ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

NEUMANN JÁNOS
INFORMATIKAI KAR

SZAKDOLGOZAT

OE-NIK	Hallgató neve:	**Szántó Lajos**
2022	Hallgató törzskönyvi száma:	**T/008057/FI12904/N**

Óbudai Egyetem
Neumann János Informatikai Kar
Biomatika és Alkalmazott Mesterséges Intelligencia Intézet

SZAKDOLGOZAT FELADATLAP

Hallgató neve: **Szántó Lajos**
Törzskönyvi száma: T/008057/FI12904/N
Neptun kódja: [redacted]

A dolgozat címe:

Információbiztonság-tudatosság fejlesztési és mérési lehetőségei vállalati környezetben
Information security awareness development and measurement opportunities in a corporate environment

Intézményi konzulens: Dr. Póser Valéria
Külső konzulens: Szarvák Anikó

Beadási határidő: 2021. december 15.

A záróvizsga tárgyai: Informatikai rendszerek üzemeltetésének biztonsága
IT hálózatbiztonság

A feladat

A 21. században az informatikai rendszerek esetében már nem elég, ha az adatok és az informatikai rendszerek védelmét csak technikai és fizikai eszközökkel próbáljuk megoldani. Ahogy egyre szélesebb körben, és egyre több eszközben megjelenik az informatika, az adatfeldolgozás, úgy lesz egyre jelentőségteljesebb az azt felhasználó ember kihasználása, befolyásolása. Már nem lehet védelmet építeni anélkül, hogy ne vennénk figyelembe a felhasználót. Számos esetben előfordul, hogy ahol a technikai módszerek nem segítenek, vagy aránytalanul nagy idő- és energiaráfordítással lehetne behatolni egy vállalati rendszerbe, ott az ember, a felhasználó kihasználása szinte rögtön eredményre vezet. Emiatt, a technikai eszközök fejlesztése mellett az információs rendszert használó ember képzése, tudatossága is kulcsfontosságú a használt rendszer biztonsága szempontjából.
A szakdolgozat célja annak vizsgálata, hogy milyen eszközökkel lehet fejleszteni a felhasználó információbiztonsági tudatosságát, hogy a támadó Social Engineer, a felhasználó manipulációja révén ne tudjon károkat okozni vállalati környezetben.
A hallgató feladata bemutatni a leggyakrabban használt támadási technikákat, ezek elleni védekezési lehetőségeket. A feladat során ki kell térni a képzések fontosságára, továbbá ki kell dolgozni, hogy milyen módszerekkel lehet mérni a felhasználók információbiztonsági tudatossági szintjét.

A dolgozatnak tartalmaznia kell:

- a Social Engineering fogalmát, jelentőségét,
- annak vizsgálatát, hogy miért működik, vagy miért nem a Social Engineering,
- a kihasználható emberi tulajdonságok ismertetését,
- támadási formákat és kockázataikat,
- a legfontosabb képzési módszerek bemutatását,
- a képzések, tudatossági kampányok várható hatásait és összegzését,
- az oktatási módszerek védelmet erősítő, kockázatot csökkentő lehetőségeit,
- az információbiztonság-tudatosság mérésére alkalmas metrikák, módszerek kidolgozását.

ÓBUDAI EGYETEM * Neumann János Informatikai Kar * Ph 1. Budapest

.....
Dr. Eigner György
mb. intézetigazgató

A szakdolgozat elévülésének határideje: **2023. december 15.**
(OE TVSz 55.§ szerint)

A dolgozatot beadásra alkalmasnak tartom: 2022. május 06.

Szurák Pál
.....
külső konzulens

.....
intézményi konzulens

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Informatikai Kar

HALLGATÓI NYILATKOZAT

Alulírott Szántó Lajos ([redacted]) hallgató kijelentem, hogy a szakdolgozat / diplomamunka saját munkám eredménye, a felhasznált szakirodalmat és eszközöket azonosíthatóan közöltem. Az elkészült szakdolgozatomban / diplomamunkámban található eredményeket az egyetem és a feladatot kiíró intézmény saját céljára térítés nélkül felhasználhatja.

Budapest, 2022. május 10.

Szántó Lajos

.....

Szántó Lajos

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Informatikai Kar

KONZULTÁCIÓS NAPLÓ

Hallgató neve: **Szántó Lajos** ..... Neptun Kód: [redacted] ..... Tagozat: **Levelező**.....

Telefon: [redacted] Levelezési cím (pl.: lakcím): [redacted] .....

Projektmunka címe magyarul:

Információbiztonság-tudatosság fejlesztési és mérési lehetőségei vállalati környezetben

Projektmunka címe angolul:

Information security awareness development and measurement opportunities in a corporate environment

Intézményi konzulens: **Dr. Póser Valéria** .....

Külső konzulens: **Szarvák Anikó**.....

Kérjük, hogy az adatokat nyomtatott nagy betűkkel írja!

Alk.	Dátum	Tartalom	Aláírás
1.	2022. 03. 04.	Előző féléves munka áttekintése	Szay
2.	2022. 03. 15.	További tartalmi elemek, kiegészítések	Szay
3.	2022. 04. 13.	Struktúra, formázás, hivatkozások megbeszélése	Szay
4.	2022. 05. 05.	Prezentáció és szakdolgozat véglegesítése	Szay

A Konzultációs naplót összesen 4 alkalommal, az egyes konzultációk alkalmával kell láttamoztatni bármelyik konzulenssel.

A hallgató a Projektlabor 1. / 2. / 3. / Záródolgozati projekt[1] tantárgy követelményét teljesítette, beszámolóra/védésre[2] bocsátható. A javasolt érdemjegy: 5

.....

Intézményi konzulens

Budapest, 20.22. május 06.

---

[1] A megfelelő bekarikázandó/aláhúzandó!

[2] A megfelelő aláhúzandó!

KÖSZÖNETNYILVÁNÍTÁS

Szeretnék köszönetet mondani konzulenseimnek és az Óbudai Egyetem oktatóinak, irodai dolgozóinak, akik közvetve, vagy közvetlenül segítettek tanulmányaimban és e szakdolgozat megírásában.

Szántó Lajos

TARTALOMJEGYZÉK

1. BEVEZETÉS

Manapság is igaz az, ha információs rendszerből szeretne valaki adatot ellopni, akkor nem kell felétlenül alapos szinten értenie az informatikai hálózatokhoz és a számítógépes rendszerekhez. A hackerek egy jó része, akik adatot lopnak, illetve információt akarnak megszerezni egy informatikai rendszerből, nem feltétlenül rendelkeznek mély tudással az informatikai hálózatok terén, inkább jó szociális érzékenységgel bírnak, jó emberismerők. Ezek a hackerek nem a számítógépes hálózaton keresztül jutnak be a hálózatunkba, és érik el az adatainkat, hanem sok esetben a bejárati ajtón jönnek be. Hiszen miért törné magát valaki a hálózat feltörésével, miért szánna rá hosszú napokat, ha csak simán bemehet a bejárati ajtón?

Bármikor, ha emberek átverésével kapcsolatos biztonsági incidensről hallunk, megjelenik a social engineer fogalma. Magát a kifejezést nem egyszerű szó szerint magyar nyelve fordítani, véleményem szerint talán átverésnek, vagy megtévesztésen alapuló támadásnak lehetne fordítani. Hogy mit is jelent ez, abban még mindig helytálló Kevin D. Mitnick megfogalmazása: *„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.”* [1]. Lényegében a social engineer hacker manipulálja és megtéveszti az embereket, nem etikus módon használja azokat az emberi kapcsolatokhoz tartozó viselkedési formákat, amit egyébként a mindennapokban használunk. Például, hogy szívességeket teszünk egymásnak, segítjük egymást, kíváncsiak vagyunk [2].

2020-ban feltörték a Twittert, a közösségi média egyik meghatározó oldalát. A Twitter több, mint 40 milliárd dollár értékű cég, komoly szakembergárdával és a legmodernebb informatikai eszközökkel rendelkezik. Ennek ellenére social engineer módszerek segítségével sikerült feltörni. Egészen addig eljutottak a támadók, hogy képesek voltak a legbefolyásosabb felhasználói fiókok bejegyzéseit is módosítani. A Twitter ezek után több biztonsági intézkedést vezetett be. Egyik ilyen az adminisztrátorok számára a kétfaktoros hitelesítés, és amit még kiemeltek, hogy az egész vállalatra kiterjedő képzést vezettek be a social engineer technikák elleni védekezés érdekében, kiegészítve folyamatos adathalász szimulált gyakorlatokkal [3][4].

A szakdolgozatom célja, hogy az előbbihez hasonló, manipulatív támadásokkal kapcsolatos védekezést segítsem. A social engineering, illetve ennek megjelenése, működése, a védekezés hatalmas terület, ennek itt egy kis szeletét tudom bemutatni. A kiemelt részek azért kerültek a dolgozatba, mert alapvetően tükrözik a social engineer szempontú eseményeket.

A szakdolgozat elején tisztázom, hogy a hackerek miért támadják az embert, az adott szervezet alkalmazottját és az információbiztonság szempontjából az emberi tényező miért fontos. Néhány területet kiemelek, ami információbiztonság-tudatosság tekintetében lényeges, mint például a közösségi média, vagy ami manapság nagyon aktuális, a Home Office. A szabványok bevezetése nagy segítséget jelent egy szervezetnek a biztonság kialakításában. Ehhez kapcsolódóan megvizsgálok néhány jelentősebb szabványt, ajánlást, hogy ezekben milyen szinten segítik az alkalmazott információbiztonság-tudatosságának növelését, fejlesztését.

Az információbiztonság-tudatossági képzések kapcsán találkozunk az információbiztonság-tudatosság fogalmával. Ennek pontos definiálása nem egyszerű feladat, mivel ahányan foglalkoznak a témával annyiféle definíciót lehet olvasni [5], persze mindegyik igaz, és megfelelő értelmezésben elfogadható. Én leginkább Tarján Gábor megfogalmazásával értek egyet, ez így hangzik: *„Az információbiztonsági tudatosság a szervezet érdekelt feleinek tudása és attitűdje a szervezet tulajdonában vagy kezelésében lévő információs javak védelmével kapcsolatban.”* [6]. A szakdolgozatommal ennek a tudásnak a bővítésében és a viselkedés, hozzáállás megértésében segítek.

A social engineeringnek komoly pszichológiai vonzata van, így megvizsgálom, hogy az emberi természetnek milyen alapvető mozgatórugói lehetnek. Ez fontos kiegészítője annak, hogy megértsük, hogy a manipulációs támadások hátterében milyen okok lehetnek, ezzel is segítve a védekezést. Ha védekezésről beszélünk, tudnunk kell, mi ellen védekezünk. Összegyűjtöm a leggyakoribb social engineer támadási formákat, melyikre mi jellemző és segítséget adok az ellenük való védekezésben. Az egyértelmű lesz, hogy a lista nem lehet teljes. Mindig van újabb támadási módozat, még kifinomultabb módszer, vagy vállalatra szabott stratégiája a hackernek.

A szakdolgozat egy jelentős részében a védekezés módjaival foglalkozom. A social engineering támadások elleni védekezés és az információbiztonság-tudatosság fejlesztése egy több lábon álló folyamat kell, hogy legyen. Ezek elemei lehetnek a kockázatok feltárása, a szabályozási környezet, a biztonságtudatossági oktatás, és a biztonságtudatossági program. Ezek lehetőségeit, illetve a megvalósítás módját részletezem, összegyűjtök számos, a biztonságtudatossági programban használható eszközt és ezek használatára adok javaslatot. A kockázatok kapcsán megemlítem, ennek milyen csökkentési módjai lehetnek, a szabályozási környezetnél az Informatikai Biztonsági Szabályzatot emelem ki. A felelősség kérdéséről is írok, de itt egy lényeges gondolata az, hogy social engineer támadások kapcsán nem lehet behatárolni egy bizonyos munkakört, vagy alkalmazottat. Mindenki célpont, mindenki befolyásolható valamivel.

Ezek után megvizsgálom, mik azok a tényezők, amelyek befolyásolják a biztonságtudatos magatartást. Ezek a tényezők alapvetően befolyásolják azt, hogy

mitől működik és mitől nem a social engineering, ezen kívül ezek ismeretében hatékonyabban lehet szervezni a biztonságtudatossággal kapcsolatos feladatokat. Ebből a szempontól az egyik legfontosabb tényező az, hogy adott személy érzelmileg hogyan áll a biztonságtudatossághoz.

Az oktatások hatékonyságának vizsgálatára a Kirkpatrik-módszer kerül bemutatásra [7]. Ez négy szintből áll: Reakció, Tanulás, Viselkedés, Eredmény szintek. Mindezeket az információbiztonsági oktatásokra vonatkoztatom, azt próbálom bemutatni, ez hogyan segíti a képzések értékelését. A biztonságtudatossági programok eredményességéhez pedig, hogy mennyire sikeres egy program, a mérőszámok jelentenek segítséget. Ezt azzal támogatom a szakdolgozatomban, hogy bemutatok egy hét lépéses módszert ezek meghatározásához, kezdve azzal, hogy mi a célja a saját mérőszámoknak, egészen addig, hogy ellenőrizzük azt, hogy elértük-e a kívánt célt. Az auditot még fontosnak tartom, mint a biztonságtudatossági mérések, értékelések egyik lényeges eszközét. Ez többfajta formában alkalmazható, ezeket is részletezem a szakdolgozatban.

2. A SOCIAL ENGINEERING JELENTŐSÉGE

Számos területen és aspektusból meg lehetne és kell is vizsgálni a social engineering, illetve a biztonság tudatosság jelentőségét egy szervezeten belül. Ebben a fejezetben néhány, a vállalati környezetet érintő területtel foglalkozom, mivel fontos megérteni, hogy az információbiztonság szempontjából az emberi tényező miért fontos. Van néhány terület, ahol az embert kihasználó támadások fokozottan jelentkeznek, és külön figyelmet érdemel.

2.1 Miért az embert?

Az embert is tekinthetjük egyfajta központi elemnek az informatikai rendszerben, és a vállalat lényeges folyamataiban. Az ember információt, adatokat juttat a rendszerbe és adatokat szed ki onnan, és nem utolsó sorban töröl, döntéseket hoz, irányít másokat, és irányítja az eszközöket. Ha támadó befolyásolni tudja az embert, mondhatjuk azt, hogy ő irányítja az információs rendszert, az átvert munkatárs pedig mintegy a támadó meghosszabbított láthatatlan keze végzi a témadó által elvárt műveletet [1][8].

Az az illető, aki használja az eszközeit, sok esetben bizalmas, vagy céges adatot tárol rajt. Ha ez egy hordozgató eszköz, akkor azt nagyon könnyen elveszítheti, vagy a támadónak igazából elég csak az adathordozót észrevétlenül ellopni.

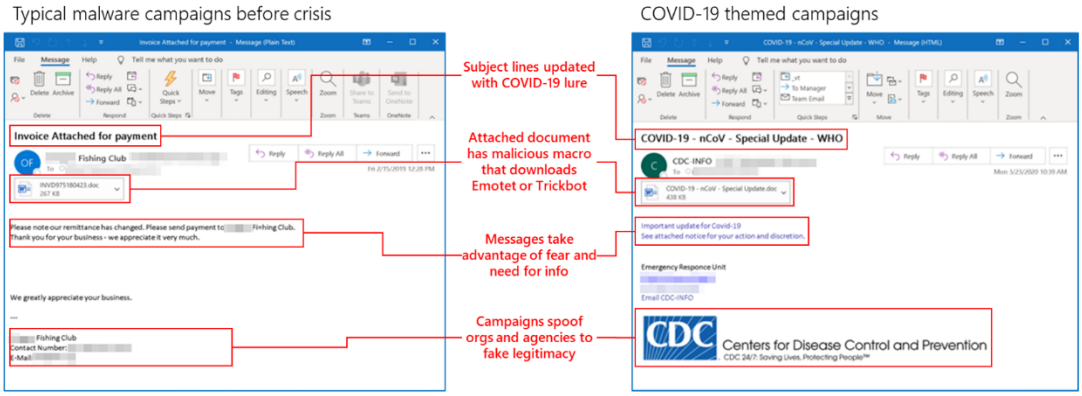
A felhasználó szoftverekkel dolgozik, ő látja a munkavégzéshez szűkséges fájlokat, megosztásokat, elér adatbázisokat, könyvtárakat. Ebben az esetben például a jogosultság igénylésben lehet kiskapukat kihasználni.

A céges alkalmazott hozzáfér belső információkhoz. A legtöbben úgy gondolják, hogy a belső információ nem értékes, hogy az az információ, amire nem mondták rá kimondottan, hogy bizalmas információ, az nem is annyira fontos, emiatt megosztható. Gyakran az ilyen belső információkat megosztják partnerekkel, vendégekkel, külső személyekkel is. A támadó belső információkhoz jut, megismeri a belső folyamatokat, kicsit a céges szokásokat is, így könnyebben kiadhatja magát kollégának, beosztottnak, hisz ismeri a belső szlenget.

Az alkalmazott tartja kapcsolatot a partnerekkel, ügyfelekkel, egymással, vezetőkkel. Ebből a szempontból azok a folyamatok jelentenek nagyobb kockázatot, ahol a tárgyaló beszélgetőpartnerek nem ismerik személyesen egymást. Ilyenkor nem, vagy csak nagyon nehéz meggyőződni, hogy a másik fél tényleg az-e, akinek mondja magát. Ilyen például az e-mailben, vagy telefonon keresztül történő kapocslattartás, ahol sok esetben csak egy nevet látunk. Az efféle csalásokhoz nem kell komoly technikai tudás. Hogy mennyire könnyű átverni az embereket, még akkor is, ha komoly technikai tudással rendelkező nagyvállalatnál dolgoznak, annak egy tipikus példája a 2017-ben történt csalás, amit egy litván férfi és emberei követtek el a világ két legnagyobb vállalata, a Facebook és a Google ellen [9]. A férfi és csapata olyan hamis céget

alapított, amelynek a neve megegyezik egy ázsiai hardvergyártó nevével, ezen kívül számos bankszámlát nyitott különböző országokban. Ezután adathalász e-maileket küldözgettek Facebook és Google dolgozóknak, amelyben azt kérték tőlük, hogy korábbi szolgáltatásért járó összeget egy megújult bankszámlaszámra küldjék. Ezzel a módszerrel, egyszerű adminisztrációval több, mint 100 millió dollárt sikerült átutaltatniuk.

Az aktualitások olyan lehetőségeket jelentenek a hackereknek, amit biztos, hogy kihasználnak. A COVID-19 világjárvány kapcsán a csaló üzenetek tartalma az általános problémáktól eltolódott a járvánnyal kapcsolatos témák felé. A 2.1. ábrán egy valós példa szerepel rosszindulatú e-mailre. Látható, hogy az e-mail szerkezete nem változik, viszont illeszkedik az aktualitásokhoz [10]. A járvány által keltett egészségügyi helyzet, a bizonytalanság, félelem, a kíváncsiság olyan lehetősséget teremtett, amit a hackerek social engineering támadásokra kihasználnak. Már 2020 első hónapjaiban jelentősen megnőtt a járvány témáján alapuló támadások száma. A Deloitte tanácsadó cég elemzése szerint a járvány korai szakaszában 234%-kal nőtt a COVID-19-hez kapcsolódó domainek regisztrációja [11].



2.1. ábra: *ugyanaz a rosszindulatú email COVID-19 járvány előtt és után.*

2.2 Közösségi média

Összesen a közösségi médiát 4,6 milliárd ember használja [12][13]. Ez a hatalmas szám az információszerzés tekintetében a támadóknak hatalmas lehetőséget jelent. Ezek az oldalak az információgyűjtésben segítenek, ugyanis a munkatársak számtalan, a munkáltató szervezetet is érintő információt megosztanak. Ezen keresztül a vállalatot is támadhatják, ha például az alkalmazott kirakja az internetre, hogy ő éppen nyaral, a megszemélyesítéses támadással célt lehet érni.

Jellemző módszer, hogy a támadó nyílt forrású információgyűjtést folytatva feltérképezi az adott cégnél dolgozókat. Ennek sikerétől függ a következő lépés, a támadó olyan jelöltet keres, aki hasznos lehet számára. Fontos azt tudni, hogy a támadónak nem feltétlenül fontos, hogy olyan embert találjon, aki magas beosztásban

van, elég olyan, akinek van hozzáférése a kérdéses rendszerhez, de a biztonság-tudatossága alacsony.

2.3 Home Office

A távmunkának egyre nagyobb a népszerűsége, és jellemző, hogy egyre több vállalat kínálja ezt a módszert a munkavállalóknak. Ennek lehetnek gazdasági okai is, vagy lehet kényszer is, mint például a COVID-19 járvány. Ekkor a munkavégzés jellemzően otthon történik saját, vagy a cég eszközein. Ebből a szempontból a cég eszközei talán biztonságosabbak mondhatók, mert egy szervezet informatikai osztálya valamennyire mindenképp figyel a biztonságos eszközhasználatra. Ha nagy szervezetről beszélünk, biztos, hogy jelszó kell a belépéshez és van erősebb vírusvédelmi szoftver a gépen. Ezek az otthon használt eszközökre általában nem jellemzőek.

A munkavállalók többsége a biztonságot a munkahelyhez köti. Pedig meg kell értenie, hogy attól, hogy otthon végzi a munkáját, ugyanúgy törődnie kell a biztonsággal. Azok a veszélyek, amit a munkahelyen megjelenhetnek, az otthoni munkavégzés során is előfordulhatnak. Sőt azokkal szemben, akik otthonról dolgoznak, a helyzetből adódóan sokkal könnyebb bizonyos social engineer támadásokat végrehajtani. A támadó megteheti, hogy végrehajt egy megszemélyesítéses támadást, hiszen ilyenkor általában telefonon, vagy e-mailben kommunikálnak a kollégák egymással. Ekkor könnyebb elhitetni az áldozattal, hogy a támadó a cég egyik alkalmazottja, vagy valaki más, magas beosztott utasítására cselekszik.

2.4 Az emberi természet működtetői

Az emberi pszichének is vannak régóta kutatott törvényszerűségei, amiket fontos megemlíteni, mivel döntő jelentőségűek lehetnek abban, hogy mennyire érvényesül az információbiztonság-tudatosság. Az ismert pszichológus, Robert B. Cialdini, több könyvében is, többek közt a Hatás – a Befolyásolás pszichológiája c. könyvében foglalkozik az emberi természet hat alapvető hajlamával [14]. Az emberben ezek nagyon mélyen gyökerező hajlamok, mindenkiben benne vannak, kisebb-nagyobb mértékben, sokszor nagyon egyszerűen lehet ezekre a jellemzőkre social engineer támadást alapozni [1].

A Hatalom: az embereket könnyű rávenni egy kérésre, ha az a felettesétől származik, vagy egy olyan személytől, akiről az áldozat azt hiszi, számára utasítás kiadására jogosult. Ez lehet egyszerűen az emberi természet velejárója, vagy vállalati kultúra, vállalati belső szabályozás. Social engineer támadóként, magát vezetőnek kiadva, remekül lehet utasítást adni az alkalmazottnak, csak azt kell elérni, hogy az áldozat higgyen abban, hogy akivel beszél, az egy számára hatalommal bíró kolléga, vezető.

A Szeretet: az egyik legerősebb késztetés. Az emberek hajlamosak sok mindent megtenni annak, akik számukra szimpatikus, vagy kiderül, hogy vagy közös

érdeklődési körük, véleményük, hasonlít hozzájuk. A támadó ebben az esetben visszaél az áldozat bizalmával, próbál kialakítani bizalmas viszonyt. Kideríti, mi érdekli az áldozatot, elhitetni vele, hogy őt is ugyanaz érdekli.

A Kölcsönösség: ha kapunk valamit, szeretjük meghálálni, ha valaki megtesz értünk valamit, szeretjük viszonozni. Nagy eséllyel az emberek teljesítenek egy kérést, ha cserébe ígérnek számukra valamit, esetleg valami értékes dolgot. A támadó arra használja ezt az emberi jellemzőt, hogy valamiféle ajándékot ad a kiszemelt személynek, akiben benne lesz az a késztetés, hogy ezt viszonozza. Az áldozatnak adott ajándék nem feltétlenül valós, fizikai tárgy, hanem lehet akár korábbi segítségnyújtás is.

A Következetesség: szeretünk következetesen viselkedni, hogy mások tiszteletét kivívjuk, elismerjenek minket. Ha valakinek megígértünk valamit, akkor az általában próbáljuk betartani. Nem akarjuk, hogy felelőtlennek, vagy megbírhatatlannak tartsanak minket. A támadó ezt azzal tudja kihasználni, hogy korábban megígértet valamit a kiszemelt személlyel. Ez lehet, hogy a korábbi beszélgetések alkalmával nem volt annyira fontos, de később az áldozattal beszélve ezt felhozhatja, és számon kéreti, hogy tartsa be az ígéretét.

A Társadalmi megerősítés: egy emberi közösség, társadalom részei vagyunk. Az emberek sokszor úgy viselkednek, hogy ne okozzanak feltűnést, ne botránkoztassanak meg embereket, cselekedeteik legyenek összhangban a társadalmi elvárásokkal, megcsináljuk azokat a dolgokat, ami mások. A támadó ezt kihasználja úgy, hogy arra hivatkozik, hogy a többiek mér megtettek valamit, ami fontos. Hivatkozik a munkatársakra, akik már együttműködtek (ami persze nem biztos, hogy igaz), ezzel ösztönözve az áldozatot, hogy ő is együtt működjön, adjon meg bizonyos adatokat.

A Szűkösség: az emberek teljesítenek egy kérést, ha cserébe kapnak egy lehetőséget, ami előnyhöz juttatja őket. Ez fokozottan igaz, ha a felkínált előnyből kevés van. A támadó felkínálhat az alkalmazottnak egy olyan ajándéktárgyat, ami érdekelheti az áldozatot, és amiért sokan versengenek. De további erős motiváció lehet az alkalmazottnak, hogy végre tudja hajtani a támadó kérését, ha anyagi jutalmat, vagy más, a munkájával kapcsolatos előnyt kaphat a kért feladat elvégzéséért.

2.5 Támadási formák és kihasználható jellemzők

Az alábbi táblázatban összefoglaltam a legjellemzőbb támadási formákat és azokat a jellemzőket, amiket az adott támadási formához a támadó kihasznál [15]. Ezt azért fontos ismerni, mert a védekezést jelentősen segíti, ha tudjuk, mi ellen kell védekezni. A felsorolt fogalmak az egyik legjellemzőbbek.

Az *Emberi tulajdonság* oszlopban azok a tulajdonságok láthatók, amik lehetnek egy ember személyiségjellemzője, viszont stresszhelyzetben előjöhetnek olyannál is, akire

egyébként nem jellemző. A *Munkahelyi szituáció* oszlopban a munkahelyen előforduló körülményeket írtam. A *Pillanatnyi érzelmi állapot* oszlopban egy jellemzően rövidebb ideig tartó, nem állandósult emberi állapot került.

Jól kivehető a táblázatból, hogy egy-egy támadásra nem jellemző csak egy adott helyzet, egyfajta támadáshoz sokszor elég egyetlen tulajdonságot kihasználni. Ha tudatosság elég magas szintű, akkor nem áll elő kihasználható tulajdonság, emiatt pedig a támadást nem lehet végrehajtani. A támadási módszerek, és jellemzők részletes kifejtése a Mellékletben található [15].

Támadási módszer	Emberi tulajdonság	Munkahelyi szituáció	Pillanatnyi érzelmi állapot
szoros követés *védekezés: megfelelő beléptető rendszer, vendégkártya*	segítőkészség, naivitás, hanyagság	segítő munkakör bosszú	fáradtság figyelmetlenség
besurranás *védekezés: megfelelő beléptető rendszer*	hanyagság, lustaság,	napi rutinmunka	fáradtság, kapkodás
rápillantás *védekezés: takarás, biometrikus azonosítás, kártyás belépés*	naivitás, barátságosság	megtévesztés bosszú	kapkodás figyelmetlenség
megszemélyesítés, megtévesztés védekezés: a partner egyértelmű azonosítása, belépőkártya	segítőkészség, barátságosság, befolyásolhatóság, lustaság	új munkatárs napi rutinmunka segítő munkakör elégedetlenség megtévesztés zsarolás bosszú	fáradtság, kapkodás figyelmetlenség túlterheltség távollét betegszabadság

Támadási módszer	Emberi tulajdonság	Munkahelyi szituáció	Pillanatnyi érzelmi állapot
kéretlen levelek *védekezés levélszemét szűrő, vírusírtó*	kíváncsiság, közösségi média	elégedetlenség	fáradtság túlterheltség távollét ünnepek
lánclevelek *védekezés: levélszemét szűrő, vírusírtó*	barátságosság, kíváncsiság, közösségi média	elégedetlenség	figyelmetlenség túlterheltség ünnepek
adathalász levelek *védekezés: a partner egyértelmű azonosítása, levélszemét szűrő, vírusírtó, rendszerfrissítések*	naivitás, kíváncsiság, befolyásolhatóság, eltúlzott közösségi média használat	megvesztegetés új munkatárs napi rutinmunka elégedetlenség megtévesztés	fáradtság kapkodás figyelmetlenség túlterheltség távollét ünnepek betegszabadság
kártékony kódok terjesztése *védekezés: központilag menedzselt vírusírtó*	lustaság, hanyagság, közösségi média	megtévesztés zsarolás bosszú	kapkodás figyelmetlenség túlterheltség
csali *védekezés: központilag menedzselt biztonsági beállítások, vírusírtó*	naivitás, kíváncsiág, hanyagság	megtévesztés bosszú	figyelmetlenség

2.1. táblázat: *Támadási formák és emberi tulajdonságok.*

3. HOGYAN LEHET VÉDEKEZNI?

Azért, hogy az információbiztonság-tudatosságot fejleszteni lehessen és az elvárt szinten legyen tartva, a social engineering támadások ellen egy több lábon álló védelmi intézkedést érdemes bevezetni, ezek a következők lehetnek [15]:

- Kockázatok feltárása: milyen emberekre jellemző tulajdonságot tud kihasználni a támadó. Fontos, mert oktatások során ehhez lehet kötni a védelmi intézkedéseket, kontrollokat.
- Szabályozási környezet: milyen betartható szabályzatokat kell létrehoznunk, ezeket el kell fogadtatnunk a munkavállaókkal, és meg kell értetni a szükségességét.
- Biztonságtudatossági oktatás: oktatások lebonyolítása, hogy a munkavállalók megértsék a kockázatokat, és védekezni tudjanak ellene
- Biztonságtudatossági program: információbiztonság-tudatosság szinten tartása

3.1 Kockázatok feltárása

Ennek során információbiztonsági kockázatelemzést végzünk. A módszer lehet egyedi, a korábban leírt lehetőségek közül a legcélravezetőbbet használva. Előfordulhat, hogy egy csoportnál a kérdőíves felmérés a legjobb, míg másoknál egyfajta személyes interjú. Itt a cél az, hogy megtudjuk, hogy a munkavállalókat lehet átverni egy social engineering támadással, az átverések ellen mennyire hatékonyak az általunk hozott biztonsági intézkedések, kontrollok [16]. Kiderülhet, hogy az előbb említett támadás mely munkavállalói csoportokat érintheti leginkább, a tudásukban hol jelentkeznek a legnagyobb hiányosságok.

A 3.1. táblázatban néhány példán keresztül kerül bemutatásra a social engineering jellegű kockázat. Természetesen ez nem egy teljes értékű kockázatelemzés, az egy sokkal összetettebb táblázatot eredményezne. Nincs figyelembe véve a károkozás mértéke és a bekövetkezés valószínűsége. Látható, hogy az ember jelentette kockázatokat milyen veszély fenyegeti és milyen témájú oktatással lehet ezen kockázatokat csökkenteni. Ahogy itt is látszik, ha oktatási módszerekkel szeretnénk a védelmet erősíteni és kockázatot csökkenteni, mindig az adott kockázatra adott válasszal kell ezt megtenni. A munkavállaó sokkal jobban megérti a kockázatot és annak csökkentési lehetőségét, ha a szervezetre, illetve rá nézve személyes veszélyekről kap tájékoztatást. Ezen kívül az oktatásnak is kell, hogy legyen konkrét, szervezetre szabott célja, csak így lehet csökkenteni azt a bizonyos konkrét kockázatot és erősíteni a védelmet.

A lista nem teljes, számos, az adott szervezetett érintő, speciális kockázatot lehet felsorolni. Egy-egy témával kapcsolatos oktatási téma sem kizárólagos, ezek a témák mind átnyúlhatnak egy másik kockázatra.

A kockázatértékelés során feltárt hiányosságokat a biztonságtudatossági oktatás, vagy kampány részévé kell tenni, a súlyosságtól függően helyet kell kapnia az oktatási anyagokban.

Emberi kockázat	Lehetséges social engineer támadási módszer	Oktatás segítségével a kockázat csökkentésének egy lehetséges módja
beléptető rendszer nem megfelelő használata	szoros követés besurranás	Példákkal, dokumentációkkal alátámasztva kell képezni a kollégákat az épületbe való belépés menetéről. A legjobb, videóval fotóval illusztrálva.
Ajtók záródására nem figyel	szoros követés besurranás	Az adatvédelem fizikai oldalát kell bemutatni képzés során
Nem figyel a képernyő, mobil eltakarására	rápillantás	El kell magyarázni, miért fontos eltakarni egy kijelzőt, amin kényes adatok jelennek meg, figyelni kell a körülötte lévő emberekre. Ez nem csak munkahelyi környezetre vonatkozhat (utazás).
Nem ellenőrzi a hívó félt (lustaság)	megszemélyesítés megtévesztés	Ajánlott képzés során szimulálni, bemutatni egy telefonhívást, a tipikus támadási módozatokat elpróbálni
Nem olvassa alaposan a leveleket	kéretlen levelek lánclevelek	Tájékoztatás a hivatalos, és nem hivatalos, kéretlen levelek felépítéséről, jellemzőiről, szóhasználatáról. Mintát mutatni.
Szórakozásból, unalomból továbbít levelet	lánclevelek	Fontos annak megértése, hogy a lánclevelek tartalmazhatnak vírust, vagy adathalász oldalra mutató linket.
Munkaállomás nem megfelelő használata	kártékony kódok terjesztése lánclevelek	A munkavállalónak meg kell értenie, hogy a munkahelyi számítógépe egy munkaeszköz, csak a munkavégzés céljára lehet használni. Tájékoztatás a malware-ek működéséről, különös tekintettel a zsaroló vírusokra.

Emberi kockázat	Lehetséges social engineer támadási módszer	Oktatás segítségével a kockázat csökkentésének egy lehetséges módja
Kíváncsi az adathordozóra	csali	Arról kell oktatás a munkavállaónak, hogy jut be kártékony szoftver az informatikai hálózatba. Erre vonatkozó szabályzatok ismertetés.
Nem szólít meg idegent az épületben	megszemélyesítés megtévesztés	Az adott helyzetre vonatkozó munkahelyi szabályozás ismertetése.
Meggondolatlan információmegosztás	adathalászat megtévesztés megszemélyesítés megtévesztés	Meg kell értetni a kollégákkal, hogy jelentéktelennek tűnő információ megosztása is fontos lehet egy támadónak.
Belépőkártya átadása kollégának, elvesztése	megszemélyesítés megtévesztés	Az adott helyzetre vonatkozó munkahelyi szabályozás ismertetése. Szankciók ismertetése
Tárgyalóasztalon, ebédlőben felejtett dokumentumok	rápillantás megtévesztés	Erre vonatkozó szabályzatok ismertetése, adatlopás következményei, szankciók ismertetése

3.1. táblázat: *lehetséges social engineer jellegű kockázatok, lehetséges támadási módok és a kockázat csökkentésének lehetőségei.*

3.2 Szabályozási környezet

3.2.1 Szabványok, ajánlások

Az információbiztonsággal foglalkozó szakembereknek rá kellett jönniük, hogy az embert, mint a vállalati rendszer információbiztonsági kockázati tényezőjét nem lehet figyelmen kívül hagyni. Így a munkavállalók képzésének fontossága, a biztonságtudatosság növelése különböző szabványokban is megjelent. Ezek közül kiemelek néhányat:

ISO27001

Az ISO27001 [17][18] szabványban is megjelennek a munkavállaó tudatossági képzésére, fejlesztésére vonatkozó előírások. A szabvány erre vonatkozó pontjának célja, hogy az alkalmazottak tisztában legyenek az információbiztonsági fenyegetésekkel, felelősségükkel, kötelezettségükkel, munkájukkal támogassák az adott szervezet biztonságpolitikáját, ezzel is csökkentve az emberi tényezőből eredő kockázatok csökkentését.

A szabvány több pontban, így itt is kiemeli a vezetők felelősségét. Ők gondoskodnak arról, hogy az alkalmazott a megfelelő biztonsági előírásokat betartsa, eszerint végezze munkáját. Továbbá ők biztosítják az alkalmazottak részére az eszközök helyes használatáról szóló információbiztonsági oktatásokat, biztonságtudatossági képzéseket.

A 7.1 pontban szerepel, hogy milyen kötelezettségek és követelmények vannak a munkavállalóval szemben. A 7.2 pontban foglaltak szerint a foglalkoztatás során fontos, hogy a tudatossági képzés itt is megtörténjen rendszeresen (éves rendszerességű), vagy valamilyen képzési program a vállalat igényeire testre szabva, az üzleti célokhoz igazítva.

Felvételkor az új dolgozó számára a lehetséges, éppen aktuális sérülékenységeket, adatszerzési kísérleteket külön érdemes kiemelni. Ezen kívül az incidensek kezelése vagy a szokatlan események kezelése is szerepet kapjon.

A 7.3.1 a foglalkoztatás utáni esettel foglalkozik, eljárásrendet ír elő a visszavételről, ennek is szerepelnie kell a szabályzatban.

NIST

Az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézete (NIST) által kiadott 800-as sorozatú ajánlása foglalkozik az informatikai biztonsággal. Ez különböző területek információ biztonsággal foglalkozó dokumentumaik összessége, biztonsági kontrollok, praktikus útmutatók gyűjteménye. Magyarázatot, implementálási segédletet és iránymutatást adnak. Az informatikai biztonság tudatosításával kapcsolatban két ajánlást emelek ki: *NIST Special Publication 800-53 Rev5* [19] és *NIST Special Publication 800-50* [20].

A *NIST Special Publication 800-53 Rev5 Security and Privacy Controls for Information Systems and Organizations* kiadvány *Awareness and training* fejezete kiemeli a biztonsági és adatvédelmi szabályzatok fontosságát, kapcsolódó kockázatkezelést. Ezen kívül útmutatást, gyakorlati tanácsot ad az információbiztonsági képzés és tudatosság növeléséhez.

A *NIST Special Publication 800-50 Building an Information Technology Security Awareness and Training Program* kifejezetten az információbiztonsági tudatosító kampányok fejlesztésével és képzésekkel foglalkozik. Nagyon jó kiindulási alap, ha teljesen az alapoktól kell felépíteni információbiztonság-tudatossági programokat, képzéseket. Az ajánlásban segítségek kapunk a programok megtervezéséhez, fejlesztéséhez és a megvalósításhoz.

COBIT 5

A COBIT (Control Objectives for Information and Related Technology) szabvány [21] az informatikai vezetés egyfajta keretrendszere [22][23]. Üzleti követelményeken alapuló vezetéstámogatási, auditálási módszertant kínál, információs folyamatokra ír elő követelményket. Az szabványban fontos szempont a vállalati cél és az érdekelt felek összefüggései, egymásra hatása. A vállalati célok egy kiemelet megvalósítási tényezője az emberi erőforrás, készségek és képességek.

Az *APO07 Emberi erőforrás kezelése* folyamat nyújt útmutatást az emberi veselkedéssel kapcsolatban. Kifejti, hogyan kell a vállalati célokat összehangolni az egyéni teljesítménnyel, hogyan kell a szerepeket és felelősségeket meghatározni. Kiemelt szerep jut az ember, mint erőforrás folyamatos képzésének, ezek rendszeres ellenőrzésének.

2013. évi L. törvény

A 2013. évi L. törvény értelmében a kormányzat eseménykezelő központot működtet a polgári nemzetbiztonsági szolgálatok irányításáért felelős miniszter irányítása alatt. Ezen eseménykezelő központ számos feladata közül az egyik az, hogy „a biztonságtudatos felhasználói magatartás elősegítése céljából oktatási anyagokat dolgozhat ki és tréningeket tarthat, felvilágosító, szemléletformáló kampányokat szervezhet.” [24].

3.2.2 Az Információbiztonsági Szabályzat

Az információbiztonsági szabályozás egyik legfontosabb dokumentuma az Információbiztonsági Szabályzat (IBSZ). Ebben a felhasználókra vonatkozó szabályokat írjuk le részletesen, érthetően, általában egy hosszú terjedelmű szabályzat. Fontos, hogy elfogadható és betartható legyen a munkavállalók számára. Ugyanebben a szabályzatban tehetjük közzé az információ biztonsági kontrollokat, védelmi intézkedéseket. Például azt, hogy a munkahelyre történő belépésnek milyen protokolljai vannak, ki, mikor, miért léphet a vállalat területére, ezt ki ellenőrzi.

A könnyebb érthetőség és elfogadás miatt érdemes lehet egyes részeket, mint külön szabályzatot létrehozni és az alap IBSZ dokumentumban hivatkozni ezekre. Ilyen önálló, de az IBSZ-hez tartozó szabályozás lehet például az Auditálási szabályzat. Ebben rögzíteni lehet, hogy mikor, hogyan lehet információ-biztonsági auditot végrehajtani, vagy hogy hogyan ellenőrizheti a munkáltató az információbiztonsági előírások betartását.

A szabályzatok egyik sarkalatos pontja az alkalmazottak felé történő terjesztése. Attól, hogy elkészül egy új szabályzat, vagy módosul egy, nem jelenti azt, hogy mindenki tud is róla. Megfelelően kell kommunikálni az alkalmazottak felé, hogy megértse, és elfogadja, hogy miért van rá szükség. Az alkalmazottak felé publikálás egyik módja a

hírlevélben való kiküldés. Ezt mindenki megkapja, viszont nagyon kevesen fogják elolvasni, mert ha látja, hogy újabb szabályzat, akkor nagy eséllyel törlik. Ezen segíthet az, ha a hírlevélben történő kiküldést, értestést kiséri egy közvetlenebb, tájékoztató üzenet, ami nem több 5-6 mondatnál. Ekkor nem annyira hivatalos stílusban leírhatjuk, miért van szükség például egy újabb szabályzat módosításra.

A munkatársak tudomást szerethetnek újabb szabályzatról oktatások alkalmával is. Ez, példákkal illusztrálva egy interaktívabb esemény lehet, de az oktatások általában nem esnek egybe a szabályzatok változásával, így a kollégák nem értesülnek egyből ezekről.

Új kolléga belépésekor a teljes szabályzat átadása ijesztő lehet. Ellenben érdemes egy pár oldalas kivonatot adni neki, a legfontosabb dolgokat kiemelve, és utalásokat arra, hogy hol találja a teljes szabályzatot.

Új szabályzat kiadásakor, és változáskor mindenképp érdemes ezt kommunikálni a kollégák felé, de ha nem is történik változás, legalább évente ajánlott informálni a kollégákat, hogy egyáltalán milyen szabályzat létezik. Ezzel elérjük azt, hogy ez benne legyen a vállalatnál a köztudatban. Erősen ajánlott a szabályzatok rendszeres felülvizsgálata.

3.2.3 Az Információbiztonsági kézikönyv

Javasolt egyfajta információbiztonsági kézikönyvet elkészíteni, ami lényegében az IBSZ egy egyszerűsített verziója, egyszerűbb nyelvezettel, és szervezeten belül korlátozás nélkül érdemes terjeszteni. Olvasmányosabbnak kell lennie, mint a IBSZ-nek, sok magyarázatot, példát lehet bele írni, az egyes témákat érdemes képekkel illusztrálni. A stílusa lehet közvetlenebb is, ezzel elérhetjük azt, hogy a kollégák szívesebben lapozgatják, bele-bele néznek. Lehet mellékelni nyomtatható lapokat (akár vicceset is), ami kirakhatnak irodába, folyosóra, portára. A tematikája nem kell, hogy kövesse az IBSZ-t, lényeg, hogy érdekes és személyes legyen.

3.3 Biztonságtudatossági oktatás

A biztonságtudatossági oktatás azon ismeretek átadását jelenti, amellyel csökkenthetjük a kockázatot, hogy a vállalatot kár éri. Fontos megértetni a munkavállaókkal, hogy ilyen jellegű támadások tényleg léteznek, és bárki lehet célszemély. Hatékony, ha az oktatás témakörei kapcsolódnak aktualitásokhoz, közelmúltbeli eseményekhez. Így a hallgató valóságosabbnak érezheti a problémát, láthatja azt, hogy ezek tényleg valós veszélyek. Néhány, általam javasolt témakör, amik köré az oktatást fel lehet építeni:

- bevezetés,
- fizikai biztonság,
- biztonságos mobilhasználat,

- levelezés biztonsága,
- biztonságos internetezés,
- adathalászat, spam,
- home office,
- közösségi média,
- szabályzatok,
- munkahelyi környezet, tiszta asztal,
- észlelt incidensek kezelése,
- egyéb, speciális.

Ezen témák mindegyikénél be kell mutatni, hogy milyen fenyegetések, és védekezési módszerek léteznek. Érdemes bemutatni a támadó által használt trükköket, módszereket. A megértést segíti a sok-sok példa. A védekezési lehetőségekkel kapcsolatban érdemes megkérdezni a hallgatóságot, hogy milyen ötleteik lehetnek a kivédésre, majd ezeket átbeszélni. Fontos az egyes témákkal kapcsolatban, hogy mit kezdjünk akkor, ha észrevesszük, hogy átvertek minket? Kinek kell jelenteni, és milyen formában, ekkor kinek mi a felelőssége?

Minél jobb, érdekesebb egy oktatás, annál maradandóbb nyomot hagy a jelenlévőkben, később felkészültebbek lehetnek egy esetleges social engineering támadással szemben. Az ilyen oktatásokat is érdemes sok példával, képpel szemléltetni. Számos gyakorlati esetet érdemes bemutatni, ezzel a hallgatóság számára érthetőbbé, megfoghatóbbá tenni ezt a témát. Ha olyan példákat említünk, amelyek köthetők a magánélethez, még jobban megérti a hallgatóság az információbiztonság fontosságát. Ilyen lehet az, ha például megemlítjük, hogy ha nem elég óvatos a felhasználó, elveszítheti a családi fényképeit, fontos számláit. A biztonságtudatossági oktatás témája az adott vállalat igényei szerint eléggé változatos lehet, de van néhány téma, amit mindenképp érdemes tartalmaznia. Ezek:

- milyen emberi tulajdonságokat használnak ki a támadók,
- mire kell figyelni, hogy lehet észrevenni egy támadást, hogy lehet védekezni, kinek kell ezt jelezni,
- milyen szabályok vannak érvényben, ezek hol találhatóak, néhány fontosabb pont kiemelése,
- a vállalatnál előforduló, gyakori problémás esetek átbeszélése (jó, ha ezt megelőzi kockázatelemzés, vagy audit),
- milyen szankció vár a munkavállaóra, ha nem tartja be a szabályokat, főleg, ha ezzel kárt is okoz.

3.3.1 Személyes képzés

A szakdolgozatban a képzés és oktatás szavakat egymás szinonimájaként használom. A képzés inkább adott témakör egy szűkebb területére fókuszál. Olyan készségeket és kompetenciát fejleszt, ami abban segít, hogy az adott területen sikeresen végezzük a munkát. Gyakorlatias, de kiegészíti elméleti tudás. Például az Információbiztonságon belül a biztonságtudatossági képzések. Az oktatás ezzel szemben egy szélesebb körű ismeretanyagot ad át, magába fogalja a kapcsolódó szakterületek témáit is. Elmélet, gyakorlattal kombinálva, például egy egyetemi oktatás.

Személyes képzés alatt azt értjük, mikor a résztvevőknek és az oktatónak egy adott helyszínre kell menniük a képzés miatt. Ami legtöbbször a szervező cég saját, vagy bérlet oktatói terme.

Az oktatás alatt javasolt, és elterjedt a prezentáció vetítése, ami segíti az anyag átadását. Jó módszer oktatás vagy előadás alatt videók vetítése, érdekesebbé teszi az előadást. Ezzel jól ehet demonstrálni bizonyos támadási formákat, mint például követés, besurranás. Ajánlott történeteket is mesélni, amivel példákat hozhatunk az adott helyzetre. Ezzel is életszerűbbé, személyessé tesszük a témát, ezen kívül megerősíthetjük az előadáson elhangzottakat. Sokat segít a megértésben, ha az oktató egy szituációt bemutatva beszélgetést, vagy vitát generál. Ez az interaktivitás segíti, hogy a mondanivaló jobban rögzüljön a résztvevőkben. Nem szabad, hogy túl sokáig tartson az oktatás, elégedetlenek lesznek a hallgatók [15][25].

A személyes képzés néhány előnye:

- egyszerre nagy mennyiségű, átfogó témát lehet átadni viszonylag sok embernek,
- a tanfolyamról felvétel készíthető, amit át lehet adni más részlegeknek, vagy időnként elővehető megnézhető,
- a prezentációk szintén megoszthatók másokkal, megerősítés céljából, jegyzetként elrakhatók,
- meg lehet vitatni témákat az oktatóval és a résztvevőknek egymással is,
- interaktív, jobban megragad az elhangzott anyag.

A személyes képzés néhány hátránya:

- a képzés hatékonysága nagymértékben függ az oktató felkészültségétől, előzetes tapasztalataitól,
- ha túl sok az anyag és szűkös az idő, előfordulhat, hogy nincs lehetőség kérdezni,
- ha nem sikerül érdekessé tenni a képzést, a nagy anyagot nem tudja befogadni a hallgatóság, így ez elveszett idő lehet,

- a nem sikerül eltalálni az optimális oktatási időt, a hallgatóság belefárad, nem akarja,
- nehéz lehet megszervezni egy személyes jelenléti képzést, főleg, ha nagy létszámú csoportról van szó. Ez időbeosztás és hely függvénye is,
- költséges lehet az étel biztosítása, oktatóterem bérleti díja, a képzés díja, utazások költsége, az oktató díja.

3.3.2 Online oktatás

Napjainkban az egyik legelterjedtebb módszer. Ebben az esetben a munkavállalók nem tanteremben ülnek, hanem a saját számítógépük előtt ülve hallgatják végig az oktatót élőben. Ennek lehetnek technikai feltételei, de ez manapság nem jelent problémát: a online videós megbeszélések, konferenciák már általánosan elterjedtek, a felhasználók sem érzik idegennek ezeket.

Nem teljes mértékben interaktív, mert a felhasználó bármikor lekapcsolhatja a mikrofont és a kamerát, az oktató így nem kap visszajelzést a csoport hangulatáról és nehezen tud illeszkedni előadásával a csoporthoz. Ha az oktató többször kérdezni az online jelenlevőket, véleményükre kíváncsi, beszélgetést kezdeményez, akkor fenn tudja tartani az érdeklődést a téma iránt [15][25].

Előnyei lehetnek:

- hasonló előnyei vannak, mint a személyes képzésnek, ez is interaktív, de ez nagyban függ az oktató személyétől,
- itt előny az, hogy nem kell kiszervezni, nem kell fizetni terem bérlést, utazást, ételt a résztvevőknek, ezért költséghatékonyabb lehet. A munkahelyen részt lehet venni a képzésben,
- nem kötődik földrajzi helyhez. A képzést több ponton, a szervezet fiókirodában is el lehet egyszere végezni.

Hátrányai lehetnek:

- hasonló hátrányai vannak, mint a személyes jelenléti oktatásnál, kevésbé interaktív,
- nehezebb, vagy egyáltalán nem lehet csoportmunkát szervezni, ez ronthatja az anyag megértését
- az oktatás egyik sarokköve a megfelelő technikai háttér

3.3.3 E-learning

A résztvevők az oktatási anyagot böngészőn vagy saját fejlesztésű szoftveren keresztül érik el és tudják olvasni, amit egy webszerveren tárolunk. Ennek megvalósítása sokféle lehet. Lehet egyszerű olvasnivaló, de lehet prezentáció jellegű, videókat tartalmazhat,

és interaktív feladatokat. A tananyag lehet saját, belső fejlesztés, vagy megbízott partner által fejlesztett anyag.

Az e-learning egy kézenfekvő módszer lehet az oktatásra, viszont egyáltalán nem biztos, hogy a leghatékonyabb. Mindezek ellenére az e-learning oktatásnak lehet szerepe az olyan cégeknél, ahol erre nincs más lehetőség. Ez még mindig jobb, mintha nem is lenne oktatás. Ekkor kiemelten fontos szerepe van annak, hogy a téma érdekesen legyen feldolgozva és átadva. Az e-learning kiválóan kiegészítheti a tantermi oktatásokat, összegezheti az elhangzottakat, és erre épülve ellenőrző tesztet lehet kitöltetni a munkatársakkal, beépíthetők teljesítmény mérési funkciók [15][25].

Előnyei:

- a tartalom könnyen frissíthető, alkalmazkodhat a szervezet aktuális igényeihez,
- az e-learning képzésben részt vevők önállóan tanulhatnak, és a saját tempójukban haladhatnak,
- mobil eszközre is lehet fejleszteni, és szélesebb körű elérést jelenthet. Itt lényeges kérdés, hogy engedjük-e az alkalmazottaknak, hogy saját mobil eszközről érjék el az anyagot,
- többször megnézhető a tananyag, visszanézhetők a beépített videók,
- igény szerint tudják elkezdeni az oktatást, amikor megfelelő időpontot találnak rá.
- az oktatóanyag előállítása, és fenntartása költségkímélőbb, mintha rendszeresen személyes képzést kellene szervezni a kollégáknak,
- könnyebb specializálni a tananyagot, például akkor, ha egy megváltozott szabályozási környezettel kapcsolatos ismeretet kell átadni,
- teszteket és ellenőrzési pontokat lehet beépíteni, ezzel mérve azt, hogy mennyire sajátították el az ismereteket.

Hátrányai:

- nem interaktív, nem tudjuk, hogy az alkalmazottunk tényleg megértette a leadott anyagot. Az alkalmazott a kitöltés során nem tud kérdezni,
- ha nem elég érdekes az anyag, vagy túl hosszú, nem követik végig az anyagot, csak gyorsan átlépkednek rajt,
- ezen kívül a kollégák csalhatnak is, mert ha az e-learning oktatás után tesztet is kell kitölteni, oda tudják egymásnak adni a megoldásokat, vagy egymás helyett töltik ki,
- lehetnek esetleg technikai korlátai a használatnak. Megfelelő sávszélesség kell, és nem jó az, ha egy speciális böngészőre, vagy böngésző kiegészítőre van szabva az anyag. Megfelelő mennyiségű számítógép, vagy mobil eszközt kell biztosítani az elvégzéshez.

3.3.4 Videó bemutató

A résztvevők egy előre elkészített oktató videót néznek egyénileg, vagy csoportba szervezve. Ne legyen több fél-egy óránál egy-egy videó hossza, mert ezután már megterhelő lehet. Ez a fajta oktatás e-learningbe beépítve lehet a leghatékonyabb [25].

Előnyei:

- a munkaidőhöz, feladatokhoz lehet időzíteni az oktató videó megtekintését,
- maximum fél órás videóval jól le lehet kötni az embert,
- már rendelkezésre állnak ingyenes és kereskedelemben megvásárolható oktató videók, így a képzés kivitelezése költséghatékonyabb és gyorsabb lehet.

Hátrányok:

- nehezen frissíthető az anyag. Ezt úgy lehet ellensúlyozni, ha már léteznek különböző témákról szól anyagaink,
- a szervezet számára hirtelen felmerülő igényeket így sem lehet, vagy nagyon nehéz kielégíteni,
- a kereskedelemben kapható anyagok általános biztonsági témákról szólnak. Az egyedi, a szervezet számára készült videó anyag fejlesztése – ami a leghatékonyabb – költséges,
- semmi nem garantálja, hogy az alkalmazottak tényleg végig nézik a videót.

3.3.5 Az oktatások célcsoportjai

Az oktatást le lehet adni egyszerre mindenkinek, ekkor mindenki ugyanazt a tananyagot kapja. Mivel egy adott cégnél mások a munkakörök, máshol vannak a munkavégzés helyei, más emberekkel találkoznak a kollégák, ajánlott az oktatásokat munkavállaók egy-egy adott csoportjára alkalmazni. A munkakörök miatt más-más támadási módszerek működnek, mások a kockázatok és mások a kollégák ilyen irányú előismeretei. Az adott témakör kidolgozottsága is függ csoporttól, minden csoport az információbiztonsági tudatosság egy más aspektusát ismerheti a beosztásból adódóan [15][25]. Főbb oktatási csoportok:

Felsővezetés

Oktatás során a felsővezetőségben tudatosítani kell, hogy nekik van a legfontosabb szerepük abban, hogy a cégnél az információbiztonság-tudatosság a vállalati kultúra része legyen. Fontos szerepük van a kollégák ösztönzésében és a fejlesztésben. A vezetőségnek, igazgatóknak általában kevés idejük van, nem biztos, hogy egy több órás oktatáson részt tudnak venni, emiatt megfelelő lehet fél órás képzés is.

Adminisztrátorok

Ez olyan munkavállalók csoportja lehet, akik nem felsővezetők, de számítógépet használnak a munkavégzéshez. Náluk kiemelet terület lehet a levelezés, telefonálás biztonsága. Az irodai dolgozók olyan tulajdonságokkal rendelkeznek, mint például a segítségnyújtás, amit előszeretettel használnak ki a támadók. Ez főleg igaz a titkársági és pénzügy irodai alkalmazottakra, ezért náluk ez az oktatás egy kiemelet pontja kell, hogy legyen.

IT üzemeltetés

Az informatikával foglalkozó személyeket általában biztonság tudatosabbnak tekintjük. Ennek ellenére lehetnek olyan gondosan felépített támadások, amik az informatikusokat célozzák. Ugyanis ők vannak birtokában annak a tudásnak, hogy az adott informatikai rendszer, hogy épül fel, milyen hardver és szoftver elemekből áll. Lényeges tudatosítani bennük, hogy munkájukból adódóan fontos szerepük van az információbiztonság kialakításában, fejlesztésében, fenntartásában.

Egyéb csoport

Lehetne még kategorizálni a felhasználói csoportokat, de ezeket az egyéb csoportokat a vállalat működése határozza meg. Ha vannak nagyon speciális munkakörök, akkor arra célszerű külön tematikájú képzés szervezni. Ilyen lehet az, ha az adott cég több olyan üzletkötőt foglalkoztat, aki sokat utazik. Náluk az adathordozók biztonsága, nyílt internet kiemelt téma lehet oktatáson.

3.4 Biztonságtudatossági program

A biztonságtudatossági program célja, hogy az alkalmazottak biztonságtudatossági szintjét megfelelő szinten tartsuk, ebben meghatározó szerepe van. Ez a teljes szervezetre, annak minden szintjére vonatkozik. Alapvető fontosságú, mivel ez az eszköze annak, hogy a cég munkavállalói, beleértve a vezetőket is, megismerjék azon a szabályokat, amik a biztonságos munkavégzést segítik. Egy hatékony információ biztonsági tudatossági program elmagyarázza az informatikai rendszerek és információkra vonatkozó viselkedési szabályokat. A program biztonsági szabályokat és eljárásokat tesz közzé, amit követni kell. Elvárásokról és szankciókról tájékoztatja a kollégákat.

Az információbiztonság tudatosítása, vagy ennek növelése nem egyenlő az oktatással. A tudatosítás egy adott problémára hívja fel a figyelmet, míg a képzés egy szélesebb körű ismeretátadás. Viszont, ha egy szervezetnek van egy jól felépített programja, ami növeli a tudatosság, éberség szintjét, az a képzési program jó alapja lehet. Az előbbi célja, a viselkedés, a céges kultúra megváltoztatása vagy a jól bevált biztonsági eljárások megerősítése. A figyelemfelkeltés célja, hogy a munkavállalókban folyamatosan tudatosítsuk a veszélyeket, és erre megfelelően reagáljanak.

A biztonságtudatossági program sikerének kulcsa a folyamatosság. Lehetőleg egész éven át tartson, a vállalattól függően havonta, vagy akár negyedévente legyen valamilyen közlendője a szervezetnek. Érdemes tartani a havi ciklust a figyelemfelhívásra, mert ha nem is tudunk adni minden hónapban egyformán fontos anyagot a kollégáknak, számít a rendszeresség. Ezzel elérjük, hogy a munkavállalók fejéből az információbiztonság, mint fogalom ne kopjon ki. A program keretében rendszeresen emlékeztetni lehet őket, hogy milyen támadási formát léteznek, szabályzat módosításokat, és újként megjelenő veszélyeket tudunk bemutatni, információbiztonsági ismeretekre tudjuk rendszeresen felhívni a figyelmet.

A 3.1. ábra bal oldala a hagyományos képzés modellt mutatja. A vörös görbe jelzi az átadott tudásanyag megtartási szintjét, a kék görbe az átadott tudásanyag mennyiségét jelzi. Ez a képzés után viszonylag magas szintet ér el, de folyamatosan csökken, év végére közel nullára esik. Az ábra jobb oldalán egy másik oktatási modell látszik. Az elején kevesebb tudnivaló kerül átadása (kék görbe), majd havonta mindig egy kicsi. Ez a havi ismétlés folyamatosan szinten tartja a biztonságtudatossági szintet. A narancssárga görbe az átlagos megtartási szintet jelzi, látszik az ábra jobb oldalán, hogy ez magasabb abban az esetben, ha a biztonságtudatossági program folyamatos.

3.1. ábra: *a képzések rendszeressége és a megjegyzett anyag összefüggése [26].*

A biztonságtudatossági programot kiegészítheti a biztonságtudatossági kampány. Ez nem egész éven át tart, hanem egy időszakos program. Ennek keretében egy-egy témát még jobban előtérbe hozhatunk, ezzel színesíteni lehet a biztonságtudatossági programot.

A biztonságtudatossági programban az üzeneteknek figyelemfelkeltőnek, érdekesnek kell lennie. Néhány javasolt témát felsorolok, amit én hasznosnak gondolok arra, hogy megjelenjen figyelemfelkeltés, tudatosítás céljából:

- jelszóhasználat,
- rosszindulatú kódok elleni védelem, vírusvédelem,

- gyanús e-mailek és jellemzői, mellékeltek kezelése,
- levelező programok használata,
- szabályzatokhoz kapcsolódó szankciók,
- internethasználat veszélyei,
- adatmentés,
- átverések,
- reagálás észlelt incidensre,
- környezeti veszélyek tudatosítása (tűz, por, stb.),
- nem használt adattárolók, eszközök kezelése,
- érzékeny adatok kezelése,
- személyes használatra kiadott eszközök biztonsága,
- kézi, mobil eszközök biztonsága,
- érzékeny adatok titkosítási céges követelményei,
- laptop biztonsága utazás közben,
- BYOD eszközök használata,
- frissítések fontossága,
- szoftver licenszek, engedélyezett szoftverek,
- ki mihez férhet hozzá,
- a fizikai biztonság elemei,
- látogatók kezelése,
- tiszta asztal politika.

A tudatossági program tervezésénél is szempont, hogy mennyire támogatja a szerveztet üzleti igényeit és mennyire van összhangban a szervezet igényeivel. Releváns legyen a szervezet működése, felépítése, informatikai rendszerei, biztonsága vonatkozásában.

3.4.1 Biztonságtudatossági program forrásai

Manapság számtalan forrás áll rendelkezésre, ha anyagot szeretnénk gyűjteni a biztonságtudatossági kampányhoz, vagy akár egy oktatást akarunk érthetőbbé tenni. Néhány forrás, ami segít az anyagok összeállításában:

- szakmai konferenciák, fórumok, szemináriumok, ahol aktuális témákkal találkoznak,
- folyóiratok, nyomtatott lapok. A nyomtatott sajtónak már kisebb a jelentősége, de egy-egy témában mélyebb ismeretet nyújt, mint az online blogbejegyzések. Magyarországon a Computerworld című lapnak van nyomtatott verziója is, ahol mindig egy-egy vállalati informatikai vezetővel olvashatunk riportot információbiztonság témában [27],
- online biztonsági lapok, híroldalak. Gyorsan kaphatunk információt az aktuális veszélyekről, például SANS OUCH! hírlevelek [28], KiberBlog, [29],

- szakmai és egyéb szervezetek anyagai. Ilyenek például a Hétpecsét Egyesület [30], WITSEC szakmai közösség [31], Nemzeti Kibervédelmi Intézet anyagai.
- minden egyéb, például napi információbiztosági hírek.

Források tekintetében külön kiemelem a Nemzeti Kibervédelmi Intézet (NKI) oldalát: https://nki.gov.hu/. Itt sérülékenységekről, aktuális sebezehetőségekről értesülhetünk és számos más, kiberbiztonsági témával kapcsolatban kapunk tájékoztatást. Forrásokat kapunk egy biztonságtudatossági program összeállításához, ebben is segít például az oldalról letölthető SANS szervezet OUCH! kiadványa. Ha például havi rendszerességű hírlevet kell összeállítani, akkor a Kiadványok menüpont alatt találunk olyan anyagokat, amit ki lehet küldeni a vállalat dolgozóinak, vagy ki lehet nyomtatni.

3.2. ábra: *az NKI oldaláról letölthető egyik szórólap [32].*

Egy másik fontos terület lehet a forrásokkal kapcsolatban az Országos Rendőr-főkapitányság weboldala: https://www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag, és Facebook oldala: „Internet tudatosan”, https://www.facebook.com/internettudatosan/. Az oldal neve tükrözi a tartalmat. Számos tájékoztatást lehet olvasni social engineering témájával kapcsolatban és az aktuális fenyegetésekről is megjelennek bejegyzések.

3.4.2 Biztonságtudatossági program sarokpontjai

Igényfelmérés

Ahhoz, hogy egy program a lehető legjobb hatást érje el, igényfelmérést ajánlott végezni. Ezzel pontosítani tudjuk, hogy mire van szükség, és meg tudjuk becsülni a forrás igényt is. Igényfelmérés során az összegyűjtött válaszok ezekere a kérdésekre válaszolnak:

- Milyen képzésre, oktatásra van szükség, milyen irányba fejlesszük a biztonság tudatossági programot?
- Jelenlegi igények, hogy vannak kielégítve? Most mi van?
- Mit kell tenni, hogy elérjük a kívánt in biztosági tudatossági szintet?
- Mennyire működik jelenleg az információbiztonsági tudatossági program?
- Mik a legkritikusabb szükségletek?

Biztonságtudatossági programterv

Az igényfelmérés alapján a szervezet tervet tud készíteni, hogy milyen információ biztonsági tudatossági programot kell fejlesztenie, végrehajtania, fenntartania. Ebbe a tevékenyégbe figyelembe kell venni be kell vonni a szervezet kulcsfontosságú személyeit, csoportjait. Ők tudnak segíteni a speciális képzési igények kialakításában, javaslatokat adni. Ilyen kulcsszereplők a következők lehetnek: felsővezetés, rendszergazdák, adminisztrátorok, és egyéb, szervezet specifikus csoportok. Ebbe a tervbe bekerülhet:

- melyik helyi vagy törvényi szabályozás teszi szükségessé az információ biztonsági tudatossági programot,
- a programot fejlesztő és megvalósító munkakörök, beosztottak, ezek felelőssége,
- a program egyes elemeitől milyen célt várunk el,
- ki a program célközönsége,
- célközönségre szabott oktatási anyagok,
- egyes képzéseken szereplő témák,
- képzés formai megjelenése, műszaki, technikai követelménye,
- a program egyes elemei hogyan kerülnek dokumentálásra,
- végrehajtási ütemterv, erőforrások, csoportok, kritikusság.

Megvalósítás

A képzési igények és az információbiztonság tudatossági anyagok fejlesztése során ezeket az szempontokat érdemes figyelembe venni:

- szervezet igényei,

- szervezeti felmérések,
- IT infrastruktúra és a munkavállaó kapcsolati pontjai,
- kockázatelemzés eredménye,
- rendelkezésre álló anyagok, tervek áttekintése,
- korábban elkészített audit eredmények elemzése,
- a főbb alkalmazások, rendszerek biztonsági rendszereinek áttekintése,
- külső, belsős támogatási rendszerek elemzése,
- rendszerek, felhasználói adatbázisok, hozzáférések elemzése,
- hivatalos felügyeleti szervektől való megállapítások, auditok,
- beszélgetések felhasználókkal, visszajelzések,
- korábbi biztonsági események elemzése, jegyzőkönyvek, esetleg naplófájlok,
- műszaki vagy IT infrastruktúra változása,
- ipari, szakági, kormányzati ajánlások,
- aktuális trendek figyelemmel követése,
- technikai (PC, hangszóró, stb), infrastrukturális (oktatóterem) feltételek rendelkezésre állnak-e?

3.4.3 Használható eszközök

A választott technikák a rendelkezésre álló erőforrásoktól és az üzenetek összetettségétől függenek.

Plakátok.

Vannak ingyenesen letölthető és felhasználható lakátok, de ha ilyet használunk, kevésbé fogja meg az kollégákat. Hatásosabb egy plakát, ha saját, testreszabottat készítünk, így sokkal jobban fog emlékezni a kolléga a mondanivalóra. Speciálisan, a vállalatnál előforduló helyzeteket, veszélyeket érdemes bemutatni.

Érdemes olyan témákat is meghirdetni, amik egyébként rendben vannak a cégnél, vagyis többnyire figyelnek rá az alkalmazottak. Ezt nem biztos, hogy komolyan veszik, mivel már természetesnek számít, de egy jó szövegezéssel, humorral emlékeztetni lehet őket arra. hogy ne lankadjon a figyelem. Fontos, hogy inkább javasolt a problémákra fókuszálni, vagy hogy mit lehetne jobban csinálni. Ezen témák kiválasztásában sokat segít az audit felmérés, vagy egy kockázatelemzés.

A plakát helye fontos. Olyan helyre érdemes rakni, ahol sokan megfordulnak, például étkező, lift, fénymásoló mellett stb. Ha ezen kívül még figyelünk arra, hogy a plakát képe, elrendezése illeszkedjen a helyiséghez, erősebb hatást érünk el.

Hírlevelek.

Egyik leggyakoribb módszer, viszont nem biztos, hogy önmagában tényleg elég hatékony, mivel egyáltalán nem biztos, hogy elolvassák. Egyszerűen közzé tudunk

tenni új szabályzatot, az oktatás egy-egy témáját is küldhetjük, figyelmeztetéseket is tudunk közzétenni. Lényeges a hírlevél megfogalmazása, és a téma érdekessége, mert az általános hírleveleket általában törlik a felhasználók. Minél érdekesebb, és a munkavállalókhoz köthető a téma annál inkább megnyitja és elolvassa a hírlevelet.

Mivel a jó hírlevélben feldolgozott téma speciálisan a vállalat igényeire és céljaira van szabva, az előállítása időigényes feladat.

Videóüzenetek, videók

Egy vállalatra szabott oktató, vagy bemutatóvideó nagyon hatásos lehet. Szemléletesen lehet bemutatni az információbiztonsági kockázatokat és a helyes, szabálykövető magatartást. Hátránya, hogy az elkészítése költséges.

Üzenőlapok.

Készíthetünk kis kartonlapokat, kártyákat, aminek a tartalma ugyanaz lehet, mint a plakátoknak. Egy ilyen elhelyezett lapocska, például a fénymásoló helyiségében elhelyezve emlékeztetni tudja a munkavállalót, hogy ne hagyjon dokumentumot a fénymásolóban még véletlenül se. De ha kampány részeként készítünk kártyanaptárat, ezt el tudjuk helyezni a portán, érkezéskor tudnak belőle venni egyet-egyet.

Képernyőkímélő.

Központilag egyszerűen beállítható, hogy az alkalmazott számítógépén milyen képernyő működjön. Olcsón megvalósítható, gyakran változtatható az üzenet.

Felbukkanó (popup) ablakok.

A felbukkanó ablakok közvetíthetnek biztonságtudatosságra nevelő rövid üzeneteket, viszont gyakori használatuk zavarhatja a dolgozót.

Képregények.

Egy jó képregény akár vicces is lehet, megfogja a munkatársat és emlékszik rá, ha ilyen lát. Viszont az elkészítése időigényes, ha csak nem találunk egy felhasználhatót, és számunkra megfelelőt. Időbe telik elolvasni is, ezért olyan helyiségbe érdemes rakni, ahol kicsit több időt töltenek. El lehet küldeni e-mailben is, de ha hosszú a képregény, félő, hogy nem olvassák el. Hatásos, ha az épp futó kampányhoz kapcsolódik a témája.

Irodai használati eszközök.

Ilyenek lehetnek: Bögrék, naptár, jegyzettömb, egérpad, tollak, kulcstartók, könyvjelzők stb. Egérpadot már nem igazán használunk, de ha mégis, akkor több ideig van szem előtt, akárcsak a naptár. Ha jegyzettömböt, vagy asztali naptárt készítünk, egy-egy oldalra tudunk különböző üzeneteket rakni.

Játékok, keresztrejtvények

Ha információbiztonsággal kapcsolatos fotópályázatot, szlogenpályázatot, vagy más játékot hirdetünk, ezzel hosszabb ideig foglalkoznak a felhasználóink. Interaktív, jobban megragad téma. Még hatásosabb, ha valamilyen nyereményt is hirdetünk a játékban résztvevőknek, vagy a játékba zsűriként bevonjuk a többi felhasználót is.

3.4.4 Ki a felelős?

A legtöbbek véleménye szerint az informatikai rendszer üzemeltetők felelősek a szervezet adatainak védelméért. Ez abból a szempontból igaz, hogy az informatikai személyzet üzemelteti a szervereket, kliens számítógépeket, vírusvédelmi szoftvereket, és a hálózatban működő biztonsági rendszereket. A legtöbb szervezet a szoftverre és hardverre támaszkodik, ha biztonságról beszélnek, így az informatikusok szerepe is erre korlátozódik. Sok informatikai részleg túl leterhelt, hogy a biztonsággal is kellően foglalkozzanak, így ez a prioritási lista végére kerül [33].

2019-ben a Toyota úgynevezett BEC (Business Email Compromise) csalás áldozatává vált [34]. A BEC lényegében egy fejlett adathalász vagy zsarolóprogram csalás, ahol arra kérik a vállalat alkalmazottját, hogy utaljon egy összeget egy megadott bankszámlaszámra. Elsősorban nagyvállalatokat, azon belül is a pénzügyi osztály munkatársait támadják ezzel a módszerrel. A Toyota esetében egy hacker a cég leányvállalata partnerének adta ki magát és a pénzügyi osztály munkatársait arra kérte, utaljanak pénzt a megadott számlaszámra. Így sikerült meggyőzni egy dolgozót, aki tényleg átutalt 37 millió dollárt.

Ebben az esetben nehéz egyértelműen megállapítani, hogy ki a felelős. Vajon elég képzést kapott a munkavállaló? Vajon megfelelően ki voltak dolgozva munkafolyamatok? Volt-e elérhető középvezető, vezető, aki jóváhagyhatta volna a folyamatot? Mivel a nagyobb összeg átutalásának több lépcsős folyamata van, több kolléga hibája játszhatott közre abban, hogy a Toyota ilyen kárt szenvedett.

IT Biztonság csoport

Sok esetben az üzemeltetők az IT biztonsági szakemberek is. A legjobb megoldás az, ha a szervezetnél van információ biztonsággal foglalkozó csoport, akik mással nem foglalkoznak. Ők sem állhatnak minden alkalmazott mellett, nem tudják megakadályozni azt, hogy veszélyhelyzetet teremtsenek. Viszont hatalmas szerepük van a biztonság tudatossági szint emelésében, fenntartásában. Emlékeztetik az alkalmazottakat a védelemmel kapcsolatos feladataikra, és ezzel kapcsolatos felelősségükre.

Elgondolkodtató, hogy egy olyan, biztonságosnak gondolt szervezetet is, mint az FBI, vagy az amerikai Igazságügyi Minisztérium, fel lehet törni social engineer módszerekkel. 2016-ban történt egy eset, mikor több ezer alkalmazott nevét, beosztását

és telefonszámát tette közzé egy hacker [35]. Már megvolt egy feltört, minisztériumi alkalmazott postafiókja, de ezzel nem tudott bejelentkezni a minisztérium privát internetes portáljára a hacker. Ekkor felhívta az illetékes osztályt, magát új munkavállalónak kiadva. Miután kiderült, hogy a hackernek nincs belépési token kódja, az ügyintéző azonnal rendelkezésre bocsátotta azt, amit ők közösen használnak.

Sajnos ebben az esetben szinte nulla volt az alkalmazottak biztonság tudatossági szintje. Egyrészt a szabályokat kellett volna betartaniuk, másrészt ismerniük kellett volna ezt a támadási módszert. Ha minimális képzést is kaptak volna a felelős információ biztonsági szakértőktől, ez nem történt volna meg. Ráadásul 2016 nem volt túl régen, ekkor már a köztudatban volt az, hogy ilyen módszerekkel is lehet adatot lopni szervezetektől.

Recepciós

Meg kell érteniük, hogy miért fontos a szerepük a biztonság terén. A legtöbb szervezetben recepciós, vagy portás a szervezet első védelmi vonala, emiatt az első számú social engineer célpont is. Ő az, aki mindig kedves, segítőkész, és az ő feladata a kérdések megválaszolása, és az érdeklődők tájékoztatása. Rendkívül fontos az ő képzésük, mivel a recepciósok nem biztonsági őrök, nem biztos, hogy van olyan tapasztalatuk. Fontos ismerniük a biztonsági szabályzatokat. A legfontosabb szerepe, hogy ne tudják átverni információkéréssel, telefonhívással, emellett a támadó fizikai bejutását akadályozhatja meg. Fel kell ismerniük a támadó szándékot, ismerni kell a védekezési lehetőséget.

Felsővezetőség

Gyakran a felsővezetőknek a legnehezebb eljutni biztonság tudatossági képzésekre, de mindenképp fontos, hogy részt vegyenek képzéseken. A szervezet szempontjából kulcsfontosságú információk birtokában vannak, bizalmas adatokhoz férnek hozzá, amit szívesen megszereznének a támadók. Különös célpont lehet a vezető számítógépe, vagy laptopja.

Az előzőleg leírt eset a Toyotánál abban az évben a harmadik bevallott eset volt. A felsővezetés felelőssége lett volna, hogy már az első eset után felkészítsék a szervezetet hasonló eset kivédésére.

A felsővezetés az, akinek példát kell mutatnia biztonság terén, támogatnia és ösztönöznie kell az alkalmazottakat. Emellett forrást is kell biztosítani, hogy a biztonságtudatossági program megvalósuljon, ehhez személyeket, az oktatához eszközöket kell biztosítania. Meg kell érteniük, hogy amellett, hogy első számú célpontok lehetnek egy social engineer támadás során, nélkülük nem tud megvalósulni semmilyen biztonságnövelő program.

Irodai dolgozók

Manapság mindenki számítógépen tárolja a munkájával kapcsolatos adatait. Egy támadónak még egy jelentéktelennek tűnő információ is fontos lehet. A központi fénymásoló környékén, a papírszemetes kosárban lehetnek jelentéktelennek tűnő információk.

A BEC támadások hatékonyságára jellemző, hogy a Cosmic Lync nevű kiberbűnözői csoport a közelmúltban ezzel a módszerrel 46 országból szedett áldozatokat [36]. Vállalti vezetőket megszemélyesítve rávettek vállalati alkalmazottakat, irodai dolgozókat, pénzügyeseket, hogy megadott számlaszámra utaljanak nagyobb összegeket. Aktuális eseményeket is felhasználtak a megtévesztésre, a koronavírus járvány kitörésével COVID-19 témájú levelekkel próbálkoztak.

Ha a támadót a pénzügyi információk érdeklik, megpróbál a pénzügy számítógépébe behatolni, vagy az ott dolgozók levelezését elérni. Nem ritkán a számítógép mellett ülök kiragasztják a bejelentkezési adatokat, számlaszámokat a számítógép környékére. De az is megesik, hogy telefonon beszélnek meg bizalmas információkat, anélkül, hogy ellenőrizték volna a volna másik végén lévő személy kilétét.

Mindenki célpont!

Egy átlagos személy viselkedése nagymértékben kiszámítható. A támadó ismeri a kihasználható emberi tulajdonságokat, ismeri a viselkedési formákat. Még olyan ember is átverhető, aki inkább biztonság-tudatosabb, az ilyen emberrel is össze elehet barátkozni, lehet olyan bizalmat kiépíteni, hogy csak akkor jön rá a kiszemelt egyén, hogy áldozat, ha már túl késő, ezért mindenki potenciális áldozat lehet.

A következő példa jól szemlélteti, hogy ha nincs kellő mértékű információbiztonsági oktatás, akkor mindegy, hogy milyen pozícióban van a munkatárs. 2019-ben egy nemzetközi nagyvállalat varsói fióktelepéhez tartozó nyilvános e-mail címeire tájékozgató levelek érkeztek, melyben az állt, hogy a környéken új pizzéria nyílik és az első vásárlónak 30% kedvezmény biztosítanak. A kollégák „Pizza napot” tartottak és rendeltek nyolc doboz pizzát. A megrendelő közt volt beosztott és vezető is. Mivel hamar adták le a rendelést, a pizzákhoz ajándékot is kaptak, ami egy USB portba dugható LED lámpa volt, ez a zene ritmusára változtatta a színét. Pár perc múlva a cég működés gyakorlatilag megbénult, az alkalmazottak nem fértek hozzá adataikhoz.

Az előbbi történet valóban megtörtént, de szerencsére csak egy sikeres social engineer behatolási teszt volt a TestArmy CyberForces csapat részéről. A pizzéria oldala hamis volt, de kellett a hitelesség kedvéért. A célpontok e-mail címeit a vállalat honlapjáról gyűjtötték össze. Az ajándék USB-s eszköz már elő volt készítve arra, hogy kártevőt juttasson a rendszerbe. Miután az alkalmazottak ezt csatlakoztatták, az épületen kívüli kiberbiztonsági szakember távolról hozzáfért az informatikai rendszerhez, titkosítani tudta az adatokat [37].

2010-ben az iráni urándúsító berendezések vezérlőit támadták meg sikeresen, ami hatalmas károkat okozott az iráni atomprogramnak. A módszer hasonló volt, egyik az egyik alkalmazott talált egy USB pendrive-ot az épület környékén, bevitte az épületbe és rádugta a számítógépére [38][39].

Ebből a példából is látszik, hogy nem lehet kijelenteni azt, hogy csak adott munkavállalói réteg felelős a biztonságért. A munkakörök, beosztástól függően különböző kockázatokat jelentenek. A magasabban képzett kollégák hihetik azt, hogy őket nem lehet átverni, de ez nem igaz. Sőt, ők gyakoribb célpontjai az ilyen jellegű támadásoknak, mivel fontosabb céges adatok birtokában vannak.

A Home Office, a közösségi média elterjedése és hogy az internet egyre inkább az életünk része, egy újfaja kockázatot jelent a szervezetre nézve. Meg kell mutatni az alkalmazottaknak, hogy hogyan használják ezt, mert önkéntelenül is segíthetik a támadók dolgát. Akartalanul is felfedhetik a szervezet működési adatait, mint például e-mail címek, telepített víruskeresők, telefonszámok stb. Meg kell érteniük, hogy felelősek azért, ha meggondolatlanul publikálnak bármit az interneten.

3.4.5 Várható hatások

Az előbb leírt képzések, tudatossági kampányok várható hatásai a következők lehetnek:

- Számos e-mail érkezik a céges postafiókokba naponta és fontos, hogy a munkavállaló tudjon különbséget tenni az informatív és adathalász e-mailek között. De itt lehet szó telefonhívásokról vagy szöveges üzenetekről is. Mindig vannak jelek, ami arra utal, hogy csalóval van dolgunk. Ha elég felkészült a munkavállaló nem fog bedőlni az e-mail-ben érkező csalásoknak, így nem lesznek káros következményei a szervezetre nézve.
- Növeli a biztonsági intézkedések hatékonyságát. A biztonságtudatosság lényeges része a gyanús tevékenységek észrevétele, megfigyelése, követése. Egy képzett alkalmazott észreveszi a csaló üzeneteket, az elvárt szabályozásoknak megfelelően cselekszik, csökkentve a lehetséges behatolás kockázatát.
- Meg lehet őrizni a szervezet belső stabilitását. Egy jól képzett munkavállalói csapat megérti az adott helyzetet, probléma esetén képes együttműködően cselekedni, ezzel akár az esetleg elszenvedett kár mértékét csökkenteni.
- Meg lehet őrizni a szervezet hírnevét. Vannak olyan iparágak, amik jobban a figyelem központjába kerülnek, ha kibertámadás során kárt szenvednek (egészségügy, bankszektor stb.). Állami szervezeteknél egy jól szervezett social engineer támadás komoly gazdasági, politikai kárt is okozhat.

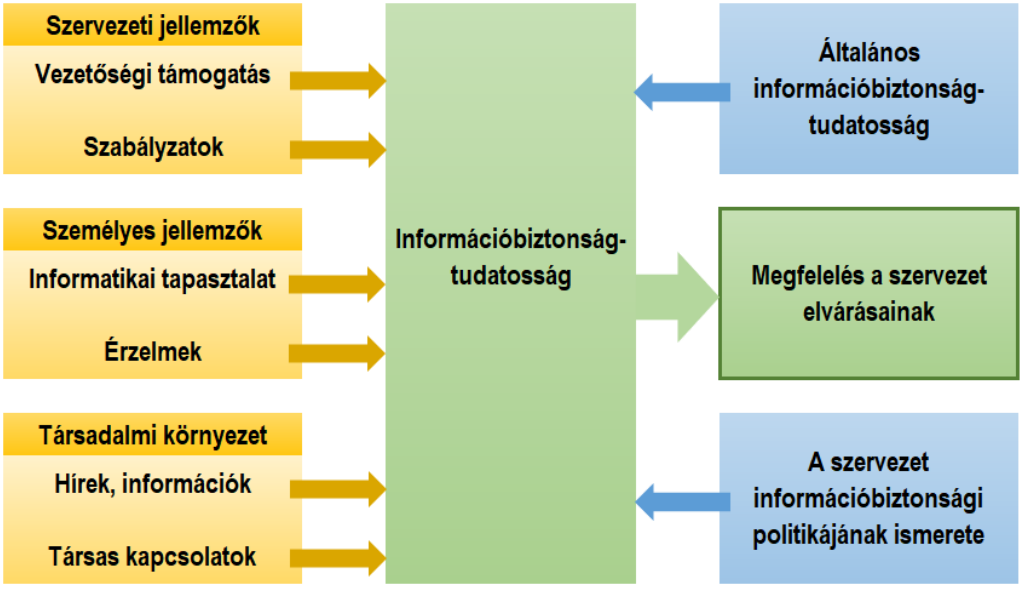
- A biztonság ezirányú ismerete növeli a munkavállalók biztonságérzetét és azt érezteti, hogy a szervezet számára ők fontosak. A visszajelzéseik segítenek egyre jobb információbiztonsági politika kialakításában.
- Egyre több vállalatnál kerül bevezetésre az otthoni munkavégzés. Az otthoni környezetet a vállalati informatika nehezebben felügyeli, mint a vállalat falain belüli rendszerhasználatot. A hackerek alkalmazkodnak a kialakult helyzethez. Ha a munkavállaló tudja, hogy hogyan őrizze meg az információ biztonságát otthon is, nagyban csökkenti annak esélyét, hogy áldozattá váljon.
- Számos szabvány írja elő a munkavállaók megfelelő képzését. A jól képzett alkalmazottak megfelelnek az előírt szabványok követelményeinek, ekkor egy audit során pozitív elbírálást kap a szervezet. Ez még akkor is fontos lehet, ha egy szervezetnél még nincs kényszer arra, hogy megfeleljen egy előírásnak, mert ha később erre szükség van, nem kell teljesen az alapoktól indulni.
- A képzéssel időt és pénz lehet megtakarítani, ez az egyik legfontosabb érv a képzések mellett. Azok a vállalatok, ahol a munkavállalók megfelelő képzést kapnak, nem, vagy csak nagyon ritkán kell szembesülniük gondatlanságól származó adatvesztéssel, vagy adatlopással. Az adatok helyreállítása, és a későbbi károk elhárítása sok pénzt, energiát, időd igényel, ezt el lehet kerülni, vagy jelentősen mérsékelni.

4. MI BEFOLYÁSOLJA A BIZTONSÁGTUDATOS MAGATARTÁST?

Az ideális állapot az lenne, ha egy szervezetnél mindenki szabálykövető módon végezné a munkáját. Ebben a fejezetben azok a sarokpontok kerülnek bemutatásra, amelyek leginkább befolyásolják az alkalmazottak biztonságtudatos magatartását. Ezen kívül az információbiztonság-tudatossági oktatások hatékonyságában is szerepet játszanak. Ezek a jellemzők azt is befolyásolják, mitől működik és mitől nem a social engineering.

A legerősebb hatást akkor lehet elérni, ha az alkalmazottban kialakul valamiféle személyes kötődés a biztonsághoz. Ha sajátjának érzi a szervezet céljait, problémáit, vagy valamilyen személes élményhez tudja kapcsolni a biztonságtudatos magatartást. Végső soron minden eszköz azt segíti, hogy a munkavállaló viselkedése megváltozzon pozitív irányba, a lehető legjobban szabálykövetővé váljon, és megértse, hogy ez miért fontos. Ha sikerül kialakítani a megfelelő elköteleződést, ez egy könnyű folyamat, szinte magától menni fog [5].

Minden egyes apró lépés, ami javít a viselkedésen, hozzáálláson, céges szokásokon emeli, az a szervezet informatikai rendszerének, adatainak biztonságát. A 4.1-es ábrán egy összefoglaló látható a befolyásoló tényezőkről [40].



4.1. ábra: *információbiztonság befolyásoló tényezői.*

Az ábrán az *Általános információbiztonsági tudatosság* jelenti a munkavállaló általános ismereteit az információs rendszerek biztonságával kapcsolatban. A *Szervezet információbiztonsági politikájának ismerete* az adott szervezet információbiztonsági szabályzatinak ismeretére utal.

4.1 A vezetőség támogatása

Az, hogy a vezetőség, felsővezetés mennyire elkötelezett a szervezet információbiztonságának egészre vonatkozóan, befolyásolja azt, hogy a beosztottak mennyire érzik sajátjuknak a szervezet biztonságát. Ha a beosztottak látják a vezető elköteleződését, az alkalmazottakban is kialakul ez a fajta hozzáállás, kialakul a munkatársakban is a szabályok betartására vonatkozó motiváció. Ha megvan a motiváció, a kollégák nem teherként fognak a biztonsági szabályokra tekinteni, a szabályok a mindennapi vállalati szokásrendszer, vállalati kultúra része lesz [41].

Már nagyon régóta ismerjük, hogy a példamutatás az legjobb tanár. Ez igaz ebben az esetben is az elköteleződés egyik oldala a vezetői példamutatás. Ha a vezető nem tartja be a szervezete szabályait, (aminek létrehozásában esetleg részt vett), az alkalmazottak szemében hiteltelenné válnak a szabályzatok, és a kontrollok, végül oda jutunk, hogy csökken a szervezet információbiztonsági szintje.

Az oktatások sikerében a felsővezetésnek jelentős a fellelősége. Ők biztosítják a forrásokat, hogy az oktatás megvalósuljon. Ez egyrészt a fizikai, kézzel fogható eszközök rendelkezésre állását jelenti. Meg kell adni a technikai eszközöket (az alkalmazottak elvétve használják a saját eszközeiket, ha a vállalat nem ad számára, de rendszeresen nem szeretik használni – jogosan), és meg kell adni a helyet is az képzéshez. Ez utóbbi, az online oktatások esetén nem az üres helyiséget jelenti, hanem azt, hogy az alkalmazottnak az oktatás ideje alatt, ne kelljen mással foglalkoznia.

Ezek mellett az emberi erőforrások biztosítása is döntő. Szakképzett oktatót kell biztosítani (itt nem mindegy az ár-érték arány), emellett támogatni, bátorítani kell azon kollégákat, akik megszólalnak az oktatások minőségének fejlesztése érdekében, és akár lehetőséget adni, hogy tevékenyen részt vegyenek benne.

Az információbiztonsági tudatossági programokat, ezek céljait egyértelművé kell tenni a szervezet minden tagja számára. Ez azért is lényeges, hogy megfelelő támogatottsága legyen, meglegyen a szükséges erőforrás a megvalósításhoz. Tisztázni kell a szerepeket, az alkalmazottaktól való elvárásokat, a programok várható eredményeit, költségeit, a szervezet hasznát. Rendkívül fontos, hogy mindenki képes legyen és hajlandó legyen ellátni a rábízott feladatokat a tudatossági programokkal kapcsolatban. A vezetőknek meg kell érteniük, hogy a szervezet információinak és infrastruktúrájának biztosítása csapatmunka. El kell készíteni ütemterveket, követelményeket minden résztvevő számára. Alapvető fontosságú, hogy a program végrehajtásában résztvevő mindenki megértse szerepét és felelősségét.

Gyakran kardinális kérdés, a tudatossági programok finanszírozása. Akár azon is elbukhat egy program, hogy nem lett eléggé megtervezve a finanszírozása.

A NIST 800-50 ajánlása megfogalmaz néhány pontot, szempontot, aminek segítségével értékelhetjük, hogy mekkorai támogatottsága van az információ biztonsági programnak [7]. Ezek a következők:

- Elegendő-e a finanszírozás az egyeztetett stratégia végrehajtásához.
- Megfelelő-e a szervezet felépítése, hogy lehetővé tegye a kulcsfontosságú felelősséggel rendelkezők számára a stratégia hatékony végrehajtását (informatikai igazgató, IT biztonsági igazgató, a program szakértői).
- Van-e támogatása a biztonság tudatossági információk széles körű terjesztésének és közzétételének. (pl. web, e-mail, intranet).
- A vezetőség közvetít-e üzenetet, van-e párbeszéd a munkavállalókkal (személyzeti értekezletek, az üzentek küldése az IT biztonság csoport segítségével).
- Mérőszámok használata (pl. a biztonsági incidensek vagy jogsértések csökkenésének jelzésére, ami jelzi, hogy a meglévő tudatosság, képzési lefedettség, és a szervezet elvárásai közti szakadék csökken, a tudatosító anyagok által elért felhasználók százalékos aránya növekszik, növekszik azon felhasználók aránya, akiknek jelentős biztonsági felelősségük van, és megfelelő képzésben részesülnek).
- A vezetők nem élnek vissza szervezeten belüli hatalmukkal, hogy a biztonsági ellenőrzéseket és felelősségre vonás elkerüljék.
- Jelentős fórumokon, tájékoztatókon való részvétel megtörténik-e?
- A biztonsághoz való hozzájárulás elismerése (díjak, versenyek).
- Motiváció azok számára, akik kulcsszerepet játszanak az biztonsági programok irányításában, koordinálásában.

4.2 Információbiztonsági szabályzatok

Az Információbiztonsági szabályzatok a biztonságos munkavégzés elsődleges forrásai. Ez a szervezet informatikai rendszerének, beleérve az embert is, egyik alapdokumentuma kell, hogy legyen. Útmutatást ad a felelősségekről, irányelvekről, iránymutatást ad a munkavállalónak, hogy hogyan használjak az informatikai erőforrásokat. A szabályzatok ésszerű kialakítása és közzététele segíti azt, hogy az alkalmazottak ne kövessenek el visszaéléseket. Ez nem biztos, hogy szándékos, mert lehet véteni a szabályzat ellen önkéntelenül is, főleg, ha nincsenek egyértelműen megfogalmazva.

Nem elég az, ha csak egyszerűen van a szabályzat, azt népszerűsíteni kell, könnyen elérhetővé, könnyen érthetővé kell tenni. Ha könnyen elérhető egy szabályzat, mindenki hozzáfér, az segíti a munkavállalót, hogy minél jobban megfeleljen a szervezet elvárásainak. Ekkor ad egyfajta biztonságot is a munkavállalónak, jobban tud alkalmazkodni azokhoz a helyzetekhez, amelyekkel kapcsolatban még nem volt

tapasztalata. Ha például a levelezésre gondolunk, és van egy jól elkészített szabályzat, ahol a levelezés, a levelező program használata dokumentálva van, akkor a munkavállaló a váratlan helyeztek kezelésére elő tudja venni az adott szabályzatot, és aszerint cselekedni. Ezzel nem rontja a biztonság tudatossági szintet.

A biztonságtudatosságot növelő eszközök (oktatás, kampányok stb) célja ebben az esetben, hogy megértesse a munkavállalóval azt, hogy a kialakított szabályok a szervezet működését segítik. Ha ezt megértik, akkor nem azért tartják be a szabályokat, mert az kötelező, vagy, mert valamilyen szankcióval sújtják, azt, aki vét ellenük. Ha sikerül elérni azt is, hogy a kolléga „érezze azt", hogy miért kell a szabályok szerint eljárni, kialakul egyfajta belső motiváció, ami a szabályok betartására ösztönöz. Ekkor a szabályok szerinti munkavégzés a mindennapok részévé válik, nem lesz teher.

4.3 Oktatások

Az adott szervezet szabályainak való elvárt viselkedést, megfelelést, az oktatás közvetíti. Az oktatások célja a szervezet információ biztonságának növelése, javítása azáltal, hogy növeli az alkalmazottak tudását és tudatosságát. Lehetséges kockázatokat mutat, felelősségeket, szabályokat, irányelveket mutat be. Felhívja a figyelmet a szervezt informatikai rendszerének humán sebezhetőségére, és az erre adott lehetséges válaszra. Felkeltheti az érdeklődést a biztonsági problémák iránt. Határozott cél, hogy az alkalmazottak mindenben megfeleljenek az szervezet által előírt szabályoknak.

Az oktatásnak, figyelemfelkeltésnek hatalmas szerepe van az információ biztonság, adatvédelem terén és egyértelműen javítja a tudatosságot. Az oktatás során a siker kulcsa, hogy a célközönség minden tagjának meg kell értenie a mondanivalót, a felhasználó nyelvén kell szólni. Olyan példákat érdemes mutatnia az oktatónak, amivel könnyen el tudják képzelni a résztvevők támadási technikákat. Ha nem a való életből vett példát mutat az oktató, vagy nem a kollégákhoz közel álló példát mutat, akkor az bármennyire jó és látványos elemeket tartalmaz, nem fogja a résztevők figyelmét lekötni. Ha túlságosan, mereven a szabályzatokra koncentrál az oktató, a résztvevő nem fogja érteni, hogy miről van szó, nem tudja mihez kötni, nem fog érdeklődni az oktatás iránt. Ráadásul nem akarnak rész venni az oktatáson, kellemetlen élmény lesz számukra.

Ajánlott az adott szervezethez kötődő példákat említeni. Ehhez főleg akkor állhat rendelkezésre anyag, ha az oktatást megelőzően már volt valamiféle audit. Az ekkor keletkezett anyagokat, fényképeket be lehet mutatni az oktatáson lehet róla beszélgetni. Mivel ez a szervezethez és az alkalmazottakhoz kötődik, ez az egyik leghatékonyabb módszer a szervezet munkavállalóinak információ biztonság tudatosságának növelésére. Tovább lehet beszélgetni közelmúltbeli információbiztonsági eseményekről, aktualitásokról, hírekről, ezzel is fenntartva a hallgatóság érdeklődését.

Ha az oktatást kivetítjük a magánéletre is, lehet fokoznia hatékonyságot. Ekkor olyan kérdéseket is lehet feszegetni egy oktatás alatt, hogy miért jó az, ha biztonságtudatosak vagyunk, függetlenül attól, hogy munkahelyen vagyunk, vagy otthon.

Tréning alatt olyan feladatokat kell összeállítani, amit a résztvevők nem tehernek élnek meg, hanem amit érdekesnek találnak. Ez egy nehéz dolog, mivel ahány ember, annyifélék vagyunk, mindenkit más-más téma köt le jobban. Itt emiatt is számít a csoport összeállítása, beosztás, részleg, munkakörök stb. szerint, ezen kívül ajánlott egy előzetes felmérést készíteni a résztvevők korábbi, témába vágó ismereteiről.

Az e-learning oktatást általában nehéz érdekesre elkészíteni. Egyébként is egy kicsit személytelen és nem mindenki szereti. Ezt a fajta képzést fel lehet dobni videókkal, vagy rajzos animációkkal, ábrákkal, illusztrációval. Az e-learning-et általában a munkahelyen csinálja meg az alkalmazott, akkor hajlamos rá, hogy elhalasztja. Ha meg nekiáll, gyakran megzavarják, vagy más ügyekben keresik. Gyakran valamiféle szankciót kell alkalmazni azokkal szemben, aki nem viszik végig a képzést.

4.4 A példák

Ha példákat, történeteket használunk az oktatásban, meg tudjuk mutatni, hogy amiről beszélünk, az nem valami légből kapott, elvont dolog, hanem nagyon is valós. Vegyünk példának a Twitter feltörését. [3]. Ha elmeséljük, hogy az egyik legnagyobb közösségi média rendszerét sikerült feltörni social engineer módszerekkel, megdöbbenek a hallgatók. Ráébredhetnek, hogy ha egy ilyen nagyméretű vállalatot sikerült feltörni, akkor tényleg senki nem lehet biztonságban.

Azért is jó, ha történeteket hallanak az oktatáson részt vevők, mert azok is emberiek. A történetekben emberek szerepelnek, nem gépek. Sok ember idegenkedik a számítógépektől, de ha van egy olyan történet, amiben az ember cselekedetét és következményeit mutatjuk be, szintén jobban megragad a hallgatóságban a mondanivaló. Ha hasonló helyzetbe kerülnek, emlékezni fognak a történetre, jobban kezelik a felmerülő problémákat, feladatokat.

4.5 Személyes jellemzők

Nem lebecsülendő szempont a biztonságtudatosság terén, hogy az illetőnek milyen személyes tapasztalatai vannak. Ez befolyásolja az oktatást, és annak hatékony megértését. Ha tudja valamihez kötni az új tudást, jobban megérti az információbiztonság fontosságát.

4.6 Informatikai tapasztalat

Pozitív kapcsolat van a munkavállaló informatikai ismeretei és az információ biztonság tudatossága között. Egy alkalmazott számítógépes, informatikai, internetes ismerete,

tapasztalata, pozitív hatással van a biztonság tudatossági magatartására. Esetleg tudja, mi miért történik, mik a veszélyek. Az általános védekezési ismeretek, mint például vírusírtó szoftverek használatának (esetleg működésének) ismerete ezt segíti. Azt tudjuk, hogy egy szervezt informatika részlegének dolgozói magasabb szintű informatikai ismeretekkel rendelkeznek, ezért az információ biztonság tudatosságuk is magasabb.

4.7 Érzelmek

A munkavállaló átélt élményei, a személyes élményekhez kötődése nagyban befolyásolja, alakítja a biztonság tudatossági szintet. Fontos megjegyezni, hogy a negatív incidensek is nagyon erősen hatnak a biztonság tudatosságra, és felkeltik az érdeklődést az ilyen incidensek megelőzési módja iránt. Ilyen negatív tapasztalat lehet, ha például átesett egy komolyabb vírustámadáson, vagy akár az is, ha megbüntették valamilyen szabály megsértése miatt.

Azok, akik közvetlent vagy közvetve érintettek negatív információ biztonsági incidensben, jobban tudatában vannak az információ biztonsági előírásoknak, szabályoknak, sokkal inkább szabálykövetőkké válnak, a viselkedésük megváltozik.

Ily módon, a személyes tapasztaltok, főleg a negatív tapasztaltok, pozitív irányba viszik a munkavállalók biztonságtudatosságát, emiatt a viselkedés is megváltozik. A személyes motiváció és a személyes képesség a befolyás legerősebb forrása. Ezért hatásos, ha az információ biztonság tudatossági oktatók a személyes motivációhoz kapcsolják az adott szabályzat pontjait. Amikor a motiváció és a személyes érdek találkozik, a munkavállaló lelkes lesz az információ biztonság irányt.

Nagyon hatásos a megértés vonatkozásában, ha a biztonság tudatossággal kapcsolatban kialakul egyfajta döbbenet, bizonyos „Aha!”, vagy „Úristen, nem gondoltam volna!” érzés. Ha ezt sikerül elérni, akkor szinte biztosak lehetünk abban, hogy az illető az információbiztonsággal kapcsolatban tudatosabban fog cselekedni.

Ha az informatikai veszélyt távolinak látja a munkavállaló, akkor kevésbé sürgeti, hogy a viselkedése megváltozzon. Mivel úgymond nem vele történik, kevésbé hat rá, nem érzi a kockázatot. Nem fél attól, hogy ez vele is megtörténhet. Ha a távoli veszélyt „közelebb” hozzuk, személyessé tesszük, jobban ösztönzi a munkavállalót, hogy változtasson a viselkedésen.

4.8 Társadalmi környezet

Lényeges tényező a dolgozó társadalomban betöltött szerepe, környezete, tanultsága. Ez megmutatja hogyan reagál a váratlan helyzetekre. A társadalmi környezet lehetnek közeli családtagok, barátok, munkatársak, de ide kell érteni a virtuális valóságot, közösségi médiában betöltött szerepet is.

De környezeten a munkahelyet, mint szűkebb környezetet is kell érteni Itt is számít, hogy az alkalmazott mennyire találja meg a helyét a kollégák közt, megbecsülik, kiközösítik-e? Ha a kollégák tisztelik a többiek, megbecsülik, akkor jobban, nyíltabban osztanak meg információkat az információ biztonság terén, és hatékonyabban segítik ebben.
Az információ biztoság tudatosságát nagyban befolyásolja életkor, itt lényeges különbségek lehetnek. A fiatalabb generáció már élete részének tekinti az informatikai eszközöket, rendszereket, ez befolyásolja alkalmazkodás képességét. Érdeklődnek iránta és ez az érdeklődés a biztonság területére is kihat, így alapvetően jobban ismerik a veszélyeket.

4.9 Hírek, Információk

A munkavállaló viselkedésére hatással vannak azok a hírek, információk, amiket olvas újságban, interneten, lát a televízióban, vagy amivel találkozik a szervezet intranetes felületén, hírlevélben. Nem elhanyagolható a közösségi média hatása. Ezek, ha nem is tudatosan, de tudat alatt befolyásoljak a viselkedést.

Fontos, hogy a munkavállaló mennyire érdeklődik az informatikai biztonság irányt, illetve ezzel kapcsolatban mennyi információ jut el hozzá. Ha érdeklődik a terület irányt, több információ jut el hozzá. Ezért is lényeges, hogy az adott szervezet folyamatosan kommunikálja az információ biztonsági tudatosság növelését célzó anyagait. Kell, hogy ezek az információk, mint másodlagos források, folyamatosan a alkalmazottak előtt legyenek.

4.10 Kapcsolat a kollégákkal

Ha egy szervezetnél az alkalmazottak alapvetően szabálykövetők, akkor ez a szabálykövető magatartás átragad majdnem mindenkire. Ha kollégák meg tudják egymással beszélni az érintett szabályokat, az jobban tudatosul bennük, végeredményben befolyásolja a viselkedést. A kollégák figyelmeztetik egymást, ha előfordul olyan eset, hogy valaki súlyosan megsérti, vagy meg akarja sérteni az érvényes információ biztonsági szabályokat. Például, ha valaki a belépéskor nem használja a belépő kártyáját, holott ez előírás, akkor a többi kolléga jelezheti, hogy ez így nem megengedett. Legközelebb tudatosabb lesz belépéskor. Másik példa lehet, hogy ha figyelmeztetik egymást a kollégák a „tiszta asztal” előírásra. Ebben az ecetben is lehet, hogy már oktatáson elhangzott ez az utasítás, de kollégák közti beszélgetéssel ez megerősítés nyer.

5. HOGY TUDUNK MÉRNI?

Információbiztonság-tudatosság szervezésének, fejlesztésének lényeges pontja a mérés. Tudni kell, hogy az adott tanfolyam, vagy kampány mennyire hatékony. Információbiztonsági mérések kapcsán a NIST SP800-55 [42] szabvány megfogalmaz néhány szempontot, amit Muha Lajos tanulmányában [43] így olvashatunk:

- a méréseknek mennyiségi információt kell nyújtaniuk (százalékok, átlagok, és számok),
- a mérések alapjául szolgáló adatoknak könnyen használhatónak lenniük,
- csak megismételhető informatikai biztonsági eljárások vehetők figyelembe a mérések során,
- a méréseknek hasznosíthatóknak kell lenniük a teljesítmény értékeléséhez és az erőforrások kezelésében.

Vagyis a mérésnek egy egyértelmű, számszerűsíthető adatot kell adnia, amiből aztán a számunkra fontos információ kinyerhető. Az adatok könnyű felhasználhatósága segíti a gyors és automatizált feldolgozást. A megismételhetőség azt szolgálja, hogy ugyanazon mérést újra végre lehessen hajtani ugyanazon körülmények között. Ez egyértelmű, mert ha egy terület fejlődését kell mérni, akkor ugyanazokat a számszerűsíthető jellemzőket kell mérni, mint korábban. A mért értékeknek a szervezet számára relevánsnak kell lennie, mert csak így lehet hasznosítani, felhasználni az információbiztonság fejlesztése érdekében.

5.1 Oktatás hatékonyságának vizsgálata

Az oktatási programok eredményességeinek értékelésére az egyik legismertebb módszer a Kirkpatrick-modell [44][45][46], ezért megvizsgálom annak lehetőségét, hogy ezt a módszert hogyan lehet átültetni az információbiztonsági tudatossági képzések, oktatási programok hatékonyságának mérésére. A módszer részletes ismertetését mellőzöm, a módszert az információbiztonsági oktatások vonatkozásában vizsgálom [47].

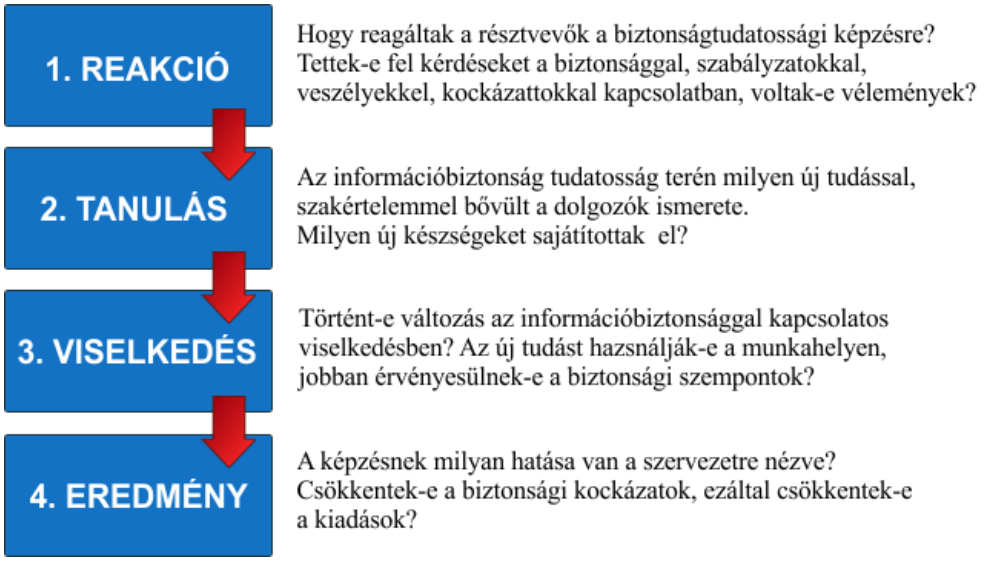
Az értékelésben négy szintet különbözet meg. Az értékelést az első szinttel kell kezdeni, majd ahogy a lehetőségek engedik, sorba kell haladni a második, harmadik, negyedik szintre. Az előző szint adatai alapjául szolgálhatnak a következő szintek elemzésének. Ennek következtében minden szint pontosabban méri a képzés hasznosságát.

1. szint: Reakció szintje. Azt méri, hogy a résztvevők hogyan reagálnak a képzésre. Mennyire elégedettek?

2. szint: Tanulás szintje. Azt vizsgálja, hogy a résztvevők valóban megértették-e a képzést. Növekedett-e a tudás, készségek, tapasztalat?

3. szint: Viselkedés szintje. Azt elemzi, hogy a résztvevők hasznosítják-e a munkájuk során a tanultakat. Változik-e a viselkedés?

4. szint: Eredmények. Azt vizsgálja, hogy a képzés, az anyag a szervezetre nézve milyen (pozitív) hatással volt



5.1. ábra: *Kirkpatrick-modell információbiztonsági szempontból.*

1. szintű értékelés – A reakció

Milyen szempontból tetszett a résztvevőknek a biztonság tudatossági képzés? Hogyan érzik magukat a résztvevők?

Enne a szintnek a célja, hogy értékelje, hogyan reagáltak a résztvevők a tudatossági képzésre, programra. Tettek-e fel kérdéseket a biztonsággal, szabályzatokkal, veszélyekkel, kockázattokkal kapcsolatban, voltak-e vélemények? Az interaktivitásból kiderül, hogy mennyire volt érdekes a képzés, és közben hajszosnak találják-e a munkájukhoz. Mérés ajánlott egy-egy oktatási nap végén.

Néhány példa az első szinten használható technikákra, módszerekre:

- képzés utáni azonnali kérdőívek, űrlapok a képzést szervezők és az oktatók számára is,
- az oktatás online értékelése,
- leírt, vagy szóbeli értélések a szervezők felé,
- oktatás utáni kötetlen, vagy személyes beszélgetések a témáról,
- mennyire elégedettek az oktatóval a résztvevők?
- kaptak-e példákat, illusztrációkat az információbiztonsággal kapcsolatban?

- mennyire elégedett a résztvevő az oktatási eszközökkel. Elég érthető-e a tájékozgató anyag, a bemutató, a videó? Ha online oktatás zajlott, megfelelő volt-e a technikai háttér?

2. szintű értékelés: A tanulás

Megjelentek-e új készségek, új tudás, új attitűdök? Mit tanultak?

Ez a szint azt értékeli, hogy az információbiztonság-tudatosság terén milyen új tudással, szakértelemmel bővült az alkalmazottak ismerete, vagy mi az, amit nem sikerült megismerünk. Milyen új készségeket sajátíthattak el, változott-e a biztonsággal kapcsolatos gondolkodásmód? Mérés ajánlott a képzés végén.

Példák a második szinten használható technikákra, módszerekre:

- interjúk, felmérések a képzés előtt és közvetlenül utána,
- az oktató megfigyelései,
- a résztvevők egymás értékelése,
- A képzés mennyire érintette a szervezet információbiztonsági kockázatait,
- visszakérdezés, vizsga, számonkérés, teszt elvégzése,
- interjú néhány kiválasztott résztvevővel
- megfelel-e az átadott tudás a szervezet elvárásainak, szabályzatának?
- a résztvevő érzi, hogy tényleg gyarapodott a tudása az információbiztonság terén?
- érdemes rákérdezni a konkrét, elhangozott tananyagra.

3. szintű értékelés: A viselkedés

Megváltozik-e a viselkedés, alkalmazzák-e a tanultakat a résztvevők?

Ez a szint elemzi a résztvevők munkahelyi viselkedésében megjelenő különbséget a program vagy képzés befejezése után. Az értékelés ajánlott a képzés befejezése után pár hónappal végezni. A változás értékelése lehetővé teszi annak kiderítését, hogy a program által tanított tudást, gondolkodásmódot vagy készségeket használják-e a munkahelyen. Ez a szint egyértelműen mutatja, hogy az előzőekben mennyire sikerült megértenie a résztvevőknek az oktatáson elhangzottakat.

Ennek a szintnek az értékelése a legfoltosabb, és egyben a legnehezebb is. Lehetetlen minden kolléga mellé odaülni, és figyelni, hogy a biztonság tudatos viselkedése változott-e? Ez megnehezíti annak meghatározását, hogy mikor, milyen gyakran és pontosan hogyan kell értékelni.

Példák a harmadik szinten használható technikákra, módszerekre:

- csoportos beszélgetés,
- automatikus módszerek, mérések, információbiztonsági audit,

- a munkavállaló hogyan látja saját magát, szerinte mi változott,
- interjúk, auditok elvégzése,
- az értékelés, ellenőrzés folyamatos lehet, mert nem biztos, hogy rögtön bekövetkezik a változás, lehet, hogy jó pár hét után érik be az alkalmazottaknál az oktatás,
- meg kell ismerni, hogy a munkavállalók tényleg felhasználták-e a megszerzett tudást,
- értékelni kell a viselkedésbeli változás időtartamát,
- az értékelés legyen munkavállaló, résztvevő számára releváns,
- fontos, hogy az értékelést végző személy elfogulatlan legyen, főleg, ha ő is a cég alkalmazottja.

4. szintű értékelés: Eredmények

Mi a képzés, a program eredménye?

A program elsődleges céljának általában tekintett negyedik szint meghatározza a biztonságtudatossági program sikerét. Itt olyan tényezők számítanak, mint a csökkent informatikai kiadások, az észszerűbb, jobb minőségű eszközbeszerzés, kockázat csökkenése, gyorsabb reagálás az incidensekre, a szabályzatokhoz igazodott-e a viselkedés. Több hónappal a képzés után ajánlott az eredmények vizsgálata.

Példák a negyedik szinten használható módszerekre, szempontokra:

- tényleg csökkent-e a kockázat bizonyos területeken,
- éves szintű vezetői szintű értékelés, hogy teljesültek-e az információbiztonsági célok, milyen közvetett hatás van más területre,
- a kollégákat érdemes bevonni az értékelési folyamatba, fontosak a tapasztalatai,
- a program hozza-e a szervezeti, jogszabályi elvárásokat,
- ki kell deríteni, mely módszerek voltak a leghatékonabbak az oktatási program céljának elérése szempontjából.

5.2 Mérőszámok meghatározása

A mérés és mérőszám (metrika) fogalmát gyakran összekeverik, így ezt tisztázni kell most is [48]. A mérés egy adott időpontban meghatározott érték, amelyet számlálással, összeszámolással áll elő. A mérésre példa a múlt hónapban jelentett fertőzött számítógépek száma. A mérőszámok a mérések elemzésével jönnek létre. A metrika két vagy több mérés összehasonlítása egy bizonyos idő alatt, és egy előre meghatározott kiindulási értékkel. Ilyen lehet például, hogy a fertőzött számítógépek száma 10%-kal nőtt a második negyedévben az első negyedévhez képest [25] [48].

A mérőszám és értékek közti különbséget jelzi az is, hogy az, hogy megemelkedik valamely incidens száma, még nem jelenti azt, hogy romlott a biztonság, biztonság-

tudatosság az adott szervezetnél. Előfordulhat, hogy nagymértékben megemelkedik az adathalász támadások száma, de a kollégák ezt az elvárásoknak megfelelően, jól kezelik.

Hogy pontos képet kapjunk a képzés, vagy biztonság tudatosság program eredményességéről, a mérőszámok egy hatékony eszközt jelentenek. Képet kapunk például arról, hogy a munkavállalók mennyire tudják kezelni a biztonsági incidenseket. A mérőszámok megmutatják egyes részterületek, csoportok, részlegek kockázati szintjét, ezáltal mutatja, hol kell további intézkedéseket bevezetni a tudatosság javítása, fejlesztése érdekében.

A mérőszámok meghatározása nem könnyű feladat, de a vezetők joggal várhatják el, hogy legyen valamiképp számszerűsítve a biztonságtudatosság szintje, illetve az azzal kapcsolatos állapotot. A biztonsági kockáztok számértékekhez rendelése szubjektív, de mégis ki kell alakítani egy szervezeten belüli rendszert, amihez kapcsolódva a továbbiakban elvégzik az értékeléseket. Minden részfolyamatnak kell legyen egy számszerűsített értéke, ami megfelel az elvárásoknak. A mérőszámok megállapításának alapja lehet a törvényi megfelelés, szabványok, céges elvárások, illetve illeszkedjen a már meglévő folyamatokba, keretrendszerekbe.

A mérőszámok szemléltetéséhez a levélszemét témáját írom. Ebben az esetben is jól látszik, hogy a mérések objektív, nyers adatok, sokszor nincs is szükség emberi beavatkozásra, hogy a mért értékeket megkapjuk.

A mérőszámok alapjául szolgáló rendszertől függetlenül az következő hét kulcsfontosságú lépést ajánlom használni a mérőszámok meghatározásával kapcsolatban. Ezek összeállításában a „A Guide to Security Metrics” (SANS) kiadványt vettem alapul [48].

1. lépés: Meg kell határozni a mérőszámok kialakításának célját és célkitűzéseit.

Egyértelmű célokat kell meghatározni, ami segíti a biztonsági kockázatok csökkentését, megfelel a szervezet elvárásainak, biztonsági szabályzatainak. A kialakításba be kell vonni az érdekelt csoportokat, kollégákat. Kommunikálni kell a szervezet minden munkavállalója számára.

Érthetővé kell tenni mindenki számára, hogy a szervezetben a spam-e tartalmazó levelek milyen károkat okozhatnak. Érdekelté kell tenni a munkavállalót abban, hogy a gyanús levelekre figyeljenek. Az lenne az ideális eset, ha egyetlen adathalász levélben történő utasítást sem követnének a munkavállalók, például nem kattint a tartalomban lévő linkre.

2 lépés: Meg kell határozni, milyen mérőszámokat kell létrehozni.

Az adott szervezeten belül zajló folyamatok, vagy keretrendszerek meghatározzák, hogy milyen mérőszámokra van szükség. Itt többféle megközelítés lehet. Előfordul,

hogy egy vállalat a biztonsági folyamatokra összpontosít, itt javít a biztonságon. A megfelelőségre is lehet törekedni, hogy alkalmazkodjunk a szabályzatokhoz, betartsunk magas szintű előírásokat.

Lehet a biztonság tudatoásági program céljából kiindulni, majd a folyamatokara vetítve meghatározni mérőszámokat, De lehet abból is kiindulni, hogy egyáltalán milyen értéket lehet mérni, ezekből mit lehet származtatni. Néhány példa: Vírusfertőzések számának csökkentése 20%-kal, szervezeten belül észlelt sérülékenységek számának csökkentése. Tiszta Asztal politika javítása 50%-kal a következő negyedévben. Adathordozók biztonságos kezelésének emelése éves szinten.

Adathalászat szempontjából fontos tényező a felismert adathalász levelek számának növelése előző hónaphoz képest. Az adathalászatot a biztonsági csoportnak jelentett gyanús e-mailek száma alapján is lehet mérni. Ennek a mérésnek a célja, hogy értékelje azon alkalmazottak számát, akik követték a bejelentésre vonatkozó szabályzatban lévő eljárást. További, automatizált mérésekkel még több információt nyerhetünk, mint például az elküldött, vagy megnyitott e-mailek száma, azon alkalmazottak száma, akik a hivatkozásra kattintottak, vagy az információt bevitt alkalmazottak száma.

3. lépés: Mérőszámok begyűjtésére vonatkozó stratégiák, módszerek.

Módszereket kell kidolgozni az adatok összegyűjtésére vonatkozóan. Meg kell határozni az adatok forrását, adatgyűjtés gyakoriságát, és hogy ki a felelős az adatok begyűjtéséért, pontosságáért.

Ki kell jelölni a személyeket, akik az adathalászattal kapcsolatos információkat gyűjtik. Ez érthetően az adott szervezet információbiztonsággal foglalkozó csoportja, de ebbe be lehet vonni más csoportokat is, például az ügyfélszolgálatot.

4. lépés: Referenciaértékek meghatározása

A képzések, avagy programok referenciaértékét kell meghatározni, ez segít összehasonlítani, meghatározni a szervezet teljesítményét és gyakorlatát az iparágon belüli társakkal. Ebben segíthetnek az úgynevezett iparági „bevált gyakorlatok”, ipari elvárások, szakmai fórumok, szakmai kiadványok, közösség.

Adathalászat szempontjából érdekes lehet a szakma véleménye vagy a szervezet elvárása. Ennek tanulmányozása és mások tapasztalata segít behatárolni, hogy milyen kockázattal kapcsolatos mérőszámok lehetnek elfogadottak.

5. lépés: Meg kell határozni a mérőszámok kommunikálásának módját.

Ha a mérőszámok megfelelő kommunikálása kulcsfontosságú, elérhetővé kell tenni azok számára, akik a döntéshozatalban ezeket fel kell használniuk. Meg kell határozni a kontextust, a formátumokat, a gyakoriságot, a terjesztési módot.

A vezetőség feladata a stratégiai döntések meghozatala, így elég, ha az adathalász e-mailek megjelenéséről és kezeléséről havi jelentést kapnak. Középvezetőknek, csoportvezetőknek, akik már operatív döntést hoznak, napi, vagy azonnali értesülés kell, hogy a megfelelő intézkedést meghozzák. Ilyen lehet a szervezet informatikai szakértőinek szóló azonnali utasítások, vagy a szervezet munkavállalóinak azonnali figyelmeztetése a veszélyes e-mailekre.

6. lépés: Cselekvési terv készítése.

A cselekvési tervnek tartalmazni kell az összes feladatot, amit a mérőszámok indukáltak. Meg kell határozni felelősöket, határidőket, kapcsolódó tevékenységeket. A cselekvési elemeknek közvetlenül a célkitűzésekből kell származniuk, az első ponthoz kapcsolódóan Ezek kapcsolatát célszerű dokumentálni, hogy látható legyen minden érintett számára, hogy miért fontos a cselekvés.

Az adathalász e-mailek kezelésével kapcsolatban megkülönböztethetünk hosszú- közép- és azonnali cselekvési terveket, utasításokat. A mérésekből kiindulva hosszútávú stratégiát kell alkotni, hogy ezek számát, kockázatait csökkentsük, igazodva a célkitűzésekhez. Ebből kiindulva aztán a képzési tervbe ezt a témát is be kell építeni. Az azonnali cselekvési tervek már konkrét utasításokat jelent, hogy mit kell csinálni akkor, ha gyanús e-mailekkel találkozunk, és mit kell akkor, ha valakit sikerült ezzel átverni (milyen rendszereket kell felülvizsgálni). Ez nem csak az IT csapatot érintheti, kiterjedhet a szervezet többi munkavállalója számára is.

7. lépés: Felülvizsgálat, ellenőrzés

Mint minden folyamatban, itt is fontos az ellenőrzés, rendszeresen újra kell értékelni a mérőszámok rendszerét. Meg kell vizsgálni, hogy a cél elérése céljából elegendő, vagy kevés emberi és technikai erőforrás áll rendelkezésre. Meg kell vizsgálni, tényleg pontosak-e a mutatók, és hasznosak-e az informatikaibiztonság tudatosság növelése szempontjából.

Itt vissza kell kanyarodni a folyamat elejére, vagyis, hogy a mérések alapján sikerült-e elérni a kívánt célt? Megértették-e a dolgozók a célt, tényleg kevesebb az adathalász e-mailekkel kapcsolatos kockázat. Csökkent-e az adathalász e-mailekkel kapcsolatos incidens?

5.3 Audit

Az auditot tekinthetjük a mérés egyfajta formájának, célja annak mérése, hogy a munkatársak biztonságtudatossága megfelel-e az elvárásoknak. Egy tiszta képet kell kapnunk mennyire tették magukévá az átadott ismereteket, mennyire veszik komolyan a szabályokat. Ez az egyik leghatékonyabb módszer a felmérésre, mivel közvetlen tapasztalat szerezhető a biztonság állapotáról.

Az audit másik célja, hogy nem csak a felhasználót tesztelik, hanem az adott vállalatot is. Meg lehet tenni a biztonsági kontrollok hatékonyságának vizsgálatát, ezt esetleg ki lehet-e kerülni, van-e kiskapu, a biztonsági elemek jól működnek-e? Például a beléptetés protokollja megfelelő-e? Mindent megtett-e a vállalat, hogy a munkavállalót tudja támogatni, és hogy az alkalmazott a social engineering támadásokat azonosítani tudja és el tudja-e hárítani.

Az audit egy további célja, hogy példákat szolgáltasson oktatáshoz, támogassa az alkalmazottak képzését. Ugyanis, ha egy általános információbiztonsági tudatossági oktatást kap egy alkalmazott, akkor az számára nem elég érdekes, és nem elég hatékony az oktatás. Egy általános oktatásban bemutatják, melyek a leggyakoribb munkavállalói hibák, általánosságban mennyire biztonságtudatosak, hogyan lehet kivitelezni és kivédeni egy támadást stb. Ezzel szemben, ha egy adott cégnél, egy audit során előfordult hibákat mutatunk be egy oktatás során, sokkal jobb érdekli az oktatáson résztvevőket, mivel ezt már inkább a sajátjuknak érzik. Érdekli őket, hogy pontosan milyen módszerekkel próbálkozott az auditor, és hogy sikerült vagy nem sikerült végrehajtani a támadást, és ki, miért dőlt be a támadásnak. Ezt meg is tudják beszélni oktatás alatt, és emiatt az interakció miatt ez nagyon hatékonnyá teszi az oktatást.

Az audit eredménye

Az információ biztonsági audit során, illetve annak befejeztével több dokumentum készülhet. Mindenképp kell egy audit jelentésnek születnie. Ez tartalmaz vezetői összefoglalót, mi volt a vizsgálat célja, ez mikor zajlott, milyen támadási technikák lettek kipróbálva, ezeknek mi lett az eredménye, és ezek értékelése. Milyen mérőszámok születtek, és ezek az elvárthoz képes hol vannak. A vezetőség számára egy összefoglaló prezentáció szükséges arról, hogy mit lehet elérni egy valós támadás során a szervezetnél, pár szóban, esetleg grafikonokkal, ábrákkal illusztrálva az audit eredményét.

Az audit jelentés még tartalmaz kockázat elemzést, ahol megjelenik, a kockázat súlyossága, és mit lehet elérni egy támadás során. Ezekhez kapcsolódóan egy leírás kell az egyes pontokra vonatkozó védelmi intézkedésekről.

Az audit eredmény felhasználása

Informatika biztonsági audit is egy eszköz, ami fokozza a biztonság tudatosságot, egyfajta szemléletváltást hozhat a munkavállalóknak. Ennek eredményeképp beláthatják, hogy bizonyos védelmi intézkedésekre miért van szükség.

Az audit eredménye felhasználható:

- logikai és fizikai biztonsági intézkedések javításához, fejlesztéséhez,
- szabályzatok módosításának alátámasztásához,
- biztonságtudatossági oktatások fejlesztéséhez,

- biztonságtudatossági kampányok, programok kialakításához.

5.4 Passzív információ gyűjtés

Nem mindenki szereti az auditokat, nem akarja kellemetlen helyzetbe hozni az alkalmazottakat, nem akar például szimulált támadást, de szeretné tudni, milyen szinten áll az adott szervezetnél az információbiztonsági tudatossági szint.

A passzív információ gyűjtés elsősorban technológia támadások elleni védelem mérésére való. Ezzel fel lehet mérni, hogy milyen programokat használnak a felhasználók, internetezési és hálózat használati szokásokat lehet mérni. Felmérést, statisztikát lehet készíteni, hogy az alkalmazottak mennyire tartják be a biztonsági szabályokat.

Az eredmények felhasználásánál figyelemmel kell lenni arra, hogy ezzel nem lehet minden social engineer támadási módszert szimulálni. Az eredmények korlátozottak, ez a vizsgálat egy szűk területre válaszol, az eredménynek korlátozottan használhatók.

5.5 Kérdőíves felmérés

A kérdőíves felmérés az egyik legegyszerűbb módja a felmérésnek. Költséghatékony, viszonylag gyorsan össze lehet állítani a kérdőívet, és pár nap, vagy hét alatt ki lehet tölteni a felhasználókkal. Ez belső erőforrással is megvalósítható, nem kell külső partnert felkérni hozzá.

Rákérdezhetünk biztonsági kontrollokra, eljárásokra, technikai tudásra, kiadott szabályzatokra, módszerekre informatikai ismeretekre.

A kérdőívben célirányos, az adott vállalat számára releváns kérdéseket érdemes feltenni. A legfontosabb kérdés, hogy mire vagyunk kíváncsiak? Mire keressük a választ? A kapott eredményeket mire tudjuk felhasználni? Már a kérdőív elkészítenél tudnunk kell, hogy egy kérdéssel, egy kérdésre adott megválaszolásával mire kapunk választ, hogy segíti a munkánkat. Azért nem jó az általános kérdés az információbiztonsági tudatossági szintről, mert nem ad reális képet az adott vállaltra vonatkozó biztonsági tudatossági szintről. Például ne a belépésekről kérdezzünk, hanem az adott vállalatnál előforduló belépési módszerekre, előírásokra. Vagy például ne magáról a levelezésről kérdezzük a munkavállalót, hanem hogy ő hogyan használja a levelezését?

Nem kell a vállalatnál elforduló minden területre kiterjedő kérdőívet készíteni, lehet fokuszálni egy-egy kiemelet területre: Home Office-ra, fizikai belépésre, mobil használatra, levelezés használatra stb. Így több kérdést is fel lehet tenni a területre vonatkozóan. Ez lehet időszakos is, tehát kialakítható az, hogy akár negyedévente más-más területre vonatkozó kérdéssort kapjanak a munkavállalók.

Fontos a jó kommunikáció, megfelelően kell motiválni az alkalmazottat, hogy neki is érdeke legyen a kitöltés. Rá lehet például kérdezni érvényben lévő szabályzatokra is, mert ha értelmetlennek, vagy feleslegesnek tartják, akkor nagyobb hajlandósággal válaszolnak az ilyen jellegű kérdésekre, ezzel is valós választ adnak.

A Kérdőív eredménye

A kérőívre adott válaszokat ugyanarra, tudjuk felhasználni, mint az audit eredményét. Vagyis milyen oktatások kellenek a későbbiekben, milyen biztonság tudatossági kampány kell, kell-e esetleg módosítani valamelyik szabályzaton.

A kérdőíves felmérés eredményéről is kell a vezetésnek bemutatót tartani, kell jelentést készíteni, mellékelteket leadni. Mik voltak a célok, milyen eredmény született. Ezek alapján intézkedési javaslatokat, következtetéseket is meg lehet fogalmazni.

5.6 Szimulált támadások

A szimulált támadások segítségével egy ellenőrzött környezetben lehet felmérni a szervezet információbiztonság tudatosságát. Ez azt jelenti, hogy létrehozunk ugyanolyan e-maileket, mint amit egy valódi támadó is készítene. Az e-mailben megjelenő linkek valódiak, viszont egy olyan oldalra mutatnak, ahol statisztikát lehet készíteni arról, hogy ki, mikor kattintott rá. A szimulált támadáshoz készített e-mail lehet általános témájú, de ha van rá lehetőség, itt is ajánlott egy-egy adott témára fókuszálni. Az e-mail témája attól is függ, a biztonság tudatosság mely részére akarunk fókuszálni. Például, ha a gazdasági osztály alkalmazottairól kell felmérést készíteni, érdemes pénzügyi témájú e-mailt küldeni. A szimulált támadásokat lehet automatizálni, de nem érdemes mindig ugyanabban az időben kiküldeni a leveleket (például havonta hétfő reggel), mert ekkor megszokják, és tudják, hogy az csak egy teszt levél. Az automatizált szimulált támadások nagy előnye lehet, hogy létre lehet hozni egy mutatót, mely jelzi a szervezet folyamatos információbiztonsági tudatosságát ezen a téren, megállapíthatjuk milyen a fejlődés mértékét.

5.7 Egy lehetséges megvalósítás

A szakdolgozat készítése közben nem találtam olyan egyértelmű, általános módszert, ami segítséget ad a biztonság-tudatosság jellemzőinek méréséhez. Számtalan javaslat van arra, hogy mérni kell, de ennek megvalósítását a szervezetre bízzák. Emiatt egy egyszerű módszert kínálok, ami bárkinek segíthet az elindulásban és a szervezet számára testre szabható.

Az előző részekben leírtak figyelembevételével meg kell határozni, mit szeretnénk mérni. Itt is lényeges, hogy olyan értéket mérjünk, ami releváns a szervezet számára. Tehát ne azt nézzük meg, hogy a munkavállalók értik-e mire való egy beléptető rendszer, hanem azt, hogy az adott szervezetnél lévő beléptetőt rendesen használják-e?

A szakdolgozathoz mellékellek egy általam szerkesztett táblázatot, amellyel az információbiztonság-tudatosság állapotát követhetjük, ennek egy részlete látható az 5.2. ábrán. A táblázatot feltöltöttem fiktív adatokkal, hogy látható legyen a működés. A táblázat *Értékek* fülének első oszlopában egy olyan lista látható, amelyben a szervezetre jellemző problémák, veszélyek lehetnek. Ez a rész helyettesíthető akár kockázatokkal, ha egy szervezet számára az értékelhetőbb eredményt ad. A további oszlopokban a szervezet munkavállalóinak csoportosítása található, itt négy jellemző csoportot hoztam létre. Természetesen ezek tovább bonthatók és itt is igaz az, hogy mindig figyelembe kell venni a szervezet sajátosságait, esetleg lehet több csoportot létrehozni, feladatkörtől, helyszíntől, beosztástól stb. függően. A csoportok alatt a havi bontás látható.

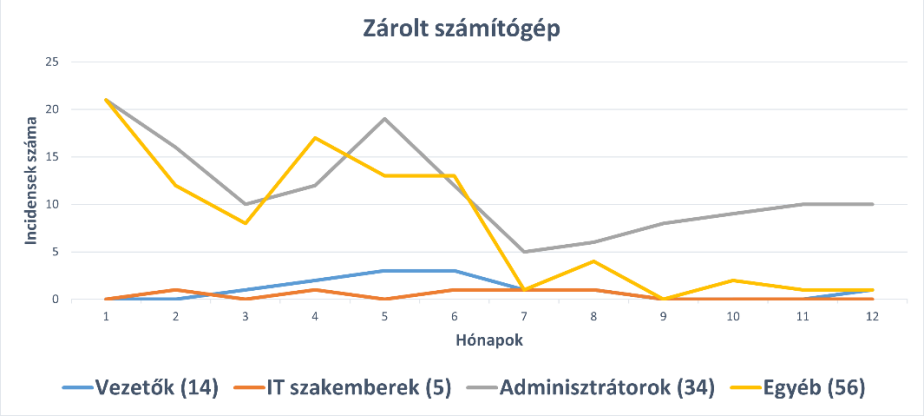
A táblázat értékei az incidensek száma. Ez kiderülhet egy audit, online felmérés, hibabejelentés, automata gyűjtés vagy bármi egyéb kapcsán. Az egyes értékek az előforduló eseteket jelentik. Például látszik, hogy az *Adminisztrátorok* munkaköri csoportban, hogy januárban kettő olyan eset volt, amikor a munkavállaló tartósan nem hagyta, hogy az operációsrendszer frissítések lefussanak, vagy egy állandó audit során kiderült, hogy egy hónapban huszonegy fordult elő az, hogy úgy hagyta ott a munkaállomást alkalmazott, hogy nem zárolta a képernyőt.

.

IT biztonság-tudatossági problémák Adatgyűjtés: 2021. év	Vezetők (14)												
	Jan	Feb	Már	Ápr	Máj	Jún	Júl	Aug	Sze	Okt	Nov	Dec	Átlag
Frissítések telepítésének engedélyezése	3	3	4	5	6	10	2	3	4	5	6	4	4,6
Zárolt számítógép	0	0	1	2	3	3	1	1	0	0	0	1	1,0
Kidobott érzékeny dokumentum	0	0	0	0	1	1	0	0	0	0	0	0	0,2
Kísérő nélküli személyek	0	0	0	0	0	0	0	0	0	0	0	0	0,0
Ellopott jelszó	0	0	0	0	0	0	0	0	0	0	0	0	0,0
Elküldött lánclevelek	0	0	0	0	0	1	0	0	0	0	0	0	0,1
Adathalász e-mailek	2	3	4	5	5	5	3	2	2	1	0	0	2,7
Megtévesztéses támadás	0	0	0	0	1	0	0	0	0	0	0	0	0,1
Beléptető rendszerek helytelen használata	3	4	4	5	3	4	5	6	4	3	3	3	3,9
Elvesztett adathordozó	0	0	0	1	0	0	0	0	0	0	0	0	0,1
Csali adathordozó használata	0	0	0	0	0	0	0	0	0	0	0	0	0,0
Szabályzatok ismeretének hiánya	1	2	2	1	1	2	2	2	2	1	3	1	1,7
Információmegosztás közösségi oldalon	0	0	1	0	0	1	0	0	0	0	0	1	0,3
Közös nyomtatóban hagyott dokumentumok	0	0	0	0	0	0	0	0	1	0	0	0	0,1

5.2. ábra: *részlet a mellékelt szintfelmérő táblázatból, adatok.*

Ezen értékek a táblázat *Összegzés* fülén grafikonban jelennek meg. Itt a hónapokat és az előforduló incidenseket látjuk. Ennek egy részlete az 5.3. ábrán látható



5.3. ábra: *részlet a mellékelt szintfelmérő táblázatból, grafikon.*

A felvett értékekből kiderül a rögzített időszakban megjelent átlagos incidens szám. A grafikon mutatja az incidensek változását havi megjelenésben. Ezek mutatják, hogy melyek azok a területek, ahol az információbiztonság-tudatosságot növelni kell. Ahol a bejelentett incidensek száma elér egy meghatározott határértéket, vagy ha egy adott problémánál emelkedés látszik a grafikonon, az a terület fokozott figyelmet igényel. Ezen a területen erősíteni kell a biztonságtudatosítási programokon, oktatást, kampányt kell szervezni, vagy egyéb módon fel kell hívni a munkatársak figyelmét a problémára. Ezen kívül ezek a mérőszámok visszajelzésként is működnek, mert ha lezajlott egy széles körű képzés, vagy kampány, megállapítható, hogy azon incidensek bekövetkezte esetében, amik a munkavállaókon múlnak, tényleg javultak-e az eredmények?

6. ÖSSZEGZÉS

A szakdolgozatommal az információbiztonság-tudatossági képzések eredményességéhez, létrehozásához, fenntartásához járulok hozzá. A bemutatott módszerek segítenek az információbiztonsági oktatások fejlesztésével foglalkozóknak és azoknak, akik a social engineering témáját vizsgálják.

A szakdolgozatban mindenekelőtt kifejtettem, hogy miért fontos tényező az ember az információbiztonság szempontjából, ezzel kapcsolatban részleteztem a munkatárs szerepét, aki adatokat kezel, feldolgoz. Ezeket a közösségi média és a Home Office kapcsán is elemeztem.

Social engineering támadási és védekezési módokat gyűjtöttem és foglaltam össze. Ezeket olyan szempontól is sikerült összegeznem, hogy mik azok az emberi tulajdonságok, szituációk, állapotok, amik segítik az adott támadást. A támadás megelőzésére védekezési módot ajánlottam, bemutattam azokat az oktatási lehetőségeket, amivel a támadás kockázata csökkenthető.

Ezek után a védekezéssel kapcsolatban egy több lábon álló védelmi intézkedést mutattam be. A kockázat kezelés fontosságáról írtam, összekapcsoltam az ember jelentette kockázatokat ezek lehetséges csökkentésének módjával. Négy szabványról, ajánlásról írtam részletesebben, amik az információbiztonságot segítik. Azért választottam ezeket, és tartottam fontosnak, mert itt konkrétam megjelennek az információbiztonság-tudatosság képzésére vonatkozó ajánlások. Az oktatásokkal kapcsolatban bemutattam azt, hogy megvalósítási lehetőségek vannak és bemutattam ezek előnyeit és hátrányait is.

Ismertettem a biztonságtudatossági program lehetséges forrásait, ezek tekintetében ajánlottam azonnal használható anyagokat, internetes forrásokat.

Az oktatások lehetséges célcsoportjait fontosnak tartottam bemutatni, mert az oktatások kapcsán nem mindegy, hogy kik a résztvevők. Más kell mondani a vezetőségnek és mást az informatikusoknak. Itt kiemeltem a vezetőség szerepét, mivel véleményem szerint ők döntően befolyásolják a biztonságtudatossági képzések, programok eredményességét.

Az oktatásokat, tudatossági kampányokat, szabályozásokat, kockázatkezelést figyelembe véve összegeztem az információbiztonság növekedésének várható hatásait, illetve azt, hogy ezek milyen előnyökkel járnak az adott szervezetet illetően.

A szakdolgozatban megvizsgáltam, mik azok a tényezők, amelyek befolyásolják a biztonságtudatos magatartást. Ezt azért tartottam fontosnak, mert alapvetően meghatározzák azt, hogy egy social engineering támadás sikeres lesz-e vagy nem? Itt kiemeltem, hogy az egyik legerősebb szempont az, ahogy az illető érzelmileg mennyire van elkötelezve az információbiztonság-tudatosság iránt.

Az oktatások hatékonyságának mérésére a Kirkpatrik-módszert mutattam be. Ez egy általános módszer az oktatások hatékonyságának megállapítására és itt arra törekedtem, hogy ezt információbiztonsági képzések vonatkozásában vizsgáljam. A mérőszámok megállapítására egy hét lépéses módszert ismertettem, ami a biztoságtudatossági programok eredményességét mutatja.

A szakdolgozat készítésekor és a szakirodalmat tanulmányozva arra a következtetésre jutottam, nem egyszerű feladat pontosan megállapítani valakiről, vagy egy dolgozói csoportról, hogy mennyire biztonságtudatos. Ennek ellenére kidolgoztam egy egyszerű módszert, amivel mégiscsak lehet valamennyire számszerűsíteni, hogy adott területen, adott munkavállalói csoportnál az információbiztonság-tudatosság milyen szintű, a méréseket rendszeresen elvégezve hosszú távú kimutatás készíthető. Ezen kívül következtetéseket lehet levonni arra nézve, hogy mely területeket kell fejleszteni, oktatásokat szervezni, vagy mely területeken elfogadható az információbiztonság-tudatosság szintje.

7. SUMMARY

With my dissertation I contribute to the effectiveness, creation and maintenance of information security awareness trainings. The methods presented will help those involved in the development of information security education and those who study the topic of social engineering.

In the dissertation, first of all, I explained why people are an important factor in terms of information security, and in this connection I detailed the role of the employee who handles and processes data. I also analyzed these in relation to social media and the Home Office.

I collected and summarized social engineering attack and defense methods. I also managed to summarize these in terms of the human characteristics, situations, conditions that help a given attack. To prevent the attack, I recommended a method of defense, I presented the educational options that can reduce the risk of the attack.

After that, I presented a multi-legged protection measure in relation to defense. I have written about the importance of risk management, linking the risks posed by people to the way they can be reduced. I have written in more detail about four standards and recommendations that help information security. I chose these and considered them important because here are the specific recommendations for training in information security awareness. In connection with education, I have shown that there are possibilities for implementation and I have also presented their advantages and disadvantages

I have described the possible sources of the security awareness program, and I have recommended materials and internet resources that can be used immediately.

I considered it important to present the possible target groups of the trainings, because it does not matter who the participants are in connection with the trainings. There is a different thing to say to management and a different thing to IT professionals. Here I highlighted the role of the management, because in my opinion they have a decisive influence on the effectiveness of safety awareness trainings and programs.

Taking into account the trainings, awareness campaigns, regulations, risk management, I summarized the expected effects of the increase in information security, as well as the benefits of these for the given organization.

In my dissertation, I examined the factors that influence safety-conscious behavior. I considered this important because they basically determine whether a social engineering attack will be successful or not? Here, I emphasize that one of the strongest aspects is how emotionally committed one is to information security awareness.

To measure the effectiveness of the trainings, I presented the Kirkpatrik method. This is a general method for determining the effectiveness of training, and here I have sought to examine it in relation to information security training. I have described a seven-step method for determining metrics that demonstrates the effectiveness of safety awareness programs.

While writing my dissertation and studying the literature, I came to the conclusion that it is not an easy task to determine exactly how safety-conscious someone or a group of employees are. Nevertheless, I have developed a simple method, which can still be used to quantify the level of information security awareness in a given area, for a given group of employees, and to make a long-term statement by taking the measurements regularly. In addition, conclusions can be drawn as to which areas need to be developed, trainings organized, or in which areas the level of information security awareness is acceptable.

8. IRODALOMJEGYZÉK

[1] Mitnick, K., D., Simon W., L.: A legendás hacker - A megtévesztés művészete, Perfact-Pro Kft., 2003, ISBN: 9789632065557

[2] Az információbiztonság lélektana, tanulmánykötet. Nemzeti Kibervédelmi Intézet, (https://nki.gov.hu/wp-content/uploads/2019/07/01-Az-inform%C3%A1ci%C3%B3biztons%C3%A1g-l%C3%A9lektana.pdf), utoljára megtekintve: 2020. 03. 03

[3] An update on our security incident, Twitter Inc. (https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident), 2022. 04. 04.

[4] Így törték fel a Twittert, (https://biztonsagportal.hu/igy-tortek-fel-a-twittert.html), utoljára megtekintve: 2022. 04.04.

[5] A. Szarvák, V. Póser: Information Technology Safety Awareness – a review of regularly used terms and methods, AIS 2020, 15th International Symposium on Applied Informatics and Related Areas organized in the frame of Hungarian Science Festival 2020 by Óbuda University, 2020, pp. 107-111., ISBN 978-963-449-209-2 utoljára megtekintve: 2020. 11. 10.

[6] Tarján Gábor, Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben, 28.o. (http://phd.lib.uni-corvinus.hu/1090/1/Tarjan_Gabor_dhu.pdf), utoljára megtekintve: 2022. 04. 27.

[7] Kurt S. Dr.: Kirkpatrick Model: Four Levels of Learning Evaluation, (https://educationaltechnology.net/kirkpatrick-model-four-levels-learning-evaluation/), utoljára megtekintve: 2022. 04. 11

[8] Hadnagy, C.: Social Engineering: The Science of Human Hacking, Wiley, 2018, ISBN: 978-1-119-43338-5

[9] Lithuanian Man Pleads Guilty To Wire Fraud For Theft Of Over $100 Million In Fraudulent Business Email Compromise Scheme, (https://www.justice.gov/usao-sdny/pr/lithuanian-man-pleads-guilty-wire-fraud-theft-over-100-million-fraudulent-business), utoljára megtekintve: 2022. 03. 01.

[10] Microsoft shares new threat intelligence, security guidance during global crisis, (https://www.microsoft.com/security/blog/2020/04/08/microsoft-shares-new-threat-intelligence-security-guidance-during-global-crisis/), utoljára megtekintve: 2020. 04. 20.

[11] COVID-19 Social Engineering Attacks, (https://www.lorca.co.uk/wp-content/uploads/2020/05/Social-engineering-attacks-and-COVID-19.pdf), utoljára megtekintve: 2022. 04. 12.

[12] Global Social Media Stats, Overview of social media use, (https://datareportal.com/social-media-users), utoljára megtekintve 2022. 04. 20.

[13] Global social media statistics research summary 2022, (https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/), utoljára megtekintve: 2022. 04. 20.

[14] Cialdini R., B.: Hatás, HVG kiadó Zrt., 2009, ISBN: 9789639686779

[15] Oroszi, E.,: Social Engineering, NetAcademia Oktatóközpont, (https://netacademia.hu/courses/socialeng), utoljára megtekintve: 2020. 10. 10.

[16] Oroszi, E.,: Social Engineering, Az emberi erőforrás, mint az információbiztonság kritikus tényezője, (http://docplayer.hu/3827943-Social-engineering-az-emberi-eroforras-mint-az-informaciobiztonsag-kritikus-tenyezoje.html), utoljára megtekintve: 2020. 10. 10.

[17] ISO27001:2013 szabvány, ISO, IEC

[18] ISO27001:2014 magyar szabvány, Magyar Szabványügyi Testület

[19] NIST Special Publication 800-53 Rev 5, Security and Privacy Controls for Information Systems and Organizations, (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf), utoljára megtekintve: 2020. 10. 10.

[20] Wilson, M., Hash, J.,: Building an Information Technology Security Awareness and Training Program, U.S. GOVERNMENT PRINTING OFFICE, (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf), utoljára megtekintve: 2020. 11. 16.

[21] COBIT 5 Vállalati IT irányítás és menedzsment üzleti keretrendszere, (letölthető regisztráció után, https://www.isaca.org/resources/cobit), utoljára megtekintve: 2020. 10. 10.

[22] Muha L.: Informatikai biztonsági szabványok és irányelvek, (http://real.mtak.hu/11149/1/1228885.pdf), utoljára megtekintve: 2020. 12. 01.

[23] Muha L, Krasznay Cs.: Az elektronikus információs rendszerek biztonságának menedzselése, (https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/7135/Az%20elektronikus%20inform%C3%A1ci%C3%B3s%20rendszerek%20biztons%C3%A1g%C3%A1nak%20menedzsel%C3%A9sej%C3%B3.pdf?sequence=5&isAllowed=y), utoljára megtekintve: 2020. 10. 10.

[24] 2013 évi L törvény, (https://net.jogtar.hu/jogszabaly?docid=a1300050.tv), utoljára megtekintve: 2020. 10. 11.

[25] Gardner, B., Thomas, V.: Building an Information Security Awareness Program, Syngress, 2014, ISBN 978-0-12-419967-5

[26] Building Serialized Phishing Simulation and Security Awareness Campaigns, (https://resources.infosecinstitute.com/topic/building-serialized-phishing-simulation-and-security-awareness-campaigns/), utoljára megtekintve: 2022. 04. 01

[27] ComputerWorld magazin, Project029 Magyarország Szolgáltató Kft., (https://computerworld.hu/), utoljára megtekintve: 2021. 12. 10.

[28] SANS OUCH! newsletter, SANS™ Institute, (https://www.sans.org/newsletters/ouch/), utoljára megtekintve: 2022. 02. 10.

[29] Kocsis T.: „Sharky", KiberBlog, (https://kiber.blog.hu/), utoljára megtekintve: 2022. 04. 12.

[30] Hétpecsét Információbiztonsági Egyesület, (https://hetpecset.hu/site/), utoljára megtekintve: 2022. 04. 12.

[31] WITSEC szakmai közösség, WOMEN IN IT SECURITY Egyesület, (https://www.witsec.hu/hu), utoljára megtekintve: 2022. 04. 12.

[32] Nemzeti Kibervédelmi intézet megszemélyesítéses támadások, (https://nki.gov.hu/wp-content/uploads/2019/03/8_Megszemelyesiteses-tamadasok.pdf), utoljára megtekintve: 2022. 01. 04.

[33] NIST 800-16 Rev1, A Role-Based Model for Federal Information Technology/Cbersecurity Training, National Institute of Standards and Technology, https://csrc.nist.gov/CSRC/media/Publications/sp/800-16/rev-1/draft/documents/sp800_16_rev1_3rd-draft.pdf), utoljára megtekintve: 2020. 10. 03.

[34] Toyota Subsidiary Loses $37 Million Due to BEC Scam, (https://www.cpomagazine.com/cyber-security/toyota-subsidiary-loses-37-million-due-to-bec-scam/), utoljára megtekintve: 2022. 04. 12.

[35] Hacker Plans to Dump Alleged Details of 20,000 FBI, 9,000 DHS Employees, (https://www.vice.com/en/article/9a3y4e/hacker-plans-to-dump-alleged-details-of-20000-fbi-9000-dhs-employees), utoljára megtekintve: 2022. 04. 12.

[36] Cosmic Lynx: A Russian Threat Hits the BEC Scene, (https://www.agari.com/email-security-blog/cosmic-lynx-russian-bec/), utoljára megtekintve: 2022. 04. 12.

[37] The "Pizza" method – a social engineering Case Study, (https://cyberforces.com/en/the-pizza-method-a-social-engineering-case-study), utoljára megtekintve: 2022. 04. 12.

[38] Iran nuclear attack: Mystery surrounds nuclear sabotage at Natanz, (https://www.bbc.com/news/world-middle-east-56722181), utoljára megtekintve: 2022. 04. 12.

[39] A Stuxnet vírus és az iráni atomprogram, (http://nuklearis.hu/sites/default/files/nukleon/Nukleon_4_1_85_Cserhati_.pdf), utoljára megtekintve: 2022. 04. 12.

[40] Haeussinger, F. J., Kranz J. J.: Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior, (https://www.researchgate.net/publication/258926834_Information_Security_Awareness_Its_Antecedents_and_Mediating_Effects_on_Security_Compliant_Behavior), utoljára megtekintve: 2021. 12. 12.

[41] Kollár, Cs., dr.: Az információbiztonság-tudatosság fejlesztése a (felső)vezetők körében, (http://www.epa.hu/02300/02303/00023/pdf/EPA02303_mc_2016_3_035-049.pdf), utoljára megtekintve: 2020. 03. 03.

[42] Chew E., Swanson M., Stine K., Bartol N., Brown A., Robinson W.: Performance Measurement Guide for Information Security, NIST Special Publication 800-55 Rev 1, National Institute of Standards and Technology, (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf), utoljára megtekintve: 2021. 10. 10.

[43] Muha Lajos, Az informatikai biztonság mérése, (http://real.mtak.hu/12938/1/1278547.pdf), utoljára megtekintve: 2022. 04.20.

[44] Kurt S. Dr.: Kirkpatrick Model: Four Levels of Learning Evaluation, (https://educationaltechnology.net/kirkpatrick-model-four-levels-learning-evaluation/), utoljára megtekintve: 2022. 04. 11

[45] Márkus D., Rácz I.: Munkahelyi képzés hatékonyságának mérése egy nagyvállalat példáján, (https://kgk.sze.hu/images/dokumentumok/kautzkiadvany2017/Markus_Racz_Kautz%202017.pdf), utoljára megtekintve: 2021. 12. 03.

[46] The Kirkpatrick Model, (https://www.kirkpatrickpartners.com/the-kirkpatrick-model/), utoljára megtekintve: 2022. 04. 12.

[47] Kárász, B.,: Biztonságtudatossági tréningek hatékonyságának vizsgálata (http://hadmernok.hu/192_26_karasz.pdf) utoljára megtekintve: 2021. 04. 02.

[48] Payne S. C.:A Guide to Security Metrics, (https://sansorg.egnyte.com/dl/kiYWJmz3vh), SANS Institude, utoljára megtekintve: 2022. 04. 03

9. ÁBRAJEGYZÉK

10. TÁBLÁZATJEGYZÉK

11. MELLÉKLET

11.1 Mit használ ki a támadó?

Személyes tulajdonságaink

Segítőkészség

Az egyik legelemibb emberi tulajdonság. Minden ember segítőkész, van, aki jobban, van, aki kevésbé. A leginkább segítőkészek azok, akiknek a munkája is megköveteli, hogy segítőkészek legyenek. Ennek a tulajdonságnak egyik legjellemzőbb kihasználási módja, ha a támadó belépő kártya nélkül akar bejutni egy épületbe. Mert ha azt látja egy kicsit is segítőkész kolléga, hogy valaki, akár egy új kolléga, bajban van, nem találja a belépőkártáját, tartja az ajtót, és beengedi. Az ilyen és ehhez hasonló helyzetet elkerülése érdekében fontos lenne vendégkártyát biztosítani a látogatóknak, és azt feltűnő helyre tenni, és bátorítani kell a kollégákat, ha idegent lát, kérdezze meg, kihez megy, igazolják jogosultságukat.

Olyan munkakörök, ahol fontos a segítőkészség a recepciós, titkárnő, portás, ügyfélszolgálati alkalmazottak stb. ezeknél különösen fontos ezen kihasználható tulajdonság tudatosítása. Külön figyelmet igényel az ügyfélszolgálatos munkakör, ez tipikusan olyan, ahol segíteni kell, nehéz kiszűrni, ha valaki ezt akarja kihasználni.

Naivitás

A naiv ember hiszékeny, ha hivatalos dokumentumot lát, egyáltalán nem fog gyanakodni, nem jár utána a valódiságának. A támadó nagyon könnyen átveri a naiv embert, könnyen tudja magát kiadni egyfajta problémamegoldónak, hiszen úgysem jár utána az áldozat, hogy a támadó az-e, akinek kiadja magát. Ha segítését kap az áldozat, nagyon örül neki, közben nem is tűnik fel neki, hogy akaratlanul is egy támadást segít. Ezen kívül a munkatársak szívesen segítenek egy olyannak, aki a munkatának adja ki magát és bajban van. Sokszor elég az, ha a támadó ismeri a szakszargont.

A naivitás a számtógépes rendszert használva is megjelenik, ezt ugyancsak gyakran kihasználják ki. Sok felhasználó könnyel elhiszi, hogy egy hívogató weblapra regisztrálva tényleg nyerhet valamit, vagy letölthet valami nagyon fontos dolgot, zenét, filmet. E-mailek használatánál is ez a helyzet, a felhasználó minden gyanakvás nélkül nyitja meg a ismeretlen feladótól származó levelet, illetve ennek csatolmányát. Ez utóbbi probléma, főleg idősebb felhasználóknál jelentkezik. Az idősebb korosztály nem szokott hozzá annyira a számítógépek világához, mint a fiatalabbak, akik már az iskolában is tanulják ezt, nem is gondolnak bele, hogy ez milyent veszélyt hordoz. Egy idősebb felhasználónak egy egészen különleges élményt jelenthet az internet világa, izgalmas lehet, ha megkapják az első e-mailt.

Barátságosság

Önmagában az sem baj, ha valaki barátságos, és nyitott. De ha valaki elég barátságosnak tűnik, a támadó megpróbálhat összebarátkozni a kiszemelt személlyel. Ez nagyon jól jöhet akkor, ha pl. karbantartóként jut be a támadó egy épületbe, irodába, ott összebarátkozhat egy ott dolgozó alkalmazottal, akinek a számítógépét valamilyen mondvacsinált hibával meg kell javítani. A barátkozás, mint figyelemelterelés működhet, az áldozat nem is nagyon figyel oda, hogy a támadó mit csinál a számítógépén. Ezt segítheti a korábbi információgyűjtés, amikor a támadó információkat gyűjt az áldozatról, és az áldozatot érdeklő témákról kezd el beszélgetni, vagy a közelgő, vagy elmúlt eseményekről stb. Egy ilyen beszélgetés hatására az áldozat jobban elfogadja a másik felet, barátságosabb lesz a támadó, majdnem ismerősként fogja kezelni. De mindenképp közelebb érzni magát a támadóhoz

Kíváncsiság

Ugyancsak egy nagyon alávető, és erős emberi tulajdonság, mivel mindenkiben lakik valamiféle kíváncsiság. Az ember még akkor is megőrzi a kíváncsiságát, mikor már kezd gyanakodni, hogy valami nincs teljesen rendben. Például annak ellenére is rákattinthat egy felettébb érdekes dolgot ígérő linkre a munkavállaló, ha már gyanakszik az e-mail tartalmát megbízhatóságát illetően. A kíváncsiságot leginkább számítógép alapú támadásoknál lehet jól kihasználni, ha például valamilyen kártékony kódot akarunk a rendszerbe juttatni.

Befolyásolhatóság

A támadó befolyást szeretne szerezi a kiszemelt személy felett, el szeretné érni, hogy elvégezze, azt, amit szeretne. Itt lényeges szempont az idő, mivel mindenki befolyásolható, de nem mindenki egyformán, van, akire több időt kell szánni a támadónak. A befolyásolás működhet meggyőzéssel, megvesztegetéssel, megfélemlítéssel is.

Lényeges, hogy a felhasználok egy része, úgy szereti végezni a munkáját, hogy mindig megmondja neki valaki, hogy mit csináljon ezek az emberek könnyebben befolyásolhatóak. Hogy melyik kolléga ilyen, azt egy profi social engineer támadó ki tudja deríteni akár egy felszínes beszélgetéssel, vagy figyelve a kollégát beszélgetését, elcsíphet olyan mondatokat, hogy kiderül valakiről, hogy könnyen irányítható. Az is embertől függ, hogy hogyan lehet befolyásolni: van, akire hatalmi szóval lehet hatni, fenyegetéssel, zsarolással, megvesztegetéssel, de van, akit nem ennyire nyíltan, hanem a bizalmába férkőzve, egyéltalán nem kemény hangnemben inkább barátságos szavakkal lehet győzködni.

Lustaság

A lustaságból adódóan a munkavállaló nem jár után annak a dolognak, amit tapasztal, még annak ellenére sem, hogy esetleg gyanús lehet, De a lustaság miatt előfordulhat, hogy az adott kollégának nincs kedve dolgozni, ezért inkább az kapott feladatot továbbadja egy másik kollégának. A kolléga, akinek a feladat jut, persze nem fog gyanakodni, nem fog sokkal több idő tölteni a feladat megbízhatóságának ellenőrzésére, hiszen egy ismert kollegájától kapta azt.

Hanyagság

A hanyag kolléga ismeri a munkahelyi szabályokat, de nem foglalkozik vele. Ha szabályellenességet tapasztal, egyszerűen megvonja a vállát. Például beengedhet egy idegent is egy beléptetőrendszerrel ellátott épületbe, ha az idegen azt mondja, hogy a kártyáját otthon hagyta, de amúgy ott dolgozik. Holott ez egyértelműen tiltott a vállalati szabályzat értelmében.

Túlzott közösségi média használat

A közösségi média az egyik forrása az támadó általi információgyűjtésnek. Aki nagy rajongója a közösségioldalaknak, nagyon sok információt oszt meg magáról, ami első ránézésre lényegtelen lehet, de egy támadó nagyon jó profilt alkothat a kiszemelt áldozatról.

Munkahelyi szituációk

Új munkatárs

A támadók egyik kedvelt kiszemelt célszemélye az új munkatárs. Új munkatársat nem túl nehéz találni, csak meg kell nézni, milyen pozíciókat hirdettek az adott cégnél, majd célirányosan az adott irodát, vagy beosztással rendelkező munkatársat keresni. Az új munkatársak kevésbé vannak tisztában az új munkahelyükön lévő szokásokkal. Ez annak ellenére lehet, hogy a munkáltató biztos, hogy a lehető legjobban felkészíti a vállalati rendről szabályozásról, de még nincs kialakult rutinja. Nem ismeri a régi kollégákat, egy támadó a telefon másik végénkönnyen elhitetni vele, hogy ő is egy régi, ott dolgozó kolléga.

Az új kolléga még bizonyítani akar, jó benyomást akar kelteni a kollégákban, nem akarja, hogy már az elején akadékoskodónak, nehéz esetnek tartanák, ezért, ha egy kérés érkezik felé, kevés eséllyel fogja visszautasítani, hiszen meg akar felelni. Nem ismeri az embereket, megoszthat érzékeny információkat olyanokkal, akivel nem szabadna. Ezen helyzeten úgy lehet javítani, hogy az új kollégákat biztonságtudatossági oktatásban kell részesíteni, és bátorítani kell őket, hogy kérdezzenek.

Persze az is előfordul, hogy maga a támadó adja ki magát új kollégának, mert az irodaházban mozogva még hihető is, hogy az új kolléga nem ismeri ki magát mindenhol. Erre hivatkozva aztán lehet kérni belépést az épületbe, irodába, mondván, hogy a belépőkártyát „otthon felejtette", vagy mielőbb belépést kér a számtógépre a vezetőtől, vagy az informatikai osztálytól, hogy minél előbb dolgozhasson.

Napi rutinmunka

Sokat végzünk ismétlődő napi rutin munkát, viszont van olyan munkakör, ahol ez fokozottabban jelentkezik, ugyanazt, vagy hasonló a kérést kell nap mint nap teljesíti. Még ha nem is gondolnánk, de ezeket a kollégákat is át lehet verni, ha mint támadó, olyan munkát adunk neki, ami illeszkedik a mindennapi feladtok közé. Ez nem fog feltűnni az áldozatnak, hiszen minden ugyanúgy történik.

Sajnos kevésbé lehet elvárni ezektől az alkalmazottaktól, hogy utána nézzenek a esetleges sok egyforma kérésnek, utasítsanak, főleg ha leterheltek. Persze egy tudatosabb, vagy tapasztaltabb kolléga, megnézi alaposabban a kérést, amit kapott, és utána jár, ha valami kicsit is gyanús. De egy új kollegának nem biztos, hogy feltűnik, ha szokatlan kérés érkezik hiszemón neki minden új. Az új kollégával ezért alaposan meg kell ismertetni a munkafolyamatokat, a rutin munka során is mire kell figyelnie.

Segítő munkakör, probléma megoldás

Ez a helyzet főleg azokban a beosztásokban lévő kollégákat érinti, aki napi szintem nyújtanak segítséget, és gyakran beszélnek idegenekkel. Alapjaiban mindenkiben meg kell bízni, ez segíti a támadó dolgát

Elégedetlenség

Az elégedetlen kolléga potenciális célszemélye lehet a támadónak. Az elégedetlen kollégát néha könnyű befolyásolni, könnyű meggyőzni, hogy olyan tegyen, ami árt a munkahelyének. Lehet bosszúvágyból, vagy akár kedvtelésből is, vagy csak egyszerűen rosszindulatból.

Megvesztegetés

Ebben az esetben elég az is, ha kisebb ajándékot ad a támadó kiszemelt személynek, vagy akár a kölcsönös segítségnyújtás is ide tartozhat. A támadó olyan helyzetet termet, hogy az áldozatnak szüksége legyen segítségre, vagy egy kisebb ajándékot kap, ha megtesz egy kis apróságot, ami a támadón egyébként fontos.

Zsarolás

A kiszemelt áldozat családi hátterét, magánéletét megvizsgálva (például közösségi oldalon), egy rutinos támadó talál olyan információkat, amivel megzsarolja az áldozatot.

Ajánlott, hogy ne osszunk meg magunkról olyan információkat, ami később kellemetlen lehet ránk nézve, ideértve a munkahelyet, a kollégákat is. Ez főleg igaz a közösségioldalka is.

Bosszú

Megsértődött, a munkáltatóval rossz viszonyban lévő kollégákra jellemző. Ez előfordul akkor, ha valamelyik kollégával közlik, hogy esetleg el lesz küldve a végtől, vagy nem rég ment el. Ezek a kollégát örömmel segítenek, vesznek részt egy támadásban, vagy ők maguk találnak ki valamit, amivel ártanak a cégnek. Ekkor nem is kell feltétlenül a social engineer támadónak lelepleznie magát, kiderülhet, hogy mi a célja, és ebben kér segítséget.

A pillanatnyi állapot

Fáradtság

A fáradtság, illetve a fáradt alkalmazott szinte biztos, hogy figyelmetlen is. Ilyenkor szeretne minélhamarabb túl lenni a feladaton, átsiklik apró, de fontos dolgok felett, ami fontos lehet egy social engineer támadás kivédéséhez.

Kapkodás

A sietség önmagában nem jelent negatív tulajdonságot, mert aki siet, az nem biztos, hogy nem tudatos a munkájában. A probléma azoknál jelentkezik, akik nincsenek hozzászokva ahhoz, hogy siessenek, ekkor előfordulhat egy negatív stresszhelyzet, amit az illető rosszul kezelhet, elkezd kapkodni. Ha hirtelen megnövekszik a munka mennyisége, akkor nem biztos, hogy elég odafigyeléssel tudja végezni elvégezni a munkát.

Figyelmetlenség

A figyelmetlenség és a feledékenység hasonló problémákhoz vezet. Ebben az esetben is igaz, hogy a figyelmetlenség nem egy állandó állapot, a feledékenységet is okozatja fáradság, munkahelyi stressz, magánéleti problémák. Az egyik olyan dolog, amit szeretnek kihasználni a támadók. A figyelmetlen munkavállaló automatikusan cselekszik, átsiklik lényeges dolgok felett, nem gondolkodik. igazából nem figyel arra, ami történik. Ez az egyik olyan tulajdonság, amit nagyon jól kihasználnak a támadók

Túlterheltség

A túlterhelt alkalmazott nem tud mindenre figyelni, ha lehet, átruház másokra feladatokat. Ekkor egy figyelmes támadó a túlterhelt alkalmazottnál, főképp, ha az vezető beosztású, elérheti, hogy a támadó által kívánt feladatot kiossza egy beosztottnak. aki persze végrehajtja, hiszen a vezetőjétől kapta.

Távollét

Egy munkavállaló szabadságát a támadó kétféleképpen tudja kihasználni. Egyrészt áldozat lehet az, aki elment szabadságra. A támadónak előzetesen fel kell mérnie, információkat kell gyűjtenie arról, hogy a célszemély mennyire odaadó a munkahelye iránt. Ha feltételezni lehet, hogy az illető nagyon lelkiismeretes, és odaadó, akkor még a szabadság alatt is hajlandó dolgozni, hogy jó benyomást keltsen a kollégáiban, főnökeiben. Ha esetleg ekkor valaki felhívja, mihamarabb túl akar lenni a feladaton, kiad olyan információkat, amit egyéb esetben nem adna ki, vagy továbbít információt, bizalmasabb anyagot olyannak, akinek nem szabadna, esetleg még szabályzat is tiltja. Nem ellenőrizni annak hitelességét, aki vele kapcsolatba lépett.

Másrészről a támadó kihasználhatja a kialakult helyzetet, és megkörnyékezheti azt a személyt, aki a szabadásgon lévő helyettesíti. Nem biztos, hogy a helyettesítő kollégának minden információ át lett adva, és mindenről tájékoztatva lett. Sőt, ha érkezik valamiféle telefonhívás vagy e-mail ismeretlentől, aki a távol lévő kollégára hivatkozik, még hihető is lehet az, hogy át kell adnia információkat valakinek, hiszen az ismert kollégára hivatkoznak.

Betegszabadság

Hasomló a helyzet a fizetett szabadsághoz, annyiban viszont nagyon eltér, hogy ha az illető hamar betegszik meg, és már reggel nem tud menni dolgozni, akkor nem tudja átadni a feladatait. Kapkodás, káosz alakulhat ki a munkahelyen. Akinek hirtelen a nyakába szakad az munka, ő is szeretne minél hamarabb túl lenni rajta, és nem lesz annyira tudatos, nem fog figyelni a részletekre. Ezen kívül egy betegszabadágon lévő kollégát nem hívnak fel szívesen a kollegát, mindenféle kérés miatt, ezért a támadónak könnyebb a dolga.

Ünnepek

Ünnepek alatt elsősorban a technológiai jellegű támadások működhetnek. Az ilyenkor kiküldött ünnepi üdvözlőüzeneteket, nyereményjátékokra hívó üzeneteket nagyobb arányban nyitják meg a kollégák. Kevésbé tudatosak, kevésbé figyelne arra, hogy esetleg az üdvözlő e-mailben lehet kártékony kód is, hasonlóan ahhoz, mint egyébként más e-mailekben. Fontos, hogy az illető, aki ünnepi smile-kat kap, továbbra is tudatos legyen, továbbra is óvatosan kezelje az e-mailjeit, számítson rá, hogy ünnepek környékén többen akarják átverni ezzel a módszerrel.

Stresszhelyzetben

Előfordul, hogy a social engineering támadás lelepleződik, illetve valaki észrevesz, tudatosul benne egy ilyen jellegű támadás. Ez egyfajta feszültséget, megdöbbenést, stresszt generál az alkalmazottakban, amire többféleképpen reagálhat, a személyiségétől függően. A reakció általában automatikus, az ember nem gondolkodik

az első másodpercekben hosszan, mit is kellene csinálni. Ez a fajta stresszhelyzet a támadónak sem kedvez, viszont ő felkészülhet arra, hogy lebukik, és emiatt könnyebben ki tudja magát hozni a kellemetlen helyzetből. Egy social engineering a támadás leleplezésekor pánikba is eshet a munkavállaló, nem gondolja végig higgadtan a tennivalókat, pont ekkor csinálhat olyan, ami nagyobb kárt okoz a cégnek, esetleg el is durvulhat a szituáció. Elképzelhető, hogy dühöt vált ki az az áldozatból a szituáció, megfenyegeti, megpróbál bosszút állni azon, aki átverte őt

Az áldozatnak a konfliktus elkerülése is egyfajta menekülés lehet a helyzetből, ha leleplez egy támadót, és látta, hogy a támadó mi csinált. Ha a munkavállaló nem akar konfrontálódni senkivel, inkább nem szól, ha látott valamit, vagy arra gondol, hogy amúgy sem tudná bizonyítani az igazát. A felelősség hárítása, illetve megosztása is egy jellemző tulajdonság ilyenkor, az áldozat nem akar felelősséget vállalni azért, amit látott, inkább szól valakinek, hogy inkább ő intézkedjen. Jellemzően egy főnöknek adjuk a feladatot, hogy intézkedjen, ha van rá lehetőségünk.

Egy social engineering jellegű támadás lehet akár fenyegető jellegű is, ami aztán félelmet generál a munkavállalóban. A támadó ráveszi az áldozatot, hogy csináljon meg valamit, akkor is, ha az áldozatnak azzal szemben kételyei vannak. A félelem is a támadónak kedvez, mert arra ösztönzi az embert, hogy elkerülje a kellemetlen helyzetet, minél előbb túl legyen rajt. Például kaphat a munkavállaló fenyegető levelet, amelyben valami nagyon rossz dolgot helyeznek kilátásba, ha nem tesz meg valamit. A negatív dologra, félelemre épülő támadás, ha előtte jól elő van készítve, nagyon hatásos tud lenni.

De ha kiderül egy oldalról, hogy adathalász oldal, és sikerült is átverni valakit, az illető dühből megpróbálhatja vizsgálgatni, hackelni (ha kicsit ért hozzá) az oldalt. Sokkal jobb az, ha egyből értesítve vannak az illetékesek, akik jelzik az alkalmazottaknalgozóknak, hogy az adott oldal egyfajta adathalász oldal. Ilyenkor meg lehet akadályozni, hogy mások is áldozatául essenek. De az ellenkezőjét is kiválthatja egy ilyen átverés lelepleződése, az áldozat magába fordulhat, szomorú, elkeseredett lesz. Ez a véglet sem jó.

11.2 Milyen módszert használ a támadó?

Szoros követés

Ebben az esetben a támadó kiszemelt valakit az alkalmazottak közül, akiről feltételezi, hogy segítőkész lesz vele, és még az épületbe való belépés előtt csatlakozik hozzá - tipikusan a reggeli időszakban – majd megpróbája átverni, mintha ő is egy új kolléga lenne. Ráveszi a régi alkalmazottat, hogy a saját belépőkártyájával engedje be az épültbe. Ezt a típusú támadást a beléptetőrendszer megfelelő kezelésével és beállításával lehet kivédeni, naplózással, egyirányú átengedéssel, vendégkártyák

használatával (megoldható az is, hogy a látogatói kártya nem ér semmit dolgozói kártya nélkül).

Besurranás

Ajtóknál, kapuknál jól használható módszer, hogy a támadó egy csoporthoz csatlakozik, akik éppen most mennek be az épültbe. Ez lehet látogató csoport, munkások, akik épp karbantartást végeznek, vagy az is előfordul, hogy az alkalmazottak egy csoportja épp visszajött ebédszünetből, és hozzájuk verődik. Látogató csoportot azért könnyű kihasználni, mert általában nem ismerik egymást. Ha pedig ebédszünetről jön vissza egy csoport, akkor általában egy kártyát használnak, ez ember nyitja a beléptetőt, és mindenki azzal lép be.

Másik gyakran alkalmazott módszer, ezt filmekben is gyakran láthatjuk a támadók részéről, hogy megvárja, amíg egy alkalmazott belép a beléptetőrendszerrel ellátott ajtón, és mielőtt az ajtó becsukódna, megfogja azt. Az alkalmazottak dolgozók általában megszokásból cselekednek ilyenkor. Nagyon kevés olyan alkalmazott van, aki maga mögé néz, hogy van-e ott valaki, vagy hogy tényleg becsukódott-e az ajtó mögötte.

Besurranás ellen is az a legjobb módszer, ha ismerjük ezt a technikát, ha hasonlót veszünk észre, meg kell kérdezni az illetőt, hogy kihez jött. Műszaki megoldások is léteznek a besurranás ellen, számos beleptető rendszer el vannak látva személyérzékelővel, ami érzékeli, ha többen lépnek be a helyiségbe egy kártyával. Ezen kívül el vannak fel vannak szerelve átbújás érzékelővel és átmászás elleni súlyérzékelővel.

Rápillantás

A rápillantás módszer akkor működik, mikor valakinek a titkos kódját akarják ellopni. Ez lehet egy beléptető rendszer PIN kódja, bankkártya PIN kódja, telefon nyitókódja, ajtó kód, de akár egy számítógépen használt jelszó, vagy alkalmazás jelszava. Egy beléptető rendszerrel ellátott ajtón ál a kódot beütve általában nem takarjuk el, Nagyon könnyen látható ez mások által, ezt használja ki a rosszindulatú, vagy kíváncsi támadó. Ha a táamdó hátunk mögött, kicsit oldalt áll, és figyeli a kezünk mozdulatát, nagyon könnyen rájöhet, hogy milyen jelszó használunk, Ez például fokozottan igaz a lépcsőházak kóddal ellátott ajtóira, amit tényleg messzebbről is lehet látni, akár a szembe lévő lépcsőházból is. Hasonlóan könnyű valakinek a használt jelszavát így ellopni, mikor éppen begépeli, hogy belépjen valamilyen rendszerbe, elég csak mellette állni, és akár a válla felett figyelni, hogy mit gépel be milyen billentyűket üt le. Innen ered az angol elnevezése ennek a típusú támadásnak: vállszörf (shoulder surfing)

Megszemélyesítés, megtévesztés

Megszemélyesítéses támadás esetén egy konkrét munkavállaló, vagy külsős bőrébe bújnak, illetve intéznek ügyeket, ezzel tévesztve meg a kiszemelt áldozatot. Ehhez persze alapos felkésülés kell, ismerni kell valamennyire a kiszelet személyt. Egyik cél, hogy a támadó bejusson épületbe, az épületen belül eltulajdonítson munkaeszközöket, telefont, laptopot, információkat szerezzen (ez lehet papír alapú is). De egy támadó be is juttathat ennek segítségével kém eszközöket, lehallgató berendezéseket, keloggert. Megszemélyesítéses támadást végre lehet hajtani telefonon, telefonhíváson keresztül is, mi talán sokkal könnyebb, mert a támadó nem találkozik a kiszemelt áldozattal.

Megtévesztés nagyon hasonlít a megszemélyesítésre, abban különbözik, hogy ebben az esetben egy nem valós, fiktív személynek adja ki magát a támadó. Ekkor is fontos felkészülés, tudnia kell a támadóak, hogy a vállalathoz való bejutáshoz milyen reális (vagy annak tűnő) információkat fogadnak el. Ha például épp állást hirdet a vállalat, akkor a támadó magát jelentkezőnek kiadva, viszonylag könnyen bejuthat az épületbe. De ilyen lehet az, ha a vállalat gyakornokokat, vagy tanulókat alkalmaz. Szinte biztos, hogy a portás nem kérdez meg mindenkit a látogatása okáról.

Kéretlen levelek

A kéretlen levelek egyrészt kellemetlenséget okoz, lassítja a munkát, eltereli a figyelmet, sok időt elrabolt. Social engineering szempontjából pedig fontos, hogy a levélben található hamis oldalra vezető linkeken keresztül adatokat lopnak a felhasználótól. Egy személyre szóló, jól megfogalmazott levélben könnyen elrejthető kártékony kód. A levélszemét szűrőket is folyamatosan fejlesztik, de meg lehet úgy fogalmazni egy levelet, hogy az átmenjen a szűrőn, és egy kevésbé tudatos felhasználó bedőljön neki, és az esetlegesen felkínált linkre rákattintson.

Lánclevelek

A lánclevelek (hoax) hasonlóak a kéretlen levelekhez, célja egyrészt a reklám, másrészt az e-mail címek összegyűjtése, ugyanis a felhasználók előszeretettel továbbítják őket a többi kollégának. A lánclevelek jellemzően a kollégák küldik egymásnak, ismerősöknek, így az megbízhatónak tűnik. Információbiztonság szempontjából azért veszélyes, mert tartalmazhat olyan információkat, utalásokat, hogy az felhasználó mit és honnan töltsön le. Tipikus példa, amikor vírusírtó letöltésének ajánlása jelenik meg a levélben, egy link, ahonnan le lehet tölteni valamilyen programot, persze megbízhatatlan forrásból.

Adathalászat

Az adathalászat egyik fajtája a *Phishing*. Mostanában az e-mailt használó felhasználók ezzel találkoznak a leggyakrabban, és az a tapasztalat, hogy ezeket már ismerik, ezzel sok esetben már nem lehet átverni a őket. Leggyakrabban banki oldalakat másolnak le

a támadók, hogy jelszavakat, bankkártya adatokat lopjanak. De gyakori az, hogy online játékok, vagy közösségi média oldalát másolják adathalászat céljából, de bármelyik szervezet vagy oldal lehet célpont.

Az egyik legnagyobb probléma információbiztonság szempontjából, ha a vállalat weboldalát, vagy belső, intrawebes oldallát másolják a támadók. Ezek az oldalak a céltól függően jelszó megadásával látogathatóak, illetve olyan tartalmak vannak fenn, amihez meg kel adni a jelszót is, vagy lehetőség van arra, hogy jelszót változtassunk. Az alkalmazott sok esetben nem arra számít, hogy a vállalat oldalát másolják le, adathalászat alatt inkább bankokkal kapcsolatos oldalakra asszociálnak. A vállalt szempontjából fontos, hogy megismertesse az alkalmazottakkal a vállalat weblapjait, és információs portáljait, intraweb oldalát, és tudatosítsa bennük, mire kell figyelni, milyen gyanús jelekre, mikor ezeket az oldalkát látogatják.

Másik adathalászat fajta a *Vishing*, ez telefonon vagy chaten keresztül zajlik. Az áldozatot gép hang hívja fel, és az mondja el, hogy mit kell csinálnia az áldozatnak. Ez jelszó változtatásra, vagy egyéb bizalmas adat megadására buzdít. Mivel ez gépi hang, és hasonlít a bankok által használt ügyfélszolgálati megoldásra, bizalmas ébreszt az áldozatban. Ugyanaz működhet chaten keresztül is, üzenetküldő alkalmazásokon keresztül. ehhez hasonló a *Smishing* típusú támadás is, amkor hivatalosnak tűnő SMS-t küldenek adott telefonszámra, ami tartalmazza, hogy mit is kellene csinálni az érinttet személynek, hogy hol, milyen adatot kell megadnia.

továbbá egyik fajtása az adtahalászatnak a *Whaling*, ezeknek kimondottan célpontja a vállalat vezetése, felsővezetése, titkársága. Ez elsősorban nagyvállalatoknál, működik, ahol az támadó azt feltételezi, - ok esetben joggal – hogy a titkárságnak küldött levelet a titkárság automatikusan továbbítja a munkavállalók részére. Ebben az esetben a munkavállaló hitelesnek gondolja a levelet, illetve az abban foglal utasításokat, hiszen az a vezetéstől kapta. Nagy eséllyel végre is hajtja, akkor is, ha ott például egy érzékeny adat továbbítására irányuló utasítása van.

Másik fajtája az adathalászatnak a *Pharming*, ahol a támadó a böngészők sérülékenységeit használja ki, gyorsítótárat módosít, így juttatja az áldozatot hamis oldalra.

Kártékony kódok terjesztése

Kártékony kód terjesztésével sok formában találkozhatunk: e-mailben, chaten kaphatunk, közösségi médián, vagy valamiféle adathordozón keresztül is érkezhet hozzánk. Manapság a legyakoribb a fertőzött fájl (pl. PDF), vagy Excel makrós állomány.

E-mailben történő ártalmas kód terjesztésesre sok lehetőség van, itt lényeges szempont a levél szövegezése. Ha reklámként (figyelemfelkeltő levél) küldenek valamit a

kiszelet cégnek, illetve a munkavállalóknak, a spam szűrő a szövegezés, vagy a túl sok, nem megbízható lineket miatt kiszűrheti.

A támadó tud szimulálni eltévedt levelet is. Eljátsza, mintha az egyik kolléga rossz címére küldte volna a bizalmas dokumentumot tartalmazó levelet. Ez egy konkrét személyre szabottan szokták végrehajtani. Mivel érdekes adat lehet a csatolmányban (például fizetési lista excelben), a kiszemelt személy szinte biztos, hogy megnyitja (és futtatja a vírust).

Az előbbi egyik változata, mikor a szabadságon lévő kolléga nevében küld egy hamis linket tartalmazó levele a támadó. Ekkor elég csalogató lehet az, ha a nyaralási képeket nézhetünk meg, csak egy a levélben található linkre kell kattintani. Ez utóbbi átverés manapság kevés jelentőséggel bír, mivel a felhasználók a közösségi oldalakra költik fel a képeiket.

A csali

Angolul *Baiting* néven találkozhatunk vele. Ez olyan különleges módszer, amikor a szándékosan helyez el a támadó adathordozókat a vállalaton belül mosdóban, konyhában, tárgyalóban, nyomtató mellett, lényegében bármilyen helyszín sóba jöhet. A kíváncsi alkalmazott persze bedugja a megtalált eszközt, ami lehet egy pendrive, a számítógépbe, és ha itt talált egy érdekes nevű programot, szinte biztos, hogy elindítja. Egy „véletlenül” otthagyott pendrive a vezető irodájában különösen veszélyes lehet, mert az ő gépén nagyon valószínű, hogy található bizalmas adat.

Ahhoz, hogy valaki a vállalatból egy adathordozót csatlakoztasson a számítógépéhez, nem feltétlenül kell az előbbi módszert használni, lehet közvetlenül a vállalathoz beküldeni adathordozót, mint ajándékot. Ez a fajta ártalmas kód terjesztés főleg ünnepek táján lehet hatékony. Egy ajándékként kapott eszközt az alkalmazott szívesen kezd használni, nem nagyon fog gyanakodni. Reprezentációs ajándékokkal hasonló a helyzet, ha a támadó tudja, hogy az adott cég kikkel áll partneri kapcsolatban, és az ő nevükben küld ajándékot. Ebben esetben például, ha egy ajándék pendrive-ot, vagy CD-t kap a dolgozó, nem gyanakszik, amikor a kezébe veszi, hogy ez esetleg veszélyt jelenthet. Nagyobb vállalatoknál, ahol nagy a dolgozói létszám, nem tudja mindenki pontosan, hogy kik is a partnercégek. Ekkor egy kitalált vállalkozás nevében is lehet küldeni ajándék adathordozót, nem fog feltűnni senkinek először, hogy nincs ilyen nevű cég [16].