SOCIAL ENGINEERING AND MANIPULATION TECHNIQUES AND METHODS - RESEARCH REPORT

A SOCIAL ENGINEERING ÉS A MANIPULÁCIÓS TECHNIKÁK ÉS MÓDSZEREK - KUTATÁSI JELENTÉS

KOLLÁR Csaba[1], ZAKAR Ákos[2]

Abstract

In the first part of our study [1], we reviewed the theoretical summary of the topic, focusing on the manipulation methods and techniques that can be related to the human soul, psychology, interpersonal communication, and also appear in the field of information security. The techniques and methods were presented along the human and IT-based divisions, and we also covered the criminal law aspects of the topic. In the second – present – part we present the results of our own research. Based on the responses to our online, large-sample questionnaire, we first provided a demographic description of the sample, then presented the responses by questions, and then analyzed the responses by group composition. In our research, we examined three hypotheses aimed at the use of passwords, the use of operating systems, and the recognition of the dangers inherent in phishing emails. After examining the relationship between the questions, we concluded our study with conclusions on the achievement of safety awareness, focusing on survey, regulation and knowledge transfer.

Keywords

information security, social engineering, manipulation, research report

Absztrakt

Tanulmányunk első részében [1] a téma elméleti összefoglalását tekintettük át, s elsősorban azokkal a manipulációs módszerekkel és technikákkal foglalkoztunk, melyek az emberi lélekhez, a pszichológiához, a személyközi kommunikációhoz köthetőek, s megjelennek az információbiztonság területén is. A technikákat és módszereket a humán, illetve IT alapú felosztás mentén mutattuk be, s kitértünk a téma büntető törvénykönyvi vonatkozásaira is. A második – jelen – részben saját kutatásunk eredményeit ismertetjük. Az online, nagymintás kérdőívünkre kapott válaszok alapján először a minta demográfiai leírását adtuk meg, majd a kérdésenkénti válaszokat mutattuk be, ezt követően pedig a csoport összetétele szerinti válaszokat elemeztük. Kutatásunkban három hipotézist vizsgáltunk, melyek a jelszavak használatára, az operációs rendszerek használatára, illetve az adathalász e-mail-ekben rejlő veszélyek felismerésére irányultak. A kérdések közötti kapcsolat vizsgálata után tanulmányunkat a biztonságtudatosság elérésére vonatkozó, felmérésre, szabályozásra, ismeretátadatásra fókuszáló következtetésekkel zártuk.

Kulcsszavak

információbiztonság, social engineering, manipuláció, kutatási jelentés

[1] kollar.csaba@phd.uni-obuda.hu | ORCID: 0000-0002-0981-2385 | associate professor/egyetemi docens | Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

[2] zakarakos85@gmail.com | ORCID: 0000-0002-3919-4098 | information security expert/információbiztonsági szakértő | állami tulajdonú gazdasági társaság

KUTATÁSMÓDSZERTANI ALAPVETÉS

Primer kutatásunk célja az volt, hogy egy közel kétszáz fő részvételével az információbiztonság tudatossággal kapcsolatos felhasználói véleményeket ismerjünk meg, s ezek feldolgozása és kielemzése után megalapozott következtetéseket vonjunk le, illetve, hogy szervezeti szinten is alkalmazható javaslatokat fogalmazzunk meg. A kvantitatív kutatási módszerek közül a kérdőívet választottuk, ennek elkészítésénél módszertanában többek között Babbie [2], Cseh-Szombathy és Ferge [3], Freedman és szerzőtársai [4], Moksony [5], Sajtos és Mitev [6], Scipione [7], Malhotra [8] műveire hagyatkoztunk. A kérdőív feldolgozásánál és az eredmények értékelésénél nevezett szerzők mellett elsősorban Bornemissza [9], Reidmacher [10] és Tóthné [11], [12] javaslatait és ajánlásait vettük figyelembe. Kérdőívünk kérdéseinek összeállításánál egyebek mellett Oroszi [13] 2008-ban végzett szekunder kutatását tanulmányoztuk, s így egy 40+1 kérdésből álló kérdőívet készítettünk a Google Űrlapok (Forms) segítségével. A 41. kérdés egy nyitott kérdés volt, melyben a kitöltők szöveges formában írhatták le véleményüket a kérdőívvel, illetve a témával kapcsolatban. A kérdőív kérdéseinél egyaránt alkalmaztunk nyitott, zárt és hibrid kérdéseket, így a válaszadási lehetőségeknél a feleletválasztós, a jelölőnégyzetes és a szabad szöveges mezők egyaránt szerepeltek lehetőségként. Az elkészült kérdőív linkjét – a GDPR előírásainak figyelembe vételével – saját ismeretségi körben (levelezőlista, telefonkönyv, Facebook ismerősök) osztottuk meg. A kitöltésre 2020. március 31. és 2020. április 8. között adtunk lehetőséget. A lekérdezési szakasz zárásakor 216 érvényes kérdőívet számoltunk össze.

KÉRDÉSENKÉNTI VÁLASZOK (KIVONAT)

A kérdésekre adott válaszoknál – terjedelmi okok miatt – bizonyos kérdésekre adott válaszokat nem, vagy csak lényegesen rövidebb terjedelemben (összegezve) ismertetünk.

Általános és demográfiai kérdések

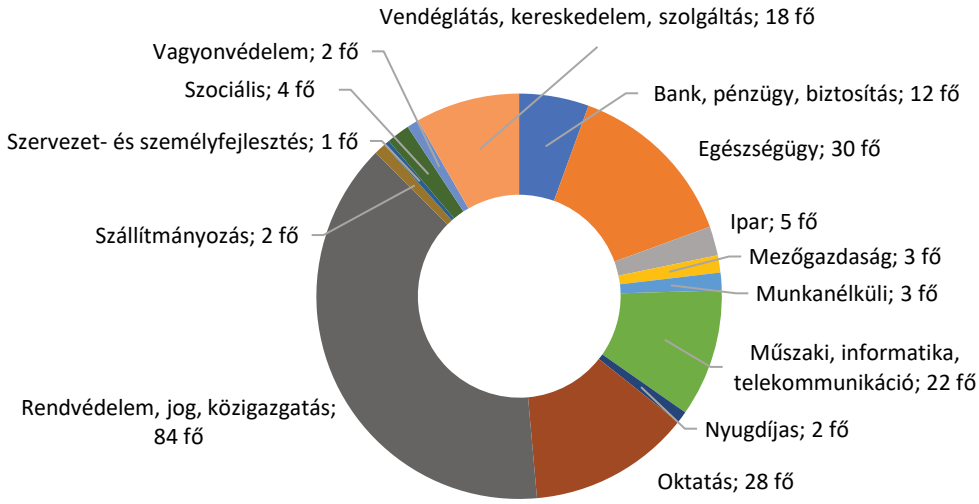
A kutatásmódszertani alapvetésben már leírtuk, hogy összesen 216 érvényes kérdőívet számoltunk össze. A mintánk demográfiai leírását a nem, az életkor, a végzettség, a munkaviszony és a munkahely ágazati besorolása alapján adjuk meg.

Generációk		Nők		Férfiak	
elnevezés	*életkor*	*%-os arány*	*fő*	*%-os arány*	*fő*
Baby boomer	56-74	10,2	22	2,3	5
X generáció	41-55	20,8	45	21,2	46
Y generáció	26-40	23,1	50	18,5	40
Z generáció	11-25	1,8	4	1,8	4
Összesen		56	121	44	95

1. táblázat: a válaszadók neme és életkora közötti megoszlás (saját szerkesztés)

Válaszadóink többsége (66%) felsőfokú végzettséggel (főiskola, egyetem) rendelkezik, ezt követi a szakközépiskola és gimnázium (30%). A vizsgált csoportnak valamivel több, mint a fele (50,5%-a) közszférában dolgozik, a versenyszférában 31,9%-uk vállal munkát alkalmazottként. 6,9%-uk közép- és felsővezető, 4,2% cég ügyvezetője vagy tulajdonosa valamely társas vállalkozásnak. Egyéni vállalkozóból 6 fő van, tanulóból 2 fő, al-

kalmi munkavállalóból 1 fő, valamint 5-en vannak, akik valamilyen oknál fogva nem aktívak a munkaerőpiacon. A válaszadók munkahelyének ágazati megoszlása az első ábrán látható.



1. ábra: a válaszadók munkahelyének ágazati besorolása (saját szerkesztés)

A válaszadók több, mint egyharmada (38,8%-a) a rendvédelem, jog, közigazgatás területén dolgozik. 13,8%-a az egészségügyből jött, 12,9%-uk oktató, nevelő tevékenységet végez. 10,2%-a műszaki, IT, telekommunikációs szektorból, 8,3%-uk vendéglátás, kereskedelem és szolgáltatás területéről, 5,5%-uk a pénzügyi világból érkezett. A fennmaradó 10,5% megoszlik a mezőgazdaság, ipar, vagyonvédelem, szállítmányozás, szociális dolgozók és az 5 fő inaktív között.

Jelszóhasználat

A jelszóhasználattal kapcsolatban öt kérdést tettünk fel, úgymint: (1) Használ-e ugyanolyan jelszavakat magán és munkahelyi fiókjaihoz? (2) Ismeri-e más a privát vagy munkahelyi fiókjai jelszavát? (3) Hogyan választja meg a használni kívánt jelszavait? (4) Milyen gyakran változtatja a jelszavait? (5) Hol tárolja a jelszavait?

A kérdésekre adott válaszok alapján megállapítottuk, hogy szinte azonos eredményt kaptunk a jelszavak megválasztása és a jelszavak másokkal való megosztása vonatkozásában. A válaszadók 30%-a használ ugyanolyan jelszavakat a magán és munkahelyi fiókjaihoz, míg 28,7%-uk másokkal meg is osztja ezen jelszavakat. A fennmaradó többség már óvatosabb e tekintetben, más jelszavakat használ privát és munka célra, valamint ezek bizalmasságára is vigyáz. A jelszó megválasztásánál a legkockázatosabb verziót, miszerint alapértelmezett jelszavakat használ, csak 2,3%-uk, mindössze 5 fő választotta. Bár hozzá kell tenni, hogy ez nagyon sok alkalmazás esetén csak ideiglenes opció. Egy új rendszerhez történő hozzáférés esetén két út áll a felhasználó előtt. Így a másik két tábor közel azonos arányban képviselteti magát. Személyhez köthető, rövid, könnyen megjegyezhető jelszavakat 51,4%-uk használ. Bonyolult, egyedi, hosszú jelszavakat különféle típusú karakterekkel

46,3%-uk alkalmaz. A jelszó megváltoztatás gyakoriságára tekintettel három táborra oszthatók a válaszadók. Lényegében minden második ember (56%-uk) csak kötelező jelleggel, a rendszer által előírt időközönként változtatja jelszavát. 28,7%-uk csak akkor változtatja meg, ha elfelejtette, vagy ha újat kell igényelni. A legkevesebben, (15,3%) azok vannak, akik tudatosan, rendszeresen saját maguk által meghatározott gyakorisággal változtatják jelszavukat. A jelszavak tárolására vonatkozóan túlnyomó többségük (közel 60%) a hagyományos tárolást választotta, vagyis az emlékei közt, saját memóriájában tárolja jelszavait. A realitások talaján maradva további négy lehetőséget kínáltunk fel. A legveszélyesebb tárolási módot 2,3%-uk alkalmazza, vagyis akiknél a számítógépük mellett van felírva a jelszavuk. A maradék három opciót, a biztonságos megoldást választók jelölték be. Nagy különbség nem mutatkozik a jelszómanagert használók 10,6%-a, és a titkosított megoldást választók közt. Utóbbinál fájlban vagy mobiltelefonon történő jelszótárolást 8,6%-uk használja. Kevésbé biztonságos, ugyanakkor hagyományos módszert választott 18,5%-uk a válaszadóknak, akik elrejtett, elzárt füzetben felírva őrzik jelszavaikat az illetéktelenek elől.

Informatikai védelem

Az informatikai védelemmel kapcsolatban összesen tizenegy kérdést tettünk fel, az ezekre adott fontosabb válaszokat alább foglaljuk össze. A válaszadók rendszerint fontosnak tartják a vírusvédelmi eszközök meglétét a különböző eszközeiken, ugyanakkor a három alapvető eszközfajta (számítógép, tablet, mobiltelefon) együttes védelmét csak közel 18% jelölte be. A vírusvédelmi szoftverek kiválasztásánál a válaszadók harmada (35,5%) kizárólag ingyenes programokat használ, míg kicsivel kevesebb, mint harmaduk (31,8%) olyan megoldás mellett dönt, ami a szokásainak leginkább megfelelő. 15,2%-uk törekszik rá, hogy ár/érték arányban a legtöbb tudást nyújtó megoldást válassza és 17,5%-uk megbízik ismerősei ajánlásában. A munkahelyi vírusvédelmi szoftverekkel kapcsolatban a válaszadók közel 60%-a nem tudta megnevezni, hogy milyen védelmi szoftvereket használ az adott szervezet/vállalat. A munkaállomástól rövid időre való felállást követő egyszerű biztonsági mozdulat[3] betartását 59,2%-uk veszi komolyan, míg 31,9%-uk semmit nem tesz annak érdekében, hogy más nem nyúljon a felügyelet nélkül hagyott számítógépéhez. A maradék 8,9% megoszlik az olyan választ adók közt, akik operációs rendszerén be van állítva az automata zárolási funkció. A válaszadók többsége (60,6%-a) már használt saját pendrive-ot munkahelyi számítógépben, vagy fordítva: vállalati pendrive-ot saját gépben. A többi 39,4%-uk ennek elkerülésére figyelmet fordít. Az informatikai eszközök (laptop, tablet, mobiltelefon) és adathordozók elvesztésével, ellopásával kapcsolatban a megkérdezettek közül 35-en már voltak áldozatai lopásnak. 24 főnél mobiltelefon, 9 főnél adathordozó, 1 főnél laptop, 1 főnél mobiltelefon és adathordozó bánta a gazdája nem megfelelő figyelmét. Köztük 42,8%-uk nem használt semmiféle titkosítási eljárást, így adataik mások számára is ismertté válhattak. A szervezeti információbiztonság szempontjából kényes kérdés, hogy mit tesz a munkavállaló, amikor a munkahelyén gazdátlan adathordozót talál. A válaszadók túlnyomó többsége (78,8%-a) még nem találkozott ilyen esettel. 18,1%-a becsületes és óvatos megtalálóként leadta egy olyan személynek a cégen belül, aki meg tudta tenni a szükséges intézkedéseket, hogy az adathordozó – feltéve, hogy szervezeten belül

[3] A leggyakrabban használt Windows operációs rendszeren az automatikus zárolás funkció, WINDOWS gomb + „L" billentyű kombinációval kiléptet az adott fiókból.

kell keresni – visszajusson a gazdájának. A válaszadók 1,9%-a teljes passzivitást tanúsított, nem foglalkozott a talált tárggyal, míg 1,4%-a, azaz 3 fő volt olyan bátor és megnézné annak tartalmát a céges vagy az otthoni számítógépen. Utóbbiak a csalizás áldozatai, mellyel akár egy komplett vállalati infrastruktúrát is lefertőzhetnek kártékony programmal.

Kíváncsiak voltunk arra is, hogy a megkérdezettek hogyan viszonyulnak a vezeték nélküli (WiFi) kommunikáció biztonságához. A válaszadók közel fele (46,3%) az otthoni router gyárilag beállított jelszavait használja, míg az egy fokkal jobb megoldást választók (41,7%) legalább az eszköz telepítésekor megváltoztatták az eszköz alapértelmezett jelszavát. A biztonságot szem előtt tartók mindössze 12%-kal vannak, ők azok, akik rendszeresen megváltoztatják WiFi jelszavukat. A nyilvános WiFi hálózatra történő csatlakozásnál a vizsgált minta több mint fele (51,9%) nem használja ezt a fajta megoldást, inkább a mobil internet adta lehetőségekre támaszkodik. Teljesen egyforma azon válaszadók száma, akik különösebb aggodalom nélkül felcsatlakoznak nyilvános hálózatokra, ők 20,8%-nyian vannak. Akik abban a hiszemben vannak, hogy egy jelszóvédelem – a titkosítás ismerete nélkül – megvédheti őket, szintén ugyanennyien képviseltetik magukat. Az IT biztonsághoz értőknek neveznénk azt a 6,5%-nyi 14 fős csoportot, akik felcsatlakoznak ugyan nyilvános WiFi hálózatra, de ezt követően egy biztonságos VPN csatornán keresztül élvezik az ingyenes internet adta lehetőségeket.

A mobiltelefonos applikációk, vagy számítógépes programok frissítésével, törlésével kapcsolatban 53,2%-uk automatikusan a rendszerre bízza az update-et, 42,6%-uk manuálisan hajtja végre a telepítést és törlést. A válaszadók 4,2%-a azonban felesleges dolognak tartja a szoftverek frissítését, e biztonsági műveletben csak az alkalmazás kinézetének esetleges megváltoztatása tölti el aggodalommal.

Fizikai biztonság

A fizikai biztonsággal kapcsolatos kérdések a beléptető rendszerre és az otthon felejtett belépésre jogosító kártyára/kulcsra vonatkoztak. A munkahelyükön lévő beléptető rendszerrel kapcsolatban a kulccsal nyitható ajtózár (61%) mellett sokan megjelölték még az élőerős védelmet (41,2%), a mágneskártyát (24,7%), valamint a belépőkód alkalmazását (20,8) és az ujjlenyomat olvasót is (2,3%). Az aktív dolgozók közül 6 személy semmiféle védelmet nem jelölt be, ami a belépést biztosítaná a munkahelyén. Mivel a jelölő négyzetes választási módok mellett egyéb lehetőséget is kínáltunk a válaszadásra, így páran beírták még a kulcsdoboz, proxy, vagy a riasztó használat mellett a „semmilyen” és „nincs” válaszokat. A válaszadók 63,9%-ával fordult már elő, hogy belépésre jogosító kártyáját, kulcsát otthon hagyta. A következő ráépülő feltételes válaszban arra voltunk kíváncsiak, hogy ezen személyek hogyan jutottak be ezt követően a munkahelyükre. A feledékeny dolgozók közül 39,7%-a más kolléga jogosultságával, vagy kulcsával jutott be a munkahelyére. Jóval többen (57,7%) választották a hivatalos utat, azaz a portaszolgálathoz fordultak. 2,6%-uk azonban olyan bejáratot választott, ahol ilyen jellegű intézkedések nem voltak szükségesek.

Biztonságtudatosság

A válaszadók biztonságtudatosságát öt kérdés segítségével vizsgáltuk meg. A válaszolóknak szinte a fele (49,5%) már elolvasta a munkahelyük információbiztonsági szabályzatát, míg 39,8%-uk nem. 6,5%-uk kategorikusan kijelentette, hogy náluk ilyen nincs, míg

4,2% volt azok aránya, akik nem tudták miről van szó, számukra ismeretlen ez a dokumentum. A megkérdezettek 17,6%-a már használta munkahelyi e-mail címét magánjellegű levelezésre, valamint 10,2%-uk ezzel a címmel már regisztrált is különböző weboldalakon, feliratkozott hírlevelekre. A nagy többség azonban ilyen módon nem ossza meg munkahelyi email címét másokkal. A közösségi oldalak használatát illetően a Facebook és a LinkedIn weboldalakat szándékosan egy kérdésbe tettük bele, mivel egy social engineering támadás információszerzési fázisa szempontjából nincs relevanciája, hogy a célszemély ellen melyik platformról szerzi be az adatokat a támadó. Egy-egy válaszadó volt, aki nem rendelkezik ilyen profillal, kamu profilt használ vagy tanulmányait, illetve szakmai önéletrajzát a LinkedIn-en megosztja, a Facebook-on viszont nem. Legtöbben nevüket (85,2%), fényképüket (68,5%), jelenlegi (27,8%) és korábbi munkahelyüket (15,7%), telefonszámukat (9,3%), valamint lakcímüket (2,8%) is közzéteszik.

Szoftverhasználat

Az otthoni és munkahelyi operációs rendszerek használatánál közel azonos eredmény született a két környezetnél. A Windows 10 vezet mind az otthoni (71,7%), mind a munkahelyi (74,5%) felhasználásnál. A Windows 8 esetén a munkahelyi területen több, mint háromszor annyian használják (11,1%), mint az otthoni környezetben, ahol csak 3,2%. Munkahelyükön 9,2% használja még a kockázatos Windows 7-es operációs rendszert. A Linuxot használók aránya szinte azonos, munkahelyen 3,7%-uk, otthon 3,2%-uk használja. A macOS nem számít elterjedt rendszernek, mindössze 3-an használják otthoni, köztük 1 fő pedig munkahelyi célra is. Volt néhány olyan válaszadó, aki több lehetőséget is bejelölt. Legtöbben, mintegy 73,1% saját tapasztalás útján, valamint 32,4%-uk ismerősök által tanulták meg a szoftverek használatát. Munkahelyi oktatás keretében szinte minden ötödik fő szerepelt, de találkozhatunk még a használati útmutató, könyvek, videók alapján történő tanulással is, ők 14%-al voltak. A legkevesebb jelölés az iskolai oktatás mellett szólt. Az ismeretlen hibaüzentre való reagálási helyzetet vizsgáló kérdésnél két közel azonos nagyobb és egy kis táborra oszlik meg a válaszadók aránya. 44,9%-uk a rendszergazdát értesíti első körben, míg 46,3%-uk megpróbálja rá megkeresni a megoldást – akár a kollégák bevonásával is – és csak végső soron jeleznék azt a help desk személyzetnek. Közel minden tízedik ember nem foglalkozik vele, mivel szerinte nem az ő dolga az ilyen jellegű informatikai problémák kezelése.

Veszélyhelyzetek felismerése

A válaszadóknak egy harmada, azaz 33,3%-a nem foglalkozik vele, ha a kollégája mögötte áll meg, miközben egy adott rendszerben megpróbál bejelentkezni. 39,8%-uk már felismeri az ebben rejlő kockázatot és inkább a másik elől takarva, gyorsabban gépelve próbálja megóvni jelszavát társa elől. Kb. egynegyedük pedig nem bízza a véletlenre a saját hitelesítő adatainak megismerését mások részére, megkéri kollégáját, hogy álljon arrébb, ezzel elejét véve a váll fölötti leskelődésnek. A munkahelyi témákról való beszélgetést vendéglátóhelyeken vagy tömegközlekedési eszközökön 52,8%-uk kerüli, 41,2%-uk pedig igyekszik rövidre fogni és halkan átadni a szükséges információkat. 6%-uk (13 fő) viszont ilyen jellegű dologgal nem foglalkozik, így hallgatózással könnyen bizalmas információk

juthatnak illetéktelenek fülébe. A munkahelyi szükségtelen iratok megsemmisítésére vonatkozóan is több válaszadási lehetőséget lehetett bejelölni. A kitöltök közel kétharmada a kötelező iratmegsemmisítő használatát választotta, őket követik azok, akik külön zsákba teszik a selejtes iratokat (22,7%). A felelőtlen megoldást választóknak két szintje van, akik a kommunális szemetesben dobják ki (17,1%), valamint akik hazaviszik elégetés vagy papírgyűjtés céljából (8,3%). Utóbbi két megoldás egyike sem nyújt biztonságot a kukabúvárkodás ellen. A munkaállomás takarítás közbeni védelmére vonatkozóan a válaszadók mintegy fele, 47,7%-a megteszi a szükséges intézkedést, azaz lezárja a szekrényeivel, fiókjaival együtt. Jóval biztonságtudatosabb az a 9,7%, akik a fizikai eszközei védelme mellett folyamatosan nyomon követik a takarító személyzetet munka közben. 21,3%-uk lezárja a számítógépét, de a dokumentumai elzárására nincs lehetősége. Ugyanennyien vannak teljes bizalommal a kisegítő személyzet iránt, nem hiszi, hogy az ő irataival foglalkozna, így nem is tesznek semmilyen óvintézkedést. Az ő esetükben könnyű lehetőség mutatkozik akár egy hardveres keylogger telepítésére, akár dokumentumok fotózására is. A belső információk gondatlan kiszivárogtatására vonatkozó kérdésünk egy ismeretlen kollégával szembeni telefonos kommunikációra utalt, aki konkrét információt szeretne megtudni. Tipikusan ilyen lehet egy megszemélyesítéses támadás. A válaszadóknak pontosan a fele választotta azt, hogy elérhetőséget és visszahívást kér. Minden ötödik, vagyis 19,4%-uk a hívás közbeni ellenőrzés módját választotta, míg szinte azonos aránnyal 19,9%-kal vannak azok, akik elhiszik, hogy valóban a munkatársukkal beszélnek. A fennmaradó 10,7% megoszlik az egyedi válaszokat adók közt. Ide sorolhatóak azok, akik semmilyen ügyben nem adnak tájékoztatást, ismerik kollégájukat, hivatalos megkeresést vagy belső e-mailt kérnek, továbbkapcsolják a vezetőjüknek stb. közt. Azzal kapcsolatban, hogy végrehajtanának-e felettesük nevében e-mailen kapott sürgős pénzügyi műveletet, közel minden tízedik megkérdezett igennel válaszolt, nem lát benne semmi veszélyt, ezzel potenciális résztvevői egy BEC (Business Email Compromise) típusú támadásnak. A válaszadók több mint fele (52,8%) más csatornán is megerősítést kérne és 38,9%-a pedig felismerné a jogtalan próbálkozást és jelentené az illetékeseknek. Az ismeretlen feladótól érkező vagy közüzemi szolgáltatóktól kapott mellékletekre 13,9%-uk azonnal rákattintana, letöltené őket, ezzel adathalász támadásnak téve ki magát. 10,2%-uk csak biztonságos zárt környezetben nyitná meg az e-mailt és mellékleteit. Meglepő, hogy közel háromnegyedük, 72,2%-uk pedig alapos elemzés után valószínűleg a törlés mellett döntene. A válaszadók maradék 3,7%-a is a biztonságos megoldást választaná, azaz a törlést, valamint figyelmen kívül hagyást választaná.

A CSOPORT ÖSSZETÉTELE SZERINTI VÁLASZOK

Annak érdekében, hogy a válaszok, illetve a válaszok kapcsolódásának rejtett dimenzióit is meg tudjuk vizsgálni, mintánkat több szempont szerint is összehasonlítottuk, s a válaszok meghatározott szempont (pl.: nem, életkor) szerinti bontása után a fontosabb kérdésekre adott válaszok hasonlóságát-különbségét vizsgáltuk rendszerint kereszttáblával. A fontosabbak megállapításokat alább közöljük.

Nemek szerinti vizsgálat

Kockázatok / Nemek	Nők (%)	Férfiak (%)
Ugyanolyan jelszavak használata magán és munkahelyi fiókoknál	57	43
Más által is ismert jelszavak használata	61,3	38,7
Érdeklődési körhöz tartozó rövid vagy alapértelmezett jelszavak használata	62	38
Soha vagy csak felejtés miatti jelszóváltoztatás	81	19
Számítógép mellé vagy füzetbe felírt jelszavak	50	50
Vírusvédelmi szoftverek használatának kerülése	100	0
Csak ingyenes (nem a felhasználói igényekhez, vagy ár/érték arányhoz szabott) vírusvédelmi szoftverek használata	70,6	29,4
Munkaállomások zárolásának kerülése a géptől való felállást követően	64,7	35,3
Pendrive munkahelyi és magán célú használata	55,8	44,2
Adathordozók titkosítás nélküli védelme	65,3	34,7
Talált adathordozó csatlakoztatása otthoni vagy céges számítógépre	66,7	33,3
Gyári jelszó használata otthoni WiFi routeren	66	34
Nyilvános, ingyenes WiFi használata	64,5	35,5
Automatikus rendszer, program frissítések mellőzése	66,7	33,3
Munkahelyi beléptető rendszer hiánya	88,8	22,2
Más belépési jogosultságának használata	46	54
Információbiztonsági Szabályzat szándékos el nem olvasása	58,1	41,9
Munkahelyi e-mail cím használata magáncélú levelezésre	42,1	57,9
Munkahelyi e-mail cím regisztrálása magáncélból hírlevelekre, webáruházba stb.	45,4	54,6
Közösségi oldalakon személyes információk megadása (pl. lakcím, telefonszám, munkahely)	63,1	36,9
Windows 7 vagy régebbi operációs rendszer otthoni használata	58,1	41,9
Bankkártya adatok, bejelentkezési adatok elmentése	51,3	48,7
Windows 7 vagy régebbi operációs rendszer munkahelyi használata	80	20
Ismeretlen számítógépes hibaüzenet figyelmen kívül hagyása	68,4	31,6
A belépési adatok leskelődéssel történő megismerésének figyelmen kívül hagyása	54,2	45,8
Nyilvános helyeken munkahelyi témákról való beszélgetés	46,2	53,8
Munkahelyi selejtes iratok kommunális hulladékként való kezelése vagy hazavitele	77,4	22,6
Számítógép le nem zárása takarítás alatt	74	26
Munkahelyi telefonon magát kollégának kiadó személy azonosságának nem ellenőrzése	67,5	32,5
Vezető nevében érkezett e-mail utasításának ellenőrzés nélkül végrehajtása	63,2	36,8
Ismeretlen feladó vagy közüzemi szolgáltató nevében érkezett email linkjének vagy mellékletének azonnali megnyitása	70	30

2. táblázat: nemek szerinti felosztás (saját szerkesztés)

A táblázat adataiból jól látható, hogy a nők jobban ki vannak téve a social engineering típusú támadásoknak. Ha a fenti felsorolásból kiveszem azon kockázatos fenyege-

téseket (beléptetési rendszer hiánya, elavult operációs rendszer használat), melyek kiküszöbölése nem egy alkalmazott felelőssége, akkor a nők átlagosan 62,6%-a, a férfiak 37,4%-a tekinthető potenciális áldozatnak ebből a szempontból.

Életkor szerinti vizsgálat

Az életkor szerinti vizsgálatot – ahogy arra korábban már utaltunk – a generációk szerinti felosztás szerint vizsgáltuk meg. Megállapítottuk, hogy az X generációs korosztály szerepel első helyen átlag 41,5%-kal, őket követi szorosan az Y generáció átlag 40,8%-kal. A Baby boomerek kockázatos válaszainak aránya 14,2% volt, a Z generációnál mindössze 3,4%. Nyikes [14] 2017-es kutatásában a 35 éves kort, mint vízválasztó vonalat húzta meg az informatikai eszközök és alkalmazások magabiztos használatában. Fontos megkülönböztetni a magabiztos és a biztonságtudatos használatot. Míg az előző gyakorlással elsajátítható képességet jelent, addig az utóbbi tudatos, veszélykerülő magatartás, melyet előzetes információszerzés nélkül nem lehet megvalósítani.

Végzettség szerinti vizsgálat

Az iskolai végzettség és a kockázatos magatartás összefüggésének vizsgálata során megállapítottuk, hogy a kockázatos magatartást tanúsítóknál a felsőfokú szakképesítéssel rendelkezők közül kerülnek ki a legtöbben. Ennek okát abban látjuk, hogy esetükben rendszerint nem választódik élesen külön a hivatali- és a magánélet, az alacsonyabb végzettségűekhez képest sokkal többször, sokkal komolyabb döntést kell hozniuk, s emiatt (is) stresszesebb a munkájuk. A végzettség szerinti öt legnagyobb különbség felsőfokú végzettséggel rendelkezők, illetve nem rendelkezők között az egyes kérdések vonatkozásában csökkenő aránnyal a következő: talált adathordozó csatlakoztatása otthoni vagy céges számítógépre (100%), munkahelyi e-mail cím használata magáncélú levelezésre (81%), ugyanolyan jelszavak használata magán és munkahelyi fiókoknál (78,8%), pendrive munkahelyi és magán célú használata (77,9%), automatikus rendszer, program frissítések mellőzése (77,8%).

Ágazatok szerinti vizsgálat

Az ágazatok szerinti bontás eredményéből megállapítható, hogy a 31 kockázatos viselkedési formából 23-ban a „rendvédelem, jog, közigazgatás” szektor áll a legrosszabb helyen, egy területen pedig az egészségüggyel azonos arányban szerepel. Ez az elkeserítő kép azt sugallja, hogy az állam működése szempontjából legnagyobb jelentőséggel bíró szektorból származott a legtöbb olyan válasz, mely a biztonságtudatos viselkedés hiányát mutatja a szervezeten belül.

HIPOTÉZISVIZSGÁLAT

A nem, kor és munkahelyi adatoknak a kockázatokhoz való viszonyításán felül többféle relációban is vizsgáltuk az eredményeket, melyek során tanulságos megállapítások születtek. Kíváncsiak voltunk, hogy különböző magatartási viselkedési minták hogyan viszonyulnak egymáshoz, megállapítható-e köztük bármilyen összefüggés. Viszonyítási alapnak így több csoportot is meghatároztunk, majd hipotéziseket állítottunk fel, melyek statisztikai értékelése után levontuk belőlük a következtetést. A skálázást 25%-os léptékben 4

részre osztottuk fel. A felétől nagyobb előfordulást mutató, 50% feletti eredményeket már igaznak vettük a bizonyítás során.

1. hipotézis

Azok, akik egyszerű jelszavakat használnak, az információ- és informatikai biztonság több területén is hanyag hozzáállással rendelkeznek.

Definíciók és kérdéskör tisztázása: egyszerű jelszavak alatt a személyhez köthető vagy alapértelmezett jelszavak használatát értjük. Hanyag hozzáállás alatt a kérdőívünkben megfogalmazott szituációk mögötti kockázatos viselkedésformákat értjük, melyhez egyéni felelősség társítható. Így nem vettük figyelembe az értékelésnél a munkahelyi beléptető rendszer, illetve az elavult munkahelyi operációs rendszer használatát sem.

Értékelés: 28 db kérdés esetén a kockázatos válaszok megoszlása

Arány (%)	0 - 25	25 - 50	50 - 75	75 - 100
Előfordulás (db)	15	9	4	0

3. táblázat: 1. hipotézis kérdéseinek megoszlása (saját szerkesztés)

Következtetés: Mivel a 28 kérdésből csak 4 kérdésre kaptunk kockázatos választ – mely nem éri el az 50%-os határt – feltevésünk nem bizonyult igaznak. A kockázatos válaszok az alábbiak voltak: adathordozók titkosítás nélküli védelme (64,8%), pendrive munkahelyi és magán célú használata (61%) gyári jelszó használata otthoni WiFi routeren (60%), valamint a munkaállomás zárolásának kerülés a géptől való felállást követően (51,4%). Összefüggésként kiemeljük, hogy akik könnyű jelszavakat választanak maguknak, azok nagy többsége még arra sem veszi a fáradtságot, hogy megváltoztassák otthoni vezeték nélküli hálózatuk gyári jelszavát. Ennek oka az lehet, hogy a könnyű jelszavakat használókat nem foglalkoztatja sem a felhasználói nevükhöz köthető adott alkalmazás, sem a saját hálózatuk biztonsága.

2. hipotézis

Azok, akik magáncélra elavult operációs rendszert használnak, nem védik kellően hálózatukat, eszközüket és felhasználói fiókjaikat sem.

Definíciók és kérdéskör tisztázása: elavult operációs rendszer alatt Windows 7 és korábbi verziót értjük, mivel a gyártói támogatása 2020.01.14-én megszűnt, így használata kockázattal jár [15]. Véleményünk szerint elavultnak számít egy újabb kiadású, de nem frissített operációs rendszer is. A nem kellő védelem alatt a hálózat vonatkozásában a nyilvános WiFi hozzáférési pontokra való csatlakozást és az otthoni WiFi hálózat gyenge jelszóval történő védelmét értjük. Eszközvédelem alatt az adathordozók titkosítását és a vírusirtók használatának mellőzését, de már a nem megfelelően kiválasztott termék használatát is ide vettük. Továbbá a munkahelyi végpontvédelmi megoldásokkal szembeni érdektelenség is kapcsolódik az eszközvédelem témájához. Felhasználói fiókvédelemnél a gyengén

megválasztott, vegyes használatú, másnak is tudomására hozott és tárolási módjából eredően könnyen megismerhető jelszavak kérdéseire adott válaszok tartoznak a régóta használt jelszavak mellett.

Értékelés: 12 db kérdés esetén a kockázatos válaszok megoszlása

Arány (%)	0 - 25	25 - 50	50 - 75	75 - 100
Előfordulás (db)	4	4	3	1

4. táblázat: 2. hipotézis kérdéseinek megoszlása (saját szerkesztés)

Következtetés: Mivel a 12 kérdésből 4-re kaptunk kockázatos választ a csoporttól, feltevésünk teljes mértékben nem bizonyult igaznak, de több területen is megállta helyét. A kockázatos válaszok az alábbiak voltak: munkahelyük vírusvédelmi szoftvere nevének nem ismerete (80,6%), gyári jelszó használata otthoni WiFi routeren (67,7%), érdeklődési körhöz tartozó rövid vagy alapértelmezett jelszavak használata (61,3%), adathordozók titkosítás nélküli védelme (54,8%). Összefüggésként megállapítható, hogy akik elavult operációs rendszert használnak, túlnyomó többségük nem ismeri, hogy munkahelyük melyik cég termékével védekezik a kártékony programok ellen. Ennek oka lehet, hogy még a saját rendszerük védelmére sem fordítanak kellő figyelmet, nemhogy érdeklődést tanúsítanának a munkahelyükön használt szoftvereket illetően.

3. hipotézis

Azok, akik felismerik egy adathalász e-mailben lévő veszélyeket, felelősséggel vannak a munkahelyük információ bizalmassága és saját munkaállomásuk védelme iránt, tehát tisztában kell lenniük szervezetük információbiztonsági szabályzatával is.

Definíciók és kérdéskör tisztázása: felismerés alatt értjük a gyanús levél törlését, csak megbízható környezetben való megnyitását vagy elemzését és összevetését korábbi hasonló e-mailekkel. A munkahelyi információk bizalmasságát nyilvános helyeken való csevegéssel, selejtes iratok nem megfelelő kezelésével és természetesen illetéktelenek részére történő adatok megadásával is meg lehet sérteni. De szintén információ kikerülésnek minősülhet, ha munkahelyi – gyengén megválasztott, másnak által ismert és felírt – jelszavunkat privát célra használjuk vagy azzal különböző weblapokra regisztrálunk. Kockázatos cselekménynek minősül továbbá más személyt saját azonosítónkkal beengedni egy objektumba. Amennyiben közösségi oldalakon munkahelyünket megemlítjük, azzal is információt teszünk közzé, bizonyos területeken (pl. rendvédelmi szervek) ez tiltva is van. Saját munkaállomásunk védelméhez a váll feletti kifigyelés elleni védelmet, valamint a takarítás vagy egyéb ok miatti zárolást vettük. Ide sorolható még az is, ha a felhasználó figyelmen kívül hagy egy számára ismeretlen hibaüzenetet.

Értékelés: 16 db kérdés esetén a kockázatos válaszok megoszlása

Arány (%)	0 - 25	25 - 50	50 - 75	75 - 100
Előfordulás (db)	1	1	7	7

5. táblázat: 3. hipotézis kérdéseinek megoszlása (saját szerkesztés)

Következtetés: mivel 16 kérdésből 14-re kaptunk kockázatkerülő, figyelmes hozzáállást tanúsító válaszokat, feltevésünk egyértelműen igaznak bizonyult. A biztonságtudatos válaszok aránya elérte a 87,5%-ot. Több megállapított összefüggés közül felsorolás szinten kiemeljük azokat, melyek olyan felhasználókra jellemzők, akik helyesen járnak el egy adathalász levél érkezését követően. Ők azok, akik ellenőrzik az idegen kollégájuk személyazonosságát, nem hagyják figyelmen kívül, ha hibaüzenet jelentkezik számítógépükön, munkahelyi e-mail címükkel nem regisztrálnak magáncélból hírlevelekre, webáruházakba. Továbbá közösségi oldalakon nem adnak meg munkahelyi információkat, munkahelyi e-mail címüket nem használják privát célra, nem írják fel jelszavukat számítógép mellé és füzetbe sem. Ennek oka lehet, a részletek felismerésének és a higgadt gondolkodásnak a képessége egy óvatos, ösztönös szabálykövető szemlélettel társul annak ellenére, hogy csak valamivel több, mint minden második ember olvasta el munkahelyük információbiztonsági szabályzatát.

A KÉRDÉSEK EGYMÁSHOZ VISZONYÍTOTT ÉRTÉKELÉSE

Hipotéziseink vizsgálata után kíváncsiak voltunk arra, hogy a kockázatos viselkedésformák hogyan viszonyulnak egymáshoz, vagyis van-e korreláció az erre vonatkozó kérdések között, s ha van, akkor hol tapasztalunk erős korrelációt. Értelmezésünkben az alábbi képlet alapján állapítottuk meg a kapcsolatot (a KVASZ a kockázatos választ adók száma):

$$\frac{viszonyított\ kérdésnél\ KVASZ}{bázis\ kérdésnél\ KVASZ} * 100$$

Az így kapott értékek besorolását az alábbiak szerint határoztuk meg: 0-25% (nincs kapcsolat), 25-50% (gyenge kapcsolat), 50-75% (közepes kapcsolat), 75-100% (erős kapcsolat). Az elemzést elvégezve a következő összegző megállapításokat fogalmaztuk meg.

- Akik ugyanolyan jelszavakat használnak magán és munkahelyi fiókjaiknál 76,9%-ban ugyanazt a pendrive-ot használják magán és munkahelyi célra is.
- Akik kerülik a vírusvédelmi szoftverek használatát, 90%-ban nem használnak titkosítást adathordozóikon és 80%-ban nem biztonságosan semmisítik meg a munkahelyi selejtes iratokat sem.
- Akik talált adathordozót behelyeznek otthoni vagy céges számítógépbe, köztük 100%-uk csak ingyenes vírusvédelmi szoftvereket használ és a pendrive-ját magán és munkahelyi célra is használja.
- Akik mellőzik az automatikus rendszer és programfrissítéseket, 88,9%-ban talált adathordozót behelyeznek otthoni vagy céges számítógépbe.
- Akik olyan munkahelyen dolgoznak, ahol nincs beléptető rendszer, 100%-ban nem biztonságosan semmisítik meg a munkahelyi selejtes iratokat, 77,8%-ban adathordozóikat titkosítási védelem nélkül használják, és gyári jelszavakat használnak otthoni WiFi routerükön.
- Akik munkahelyi e-mail címüket használják magáncélú levelezésre, 86,8%-ban pendrive-jukat magán és munkahelyi célra is használják.
- Akik elmentik bankkártya adataikat és belépési adataikat hordozható eszközeiken, 79,5%-ban pendrive-jukat magán és munkahelyi célra is használják.

- Akik munkahelyén Windows 7 vagy régebbi operációs rendszer üzemel, 80%-ban adathordozóikat titkosítási védelem nélkül használják.
- Akik ismeretlen számítógépes hibaüzenetet figyelmen kívül hagynak, 89,5%-ban adathordozóikat titkosítási védelem nélkül használják.
- Akik nyilvános helyeken munkahelyi témákról is beszélgetnek, 84,6%-ban gyári jelszavakat használnak otthoni Wifi routerükön és 76,9%-ban adathordozóikat titkosítási védelem nélkül használják.
- Akik munkahelyi selejtes irataikat kommunális hulladékként kezelik vagy hazaviszik, 77,4%-ban adathordozóikat titkosítási védelem nélkül használják.
- Akik nem zárják le számítógépüket munkahelyükön takarítás alatt, 80,4%-ban adathordozóikat titkosítási védelem nélkül használják.
- Akik nem ellenőrzik telefonon keresztül magukat kollégájuknak kiadó személy azonosságát, 79,1%-ban adathordozóikat titkosítási védelem nélkül használják.
- Akik ismeretlen feladótól vagy közüzemi szolgáltató nevében érkezett e-mailben lévő linkre vagy mellékletére azonnal rákattintanak, 83,3%-ban használnak nyilvános helyeken ingyenes WiFi hálózatot.

A fentiek alapján azt a következtetést vonjuk le, hogy amennyiben a munkahelyek vezetői – az operációs rendszer és beléptető rendszer korszerűsítéssel kapcsolatban – valamint felmérésben részt vevő személyek a többi kérdés vonatkozásában biztonságtudatosabb viselkedésre váltanának át, az pozitív változásokat idézhetne elő az erős kapcsolódással rendelkező kérdéseknél is.

Pozitív megállapítások

Az utolsó hipotézisünkben felállított pozitív gondolatmenetet tovább folytatva, a biztonságtudatos szemléletet követő felhasználók szokásait is elemeztük, mely során a bázis és viszony kérdések kiválasztását egyéni preferencia alapon döntöttük el. Ennek alapján a következő megállapításokat fogalmaztuk meg.

- Akik különböző jelszavakat használnak magán és munkahelyi fiókjukhoz, 72,8%-ban nem osszák meg másokkal jelszavukat, továbbá 56,3%-ban bonyolult, összetett jelszavakat alkalmaznak.
- Akik odafigyelnek, hogy más mögöttük állva ne láthassa meg begépelt hitelesítő adataikat, köztük 79,3%-ban nem osszák meg másokkal jelszavukat, továbbá 60,3%-ban bonyolult, összetett jelszavakat alkalmaznak.
- Akik tudatosan válasszák meg vírusvédelmi szoftverüket, 50,5%-uk meg tudta nevezni a munkahelyükön használt vírusirtójuk nevét is. Akik ismerős ajánlása alapján választanak otthonra ilyen védelmi programot, csak 37,8%-uk volt tisztában a munkahelyükön használttal. Míg, akik nem használnak semmiféle vírusvédelmet csak 10%-ban ismerték a munkahelyi vírusvédelmi programjuk nevét.
- Akik rendszeresen naprakészen karbantartják operációs rendszerüket, a szükségtelen programokat törlik, 53,2%-uk tudatosan választja ki vírusirtóját is. 56,5%-uk soha nem használ ingyenes WiFi hálózatot.
- Akik elolvasták munkahelyük IBSZ-ét, 83,2%-uk nem használja munkahelyi email címét magán célra és 89,7%-uk semmilyen weboldalra, hírlevélre nem regisztrált

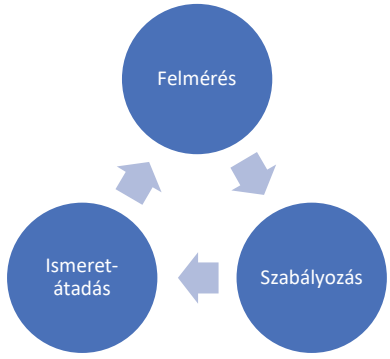
vele. 73,8%-a zárolja munkaállomását miután feláll tőle, 86,9%-uk pedig takarítás közben is vigyáz a bizalmas munkahelyi adataira. Köztük csak 14,9%-uk oszt meg magáról közösségi oldalakon olyan adatokat, mely alapján személyük beazonosíthatóvá válik és csupán 12,1%-a engedné be kollégáját saját azonosítójával. Munkahelyi témákról is 4,7%-uk beszélne nyilvános helyeken.

KÖVETKEZTETÉSEK

Kérdőíves kutatásunk eredményeként, valamint a tanulmányunk első részében nevesített hazai és nemzetközi szakirodalom feldolgozása alapján az alábbi javaslatokat teszszük az emberi jellemből fakadó social engineering típusú támadások elkerülése, felismerése és megakadályozása érdekében.

Javaslatok a biztonságtudatosság elérésére

Mint ahogy az alfejezet címe is mutatja, az elérendő cél a szervezet dolgozóiban a biztonságtudatos gondolkodás és viselkedés kialakítása, megteremtése. Hogy mi is az a fajta gondolkodásmód, ami felé terelni akarjuk a dolgozókat, ezáltal a szervezetet, mindenképp tisztázni szükséges. Az ISACA [16] definíciója a tudatosság alatt azt érti, hogy „értesültnek lenni, figyelembe venni, tudatosnak és jól informáltnak lenni egy olyan szakmai tárgykörben, mely magába foglalja az adott témakör tudását és megértését és az annak megfelelő cselekvést.” Nemeslaki és társa [17] az információbiztonsági tudatosságról alkotott fogalmában konkretizálja ezt a kérdéskört, miszerint az tulajdonképpen „egy munkavállaló általános tudása az információbiztonságról és az információbiztonsági szabályzat tudomásul vétele a szervezetben”. A fentiek tükrében megfogalmazott módszert különböző megközelítés szerint osztályoztuk, melyek egymással szoros kölcsönhatásban lévén, egymásra épülő elemeknek tekinthetőek. A kérdőív válaszaiból megállapított problémák, hiányosságok alapján egy komplex egymásra épülő megoldást javasolunk a 2. ábrán, Oroszi [13] munkájára alapozva.



2. ábra: biztonságtudatosítási folyamat körforgása (saját szerkesztés)

Felmérés. A fejlődési igénynek mindig felülről kell jönnie, azaz amíg a szervezet vezetősége nem határozza meg ezt az utat maga előtt, addig a dolgozóktól is hiú ábránd ilyet elvárni. Egy adott szervezet biztonságtudatosságát először fel kell mérni, melynek eredménye kiindulópont lesz a továbbiakban. Ez történhet kérdőívekkel, külsős személy

általi váratlan ellenőrzéssel (penetration test) vagy audit által is. Bármelyiket is választjuk, mindenképp az adott szervezetre kell szabni a kérdéseket. Ehhez a vállalat szervezeti felépítését, infrastruktúráját, bizonyos belső szabályozásait ismerni kell, hogy minél inkább életszerűbb, személyre szabottabb kérdéseket lehessen alkotni. A fentebb említett vezetőség általi támogatottság nyújtása így rendkívül fontos. Azonban nem szabad figyelmen kívül hagyni azt a tényt, hogy a felmérés tulajdonképpen már a befejezésével elavulttá válik. A kiértékelés közt eltelt időben egy új alkalmazott felvétele, új technológia bevezetése, mint eddig ismeretlen tényező, olyan kockázat megjelenését jelenti, ami nem ismert sebezhetőséget rejt magában. Fontos elérnünk a munkavállalókban, hogy egy kérdőíves felmérés kötelező jellegű kitöltését kellő komolysággal hajtsák végre, hiszen ellenkező esetben fals eredmények születhetnek. A dolgozóknak tehát meg kell érteni a social engineering jelentőségét, amivel támadás érheti egyénüket, családjukat és a szervezetüket is. Manapság egy kis családi vállalkozástól kezdve egy multinacionális cég ügyvezetője is célponttá válhat. A leghatékonyabb ellenintézkedés így az oktatáson keresztül valósulhat meg. Ismerniük szükséges a gyakori social engineering támadásokat és amennyiben találkoznak egy gyanús szituációval, kövessék az alapvető biztonsági intézkedéseket. A social engineerek ugyanis az emberi hiszékenység mellett a korlátozott mennyiségű információkra hagyatkoznak, amik az idegen emberek azonosságának ellenőrzését elősegítik. Ez utóbbi információk hiányában az áldozat el fogja hinni, hogy a támadó az, akinek kiadja magát. Felkészültnek kell lenni a gondolkodás terén is, ehhez a szkepticizmus mellett folyamatos éberség kifejlesztése is szükséges.

Szabályozás. A felmérések kiértékelését követően a már meglévő szabályzatok, előírások felülvizsgálata – vagy amennyiben nem léteznek ilyenek, akkor elkészítésük – következik. Visszautalva a kérdőívünkre a válaszadók 6,5%-a szerint a munkahelyük nem rendelkezik információbiztonsági szabályzattal. Amennyiben olyan újfajta sebezhetőségeket tárt fel a felmérés, melynek megelőzéséről eddig nem rendelkezett a szervezet, ennek megfelelő módosítása szükséges. Saját kutatásunk alapján a következő területeket szükséges szabályozni: jelszókezelés, elektronikus levelezés, munkaterület védelme, adathordozók védelme, számítógép használat, beléptetés rendje, hulladék kezelése, információk továbbítása, kommunikációs csatornák használata. Szakmailag az egyik legkézenfekvőbb választás az MSZ/EN ISO 27001:2014-es szabvány „A” mellékletét ajánlani, mely a szervezet valamennyi területét lefedi.

Ismeretátadás. Egy munkahelyi oktatási sorozat felépítésének az előzetesen elvégzett felmérések eredményein kell alapulnia, hivatkozva a szervezet aktuális szabályozásaira. Egy köremailben kiküldött szabályzatváltozásnak, újfajta rendelkezés ismertetésének a gyakorlati szinten a hatékony tudásátadás szempontjából meglátásunk szerint nem sok értelme van. Ezek az üzenetek rendszerint a napi munkamenet közben érkező levelek közé vegyülnek, kevesen vannak, akik alaposan, nyugodt körülmények közt át is olvassák őket. Így mindenképp a példákkal színesített, élő személy általi oktatást tartjuk az egyik jól bevált módszernek. E mellett persze számos másfajta lehetőséggel is élhetünk úgymint e-learning oktatás, kiscsoportos tréningek, vagy a figyelem fenntartását szolgáló kampányok és programok. Mindezek célja az ismeretterjesztés, melyet meghatározott időközönként ismételni

szükséges. A képzéseket a célcsoport igényeire és veszélyeztetettségi szintjéhez kell igazítani. Gondolunk itt a felsővezetésre, adminisztratív feladatot ellátó titkárnőkre, IT-ra, kiváltképp az üzemeltetésre valamint bármilyen speciális munkaterületre, ahol eltérő kockázatok merülhetnek fel. Az oktatást követően – rendhagyó módon – pár nappal érdemes lehet egy gyors ellenőrzés gyanánt rövid teszt kitöltése is, mely a megmaradt tudás visszamérését szolgálja. Meghatározott időközönként – amennyiben incidens nem következett be – ismételten elő kell venni az ellenőrzés eszköztárát (felmérés, pentest, audit) annak megállapítására, hogy a mindennapi munkavégzés során a dolgozókba mennyire ivódott bele az új ismeretek elméleti szinten való befogadása és implementálása a gyakorlatban. Amint látszik, ahhoz kétség sem férhet, hogy egy szervezet védekezése a social engineering ellen – annak összetettsége miatt – több dimenziós folyamat. Csak a hardveres és szoftveres védelem ez esetben nem elegendő, azonban sok esetben segítség lehet. Vírusírtók, tűzfalak, IDS/IPS-ek, honeypot-ok, phishing oldalakat észlelő böngésző bővítmények, beléptető és megfigyelő rendszerek, mind-mind hasznosak lehetnek, de a támadások középpontjában végső soron az ember áll.

FELHASZNÁLT FORRÁSOK

Irodalom

[1] Cs. Kollár, Á. Zakar, „A social engineering és a manipulációs technikák és módszerek” *Biztonságtudományi Szemle*, 2. évf. 2. szám, pp. 23-38, 2020.
[2] E. Babbie, „A társadalomtudományi kutatás gyakorlata”, Budapest: Balassi Kiadó, 2017.
[3] L. Cseh-Szombathy és Z. Ferge, *„A szociológiai felvétel módszerei”*, Budapest: Közgazdasági és Jogi Könyvkiadó, 1971.
[4] D. Freedman, R. Pisani és R. Purves, *„Statisztika”*, Budapest: Typotex, 2005.
[5] F. Moksony, *„Gondolatok és adatok”*, Budapest: Osiris Kiadó, 1999.
[6] L. Sajtos és A. Mitev, *„SPSS Kutatási és Adatelemzési Kézikönyv”*, Budapest: Alinea Kiadó, 2007.
[7] P. A. Scipione, *„A piackutatás gyakorlata”*, Budapest: Springer-Verlag, 1994.
[8] N. K. Malhotra, *„Marketingkutatás”*, Budapest: KJK-Kerszöv, 2002
[9] Zs. Bornemissza, *„Microsoft Excel függvényei a gyakorlatban”*, Budapest: Szalay Könyvkiadó, 2003.
[10] H. P. Reidmacher, *„Excel közgazdászoknak”*, Budapest: Aula Kiadó, 2000.
[11] K. L. Tóthné, *„Összefüggés vizsgálatok”*, Gödöllő: Gödöllői Innovációs Központ, 2009.
[12] K. L. Tóthné, *„Következtetés statisztika”*, Gödöllő: Gödöllői Innovációs Központ, 2009.
[13] E. Oroszi, *„Social engineering – Az emberi erőforrás, mint az információbiztonság kritikus tényezője”*, Budapest: Corvinus Egyetem, 2008.
[14] Z. Nyikes, „A biztonságtudatosság fejlesztésének egyes lehetőségei”, *XXII. Fiatal Műszakiak Tudományos Ülésszaka*, Kolozsvár, 2017.
[15] https://support.microsoft.com/hu-hu/help/4057281/windows-7-support-ended-on-january-14-2020 (letöltve: 2020.04.12.)
[16] ISACA: Glossary of terms, Rolling Meadows, IL 60008 USA, ISACA 2015.
[17] A. Nemeslaki, P. Sasvári, *„Empirical Analysis of Information Security Awareness in the Business and Public Sectors in Hungary”* Central and Eastern European e|Dem E|Gov Days 2015, Conference Proceedings