélésekkel. A megosztott információk eljutottak nem csupán az ismerőseinkhez, de azokhoz is, akik azt szándékosan vagy véletlenül felhasználhatták saját vagy rosszindulatú cselekedeteikhez. A jog a következők szerint ideje korán próbált szabályozások által biztonságot nyújtani a személyeknek (Jóri, 2005).

Releváns adatvédelmi jogszabályok

Magyarországon az 1949. évi XX. törvény a Magyar Köztársaság Alkotmánya 59. § (1) helybenhagyta a személyes adatok védelméhez való jogot. A törvény 2012. január 1-jén hatályát veszítette, a magyar állampolgárok számára azonban a jog továbbra is életben maradt, majd az Országgyűlés 1992. november 17. napján közzétette a 1992. évi LXIII. adatvédelmi törvényt, amely a személyes adatok védelméről és a közérdekű adatok védelméről szóló útmutatás. Ennek 2004. január 1-jén hatályba lépett módosítása tartalmazta a 95/46/EK európai parlamenti és tanácsi irányelvet, melyet 1995. október 24-én elfogadtak. Ez

tulajdonképpen a 2011. évi CXII. információs törvény megfelelője; amely az információs önrendelkezési jogról és az információszabadságról szól. Az Európai Parlament és a Tanács (EU) 2016/679 rendelete 2016. április 27. napján hatályon kívül helyezte a 95/46/EK rendeletet, és garantálta a továbbiakban azt, hogy a természetes személyek adatainak kezelésével, illetve az adatok akadálytalan áramlásának szabályozásával a környezeti elvárásokhoz illő további kiterjesztést nyerjen a korábban hozott törvény. A rendelet hatályba lépése 2016. május 24. A kétéves türelmi időszak után 2018. május 25-től lépett életbe. Ezzel párhuzamosan az adatvédelmi újítás keretében 2018. május 6. napján életbe lépett az Európai Parlament és a Tanács (EU) 2016/6806 irányelve 2016. április 27. napján az adatvédelem bűntetőjogi vonatkozását illetően.

Ezek szükségessége az információ felértékelődésével fogalmazódott meg és igyekezett, illetve igyekszik támogatni a személyes adatok védelmét a fentebb leírtak alapján. Tehát jelenleg az utóbbiként említett EU 2016/679 számú Általános Adatvédelmi Rendelet az irányadó.

A téma reprezentációja az MTMT-ben és az Elsevier-ben

A social engineering magyar definíciója a szakirodalom elemzése során fellelt számos hazai és nemzetközi tanulmány vizsgálata során sem jutott egységes megfogalmazásra, azonban magyar fordítása inkább a pszichológiai manipulációval megfelelő. A szakirodalomban leírtak alapján mindben közös a fogalom magyarázata folyamán az emberi tényező, mint gyenge láncszem jelenléte, illetve a manipuláció, a befolyásolás, az információkommunikációs eszközök gyengesége és sérülékenysége. A Magyar Tudományos Művek Tárának keresőjében a social engineering témájával foglalkozó műveket idézőjellel kerestük annak érdekében, hogy a kereső téves találatait kiszűrjük. Ennek eredményeképpen 120 darab művet találtunk, közöttük többek között tudományos publikációkat, előadásokat. A nemzetközi kereséshez a www.elsevier.com adatbázisában folytattunk le hasonlóan böngészést, melyre 830 darab találat támasztotta alá szintén különböző tudományos és egyéb publikációk létét. A téma jelentőségét erősíti, hogy az adatbázisokban keresve évről évre több munka jelenik meg.

A szakirodalmi elemzés eredményeképpen a leginkább hivatkozott Kevin D. Mitnick *A legendás hacker* című könyve alapján használt fogalomból indulunk ki jelen tanulmányunk feldolgozása során. Mitnick, aki az eddigi történelem leghíresebb hackere, könyvében definiálta is a social engineeringet, mely definíciót tanulmányunk bevezetésében ismertettünk.

A kutatásról

Primer kutatást végeztünk, melyhez Google kérdőív szolgáltatás által a közösségi oldalakon való megosztással juttattuk el kérdőívünket minél nagyobb számú közönség felé. A kérdőív 34+1 kérdésből állt, mely kérdések csoportokra osztva az alábbi megosztást képviselték:

1) Leginkább demográfiai kérdéseket gyűjtött össze az 1–16. kérdés, melyek által a megkérdezetteket próbáltuk megismerni, többek között a nemre, korosztályra, iskolázottságra, elhelyezkedésre, foglalkoztatottság szintjére, kapcsolódó szervezetre, illetve nyelvtudásra, tájékozottságra utaló kérdések formájában.
2) Információbiztonsággal foglalkozó kérdéseink a 17–19. kérdések formájában arra vonatkozó információkra kérdeztek rá, melyből megállapítható, hogy a válaszadó mennyire tekinthető információbiztonság szempontjából tudatosnak.
3) A 20–28. kérdések a kitöltő social engineering ismeretét, tapasztalatait felmérő információkra kérdeztek rá.
4) A 29–34. kérdéscsoport a válaszadót foglalkoztató szervezet attitűdjét felmérő kérdéseket gyűjtötte egy csokorba, melyekkel a tájékoztatásra, felkészültségre, oktatásokra deríthető fény.
5) Az utolsó kérdés egy nyitott kérdés volt azért, hogy lehetőséget adjunk a kitöltőknek arra, hogy a témára vonatkozó észrevételeiket megoszthassák.

Kutatási fő kérdéseink

A kérdőívünk elemzése során releváns, objektív választ kerestünk az alábbi fő kérdésekre.

K1: Milyen területeket és milyen mértékben érintettek a social engineering támadások?

Első főkérdésünk a 12–14. demográfiai kérdések és a 28. social engineering támadásokra vonatkozó kérdések kapcsolatának vizsgálatával elemezzük.

K2: Milyen tapasztalatokat szereztek a megtámadott szervezetek, hogyan védekeztek, és miként csökkentették a veszteségeket?

Második feltevésünkre a kérdőív negyedik kérdéscsoportjára kapott és 28. social engineering támadásokra vonatkozó kérdésre kapott válaszok összevetésének segítségével keresünk választ, az előző feltevés alátámasztásához hasonlóan kapcsolatvizsgálat módszerével.

K3: Megfigyelhető-e hasonlóság a szervezetek védekezési és felkészülési technikáiban?

Harmadik vizsgálati tárgyunk alátámasztását hivatott támogatni a kérdőív 12–14. demográfiai és 29–34. szervezeti felkészültséget felmérő kérdések statisztikai elemzése, szintén kapcsolatvizsgálat módszerével.

Az elemzés

Elemzésünkhöz online környezetben a Google által biztosított kérdőív szolgáltatással saját készítésű kérdőívet továbbítottuk közösségi média felületeken ismerőseink körében. A mintavétel folyamán Jagodics Ibolya Facebook ismerősei (721 fő), Kollár Csaba Facebook ismerősei (4700 fő), Jagodics Ibolya LinkedIn ismerősei (331 fő), Facebook-kérdőív kitöltő csoportok (Kérdőív Pont: 16400 tag, Kérdőív Kitöltők Klubja: 4700 tag, Kérdőív kitöltés, diploma kérdőívek csere-bere: 6300 tag), NKE PhD (105 tag) és KMDI 2019 (22 tag), vagyis összesen 33 179 fő felé tettük elérhetővé. Ezzel a mintavételi halmaz sokrétűségét biztosítottuk 2022. április 4. és 2022. április 26. napja között.

Az összesen 561 darab kitöltött kérdőív válaszadóit a következők jellemzik: 239 fő, tehát a kitöltők 42,6%-a férfi, 322 fő, vagyis 57,4%-a nő; a válaszadók 27%-a (149 fő) szakmunkás vagy szakirányú végzettségű, 69%-a (388 fő) főiskolai vagy egyetemi diplomás és további 4% (24 fő) rendelkezik doktori fokozattal.

A válaszadók 8%-a (47 fő) tanácsadás, 18%-a (99 fő) kereskedelem, 17%-a (95 fő) gyártás és termelés, 42%-a (234 fő) szolgáltatás és 15%-a (86 fő) közszolgálati tevékenységet ellátó szervezetnél tevékenykedik.

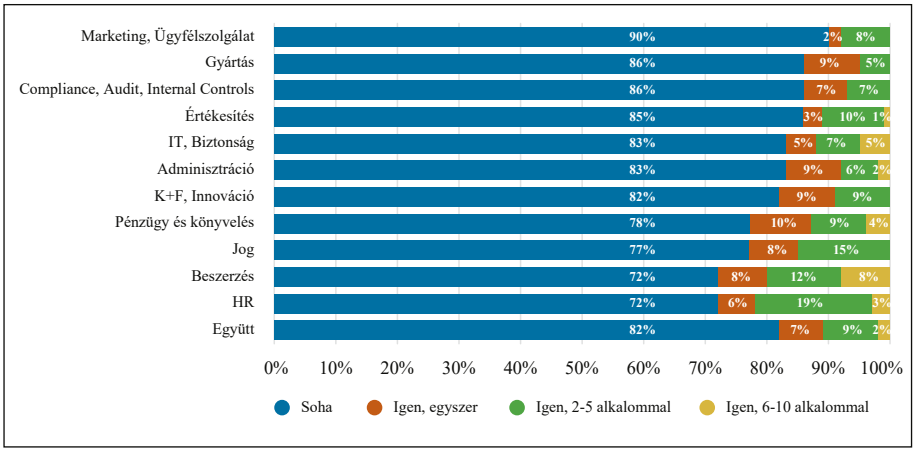
Az 561 darab kitöltött kérdőív válaszaiból adatbázist építettünk, és PSPP szabad felhasználású statisztikai szoftver segítségével kapcsolatvizsgálati módszerrel elemzésnek vetettük alá. A következőkben ismertetjük a fő kérdéseink alátámasztására használt módszer eredményeit.

K1: Milyen területeket és milyen mértékben érintettek a social engineering támadások?

A kérdőív elemzése során az első kapcsolat vizsgálatához a 12. kérdés (Az Ön szakterülete) és a 28. kérdés (Szenvedett már el social engineering támadást?) válaszait analizáltuk. A 12. kérdésre a válaszadók a következő lehetőségek közül választhattak: adminisztráció, beszerzés, compliance/audit/internal controls, értékesítés, gyártás, emberi erőforrások, IT és biztonság, jog, kutatás/fejlesztés/innováció, marketing és ügyfélszolgálat, illetve pénzügy és számvitel. A 28. kérdésre a válaszadóknak lehetősége volt több választ is megjelölni, melyek között két csoportot lehetett felállítani a magánéleti és a céges környezetben elszenvedett támadásokat, illetve mindkettőben.

A kapcsolatvizsgálat eredményeképpen elmondható, hogy a céges környezetben előforduló social engineering támadások legkevésbé a marketing, ügyfélszolgálat (10%), a gyártás (14%), és a compliance, audit, internal controls (14%) területeket érintették, leginkább pedig a jog (23%), beszerzés (28%) és a HR (28%) voltak ilyen támadásnak kitéve. Ennek ellenére az egyes szakterületek eltérése a támadás gyakoriságát tekintve nem szignifikáns [c2(30) = 24,183; p = 0,764], mely összefüggés az esetben sem szignifikáns, ha csupán a támadás megléte/nem léte szerint vizsgáljuk [c2(10) = 9,263; p = 0,561] – lásd 2. számú ábra.

2. számú ábra: *A céges környezetben elszenvedett social engineering támadások gyakoriság szerinti megoszlása szakterületenként*



Forrás: A szerzők saját szerkesztése.

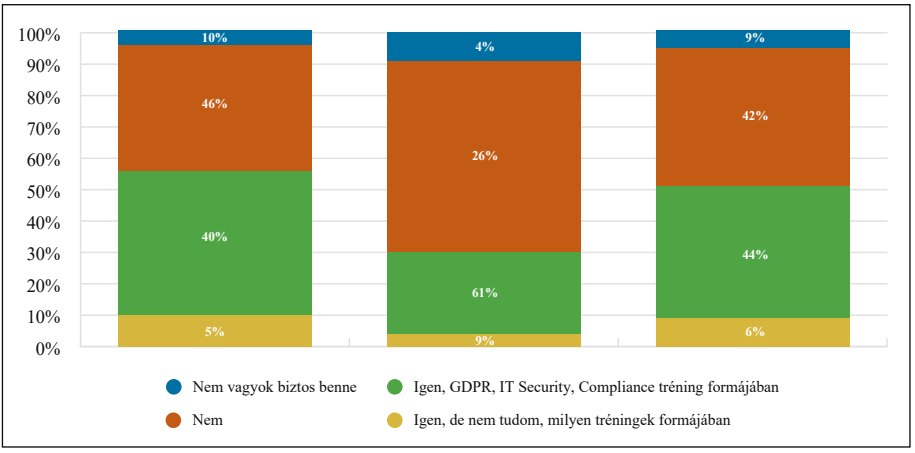
K2: Milyen tapasztalatokat szereztek a megtámadott szervezetek, hogyan védekeztek, és miként csökkentették a veszteségeket?

Második feltevésünk igazolására a kérdőív fentebb részletezett 28. kérdésének kapcsolatát vizsgáltuk a 29. kérdéssel (29. Kapott oktatást social engineering támadások felismerésére?). Kitöltőink a 29. kérdésre a következő válaszok közül választhattak: „nem”; „nem vagyok biztos benne”; „igen, de nem tudom milyen tréningek formájában”; illetve „igen, GDPR, IT security, compliance tréning formájában”.

Ezen kérdések mentén látható, hogy azok a válaszadók, akik olyan szervezetnél dolgoznak, ahol céges környezetben tapasztaltak social engineering jellegű támadást, azok esetében nagyobb arányban fordult elő, hogy kaptak oktatást akár GDPR, IT security, compliance tréning, akár egyéb formában [$c^2(3) = 21,634$; $p<0,001$] – lásd 3. számú ábra. Tehát a kitöltők válaszainak fényében

megállapítható, hogy azon szervezetek, amelyek érintettek voltak social engineering támadásokban védekezésük részeként oktatásokkal igyekeznek munkavállalóikat felkészíteni az esetleges támadásokra, illetve ezen keresztül csökkenteni próbálják a várható veszteségeket.

3. számú ábra: *A „29. Kapott oktatást social engineering támadások felismerésére?" kérdésre adott válaszok megoszlása a céges környezetben elszenvedett social engineering támadás alapján*



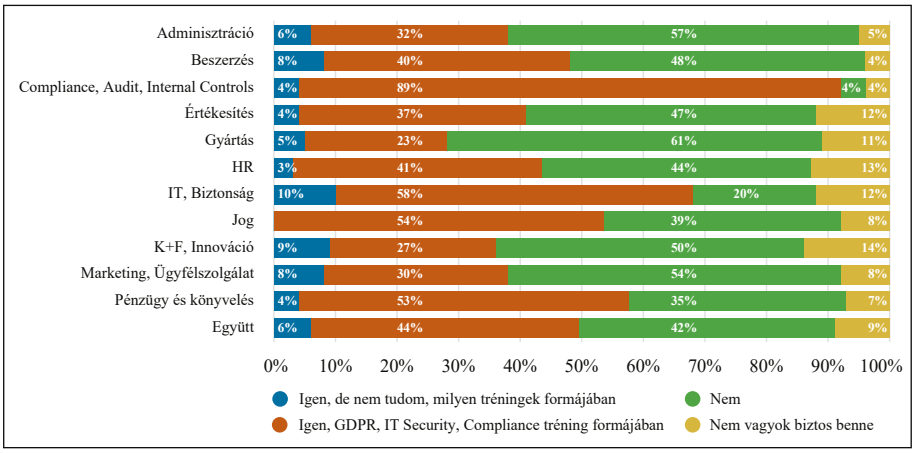
Forrás: A szerzők saját szerkesztése.

K3: Megfigyelhető-e hasonlóság a szervezetek védekezési és felkészülési technikáiban?

A harmadik kérdés alátámasztására a fentebb részletezett 29. kérdés került kapcsolatvizsgálat alá a válaszadók által kitöltött 12. kérdésre kapott válaszokkal.

Ezekkel az oktatás és a válaszadó által képviselt területek közötti kapcsolat révén szignifikáns eltérés mutatható ki az egyes szakterületek között a tekintetben, hogy kaptak-e oktatást social engineering támadások felismerésére [$c^2(30) = 70{,}813$; $p<0{,}001$]. Legnagyobb arányban a compliance, audit, internal controls (4 + 89%); az IT, biztonság (10 + 58%) és a pénzügy és könyvelés (4 + 53%) területeken dolgozók nyilatkoztak úgy, hogy „igen, GDPR, IT security, compliance tréning formájában" kaptak oktatást. A legelhanyagoltabb területek pedig a gyártás (5 + 23%); a K+F, innováció (9 + 27%); a marketing, ügyfélszolgálat (8 + 30%) és az értékesítés (4 + 37%) voltak (lásd 4. számú ábra).

4. számú ábra: *A „29. Kapott oktatást social engineering támadások felismerésére?” kérdésre adott válaszok megoszlása szakterületenként*



Forrás: A szerzők saját szerkesztése.

Összegzés és következtetések

Napjainkra újabbnál újabb támadási formáknak vagyunk kitéve a mindennapi életben és munkahelyünkön egyaránt. A technológia fejlődése nem csupán egyszerűsíti a folyamatokat, gyorsítja azokat, de az ismeretlenség veszélye is körbe lengi. Ezt alátámasztja a Belügyi Statisztikai Rendszer által elérhető statisztika is, mely 2018 és 2022 közötti időszakból egyértelmű bizonyítékot szolgáltat afelől, hogy a Büntető Törvénykönyv által definiált információs rendszerek elleni, vagy azok felhasználásával elkövetett és lezárt visszaélések száma évről évre emelkedik, illetve magas. További nyilvánosan elérhető statisztikáknak köszönhetően tanulmányunkban igazoltuk, hogy a magyar lakosság körében is szinte bárki kitett annak, hogy pszichológiai manipuláció áldozatává váljon az általa használt internetes felületeken át. Az internet elterjedése mára a magyarok 89%-át tette felhasználóvá. Munkánk alapvetően a hírhedt hacker, Mitnick által definiált fogalomból indult ki, amely szerint az emberek megtéveszthetők, manipulálhatók pszichológiai módszerekkel úgy, mint rábeszélés vagy megtévesztés, elhitethető velük, hogy a szemben álló hacker valós ügyben keresi fel, így információt szerez be rajtuk keresztül.

Három feltevést fogalmaztunk meg annak érdekében, hogy vizsgálatunk alátámasztást nyerjen. Ezen fő kérdések kapcsolatvizsgálaton keresztül arra irányultak, hogy az online kérdőívet kitöltő 561 fő válaszain át rálássunk milyen szervezeti területek érintettek, illetve milyen arányban a social engineering

támadásokban, védekeznek-e valamelyest a szervezetek, illetve biztosítanak-e oktatást munkavállalóik számára.

Online kérdőívünket a közösségi oldalakon több ezer fő felé tettük elérhetővé 2022. április 4. és 2022. április 26. napja között, melyből összesen 561 darab kitöltött kérdőív válaszait elemeztük kapcsolatelemzés módszerével PSPP statisztikai szoftver használatával. Kitöltőink heterogén halmazt biztosítottak, különböző korosztályból, szakterületről és végzettséggel.

A válaszadók 66%-a (369 fő) nyilatkozott arról, hogy tudja vagy ismeri a social engineering fogalmát, és 34%-a (190 fő) nem rendelkezik ismerettel erről a területről. A megkérdezettek 37%-a (210 fő) nyilatkozott arról, hogy visszaélés áldozata, 15%-a (83 fő) bizonytalan abban, hogy visszaélés áldozatául esett, és további 48%-a (268 fő) válaszolta, hogy nem volt még visszaélésben része.

Az elemzés eredménye rávilágított arra, hogy social engineering támadásban érintett területek leginkább a jog, beszerzés és humán erőforrás, legkevésbé a marketing, ügyfélszolgálat, gyártás, illetve ellenőrzési területek a válaszadók által tapasztaltak szerint annak ellenére, hogy szignifikáns eltérést nem mutatott egyik terület sem. Szintén a kitöltők válaszain át látható az elemzés azon konklúziója, miszerint azok a szervezetek, amelyek már szenvedtek el social engineering támadást, oktatást biztosítanak felkészítésként a munkavállalóik részére, ezzel úgymond védekezést demonstrálnak. Végül az analízis kimutatta azt is, hogy szignifikáns eltérés mutatkozik a területek között az oktatások tekintetében. Miközben az IT, pénzügy és számvitel, compliance, illetve belső ellenőrzési terület különböző tréningekben kap felkészítést, úgy a gyártás, kutatás és fejlesztés, marketing és értékesítési területek jelentősen elmaradnak, így nem kapnak oktatást social engineering támadás felismerésére sem GDPR, sem compliance, sem pedig IT tréningek formájában.

A tanulmány következtetéseként kívánjuk megfogalmazni azon javaslatunkat, hogy azon szervezetek életében is érdemes felkészülni a jövőbeni online visszaélésekre, akik még nem tapasztalták meg, milyen károkat okozhat ezen szervezetek működésében. Ezen kívül a gyártás, értékesítés, marketing, illetve kutató területeken is érdemes bevezetni a munkavállalók oktatását, felkészítését a biztonságtudatosság fokozásának érdekében.

Felhasznált irodalom

Bányász P., Bóta B. & Csaba Z. (2019). A social engineering jelentette veszélyek napjainkban. In Zsámbokiné Ficskovszky Á. (Szerk.), *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében* (pp. 12–37). Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat. https://doi.org/10.37372/mrttvpt.2019.1.1

Deák V. (2019a). Kártékony programok terjedése social engineering technikákon keresztül. *Hadmérnök, 14*(2), 256–271. https://doi.org/10.32567/hm.2019.2.21

Deák V. (2019b). Social engineering alapú információszerzés a kibertérben megvalósuló lélektani műveletek során. *Hadtudományi Szemle, 12*(3), 95–111. https://doi.org/10.32563/hsz.2019.3.6

Dub M. (2021). A social engineering támadások megelőzésének lehetőségei. *Hadmérnök, 16*(3), 137–187. https://doi.org/10.32567/hm.2021.3.10

Dyson E. (1998). *2.0 verzió (életünk a digitális korban*). HVG Kiadó.

Haig Zs. (2018). *Információs műveletek a kibertérben*. Dialóg Campus Kiadó.

Jóri A. (2005). *Adatvédelmi kézikönyv*. Osiris Kiadó.

Jóri A. (2012). *Adatvédelem és információszabadság a gyakorlatban*. Wolters Kluwer Kft.

Kollár Cs. (2018). Az információbiztonság humán aspektusai: A biztonságtudatossági ellenőrzés során alkalmazott social engineering technikák elemzése a SPEAKING modell segítségével. *Belügyi Szemle, 66*(2), 22–45. https://doi.org/10.38146/BSZ.2018.2.2

Mitnick D. K. & Simon L. W. (2002). *A legendás hacker – A megtévesztés művészete.* Perfact-Pro Kft. Kiadó.

Winder D. (2020). *Microsoft Security Shocker As 250 Million Customer Records Exposed Online*. Forbes. https://www.forbes.com/sites/daveywinder/2020/01/22/microsoft-security-shocker-as-250-million-customer-records-exposed-online

A cikk APA szabály szerinti hivatkozása

Jagodics I. & Kollár Cs. (2023). 21. századi social engineering támadások, védekezés és szervezeti hatások Európában. *Belügyi Szemle*, *71*(1), 113–126. https://doi.org/10.38146/BSZ.2023.1.6