NETWORK OF USER-RELATED HUMAN RISK FACTORS IN INFORMATION SECURITY

AZ INFORMÁCIÓBIZTONSÁG FELHASZNÁLÓI OLDALI HUMÁN KOCKÁZATI TÉNYEZŐINEK HÁLÓZATA

KÁRÁSZ Balázs[1]

Abstract

Critical and weak points of developing information security awareness can be mapped by conducting a process-based analysis of particular human risk factors in-fluencing information security as well as the common effect of the coherence of re-lations between these factors. This paper aims to delineate the network of human risk factors related to information security considered on the users' behalf, on both employee and leadership levels, with the help of creating suitable clusters. In the knowledge of all above, learning and other professional service conceptions can be set up and tailored to the organization, the effectiveness of which depends to that of information security purposes. In practice, with the help of such conceptions, in-formation security can be improved in the organization, the effectuation of which has its roots in the command function of leadership.

Supported by the ÚNKP-19-3-I-NKE-14 New National Excellence Program of the Ministry for Innovation and Technology.

Keywords

information security, network of human risk factors, organizational learning concepts, security awareness

Absztrakt

Az egyes, az információbiztonságot befolyásoló humán tényezők, valamint a közöttük fennálló összefüggések együttes hatásának folyamatalapú elemzésével feltérképezhetők az információbiztonság-tudatosság kialakításának és fejlesztésének kritikus és gyenge pontjai. Jelen közlemény célja, hogy a megfelelő klaszterek kialakítása segítségével felvázolja a felhasználói oldalon, beosztotti és vezetői szinten kockázati hatással bíró humán tényezők információbiztonsági vonatkozású hálózatát. Ennek ismeretében testre szabott képzési és egyéb szakmai szolgáltatási koncepciók állíthatók fel, amelyek hatékonysága szervesen kapcsolódik az információbiztonsági törekvések hatékonyságához. A gyakorlatban segítségükkel fejleszthető az információbiztonság-tudatosság a szervezetben, melynek megvalósulása a vezetés irányítási funkciójában gyökerezik.

Az Innovációs és Technológiai Minisztérium ÚNKP-19-3-I-NKE-14 kódszámú Új Nemzeti Kiválóság Programjának szakmai támogatásával készült.

Kulcsszavak

információbiztonság, humán kockázati tényezők hálózata, szervezeti képzési koncepciók, biztonságtudatosság

[1] karaszb@gmail.com | ORCID: 0000-0003-2065-4928 | PhD hallgató / PhD Student | National University of Public Science Doctoral School of Military Engineering / Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola

BEVEZETÉS

Napjaink vállalati, szervezeti tudása az adatokon és az információkon alapul, amelyek elemző, feldolgozó, továbbító, tároló stb. rendszerek összességében összpontosulnak. Adatbányászati megközelítése szerint az adatelemzés az adatok értékelésének, azaz ellenőrzésének, letisztításának, átalakításának és modellezésének folyamatát jelenti, amely hasznos információ feltárásán, következtetések levonásán keresztül az analitikus, logikus érveléshez, döntéstámogatáshoz szükséges. Az adatelemző rendszerek védelme komplex módon értelmezendő, mivel civil és katonai szervezetek, így köztük kritikus infrastruktúrát fenntartó és üzemeltető vállalatok szervezeti egységei számára az információbiztonság műszaki megközelítése elképzelhetetlen a humán tényezők vizsgálata nélkül.

A humán tényezők jelentős része (pl. emberi teljesítmény, munkavállalói attitűd, biztonságtudatosság, vezetés minősége, vezetői példamutatás stb.) alapvető hatást gyakorolhat a komplex informatikai rendszerek megbízhatósági és biztonsági szintjére. A hibrid hadviselés elterjedésével a social engineering növekvő szerepe is befolyással bír a szervezeti információbiztonsági folyamatokra, ezért elengedhetetlen a kibertámadási pontok azonosítása, a kockázatok kezelése.

Tudományos probléma és kutatási célkitűzés

A fentiekből következően felmerül az a komplex kérdés, hogy milyen mértékben, ill. egymáshoz viszonyítva milyen arányban járulhatnak hozzá az információbiztonság-tudatosság fejlesztéséhez a civil szférában alkalmazott menedzsment módszerek – az egyes social engineering és egyéb típusú támadások befolyásoló hatása részleteinek fényében.

Jelen közlemény a probléma tágabb vizsgálatához kíván részkutatási eredményeket nyújtani, amelynek hipotézise, hogy az információbiztonság-tudatosság fejlesztésének hatékonysága a vezetés irányítási funkciójában gyökerezik. A közlemény célja, hogy az elmetérkép módszerének segítségével felrajzolja azon humán tényezők hálózatát, amelyek vezetői és beosztotti szinten kockázati hatással bírnak az információbiztonság-tudatosságra a szervezetben. E hálózat ismeretében bármely szervezet képes lehet olyan képzési és egyéb szakmai szolgáltatási koncepciókat felállítani, amelyek segítségével fejleszthető a szervezeti biztonságtudatosság.

HUMÁN TÉNYEZŐK AZ INFORMÁCIÓBIZTONSÁGBAN

A humán tényezők szerepét az információbiztonság holisztikus értelmezésében több szakirodalom feldolgozta, melyek közül Cains és társai közleménye [1] megfogalmazta, hogy az emberi viselkedés több irányból befolyásolja a biztonságot: ezért fontos annak megértése a felhasználói, a védelmi és a támadói oldalról egyaránt. Kiemelve a bizalom kérdéskörét, a szerzők kifejtik, hogy a bizalom kéttényezős, az egyén részeként megnyilvánuló inherens tulajdonságok, valamint az egyénen kívülről érkező, ún. szituációs tulajdonságok alkotják. Alapvető befolyással bír továbbá a kockázattudatosság és a kockázatok kezelésével kapcsolatos attitűd alakításában.

Jelen közlemény fenti kategóriák közül kizárólag a felhasználói oldal (egyúttal a három közül a legszélesebb kör) részletesebb tárgyalására szorítkozik, kiemelve ugyanakkor a felhasználói viselkedésnek a támadói oldal jelentette fenyegetésekkel szemben megmutatkozó tulajdonságait.

Az emberi viselkedés sebezhetőségből fakadó kiszámíthatatlan természete mögött egy komplex, személyközi, meghatározott csoport viszonylatában értelmezhető interakciókhalmaz áll, mely Oroszi [2] és Kollár [3] gyűjtését kiegészítve a következő klasszifikáció mentén számba vehető emberi tulajdonságokban érhető tetten:

- Hanyagság
- Kihasználható emberi tulajdonságok
- Vezetői viselkedés és interakciók
- Tudatosság hiánya

Az alábbi felsorolásban részletesebb áttekintést kívánok nyújtani a fenti kategóriákba sorolható egyes felhasználói oldalon jelentőséggel bíró emberi tulajdonságokról. Amelyek esetében elérhető, információbiztonsági vonatkozású példák segítségével szemléltetem a mindennapi vállalati gyakorlatban előforduló eseteket. A felsorolás és a jellemzések továbbá a beosztotti és vezetői szint összehasonlító elemzésének alapját képezik.

Hanyagság

1. Figyelmetlenség: tetten érhető a hardvereszközök, helyiségek őrizetlenül hagyásában, fizikai biztonsági előírások nem tudatos megkerülésében.
2. Feledékenység: hatása megmutatkozik pl. a jelszókezelési kultúrában.
3. Kényelem: leggyakrabban biztonsági előírások megkerülésével érhető el.
4. Konfliktuskerülés: adatvédelmi előírások betartására való felszólítás tudatos elmulasztása más érdekek előbbre helyezése miatt.
5. Munka-magánélet nem megfelelő elválasztása: megnyilvánul a saját és vállalati eszközök és az azokon tárolt információk kezelésekor.
6. Közönyösség: „tudatos figyelmetlenség”, biztonsági szabályok hiányos vagy elhanyagolt figyelembevétele.

Kihasználható emberi tulajdonságok

1. Segítőkészség: a támadó tudatlanul, de készségesen történő segítése a jogosulatlan információszerzés végrehajtásában.
2. Befolyásolhatóság: a támadó manipulációjának való áldozatul esés, jogosulatlan módon történő információszerzésének segítése.
3. Bosszúállás, félelem: megtestesülhet meggondolatlanságból, számításból fakadó tudatos cselekvésben, pl. dezinformálásban.
4. Kíváncsiság, nyitottság, érdeklődés: információk kezelése a megfelelő jogosultsági körökön túl, szivárogtatás, egyes információk félremagyarázása.
5. (Lét)bizonytalanság: a támadó zsarolásának áldozatául esés, a szabályok beszűkült tudatállapotban történő áthágása, akár radikalizáció útján a kiberterrorizmusba történő bevonódás, kompromittálhatóság.
6. Leterheltség, fáradtság, monotonitás, stressz: elsődlegesen a hanyagság csoportjába tartozó tényezők előidézése.
7. Viszonzási igény: mind szívességtevés, mind szakmai segítségnyújtás esetében előforduló, kimondott vagy meg nem fogalmazott igény.

Vezetői pozíció sajátosságaiból adódó tulajdonságok

1. Tekintélyelvűség - felsőbbrendűségi érzés: megnyilvánulhat a vezetői utasítás, iránymutatás megkérdőjelezhetetlenségének kommunikációjában.
2. Felelősségvállalás és annak hiánya: információbiztonsági erőfeszítések finanszírozásáról szóló döntéshozatal és következményeinek vállalása, kommunikációja.
3. Előítéletesség: hiányos ismereten alapuló vagy megalapozatlan, túlnyomórészt befolyáson és személyes elgondolás vagy meggyőződés által befolyásolt döntéshozatal.

Tudatosság hiánya

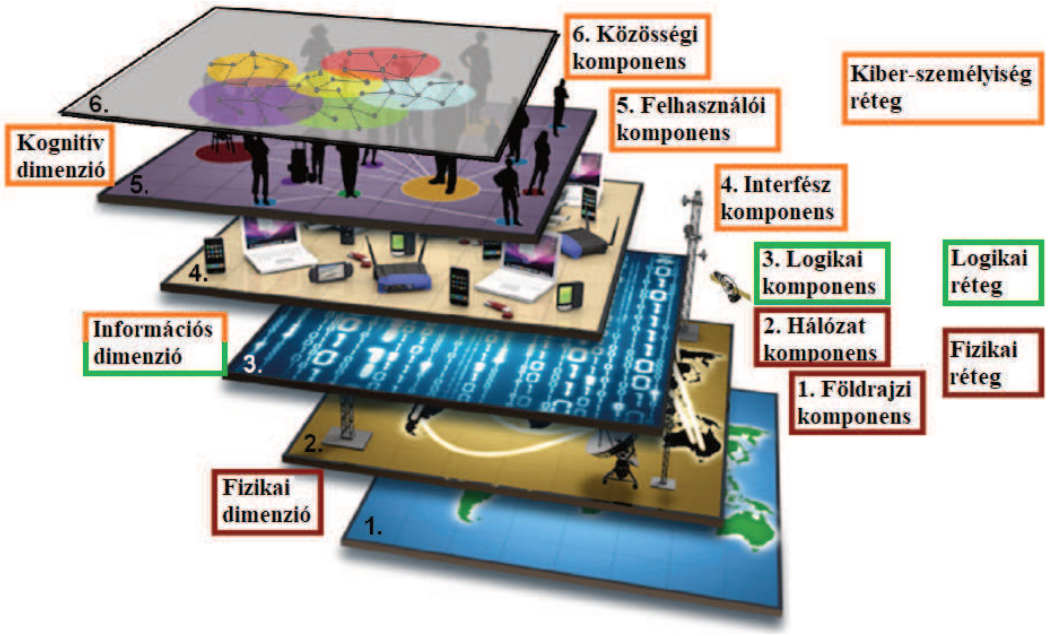
1. Tudatlanság (ismerethiány): hiányos/rendszertelen információbiztonsági képzés, illetve az azon való részvétel nem kielégítő előmozdításának eredménye lehet – mind a szervezetekben, mind iskolai keretek között.
2. Szakképzetlenség: saját szakterülethez, valamint a magánélethez kapcsolódó informatikai és információbiztonsági ismeretek nem megfelelő elsajátítása.
3. Hiszékenység (naivság, jóhiszeműség): a racionalitás és a biztonsági szabályok fényében történő józan ítélőképesség háttérbe szorulása.

A HOZZÁFÉRÉS, JOGOSULTSÁG SZEREPE

Bármely szervezet informatikai rendszereiben az egyes funkciókhoz, területekhez, fájlmappákhoz, programokhoz való jogosultságok szigorú rendszerben kerülnek hozzárendelésre a felhasználókhoz. Az ún. jogosultságkezelés ennek megfelelően dokumentált módon történik, az egyes felhasználók a szervezete által kezelt és tárolt adatokhoz és rendszerekhez kizárólag az ahhoz hozzáférési jogosultsággal férhetnek hozzá meghatározott ideig, illetve módon (írás-olvasás, csak olvasás, csak írás, törlés). Alapelvként kerül megfogalmazásra számos szervezet vonatkozó szabályozó dokumentumaiban (a szabványok ajánlásainak megfelelően), hogy minden felhasználó csak a számára szükséges és elégséges jogosultságokkal rendelkezzen (pl. az indokolatlan többletjogosultságok visszavonandók).

A jogosultságkezelés szigorának fontossága nem csupán a szabályozottság, a felelősségre vonás szempontjából jelentő visszakövethetőség, hanem az információbiztonság megvalósulása miatt is kiemelkedő. Bármely támadás a kibertér virtuális dimenziójában addig terjedhet ugyanis, ameddig a megtámadott felhasználó és ezáltal az ahhoz rendelt, már megváltozott irányítású jogosultsági kör terjed. Ennek megfelelően az adminisztrátor (vagy magasabb) szintje magasabb biztonsági kockázatú, így magasabb védelmi szintet követel meg – a technikai és a humán kockázati tényezők oldaláról egyaránt.

A jogosultság ellenőrzésére is szolgálnak az autentikációs vagy azonosítási megoldások, melyek biztonsági és a technikai oldalról megvalósuló megbízhatósági problémái mentén társadalmilag is jelentős, de fontos jogi vonatkozású kérdések is megfogalmazhatók [4]. Az 1. ábrán látható információs környezeti dimenziók és a párhuzamos értelmezés szerinti kibertéri rétegek felépítéséből kiindulva megállapítható, hogy az egyes rétegek és komponenseik jól körülhatárolható funkciói és önálló voltuk ellenére számos módon kapcsolódnak egymáshoz. Az autentikáció közvetítő szerepet tölt be annak értelmezésében, hogyan épülnek egymásra a kibertéri rétegek.



1. ábra Az információs környezet dimenziói és a kibertéri rétegek komponensei (saját szerkesztés [5] alapján)

Az autentikációs megoldások használata annak ellenére nem korlátozódik a kiberszemélyiség rétegre, hogy gyökereik a felhasználói komponensben találhatók (egyedi felhasználói, IP és e-mail címek stb.), továbbá elsődleges funkciójuk, hogy kapcsolatot teremtsenek az interfész és a felhasználók között, segítve a felhasználókat közösségi hálózatok kialakításában. Sokkal inkább meghatározó kapcsolódás szerepét tölti be az azonosítás a logikai réteg felé (amelybe a következő elemek sorolhatók: információ, átviteli protokollok, szoftveres alkalmazások, felhasználói adatok, internetes tartománynevek), sőt a fizikai réteg felé is (ennek néhány releváns eleme: szerverek, rádiófrekvencia-továbbító eszközök, elektromágneses spektrum).

SOCIAL ENGINEERING

Az ún. social engineering (más kifejezéssel pszichológiai manipuláció) minden olyan technikát magába foglal, amelyik révén az emberi természet, lélek, társas- és csoportkapcsolatok és azok dinamikája ismeretében, a személyközi, illetve csoporton belüli interakciók felhasználásával a manipulátor kijátssza az embereket, feltöri és megfertőzheti az alapszintű védelemmel ellátott informatikai rendszereket (bizalmas adatokhoz, adatbázisokhoz fér hozzá). Mitnick biztonságtechnikai tanácsadó könyvében [6], mely szemléletesen mutatja be e technikák mibenlétét, kivitelezésének részleteit, saját korábbi, elkövetőként szerzett tapasztalataiból merít a megtévesztés művészete megfogalmazásához, ami hitelessé, életszerűvé teszi az abban foglaltakat.

Oroszi értekezése [2] alapján egy támadás kivitelezése során leggyakrabban alkalmazott technikák között megkülönböztethetünk humán és számítógép alapú social engineering technikákat az alábbiak szerint:

Humán alapú social engineering technikák

- Segítségkérés
- Segítségnyújtás
- Valamit valamiért
- Megszemélyesítés (fontos/új munkatárs)
- Felhatalmazás
- Reverse social engineering
- Dumpster diving – kukaátvizsgálás
- Shoulder surfing – „váll-szörf”
- Tailgating – szoros követés
- Elejtett, „csali” adathordozó
- Piggybacking
- Helpdesk átverése

Számítógép alapú social engineering technikák

- Ál-weboldalak
- Phishing, vishing, smishing
- Trójai programok
- Keyloggerek
- Man in the middle
- Brute force

A felsorolt technikák többsége ellen foganatosítható védelmi megoldásként a támadás lehetőségének tudatosítása, szigorított beléptetési rend, irodai hulladék szakszerű megsemmisítése, infokommunikációs eszközök, munkavégzési platformok szabályozott használata stb. merülhet fel. Mindez átfogó megközelítésből úgy lehetséges, ha egy szervezet koordinált adatbiztonsági és adatvédelmi stratégiával rendelkezik, amely lehetővé teszi a szabályozásban bekövetkezett változások, sőt fejlesztések szervezeten belüli, illetve tevékenységbe történő átültetését. Az előírások betartására komplex képzés-fejlesztési program megvalósítása nyújthat megoldást, melynek pillérei lépésenként: esettanulmányok és szimulációs helyzetgyakorlatok, elmélet levezetése, alkalmazás, majd akcióterv készítése egyéni és szervezeti szinten. [4]

A Social Engineering szerepe a jogosultságokkal kapcsolatban

A technikai megközelítésű háttértől visszakanyarodva témánk társadalomtudományi aspektusaihoz, számba veendő, hogy nem csupán a szervezeten kívülről érkező támadások jelentenek veszélyforrást az információbiztonságra, hanem a szervezeten belülről is számítani kell rosszindulatú tevékenységre, amelynek tehát az alábbi megvalósulási formái lehetnek:

- a szervezeten kívüli személy vagy számítógép jut be a szervezet belső hálózatába,
- a szervezetbe beépülve fejti ki tevékenységét a támadó,
- a szervezethez tartozó személy válik támadóvá.

A jelszókezelési hiányosságokat pontosan megnevezve és kategóriákba sorolva megtalálhatók a kapcsolódásokat az előző fejezetben leírt emberi tulajdonságokkal:

- jelszavas védelem hiánya, hivatkozások előzetes ellenőrzés nélküli megnyitása,
- alapértelmezett, illetve túl egyszerű jelszavak használata,

- „túl bonyolult” jelszavak nem megfelelő kezelése (pl. felírása cetlire),
- azonos jelszó használata különféle felületeken – akár többszintű autentikáció miatt,
- ritka jelszócsere, jelszó megjegyeztetése böngészővel számítógépen, ill. mobileszközön,
- alapértelmezett ellenőrző kérdés és egyszerű válasz alkalmazása visszaállításhoz,
- jelszótároló alkalmazás nem megfelelő használata („saját” jelszavak tárolása),
- mobileszköz nem megfelelő védelme (pl. feloldása mintával vagy számkóddal),
- fizikai biztonsági előírások (pl. üres íróasztal politika) figyelmen kívül hagyása,
- nem megfelelő hulladékkezelési és iratmegsemmisítési gyakorlat,
- felületesség az előírások elsajátításában és tudatossági képzésen való részvételben.

Nevezett hiányosságok egyenként az emberi alaptulajdonságok közül összefüggésben állnak a hanyagság több tényezőjével, különösen a kényelem, feledékenység, közönyösség és figyelmetlenség tényezőjével. Kevesebb szerep jut, de nem elhanyagolható jelentőséggel bír a jelszóhasználat során a munka-magánélet nem megfelelő szétválasztása és a konfliktuskerülés. Negatívan hat a jelszóhasználati kultúrára továbbá a tudatosság hiánya, azon belül pedig elsődlegesen a naivság, jóhiszeműség tényezője, melynél fogva a felhasználó nem tulajdonít megfelelő mértékű jelentőséget a biztonsági előírások betartása fontosságának.

A VEZETÉS RELEVÁNS FUNKCIÓI

A rendelkezésre álló szakirodalom feltárása és összegzése fényében az alábbi hangsúlyos gondolatok emelendők ki arra vonatkozóan, hogy a Social Engineering-típusú támadások elleni hatékony védekezés fő pillére a tudatosítás, melynek szervezeti keretek között történő előmozdítása a vezetői elkötelezettség és példamutatás függvénye.

Deák közleményében [7] megállapítja, hogy a támadási módszerek ismeretében jelentősen csökkenthető az információ kiszivárgása és illetéktelen felhasználása, egyúttal pedig növelhető az állami szervek működésének stabilitása, a társadalom és a gazdaság részvevőinek biztonsága. E fejlesztési tevékenység során az első lépés a vezetők, majd pedig a beosztottak információbiztonság-tudatosságának fejlesztését és elköteleződésük erősítését kell, hogy célozza, komplex fejlesztési stratégiába ágyazva, de operatív szinten elsősorban a célképzésekbe emelt esettanulmányok, illetve valós környezetbe ágyazott, de mesterséges kibertámadási helyzetek elemzése útján. Ezt annak alapján állapítható meg, hogy alapvető kockázatkezelési módszertan a precedensesetek vizsgálata, trendek, minták azonosítása.

Erre alapozta közleményének fő mondanivalóját Wilson és Hash [8] is, publikációjukban a tudatosság, képzés és oktatás fogalmainak tisztázását követően azt fogalmazzák meg, hogyan tervezhető meg egy biztonságtudatossági tréningprogram. A tervezés főbb kapcsolódó lépései a program személyre szabott tervezése célcsoportok meghatározása útján (ennek elsődleges szempontjai: szervezetben betöltött szerep, hierarchiában elfoglalt szint, fenyegetettség célja szerinti veszélyeztetettség), valamint a belső PR mind személyes, mind csoportos (szervezeti egység szintű) megvalósítása. Ezt egészíti ki iránymutatásuk, hogy a programhoz kapcsolódóan hogyan építhető fel oktatóanyag, majd legfontosabb tényezőként figyelembe veszik a program és az anyag hasznosulását egyfelől az implementáció lehetőségeinek számba vételével, majd az utánkövetés szerepének hangsúlyozásával.

Chestnut értekezésében [9] gondosan felépített, a biztonsági kockázatokat érintő bemutatását követően az elkövetett/előfordult hibák valós hatására helyezi a hangsúlyt. Számos módszertant áttekint és vizsgál annak fényében, hogy milyen adminisztratív és irányítási feladatok vannak közvetlen hatással az emberi tényezőre az információbiztonság szintjének befolyásolása kontextusában. Gazdasági megfontoláson alapuló ajánlásokat tesz a kockázatok csökkentésére, és javaslataiban összességében a visszamérés és ellenőrzés fontosságára helyezi a hangsúlyt.

A vezetői elkötelezettség szerepe

Napjainkban bármely szervezet egyik legfőbb vagyona az adat, ennek jelentős része az általa kezelt személyes adat, amely egyúttal az adott személyé is, akire vonatkozik. A megfelelő adatbiztonsági gyakorlatok és adatvédelmi eljárások kialakítása, és a vonatkozó előírásoknak való folyamatos megfelelés biztosítása azonban a személyes adatot kezelő szervezetet terheli. Az adatvédelem és az információbiztonság megvalósulása érdekében nem elegendő szabályokat életbe léptetni, technológiai kontrollokat kialakítani, naplózni és tesztelni, magának a vállalati kultúrának is ösztönöznie kell a tudatos adatkezelésre vonatkozó gyakorlat kialakítását és alkalmazását.

Ennek egyik alapja a személyzetfejlesztési rendszer hatékony kialakítása és folyamatos fejlesztése, melyet Karoliny és társai kézikönyvének vonatkozó fejezete [10], amely elhelyezi a tréninget a személyzetfejlesztési rendszerben, és a karriervezetésre helyezve a hangsúlyt, a vezetés funkcióit emeli ki mind a tudásmenedzsment, mind pedig a karriertervezés során elsődleges szerepet játszó tényezőkként. Megfogalmazódnak a vezető személyével, vezetőként betöltött szerepével szemben kialakult újszerű követelmények, valamint az ezekre válaszként kínált személyzetfejlesztési rendszer.

Fentieken kívül a témakör feldolgozásával foglalkozik még többek között Hámornik és társa konferenciacikkében [11], amely elsődlegesen a csoportközi interakciók fényében tárgyalja a kiberbiztonság emberi tényezőit, illetve Stewart és társa hosszabb tanulmányában [12] szintén a szervezetben megnyilvánuló humán kockázatok és az információbiztonsági irányítás kapcsolatát vizsgálja. Közös megállapításuk – mellyel a mindennapokban a leginkább szembetűnő módon a tanúsított információbiztonsági vagy egyéb vállalati irányítási rendszert működtető vállalatok szembesülne: az ISO irányítási rendszerekre vonatkozó szabványok egységes szerkezetének első fejezeteként feltüntetve –, hogy a vezetői elkötelezettség kiemelt helyen szerepel minden rendszer hatékony működtetésében.

A vezetői példamutatás szerepe

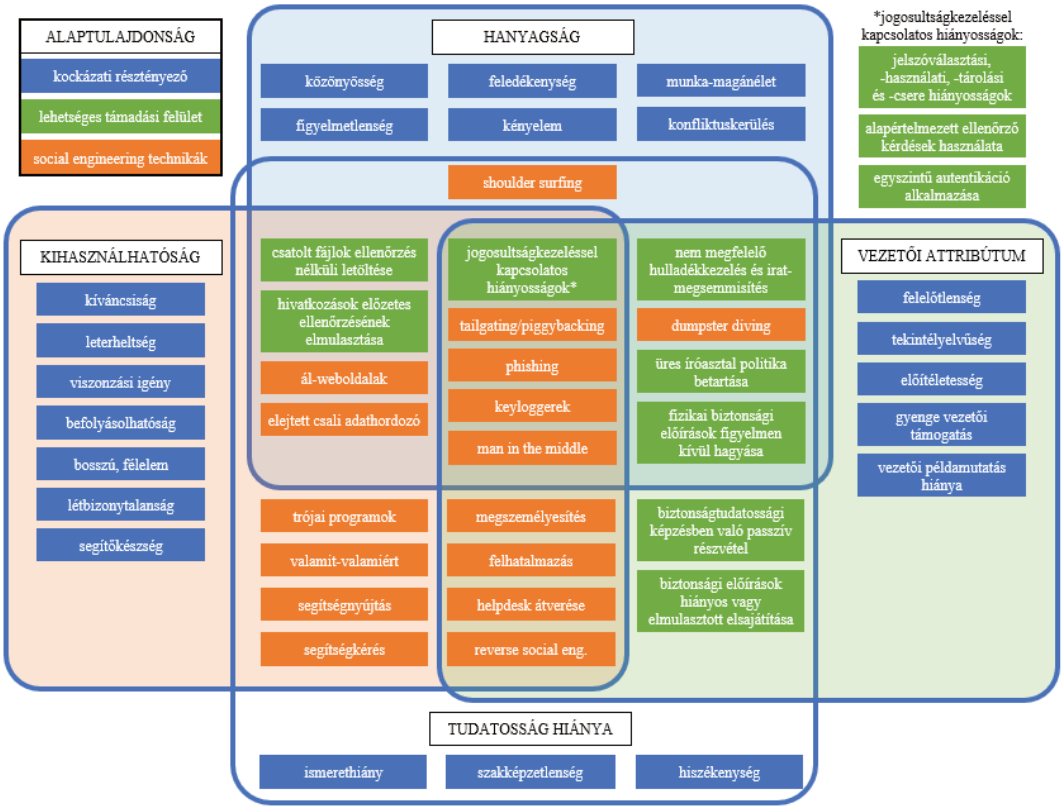
Különösen a vezetői szintekhez kapcsolódó, adott esetben bővebb vagy érzékeny adatokat kezelő tárhelyhez hozzáférést nyújtó jogosultság védelmében fontos a vezetői példamutatás a biztonsági előírások betartásában, azok betartatásának támogatása érdekében. A példamutatás azonban nem értelmezhető önállóan létező vezetői attribútumként vagy készségként, az a főbb vezetői felelősségek maradéktalan vállalásában és megfelelő feladatvégzésben, továbbá azok kommunikációjában teljesedhet ki.

Bármely szervezetben vezetői beosztásban – szintenként eltérő hangsúllyal – a következő területek megfelelő egyensúlyban tartása szükséges a példamutatáshoz: célkitűzés, döntéshozatal, változáskezelés, delegáció, értékelés, irányítás, visszajelzés, problémakezelés (korrekció), konfliktuskezelés, tárgyalás (értekezletvezetés), hierarchikus eligazodás és

kreativitás. [13] Kiemelendő az irányítás, mint az egyetlen funkció, amely nem delegálható, hiszen a vezetői felelősség és pozíció lényegéhez kötött.

EREDMÉNYEK: A HUMÁN KOCKÁZATI TÉNYEZŐK HÁLÓZATA I.

A közlemény kutatási célkitűzésénél fogva a felhasználói oldal szempontjából szemlélteti a humán tényezőket, annak tükrében, hogy az egyes technikák milyen kapcsolódást mutatnak a támadási felületeken keresztül. Kutatásom későbbi szakaszában fogom elvégezni a hálózat kiegészítését, kiteljesítését mind a védelmi, mind a támadói oldal vonatkozásában felmerülő tényezőkkel.



2. Ábra: Az információbiztonság felhasználói oldali humán tényezőinek összefüggései a támadási felületekkel és technikákkal (saját szerkesztés)

A feltárt humán tényezők, az azok által képzett támadási felületek és a kapcsolódó social engineering technikák összefüggéseinek hálózata a 2. ábrán a lehetséges vizualizációs módszerek közül választott halmazábra segítségével kerül felrajzolásra, az elkészítés során azonban az elmetérkép módszerét alkalmaztam. Megjegyzendő az ábra kapcsán, hogy egyes social engineering technikák akár körvonalazható támadási felületek hiányában is hatékonyan működhetnek a humán kockázati résztényezőkön keresztül. A következő oldalon

szövegesen kiegészítem az ábrán látható viszonyok egy kiemelt részét, a halmazok elemei közötti összefüggések felrajzolása ugyanis az ábrázolás áttekinthetőségének rovására lett volna kivitelezhető. A halmazokkal történő felrajzolás ugyanakkor segít a jelenlegi korlátok között az összefüggések értelmezésében.

A szöveges kiegészítések elé bocsátom, hogy az ábrán látható egyes halmazok, metszeteik és az elemek elhelyezkedése egyik elem vonatkozásában sem jelent kizárólagosságot, azaz pl. egy social engineering technika lazán kapcsolódhat más metszethez, más alaptulajdonság által befolyásolt, illetve a szervezeti sajátosságok által meghatározott egyéb körülményekre tekintettel. Fennállnak továbbá olyan összefüggések is, amelyekben egy social engineering technika más metszetben helyezkedik el, mint amelybe elsődlegesen sorolható a kapcsolódó támadási felület (ilyen viszony mutatkozik pl. a trójai programok és a velük összefüggésben álló, technikai fókuszú ellenőrzés elmulasztása között).

Az egyszerűbb támadási felületképző hiányosságok egyszerű, valamilyen alapszintű cselekvéssel megvalósítható, ezáltal kevesebb kockázati tényező által befolyásolt social engineering technika alkalmazását (pl. shoulder surfing) vonják magukkal. A fizikai biztonsággal, előírások betartásával és szintén egyszerűen kialakuló támadási felületekkel kapcsolatos hiányosságok már minden esetben feltételezik a vezetői attribútumok hiányát, nem megfelelő megnyilvánulását, amely a tudatosság hiányának köszönhető.

Megközelítésem szerint és a rendszerezésem alapján a tudatosság hiánya minden támadási felület képzésénél tetten érhető, ennél fogva foganatosíthatók a különféle social engineering technikák attól függően, hogy a szervezetben milyen szinten (általában nem azonos szinten) szerveződik a másik három alaptulajdonság. Elmondható továbbá, hogy a legtöbb összefüggésben annak ellenére történhetnek meg a támadások, hogy belső képzésekkel, tudatosság-fejlesztéssel a támadási felületek kialakulása jelentős mértékben csökkenthető (ld. következő fejezet).

A humán alapú social engineering technikák a humán kockázati részténye zők összefüggéseinek fényében javarészt a kihasználhatóságban, mint alapszintű felhasználói tulajdonságban gyökereznek. A szervezeti viszonyok ismeretén alapuló technikák (pl. megszemélyesítés, felhatalmazás, helpdesk átverése) minden esetben a vezetői hiányosságokat használják ki, hiszen megelőzhető az ilyen támadási felületek képzése a vezető általános jelenlétével, támogatásával, példamutatásával, továbbá a kapcsolódó képzések, tudatosítás elvégzésével.

A számítógép-alapú social engineering technikák összességében a legbonyolultabb összefüggésekkel rendelkeznek (ld. a 2. ábrán pl. a négy alaptulajdonság közös metszetét). Esetükben szerepet kap ugyanis a hozzájuk kapcsolódó támadási felületek képzésében mind a tudatosság hiánya, mind a kihasználhatóság, mind pedig a hanyagság. A jogosultságkezeléssel kapcsolatos, feljebb részletesen kifejtett hiányosságok adnak lehetőséget a támadói oldal részére a legváltozatosabb technikák alkalmazására, így ebben a körben szerepet kapnak már vezetői attribútumok is.

KÖVETKEZTETÉSEK, KITEKINTÉS

A biztonságtudatossági programok megvalósítása önmagában nem eredményezi a biztonságtudatosság megvalósulását (ld. előző fejezet). Az ilyen tekintetben hatékony és sikeres fejlesztés érdekében elengedhetetlen a tervezéshez szükséges információk teljes körű feldolgozása, a vezetői elkötelezettség és az ezt leképező példamutatás, a program

megvalósítását követően pedig korrekciók foganatosítása a programhoz kapcsolódó visszajelzések alapján. Következtetéseimet a fenti elemekkel kapcsolatos megállapítások formájában fogalmazom meg.

A vezetői példamutatással szemléltethető a vezetés irányítási funkciójának kiemelt szerepe az információbiztonság-tudatosság megvalósulásában, hiszen annak „célközönsége" lehet közvetlen beosztott, nem közvetlen beosztott, azonos vagy alacsonyabb szervezeti szintű munkatárs, de akár magasabb beosztású vezető is, azaz potenciálisan a teljes szervezet. Kiemelt fontosságú a példamutatás a biztonsági területen, ahol nem csupán a vezető, hanem a teljes szakterülethez tartozó minden munkatárs felelőssége egyaránt megmutatkozik

A korrekciók implementálásához (PDCA: Act) szükséges visszajelzés (PDCA: Check) változatos formában, változó számszerűsíthetőség mellett történhet biztonságtudatossági programok esetén. Ilyen módszerek például: közvetlen reakcióértékelés, munkateljesítmény mérése a képzést követő longitudinális értékelés, a munkatársak és vezetők informális értékelése az érintett munkavállaló fejlődéséről, online valós idejű adatgyűjtés, magatartásváltozás. [14]

A számszerűsített visszajelzések elemzése objektivitást kölcsönöz, hiszen a teljesítmény, a kockázat és az ellenőrzési mutatók közötti statisztikai összefüggés kulcsfontosságú visszacsatolás, amelyre a szervezetnek szüksége van ahhoz, hogy meggyőződhessen arról, hogy a kiberbiztonsági intézkedései megfelelőek. Ugyanakkor nagy mennyiségű adat kezelésére, és megvalósítható output-ra van szükség, egyúttal a következetes és megbízható információbiztonsági mutatók felállítása bonyolult, és szakértelmet igényel. [15] Az információbiztonsági kockázatok valós idejű azonosításához és kezeléséhez segítséget nyújtanak a kulcs teljesítménymutatók, amelyekből mélyebb összefüggések mérésére alkalmas komplex mutatószámok származtathatók.

Kutatásom további szakaszára nézve az alábbi célkitűzéseket fogalmazom meg a jelen közleményben bemutatott eredményekre alapozva. Egyrészt a humán kockázati tényezők információbiztonsági vonatkozású hálózata kiegészítendő, teljessé tehető a támadói és a védelmi oldal teljes körű feldolgozásával. Másrészt tudományos-szakmai kutatási célom egy keretrendszer felállítása, mely a hálózat alapján végzett folyamatalapú elemzés outputjától függő szakmai szolgáltatási koncepció kidolgozását teszi lehetővé.

Folyamatban van továbbá részkutatásom, mely a kockázatok számszerűsítését támogató módszerek, mutatószámrendszerek egységesítését célozza, beemelve a kulcs teljesítménymutatók mellé a ROI (befektetés-megtérülési mutató) megközelítést is, így módszertani segítséget nyújtva polgári és katonai szervezeteknek egyaránt abban, hogy a most tárgyalt humán tényezők komplex kezelésének hatékonysága is mérhetővé váljon. A hálózat, valamint az egységes számszerűsítési módszertan lehetőséget teremt a vállalatok számára folyamatalapú elemzés, visszamérés elvégzéséhez: ennek ismeretében testre szabott képzési és egyéb szakmai szolgáltatási koncepciók állíthatók fel a szervezet egésze tekintetében, amelyek hatékonysága így szervesen kapcsolódik az információbiztonsági törekvések hatékonyságához, sőt abból származtatott módon kifejezhető.

FELHASZNÁLT IRODALOM

[1] M. G. Cains, B. Hoffman, T. Kelly and D. S. Henshel, „*Trust as a Human Factor in Holistic Cyber Security Risk Assessment*" presented at 6th International Conference on Applied Human Factors and Ergonomics 2015.

[2] E. D. Oroszi, „*Social Engineering. Az emberi erőforrás, mint az információbiztonság kritikus tényezője*," B.S. szakdolgozat, Budapesti Corvinus Egyetem GK, Budapest, 2008.

[3] Cs. Kollár, „*Social engineering a gyakorlatban – Manipulációk értelmezése a SPEAKING modellben*" Jel-Kép 2017/3. pp. 62-77, 2017.

[4] B. Kárász, „ *Social Aspects of Reliability and Security Issues of Authentication Solutions*," Hadtudományi Szemle vol. XIII. No 1

[5] Zs. Haig, „*Információs műveletek a kibertérben*," Budapest: Dialóg Campus Kiadó, 2018.

[6] K. D. Mitnick, W. L. Simon, „ *The Art of Deception. Controlling the Human Element of Security*," Indianapolis, IN: Wiley Publishing, Inc., 2002.

[7] V. Deák, „ *Biztonságtudatosság az információs környezetben*," Katonai Nemzetbiztonsági Szolgálat Szakmai Szemle Vol, XV. No. 3., pp. 59-76, 2017

[8] M. Wilson, J. Hash, „*Building an Information Technology Security Awareness and Training Program*," National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication (SP) 800-50, October 2003.

[9] J. A. Chestnut, „ *Assessing the Impact of Human Error in Information Security Incidents*," Mississippi, MI: Bell & Howell Information and Learning Company, December 2000.

[10] M. Karoliny, J. Poór Eds., „*Emberi erőforrás menedzsment kézikönyv – Rendszerek és alkalmazások*," Budapest: Wolters Kluwer Kiadó, pp. 365-383, 2015.

[11] B. P. Hámornik, Cs. Krasznay, „*A Team-Level Perspective of Human Factors in Cyber Security: Security Operations Centers"* In: D. Nicholson Ed. *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity*; Springer International Publishing, pp. 224-236. 2017.

[12] H. Stewart, J. Jürjens, „*Information Security Management and the Human Aspect in Organizations*," Information & Computer Security Vol. 25 No. 5, pp. 494-534, 2017.

[13] D. Eppling, L. Magnien, „Leadership in Action – What Great Managers Really Do" Krauthammer, 2005.

[14] B. Kárász, „*Biztonságtudatossági tréningek hatékonyságának vizsgálata,"* Hadmérnök, Vol. XIV. No. 2., pp. 313-324. [online] http://hadmernok.hu/192_26_karasz.pdf (Letöltés ideje: 2020.03.31.)

[15] Cs. Kollár, „Mutatószámok a szervezetek életében, különösen az információbiztonság területén," pp. 111-125. In. B. Bencsik, I. Sabjanics Eds., I. „*Digitális környezetünk fenyegetettsége a mindennapokban*," Budapest: Dialóg Campus 2018.