HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

NÉMETH ZITA[1] – VÖLGYI ZOLTÁN[2]

A kritikus információs infrastruktúra védelem pszichológiai szempontú megközelítése
(Humán biztonsági kockázat elemzés)

The Psychological Aspects of Critical Informational Infrastructure
(Human Security Risk Analysis)

Absztrakt

A társadalmi szempontból létfontosságú informatikai rendszerek elleni támadások elleni védekezés egyre fokozottabban múlik a dolgozók felkészültségén. A felkészültség mérésében, növelésében jelentős szerepet játszik a pszichológiai szempontú kiválasztás, szűrés és felkészítés. A cikkben bemutatásra kerül a humán biztonsági tényezőkkel kapcsolatos jelenlegi szabályozók beazonosítása és annak lehetséges besorolása a kritikus információs infrastruktúra védelem fogalom rendszerében. A cikk második részében egy, a gyakorlatban is kipróbált humán biztonsági kockázat elemzés kidolgozásának teljes folyamatát adjuk közre. A pszichológiai szempontból kockázati tényezőt jelentő személyiségjellemzők beazonosítását követően kerülhet sor azon személyek beazonosítására, akik nagyobb valószínűséggel lehetnek célpontjai az információs támadásoknak.

Kulcsszavak: humán biztonsági kockázat, kompetenciaelemzés, pszichológiai kockázati szint, fejlesztő központ.

Abstract

The defense against the attacks on IT systems with high social importance depends more and more on the preparedness of the human operators. In the estimation and increasing of this preparedness the psychological selection, sifting and preparation plays and important role.

In present article we firstly identify the legal regulators concerning the human

[1] Budapesti Műszaki és Gazdaságtudományi Egyetem, doktorandusz – Budapest University of Technology and Economic, PhD student, E-mail: neemeth@t-online.hu, ORCID: 0000-0001-7392-7817
[2] Nemzeti Közszolgálati Egyetem- National University of Public Service, E-mail: volgyi.zoltan@uninke.hu, ORCID: 0000-0001-5779-9536

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

security risk factors and we also take a look at their classification into the conceptual framework of the defense of the critical informational infrastructure. In the second part of the article we publish a comprehensive and elaborated process for analysing the human security risks, which was also implemented in practice. Following the identification of the personality traits that are resulting in risky behaviours one can sift those people who could be the targets of social engineering.

BEVEZETÉS

A XXI. században a hadviselés megváltozása katonai, politikai és gazdasági szinten is paradigmaváltást eredményezett. Ennek egyik legjelentősebb állomása a 2001. szeptember 11-ei események voltak, melyek a civil lakosság sebezhetőségét állították a figyelem fókuszába. A terrortámadások kapcsán egyértelművé vált, hogy a nemzetek és nemzetközi szervezetek egyik legnagyobb feladata a saját lakosság életének, javainak közvetlen megvédése mellett az ezeket érintő támadások kivédése megelőzése és bejóslása lett. Az említett támadások a polgári lakosság egyre nagyobb mértékű függőségét használják ki, mely az energiaellátástól az étkezésig és a szórakozástól az oktatásig, az élet minden területén megnyilvánul. Ebből eredően a támadások bizonyos mértékben bejósolhatóak, mivel beazonosíthatóak azok a potenciális célpontok, amelyek kiiktatása élet fenntartásával összefüggő hiányállapotot okozhat, ezzel együtt az ország működését, biztonságát veszélyezteti.

A támadások egyre kifinomultabb formát mutatnak. Kezdetben épületek, objektumok, fizikai létesítmények, majd az információs rendszerek, hálózatok szerepeltek az elsődleges célpontok listáján. A védelmi rendszerek fejlődésével az informatikai rendszerek ellen elkövetett támadások kivitelezésében egyre nagyobb teret hódít a humán biztonsági kockázatok kihasználásával terjedő social engineering. „A Social Engineering az emberek természetes, bizalomra való hajlamát használja ki a számítógép-hálózatokba való bejutáshoz. E tevékenység keretében a hálózat gyenge pontjaira vonatkozó adatokat, a legfontosabb jelszavakat, stb. attól a személytől szerzik meg félrevezetés, zsarolás, csalás, esetleg fenyegetés útján, aki azokat kezeli, vagy aki azokhoz hozzáfér. (Haig – Kovács, 2012, 158. o)

A továbbiakban bemutatjuk a Social Engineering elleni védekezés jogszabályi hátterét, valamint egy pszichológiai eszközökkel megvalósított humán biztonsági kockázatra vonatkozó gyakorlatban kivitelezett elemzést is.

JOGSZABÁLYI HÁTTÉR MAGYARORSZÁGON

Az új típusú támadások számának lecsökkentésére, negatív hatásainak mérséklésére, valamint a váratlanságából eredő lakossági félelem és bizonytalanság csökkentésére a nemzetközi szervezetek és az egyes nemzetek eljárásokat, szabályzókat alkottak, melyek a célpontok beazonosítását és biztonságos működéséhez szükséges szempontokat tartalmazzák. A potenciális célpontokat kritikus infrastruktúrának nevezzük, „melyeknek a

működése alapvető fontosságú és nélkülözhetetlen a társadalom működtetéséhez. Amennyiben ezek valamilyen beavatkozás következtében működésképtelenné válnak, az beláthatatlan következményekkel járhat az ország gazdaságára és védelmére, azaz maga az ország biztonsága kerülhet veszélybe." (Haig – Kovács, 2012, 45-46. o)

Magyarországon az első új típusú támadásokra vonatkozó szabályzó a 2080/2008. (VI. 30) Kormány határozat, mely a Kormányzati Koordinációs Bizottság javaslatára elfogadta a hazai infrastruktúra létfontosságú elemeinek védelméhez kapcsolódó további konzultációk alapjául szolgáló a nemzeti programról szóló Zöld Könyvet, aminek a 3.2. pontjában így definiálja a kritikus infrastruktúra fogalmát:

„Kritikus infrastruktúrák alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában.

Kritikus infrastruktúrának minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére"[3]

A Zöld Könyvben a kritikus infrastruktúra védelem fogalmi meghatározása során egyértelműen megjelenik a humán biztonsági kockázatra vonatkozó utalás a személyi jellegű védelmi-intézkedések formájában.

3.4. Kritikus Infrastruktúra Védelemmel kapcsolatos fogalmak

„A kritikus infrastruktúra védelem a kormány, az infrastruktúra tulajdonosok és üzemeltetők által alkalmazott programok, tevékenységek összessége, amelyek a kritikus infrastruktúra rendszerek működőképességének és az infrastruktúra elemek biztonságának garantálására, kockázatok csökkentésére irányuló informatikai, fizikai, személyi és eljárási jellegű elemzési, tervezési, végrehajtási és ellenőrzési védelmi-intézkedéseket foglalja magában."

A 2012. év a kritikus infrastruktúra védelem szabályozásában meghatározó volt. Ebben az évben több hosszú távú tervszerűen átgondolt és egymásra épülő szabályozó is kitér az új típusú támadások elleni védekezés szükségességér. Magyarország Nemzeti Biztonsági Stratégiája a 29. d) pontban kiemelt területként azonosítja a kritikus infrastruktúrák védelmét, igaz a terrorizmus elleni harc vonatkozásában. Azonban külön pontként jelenik meg a kiberbiztonság témaköre, és ezzel szabályozás szintjén is külön válik a kritikus infrastruktúra és a kritikus információs infrastruktúra rendszere. Igaz a fogalom használata ebben a formában csak a később bukkan fel.

[3] 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

Az információbiztonsággal kapcsolatban a Nemzeti Biztonsági Stratégia 48. pontját emelnénk ki, amely fontosnak tartja a politikai, katonai, gazdasági információk megvédését és az ezzel kapcsolatos elhárító képességek meglétét.[4] Ez bizonyos mértékben összefüggésbe hozható a social engineering tevékenység elleni védelemmel, hiszen a titkos információk megőrzéséhez, megtartásához szükséges humán tényezők feltárása, fejlesztése az elhárító tevékenységek részének tekinthető.

Magyarország Nemzeti Katonai Stratégiájának 34. pontjában is határozottan előtérbe kerül az információs társadalommá válás negatív hatása, mely szerint „egyes állami és nem állami szereplők által alkalmazott modern infokommunikációs eszközök biztonsági kockázat előidézéséhez járulhatnak hozzá."[5]

A Zöld Könyvet 2012 novemberében felváltotta a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény, valamint a törvény végrehajtására kiadott 65/2013. (III. 8.) kormányrendelet. A törvény és a kormányrendelet pontosan meghatározza, hogy mit nevezünk létfontosságú rendszerelemnek:

"létfontosságú rendszerelem: az 1-3. mellékletben meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna,"[6]

Ezen kívül pontos utasításokat ad a védelem megvalósításáról és az üzemeltető felelősségébe utalja a kijelölő hatóság által meghatározott határidőre a szervezetre jellemző üzemeltetői biztonsági terv elkészítését. A végrehajtásra vonatkozó kormányrendeletben egyértelműen meghatározásra kerül a 11. § (3) bekezdésben és a 2. mellékletben a létfontosságú rendszerelemek felügyeletét és működtetését végző személyek fizikai, humán és informatikai kockázataival kapcsolatos elvárások pontos meghatározása, azok definiálása.[7]

2013 márciusában egy újabb nagy lépés következett az új típusú támadások elleni védelem szabályozásának tekintetében. A Kormány elfogadta Magyarország Nemzeti Kiberbiztonsági Stratégiáját, amiben meghatározásra került, hogy a kibertér az elektronikus információs rendszerek és az ezeken keresztül áramló adatok és információk összességét jelenti. A kiberbiztonsági stratégia szükségessé vált, mivel nagy mértékben megnövekedett azon állami és nem állami felhasználók száma, akik kritikus adatok és információk illegális megszerzésére, vagy károkozásra használták a kiberteret. Külön pontban (9.) jelenik meg

[4] A Kormány 1035/2012. (II.21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról
[5] 1656/2012. (XII. 20.) Korm. határozata Magyarország Nemzeti Katonai stratégiájának elfogadásáról
[6] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
[7] 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

az információszivárogtatás jelensége, mint kockázati tényező.[8] A Nemzeti Kiberbiztonsági Stratégia kiadása egyértelműen meghatározza a létfontosságú rendszerelemek (kritikus infrastruktúrák) védelmének legmarkánsabb irányait.

Ezen stratégia mentén készült el és került elfogadásra az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, melynek 22. pontjának értelmezése szerint a globális kibertér tartalmazza az elektronikus információs rendszereket és az azokon keresztül történő adat és információáramlást. A 14b. pont pedig kiemeli, hogy az elektronikus információs rendszerek közé besorolandó az adatok és információk kezelésére használt eszközök mellett az azokat működtető személyzet is. Ezen kívül a 19. pontban fenyegetésként definiálja az elektronikus információs rendszer védettségét veszélyeztető eseményt, műveletet, vagy mulasztásos cselekményt. Ezen kívül kitér arra is a 11. § (1), hogy az elektronikus információs rendszer védelméről a szervezet vezetőjének gondoskodnia kell. Ez azt jelenti, hogy információbiztonsági oktatásokat kell tartani, valamint folyamatos elemzéseket ellenőrzéseket, auditokat kell végrehajtani.[9]

A 2013. évi L. törvény kiegészíti a Nemzeti Kiberbiztonsági Stratégiát, ezen kívül a social engineering tevékenységek elleni védelem tekintetében is több fogalomtisztázásra is alkalmas előremutató intézkedést tesz. Lényegi elem, hogy az elektronikus információs rendszerek közé beemeli a személyi állománnyal összefüggő károkozást és humánbiztonsági kockázatot is megfogalmaz a mulasztásos cselekmények bevezetésével, ezen kívül bizonyos munkakörök esetében javaslatot fogalmaz meg a humán kockázatok felmérésére és időszakos ellenőrzésére. Ezt egészíti ki a 41/2015. (VII. 15.) BM rendelet konkrét meghatározásokkal, amely az elektronikai információs rendszerelemekkel rendelkező szervezetek biztonsági osztályba és szintbe sorolását tartalmazza. A rendelet 5 biztonsági osztályt különböztet meg, amelyben az 1. a legenyhébb, ebben károkozásról nem beszélhetünk, az 5. osztály a legsúlyosabb. Humán kockázatról a 2. osztálytól kezdve beszélhetünk, ami az enyhe károkozás kategóriájába sorolható. Ezen kívül annak alapján, hogy a szervezet üzemeltet, esetleg tervez elektronikai információs rendszert, vagy azt külső szereplőkkel üzemelteti, megállapítanak biztonsági szinteket is.

A 3. mellékletben 3 kategóriába sorolva találhatók meg a védelmi intézkedések:

- Adminisztratív (szervezeti szintű alapfeladatok, kockázatelemzés, rendszer és szolgáltatás beszerzés, üzletmenet folytonosság tervezése, biztonsági események kezelése, emberi tényezőket figyelembe vevő – személy – biztonság, tudatosság és képzés).
- Fizikai (fizikai és környezeti védelem).
- Logikai (általános védelmi intézkedések, tervezés, rendszer és szolgáltatás beszerzés, biztonsági elemzés, tesztelés, képzés és felügyelet, konfiguráció kezelés, karbantartás, adathordozók védelme, azonosítás és hitelesítés, hozzáférés

[8] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
[9] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

engedélyezése, rendszer és információsértetlenség, naplózás és elszámoltathatóság, rendszer és kommunikáció védelem).

Írásunk, összefoglalónk témája szempontjából a leginkább releváns kategória az adminisztratív, és a logikai kategória használata. Nagyon gyakran a logikai védelmi rendszer működésére vagy a védelem kiskapuira vonatkozó információk megszerzésének megakadályozását szolgálják az adminisztratív védelmi kategória intézkedései. Pszichológiai szempontból a legérdekesebb humán biztonsági kockázatok felértékelődése, mely a 3.1.6. pontban kerül kifejtésre az emberi tényezőket figyelembe vevő – személy – biztonság címszó alatt. Az ezzel kapcsolatos eljárásrend tájékoztat arról, hogy a személybiztonsággal kapcsolatos eljárások a teljes személyi állományra kiterjednek, de nem egyforma mértékben. Az információbiztonsággal kapcsolatos elemzések a betöltött munkakör és feladatvégzés biztonsági szempontú besorolásától függenek. A besorolást bizonyos időnként felül kell vizsgálni. A személyi állomány ellenőrzésére az információhoz való hozzáférési jogosultság megadása során kerül sor, valamint időközönkénti ellenőrzéseket valósít meg az adott szervezet.[10]

SOCIAL ENGINEERING INFORMÁCIÓS MŰVELETEK SZERINTI BESOROLÁSA

A kritikus információs infrastruktúra védelemben a humán faktor megjelenése a jogszabályi környezetben megemlítésre kerül, azonban leginkább az IT oldali védekezés van a figyelem középpontjába. A tudományos megközelítés fokozottabban kiemeli az emberi kockázat szerepét az információs műveletek esetében a következő képpen.

DIMENZIÓ SZERINTI ELKÜLÖNÍTÉS

A kritikus infrastruktúrák elleni támadások és az ehhez kapcsolódó védekezés három dimenzióban valósítható meg:

„A *fizikai dimenzióban* folytatott információs tevékenységek a különböző információs infrastruktúrák, infokommunikációs rendszerek elemei elleni ún. kemény típusú (Hard Kill) fizikai eltulajdonítással járó támadásokat, illetve azok fizikai védelmét jelentik.

Az *információs dimenzióban* folytatott információs tevékenységek a különböző információs folyamatok (adatszerzés, adatfeldolgozás, kommunikáció stb.) többnyire elektronikus úton való lágy típusú (Soft Kill, ide értjük a szándékos hackelést) támadását jelenti annak érdekében, hogy a célpontokra való közvetlen pusztító, romboló fizikai ráhatás nélkül közvetlenül befolyásoljuk azokat. Másik oldalról ide tartozik a másik fél saját információs folyamatainkra irányuló hasonló támadásának megakadályozása is (etikus hack).

[10] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

A *tudati dimenzióban* megvalósuló információs tevékenységek közvetlenül az emberi gondolkodást – észlelést, érzékelést, értelmezést, véleményt, vélekedést – veszik célba valós, csúsztatott vagy hamis üzenetekkel, amelyeket többnyire elektronikus és nyomtatott médián keresztül vagy közvetlen beszéd formájában továbbítanak." (Haig, 2006, 4. o)

A social engineering tevékenység természetesen a tudati dimenzióban valósul meg, így az ehhez kapcsolódó védekezés is ezen dimenzióhoz kell, hogy kötődjön.

Információs tevékenység alapú elkülönítés

Az információhoz kötődő tevékenységek két típusát különböztethetjük meg:

- „a kommunikációs előny növelése, vagyis információszerzés;
- a kommunikációs hátrány csökkentése, vagyis információvédelem.

Mindkét információs terület esetében jelentős tényezőként említhetjük az emberi kapcsolatok alakítását befolyásoló pszichológiai hatásokat, úgymint szimpátia, benyomáskeltés, befolyásolás, előítéletek, melyek a szociálpszichológia tudományának jellegzetes kutatási területeit jelentik.

„Az információvédelem szempontjából… kiemelt jelentőségű a kommunikációs folyamatok verbális és nem verbális elemeinek tudatos használata annak érdekében, hogy kiküszöbölhető legyen a saját szempontból titkosnak nevezhető stratégiai információk „kifecsegése", a tárgyalások, megbeszélések során mutatott viselkedéssel összefüggő kommunikációs zavarok beazonosíthatósága." (Völgyi, 2017, 90. o)

A social engineering jelensége az információt birtokló ember pszichológiai jellemzőin alapul. Két típusát különböztethetjük meg:

- tudatos információkiadás, amikor a támadó a zsarolás, fenyegetés módszerét használva csal ki a támadás végrehajtásához szükséges információkat;
- nem tudatos információkiadás, amikor az információ birtokában levő személy nem tudja, hogy az általa kiadott adatok, információk a másik fél számára jelentőséggel bírnak, esetleg egy támadás előkészítését támogatják.

A nem tudatos információkiadás egyik formája, amikor kicsalt, vagy ellopott belépési jogosultságokat használnak illetéktelenek, a másik pszichológiai szempontból érdekesebb, amikor az információ birtokosának viselkedés szinten is megnyilvánuló kontrollfunkció gyengesége detektálható. Ilyen például a kritikus információk kifecsegése a figyelem felkeltése céljából. Ez utóbbi biztonsági szempontból minősülhetne kevésbé veszélyesnek, ám ezek a kontraproduktív magatartások a szervezetről alkotott külső képet is rombolhatják, amikor nyilvánosságra kerülnek, ilyen értelemben közvetett gazdasági kárt okozva az adott cég értékében (pl. tőzsdeindexek változása a híresztelések hatására, függetlenül azok teljes valóságtartalmától).

A fent említett támadások elleni védekezés alapvető része a kritikus információval kapcsolatba kerülő alkalmazottak személyiségének vizsgálata, mely a pszichológia fontos részterülete. Ehhez szükséges meghatároznunk azokat humán biztonsági kompetenciákat, amelyek csökkent értékűsége vagy éppen extrém emelkedett szintje kockázati tényezőt

jelent az információs támadások során. Ennek hiányában a biztonsági kockázatok megállapítása, az intézkedések kialakítása és végrehajtása nem lehet eredményes. A jelenlegi szabályozók tekintetében releváns útmutatás nem található a biztonsági elemzések ezen szegmensének kidolgozottságára. Ezt a jogalkotó az üzemeltető felelősségi körébe utalja.

Humán biztonsági kockázat elemzés

A social engineering kivédésére, a hatásaira való felkészítésre több módszertan is rendelkezésre áll. Az egyik vonulatban a meghatározott támadási felületeken színlelt próbálkozásokat hajt végre a Humán Biztonsági Kockázatok felmérésével megbízott szervezet, melyek eredményeképpen konkrét cselekvési terveket dolgoznak ki azok megelőzésére.
Ezek többek között a következő elemekből állhatnak:

- *nyílt forrású információszerzés*, amikor a szervezetről nyilvánosan elérhető adatok kutatása, melyekből támadások eredeztethetők bizonyos körülmények között;
- *hideg hívás*, amikor telefonos információ gyűjtés történik a lehetséges támadási pontok tekintetében, amelynek során a munkatársak biztonsági tudatossági szintjét mérik fel;
- *pishing*, vagyis célzottan küldött e-mailes megkeresés a személyzet azon részére, akik a kritikus adatokhoz hozzáférnek, és tőlük trükkös módon hozzáférési kódok kérése;
- *direkt bejutás*, vagyis helyszíni közvetlen fizikai kapcsolatfelvétel a biztonsági intézkedések erősségének vizsgálatára.

A fenti megközelítés a munkatársak biztonság tudatosságát cselekvéses szinten méri fel. A mi megközelítésünk ezzel szemben arra fókuszált, hogy a személyes jellemzőkből kiindulva is feltárhatók a kontraproduktív viselkedésre való tendenciák és hajlandóságok, és ezzel már a kiválasztás, illetve belső vizsgálatok alkalmával is előre jelezhető a személyi kockázat.

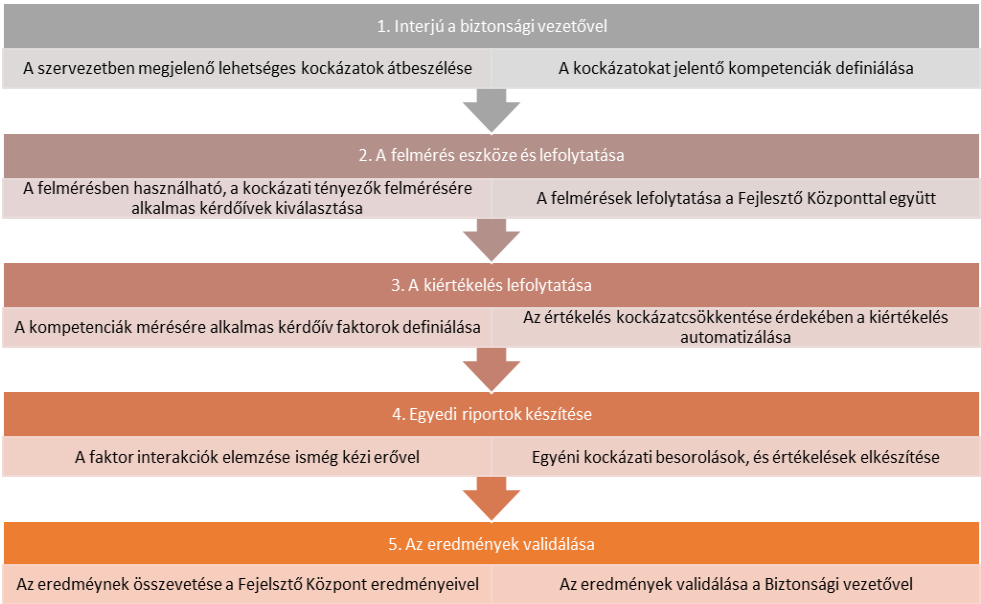
A humán biztonsági kockázat elemzés célja, hogy a szervezetben dolgozó személyi állomány esetében beazonosításra kerüljenek azok az alkalmazottak, akik a pszichológiai jellemzőik kapcsán nagyobb valószínűséggel lehetnek áldozatai a social engineering tevékenységet végző támadók működésének. Elgondolásunk szerint a viselkedést meghatározó személyiségjegyek viszonylag magas biztonsággal bejósolhatják a befolyásolhatóságot, a pszichológiai manipulációnak való ellenállás mértékét. A következőkben egy megvalósított humán biztonsági kockázat elemzést mutatunk be.

Az általunk elvégzett elemzésnek két célja volt. Egyrészt a vezetői kompetenciák meghatározása, másrészt a humán biztonsági kockázatok feltárása. Az első célhoz Fejlesztő Központ metódust használtunk, amelyben egy kb. 2000 fős szervezet megközelítőleg 150 vezetője szerepelt célcsoportként. A szervezeti átalakítások és a növekedés szükségessé tette a vezetőség képességeinek, kompetenciáinak felmérését. A felmérés leghatékonyabban egy szituatív feladatok megoldására támaszkodó, de kérdőívekkel kibővített Fejlesztő Központ komplex módszertannal volt kivitelezhető. Az eljárás során elsősorban arra vol-

tunk kíváncsiak, hogy a vezetők mennyire képesek az átalakítással járó stresszre reagálni, hogyan tudják hatékonyan kezelni a változásokat, és mennyire tudják kezelni a nagyobb felelősséggel járó feladatokat. A projekt másik célja a humán biztonság felmérése és megerősítése volt. Ennek létjogosultsága megkérdőjelezhetetlen, mert a szervezet korábban szinte csak az IT rendszerek korszerűsítésével igyekezett megoldani a kockázatos események megelőzését és elhárítását.

A HUMÁN BIZTONSÁGI KOCKÁZAT ELEMZÉS PROJEKT FOLYAMATA

Az 1. számú ábrán bemutatjuk, és a későbbiekben kifejtjük a humán biztonsági kockázat elemzés folyamatát lépésenként.



1. sz. ábra: A humán biztonsági kockázat elemzés folyamata. Forrás: saját készítés.

1. INTERJÚ A BIZTONSÁGI VEZETŐVEL

A szervezetben végrehajtásra tervezett humán biztonsági kockázat elemzés első fázisában a szervezet biztonsági szakembereivel végzett interjú alapján egy kompetencia lista meghatározása szükséges. Ezen alkalommal a szervezet különböző munkaköreiben esetlegesen előforduló kockázatokról készítünk egy listát. Ezt követően a kockázatokat tovább erősítő „kompetenciákat” határoztuk meg, amelyekre a mérésből információkat akartunk gyűjteni.

A 2. ábra az említett interjú alapján készült kompetenciaelemzés végeredményét mutatja be táblázatos formában.

Kockázatos viselkedés megnevezése	A viselkedésre való hajlandóság lehetséges negatív következménye
Következmény Kontroll	A kockázatos viselkedési mintázat megjelenése esetén a személy a következmények kellően alapos mérlegelése nélkül, elhamarkodottan cselekszik. Impulzívan, érzelemből cselekszik, nagyobbnak érzékeli a kontrollját a helyzetben, mint amivel valóban rendelkezik.
Irracionális Önértékelés	A személy hajlamos arra, hogy képességeit és határait túlbecsülje, és ezek alapján több kockázatot vállaljon, nagyobb dolgokba is belevágjon, mint amit képes kontrollálni.
Inadekvát környezetészlelés	Viselkedését nem a valóság, hanem az ő általa észlelt környezet és körülmények irányíthatják, a téves következtetések kapcsán fontosnak ítélt helyzet alkalmával kockázatvállalásra is hajlamos. Önmagában a döntése mérlegelt, de a környezetet torzítva látja, ezért jelenthet veszélyt.
Figyelemigény	Annak érdekében, hogy a középpontba kerülhessen, biztonsági kockázatot jelentő információkat is kiadhat.
Instabilitás	Extrém stressz helyzetben viselkedése kiszámíthatatlanná válhat. Instabilitása kihasználhatóvá (zsarolás, befolyásolás) teszi.
Irreleváns Döntés előkészítés	Magas kockázattal járó döntéseknél hajlamos a mérlegelés elmulasztására, és a határok kitolására, a tárgyi környezetben, bár arra törekszik, hogy mások személyeknek ne ártson ezzel.
Befolyásolhatóság	Nehezen mond ellent az általa elismert referenciaszemélynek, az általa adott utasításokat megkérdőjelezés nélkül megteszi ez alapján realitásnak ellentmondó dolgokat is végrehajt.
Megfelelésigény	A referencia személy elismerésére vágyik, ez motiválhatja a realitásnak ellentmondó cselekvések kivitelezésére.
Pénz által motivált kockázatvállalás	Anyagi juttatás ellenében hajlandó lehet magasabb szintű kockázatot vállalni.

2. sz. ábra: Humán biztonsági kockázatelemzés kritikus kompetencia tára. Forrás: saját készítés.

Azt is tudjuk azonban, hogy vannak olyan személyiség tényezők, melyek a kockázatok csökkentésének irányába mutatnak, és amelyek mintegy védelmi funkcióként állnak a személy rendelkezésére a kockázatok viselkedések kivitelezésében.

A 3. ábra a protektív faktorként működő személyiség jellemzőket mutatja, melyek jelenléte csökkenti a kockázatvállalási hajlandóságot.

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

Kockázat csökkentő viselkedés neve	Hatása
A Személyiség Önszabályozó alrendszere	Magas szintű működés esetén a személy viselkedésében kisebb valószínűséggel jelenik meg a kockázatos elem.
Tervezettség és szervezettség	Magas szintű működése a hirtelen, impulzív cselekedetek megjelenési valószínűségét csökkenti.
Elővigyázatosság, mint extrém stressz reakció	Megbízható és alacsony kockázatú döntések meghozatalára törekszik. Biztosítékra, konzultációra van szüksége, és hibáin hajlamos sokáig rágódni, amiből sokat tanul.

3. sz. ábra: azonosított protektív faktorok. Forrás: saját készítés.

2. A MÉRÉS ESZKÖZÉNEK DEFINIÁLÁSA

A személyiségmérő eljárások révén objektív módszerünk van arra, hogy megvizsgáljuk, milyen szinten rendelkeznek a vizsgálat résztvevői adott kompetenciákkal. A vizsgálatban azonban csak olyan eszközt szabad alkalmaznunk, mely megfelel a legfőbb pszichometriai kritériumoknak.

A mérőeszköz akkor mér jól, ha:

- érvényes: azt a fogalmat méri, amit mérni szeretnénk,
- megbízható: nem hangulatot mér, és több különböző alkalommal hasonló eredményre jut,
- normázott: rendelkezik nemzeti vagy nemzetközi referenciaadatokkal, amelyek segítségével az átlagos és az átlagtól eltérő értékek meghatározhatóak.

Az elemzés során a megvizsgált személyi állomány kritikus kompetenciáinak és protektív faktorainak beazonosítása több, hatékonyan működő pszichológiai kérdőív eredményeinek összesítéséből keletkezett, melyek a fent kifejtett kritériumoknak megfeleltek.

A mérés objektivitásának további erősítésére minden faktor esetében legalább kétféle kérdőív minimum 2 skálájának értékelését vettük figyelembe a kockázati kategória meghatározásánál. Az értékek kijelölésében pedig erőteljesen támaszkodtunk a normázott átlagértékekre és az átlagtól való átlagos eltérésre (szórási eredményekre) is.

A kérdőívek adatainak elemzését követően minden kritikus kompetencia esetében beazonosítottuk a személy kockázati szintjét, amit 5 kategóriába soroltunk:

- Nincs kockázat: egyik skálán sem jelenik meg emelkedett vagy csökkent érték.
- Alacsony kockázat: egy vagy kevés skálán van kockázatot jelentő érték
- Közepes kockázat: egy skálán jelentős, vagy több skálán közepes kockázatú értékek vannak.
- Magas kockázat: több skálán jelentős és mellé máshol is közepes értékek vannak.
- Extrém magas kockázat: több skálán figyelhető meg jelentősen kockázatos érték.

HADTUDOMÁNYI SZEMLE

2018. XI. évfolyam 3. szám

3. A KIÉRTÉKELÉS LEFOLYTATÁSA

A kérdőívek kockázati faktor és protektív faktor kombinációinak meghatározását egymástól függetlenül foglaltuk rendszerbe, majd egy egyeztetés során validáltuk a végleges formátumot.

Az objektivitás további növelése érdekében a kiértékelést algoritmusokba foglaltuk, melyet egy számítástechnikai szakértő segítségével automatizált kiértékelő rendszer segítségével futtattunk le az adatsorokon.

Így minden résztvevő számára elkészült egy komplex, színkódokkal egyértelműsített kockázati profil, mely az értékelés végén faktoronkénti és egy összesített kockázati besorolást is mutatott.

4. EGYEDI RIPORTOK KÉSZÍTÉSE

A számszerű besorolásokat követően a faktorok összefüggéseit és értékeit értelmezve minden résztvevőről egyedi riport készült.

5. AZ EREDMÉNYEK VALIDÁLÁSA

Az eredményeket több módon is validáltuk, mivel általános személyi jellemzők voltak a megfigyelés tárgya, így feltételeztük, hogy a vizsgálat végeredményében a kockázatok gyakorisága majd normál eloszlást követ, ami be is igazolódott. Továbbá más szakemberekkel is egyeztettünk, akik hasonló méretű projekten hasonló kockázati eloszlást tapasztaltak.

A harmadik validálási szempont a random-szerű Fejlesztő Központ eredményével való összehasonlítás volt, ahol a vártnak megfelelően a személyenként definiált kockázatos viselkedések valóban meg is jelentek.

A negyedik validálás pedig a Biztonsági vezetővel folytatott beszélgetés, ahol összevetettük a részleg adatait és az általunk azonosított kockázatosnak ítélt személyeket, és ebben is teljes egyezőséget találtunk. Minden, általunk magas és extrém magas értékelés kapó személy bekerült már a Biztonsági Osztály látókörébe is valamilyen módon. A viselkedéses jellemzőkben azonban tudtunk a vezetőnek új, használható, cselekvési tervbe szőhető információval szolgálni.

A visszajelzés alapján kiderült az is, hogy az általunk felállított rendszer átlátható, laikus számára is jól érthető és értelmezhető, a többszöri verifikálások alapján pedig kellően megbízhatónak is tekinthető.

KÖVETKEZTETÉSEK

A Social Engineering tevékenységekhez kötődő információvédelem jelenkorban egyre nagyobb jelentőséggel bír mind a civil, mind a katona szervezeteknél. Mivel a katonai, politikai, gazdasági információk megszerzése során egyre gyakrabban alkalmazott technika a személyi állomány pszichológiai manipulálása. A kritikus infrastruktúra védelemhez

kapcsolódó szabályozók változásával is egyre nagyobb hangsúlyt kap az információvédelem és ezen belül is a személyi állományhoz kötődő biztonság, melynek megjelenési formája viselkedésben lelhető fel, azonban a viselkedést meghatározó pszichológiai jellemzők határozzák meg kitettség mértékét.

A pszichológiai jellegzetességek mérése pszichológiai eszközökkel lehetséges bejóslást ad a vizsgálat alá vont dolgozók humán biztonsági kockázatának mértékéről és segít a szervezet biztonsági vezetőjének a humán erőforrás gazdálkodást érintő döntéseiben. Az elemzések során beazonosításra kerülnek a kritikus kompetenciák, melyek a szervezet szempontjából aktív, vagy passzív károkozást eredményeznek, de minden esetben kockázatos viselkedést jelentenek. Ezen kívül a kockázatos viselkedést csökkentő protektív faktorokat is megjelöljük és a kettő összegzett értékeléséből alkotunk egy összesített értéket, ami tájékoztató jellegű. Az elemzések felhasználása eddig minden esetben döntéstámogató funkcióval bírt, önmagában nem bizonyító erejű.

IRODALOMJEGYZÉK

1. 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.
2. 1656/2012. (XII. 20.) Korm. határozata Magyarország Nemzeti Katonai stratégiájának elfogadásáról.
3. 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.
4. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.
5. 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról.
6. 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről.
7. 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról.
8. 1035/2012. (II.21.) Kormány határozata Magyarország Nemzeti Biztonsági Stratégiájáról.
9. Green Paper on a European Programme for Critical Infrastructure Protection. Brussels, 17.11.2005. COM(2005) 576 final.
10. Haig Zsolt (2006): Az információbiztonság komplex értelmezése. Robothadviselés 6. tudományos konferencia kiadványa. Hadmérnök különszám. Elérhető: http://hadmernok.hu/kulonszamok/robothadviseles6/haig_rw6.pdf (Letöltve: 2018. 06. 25.)

11. Haig Zsolt-Kovács László (2012): Kritikus infrastruktúrák és kritikus információs infrastruktúrák. Nemzeti közszolgálati Egyetem jegyzete
12. Nemzeti Infokommunikációs stratégia 2014-2020 (2014. 02. 04.) Az infokommunikációs szektor fejlesztési stratégiája (2014-2020) v7.0
13. Völgyi Zoltán (2017): A személyközi kapcsolatokon alapuló információs műveleteket végrehajtó állomány kiképzésének pszichológiai támogatása. Honvédségi szemle, (3): 87-97 Elérhető: http://docplayer.hu/67971584-A-szemelykozi-kapcsolatokon-alapulo-informacios-muveleteket-vegrehajto-allomany-kikepzesenek-pszichologiai-tamogatasa.html (Letöltve: 2018. 06. 25.)