NEMZETBIZTONSÁGI SZEMLE

Kiemelt közlemények

9. évf. (2021)
4. szám

ISSN 2064-3756 (elektronikus)

LUDOVIKA
EGYETEMI KIADÓ

Impresszum

Nemzetbiztonsági Szemle
A Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézetének elektronikus (online) megjelenésű tudományos folyóirata

HU ISSN 2064-3756 (elektronikus)

Kiadó
Nemzeti Közszolgálati Egyetem | Ludovika Egyetemi Kiadó
Kapcsolat: www.ludovika.hu; kiadvanyok@uni-nke.hu
Székhely: 1083 Budapest, Ludovika tér 2.
A kiadásért felel: Deli Gergely rektor
Olvasószerkesztők: Bujdosó Hajnalka, Gergely Zsuzsánna, Resofszki Ágnes
Tördelőszerkesztő: Kőrösi László

Tartalom

NEMZETBIZTONSÁGI SZEMLE
9. évfolyam (2021) 4. szám 3–17. • DOI: 10.32561/nsz.2021.4.1

Jasenszky Nándor[1] – Regényi Kund Miklós[2] – Lippai Zsolt[3]

A biztonságtudatosság fogalma, fejlődése nemzetbiztonsági, terrorelhárítási és magánbiztonsági szempontból

The Concept and Evolution of Security Awareness in National Security, Counterterrorism and Private Security

Cikkükben a szerzők összehasonlító megközelítést alkalmazva mutatják be a biztonságtudatosság aktuális kérdéskörét. A biztonság fogalmából indulnak ki, majd áttérnek a biztonságtudatosság fogalmára, és a nemzetbiztonsági szolgálatok vonatkozásában vázolják fejlődésének jelentős mozzanatait. Ezt követően röviden felvillantják a rendőri bűnmegelőzést, majd áttérnek a biztonságtudatosítás terrorelhárítási szempontú ismertetésére. A cikk a téma magánbiztonsági szempontú bemutatásával és egy nemzetközi környezetből vett esettanulmánnyal fejeződik be. Az összegzésben a szerzők hitet tesznek amellett, hogy a hasonló módszertanon túl, a nemzetbiztonsági, terrorelhárítási és magánbiztonsági biztonságtudatosság egymást támogatja és kiegészíti.

Kulcsszavak: *biztonságtudatosság, nemzetbiztonság, terrorelhárítás, magánbiztonság, rendőri bűnmegelőzés, szállodaláncok biztonsága*

In their article, the authors present – using a comparative approach – the current issue of security awareness. In doing so, they start from the concept of security, then move on to the concept of security awareness, and outline the significant moments of its development in relation to national security services. They then briefly flash police crime prevention and then move on to the security awareness presentation from a counterterrorism perspective. The article concludes with a presentation of the topic from a private security perspective and a case study in an international context.

[1] Vezető, Terrorelhárítási Központ, Társadalmi Kapcsolatok Osztály; e-mail: jasenszky.nandor@tek.gov.hu
[2] Adjunktus, Nemzeti Közszolgálati Egyetem Polgári Nemzetbiztonsági Tanszék; e-mail: Regenyi.Kund@uni-nke.hu
[3] R. alezredes, mesteroktató, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Magánbiztonsági és Önkormányzati Rendészeti Tanszék; doktori hallgató, Rendészettudományi Doktori Iskola; e-mail: lippai.zsolt@uni-nke.hu

In the summary, the authors believe that, in addition to a similar methodology, national security, counterterrorism, private security and security awareness support and complement each other.

Keywords: *security awareness, national security, counterterrorism, private security, police crime prevention, security of hotel chains*

1. Gondolatok a biztonságról

A biztonság az egyének, az emberi közösségek, a különböző társadalmak talán egyik legrégibb igénye és vágya. A biztonság igényét korábban megtörtént vagy folyamatosan jelen lévő, nemkívánatos veszélyes események megtörténte vagy történése váltja ki. A közösség igyekszik tenni azért, hogy a helyzet megváltozzon és a kívánatos rend helyreálljon. Ebből a cselekménysorból, az adott válaszokból alakul ki a védelem. A védelmi intézkedések a konkrét, azonnal kezelendő eseményekre adott direkt válaszok. Az állandósuló ilyen irányú feladatok hozták, hozzák létre azokat a védelmi – nemzetvédelmi és rendvédelmi – szervezeteket, amelyek hivatásszerűen foglalkoznak a problémák kezelésével. Ezektől a szakmai közösségektől elvárható volt, hogy ne csak az akutan jelentkező nemkívánatos eseménnyel foglalkozzanak, hanem azt összefüggéseikben, rendszerben vizsgálják. A további bemutatás érdekében maradunk az akut kifejezés használatánál, amely leginkább az egészségügyi, orvosi ellátási nyelvezet része. Nézzük az orvoslás működési logikáját:

- tünetek azonosítása;
- diagnózis felállítása;
- tüneti kezelés;
- gyógyítás;
- utókezelés;
- megelőzés.

Amennyiben ezt a közérthető egészségügyi „kezelési" sort lefordítjuk – például a terrorelhárítás nyelvére, akkor a következőt látjuk:

- tünetek = észlelés, detektálás;
- diagnózis = elemzés, értékelés;
- tüneti kezelés = felderítés, felszámolás;
- gyógyítás = az okok feltárásával az ellenséges lehetőségek korlátozása, megszüntetése;
- utókezelés, megelőzés = társadalmi párbeszéd, tájékoztatás, nevelés, oktatás, a biztonságtudatos magatartás kialakítása, karbantartása és fejlesztése.

Jelen cikk a biztonságtudatossággal kapcsolatos témák tárgyalását tűzte ki célul.

2. A biztonságtudatosság mint fogalom és jelenség kialakulása

A biztonságtudatosság, vagy régebbi megjelöléssel *awareness* tevékenység, a 2010-es évek végén felértékelődni látszik a címben említett, tágabb értelemben vett rendvédelmi szervek működésében. A szerzők ezért elérkezettnek látták az időt, hogy bemutassák a biztonsági tudatosság fogalmát, és röviden vázolják annak tartalmát a megelőzésre törekvő állami, illetve magánbiztonsági szolgálatok tevékenységében.

Első mozzanatként a fogalom tartalmát érdemes körüljárni. Ha az angol szó jelentéséből indulunk ki, úgy az awareness legtalálóbb fordítása valóban a tudatosság lesz. Ha a később vázolandó tevékenységet vizsgáljuk, akkor az említett tudatosság ehelyütt nem más, mint a célul kitűzött állapot, tudniillik az a fajta magas szintű (biztonsági) tudatosság, amely a szolgálatok komplex felvilágosító, oktatási tevékenysége eredményeképpen jön létre. A fogalmat tovább vizsgálva azt is elmondhatjuk, hogy annak tartalmi eleme a tudatosságból fakadó cselekvés is, azaz a biztonsági eljárások és ajánlások megismerésén túl annak betartása; illetve ha ezek megsérülni látszanak, úgy a szolgálatok tájékoztatása is.

Tágabb értelemben a fogalomhoz soroljuk azokat a művészi vagy legalábbis szórakoztató igénnyel készült irodalmi és/vagy filmalkotásokat is, amelyeknek járulékos célja, hogy pozitív képet alkossanak, mutassanak honvédelmi, rendvédelmi és nemzetbiztonsági szervezetekről, megteremtve ezzel esetleges megkeresésük, kapcsolatfelvételük esetére a fogadókészséget.

Ha tehát tartalmi definíció megalkotására vállalkozunk, úgy az a következőképpen hangzik. Biztonsági tudatosság alatt a tágabb értelemben vett rendvédelmi és magánbiztonsági szervek komplex, plakátok, emléktárgyak előállításában és átadásában; előadások, filmvetítések, e-learning-anyagok létrehozatalában és megtartásában megnyilvánuló oktatási képzési tevékenységet értjük. Eredményeképpen létrejön a biztonsági kihívásokat jól ismerő, a megelőzéshez és elhárításhoz szükséges magatartási formákat szintén ismerő és a gyakorlatban azokat alkalmazó, implementáló attitűd, viszonyulás, eljárásrend, amely kiterjed a biztonság sérülése esetén a rendvédelmi szervek megkeresésére, tájékoztatására is.

(Közbevetett megjegyzés, hogy a biztonságtudatosság helyett érdemes lenne más *terminus technicus*t használni, így például javasoljuk a biztonsági tudatosítás vagy az érzékenyítés fogalmának alkalmazását, tekintve, hogy ez sokkal kifejezőbb az említett szerzők által fontosnak tartott tevékenység vonatkozásában.)

3. A biztonságtudatosság rövid áttekintése nemzetbiztonsági vonatkozásban

Térjünk át a biztonsági tudatosítás kialakulására és fejlődésére. A biztonsági tudatosítás megjelenése mögött az a nyilvánvaló körülmény áll, hogy a szolgálatok egyetlen korban sem voltak képesek valamennyi ellenérdekelt vagy potenciálisan ellenérdekelt tevékenység észlelésére. Annak érdekében, hogy munkájukat hatékonyan tudják végezni, szükségük volt potenciális fenyegetéseket hordozó személyekre vonatkozó

jelzésekre, illetve indokolt volt biztonságtudatos magatartás kialakításával megnehezíteni az ellenérdekelt fél dolgát.

Ez napjainkban is így van. A nemzetbiztonság, a terrorelhárítás, a bűnüldözés, a szervezett bűnözés elleni harc információéhsége szinte csillapíthatatlan. Az elkövetett cselekmények *modus operandi*jának változása – magasabb szervezettség, intenzívebb konspiráció, a magányos elkövetők térnyerése, a terrorizmus és a szervezett bűnözés összefonódása – egyre inkább igényli, hogy a társadalomból, a kis közösségekből érkezzenek információk, mert sok esetben ezek az adatmorzsák a megoldáshoz vezető út iránypontjai. Ahhoz, hogy ezekből a forrásokból a felsorolt szakmai területek információhoz jussanak, élvezniük kell az emberek, a társadalom bizalmát. A bizalom roppant illékony. Megszerzéséhez, és főleg a megtartásához, sok tennivaló vár az érintettekre. Átlátható, a közösség által megérthető tevékenység, gyors és tényszerű szakmai kommunikáció az alapjai a bizalom építésének. Ugyanakkor a bizalom rombolásában – ami sokkal, de sokkal gyorsabb, mint az építés – megkerülhetetlen a „nyilvánosságcsinálók" szerepe. Rögtön szögezzük le, hogy nem azzal van a baj, ha foglalkoznak ezekkel a kérdésekkel, még azzal sem, ha kritikusok, hanem az esetenként ellenőrizetlen, torzított, olykor félrevezető állításokkal. A felelőtlenül pellengérre állított hatóságok minősítésével a „hozzá nem értő", „feladatát megoldani nem tudó", de legalább „semmit nem tévő" jelzők hihetetlenül gyorsan erodálják a nemzetbiztonsági és rendvédelmi szervek bizalmi bázisát. Határozott álláspontunk, hogy a minőségi politizálást és újságírást a felelősségteljességnek is jellemeznie kell.

Régebbi időszakokban a kihívásokat hordozó személyek azonosítása, hatóságok részére való feljelentése volt az előtérben. Már a középkor nagy háborúiban is megfigyelhetünk egyfajta kémpánikot. A történeti emlékezet ennek elsősorban negatívumait, túlhajtott vonásait őrizte meg. Szakmai szemmel azonban jogos az az értékelés, miszerint sikerült felkelteni az ellenérdekű kémekkel szembeni éberséget, és a bármilyen néven nevezendő szolgálatokhoz számos indító jelzés érkezett. Ennek emlékét őrzi mind a mai napig bizonyos súlyos, elsősorban államellenes és emberiségellenes bűncselekményekhez kapcsolódó feljelentési kötelezettség.[4]

A 19. század harmadik harmadára nemcsak a modern értelemben vett nemzetbiztonsági szolgálatok jelennek meg, hanem a megelőzésre való törekvés felértékelődésével új eszközökkel bővül az awareness-tevékenység is. Ehelyütt elsősorban a plakátokat,[5] illetve figyelemfelkeltő feliratokat[6] emeljük ki, amelyek a korszak konfliktusaiban, így a rövid 20. századot bevezető I. világháborúban tömegével készültek. Elmondható, hogy a fennmaradt plakátok jelentős része a tágabb értelemben vett háborús propaganda céljait szolgálta mindkét oldalon, azonban a mai értelemben vett biztonsági tudatosítás céljai is jól megragadhatók. Ugyancsak az I. világháború utáni időszakra vonatkozóan említhetjük a különböző, változó igényességgel készült

[4] Görgényi Ilona et al.: *Magyar büntetőjog általános rész.* Budapest, 2019. 4.2.4. fejezet (A feljelentési kötelezettség elmulasztása).

[5] Lásd: https://pbs.twimg.com/media/C8scr59WsAAxGiQ.jpg és https://media.gettyimages.com/photos/telling-a-friend-may-mean-telling-the-enemy-shes-not-so-dumb-careless-picture-id138603173?s=612x612

[6] Például: lehallgatás lehetőségére való figyelmeztetés tábori telefonon: www.worthpoint.com/worthopedia/original-wwii-hungarian-military-1817694951

regények,[7] pamfletek megjelenését is. A II. világháborúra a biztonsági tudatosítás eszköztára a filmekkel is kibővült, és elmondható, hogy ez az eszköztár jórészt napjainkig használatos.

Magyarország vonatkozásában az előbb vázolt fejlődés jól bemutatható. Az I. világháború után az önálló, független Magyarország és az önálló nemzetbiztonsági szolgálatok megjelenésével az I. világháborúban kialakult eszköztár továbbélését és fejlődését láthatjuk. A korszakból nemcsak plakátok, hanem irodalmi igényű, tágabb értelemben a biztonsági tudatosításhoz sorolható alkotások is fennmaradtak. A nemzetbiztonsági szolgálattal szorosan együttműködve, később pedig azzal szervezetileg is összevont módon létezett egy hazafias propagandáért felelős szervezet is.[8]

A II. világháborút követően, ideológiailag átkeretezve, a biztonsági tudatosítás tovább élt és fejlődött. Korunkra maradt emlékei közül elsősorban itt is a szélesebb közönség számára készült, biztonságtudatosítási funkciót is ellátó regényeket, illetve filmeket emelhetjük ki.

A rendszerváltást követően a biztonsági tudatosítás átmeneti időre háttérbe szorult, hogy a feladatrendszer és a küldetés egyértelművé válásával a 2000-es években újra megjelenjen, betöltve hasznos és nélkülözhetetlen szerepét.

Ma a nemzetbiztonsági szolgálatok biztonsági tudatosító tevékenységüket elsősorban az úgynevezett intézményvédelem keretében, vagy azzal szorosan együttműködve látják el. A biztonsági tudatosítás első lépéseként előadásokat rendeznek, tájékoztatókat tartanak, amelyek keretében, illetve azokhoz kapcsolódóan papíralapú vagy elektronikus tájékoztató anyagok, szórólapok átadására is sor kerül. A tájékoztatók mellett megtalálhatók a plakátok és az emléktárgyak is. A hatékonyság növelése érdekében a tájékoztatók testreszabhatók a célközönség igényeinek, illetve fenyegetettségi szintjének megfelelően.

A technika fejlődésével párhuzamosan a biztonsági tudatosítás súlypontja elsősorban az informatikai és kiberbiztonságra tevődik át. Ez a felület annyira előtérbe került, hogy önállósodott is, illetve esetenként maga a fogalom is sokak számára csak erre vonatkozik. A nemzetbiztonsági szolgálatok azonban megőrzik a biztonság és a fenyegetés komplex megközelítését. Természetes, hogy az IT-, illetve kiberbiztonsági tudatosítás mára kommercializálódott, és az e területen aktív vállalkozások tevékenységének egyik elemévé vált.

A folyamatot tovább kísérve elmondható, hogy optimális esetben biztonsági tudatosítás eredményeképpen jelzések érkeznek a szolgálatokhoz, megalapozva azok hatékony fejlődését.

Az elhárító szolgálatok eszközrendszerének egyéb elemeivel összehasonlítva igazolható az a megállapítás is, hogy a biztonsági tudatosítás egyfajta kapunyitó szerepet is betölthet, mivel ennek során a szolgálatok segítő-támogató attitűdje válik kézzelfoghatóvá.

---

7 Viszonylag ismert magyar példák Mattyasovszky Jenő Hód-könyvei, és Mág Bertalan: *Öt méregfiola.* Budapest, Zrínyi, 1984; vagy a Berkesi András – Kardos György szerzőpáros könyvei, például *Kopjások*. Budapest, Magvető, 1986.

8 Lásd Kádár Gyula: *A Ludovikától Sopronkőhidáig.* Budapest, Magvető, 1984. A részleget Somogyváry Gyula, I. világháborús veterán, hazafias könyvek szerzője (például: *Virágzik a mandulafa; Ne sárgulj, fűzfa!; És Mihály harcolt* stb.) vezette.

4. Kitekintés – rendőri bűnmegelőzéssel kapcsolatos tapasztalatok

Ahhoz, hogy jobban átlássuk a helyzetet, az „idősebb rokont", a bűnmegelőzést, annak rendszerét célszerű segítségül hívni. Az egyik szerzőtárs, Jasenszky Nándor személyes élményanyagát hívjuk segítségül.

Az 1980-as évek elején a Budapesti Rendőr-főkapitányság (BRFK) Betörési Csoportjának fő profilját a kiemelt – a ma már megmosolyogtató 100 000 forint és az afeletti – kárértékű, illetve a sorozatban elkövetett betörések képezték. A szakmai közösség és annak vezetői elvárták és megkövetelték, hogy a nyomozások során vizsgáljuk a lehetővé tevő körülményeket és persze azt is, hogy mit és milyen formában tehetünk ezek ellen. Csak egy példát ragadnék ki a számtalanból. Amikor 1982 márciusában megindult – a korábban Magyarországon szinte ismeretlen – hengerzártörés módszerével elkövetett lakásbetörési sorozat, az első perctől kiemelt feladat volt az elkövetés vizsgálata. A módszer gyors, egyszerű, csekély eszközigényű, nyomszegény zárnyitást tett lehetővé. A másik fontos momentum volt, hogy Magyarországon a leggyakrabban használt, úgynevezett „körte alakú" hengerzárbetétet támadta. Tapasztalatainkkal – a még zajló felderítés mellett – megkerestük a kérdéses Elzett zár gyártóját, és elkezdődött a lehetőségek vizsgálata a zárak és zárkörnyezetek átalakításáról a behatolási módszer megakadályozása érdekében. Az akkor kimunkált megoldások a mai napig élnek, és beépültek a biztonságos zárrendszerek gyártási folyamatába.

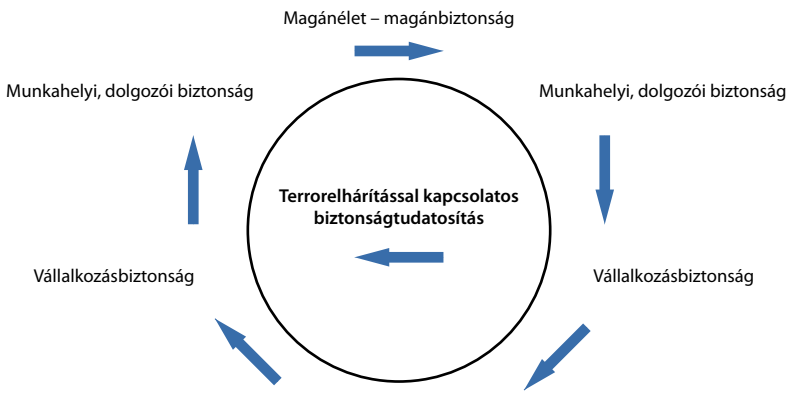
A nyolcvanas évek elején a BRFK vagyonvédelmi szakterületének szervezeti válasza is volt a betöréses lopások visszaszorítására, létrehozta a Vagyonvédelmi Tanácsadó Szolgálatát, amely a maga korában az első és egyetlen volt, ahol rendőri és megfelelő műszaki tapasztalattal is rendelkező munkatársak adtak a komplex védelmi rendszerek kialakítása érdekében tanácsokat, és kötötték össze az állampolgárokat a biztonsági szolgáltatókkal. A későbbiek során a bűnmegelőzés önálló szakterületté vált, széles körben, megfelelő szervezeti háttérrel, külső társadalmi kapcsolatrendszerrel végzik munkájukat napjainkban is.

5. Biztonságtudatosság a terrorelhárításban

A terrorizmussal, a terrorelhárítással a rendszerváltás előtt csak nagyon sajátos módon, szinte a nyilvánosság, a társadalom teljes kizárásával lehetett foglalkozni. Ugyan együtt éltünk vele, hiszen ha csak a modern kori terrorizmus alapkövének tekinthető 1972-es müncheni olimpiai támadásra gondolunk, vagy a Vörös Brigádok, a Vörös Hadsereg Frakció tevékenységére, ezek ismert események voltak a nyilvánosság számára is. Ugyanakkor a kétpólusú világrendben ezek olyan cselekményekként lettek tálalva, mint amelyek nálunk meg sem történhetnek. Az időszakot meghatározta a „te terroristád – az én szabadságharcosom" nézőpont szerinti – finoman fogalmazva – átpolitizált hozzáállás.

A rendszerváltás után a helyzet alapvetően megváltozott. A magántulajdon erőteljes fejlődése, a gazdasági szerkezet átalakítása, a társadalom, a jogrendszer, a nemzetbiztonsági szervezetek, a rendvédelmi szervek kihívásainak, feladatainak változása új helyzetet teremtett. A körülmények ilyen nagymérvű, komplex változása oda vezetett, hogy a jelen tanulmányban leírt kezelési modellből a legoptimálisabb esetben is csak a tüneti kezelésig jutottunk. Ez tetten érhető volt a terrorelhárítás és a szervezett bűnözéssel való foglalkozás területén is. Nem voltak mélyreható, ok-okozati összefüggéseket feltáró elemzések, nem voltak kiérlelt javaslatok, sok esetben a társadalom és a politika is adós volt azzal, hogy mit vár el a felelős szakmai szervezetektől. Determinált volt a kapkodás, rögtönzés, a pillanatnyi felszíni problémák eseti kezelése. Ebben az időben a biztonságtudatos magatartások speciális formálása erősen háttérbe szorult, illetve inkább nem is volt. Az egyre aktívabb, öntudatosabb társadalom kialakulása, fejlődése folyamatosan fejlesztett egy nyitottabb, sokkal szélesebb alapokon nyugvó kommunikációt. A megjelenő információk mennyisége és gyorsasága egyre nagyobb mértékben befolyásolta a mindennapokat. Természetesen sokkal nagyobb teret kaptak a negatív jelenségekkel kapcsolatos felvetések is. A hirtelen sokszereplőssé váló hírverseny káros mellékhatása volt, hogy a gyorsaság és a mennyiség a hiteles tájékoztatás és a minőség rovására ment. A média a biztonságérzetet befolyásoló tényezővé vált.

A következő, szerencsés mozzanat a konszolidáció bekövetkezése, amelynek terrorelhárítási, egyben felderítési szempontból határköve és kiindulópontja a Terrorelhárítási Központ (TEK) 2010-es megalakulása. A TEK hosszú évek óta igyekszik, hogy szélesítse a párbeszédet a társadalommal. Jelenleg bizonyos célcsoportokra fókuszál, de törekszik folyamatosan bővíteni a kört a tömegtájékoztatás eszközein túl a helyszíni személyes megjelenés lehetőségével, előadások, tájékoztatók megtartásával is. Az így átadott információkkal szeretnénk elérni a biztonságtudatossági folyamat vagy körforgás kialakulását. Ennek lényege – véleményünk és tapasztalataink szerint – az egymásra épülő biztonság, a biztonsági szintek körforgása.



1. ábra

Biztonságtudatossági körfolyamat

Forrás: Jasenszky Nándor kutatása és szerkesztése

6. Magánélet – magánbiztonság

Az embereknek, közvetlen környezetüknek, családjuknak az általános biztonsággal kapcsolatos szabályaik szinte genetikailag kódoltak: a gyermek, a lakás, az értékek védelme hosszú évek tapasztalata alapján, illetve korábbi generációk által átadott szokások, szabályok által determináltak. A szabályok külső hatások által változnak, illetve változhatnak, de általában csak kis mértékben – néha csak a technikai lehetőségek fejlődése mentén – finomhangolódnak.

7. Munkahelyi, dolgozói biztonság

A munkahelyi, dolgozói biztonság nagymértékben befolyásolt azáltal, hogy a munkahelynek milyen a vállalati kultúrája, a foglalkoztató mennyire kitett biztonsági kihívásoknak, mennyire volt korábban érintett rendkívüli eseményekkel, illetve mennyire korszerűen előrelátó. Összetett folyamatokról beszélünk, hiszen itt már a személyes biztonságon túl megjelenik többek között a vagyonvédelem, vagy az adat- és információbiztonság és egyéb, az adott munkahelyre jellemző biztonsági igények is. A munkahelyi biztonsági kultúra már hatással lehet az egyén magánbiztonságára is.

8. Vállalkozásbiztonság

Fontos rögtön tisztázni, hogy a vállalkozásbiztonság nem egyenlő a vállalatbiztonsággal. Az eltérés formailag csak pár betű, de a tartalomban óriási. A vállalkozásbiztonság a vállalkozás teljes működési vertikumáért felel. A működési környezet, az emberi tényezők, a munkavállalók, a beszállítók, alvállalkozók, a termékek piaci helyzete, versenytársfigyelés, kereskedelem, marketing, szállításbiztonság folyamatos monitoringozása, a belső és külső visszaélésekkel szemben való fellépés, a folyamatos működés, szolgáltatás vagy termelés biztosítása is a feladata. Nagyon széles körű, sok területet átfogó tevékenység. A nemzetközi és hazai tapasztalatok alapján a komplex üzleti hírszerzés – annak offenzív és defenzív területe – a letéteményese ennek a legmagasabb szintű vállalati biztonsági kultúra kialakításának. Természetesen ez nagymértékben tudja befolyásolni a benne részt vevő, illetve érintett személyek biztonsághoz való hozzáállását. Egy vállalaton, munkahelyi közösségen belül a biztonsági tudatformálás során meg kell élni azt és meg kell harcolni azért, hogy a fejekben eljussunk a „vállalati Gestapótól" a „megkerülhetetlenül szükséges" megítélésig és az ezzel kapcsolatos biztonsági szervezet és a biztonságrezsim elfogadásához.

9. Terrorelhárítással kapcsolatos biztonságtudatosítás

A terrorelhárítással kapcsolatos biztonságtudatosítás területén meg kell próbálni logikai sorba rendezni és eszerint felépíteni a munkánkat. Döntően kétfelé ágazik a munka, a megelőzés-felkészítés és a bekövetkezett események kezelése felé.

a) Megelőzés-felkészítés: általános tájékoztatás, információadás a megelőzés érdekében:

- a terrorizmus mint jelenség története, megjelenési formái, trendjei napjainkban;
- a terrorjellegű cselekmények bemutatása;
- a végrehajtási magatartások, ezek előkészületének felismerése, felismerhetősége, a ráutaló magatartások megismerése;
- a „veled is megtörténhet" gondolat elültetése;
- a terrorcselekményekkel kapcsolatos társadalomérzékenyítési munka a megfelelő szinteken, a szintekhez rendelt és illesztett tartalommal.

Iskoláskortól fontos, hogy a megfelelő formában foglalkozzunk azokkal a kérdésekkel, hogy „mire kell odafigyelni", „mit kell észrevenni", „kinek kell szólni", valamint, „ha megtörténne, mit kell tenni".

Ezekre a gyermek- és fiatalkorban lefektetett alapokra lehet később, már a munka és mindennapok felnőtt világában felépíteni a terrorcselekményekkel kapcsolatos további érzékenyítési feladatokat.

b) A bekövetkezett események kezelése: a „megtörtént és benne vagyunk" helyzet. A munka alapja ez esetben a világban megtörtént események folyamatos és gyors elemzése és értékelése, a jelenségek okainak és körülményeinek feltárása. Ezeket az információkat kell tudnunk ajánlott magatartási szabályokká, viselkedési tanácsokká konvertálni.

A terrormegelőzéssel foglalkozó szakemberek meggyőződése és egyben küldetése is az, hogy egy tartalmas, szakmailag megalapozott, érthető és a gyakorlatban felhasználható információs csomaggal segítsük az emberek mindennapjait. Ezzel kapcsolatban a TEK által kiadott *Mindennapi biztonság* című kézikönyv[9] (megelőző-védelmi ajánlások) letölthető a TEK honlapjáról e-book-formátumban. Előszavában Hajdu János r. altábornagy, a TEK főigazgatója így fogalmazott:

> „Valami megváltozott Európában. A 2015 novemberében Párizsban kezdődött terrortámadás-sorozat alapjaiban átformálta a kontinens biztonsági viszonyait. A terrorszervezetek aktivitása, a rendszeres támadások, az elkövetői magatartások változása, a magányos elkövetők nagyobb számú megjelenése más típusú rendvédelmi válaszokat igényelt. Az elkövetők, a véghezvitt cselekmények körülményei, a támadott létesítmények és a rendezvények egyértelműen jelzik, hogy fokozni kell a párbeszédet a társadalmi csoportokkal, és törekedni kell az állampolgári biztonságtudatosság kialakítására, gondozására."

A terrorelhárítással és -megelőzéssel kapcsolatos fejtegetések végéhez közeledve fontos megemlíteni egy dilemmát. Képletesen fogalmazva: a „mit miért" kell csinálni kérdés körvonalazódik, a „kinek és hogyan" kell megcsinálnia egyértelmű megválaszolása viszont még várat magára.

A TEK felderítő, elhárító szervezet, amely rendelkezik műveleti, felszámolói és kiemelt személyvédelmi képességekkel és kapacitásokkal. Jelenlegi szervezetében

[9] Lásd: www.tek.gov.hu/letoltes.html

képes arra, hogy tapasztalataival, értékeléseivel, elemzéseivel támogassa a biztonságtudatosítás, a társadalmi érzékenyítés programját. Ennek megfelelő minőségi és főleg eredményes megvalósítása humán és egyéb erőforrásokat igényel. El lehetne gondolkodni azon, hogy ez az irány hogyan épülhetne be a TEK, illetve más nemzetbiztonsági, valamint rendvédelmi szervek életpályamodelljébe. Az évtizedek tapasztalatával rendelkező kollégáink garanciái lehetnének egy szakmailag hiteles, magas színvonalú, tudatformáló programnak. E téma kifejtése már egy következő cikkért kiált.

10. A magánbiztonság esszenciális szerepe

A rendszerváltást követő, elmúlt három évtized során a rendőrség, monopolhelyzetét elveszítve, identitásválságot is előidézett, miközben jónéhány magán- és közösségi rendészeti szervezetet termelt ki. A posztmodern átalakulás, a rendfenntartás pluralizmusa két dolgot jelentett egyszerre: egyrészt az állami rendészeti monopólium megtörését, másrészt a magánbiztonsági és polgári rendfenntartás előtérbe kerülését, jelentős növekedését.[10] A szabad piacgazdaság és a magántulajdon rendszerváltást követő térnyerése és rohamos ütemben növekvő védelmi igénye pedig, szükségszerűen hívta létre az üzleti alapon működő, a közbiztonságot kiegészítő tevékenységű és a későbbiekben polgárjogot nyerő magánbiztonsági vállalkozásokat, amelyek – szakmai és üzleti tapasztalataik növekedésével – napjainkra egyre meghatározóbb jelentőséggel bírnak az érték- és vagyonvédelem valamennyi területén. A biztonsági ágazat léte *és növekedése a bizonyíték arra, hogy az állampolgár saját kezébe veszi a biztonságáról való gondoskodást, ezzel visszaveszi a korábban az államra testált jogot.*[11]

Figyelemre méltó, hogy Magyarország már 2008-ban azon tíz európai állam közé tartozott, ahol a piaci nyitás következtében nagyobb létszámban voltak jelen a magánbiztonsági szolgáltatók, mint az állami biztonsági szerveké.[12] 2020-ban a hazai magánbiztonsági vállalkozások száma 6461, míg a kiadott személy- és vagyonőri igazolványok[13] száma 96 008 darab volt.[14]

Legyen bármennyire is felkészült egy magánbiztonsági szolgáltató, eredményességének legszűkebb keresztmetszetét a szolgáltatás leggyengébb láncszeme, a rész(ek) egészre való hatása adja, így a tevékenység stabilitása is – adott esetben – a leggyengébb elem erősségétől függhet. Ennek alapján el kell tudnunk érni, hogy a biztonság

[10] Kerezsi Klára – Nagy Veronika: A rendészettudomány kritikai megközelítése. In Boda József – Felkai László – Patyi András (szerk.): *Ünnepi kötet a 70 éves Janza Frigyes tiszteletére.* Budapest, Dialóg Campus, 2017. 275.

[11] Kerezsi Klára – Pap András László: A bűnözés és a bűnözéskontroll jövője. In Finszter Géza – Sabjanics István (szerk.): *Biztonsági kihívások a 21. században.* Budapest, Dialóg Campus, 2017. 573.

[12] Tóth Judit: Közrendészeti magánbiztonság és magánrendészet közpénzből. *Belügyi Szemle,* 65. (2017), 5.

[13] Vállalkozások (személy- és vagyonvédelmi, magánnyomozói, tervező-szerelő), igazolványosok (személy- és vagyonőr, magánnyomozó, vagyonvédelmi rendszert tervező-szerelő, vagyonvédelmi rendszert szerelő).

[14] Az Országos Rendőr-főkapitányság Rendészeti Főigazgatóság Igazgatásrendészeti Főosztály által biztosított, összesített, 2020. december 31-ei állapotnak megfelelő statisztikai adatok szerint. Christián László – Lippai Zsolt: Kakukktojás vagy új rendészeti alappillér? In *„Tehetség, szorgalom, hivatás": Tanulmánykötet.* Budapest, Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 2021. 18.

mint termék megteremtésében érintett valamennyi szereplő azt sajátjának tekintse, annak folyamatában, kvázi biztonsági szakemberként vállalja magára a rá háruló részt. Egy professzionális magánbiztonsági szolgáltató az egyéni és kollektív biztonsági tudatosság erősítésével szinte észrevétlenül vonja be és teszi – a rá vonatkozó módon és mértékben – érdekeltté a tevékenységében érintett valamennyi személyt a biztonság közös érdekű megteremtésében, a vétkezés előre megakadályozása lehetőségének minimalizálásában.

11. A biztonságtudatosság fejlesztése a magánbiztonságban

Annak felismer(tet)ése, hogy a biztonság megteremtése mindenki felelőssége, amelyben csak közösen érhetünk el érdemleges eredményt, akár már félsikernek is tekinthető. Ugyanakkor fontos, hogy a tudatosság fejlesztését ne a direkt tények, a biztonsági direktívák ismertetésével kezdjük, hanem annak megértetésével, hogy tudatos magatartásunkkal a saját életünket és környezetünket, így családtagjaink, szeretteink életét is biztonságosabbá tehetjük. Értve ez alatt például a lakásajtónk bezárását, a közlekedési szabályok betartását, értékeink megfelelő védelmét, vagy akár az ATM-ből történő pénzfelvételünk körültekintő gondosságát, tehát a gondolkodásunk ilyen irányú átalakulását.

Tudatosítani kell az egyénben, hogy nincsen egyedül, és bár többnyire észrevétlenül, de mindig ott állunk mellette, mögötte, és mindenkor számíthat ránk. Rendelkezésére kell bocsátani az éjjel-nappal működő elérhetőségeinket és elmondani, nincsen felesleges jelzés, csak olyan van, amelyet ő fontosnak érez közös küldetésünk érdekében a tudomásunkra hozni. Ugyanakkor megmutatni azt is, hogy mit és hogyan kell tennie, ha harmadik fél kényszeríti az említett jelzés adására, azt hogyan tudja – saját veszélyeztetése nélkül – a tudomásunkra hozni.

A munkáltató által megkövetelt speciális biztonsági szabályokra a munka-, baleset-, tűz- és egészségvédelmi alapok elsajátítását követően érdemes komolyabb hangsúlyt fektetni, azt a már meglévő alapok kibővítésével kontextusba helyezni. Ez megvalósulhat jelenléti, e-learning vagy blended learning (tematikus, egy-egy témakört felölelő, például iratkezelési, titokvédelmi szabályok, munkahelyi erőszak felismerése stb.) képzések során, amelyek végrehajthatók szervezett munkahelyi körülmények vagy akár önképzés keretében is. A képzéseknek tematikusan egymásra épülően, a biztonság kérdését megfelelő szakmaisággal, a nem biztonsági szakemberek számára is érthető, feldolgozható módon, megtörtént, valós helyzetek elemzésével szükséges felépíteni.

A biztonsággal kapcsolatos intézkedéseket megfogalmazó tájékoztatásoknak, a kiadott brosúráknak, kifüggesztett tájékoztatóknak egyértelmű, egyszerű és biztos üzenetet/üzeneteket indokolt hordozniuk. Bemutatva a veszélyt jelentő vagy annak bekövetkezésére utaló helyzetek felismerésére és beazonosítására vonatkozó, egyértelmű tájékoztatásokat, illetőleg azt, hogy ezen esetekben pontosan mit, mikor és hogyan szükséges megtenni (például, hogy kapcsoljuk ki a számítógépünket, ha elhagyjuk a munkaállomásunkat, csak céges adathordozót csatlakoztassunk, zárjuk

be az íróasztalunk, tárolószekrényünk fiókjait, vagy tűzriadó esetén merre hagyjuk el az épületet stb.).

12. Esettanulmány: biztonságtudatosság a szállodákban

Alan Orlob, a Marriott International[15] szállodaipari óriáscég volt biztonsági igazgatója szerint figyelemmel kell kísérni a terrorizmus változásait és lépést tartani velük, csökkenteni a sebezhetőséget és a szükséges mértékben keményíteni a puha célpontokat. A védelmi intézkedéseket és eljárásokat a változó kockázatokhoz kell igazítani, és ahogy a terrorszervezetek fejlesztik a támadásaikat, a biztonsági szakembereknek fejleszteniük kell a megelőzésükre tett intézkedéseket.[16]

1990-ben, az Amerikai Egyesült Államok panamai inváziója követően Ed Fuller,[17] a Marriott International egykori vezetője érezte először szükségét annak, hogy válságkezelési programot kell kidolgozni a szállodák számára, mert a Marriott szálloda vendégei – válságkezelési terv hiányában – a szálloda mosó- és szárítógépeiben rejtőztek el a panamai katonák elől. A vállalat válságkezelési stratégiájának újabb fordulópontját a 2001. szeptember 11-i terrortámadások jelentették, amikor – az amerikai Homeland Security Advisory System[18]-hez hasonlóan – létrehoztak egy veszélyeztetettségiszint-rendszert, amely öt kategóriába sorolta a veszélyeztetettséget, és a szintekhez kötelező biztonsági intézkedéseket határozott meg.

Felismerték annak tényét, hogy egy potenciális terrortámadás megelőzésében óriási előnyt jelenthet, ha a szálloda alkalmazottai is alapvető biztonságtudatossági ismeretekkel rendelkeznek, észreveszik és jelzik a biztonsági szolgálatnak, ha bármi rendellenességet tapasztalnak. Bár a vállalat szállodái a világ minden részén többnyire eltérő biztonsági környezetben működnek, bizonyos oktatási elemek mindegyikük esetében egyformán jelen vannak. Ezek közé tartozik egyebek közt a válságkezelési terv[19] megismerése és annak tudatosítása, hogy biztonságtudatos magatartásukkal nemcsak a vendégeiket, de egymást is védik.

---

15 A Marriott International a világ legnagyobb szállodaipari vállalataként (több mint 6000 szálloda a világ 122 országában) élen jár a válsághelyzeti protokollok kidolgozásában.

16 Alan Orlob: Protecting soft targets in hostile environments. Recent attacks expose vulnerabilities. *The Guardian, The Source of Antiterrorism Information,* (2009), 11. 7.

17 A Marriott International volt elnöke, tanácsadó, szerző és előadó.

18 Az Amerikai Egyesült Államok belbiztonsági tanácsadó rendszere, egy színkóddal ellátott terrorizmus-fenyegetési tanácsadóskála volt.

19 Minden szálloda válságkezelési terve egyénre szabott, abban általános irányvonalakat lehet felvázolni, de az akár egy városon belüli szállodák között is lényeges eltérések lehetnek. Azok az elemek, amelyeknek célszerűen szerepelniük kellene valamennyi válságkezelési tervben az alábbiak:

- **e**lérhetőségek (a központi szervezet, a szálloda vezetése, hatóságok, hibaelhárító és karbantartó cégek, beszállítók, hivatalok, nagykövetségek, szerződéses partnerek vagy bármilyen más szervezet vagy személy, akivel válsághelyzet esetén szükséges vagy lehet kapcsolatba lépni);
- **é**rtesítési eljárás (ki kit, milyen esetben, miért és hogyan fog értesíteni);
- **a** szállodában tartózkodó személyek (hogyan állapítható meg bármelyik pillanatban, hogy hányan és kik tartózkodnak a szállodában [vendégek, alkalmazottak, látogatók stb.]);
- **a** szálloda válságkezelési szervezetei, azok felépítése, működése, felelőssége;
- **h**ol legyen a szállodában látható biztonsági személyzet (visszatartó erő);
- **s**tratégiai pontok válsághelyzet esetén (vezetési pont, kiürítési pont, belső kiürítési pont, befogadó pontok és mindezek másodlagos vagy harmadlagos helyszínei);

A személyzet tagja az első biztonsági ismereteket átadó képzést a felvételét követően, de még munkába lépése előtt kapja meg, amely oktatás alapesetben évente egyszer, két óra időtartamban, illetőleg speciális ismeretek átadásának szükségessége – például rendkívüli események, terrortámadások bekövetkezése – esetén három-négy óra időtartamban, a munkaidő terhére valósul meg.

Az oktatások során a szállodalánc által, egységes szempontrendszer alapján felkészített – sok esetben rendészeti, harctéri, terrorelhárítási gyakorlattal rendelkező – magánbiztonsági szakemberek tudatosítják a személyzetben egy esetleges támadás veszélyeit, következményeinek súlyosságát, és felhívják a figyelmüket, hogy a megszerzett ismeretek és azok alkalmazása a magánéletükben is előnyössé válhatnak. A képzések személyre szabottan, az adott beosztásnak megfelelő általános és speciális ismeretek készségszintű elsajátítását célozva tartalmazzák a szálloda krízismenedzsmenttervének és biztonsági protokolljainak ismertetését, a vészhelyzeti teendőket, az elkövetők módszereit és azok felismerését, valamint beszélnek a terrorizmus átalakulásáról, az új típusú veszélyekről, azok felismeréséről és jelzéséről. Megfelelő felkészítés esetén ugyanis ez a személyzet fogja képezni a szálloda biztonságának egyik hatékony jelzőrendszeri pillérét, ők lesznek azok, akiknek először feltűnik, ha a közvetlen munkakörnyezetükben bármi változás vagy gyanús esemény történik, hiszen ők ismerik legjobban az adott környezetet.[20]

A képzés kiemelt elemeként szerepel az egyes bűncselekményi kategóriák elkövetésének, valamint az azok elkövetésére történő előkészítő cselekmények felismerésének, többnyire megtörtént esetek,[21] illetőleg a Mariott munkatársai által elkészített, alábbi témákat feldolgozó oktatófilmek bemutatása és az adott munkakörnek megfelelő elemzése:

- ismeretlen személyek hosszabb ideig vagy visszatérően megjelennek az épület körül;
- elhagyott gépjármű az épület környezetében;
- rendszámtábla nélkül vagy piszkos, nem látható rendszámtáblával érkező jármű;
- túlsúlyos jármű;
- csomagok nélkül, vagy feltűnően sok vagy nehéz csomaggal érkező szállóvendég;
- az időjáráshoz képest feltűnően vastag ruházatban lévő személy;
- elhagyott csomag a szálloda területén;

- gyakorlatok válsághelyzetre való felkészülésre (hogyan, mire és milyen gyakorisággal);
- az épülettel kapcsolatos információk (az épület szerkezetéről, az elektromos, légtechnika-, gáz-, víz-, informatikai, biztonságtechnikai, kommunikációs stb. rendszerekről);
- válsághelyzeti tartalékok (mi, hol és milyen mennyiségben);
- események rögzítése (mikor, hogyan és ki által);
- biztonsági protokollok konkrét vészhelyzetekre (természeti csapások, bűncselekmények, tűz, robbanás, zavargás, kiürítés, műszaki meghibásodások, balesetek, egészségügyi vészhelyzetek, terrorcselekmények);
- károk felmérése és helyreállítás (hogyan, miből, ki által, mennyi idő alatt).

20 Lippai Zsolt – Thieme-Eső Milán: A szállodák, mint „puha célpontok”. In *Közös kihívások – egykor és most. Tanulmánykötet.* Budapest, Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 2020. 175.

21 Értve ez alatt a Mariott szállodalánc elleni, már bekövetkezett terrorcselekmények (Pakisztán Islamabad 2008. 56 halott, 265 sérült; Amman Jordánia 2005. 60 halott, 115 sérült; Mumbai India 2008. 166 halott, több mint 300 sérült) eredeti felvételei, valamint a cselekmények előkészületének, végrehajtásának, utóéletének és egy lehetséges terroristatámadási ciklus részletes elemzését.

- vendég, aki készpénzzel fizet olyan nagyobb tételekért, amelyekért rendszerint bankkártyával szokás fizetni;
- ha bárki nem vendég számára szükséges információkat kérdez a személyzettől;
- az épületet fényképező vagy arról rajzokat készítő személyek;
- vendégszobában hagyott nagyobb mennyiségű készpénz, térképek, alaprajzok, kábelek, elemek, fém alkatrészek, vegyszerek, lőszerek, lőfegyver vagy lőfegyveralkatrészek, rádiókommunikációs eszközök;
- „*Ne zavarjanak*" tábla kitéve az ajtóra 24 óránál hosszabb ideig;
- idegen személyek üzemi területen azonosító nélkül stb.[22]

Itt kell megemlítenem a szállodalánc „See something? Say something!" azaz „Látsz valamit? Mondj valamit!" programját, amelynek alapjait a személyzet valamennyi tagja az ismétlődő oktatások során sajátítja el. A program részeként a vendégtértől elzárt, a szálloda személyzete által bejárt részeken figyelemfelhívó színes ábrák vannak elhelyezve a biztonságtudatossági képzés főbb elemeit tartalmazó képekkel és azok szöveges magyarázatával. Egy a szállodai vendégtérben elhagyott csomag fotója alatt például a szöveg: „Elhagyott csomag", illetőleg fegyver, kábítószer vagy gyanús tárgyak fényképe és leírása stb.

Összegzésképpen elmondható, hogy – a biztonság komplex és sokrétű jellegének megfelelően – a biztonsági tudatosítás során a nemzetbiztonsági, terrorelhárítási és magánbiztonsági szervek hasonló módszertan alapján és hasonló vagy sok esetben azonos célok elérése érdekében tevékenykednek. Érzékenyítő tevékenységük során átvehetik és testreszabhatják egymás módszereit. Munkájuk ezzel együtt vagy ettől függetlenül egymást kiegészít(het)i és támogat(hat)ja. Tevékenységük együtt vezet el mindannyiunk nagy becsben tartott közös kincséhez: a komplex biztonsághoz.

Felhasznált irodalom

Christián László – Lippai Zsolt: Kakukktojás vagy új rendészeti alappillér? In *„Tehetség, szorgalom, hivatás": Tanulmánykötet.* Budapest, Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 2021. Online: https://doi.org/10.37372/mrttvpt.2021.1.1

Görgényi Ilona – Gula József – Horváth Tibor – Jacsó Judit – Lévay Miklós – Sántha Ferenc – Csemáné Váradi Erika: *Magyar büntetőjog általános rész.* Budapest, 2019.

Kádár Gyula: *A Ludovikától Sopronkőhidáig*. Budapest, Magvető, 1984.

Kerezsi Klára – Nagy Veronika: A rendészettudomány kritikai megközelítése. In Bofa József – Felkai László – Patyi András (szerk.): *Ünnepi kötet a 70 éves Janza Frigyes tiszteletére.* Budapest, Dialóg Campus, 2017.

Kerezsi Klára – Pap András László: A bűnözés és a bűnözéskontroll jövője. In Finszter Géza – Sabjanics István (szerk.): *Biztonsági kihívások a 21. században.* Budapest, Dialóg Campus, 2017.

[22] Lippai et al. (2020): i. m. 174–175.

Lippai Zsolt – Thieme-Eső Milán: A szállodák, mint „puha célpontok”. In *Közös kihívások – egykor* és *most. Tanulmánykötet.* Budapest, Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 2020. Online: https://doi.org/10.37372/mrttvpt.2020.1.9

Orlob, Alan: Protecting soft targets in hostile environments. Recent attacks expose vulnerabilities. *The Guardian, The Source of Antiterrorism Information,* (2009), 11. Online: www.hsdl.org/?view&did=706275

Tóth Judit: Közrendészeti magánbiztonság és magánrendészet közpénzből. *Belügyi Szemle,* 65. (2017), 5. 5–24. Online: https://doi.org/10.38146/BSZ.2017.5.1

NEMZETBIZTONSÁGI SZEMLE
9. évfolyam (2021) 4. szám 18–34. • DOI: 10.32561/nsz.2021.4.2

Dobák Imre[1] – Babos Sándor[2]

A biztonságtudatosítás lehetőségei a 21. századi platformok fényében[3]

Opportunities for Security Awareness Activities in the Light of 21st Century Platforms

A biztonsági ágazat szereplői napjainkra már széles körben alkalmazzák a biztonságtudatosítás, internet világához és a digitális platformokhoz illesztett megoldásait, amelyek folyamatos fejlődésen mennek keresztül. Számos kutatás ismertette az IKT-eszközök és az e-learning-megoldások meghatározó szerepét, amelyek mellett azonban számos területen (különösen a biztonsági területeken) a közvetlen, személyes megoldások továbbra is kiemelt jelentőséggel bírnak. Ennek okai között jelennek meg, hogy az IKT-környezet már önmagában is a biztonságtudatosítás és az információbiztonság vizsgálati területeként jelenik meg (gondoljunk csak az online oktatással párhuzamosan felerősödő, kibertérből érkező veszélyekre, kihívásokra). A tanulmány a biztonságtudatosítási programok belső tartalmától, irányultságától függetlenül kívánja áttekinteni és tipizálni a napjainkban látható megoldásokat, előtérbe helyezve a 21. századi digitális platformok még hatékonyabb alkalmazásának kérdéskörét, valamint a fiatalabb generációkat is megszólító megoldások fejlődését. A hagyományos biztonságtudatosítási módszerek mellett a kibertérben való aktív részvétel (interakció), a speciális csoportok megszólításának lehetősége, valamint a programok tervezésekor figyelembe veendő módszertani szempontok feltárása olyan területek, amelyek kutatásra érdemesek.

Kulcsszavak: *biztonság, biztonságtudatosítás, nemzetbiztonság*

Security actors are now widely using the security awareness solutions adapted to the internet and digital platforms, which are constantly evolving. Numerous studies have described the crucial role of ICT tools and e-learning solutions, but in many areas

[1] Egyetemi docens, Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet; e-mail: dobak.imre@uni-nke.hu
[2] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola; e-mail: babos.sandor@uni-nke.hu
[3] A mű TKP2020-NKA-09 számú projekt a Nemzeti Kutatási Fejlesztési és Innovációs Alapból biztosított támogatással, a Tématerületi Kiválósági Program 2020 pályázati program finanszírozásában valósult meg.

(especially security), direct, face-to-face solutions remain of paramount importance. One reason for this is that the ICT environment is itself an area of security awareness and information security as well (think of the threats and challenges from cyberspace, which have increased in parallel with online education.) Regardless of the internal content and orientation of security awareness programs, the study aims to review and typify the awareness forms that can be seen today, focusing on the more effective use of 21st century digital platforms and the development of solutions that also address younger generations. In addition to traditional security awareness methods, the active participation (interaction) in cyberspace, the possibility of addressing specific groups, and the exploration of methodological aspects to be taken into account when designing programs are areas worthy of research.

Keywords: *security, security awareness, national security, cybersecurity*

1. A „biztonságtudatosítás" mint vizsgálati terület

Az elmúlt évtizedekben a szakirodalomban egyre nagyobb teret nyert a biztonságtudatosítás jelensége, amelynek mögöttes tartalma, a biztonság különböző elemeinek, szempontjainak figyelembevételére történő felhívás azonban nem napjaink terméke. Mivel a biztonság fogalma is rendkívül összetett, és az egyéni szinttől kezdve egészen a nemzetközi színtérig értelmezhető, a „biztonság növelésének" szempontjaira felhívó megoldások is rendkívül sokrétűek. Az egyéni szintet tekintve gondoljunk csak az olyan technikai eszközök használatára, ahol a biztonsági óvintézkedések figyelmen kívül hagyása súlyos veszélyeket okozhat, majd az érintettek körét növelve egy nagyobb üzem, szervezet biztonsági intézkedéseire, de még továbblépve idesorolható egy-egy biztonságot befolyásoló jelenséghez (például terrorizmus, szervezett bűnözés vagy akár a globális szintű pandémia) kapcsolódó egyéni vagy csoportos szintű tudatos viselkedésre való felhívás.

A biztonságtudatosítás *(awareness)* fogalmi értelmezése kapcsán több meghatározással is találkozhatunk, amelyekben alapvetően egy adott személy vagy csoport valamely biztonságot befolyásoló tényezőhöz kapcsolódó ismereteinek szempontjai és a védelemhez szükséges hozzáállása jelennek meg. A biztonságtudatosítási programokat a hétköznapok során gyakran egyszerűen képzésként értelmezik, azonban számos elemében attól eltérő tevékenységről beszélhetünk. Helyét és szerepét keresve Krasley hivatkozza munkájában[4] a NIST 800-16 (1998) dokumentumot,[5] ahol a kifejezés kapcsán megfogalmazzák, hogy: „A tudatosítás nem képzés. A tudatosítási előadások célja egyszerűen a figyelem biztonságra történő irányítása. […] A figyelemfelkeltő

[4] Paul F. Krasley: *A study of security awareness information delivery within the defense intelligence community.* A Dissertation Presented in Partial Fulfillment Of the Requirements for the Degree Doctor of Philosophy. Capella University, 2010.

[5] National Institute of Standards and Technology Special Publication 800-16: *Information Technology Security Training Requirements: A Role- and Performance-Based Model.* Gaithersburgh, U.S. Department of Commerce, 1998.

tevékenységekben a tanuló az információ befogadója, míg a képzési környezetben a tanuló aktívabb szerepet játszik."[6] A sajátosságokra példaként az Egyesült Államok védelmi területének értelmezéseit emeljük ki, ahol a biztonsági képzések *(security training)* azok a hivatalos tevékenységek, termékek és szolgáltatások, amelyek célja a személyek biztonsági ismereteinek vagy készségeinek megteremtése vagy fejlesztése, illetve teljesítményük, motivációjuk vagy működésük színvonalának növelése.[7] A biztonsági tudatossággal kapcsolatos képzés (*security awareness training*, SAT), ezzel szemben az a tevékenység, amely során

> „tájékoztatják a személyzetet, beleértve a szerződő feleket és az ügynökség működését és eszközeit támogató információs rendszerek egyéb felhasználóit, a tevékenységükhöz kapcsolódó információbiztonsági kockázatokról; és felelősségükről az ezen kockázatok csökkentésére tervezett ügynökségi politikák és eljárások betartásában."[8]

A biztonságtudatosítás során fontos szempontként jelenik meg, hogy az az egyén szintjét kívánja megcélozni, vagy összességében a szervezeti szintű biztonságtudatosságot kívánja növelni. Habár az utóbbi feltételezheti az elsőt, a csoportszintű tudatosságban már kiemelt szerep jut a szervezeti kultúrának, értékeknek, ami a szervezet oldaláról elvárásként fogalmazódik meg az egyén irányába. A szervezeti szintű biztonságtudatosság így nem nélkülözheti az egyének szintjén jelentkező tudatosságot, és végeredményként az egyének összesített biztonságtudatossága jelenik meg.

Míg a szervezeti tudatosság középpontjában a szervezet mint integrált egység összesített tudása és hozzáállása áll, az egyéni tudatosság figyelmének középpontjában inkább az egyes szervezeti tagok ismerete és az adott fenyegetéssel kapcsolatos, előírt szervezeti politikával kapcsolatos attitűdök és a fenyegetéscsökkentés állnak. Másképpen fogalmazva, a szervezeteket nem feltétlenül az érdekli, hogy tagjaik általában tisztában vannak-e a problémával, hanem inkább az, hogy tagjai tisztában vannak-e azokkal az utasításokkal, amelyekről a szervezet szeretné, hogy tájékozódjanak.[9]

A szervezeti tudatosság és az egyéni tudatosság közötti különbség azt jelzi, hogy az utóbbi csak akkor vizsgálható, ha az előbbi jelen van. Más szóval, ha az egész szervezet mint egységes szereplő nincs tisztában egy adott fenyegetéssel, akkor nem lehet szervezeti politikát kidolgozni erre a fenyegetésre. Az egyéni tudatosság értelemszerűen hiányzik, mivel a szervezet egyes tagjainak nincs tudomása arról.

Reveraert és Sauer, más szerzőket hivatkozva hívják fel tanulmányuk bevezetőjében a figyelmet a tudatosítási megoldások kapcsán annak egy sajátos, azonban nagyon fontos megközelítésére. Mint megfogalmazzák, a meglévő „tipológiák" megkülönböztetik a problématudatosítás *(problem awareness)* és a megoldástudatosítás

---

6 Mark Wilson (szerk.): *Information Technology Security Training Requirements: a Role- and Performance-Based Model.* Gaithersburg, Information Technology Laboratory, National Institute of Standards and Technology, 1998.

7 US Department of Defense Instruction Number 3305.13 December 18, 2007. 2.

8 Lásd: FISMA 2002 PLAW-107publ347.pdf

9 Felix J. Haeussinger – Johann J. Kranz: *Information security awareness: Its antecedents and mediating effects on security compliant behavior.* Paper Thirty Fourth International Conference on Information Systems, 2013. 1–16.

(solution awareness), illetve a leíró tudatosítás *(descriptive awareness)* és az előíró tudatosítás *(prescriptive awareness)* típusait.[10] Ennek jelentősége a biztonságtudatosítás során kiemelten fontos, hiszen a biztonságtudatosító tevékenység nem biztos, hogy minden esetben választ kíván és tud adni egy-egy biztonsági fenyegetésre, így ekkor célja az arra történő figyelemfelhívás. Azzal, hogy tisztában vagyunk egy-egy olyan problémával, amely a biztonságunkat valamilyen módon fenyegeti, az még nem eredményezi közvetlenül, hogy annak elkerülése, kiküszöbölése számunkra biztosan lehetővé válik. *A biztonságtudatosítás célja azonban a fenyegetés, veszély ismerete révén a biztonság valamilyen mértékű növelése.*

Jelen tanulmány ennek a tudatosító tevékenységnek napjainkban látható főbb típusait,[11] platformjait kívánja áttekinteni, elvonatkoztatva a biztonságtudatosítással érintett tevékenység belső tartalmától és irányaitól, azonban a nemzet(biztonsági) tématerülethez[12] kapcsolódva példáinkat erre a szegmensre irányítottuk. Célunk, hogy elősegítsük a tágan értelmezett biztonságunkat növelő ismeretek kívánt célcsoporthoz történő eljuttatásának további fejlődését, a leghatékonyabb módszerek megválasztását.

2. A biztonságtudatosítási tevékenység kategorizálása

A történelemben visszatekintve, a biztonságtudatosítás módszerei mindig alkalmazkodtak az adott korszak lehetőségeihez, amelyek köre a megjelenő információtovábbítási megoldások, formák fejlődésével párhuzamosan bővült. A biztonság, nemzetbiztonság kérdésköréből merítve már a 20. század elejének konfliktusokkal terhelt időszakában is találhatunk példákat, gondoljunk csak az ellenség kémtevékenységére felhívó plakátokra és az elvárt viselkedést ismertető hirdetményekre.[13] A század második felére a gyakorlat hátrébb szorult a nyilvános felületekről, azonban a hidegháborús biztonsági gondolkodásban és az érintett szervezetek biztonsági felkészítésében továbbra is meghatározó maradt. Gyakorlati elemei között elsődlegesen a személyes

[10] Tanulmányában a szerzőpáros a már vázolt tipológiák ismeretében új, 4 elemű tipológiát alkotott, amelynek elemei:
- *cognitive awareness of the threat* (a fenyegetés kognitív tudatossága, ahol az érintett ismeretekkel rendelkezik a fenyegetés jellemzőiről);
- *attitudinal awareness of the threat* (a fenyegetés attitűdbeli tudatossága azt jelzi, hogy a szereplő milyen attitűddel viszonyul a fenyegetéshez, és milyen annak a mértéke);
- *cognitive awareness of the mitigation* (a fenyegetések mérséklésének kognitív tudatossága, vagyis a tudás a fenyegetés elleni intézkedésekről);
- *attitudinal awareness of the mitigation* (az attitűdbeli tudatosság a fenyegetés mérsékléséről, ami a fenyegetés mérsékléséhez való viszonyt jelzi [attitűd – motiváció]).

Mathias Reveraert – Tom Sauer: A four-part typology to assess organizational and individual security awareness. *Information Security Journal: A Global Perspective,* 2020.

[11] Fontosnak tartjuk megjegyezni, hogy a biztonságot szem előtt tartó viselkedésre történő figyelemfelhívás az élet szinte minden területén jelen van, a közlekedéstől kezdve az információbiztonság-tudatosító tevékenységig. Az egyes területek számos eltérő sajátossággal rendelkeznek, így a tudatosító tevékenységre – amelyeknek igazodnia kell a tevékenység jellegéhez, valamint az elérni kívánt célcsoporthoz – általánosan elfogadott legjobb megoldás nem adható.

[12] A tanulmány a biztonságtudatosítási oktatásmódszertani kérdéseinek kutatása témakörében, a Nemzetbiztonsági Intézet kutatási irányához kapcsolódik.

[13] Lorenzo Franceschi-Bicchierai: The NSA Just Released 136 Historical Propaganda Posters. *Vice,* 2018. június 4.

kontaktust igénylő szóbeli tájékoztatás-felkészítés, és a szabályzatok mentén történő oktatás volt meghatározó. A biztonságtudatosság elemei között gyakran találkozhattunk a hagyományos értelemben vett rezsimintézkedések területeivel is, amelyek jól jelzik, hogy azok már a 20. század során is széles körben jelen voltak akár az állami szereplők, akár az üzleti élet működésében.

A tudományos gondolkodásban vélhetően az üzleti-gazdasági szektorban megjelenő információk védelmének hangsúlyossá válása segíthette – főként az utóbbi 20 évben – a témakör szélesebb körű vizsgálatát. Változást jelentett továbbá a század végén átalakuló biztonsági környezet, az új típusú kihívások és veszélyek felértékelődése, valamint a társadalom felé történő nyitás is. Ezzel párhuzamosan megjelentek azon technológiai megoldások is, amelyek lehetővé tették, hogy a biztonságot növelő ismereteket a megcélzott társadalmi csoportokhoz gyorsabban eljuttassák, azokat megszólítsák. Az internet térhódításával párhuzamosan mind technikai, mind módszertani értelemben új megoldások jöttek létre, amelyek már meghatározzák napjaink „biztonságtudatosításának" újszerű formáit. Sajátos elemként jelenik meg a hagyományos biztonságtudatosítási módszerekkel szemben a kibertérben megjelenő passzív és aktív közreműködés (interakció) kérdése is, az adott rétegek, csoportok megszólíthatóságának, a programok kialakításánál figyelembe veendő oktatásmódszertani szempontok későbbi feltérképezése.

Mint a bevezetőben kitértünk rá, a biztonságtudatosító tevékenységek számos választóvonal mentén csoportosíthatók, ahol jelen tanulmány az információk célcsoportokhoz történő eljuttatásának módja szerinti felosztást alkalmazza. Ennek alapján a biztonságtudatosítás tevékenységét a tanulmány szerzői a következőkben felállított 3 alaptípus alá sorolják be, és kívánják áttekinteni:

1. közvetlen, személyes jelenléttel járó, valós időben végzett információátadás (például biztonságtudatosítási előadás, tájékoztató, gyakorlati bemutató);
2. a média hagyományos megoldásaira építő információátadás (például plakát, nyomtatott felkészítő anyagok, audiovizuális megoldások, oktatófilmek);
3. a digitális térben végzett információátadás különböző formái.

2.1. A biztonságtudatosítás közvetlen (személyes) formájának főbb sajátosságai

Az információtovábbítás e módszere a legalapvetőbb, napjainkban is előszeretettel alkalmazott formája. Ennek során az információt átadó és vevő között az akár kétoldalú, akár csoportos jelleggel tartott megoldásnál rendkívül fontos az információk közlésének módja, amely alapvetően az oktatás hagyományos elveire épít (megismertetés–szemléltetés–cselekedtetés). Ennek során az információt átadó biztos abban, hogy a szükséges információk közlésre, és azok – valamilyen mértékben – a fogadó fél részéről megismerésre kerültek. A megoldás sajátos, hatékonyabb formája, amikor az *ismeretek közlése gyakorlati elemekkel, a személyes tapasztalás lehetőségével egészül ki.*

A biztonságtudatosító megoldások közvetlen formáját napjainkban is (például biztonsági szervezetek) előszeretettel alkalmazzák, hiszen az átadni kívánt információt csak és kizárólag az érintetti kör részére adják át (például minősített információk

átadása). A szélesebb csoportok irányába történő, nyílt információk továbbítására azonban lehetőséget biztosíthatnak a tájékoztató jellegű előadások. Idesorolhatók ezek gyakorlati elemekkel kiegészített változatai, vagy akár a biztonsági jellegű gyakorlatok végrehajtása, amelyek információátadási hatásfoka – a megcélzott kör bevonása miatt – még nagyobbnak tekinthető. Példaként gondoljunk egy, pusztán a szóbeli közlés lehetőségével élő tűzvédelmi előadásra, vagy egy elsősegélynyújtó előadásra, illetve az utóbbi esetében egy gyakorlati elemekkel kiegészített felkészítés hatékonyságára. Az egyéni gyakorlati tapasztalás szerepét hangsúlyozva másik példaként, a biztonsági ágazat intézményeinél gyakorta találkozhatunk az irodák biztonságához kapcsolódó különböző szempontokkal. Ki ne emlékezne az irodaajtó zárásának elvárására, ha néhány perces irodai távolléte után az irodáját zárva találja, és a kulcsot csak a vezetőjétől veheti át, vagy ha egy nyitva felejtett ablak miatt az éjszaka visszahívják, hogy személyesen zárja azt be. A későbbiekben vélhetően jobban emlékszik e szempontokra, mintha csak egy írott anyagban tájékozódott volna az elvárásokról.

A hagyományosnak tekinthető megoldások napjainkban sem hagyhatók figyelmen kívül, hiszen a közvetlen kommunikációs térben végzett figyelemfelhívás bizonyos esetekben sokkal hatékonyabban tudja biztosítani a „címzettek" leggyorsabb és legeredményesebb elérését. Példaként a közlekedésbiztonsághoz[14] köthető biztonságtudatosító elemeket emelhetjük ki, ahol a hazai gyakorlat számos értékes példával szolgálhat. A megállapítás igaz a személyes jelenléttel járó, a biztonság témakörét érintő versenyekre is (például közlekedésbiztonság, kiberbiztonság), ahol akár különböző alapismeretekkel rendelkező célcsoportoknak állíthatók össze célzott programok. Mindezek már számos gyakorlati elemet is ötvözhetnek, amelyek eredményesebben segíthetik az átadott ismeretek tartós rögzülését.

A személyes kommunikációs megoldások ezen előnyei mellett ugyanakkor hátrányként jelenik meg, hogy azok csak szűkebb célcsoport elérését biztosíthatják. Ennek ellensúlyozására, a tudatosító tevékenységgel megcélzott kör bővítését a média megoldásai és az információs társadalomra jellemző egyéb platformok segíthetik. Amíg mindez előnyként a résztvevők körének bővítését eredményezi, hátrányként jelenik meg a gyakorlati elemek alkalmazási lehetőségének beszűkülése. A hagyományos média (például nyomtatott termékek, oktatófilmek) mellett ugyanakkor a kibertér ismét kinyitotta a gyakorlati elemek alkalmazásának lehetőségeit, ahol az interaktivitás felértékelődő szerepét láthatjuk.

Érdekes példákat láthatunk az információbiztonság területéről is, ahol már egy 1998-ban megjelent információbiztonsági képzés kérdéseivel foglalkozó tanulmány[15] is kitért néhány olyan informatikai biztonságtudatosítási eszköztárra, amelynek a technológiai környezet fejlődésének köszönhető módosult megoldásai ma is jelen vannak. Ilyen példaként említik a különböző motivációs szlogenekkel ellátott promóciós ajándékokat, a felhasználó számítógépen történő bejelentkezése során megjelenő, a számítógép képernyőjén felugró biztonsági emlékeztetőt, a biztonságtudatosítási

[14] A közlekedési balesetek veszélyére táblákon, plakátokon történő figyelemfelhívás más megoldásokkal együttesen már komplex biztonságtudatosító tevékenység részeként is értelmezhető.

[15] Wilson (szerk.) (1998): i. m.

videókazetták alkalmazását, vagy akár a plakátokat és szórólapokat, tudatosítási bemutatókat.

2.2. A média hagyományos megoldásaira építő információátadás

A megoldás a közvetlen közreműködéssel járó oktatási megoldás mellett, szélesebb érintetti kört, illetve az információk akár későbbi tartós elérését biztosító forma. Ennek során olyan információk átadását láthatjuk, amelyeket tartósan, többször is felhasználható módon rögzítenek, de szolgálhatnak a biztonságtudatosítás során elhangzottak szemléltetésére, a gyakorlati rész erősítésére is. Gondolhatunk itt egy-egy figyelemfelhívó videó közzétételére, vagy akár önálló oktatófilmek létrehozására. A biztonság kérdéskörénél maradva az első esetében ilyen példákat láthatunk egy közúti baleset bekövetkezéséről, szabálytalanság elkövetéséről szóló videó közzététele esetén, míg az oktatási célú filmekre példaként a rendszerváltás előtti állambiztonsági időszak, színészek bevonásával rendezett, széles körben ismert oktatófilmjei[16] említhetők. Míg előbbi akár az életben megjelenő valós esemény (például figyelemfelhívó videó) bemutatása is lehet, addig utóbbi, meghatározott metodika szerint létrehozott oktatási anyagként értelmezhető.

A szerzők ebbe a kategóriába sorolják a különböző hagyományos nyomdai úton készített információtovábbítási megoldásokat is, így a biztonságtudatosítást szolgáló prospektusokat, szórólapokat, amelyek egy-egy témakörre hívják fel a figyelmet, és adnak útmutatást a biztonság növelése érdekében. Minderre a biztonsági szervezetek oldaláról a nemzetközi színtéren is találunk példákat, de a hazai (nemzet) biztonságért felelős szervek gyakorlatában is alkalmazott megoldás.[17]

2.3. A digitális térben végzett információátadás különböző formái

A 21. század meghatározó jelensége az infokommunikációs eszközök nélkülözhetetlen alkalmazása. A biztonságtudatosítás korszerű elemei az elmúlt évtizedek során folyamatosan alkalmazkodtak ehhez a környezethez, alapvetően a digitális oktatás általános lehetőségeit felhasználva. A különböző online, webes alkalmazások oktatási célú megoldásai már régóta jelen vannak, igazi jelentőségük azonban csak az elmúlt időszakban értékelődött fel. Ennek okai között az egyre szélesebb körű IKT-használatot, a közösségi oldalak napjainkra meghatározóvá vált szerepét, vagy akár az e-learning mint oktatási forma általánossá válását kereshetjük. Nem hagyhatjuk továbbá figyelmen kívül a fiatalabb generációkra jellemző sajátosságokat, ahol a képzéssel érintett csoportok alapvetően a Z generációhoz (1995–2009 között születettek), illetve az Y generációhoz (1980–1994 között születettek) sorolhatók.[18] Sajátos jellemzőjük az IKT-eszközök elterjedt használata, az online térben való szinte

[16] Lásd: www.abtl.hu/szolgaltatasok/nyilt-ter/videok/ab_oktatofilmek
[17] Lásd: https://ah.gov.hu/en/the-awareness-programme/
[18] Kövecsesné Gősi Viktória: *A digitális korszak oktatásmódszertani kihívásai, 2017. Útkeresés és újratervezés.* XXI. Apáczai Napok Konferencia. Conference Paper, 189–200.

állandó jelenlét, az elektronikus formában elérhető információk iránti fokozott igény, amelyek sajátos válaszokat igényelnek a biztonságtudatosító tevékenység oldaláról is. Idesorolható például a fiatalabb generációkra jellemző interaktivitás iránti elvárásra való reagálás, valamint a csoportmunka – akár online térben történő – fejlesztésének további elősegítése. Fontos elem a különböző típusú vizualizációs megoldások növekvő használata, amelyek szintén hatékonyan segíthetik az oktatási célok teljesülését.[19]

Az online megoldások kiemelt szerepét az oktatásfejlesztéssel foglalkozó nemzetközi üzleti szereplők is felismerték és általánosan elterjedt megoldásokat hoztak létre. Itt említhetők a különböző e-learning-keretrendszerek, például a Moodle, vagy az 1998-ban a kölni egyetemen létrehozott nyílt forráskódú Ilias,[20] amely a biztonsághoz kapcsolódó területeken (például NATO-e-learning-rendszer) is jelen van.

Más megoldások a hallgatói interaktivitás, illetve a csoportkommunikáció terén[21] váltak meghatározóvá (ilyen például a több millió felhasználóval rendelkező Socrativ.com, amely minimális képességet biztosító ingyenes változata mellett a szélesebb funkcionalitást biztosító megoldásokat már fizetős változatban teszi elérhetővé). Az interaktív szó jelentését tekintve, „kölcsönös, kétirányú kapcsolaton alapuló" jelentést hordozó definícióval találkozhatunk,[22] amely a kooperatív oktatási formák körében válik fontossá. Ebben az értelmezésben az ismeretek elsajátításának lehetősége nem az egyéni, elkülönült megoldásokon alapul, hanem a csoportos tevékenységeken. A témakörben az elmúlt évtizedben számos kutatás, tanulmány készült, hiszen az interaktivitás lehetőségét rendkívül mértékben elősegítheti a korszerű IKT-környezet.

A számítógéppel támogatott oktatás több fejlődési szakaszon ment keresztül. Már a kezdetben megjelenő modellekben láthatók voltak a ma is ismert és alkalmazott „szerepkörök", vagyis az úgynevezett szakértői modul (a tanítási folyamat szervezőjének funkciója), valamint a tanulói modul, továbbá a multimédiás elemek fokozott használata.[23] Gondolhatunk a vizualizáció jelentőségére is, ahol a hagyományos információmegjelenítési megoldásokat (írott anyagok) kiegészítették például az oktatóvideók. Mindennek hatása azonban még tovább fokozható, ha az adott vizuálisan látható események valamilyen szintű befolyásolására a hallgatóságnak közvetlen lehetősége nyílik. A webalapú összetett interaktív oktatási megoldások elterjedésének köszönhetően ezek módszertana és vizsgálati elemei is sokrétűnek tekinthetők[24] (például problémamegoldás, aktivitás, döntési lehetőség stb.).

A digitális térben végzett oktatás követelményei között fokozottan jelenik meg tehát a közös alkotás (tudásalkotás) és ezen keresztül a fiatalabb generációknál

---

19 Tóth-Mózer Szilvia – Misley Helga: *Digitális eszközök integrálása az oktatásba. Jó gyakorlatok, tantárgyi példákkal, jó gyakorlatokkal.* Budapest, ELTE, 2019.

20 Lásd: www.ilias.de/en/

21 Az interneten számos, különböző funkciókat tartalmazó, a csoportkommunikáció oktatási célú felhasználását segítő megoldás található (például: https:/.doodle.com; https://keamk.com; https://trello.com; https://connect-innovation.com).

22 Lásd: https://idegen-szavak-szotara.hu

23 Tóthné Parázsó Lenke: *Interaktív tanítási-tanulási technikák.* PhD-értekezés. Budapest, Budapesti Műszaki és Gazdaságtudományi Egyetem, 2001. 26–27.

24 Nagy Elemérné – Hampel György – Fabulya Zoltán: A számítógépek oktatási alkalmazásai (Az első oktatógéptől az e-learningig). *Szegedi Tudományegyetem Szegedi Élelmiszeripari Főiskolai Kar, Tudományos Közlemények,* (2001), 22. 205–210.

igényként jelentkező hálózatiság élménye, a tartalomalkotási és véleményalkotási lehetőség, továbbá a folyamatban való, időponttól független részvétel lehetősége.

Napjainkban leginkább a társadalmi környezet egészét érintő információbiztonsági területen láthatjuk a legszerteágazóbb – főként az infokommunikációs platformokon megjelenő – tudatosító megoldásokat. Mindez egyrészt a kibertér biztonsági szempontból történő felértékelődéséhez, kiemelt jelentőségéhez, másrészről magából az infokommunikációs platformok használatából adódhat (vagyis azon a platformon történik a tudatosítás, ahol maga a veszély is jelentkezik.) Ebben a szegmensben kölcsönösen találkozik az állami és az üzleti szféra érdeke, valamint az információs társadalom résztvevőjeként megjelenő egyének elvárásai. Mindezt jól mutatják a hazai és a nemzetközi színtéren zajló folyamatok. Hazánk Nemzeti Biztonsági Stratégiája is kiemeli a felhasználók alacsony információbiztonsági tudatosságának szintjét, „holott a felhasználók megfelelő információbiztonsági tudatossága a kiberincidensek megelőzésének egyik kulcseleme”.[25]

A nemzetközi színtérre kitekintve, az üzleti és állami szféra partnersége kapcsán az Egyesült Államok elnökének 2021-ben, nagyvállalati és képzési vezetőkkel tartott találkozója említhető, amely során a kiberbiztonság javítása érdekében számos ipari és egyéb partner jelentette be többek között a kiberbiztonsági képzések (például Microsoft, Apple, Google, IBM stb.) kiterjesztésének céljait.[26]

3. Alkalmazott módszerek

A témakörben áttekintett szakmai tanulmányokat és az elektronikus felületeken vizsgált biztonságtudatosítási „megoldásokat” tekintve, rendkívül szerteágazó, többnyire komplex megoldásokkal találkozhatunk. Ezek egy része épít a hagyományos eszköztárra, így továbbra is jelen vannak a közvetlen megszólítást biztosító brosúrák és szórólapok, plakátok, a tudatosító napok, események, gyakorlati elemeket tartalmazó versenyek, amelyek hatékonysága függ a megvalósítás kreativitásától. Más részeik már a kibertér platformjaira építve jelennek meg, így például

- a biztonságtudatosítás témakörében webhely működtetése, amely alkalmas az adott témakörre jellemző tudásbázis koncentrálására, aktuális ismeretek megjelenítésére;
- a már említett e-learning-programok, amelyek koncentrált, ugyanakkor különböző szempontok szerint célirányosítható tananyagokkal széles kör elérését biztosíthatják, miközben ellenőrizhetővé válik az adott program elvégzése;
- e-mailek alkalmazása, amelyekkel egyszerűen, gyorsan, tömeges jelleggel széles kör érhető el;
- elektronikus formátumú időszakos hírlevelek, amelyek biztosíthatják az információk ütemezett, akár tematikus átadását, és alapot adhatnak (például szakirodalom ajánlása) az önképzés folytatására;

[25] 163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról, 32. pont.

[26] The White House: *Fact Sheet: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation’s Cybersecurity* (2021. augusztus 25.).

- komplex megoldások. Ilyenek lehetnek például a *Security Awareness Training* megoldások,[27] amelyek felkészíthetik a felhasználókat a biztonságtudatosabb viselkedésre. Az idesorolható, nyíltan elérhető kiberbiztonsággal kapcsolatos oktatási anyagokon túl, az interaktív vetélkedőkkel, tesztekkel, szimulált helyzetekkel kialakított feladatok segíthetik a megcélzott kör minél teljesebb felkészülését.

A tudatosítással foglalkozó képzési terület napjainkra szinte önálló üzleti területté vált, és az általuk létrehozott felületek folyamatosan információkat, oktatási megoldásokat biztosítanak a kiberbiztonsági területen. A legjobb gyakorlatokat keresve e kiberbiztonsági tudatosításra szakosodott üzleti szereplők képzései elemeiben az alábbi sajátosságokat figyelhetjük meg:

- a képzések adott területhez igazodhatnak, figyelembe véve a meglévő ismereteket (skálázható képzések);
- jelen vannak a szimuláció különböző formái;
- jelentős mértékben építenek az e-learning-megoldásokra (ezen belül oktatóanyagok, videók, infografikák);
- képzéseik módszerei között jelennek meg az interaktivitást biztosító megoldások;
- modulrendszerű felépítés, ahol az egyes képzési modulok viszonylag rövid idő alatt teljesíthetők (többlépcsős ismeretátadás);
- folyamatosan bővülő tudásbázis;
- a képzési anyagok mögött széles szakértői támogatás;
- kreatív, figyelemfelhívó, játékos megoldások alkalmazása;
- egymásra épülő, komplett biztonságtudatosítási rendszer;
- ingyenes és fizetős képzési elemek;
- a biztonságtudatosság hatékonyságát tesztelő megoldások.

Fenti, a biztonságtudatosító tevékenység internetes platformokon végzett megoldásai alapvetően a rendkívül dinamikusan fejlődő kiberbiztonság területére jellemzők, köszönhetően a témakörrel foglalkozó piaci szereplők versenyének. Számos elemük azonban, átültetett gyakorlatként, a biztonságtudatosítás egyéb területein is segítheti a tudatosítási célok elérését.

4. A nemzetbiztonsági ágazat

A (nemzet)biztonsági ágazathoz kapcsolódó biztonságtudatosítás kérdéskörében értelemszerűen elkülöníthető két fő irány: a szervezet saját állománya felé történő biztonságtudatosítási megoldások, valamint az adott szervezet feladatrendszerében megjelenő, a külső környezet irányába jelentkező biztonságtudatosító programok (például a terrorizmus, illetve a korrupció elleni küzdelem, elhárítási tevékenységhez

[27] Expert Insights: *The Top 10 Security Awareness Training Solutions For Business* (Updated 2022. január 7.).

sorolható elemek, vagy akár a kiberbiztonság jelentőségének szélesebb körben történő tudatosítása).

Mindkét irány esetében fontosnak tartjuk kiemelni a biztonságtudatosságra negatívan ható hamis biztonságérzet, és így az arra való figyelemfelhívás szükségességének kérdését. Ez eredeztethető egyrészről a veszélyek lebecsüléséből – amely tipikusan a hiányos ismeretekre vezethető vissza –, továbbá abból, hogy az egyén szintjén a felszínes tájékozottság miatt olyan percepciók alakulnak ki, amelyek szerint a biztonság garantálására létrehozott állami szervek vagy magánvállalatok képesek megvédeni a társadalom tagjait az ő közreműködésük, erőfeszítéseik nélkül is. A biztonság fokozása érdekében az állam–magánvállalatok–egyén relációban nem állapítható meg optimális vagy szükséges arányosság, azonban az elmondható, hogy egyik szereplő esetében sem lehet zéró a részvétel. Mindez igaz a terroristacselekmények megakadályozásától a szervezett bűnözői tevékenységen át a kibervédelemig, bár az egyes szereplők feladatai a különböző veszélyekkel szemben más-más arányban és jelleggel jelentkeznek.

4.1. A biztonsági ágazat versus e-learning biztonságtudatosítási platform

A nemzetbiztonsági közösségekben különösen fontos elem a biztonsági szempontok figyelembevétele. Ennek jelentősége napjainkban is jelen van akár a hazai, akár a nemzetközi színtérre kitekintve vizsgáljuk a titkosszolgálatok zárt világát. Ez a zártság többek között annak az erős szervezeti kultúrának is köszönhető, amely a különböző típusú belső biztonságtudatosító tevékenységek során az ott dolgozók tudatosságára hatást gyakorol. Hazai történeti visszatekintéssel a hidegháború éveiben a rendkívül szigorú rezsimintézkedésekre való figyelemfelhívással és az attól való eltérés eredményezte szankciók tudatosításával találkozhattunk, majd később a tudatosítás módszerei közeledtek a kereskedelmi-üzleti szférában is dinamikusan fejlődő megoldásokhoz. Mindazonáltal ezen szervezetekre gyakran sajátos, eltérő megoldások jellemzők figyelemmel a biztonsági szempontok kiemelt jelentőségére. A zártság mellett azonban e szervezetek sem zárkózhatnak el a külvilágtól, hiszen feladatrendszereikben megjelenik az információk megszerzésének és értékelésének, megosztásának a feladata. Általános értelmezésben az egyes országok nemzetbiztonsági rendszereit tekintve több szolgálatot láthatunk, amelyek között, illetve más felek, valamint a döntéshozók irányába jelen van az információk átadásának gyakorlata. Mindez előrevetíti, hogy az információk védelmének szempontjából azonos szintű biztonsági elemek legyenek, ahol az egységes értelmezésben szintén segíthetnek a biztonságtudatosítás különböző megoldásai (például egységes e-learning-tananyag).[28] Az érintett szervezeteknél a biztonságtudatosítás alapvetően két irányú lehet, így a technológiai környezetből érkező fenyegetésekhez kapcsolódó tudatosítás, másrészről az emberi tényezőhöz kapcsolódó veszélyek.

[28] Krasley (2010): i. m.

A szűkebb, ugyanakkor a modern kori veszélyeknek kiemelten kitett területként értékelhető katonai szféra vonatkozásában nemcsak nemzeti, hanem nemzetközi szinten is erőfeszítések figyelhetők meg a minél szélesebb közönséget elérő oktatási platformok fejlesztésére. Az e-learning képzési formák a hazai biztonsági ágazat számos területén már évek óta jelen vannak, gyakran egy nagyobb képzési rendszer részeként (annak kiegészítéseként) kötelező jelleggel teljesítendő – már a biztonságtudatosítás szűkebb területén túlmutató – tananyagot is felölelnek. A nemzetközi színtérre kitekintve a NATO e-learning-rendszere emelhető ki, amely egyszerű autentikációt – jellemzően katonai e-mail-cím megadása – követően szabadon választható, és bizonyos nemzetközi beosztásokhoz elő is írt online tanfolyami lehetőségeket biztosít a biztonság széles körét felölelő területeken. A kurzusok felelősei és fejlesztői jellemzően azon Kiválósági Központok (*Centre of Excellence,* CoE), amelyek az adott szakterületet érintően a szövetség kijelölt tudásközpontjai.[29]

A Kiválósági Központok által a biztonságtudatosság területével kapcsolatban folytatott tanfolyamok széles kört ölelnek fel az egyéni biztonságtudatosság erősítésétől a legmagasabb szintű információbiztonsági szakemberek képzéséig.[30] Fontos megjegyezni, hogy az ilyen, internetes platformokon folytatott oktatási tevékenységek nem foglalhatnak magukban minősített anyagot (ezek feldolgozása kizárólag személyes vagy fizikailag is zárt hálózaton keresztül történhet). A nyíltan elérhető anyagok mindazonáltal megfelelő alapot biztosítanak bármely NATO-beosztásra történő felkészülésre, így az még a küldő országban végrehajtható. A szabadon választható tanfolyamok esetében ugyanakkor nem előfeltétel a NATO-beosztásba helyezés, azt bármely, a szövetségi rendszer haderejébe tartozó katona elvégezheti. Az egyes nemzetek számára mindez erőforrás-megtakarítást is jelent, hiszen a közösségi finanszírozással működtetett Kiválósági Központ naprakészen tartja és minden tagország tapasztalatát bedolgozva szabadon hozzáférhetővé teszi a tananyagot, amely így korszerűnek és gyakorlatiasnak értékelhető.

Magyar viszonylatban megjegyzendő, hogy a közigazgatás egészét, ezen belül különösen a rendvédelmi és a honvédelmi ágazatot érintően az elmúlt években jelentős fejlesztések történtek a virtuális hálózatokon keresztül történő oktatás és vizsgáztatás területén. A rendvédelmi és katonai szférában az előmenetel feltételeként meghatározott vizsgák letétele és az azokra való felkészülés a mindennapi életben is használt, így mindenki számára elérhető hálózatokon keresztül történik. Ugyanez a folyamat figyelhető meg a polgári életben is azzal a különbséggel, hogy a cégek tipikusan kisebb mérete miatt nem saját maguknak fejlesztenek online tananyagot és vizsgarendszert, hanem beiskolázzák munkavállalóikat valamely kifejezetten oktatással foglalkozó szervezet tanfolyamára (gondolhatunk itt akár a Microsoft-minősítés megszerzésére, vagy olyan weboldalakra, mint a Udemy vagy a Coursera).

[29] Például *Cooperative Cyber Defence CoE* – Tallin; *Military Medicine CoE* – Budapest.

[30] Például *cyber defence awareness course* – szabadon elvégezhető tanfolyam; *cyber awareness course for system administrators* – kötelező tanfolyam a rendszergazdák részére.

4.2. A biztonságtudatosítási tevékenység formái

4.2.1. Generális mechanizmusok kialakítása (ismétlődő veszélyekre történő reagálás)

Általános felkészítésen az egyén és a szervezet vonatkozásában is az azonosított veszélyek sematizált, közös jellemzőiből kiinduló oktatást értjük, amelyek megfelelő kiindulópontot teremtenek az elterjedt biztonsági incidensek alapszintű kezelésére (például *social engineering* felismerése, kártékony tartalmak elleni felhasználói szintű védekezés, a fizikai valóságban a tömegrendezvényeken személyes tárgyak biztonsága). A sematizálás alapját a veszélyek közös jellemzői jelentik, amelyekből generális védekezési mechanizmusok vezethetők le és oktathatók. Előző példánkkal élve a social engineering és a kártékony tartalmak terjesztése is felhasználói aktivitást igényel, például egy külső linkre való kattintással. Ugyanez mondható el a mindennapi életben, amennyiben a tömegrendezvényeken és a tömegközlekedés során azonosítható veszélyeket vizsgáljuk, hiszen fizikai tárgyaink biztonsága mindkettő esetében jogellenes elvétellel kerülhet ki tulajdonunkból, ezek ellen pedig hasonló technikákkal védekezhetünk.

A generális mechanizmusok kialakításának elvitathatatlan előnye a viszonylag rövid idő alatt, aránylag nagy mennyiségű veszély elhárítására való felkészítés lehetősége. Hátránya ugyanakkor, hogy a megtanult, esetleg begyakorolt sémák az akár kis mértékben megváltoztatott körülmények esetében is kudarcot vallhatnak, továbbá hamis biztonságérzet kialakulásához vezethetnek. A sematizálás során egy-egy veszély kezelésére történő válaszadás „felelősséggel" is jár a válasz kidolgozója számára, hiszen a biztonságtudatosítás sikere esetén az érintettek az ott megadott magatartásformát fogják követni. Ennek pontatlansága, esetlegesen félreérthetősége téves minták közléséhez vezethet. Mindez azonban már a biztonságtudatosítási programok belső tartalmának kérdéskörét érinti.

4.2.2. Szakterület-specifikus felkészítés (beosztásra, élethelyzetre történő felkészítés)

Mind az állami (például közigazgatás és rendvédelmi szervek, honvédség), mind a polgári szféra (például nemzeti és nemzetközi üzleti szereplők) esetében, elsődlegesen a tevékenység jellegéből és így az arra ható veszélyekből kiindulva, meghatározhatók olyan specifikumok, amelyek különleges, több esetben kizárólag az adott szakterületet érintő biztonsági felkészítést, biztonságtudatosítást követelnek meg. Példaként a bankszektort érintő támadások esetében tipikusan az anyagi javak megszerzését azonosíthatjuk, ugyanakkor a katonai szférában például a válságövezetekben történő feladat-végrehajtás idején a biztonságot veszélyeztető esetleges támadásokra történő felkészülés egyéb, sajátos szempontjai kerülnek előtérbe. A példákból is kitűnik, hogy az egyes szerveket és vállalatokat érintő támadások célja ugyan a rendeltetésszerű, biztonságos működés ellen irányul, ugyanakkor mindez az egyénen és az ő fizikai

és online jelenlétén keresztül valósul meg, még ha más és más információgyűjtési módszerrel is.

Mindez megköveteli, hogy a különböző tevékenységet végző szervezetek esetében különböző, szakterület-specifikus felkészítést dolgozzunk ki. Napjainkban a rendvédelmi szervek és a honvédség tagjai feladat-végrehajtás közben, a korábbiaktól eltérően, azonosító számsort viselnek névtáblájuk helyett, amely biztosítja jogszerű eljárás keretében történő azonosításukat, azonban lehetetlenné teszi azt pusztán a közösségi médiafelületeken keresztül. Ugyanezen célt éri el a szolgálati mobiltelefonok, hívószámok használata, hiszen magántelefon szolgálati célra való felhasználása esetén az online regisztráció és autentikáció miatt ezen keresztül is megtalálhatók lennének.

A szakterület-specifikus felkészítés célja tehát mind az egyén, mind a szervezet, mind a szervezet ügyfeleinek, így végső soron a társadalom védelme, amely az adott beosztást betöltő személy legmagasabb fokú biztonságtudatosításán keresztül érhető el.

5. A biztonságtudatosító tevékenység hatékonyságának mérése

A szakirodalomban, főként az információbiztonsági programok kapcsán, gyakran felszínre kerülő téma, hogy hogyan mérhető az egyes biztonságtudatosító programok hatékonysága. Ennek jelentősége egyrészről az átadott információk valós hasznosulásának megítélése, másrészről az adott tevékenység (például program, figyelemfelkeltő kampány) továbbfejlesztésének és hatékonyságának növelése miatt is elengedhetetlen.

A kérdés, hogy hogyan, milyen metodikával érdemes egy szervezet esetében ennek hatékonyságát mérni. A program által közölt részismeretek megismerését (vizsgáztatás, teszt), vagy pedig hosszabb időtávra kitekintve a szervezet egészében a biztonságtudatosság növekvő szintjét érdemes-e vizsgálni.

A témakör módszertani kérdéseit elemző releváns tanulmány[31] szerint az alkalmazott értékelési módszerek között találhatjuk a kvantitatív (minőségi), a kvalitatív (mennyiségi), illetve a kombinált módszereket. Amíg az elsőnél annak meghatározása történhet, hogy valóban gyakorolják-e a biztonsági tudatosságot, addig a mennyiségi technikánál mérhető teljesítménymutatókat kívánnak létrehozni és azok alakulását vizsgálni. Sajátosságként jelenik meg továbbá, hogy egy-egy szervezetnél a hatékonyság mutatói nem feltétlenül vethetők össze más szervezet mutatóival, hiszen az egyes szervezetek belső folyamatai, szervezeti kultúrája jelentősen eltérhetnek egymástól. A megoldások terén egyfajta megoldásnak tűnik, ha a biztonságtudatosítással érintett kérdéskörben a kezdeti állapotfelvétel biztosít olyan referenciaadatot, amely a későbbi értékelések alapját jelentheti, de gyakran találkozhatunk a kérdőíves

[31] Konstantinos Rantos – Konstantinos Fysarakis – Charalampos Manifavas: How effective is your security awareness program? An evaluation methodology. *Information Security Journal: A Global Perspective*, 21. (2012), 6. 328–345.

vizsgálat, felmérések módszereivel is, valamint a különböző programokon részt vevők létszámához kapcsolódó mennyiségi jellegű szemlélettel.

6. A jövő

A jövőbeni biztonságtudatossággal kapcsolatos tevékenységgel összefüggésben érdemes támaszkodni arra a pedagógiai elméletre, hogy a felkészítés célját a napjainkban jelen levő társadalmi igények, szükségletek határozzák meg. Minden kor társadalma feladatának tekinti, hogy készségszinten átadja azt a korábbi korokban felhalmozott ismeretanyagot, amely nemcsak az egyén, hanem a társadalom egésze számára nélkülözhetetlen. A később ezen az ismeretanyagon felnövekvő nemzedék magáévá teszi a kor által preferált, elvárt szokásokat, erkölcsöt, a társadalomról alkotott nézeteket, végső soron annak egész érzelemvilágát, életszemléletét, és mindennapi tevékenysége során tovább fejleszti, a kor kihívásainak megfelelően magasabb szintre emeli, vagy módosítja ezeket a társadalmi normákat. Természetesen így van ez a biztonságtudatossággal kapcsolatos ismeretanyaggal is. A különbség egyik sajátosságát abban kereshetjük, hogy a biztonságtudatosítás során – annak megnevezéséből is látható módon – a biztonság kérdésköre válik azon tényezővé, amellyel kapcsolatos információt a fogadó fél számára a leghatékonyabb módon át kell adni. Ennek elemei olyan viselkedési, magatartási, illetve egyéb követendő „szabályok", amelyek betartásával növekedhet az egyén, csoport biztonságának szintje. Az átadás formái, platformjai mindig alkalmazkodnak azokhoz a változásokhoz, amelyek az információk leghatékonyabb közlését szolgálhatják. Minderre számos, egyre bővülő eszköztár áll rendelkezésre. Egy, az Egyesült Államokban végzett kutatás alapján[32] bizonyítást nyert, hogy a valóban kiváló képességű vezetők és alkalmazottak a pályafutásuk során fokozatosan fedezik fel azokat a kompetenciafejlesztési módszereket, amelyek sikeressé teszik őket. Az egyik ilyen az önképzés során elsajátított tudás. Ehhez azonban belső motiváltságra van szükség, mert ha valamiféle külső kényszer hatására kezdi el valaki fejleszteni magát, amint a kényszerítő erő megszűnik, a motiváltság is alábbhagy. Igaz ez a biztonságtudatossággal kapcsolatos önképzésre is, ugyanakkor, ha sikerül alapvető értékként alkalmazni, meghonosítani, akkor az önálló tanulás egy jól teljesítő szervezet egyik meghatározó tulajdonságává válhat.

Richard Boyatzis tanulmánya[33] alapján az alábbi folyamat szükséges egy önképzési rendszer sikeres eléréséhez. Ezek egyfajta útjelző táblák az önálló tanuláshoz vezető úton: az elkötelezettség, önismeret, valamint annak megállapítása, hogy milyen tulajdonságokat szükséges megváltoztatni, és ehhez milyen erősségekkel és gyengeségekkel rendelkezünk. Elsősorban szükséges saját, személyre szabott tanulási program kialakítása, majd gyakorlatok végrehajtása az új szokások és cselekedetek megalapozása céljából. Ha az alapok megerősödtek és biztonságban alkalmazhatók, akkor a fennálló társas kapcsolatok saját érdek mentén fejleszthetők és hasznosíthatók

32 Matthew Mangino – Christine Dreyfus: *Developing Emotional Intelligence Competencies.* Cambridge, MA, Consortium for Research on Emotional Intelligence in Organizations, 2001.

33 Richard E. Boyatzis: *Unleashing the Power of Self-Directed Learning.* Weatherhead School of Management, Case Western Reserve University, 2001.

a tanulási folyamatban. Később elkezdhető mások önirányított tanulási folyamatának segítése is.[34] Ez az utolsó folyamat tulajdonképpen végig kell hogy kísérje az összes fázist, hiszen ez segíti a betanulást, mert a kialakult kapcsolatok alapján kapott visszacsatolások mutatják meg, hogy hol tartunk a tanulási folyamatban.

Véleményünk szerint mindezen önképzési folyamatok támogatására a modern szervezetek (ideértve állami és nem állami szereplőket egyaránt) tudatosan, a kor követelményeinek megfelelően folyamatosan készülnek és fejlődnek. A koronavírus-járvány okozta zavar kapcsán ez a folyamat különösen felerősödött, előtérbe kerültek az otthoni munkavégzés melletti otthoni képzések, ismeret-ellenőrzések, amelyek egyéni tempójú, akár egyéni érdeklődést is kiszolgáló ismeretátadást biztosítanak. Mindez ugyanakkor a külső kényszer melletti belső motivációt, fejlődési igényt is megköveteli az egyéntől, amely viszont végső soron nem kizárólag a személy, hanem az egész társadalom biztonsági szintjének fokozásához vezet.

Felhasznált irodalom

Boyatzis, Richard E.: *Unleashing the Power of Self-Directed Learning.* Weatherhead School of Management, Case Western Reserve University, 2001.

Expert Insights: The Top 10 Security Awareness Training Solutions For Business (Updated 2022. január 7.). Online: https://expertinsights.com/insights/the-top-security-awareness-training-platforms-for-businesses/

FISMA 2002. Online: PLAW-107publ347.pdf (govinfo.gov)

Franceschi-Bicchierai, Lorenzo: The NSA Just Released 136 Historical Propaganda Posters. *Vice,* 2018. június 4. Online: www.vice.com/en/article/43548d/nsa-historical-propaganda-posters-foia

Haeussinger, Felix J. – Johann J. Kranz: *Information security awareness: Its antecedents and mediating effects on security compliant behavior.* Paper Thirty Fourth International Conference on Information Systems, 2013. 1–16 Online: www.researchgate.net/publication/258926834_Information_Security_Awareness_Its_Antecedents_and_Mediating_Effects_on_Security_Compliant_Behavior

Kövecsesné Gősi Viktória: *A digitális korszak oktatásmódszertani kihívásai, 2017. Útkeresés* és újratervezés. XXI. Apáczai Napok Konferencia, Conference Paper, 189–200.

Krasley, Paul F.: *A study of security awareness information delivery within the defense intelligence community.* A Dissertation Presented in Partial Fulfillment Of the Requirements for the Degree Doctor of Philosophy. Capella University, 2010. Online: www.proquest.com/openview/681c9da643fb15d61251d2438c44af19/1?pq-origsite=gscholar&cbl=18750

Mangino, Matthew – Christine Dreyfus: *Developing Emotional Intelligence Competencies.* Cambridge, MA, Consortium for Research on Emotional Intelligence in Organizations, 2001.

[34] Boyatzis (2001): i. m. 24.

Nagy Elemérné – Hampel György – Fabulya Zoltán: A számítógépek oktatási alkalmazásai (Az első oktatógéptől az e-learningig). *Szegedi Tudományegyetem Szegedi Élelmiszeripari Főiskolai Kar, Tudományos Közlemények*, (2001), 22. 205–210. Online: http://acta.bibl.u-szeged.hu/39152/1/szef_tudkozl_022.pdf

Rantos, Konstantinos – Konstantinos Fysarakis – Charalampos Manifavas: How effective is your security awareness program? An evaluation methodology. *Information Security Journal: A Global Perspective*, 21. (2012), 6. 328–345. Online: https://doi.org/10.1080/19393555.2012.747234

Reveraert, Mathias – Tom Sauer: A four-part typology to assess organizational and individual security awareness. *Information Security Journal: A Global Perspective,* 2020. Online: https://doi.org/10.1080/19393555.2020.1855374

The White House: Fact Sheet: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity (2021. augusztus 25.). Online: www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/

Tóth-Mózer Szilvia – Misley Helga: *Digitális eszközök integrálása az oktatásba.* Jó gyakorlatok, tantárgyi példákkal, jó gyakorlatokkal. Budapest, ELTE, 2019. Online: http://mindenkiiskolaja.elte.hu/wp-content/uploads/2019/09/Digit%C3%A1lis-eszk%C3%B6z%C3%B6k-integr%C3%A1l%C3%A1sa-az-oktat%C3%A1sba_INTERA.pdf

Tóthné Parázsó Lenke: Interaktív tanítási-tanulási technikák. PhD-értekezés. Budapest, Budapesti Műszaki és Gazdaságtudományi Egyetem, 2001. Online: http://hdl.handle.net/10890/114

US Department of Defense Instruction Number 3305. 13 December 18, 2007.

Wilson, Mark (szerk.): *Information Technology Security Training Requirements: a Role- and Performance-Based Model*. Gaithersburg, Information Technology Laboratory, National Institute of Standards and Technology, 1998. Online: https://doi.org/10.6028/NIST.SP.800-16

163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

Internetes oldalak

www.abtl.hu/szolgaltatasok/nyilt-ter/videok/ab_oktatofilmek
ah.gov.hu/en/the-awareness-programme/
www.ilias.de/en/
https:/.doodle.com
https://keamk.com
https://trello.com
https://connect-innovation.com

NEMZETBIZTONSÁGI SZEMLE
9. évfolyam (2021) 4. szám 35–47. • DOI: 10.32561/nsz.2021.4.3

Mezei József[1] – Koncz Veronika[2] – Jasenszky Nándor[3]

Biztonságtudatosság – hazai helyzetkép, hazai gyakorlat és példák 1.[4]

Security Awareness – Domestic Situation, Domestic Practice and Examples 1

A 21. század elején számos olyan esemény és változás történt a világban, amely jelentős hatást gyakorolt a titkosszolgálatok tevékenységére is. Ezek közül kiemelkednek a nyugati társadalmakat sokkoló terrorcselekmények az Amerikai Egyesült Államokban és Európában, az információtechnológia rohamos fejlődése, valamint ezzel együtt, az ezzel kölcsönhatásban álló információrobbanás. Ezen tényezők egyik következménye lett a biztonságtudatosító programok rendszerszintű megjelenése a nemzetbiztonság területén például a terrorelhárítással és az információvédelemmel összefüggésben. E két részből álló publikáció célja, hogy bemutassa a magyar titkosszolgálatok, illetve a Terrorelhárítási Központ által aktuálisan folytatott ilyen típusú programokat. A publikáció a Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézete által folytatott ez irányú kutatás részeként került összeállításra azzal a céllal, hogy a kutatásban kiindulási alapot biztosítson a nemzetközi példákat is figyelembe vevő, a hazai programok eredményességét elősegíteni kívánó módszertani ajánlásokhoz.

Kulcsszavak: *biztonságtudatosság, nemzetbiztonság, kémelhárítás, információbiztonság, terrorelhárítás*

At the beginning of the 21st century, there were a number of events and changes in the world that also had a significant impact on the activities of the intelligence services. Among these are the terrorist attacks that shock Western societies in the United States of America (USA) and Europe, the rapid development of information technology and the information explosion. One consequence of these factors is the

[1] Tanársegéd, Nemzeti Közszolgálati Egyetem Polgári Nemzetbiztonsági Tanszék; e-mail: Mezei.Jozsef@uni-nke.hu
[2] Alkotmányvédelmi Hivatal; e-mail: konczjuhasz@gmail.com
[3] Vezető, Terrorelhárítási Központ, Társadalmi Kapcsolatok Osztály; e-mail: jasenszky.nandor@tek.gov.hu
[4] A mű a TKP2020-NKA-09 számú projekt a Nemzeti Kutatási Fejlesztési és Innovációs Alapból biztosított támogatással, a Tématerületi Kiválósági Program 2020 pályázati program finanszírozásában valósult meg.

emergence of security awareness programs at the system level in a number of areas that are primarily the responsibility of intelligence services, such as counterterrorism and information security. The purpose of this two-part publication is to present the programs currently being run by the Hungarian secret services and the Counter-Terrorism Centre. The publication was compiled as part of the research carried out by the Institute of National Security of the University of Public Service with the aim of providing a starting point for methodological recommendations that take into account international examples and seek to promote the effectiveness of domestic programs.

Keywords: *security awareness, national security, counter-espionage, information security, counterterrorism*

1. Bevezetés

A nemzetbiztonság körébe tartozó kockázatok, az azzal kapcsolatos események, kiemelten például a más országok titkosszolgálatai[5] által folytatott titkos információgyűjtéssel, közismert elnevezéssel a kémkedéssel vagy a terrorcselekményekkel kapcsolatos esetek bemutatása a társadalom szélesebb köréhez elérő médiumokban már régóta jelen van. Ennek elsődleges oka azonban az ilyen típusú cselekmények társadalom által érdeklődésre számot tartó, hírértékkel bíró mivolta, és nem az emberek bizonyos célok érdekében történő tudatos tájékoztatása a titkosszolgálatok részéről.

Az elmúlt néhány évtizedben olyan változások történtek a világban, amelyek rövid időn belül igen komoly kihívások elé állították a szolgálatokat. Az egyik ilyen a terrorizmus jelenléte Európában[6] és az USA-ban[7], amely a társadalmat sokkoló terrorcselekményeken túl összefüggésbe hozható más, szintén a nemzetbiztonság feladatkörébe (is) tartozó kihívással, így az illegális migrációval, a szervezett bűnözéssel vagy akár a proliferációval. További jelentős változás például az információtechnológia rohamos fejlődése, vagy ezzel összefüggésben, a globalizáció részeként a világ egészét behálózó informatikai hálózatok kiépítése, ami több szegmensében is érinti a nemzetbiztonsági szempontú információ- és adatvédelem kérdéskörét.

A nemzetbiztonsági szolgálatok által a társadalom biztonságtudatosságának fokozása érdekében folytatott tudatosító tevékenysége az általános tájékoztatáson túl több célt is magában foglal. Beletartozik:

- az állampolgárok tájékoztatása a biztonsági kockázatokról;
- nem kötelező érvényű javaslatok, ajánlások megfogalmazása a veszélyhelyzetek megelőzése érdekében és a vészhelyzet bekövetkezése során követendő magatartásra vonatkozóan;

[5] A fogalmat jelen tanulmányban gyűjtőfogalomként használjuk, ide sorolva a hírszerző szervezeteket, a nemzetbiztonsági szolgálatokat, az állambiztonsági szerveket.

[6] 2004. március 11-én Madrid közelében található vasútállomásokon (Terrorists Bomb Trains in Madrid. *History,* 2004. március 11.), majd 2005. július 7-én London tömegközlekedési rendszerét érintően hajtottak végre terrortámadást, amelyekkel összefüggésben több mint 200 ember vesztette életét (Terrorists attack London transit system at rush hour. *History,* 2005. július 7.).

[7] 2001. 09. 11-én az al-Kaida repülőgépekkel támadást intézett az USA-ban, amelynek következtében közel 3000 ember halt meg. (September 11 Attacks. *History,* 2018. augusztus 5.)

- a kölcsönös információcserét lehetővé tevő csatornák kialakítása;
- az esetleges későbbi együttműködés kereteinek megteremtése;
- a szolgálatok iránti bizalom kialakítása;
- a szolgálatok társadalmi elfogadottságának növelése;
- a társadalommal való kapcsolat erősítése.[8]

A biztonságtudatosság növelésének általános célja, hogy az érintett személy valamilyen kockázattal szemben eredményesebben léphessen fel, akár megelőző jelleggel is. Ezt figyelembe véve a titkosszolgálatok közül a társadalmat célzó biztonságtudatosító tevékenységnek elsődlegesen az elhárító szolgálatok által folytatott tevékenységekhez kötötten van létjogosultsága. Ezen szervezetek azok, amelyeknek a nemzet biztonságát veszélyeztető leplezett törekvésekkel szemben megelőző jelleggel kell fellépniük, és meg kell védeniük a nemzet biztonsága szempontjából fontos értékeket. A hatályos nemzetbiztonsági törvény szerint „Magyarország nemzetbiztonsági szolgálatai:

a) az Információs Hivatal,
b) az Alkotmányvédelmi Hivatal,
c) a Katonai Nemzetbiztonsági Szolgálat,
d) a Nemzetbiztonsági Szakszolgálat, valamint
e) a Terrorelhárítási Információs és Bűnügyi Elemző Központ”.[9]

A szolgálatok közül az Alkotmányvédelmi Hivatal mint polgári elhárító és a Katonai Nemzetbiztonsági Szolgálat mint a katonai hírszerzéssel és elhárítással is foglalkozó szolgálat, amely ebből a szempontból figyelmet érdemelhet. Mindazonáltal a szakterületet érintő átszervezések következtében a korábban a Nemzetbiztonsági Hivatal által ellátott terrorelhárítási feladat, amely meghatározó része a nemzetbiztonsági munkának, 2010-ben az akkor létrehozott Terrorelhárítási Központhoz került. További lényeges körülmény, hogy a Nemzetbiztonsági Szakszolgálat az elmúlt években új feladatokat kapott az informatikai rendszerek védelme területén, így napjainkra ezen a téren az egyik, ha nem a legfontosabb szereplővé vált.

A Katonai Nemzetbiztonsági Szolgálat tekintettel arra, hogy feladatai elsődlegesen a katonai területhez köthetők, aktuálisan nem végez a társadalom széles körében biztonságtudatosító tevékenységet, így ebbe a kutatásba nem került bele. Ennek ellenére megemlítendő a 2018-ban, a szolgálat fennállásának 100. évfordulójára, a szolgálat volt és jelenlegi munkatársai által írt *A magyar katonai elhárítás története 1918–2018* című könyv,[10] amely a szervezet történetén keresztül bemutatja a katonai kémelhárítás korábbi és jelenlegi szervezeteit, a katonai elhárítás feladatrendszerét, esettanulmányokkal szemléltetve a problémakör összetettségét, jelentőségét. Vagy a hírszerzés területét is magába foglaló hasonló jelentőségű, szintén a centenárium

[8] Nagy Katalin – Mezei József: A biztonságtudatosítás megjelenése a terrorelhárítás területén. *Nemzetbiztonsági Szemle,* 7. (2019), 4. 105–117.
[9] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról.
[10] Jagadics Péter et al.: *A magyar katonai elhárítás története 1918–2018.* Budapest, Metropolis Media Group Kft., 2018.

alkalmából elkészített kiadvány, amelynek címe: *100 éves az önálló magyar katonai felderítés, hírszerzés és elhárítás 1918–2018.*[11]

A biztonságtudatostó tevékenység eredményessége szempontjából kiemelt jelentősége van többek között annak, hogy az érintett titkosszolgálat és a társadalom milyen kapcsolatban van egymással, mennyire ismertek a szolgálatok, illetve feladataik, továbbá milyen a szolgálatok megítélése az állampolgárok részéről. Itt nem mehetünk el szó nélkül amellett, hogy a magyar államvédelmi/állambiztonsági[12] szervek tevékenységét, vagy annak egy részét, a magyar emberek közül sokan nem minden esetben ítélték meg pozitívan. Ennek egyes hatásai a közbeszédben máig jelen vannak. A jelenre tekintve hasonlóan negatív hatást válthat ki az állampolgárokban az, ha a titkosszolgálatok vagy az általuk végzett tevékenység érdekcsoportok közötti csatározások részévé válik. Ezekre tekintettel, ha a szolgálatok eredményesek akarnak lenni biztonságtudatosító szerepkörükben, úgy tenniük kell azért, hogy a társadalom irányából szükséges támogatottság és bizalom megfelelő szintű legyen.

A biztonságtudatosság eredményessége tekintetében kiemelt jelentősége van, hogy milyen tartalommal, nyelvezettel, milyen felületen, milyen módszerek és eszközök alkalmazásával szólítják meg az állampolgárokat a szolgálatok. Ezek kiválasztása során számos külső tényezőt is figyelembe kell venni, így többek között a szociális viszonyokat, a fordított szocializáció jelenségét, a társadalomban megtalálható generációk közötti jelentős különbségeket, a globalizáció hatásait, az embereket körülvevő információdömpinget, az információtechnológia rohamos fejlődését. Ehhez is köthető a következő hasonlóan fontos szempont, hogy melyek azok a civil vagy állami szervezetek, amelyekkel együttműködve tovább növelhető a tevékenység hatékonysága.

A titkosszolgálatoktól a közelmúltig alapvetően idegen volt a társadalom irányába történő tájékoztatás. A biztonságtudatossági programok alapjaiban új felfogást kívánnak meg a szolgálatoktól, az állampolgárokkal való eddig jellemzően ügyszerű, bizalmas, személyes kapcsolat mellett megjelenik a széles körű, célhoz kötött, de mégis általános, sokszor személytelen együttműködés. Ezt is figyelembe véve, a tevékenység minden irányú legitimitása kapcsán jelentősége van annak, hogy milyen szintű támogatás van e programok mögött, milyen jogszabályok alapján végzik ezeket a tevékenységeket a szolgálatok.

A biztonságtudatosító tevékenység megjelenése a nemzetbiztonsági kockázatok területén nem magyar sajátosság. A terrorelhárítás területén láthatunk rá példát többek között az USA-ban,[13] az Egyesült Királyságban,[14] Izraelben,[15] míg a gazdaság területén jelen lévő ellenséges hírszerző tevékenység kapcsán jó példa lehet a Német

[11] Árvai Zoltán – Gyaraki Károly: *100 éves az önálló magyar katonai felderítés, hírszerzés és elhárítás 1918–2018.* Budapest, Zrínyi, 2019.

[12] A tanulmányban az államvédelmi/állambiztonsági szervek alatt a II. világháborút követő és egészen a rendszerváltásig terjedő időszakban működő magyar titkosszolgálatokat értjük.

[13] Nagy Katalin – Mezei József: Nemzetközi kitekintés a terrorelhárítás területén folytatott biztonságtudatosítási programokba. *Nemzetbiztonsági Szemle,* 8. (2020), 2. 50–65. 52.

[14] Nagy–Mezei (2020): i. m. 55.

[15] Nagy–Mezei (2020): i. m. 58.

Alkotmányvédelmi Hivatal[16] ez irányú programja. Ezek mintaként szolgáltak, illetve szolgálhatnak a továbbiakban a magyar rendszer fejlesztése során.

A dolgozatban a Nemzetbiztonsági Szakszolgálat, az Alkotmányvédelmi Hivatal és a Terrorelhárítási Központ ilyen jellegű programjait tekintjük át annak érdekében, hogy tényszerű kiindulási alapot képezzünk e tevékenységek esetleges további fejlesztéséhez. A dolgozatban rövid kitérőt teszünk a múltba is, annak szemléltetése érdekében, hogy a tudatosítás kézzelfogható lehetőség, amely különböző viszonyok között is alkalmazható, lényegi elemei állandók.

2. Visszatekintés

Az elmúlt évtizedig a magyar társadalom széles köre a titkosszolgálatokról, tevékenységükről, eszközrendszerükről, de magukról a nemzetbiztonsági kockázatokról – néhány kivételtől eltekintve – nem rendelkezett széles körű ismerettel. Egy-egy időszakban azonban, például a nemzetbiztonsági kockázatok számának jelentős növekedése okán, a szolgálatok kilépve az addig megszokott működési mechanizmusokból kísérletet tettek a társadalom bizonyos mértékű bevonására a kockázatokból adódó esetlegesen bekövetkező negatív események megelőzése érdekében. Ennek magyarázata kézenfekvő. A nemzetbiztonsági kockázatok a társadalom tagjait érintik, rajtuk keresztül, általuk realizálódnak, őket célozzák. Az állampolgárok jelentősen növelhetik a titkosszolgálatok elhárító munkájának hatékonyságát.

A múlt század során több olyan esemény, változás is történt,[17] amely jelentős hatással volt Magyarország biztonsági helyzetére, és komoly kihívást jelentett az ahhoz szorosan kötődő – és abban az időszakban már szervezett keretek között végzett – titkosszolgálati munkára is. Az I. világháborút követő években például néhány Magyarországgal szomszédos ország, így Csehszlovákia, Románia és a Szerb–Horvát–Szlovén Királyság szövetségre lépett, amelynek elsődleges célja a magyar revizionista törekvések megakadályozása volt.[18] A cél eléréséhez szükségük volt arra, hogy az érintett kormányok folyamatosan naprakész, érdemi ismeretekkel rendelkezzenek Magyarország gazdaságáról, politikai elképzeléseiről és katonai terveiről, képességeiről. Az állandósult, fokozott hírigény aktivizálta ezen országok Magyarországgal szemben folytatott hírszerző tevékenységét, amely elleni fellépés a magyar elhárítás feladatrendszerében jelentkezett. A fokozott kihívásra válaszul 1936-ban kiadták a nemzetbiztonsággal foglalkozó magyar nyelvű szakirodalom egyik meghatározó jelentőségű munkáját, *A hírszerzés és kémkedés története*[19] című háromkötetes, közel ezerkétszáz oldalas összefoglaló művet, amelyet Pilch Jenő ezredes,[20] magyar katonatiszt szerkesztett. A kiadvány előszavában a „szerzőktől", a könyv megszületésének indokai között az alábbiakat olvashatjuk:

16 Lásd: www.verfassungsschutz.de/DE/themen/wirtschafts-wissenschaftsschutz/praeventionsansatz/praeventionsansatz_node.html#doc714168bodyText2

17 Többek között az I. és a II. világháború, valamint a hidegháború és ezek következményei.

18 Tarján M. Tamás: 1921. június 7. |Megalakul a kisantant. *Rubicon Online,* (é. n.).

19 Pilch Jenő: *A hírszerzés és kémkedés története.* Budapest, Franklin, 1936.

20 Pilch Jenő (1872–1937), hadtörténész, író.

> „…elrettentsük honfitársainkat olyan cselekményektől, amelyek miatt, akárcsak a bélpoklosokat, kitaszítják őket a nemzet és a becsületes társadalmi osztályok kebeléből."[21]
> „De azt is akarjuk, hogy ennek az agyonsanyargatott magyar hazának minden becsületes polgára felfigyeljen és az ádáz ellenségeink által ellenünk irányított kémkedés elhárításában és kiirtásában segítőkezet nyujtson (sic!) azoknak, akik erre intézményesen hivatottak."[22]

Az elrettentés alátámasztására a mű első kötetében a szerzők több tíz olyan bírósági ítéletről számoltak be, amelyek érintettjei a kisantant országai számára folytattak kémtevékenységet 1935-ben és 1936-ban.[23] Vitéz József királyi herceg[24] tábornagy a könyv bevezetőjében az alábbiakat írta:

> „Mint ezen a téren is sokat látott katona és mint hazámért aggódó honfi, örömmel látom, hogy lelkes tudósok feltárják a tájékozatlan közönség előtt a katonai hírszerzés, kémkedés és propaganda rejtelmeit. A közönség ezen nagyarányú műben nemcsak színes, érdekes és úgyszólván kalandos olvasmányt kap kezébe, hanem ennek hatalmas tanulságai kell, hogy visszhangot keltsenek minden jó magyar ember lekében. Védekezni a kémek ellen, el nem árulni még a legjelentéktelenebbnek látszó adatot sem, óvakodni a gyanús elemektől szigorú hazafias kötelesség! Melegen ajánlom ezt a művet a magyar közönség figyelmébe, mely hazafias és nemzetnevelő, hatalmas figyelmeztetés legyen az új nemzedéknek."

A II. világháborút követő időszakot tekintve más körülmények között, de hasonló helyzetet figyelhettünk meg Magyarországon. A világ kétpólusúvá válása, a két tábor katonai szembenállása, a keleti blokk szinte szó szerinti bezárkózása jelentősen fokozta a szemben álló felek egymással szembeni bizalmatlanságát, ezáltal a titkosszolgálatok aktivitását. Kémelhárítási szempontból a helyzetet tovább nehezítette, hogy a „magyar ügyet" 1962 végétől az Egyesült Nemzetek Szervezete levette a napirendjéről.[25] Ennek következtében felélénkültek Magyarország és a nyugat-európai országok, valamint az USA közötti gazdasági kapcsolatok, továbbá az idegenforgalom is komoly lendületet kapott.[26] Ilyen körülmények között az 1960-as évek elejére jelentősen megnövekedtek és megváltoztak a kémelhárítási feladatok, amire Pap János, akkori belügyminiszter is felhívta a figyelmet: „Korábban főleg beküldött ügynökökkel próbáltak ügynökségeket,

---

21 Pilch (1936): i. m. VIII.
22 Pilch (1936): i. m. VIII.
23 Pilch (1936): i. m. VIII.–X.
24 „József nádor unokája, osztrák főherceg, magyar királyi herceg, honvéd tábornagy, felsőházi tag. 1918-ban királyi helytartó, 1919-ben kormányzó, 1936–44-ig az MTA elnöke." Lásd: https://dspace.oszk.hu/handle/20.500.12346/57347?show=full
25 Békés Csaba – D. Kecskés Gusztáv (szerk.): *A forradalom és a magyar kérdés az ENSZ-ben, 1956–1963: Tanulmányok, dokumentumok és kronológia.* Budapest, Magyar ENSZ Társaság, 2006. 46.
26 Somlai Katalin: *Go West! A nyugati ösztöndíj-politika diskurzusai az 1960-as – 1970-es évek Magyarországán.* Előadás: Országos Széchényi Könyvtár, 2015. november 25.

hálózatokat szervezni. Most a kimenő és bejövő turistaforgalmat próbálják kihasználni erre a célra."[27]

A társadalommal való együttműködés szükségessége a bűncselekmények megelőzésének érdekében a legfelsőbb politikai szinten[28] fogalmazódott meg, „hogy a bűnözők elleni fellépésben az állami szervek mellett meg fog növekedni a »dolgozók tömegszervezeteinek szerepe«, ami növelni fogja annak hatékonyságát", másrészt, hogy „elsődlegesen a prevencióra kell törekedni a bűncselekmények kapcsán".[29]

A fentiekre válaszul Magyarországon az 1960-as évek elején szakmai szinten is megfogalmazódott a társadalom bevonásának szükségessége az állam elleni bűncselekmények megelőzésébe. Ennek egyik módját az 1962-ben született Be.[30] 13. §-a alapján folytatható szignalizáció[31] jelentette. Lényege, hogy a kémkedéssel összefüggő eljárások keretében megállapított azon körülményeket, amelyek valamely szervezetnél fellelhető államtitok jogellenes megszerzését lehetővé tették, közölni kellett az érintett szervezet munkatársaival, mivel ezen ismeretek közlése jelentősen csökkenthette az ilyen jellegű kockázatok ismételt bekövetkezését.[32]

Emellett az 1960-as években az amerikai hírszerzés által kémtevékenységre beszervezett és foglalkoztatott, majd a magyar elhárítás által azonosított személyek ügyeiről megelőző célzattal, részleteiben tájékoztatták a társadalmat, amelynek során több médiafelületet is felhasználtak. Az egyik nyilvános kiadványban[33] képekkel színesítve, közérthetően tárták az állampolgárok elé azt, amit az ügyek felderítése során megállapítottak. Például hogy az USA Központi Hírszerző Ügynöksége (CIA) hogyan szervezte be, képezte ki, foglalkoztatott magyar állampolgárokat, illetve hogy az ellenőrzés során a CIA hazugságvizsgálót is alkalmazott, az „ösztönzés" részeként pedig meg is fenyegette az együttműködőt azzal, hogy szükség esetén készek a kémtevékenységről a magyar állambiztonsági szervet tájékoztatni.[34] Az esetekről megjelentek információk a napi sajtóban is,[35] továbbá egy oktatási céllal készített diasor.[36] A belügyminiszter egy másik nyilatkozatában úgy fogalmazott, hogy a társadalom támogatja az állambiztonsági szerveket,[37] és ennek eredményeként többek között több kémet sikerült azonosítaniuk.[38]

---

27 Szabó László: Adalék a rendőrség és a sajtó vitájához. *Belügyi Szemle,* 2. (1964), 3. 76.

28 A Szovjet Kommunista Párt (SzKP) 1961. október 17. és 31. között megtartott XXII. kongresszusán Nyikita Szergejevics Hruscsov, a párt első titkára fogalmazta meg ezeket a gondolatokat. Csáki Ernő: A Szovjetunió Kommunista Pártja XXII. Kongresszusa után. *Rendőrségi Szemle,* 9. (1961), 12. 973.

29 Mezei József: A (Rendőrségi) Belügyi Szemlében közölt, az állambiztonság területével foglalkozó írások áttekintő elemzése az SzKP XXII. kongresszusát követő időszakban. *Magyar Rendészet,* 21. (2021), 2. 189–200.

30 1962. évi 8. törvényerejű rendelet a büntető eljárásról.

31 A szignalizáció tartalma: a megtörtént bűncselekményeket előidéző okok, körülmények és lehetőségek feltárása, s azoknak a hasonló bűncselekmények megelőzése céljából az érdekelt szervekkel való közlése.

32 Pásztor Dezsőné: Az állam elleni bűncselekmények megelőzésének néhány kérdése. *Belügyi Szemle,* 2. (1964), 12. 25.

33 Bán Ernő: *Kémek – hazaárulók.* Budapest, Zrínyi, 1966.

34 Bán (1966): i. m. 18.

35 MTI: Amerikai hírszerzők a bíróság előtt. *Békés Megyei Népújság. A megyei pártbizottság és a megyei tanács lapja,* 21. (1966), 124. 2.

36 *A fellazítási politika.* Diafilm. Budapest, Magyar Néphadsereg Központi Klub Módszertani Osztály, 1967.

37 Köteles István: Az állambiztonsági munka alapja – a szocialista törvényesség. *Belügyi Szemle,* 1. (1963), 6. 9.

38 Pap János: A „Belügyi Szemle" elé…. *Belügyi Szemle,* 1. (1963), 1. 9.

Mindkét eset kapcsán elmondható, hogy a kockázatok megsokszorozódása, politikai, illetve vezető személyiségek támogatása mellett váltotta ki a társadalom megszólítását, a kémelhárítási tevékenységbe történő bevonását. Az együttműködés keretében az állampolgárok értesülhettek a kémkedésről mint az egyik meghatározó, a nemzet biztonságát jelentősen befolyásoló kockázatról, az az ellen küzdő magyar szervezetekről. Megjelent továbbá az együttműködésre való ösztönzés ugyanúgy, mint a jogellenes tevékenységtől való elrettentés szándéka, vagyis azon tényezők közül több, amelyek a tudatosító tevékenység szempontjából ma is fontosak, illetve amelyeket a biztonságtudatosság céljaként fogalmazunk meg.

3. Nemzetbiztonsági Szakszolgálat

3.1. A biztonságtudatosítás feladatkörének megjelenése, tartalma, jogszabályi háttere

A Nemzetbiztonsági Szakszolgálat (NBSZ) önálló nemzetbiztonsági szolgálatként 1996-ban kezdte meg működését. Legfőbb feladata kezdetektől a magyar rendvédelmi szervek által folytatott titkos információgyűjtés támogatása volt. Az elmúlt években azonban feladatköre jelentősen kiszélesedett, többek között részévé vált az adat- és információbiztonság szempontjából kiemelten fontos terület, az informatikai rendszerek védelme.

2013-ban hatályba lépett az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.), amely jelentős mérföldkőnek számított a hazai, kormányzati, illetve nemzetbiztonsági szempontból releváns informatikai rendszerek, illetve az azokban tárolt információk védelme tekintetében. A jogszabály többek között rendelkezett arról, hogy az érintett informatikai rendszereket célzó támadások elhárításával kapcsolatos feladatok ellátása érdekében „a polgári nemzetbiztonsági szolgálatok irányításáért felelős miniszter irányítása alatt”[39] eseménykezelő központot kell létrehozni. A jogszabály rögzítette továbbá az eseménykezelő központ feladatait, amelyek között rögzítették, hogy a szervezet „a biztonságtudatos felhasználói magatartás elősegítése céljából oktatási anyagokat dolgozhat ki és tréningeket tarthat, felvilágosító, szemléletformáló kampányokat szervezhet”.[40]

A feladatok hatékonyabb végrehajtása, egy, az „erőforrásokkal hatékonyan gazdálkodó modell” kialakítása érdekében az NBSZ keretén belül 2015. október 1-jével létrehozták a Nemzeti Kibervédelmi Intézetet (NKI), amelybe integrálták a problémakörrel foglalkozó, de addig külön szervezeti egységekben működő szervezeteket.[41]

[39] Ibtv. 19. § (1) *c).*
[40] Ibtv. 20. § (1) *k).*
[41] Belügyminisztérium: *Megalakul a Nemzeti Kibervédelmi Intézet* (2015. október 1.).

Az intézet szervezeti elemei és azok feladatai a következők:

- GovCert Incidenskezelő osztály:
  - biztonsági események kezelése,
  - fenyegetésmenedzsment,
  - ügyeleti szolgálat,
  - elemzés/értékelés,
  - kibervédelmi gyakorlat,
  - képzés, tudatosítás;
- Nemzeti Elektronikus Információbiztonsági Hatóság (NAIH):
  - ügyfelek és rendszerek nyilvántartása,
  - biztonsági osztályba és szintbe sorolás ellenőrzése,
  - követelmények teljesülésének ellenőrzése,
  - javaslat információbiztonsági felügyelő kirendelésére;
- Biztonságirányítási és Sérülékenységvizsgálati Osztály:
  - sérülékenységvizsgálat,
  - EMIR/FAIR-rendszerekkel kapcsolatos informatikai biztonsági feladatok ellátása,
  - IT-biztonsági tanácsadás.[42]

Figyelmet érdemel az intézetnek a biztonságtudatosság fokozását célzó tevékenységével összefüggésben megfogalmazott álláspontja is, amely amellett, hogy rávilágít a tevékenység fontosságára, több lényegi elemre is kitér a biztonságtudatosság hatékonysága kapcsán.

> „A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet egyik kiemelt feladata a biztonságtudatosság növelése a felhasználók vonatkozásában. A kibervédelem legolcsóbb és leghatékonyabb módja a biztonságtudatos használat. A védelemre fordítható összegek ugyanis korlátozottak, ráadásul a megfelelő biztonság technikailag sokszor nem, vagy csak irreálisan magas költségek mellett lenne a megfelelő szinten kialakítható. A tudatosítás számos formában megjelenhet, mint például szakmai anyagok és útmutatók készítése, közvetlenül kifejtett oktatási vagy képzési tevékenység, a kiberbiztonság hangsúlyának növelése a médiában. A tudatosító tevékenység számos réteget céloz, ezek közt elsősorban kell említeni a döntéshozókat (szervezeti vezetőket, akik a rendszerek védelméért felelősek), az üzemeltetőket (akik ellátják a rendszerek működtetését, és tőlük várható el a védelmi intézkedések működtetése), és a felhasználókat, akiket meg kell tanítani az internet és az információs technológiák biztonságos használatára, saját és a rájuk bízott adatok felelős és szakszerű kezelésére.” [43]

A fentiek alapján kijelenthető, hogy az NBSZ jogszabályi felhatalmazás alapján végzi az informatikai rendszerekkel kapcsolatos tudatosító tevékenységét, a védelmi feladat végrehajtására létrehozott szervezeti egység keretében. Ez utóbbi azt mutatja, hogy

[42] Kiss Tibor: *Kibervédelem a bűnügyi tudományokban.* Budapest, Dialóg Campus, 2020. 70.
[43] Lásd: https://nbsz.gov.hu/tevekenyseg-mukodes/nemzeti-kibervedelmi-intezet

a biztonságtudatosság fejlesztését az NBSZ integrálta a védelmi feladatok közé, azoknak szerves részét képezi. Ez a fajta megközelítés több szempontból is pozitív hatással van a tevékenységre, például lerövidíti az információáramlást a tényleges védelmi feladatokat ellátó személyek és a biztonságtudatosságért felelős munkatársak között.

3.2. A biztonságtudatosítás megjelenése a gyakorlatban

A szolgálat által a biztonságtudatosításra igénybe vett felületeket sorba véve megállapítható, hogy a legfontosabb eleme, az NKI önálló honlapja, amely könnyen áttekinthető és rendkívül informatív. Az oldalt megnézve látható, hogy napi szinten jelennek meg új ismeretek, ami a védelmi feladat jellegét tekintve természetesnek vehető. A honlapon túl a szolgálat jelen van a fiatalok által kedvelt közösségimédia-felületen, a Facebookon – aktuálisan 18 057 ember követi –, illetve az Instagramon – követőinek száma jelenleg 1426. A közösségimédia-felületek mellett a tartalommegosztó oldalakat is használja ismeretek terjesztésére.[44] A felületek kapcsán elmondható, hogy színesek, látványosak, rengeteg információt tartalmaznak, és ami különösen fontos, hogy a szolgálat folyamatosan aktív a felületeken. Amellett, hogy a közösségi média és tartalommegosztó oldalak alkalmasak a biztonságtudatosság fokozását célzó ismeretek közlésére, a szolgálat ismertségét, népszerűsítését is jól szolgálják. A szolgálat jelen van a hagyományos médiafelületeken, mint például a rádió- és tévéműsorokban.[45] A bizalomépítést, az ismertség növelését nagyban segíti, hogy az intézet egy szakmailag felkészült szóvivőt is foglalkoztat. Az állandó felületek mellett előadásokat tart, továbbá rendezvényeken is megjelenik,[46] sőt konferenciákat is szervez.[47]

Az alkalmazott módszereket tekintve megtalálhatók mélyebb szakmai elemzések,[48] a rövid szakmai tájékoztatók, egy-egy biztonsági kérdést bemutató, szórólapszerű kiadványok,[49] esettanulmányokat feldolgozó videók[50] éppúgy, mint a manapság egyre népszerűbb podcastok. A szervezet elfogadottságának erősítése kapcsán fontos megemlíteni, hogy a szférában egyedülálló módon a szolgálat főigazgatója is meghívottja volt egy ilyen beszélgetésnek.[51]

A korábbiakban említettük, hogy a biztonságtudatosság eredményessége szempontjából fontos, hogy mennyire ismerik az állampolgárok a szolgálatot, illetve milyen a viszonyulásuk hozzá. Ennek kapcsán figyelmet érdemel, hogy az NBSZ-nek több olyan kezdeményezése is van, amelyek ugyan nem tartoznak szorosan a biztonságtudatosító tevékenységhez, azonban a szervezet ismertségét, társadalmi elfogadottságát növelik, ami viszont pozitív hatást gyakorolhat a biztonságtudatosító

44 Lásd: www.youtube.com/watch?v=Q0xZyLQ6QLs
45 Lásd: www.youtube.com/watch?v=V889_41j0gc
46 Lásd: www.budaorsiinfo.hu/blog/2021/02/10/szakertok-fel-kell-kesziteni-a-gyerekeket-a-biztonsagos-internetezesre/
47 Lásd: https://nki.gov.hu/intezet/kozlemenyek/nemzeti-kiberbiztonsagi-konferencia-2020-kicsit-maskepp/
48 Lásd: https://nki.gov.hu/wp-content/uploads/2021/09/NBSZ-NKI-Kiberbiztons%C3%A1gi-elemz%C3%A9s-a-SolarWinds-incidensr%C5%91l.pdf
49 Lásd: https://nki.gov.hu/wp-content/uploads/2019/03/14_Adatbiztons%C3%A1g-a-munkahelyen.pdf
50 Lásd: https://nki.gov.hu/it-biztonsag/mediatar/spear-phishing-kisfilm/
51 Lásd: https://kibertamadas.simplecast.com/episodes/boldog-szulinapot-nbsz

tevékenységére is. Ilyen például a nemzetbiztonsági szektorban példa nélküli „zöld NBSZ"[52] program, vagy az állatkerti örökbefogadás projekt,[53] vagy akár a nyilvános kiberversenyek szervezése.[54] A társadalmi felelősségvállalás ilyen formában történő megnyilvánulásai amellett, hogy komoly környezettudatosságot mutatnak, sokak szemében „trendi", és szimpátiát ébreszt az emberek jelentős részében. Hasonló a helyzet a nyilvános kiberversennyel is, amely rendkívül jó reklám a szolgálatnak, növeli a szervezet, illetve az általa folytatott védelmi tevékenység társadalom általi ismertségét, remek lehetőség a – manapság komoly feladatként jelentkező – megfelelő képességű munkatársak kiválasztásához is.

4. Befejezés

Összegzésképpen elmondható, hogy az NBSZ egy jogilag egyértelműen szabályozott helyzetben néhány év alatt meghatározó szereplővé vált Magyarországon az informatikai rendszereket, illetve az abban tárolt adatokat érintő kockázatok felderítése és elhárítása terén. Ezen tevékenysége magában foglalja a társadalom széles körű tájékoztatását, az állampolgárok biztonságtudatosságának fejlesztését is. Ennek érdekében egyrészt megjelent azokon a felületeken, amelyeken keresztül az állampolgárok jelentős számát eléri, másrészt változatos módszerek, eszközök alkalmazásával, az érintett személyi körnek megfelelő tartalommal készíti el és teszi közzé tájékoztatóit. A szolgálat ismertségét, szakmai elismerését jól jelzi, hogy az információbiztonsági incidensekkel kapcsolatosan kiadott tájékoztatóit általában a hazai médiumok rendszeresen átveszik és közlik.

Felhasznált irodalom

Bán Ernő: *Kémek – hazaárulók.* Budapest, Zrínyi, 1966.

Békés Csaba – D. Kecskés Gusztáv (szerk.): *A forradalom és a magyar kérdés az ENSZ-ben, 1956–1963: Tanulmányok, dokumentumok és kronológia.* Budapest, Magyar ENSZ Társaság, 2006.

Csáki Ernő: A Szovjetunió Kommunista Pártja XXII. Kongresszusa után. *Rendőrségi Szemle,* 9. (1961), 12. 963–971.

Jagadics Péter – Rajos Sándor – Simon László – Szabó Károly: *A magyar katonai elhárítás története 1918–2018*. Budapest, Metropolis Media Group Kft., 2018.

Kiss Tibor: *Kibervédelem a bűnügyi tudományokban*. Budapest, Dialóg Campus, 2020. Online: https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/web_PDF_Kibervedelem_bunugyi_tudomanyokban.pdf

Köteles István: Az állambiztonsági munka alapja – a szocialista törvényesség. *Belügyi Szemle,* 1. (1963), 6. 5–12.

[52] Lásd: https://nbsz.gov.hu/zold-nbsz
[53] Lásd: www.youtube.com/watch?v=twuEct9_jAY
[54] Lásd: www.youtube.com/watch?v=9NEIvGh6ibQ

Mezei József: A (Rendőrségi) Belügyi Szemlében közölt, az állambiztonság területével foglalkozó írások áttekintő elemzése az SzKP XXII. kongresszusát követő időszakban. *Magyar Rendészet* 21. (2021), 2. 189–200. Online: https://doi.org/10.32577/mr.2021.2.12

MTI: Amerikai hírszerzők a bíróság előtt. *Békés Megyei Népújság. A megyei pártbizottság és a megyei tanács lapja,* 21. (1966), 124. 2. Online: https://library.hungaricana.hu/hu/view/BekesMegyeiNepujsag_1966_05/?pg=192&layout=s

Nagy Katalin – Mezei József: A biztonságtudatosítás megjelenése a terrorelhárítás területén. *Nemzetbiztonsági Szemle,* 7. (2019), 4. 105–117. Online: https://doi.org/10.32561/nsz.2019.4.9

Nagy Katalin – Mezei József: Nemzetközi kitekintés a terrorelhárítás területén folytatott biztonságtudatosítási programokba. *Nemzetbiztonsági Szemle,* 8. (2020), 2. 50–65. Online: https://doi.org/10.32561/nsz.2020.2.4

Pap János: A „Belügyi Szemle" elé…. *Belügyi Szemle,* 1. (963), 1. 5–12.

Pásztor Dezsőné: Az állam elleni bűncselekmények megelőzésének néhány kérdése. *Belügyi Szemle,* 2. (1964), 12. 24–30.

Pilch Jenő: *A hírszerzés és kémkedés története*. Budapest, Franklin, 1936.

Somlai Katalin: *Go West! A nyugati ösztöndíj-politika diskurzusai az 1960-as – 1970-es évek Magyarországán.* Előadás: Országos Széchényi Könyvtár, 2015. november 25. Online: www.rev.hu/hu/node/138.

Szabó László: Adalék a rendőrség és a sajtó vitájához. *Belügyi Szemle,* 2. (1964), 3. 72–76.

Tarján M. Tamás: 1921. június 7. |Megalakul a kisantant. *Rubicon Online,* (é. n.). Online: www.rubicon.hu/magyar/oldalak/1921_junius_7_megalakul_a_kisantant/

Internetes források

A fellazítási politika. Diafilm. Budapest, Magyar Néphadsereg Központi Klub Módszertani Osztály, 1967. Online: https://ritkanlathatotortenelem.blog.hu/2015/02/05/regi_magyar_diafilmek_5_a_kapitalistak_modszerei#gallery-1421327364_57.

Belügyminisztérium: *Megalakul a Nemzeti Kibervédelmi Intézet* (2015. október 1.). Online: https://2015-2019.kormany.hu/hu/belugyminiszterium/rendeszeti-allamtitkarsag/hirek/megalakul-a-nemzeti-kibervedelmi-intezet

September 11 Attacks. *History,* 2018. augusztus 5. Online: www.history.com/topics/21st-century/9-11-attacks

Terrorists Bomb Trains in Madrid. *History,* 2004. március 11. Online: www.history.com/this-day-in-history/terrorists-bomb-trains-in-madrid

Terrorists attack London transit system at rush hour. *History,* 2005. július 7. Online: www.history.com/this-day-in-history/terrorists-attack-london-transit-system-at-rush-hour

Jogi források

1962. évi 8. törvényerejű rendelet a büntető eljárásról
1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról
2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

NEMZETBIZTONSÁGI SZEMLE
9. évfolyam (2021) 4. szám 48–61. • DOI: 10.32561/nsz.2021.4.4

Mezei József[1] – Koncz Veronika[2] – Jasenszky Nándor[3]

Biztonságtudatosság – hazai helyzetkép, hazai gyakorlat és példák 2.[4]

Security Awareness – Domestic Situation, Domestic Practice and Examples 2

A 21. század elején számos olyan esemény és változás történt a világban, amelyek jelentős hatást gyakoroltak a titkosszolgálatok tevékenységére is. Ezek közül kiemelkednek a nyugati társadalmakat sokkoló terrorcselekmények az Amerikai Egyesült Államokban és Európában, az információtechnológia rohamos fejlődése, valamint ezzel együtt az ezzel kölcsönhatásban álló információrobbanás. Ezen tényezők egyik következménye lett a biztonságtudatosító programok rendszerszintű megjelenése a nemzetbiztonság területén például a terrorelhárítással és az információvédelemmel összefüggésben. E két részből álló publikáció célja, hogy bemutassa a magyar titkosszolgálatok, illetve a Terrorelhárítási Központ által aktuálisan folytatott, ilyen típusú programokat. A publikációt a Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézete által folytatott ez irányú kutatás részeként állítottuk össze azzal a céllal, hogy a kutatásban kiindulási alapot biztosítson a nemzetközi példákat is figyelembe vevő, a hazai programok eredményességét elősegíteni kívánó módszertani ajánlásokhoz.

Kulcsszavak: *biztonságtudatosság, nemzetbiztonság, kémelhárítás, információbiztonság, terrorelhárítás*

At the beginning of the 21st century, there were a number of events and changes in the world that also had a significant impact on the activities of the intelligence services. Among these are the terrorist attacks that shock Western societies in the United States of America (USA) and Europe, the rapid development of information technology and the information explosion. One consequence of these factors is the

[1] Tanársegéd, Nemzeti Közszolgálati Egyetem Polgári Nemzetbiztonsági Tanszék; e-mail: Mezei.Jozsef@uni-nke.hu
[2] Alkotmányvédelmi Hivatal; e-mail: konczjuhasz@gmail.com
[3] Vezető, Terrorelhárítási Központ, Társadalmi Kapcsolatok Osztály; e-mail: jasenszky.nandor@tek.gov.hu
[4] A mű a TKP2020-NKA-09 számú projekt a Nemzeti Kutatási Fejlesztési és Innovációs Alapból biztosított támogatással, a Tématerületi Kiválósági Program 2020 pályázati program finanszírozásában valósult meg.

emergence of security awareness programs at the system level in a number of areas that are primarily the responsibility of intelligence services, such as counterterrorism and information security. The purpose of this two-part publication is to present the programs currently being run by the Hungarian secret services and the Counter-Terrorism Centre. The publication was compiled as part of the research carried out by the Institute of National Security of the University of Public Service with the aim of providing a starting point for methodological recommendations that take into account international examples and seek to promote the effectiveness of domestic programs.

Keywords: *security awareness, national security, counter-espionage, information security, counterterrorism*

Jelen írás egy kétrészes tanulmány második része. Az első tanulmányban az elméleti megalapozáson és egy rövid visszatekintésen túl a Nemzetbiztonsági Szakszolgálat biztonságtudatosító programját mutattuk be. Most az Alkotmányvédelmi Hivatal és a Terrorelhárítási Központ kapcsolódó programjait tekintjük át.

1. Alkotmányvédelmi Hivatal

Az Alkotmányvédelmi Hivatal (AH) sok szempontból izgalmas időszakot zárt idén ősszel, amelynek, többek között, egy jubileumi évforduló is része volt: a hivatal idén ősszel 10. éve működteti biztonságtudatossági képzését, a security awareness tevékenységet, amely a nemzetbiztonsági védelemben részesülő állami intézmények, illetve a civil szféra stratégiai szereplői számára biztosít folyamatos képzési lehetőséget.

1.1. Tíz éve partnerségben

2011-ben újszerű projekt kezdődött az AH-ban, amelyet egy nemzetközi szintű felmérés előzött meg. A hivatal munkatársai áttekintették külföldi partnereik megelőző-védelmi képességeit, és hamar kiderült, hogy a korai prevenció mint új szakmai irány lesz a követendő példa. Ez a tevékenység részleteiben mindig is az elhárító munka egyik alappillére volt, azonban 2011-től program szintjére kellett emelni, és az addigi prevenciós tanácsokat kidolgozott képzési program keretein belül működtetni.

Visszatekintve a kezdetekre megállapítható, hogy az első tíz évben az Awareness Program néven megismert oktatás attól válhatott rövid időn belül sikeressé, hogy egy új típusú munkaadói és munkavállalói igényre adott választ, nevezetesen a munkavállalók biztonsági tudatosságának kialakítására és szinten tartására. Amikor a munkavégzés biztonságáról hallanak a munkavállalók, a legtöbben munka-, tűzvédelmi és IT-kérdésekre gondolnak, amelyek természetesen részét is képezik a nagy egésznek, azonban ezeket a témákat eddig is feldolgozták az állami intézmények és a civil szektor szereplői. Az Alkotmányvédelmi Hivatal oktatásának fókuszát a globális biztonságtudatosság főszereplője, maga a munkavállaló, az ő gyengeségei,

rossz szokásai, figyelmetlensége adja. Minden biztonsági incidens elengedhetetlen része, sokszor kiváltó oka a munkavállaló, aki speciális felkészítés hiányában nem tudja megvédeni munkáltatója információit, sokszor nem is detektálva a veszteséget.

2011-ben szakmai oka is volt e járatlan út kipróbálásának, ugyanis Magyarország európai uniós elnökségi feladatai ellátása közben hatalmas érdeklődés középpontjába került, felértékelődött az elnökségi részfeladatokat végző állami intézmények munkatársainak szerepe, akik a hirtelen kialakult – sokszor személyüket közvetlenül érintő – külföldi, újságírói vagy egyéb szakmai érdeklődés mögött önállóan nem mindig tudták kiszűrni az ellenérdekelt motivációt.

Az AH biztonságtudatossági tevékenysége a legaktuálisabb kihívásokra igyekszik válaszokat adni, gyakorlati, illetve munkakörbe illeszthető ismeretek átadásával, így a konzultációs lehetőség kialakítása már a korai időszakban személyre szabott tanácsadást tett lehetővé.

Az évek során rendszerbe foglalt ismereteket állítottak össze, több témakörben elérhető modulok oktatása zajlott, a félévente-évente ismétlődő képzések megújult tartalommal igyekeztek szinten tartani a téma iránti érdeklődést. Annak érdekében, hogy a partnerek valódi szolgáltatásnak éljék meg és ne kellemetlen kötelezettségnek, a tréningek ismereteit például leafletek foglalják össze, nincs szükség a szigorúan vett oktatási jelleg megtartására.

A felgyorsult világnak megfeleltetett formában és a folyamatos modernizáció jegyében rövid, az oktatáson hallott tudásanyagot szintetizáló filmek is készültek, amelyek segítségével még jobban elmélyíthető a gyakorlati tudás. Ahhoz, hogy a partnerek építeni tudjanak az AH képzéseire, azok több esetben a step-in ponton jelen vannak, továbbá bizonyos kiemelt felsőoktatási szakokon órarendbe épített formában hallgathatók a biztonsági tudatosság alapismeretei.

A kiváló visszhang ellenére az AH biztonságtudatossági szakembereinek mégis hiányérzete támadt. Nem látták a partnereik közötti tapasztalatcsere lehetőségét, azaz azt a fórumot, ahol a magyar gazdasági élet meghatározó szereplőinek lehetősége nyílik a leghitelesebb szakértőktől rövid jövőképet kapni, amely mentén biztonsági feladataik tervezhetőbbé válnának. Hogy ez a fórum létrejöhessen a magyar gazdasági szereplők, külföldi szakértők és a biztonsági szféra jeles képviselői között, 2016-ban az Alkotmányvédelmi Hivatal által hazánkban először került megszervezésre az Awareness Konferencia, amely azóta minden évben egy asztalhoz ülteti a szereplőket.

1.2. Új keletű bizonytalanság

A koronavírus-járvány hazai hozadéka a home office széles körű elterjedése volt. Sok intézmény vagy cég egyik napról a másikra állt át a távoli elérésekre, ezért a vállalati környezetre írt IT-szabályzók fellazultak, és sok esetben szabad teret engedtek a kiberbűnözésnek. El kell fogadni, hogy a világunk átalakult: jelenleg kevesebb betörés várható a lakásainkba, viszont egyre több célzott kibertámadás.

A svájci Deloitte cég – 2020. április 10. és 15. között elvégzett – felmérése[5] alapján a koronavírus első hullámának idején Svájcban a távmunkát végzők körében 25%-kal nőtt a kibertámadások száma adathalász vagy spam e-mailek, illetve zsarolóvírusok formájában. Ennél ijesztőbb eredményt is mutatott ugyanez a kutatás: a nagy számú elbocsátások hatására a munkavállók körében eluralkodott a bizonytalanság érzése, ennek folyományaként a munkavállalók által „kicsempészett" céges/hivatalos dokumentumok száma 26%-kal nőtt ebben az időszakban, mondván, otthoni munkavégzésük alkalmával a szakmai know-how alapköveit sokan maguknál kívánják tartani.

Mit lehet tenni? Hogyan érhető el, hogy az új megjelenési formákban felbukkanó bizonytalanságnak a távmunka idején ne adatvesztés legyen az eredménye?

- A kiberfenyegetettség tükrében előzetesen fel kell készíteni a munkavállalót az új helyezetre, kommunikálni kell a munkáltató konkrét elvárásait adatvédelem és információbiztonság terén, folyamatosan szenzibilizálni a téma iránt, majd rendszeresen aktualizálni és ismételni a felkészítést – például ebben segít az Alkotmányvédelmi Hivatal biztonságtudatossági képzése.
- Az újonnan bevezetett információbiztonsági szabályzók betartását és rendeltetésszerű működtetését a munkáltató IT-szakembereinek időszakosan ellenőrizniük szükséges.
- Egy esetleges felhasználói mulasztásra is fel kell készülni, és végponti megerősítést foganatosítani a későbbi károk minimalizálása érdekében.
- Az érintett cégeknek is érdemes felkészülniük a legrosszabbra és kalkulációt végezni, hogy milyen mértékű módosításokkal tudnák az IT-infrastruktúrát például teljes lefedettségű szabotázzsal járó támadást követően gyorsan helyreállítani.
- Ilyen mértékű átállásoknál nem elegendő a cég saját, információvédelmet szavatoló szabályzóinak áttekintése, hanem érdemes ezeket a szolgáltatókkal, beszállítókkal és értékesítési partnerekkel közösen áttekinteni.

A fentieket követően megnyugtató helyzet alakítható ki a munkafolyamatok biztonsága érdekében, és minimalizálható az információvesztés.

A kiberbűnözők azonnal képesek voltak taktikát váltani és a lakosság körében eluralkodó bizonytalanságból hasznot kovácsolni. További fontos felismerés, hogy a hiányos technikai infrastruktúra és a munkavállalók nem megfelelő szintű biztonságtudatossága vezethet adatvesztéshez. Amikor vállalkozások és intézmények évtizedes munkájába telik a reputáció felépítése, nem nézhető tétlenül a szerencsében bízva, hogy egy percek alatt lezajló kibertámadás tönkretegye, ezért is az örökérvényű megállapítás: a bizalom jó, az ellenőrzés jobb.

[5] Lásd: Cyberkriminalität – die Gefahr aus dem Home Office. A felmérés 1500 fő Svájcban élő, 16 és 64 év közötti munkavállaló bevonásával készült.

1.3. A közelmúlt gyakori biztonsági incidensei

Az Alkotmányvédelmi Hivatal biztonságtudatossági képzési szakterülete kiemelt figyelemmel követte a partnereitől kapott visszajelzéseket, amelyek során a közelmúlt tendenciái a következőképpen alakultak.

A legelső, pandémiás időszak hozadékaként elkönyvelt új támadási forma a távmunka bevezetését követő egy hónapon belül szaporodott el és kártékony szoftverek segítségével valósult meg. A támadók a személyes és az elektronikus rendszerekbe történő belépésekhez szükséges adatokat lopták el. Az adatcsomagokkal céljuk a darkweb webshopjaiban történő érékesítés volt, amely természetesen komoly biztonsági rést generálhat.

Az adatvesztés folyamata minden esetben az alábbi forgatókönyv szerint történt: az egyes rendszereket – annak ellenére, hogy megfelelő vírus- és rendszermenedzsmenttel ellátott eszközöket tudott biztosítani a munkáltató – az alkalmazottak saját, otthoni informatikai eszközeikről használták. A munkavállalók saját tulajdonú számítógépei nagyobb felhasználói élményt biztosító hardveres konfigurációval rendelkeznek, mint a munkáltató otthoni munkavégzésre biztosított eszközei, azonban az alkalmazottak eszközein nem minden esetben biztosított a jogtiszta és frissített szoftveres környezet (például operációs rendszer, vírusirtó). Ennek eredményeként következhetett be, hogy a saját eszközt ért vírustámadás „elmentette" a felhasználónév és jelszó-emlékeztetőben tárolt adatokat.

A másik aktuális és igen gyakori biztonsági incidens a hivatalos vagy üzleti levelezést manipuláló kibertámadás. A BEC *(business email compromise)* típusú támadás során kiberbűnözői csoportok az e-mailes kommunikáción keresztül olyan tranzakcióra próbálták rávenni áldozataikat, amely során az eredeti partner helyett a csalók bankszámlájára utalták volna az összeget. A BEC-típusú támadásokat azért nehéz felismerni, mert a támadók számos pszichológiai trükkel dolgoznak. Eleve nyílt platformokon (például Facebook, LinkedIn) informálódnak a beosztási szintekről, majd az önálló pénzügyi lépésekre képes, tranzakciókat felügyelő döntéshozói szintet célozzák meg (például gazdasági igazgató), a támadás során pedig gyakran a munkahely vezetője e-mail-címét tüntetik fel (például vezérigazgató), illetve a levelüket formailag és tartalmilag is tökéletesen megfeleltetik a cég kommunikációs szokásainak. Az általunk megismert esetekben a valótlan projektekre való hivatkozás vagy a levélben szintén megjelenő, a küldő valódi e-mail-címét tartalmazó záradék hívta fel a szemfüles kollégák figyelmét a csalásra. További nagy összegű tranzakcióknál a támadók leveleikben kérték a címzettet, hogy a levél tartalmát kezeljék bizalmasan, amivel időt próbáltak nyerni az utalás teljesítéséig.

A home office mindkét fent leírt incidenshez tökéletes hátteret biztosított, azonban tudatossággal, szigorú kontrollal és gyors reakcióval ezek megelőzhetők.

1.4. Jövőkép

A lezárások utáni munkapiac három munkavégzési formában valósulhat meg. Az alapvetően személyes jelenlétet igénylő munkahelyekre visszatérnek a munkavállalók;

a bezárások idején sikeres távmunkai rendszert működtető cégek – költséghatékonysági szempontokat szem előtt tartva – folytatják ezt a rendszert; és végül marad a hibrid megoldásban megvalósuló munkavégzés, amely csakúgy, mint az előző, kizárólag hosszú távon válhat anyagilag kedvezővé. A homeoffice-szemléletet is folytató cégek ugyan jelentős összegeket spórolhatnak például kevesebb iroda bérlésével, azonban számítástechnikai rendszereiket ugyanolyan szintre szükséges fejleszteni, mint a teljes online munkavégzési modellben gondolkozó intézményeknél. Az első körös infrastruktúra-fejlesztés után adódhat a következő nagy kérdés: rendelkezésre áll-e a távmunkarendszerben is hatékony szakembergárda, vagy az új struktúra tömeges személycserékkel fog járni? Az új típusú munkavégzés számos addig működő szabályzó, szokásrendszer, munkafolyamat és képesítés felülvizsgálatát teszi szükségessé, tehát az első időszakban jelentős kiadással kell számolni. Az előzőeken felül pedig nem hagyható figyelmen kívül az IT-felhasználó biztonságtudatosságának fejlesztési igénye sem, amely tréningek segítségével aprólékosan formálható annak érdekében, hogy a munkáltató szempontjából szenzitív információk ne kerülhessenek ki a kibertérbe.

2. A Terrorelhárítási Központ[6]

Ahhoz, hogy megértsük a terrorelhárítás területén eddig végzett és a tapasztalataink szerint a jövőben végzendő felvilágosító munkát, kicsit messzebbről kell indulnunk.

Magyarországon a terrorelhárítás rendszerét nagy változatosság jellemezte. Függetlenül attól, hogy a korábbi állambiztonsági és rendőrségi szervezet „nyomokban" tartalmazott ilyen jellegű feladatokat, 1978-ig intézményesített terrorelhárításról nem beszélhetünk.

A Balassagyarmaton 1973-ban történt túszdráma eseményei – közvetlenül a müncheni olimpián elkövetett terrortámadás után – katalizátorként hatottak. A terrorelhárításra kijelölt szakmai szervezeteket az erős változatosság jellemezte. Megtaláljuk a felderítésért és elhárításért felelős BM III/II 8. Osztályának egy csoportját, a nyomozásért felelős BM Vizsgálati Osztályát és a felszámolásért felelős BM Forradalmi Rendőri Ezred akciószakaszait.

A rendszerváltás finomított a szakmai, illetve jogszabályi kereteken – állambiztonsági érdek = nemzetbiztonsági érdek, Forradalmi Rendőri Ezred = Készenléti Rendőrség, akciószakaszok – RKSZ – TESZ –, de összességében meghagyta a korábbi időszak szabályozási és szervezeti rendszerét.

A helyzet átéléséhez és az évtizedek óta működő rendszer hatékonyságának értékeléséhez olvasásra ajánlom az *Origo* 2014. január 16-án megjelent *Ki robbantgat itt 25 éve? – Nem tudjuk* című cikkét.[7] A cikkben elérhető felsorolás azért is tanulságos, mert később, a Terrorelhárítási Központ (TEK) megalakulásakor sokszor hallhattuk és olvashattuk, hogy nem voltak Magyarországon terror jellegű cselekmények.

[6] A tanulmány e részének szerzője Jasenszky Nándor, a TEK osztályvezetője.

[7] Ki robbantgat itt 25 éve? Nem tudjuk. *Origo,* 2014. január 13.

> „A rendszerváltással Magyarország bekerült a világnak abba a zónájába, ahol efféle cselekmények történnek – kommentálta a rendszerváltás utáni Magyarország első robbantásos merényletét Antall József miniszterelnök. Bár neki rögtön egy súlyos, nemzetközi robbantásos ügy jutott, kormányzása alatt nem kellett, hogy sokat fájjon a feje ilyen esetek miatt."[8]

Ezek a korábbi események egyértelműen mutatták, tudomásul kellett volna venni, hogy hazánkba beköszönt a terrorizmus. Alig több mint tíz évet kell várni arra, hogy az egész világ döbbenten szemlélje a 9/11-et. Ott minden megváltozott, soha nem látott szervezettség és kegyetlenség volt tapasztalható az elkövetésben. A világ legerősebb országában a legnagyobb múltú és tapasztalatú felderítő szervek mondtak időlegesen csődöt, és kellett átértékelniük egész addigi tevékenységüket. Az al-Káida globálissá tette a terrorizmust. Globális kihívás ellen csak a globális rendőri és titkosszolgálati együttműködés biztathatott sikerrel.

A terrorizmus végrehajtásában, szervezetében folyamatosan és dinamikusan változik. Ezeknek a jelenségeknek a monitorozása, a naprakész információk beszerzése, elemzése és értékelése csak egy erre szakosodott, a teljes feladatrendszerrel hatáskörileg egy helyen foglalkozó szervezet keretein belül lehetséges. A hazai és a külföldi szakemberek, rendőrségi és rendvédelmi vezetők itthon és a világban igyekeztek a politikai vezetők figyelmét arra irányítani, hogy a terrorizmus elleni küzdelem mármár háború, és sokkal komplexebb intézkedési rendszerre van szükség a végrehajtás szintjén. Meg kellett volna érteni, hogy sehol, senki nem fog tudni hosszabb távon ebből a küzdelemből kimaradni. A politikai vezetők átaludták a kétezres évek elejét, nem volt elég riasztó figyelmeztetés 2004-ben Madrid, sem pedig 2005-ben London. 2010-ig itthon nem történt érdemi változás, lényegében maradt a több mint 30 éve kialakított, a rendszerváltásnál csak finoman „ráncfelvarrt", megosztott, sokfelé leágyazott, tisztázatlan felelősségi viszonyokat tükröző feladatellátási struktúra. Magyarország kormánya 2010-ben – részben a korábbi állapotok megszüntetése érdekében – létrehozta a TEK-et.

A TEK ünnepélyes alakuló állománygyűlésén felszólalt Gilles de Kerchove, az Európai Unió terrorelhárítási koordinátora is, aki arról beszélt, hogy a szeptember 11-i terrortámadás, valamint a 2009-es detroiti eseményekről szóló jelentések világítottak rá arra, hogy nem volt megfelelő a belbiztonsági szervek közötti információáramlás, továbbá ezeket ki kellett volna egészíteni a magánszektor – elsősorban a bankszektor – adataival. Mint mondta, információdarabkák voltak, amelyeket egymással nem kötöttek össze.

Gilles de Kerchove utalt arra, hogy volt alkalma megismerni a TEK-et, központi szervezeti felépítése és feladatköre egyértelmű, a központban integrálódik a megelőzés, a felderítés és a megsemmisítés, így az információáramlás felgyorsul. A nyugat-európai országok többségében terrortámadás után jöttek létre jelentős terrorellenes szervezetek, így szerinte Magyarország egyike az elsőknek, amely felismerte a jelentőségét, hogy egy jó struktúrában létező, hatékonyan működő szervezet segíteni tud a tragédia megelőzésében.

[8] Ki robbantgat… (2014): i. m.

A TEK feladataival – tizenegy év távlatából mondhatjuk, – már nagyon sokat foglalkoztak. Itt most csak röviden:

- a TEK jelenleg – országos hatáskörrel – nyomozati jogkör nélkül végzi a terrorcselekmények és más, ezekkel összefüggő cselekmények felderítését, megelőzését, megszakítását és az elkövetők elfogását;
- feladata továbbá a Magyarországon kívül bajba jutott magyar állampolgárok részére a biztonságos hazajutásban tevőlegesen közreműködni;
- gondoskodik a törvényben, illetve kijelölés alapján meghatározott személyek védelmének megszervezéséről és biztosításáról;
- szakmai feladatainak végrehajtása során szorosan együttműködik a bel- és külföldi partnerszolgálatokkal;
- a nyomozó hatóságok, a rendvédelmi szervek, továbbá az ügyészség felkérésére végrehajtja a felfegyverkezett személyek elfogását, és az ön- vagy közveszélyes állapotban lévő fegyveres vagy felfegyverkezve ellenálló személyek elfogását.

Megállapíthatjuk, hogy a rendőrségen belül, önálló költségvetési szervként, közvetlen belügyminiszteri irányítás mellett létrejött egy önálló, kettős jogállású – a rendőrségi törvény és a nemzetbiztonsági törvény hatálya egyaránt vonatkozik rá – terrorelhárító szervezet, amely a szakterület elsődleges gazdájává és felelősévé vált, rendvédelmi, speciális titkosszolgálati jogkörrel, felhatalmazással és feladatrendszerrel.

A legfontosabb látni azt, hogy így a TEK szervezetileg képes és jogosult valamennyi részfeladatot – titkosszolgálati felderítés, hírszerzés, elemzés, értékelés, szűrés, potenciálisan veszélyeztetettek védelme, a szükséges taktikai műveletek – az eredményes terrorelhárítási munka érdekében végezni. Természetesen ez nem azt jelenti, hogy csak a TEK-nek vannak feladatai, hiszen a terrorizmus elleni küzdelem „összkormányzati" és össztársadalmi tevékenység.

A biztonságtudatos magatartás kialakításával, egyáltalán a terrorizmussal kapcsolatos társadalmi párbeszédről a TEK megalakításáig nem nagyon beszélhetünk. A különböző korszakokra rányomta bélyegét az aktuálpolitika. A hetvenes-nyolcvanas éveket „a te terroristád az én szabadságharcosom" nézőpont uralta, és sok esetben a „terrorizmus csak nyugaton van" álláspont érvényesült. A rendszerváltás után bekövetkező esetek kapcsán különböző dialektikus szaltókkal kerüljük el, hogy kimondásra és megállapításra kerüljön, hogy terrorcselekményt követtek el hazánkban.

Azért tartottam fontosnak a kor hangulatának megidézését, mert a társadalommal, csoportokkal, emberekkel nem lehet akaratuk ellenére párbeszédet folytatni. Ez kölcsönös feladatokat ró az érintettekre. Tapasztalataink szerint az összekötő kapocs a bizalom. Nehéz megszerezni, és még nehezebb megtartani, nagyon illékony, és nagyon könnyen erodálható. Ebben az összefüggésrendszerben is illenék vizsgálni a sok esetben felelőtlen, minden szakmaiságot nélkülöző politikusi és médiamegnyilvánulásokat.

A következőkben a terrorelhárítás területén kifejtett biztonságtudatosítással és társadalmi érzékenyítéssel kapcsolatos munkát, illetve a jelentősebb stációkat mutatjuk be.

Azzal kellett a kezdetekben szembesülni, hogy amikor a nyilvánosság előtti vita arról szól, hogy mi a terrorizmus, van-e reális veszély Európában, illetve Magyarországon,

a szervezetnek a nemzetközi és saját értékeléseink alapján már azzal kellett foglalkozni, hogy mit lehet, illetve kell tenni a megelőzés és megakadályozás, majd az eredményes felderítés érdekében.

A társadalmi párbeszéd kialakításában a kezdeti időkben a prioritást a szervezet bemutatása jelentette, és a kommunikálható napi feladatok nyilvánosság elé tárása mellett, előadás és prezentáció formájában kezdődött az újkori terrorizmus hazai és nemzetközi módozatainak feldolgozása és a különböző társadalmi csoportok számára történő bemutatása. A TEK szakemberei számára egyértelmű volt, hogy a megelőzési feladat az egyik legfontosabb, ezt Hajdu János a TEK főigazgatója számtalanszor megfogalmazta, és végrehajtandó feladatként meghatározta. A megelőzési feladatkörben kiemelt figyelmet kell fordítani a biztonságtudatossági tájékoztatásra, képzési rendszerek felépítésére, a társadalom érzékenyítésére. Csak ezen az úton haladva lehet bízni abban, hogy egy hatékonyabban működő, idővel több és érdemibb információt adó társadalmi jelzőrendszer alakul ki.

A 2015–16-ban Európában elkövetett, majd sajnos minden évben több alkalommal előforduló terrorcselekmények más optikába húzták a terrorizmust, és más érdeklődő közönséget generáltak. A napi események tükrében egyre nagyobb figyelem mutatkozott a TEK irányába, egyre több helyre hívták szakembereit előadásokat tartani. A kifejezetten szakmaspecifikus meghívásokon túl egyre több lett a megkeresés a társadalom egyéb területeiről, például a felsőoktatási intézmények részéről. Kihasználva ezeket a lehetőségeket, első körben egy tájékoztatási csomagot dolgoztunk ki, amelyben helyet kapott:

- a terrorizmus kialakulása és története,
- napjaink terrorizmusa,
- a TEK megalakulásához vezető út,
- a TEK mint szervezet,
- a TEK és a média.

Az oktatási intézmények esetén nagyon fontos, hogy az aktuális korcsoportokhoz igazítsuk mondanivalónkat és az előadásunkat, illetve előadói stílusunkat. Több korosztályos interjú és előadásokat követő hallgatói vélemény tapasztalatait felhasználva igyekszünk még pontosabban igazodni a mindenkori hallgatóságunkhoz és persze az adott rendezvényhez is, ahova a meghívást kaptuk. Személyes tapasztalatom, hogy a középiskolák felsőbb osztályaiba járók, illetve a felsőoktatásban részt vevők már abszolút partnerek tudnak lenni egy jól felépített és kellően interaktív előadásban. Az általános iskolás korosztálynál tapasztaltak szerint a hangsúlyt inkább a tanárok, illetve a pedagógusok felkészítésére, kellő ismeretanyaggal történő ellátására volna célszerű helyezni. Talán megfontolandó távlatos cél lehetne pedagógusi alapképzésbe, majd a későbbi továbbképzésekbe integrálni a terrorelhárítási ismereteket akár a bűnmegelőzési témakörrel karöltve.

1. ábra
Rendezvénymeghívó, ELTE

Forrás: Facebook

Az oktatás területén a felkéréseken túl természetesen megjelennek a kötelezettségek is. A nemzetközi tapasztalatok azt mutatják, hogy sajnos vannak olyan iskolai közösségek, ahol a támadások gyakoribbak, sajnálatos módon kiemelt célpontként merülhetnek fel az elkövetők oldaláról. Ezeken a helyeken az érzékenyítés konkrét biztonsági ajánlások, védelmi intézkedések, szükség szerint közös gyakorlatok formájában realizálódik. Kiemelt területként kell kezelni – folyamatos kapcsolattartás mellett – azokat a stratégiai cégeket, amelyek például az energiaellátás, a közműszolgáltatás, a tömegközlekedés területén végzik feladataikat.

A TEK rendezvénybiztosítással kapcsolatos feladatokat – részben vagy egészben – a belügyminiszter feladatszabó kijelölése alapján lát el. A közelmúltban ilyen feladataink voltak a FINA vizes világbajnokság, illetve a Maccabi Világjátékok kapcsán. Ennek során aktív és széles körű együttműködésre van szükség a civil biztonsági cégekkel és azok dolgozóival. A civil biztonsági szakmával a folyamatos kapcsolattartás célja minimum kettős; egyrészt a konkrét, számunkra kijelölt rendezvény maximális biztonsága, másrészt ennek a szakembergárdának – akik nap mint nap a társadalom és a gazdaság nagyon széles spektrumán vannak jelen – az érzékenyítése a terrorista-kihívások irányában, bevonásuk a társadalmi jelzőrendszerbe, bennük a biztonság tudatosítása. Itt kell rögtön megemlíteni, hogy a polgárőrség bevonása ebbe a körbe szinte megkerülhetetlen.

2. ábra

Jasenszky Nándor előadása a Magyar Biztonsági Fórum konferenciáján, 2020

Forrás: az MBF archívumából

A kezdeti lépéseken túl vagyunk, tapasztalataink pozitívak. Két olyan szakmai csoportról beszélünk, amelyeknek felkészültsége, elhivatottsága jó alapot szolgáltathat az érdemi, szakmailag hasznos együttműködésre.

Különleges együttműködésként értékelhetjük, hogy rendszeresen megrendezzük – ez ideig öt alkalommal – a *Terrorelhárítási Központ a bíróságok biztonságáért* című bírói szimpóziumot az Országos Bírósági Hivatal és a TEK szervezésében.[9]

A leírt területeken végzett folyamatos munka tapasztalatai egy összegző, az általunk fontosnak tartott ajánláscsomag összeállítását igényelte.

Miben láttuk mi a biztonságtudatosítás célját?

Tudati felkészítés:

- a „veled is megtörténhet" tudat kialakítása;
- hogy gyermekeinket ne csak az idegenektől, de az őrizetlenül hagyott csomagoktól is óvjuk;
- kicsit járjunk nyitottabb szemmel, legyünk érzékenyebbek a környezetünkben lezajló eseményekre;

[9] Túszdráma is volt az 5. „Terrorelhárítási Központ a bíróságok biztonságáért" szimpóziumon. *Magyarország bíróságai,* 2018. szeptember 26.

- higgyünk és bízzunk abban, hogy a rendvédelmi és terrorelhárító szervek nyitottak minden kívülről jövő információra, és azokat a legjobb szakmai tudásuk szerint fel is dolgozzák.

Megelőzés lehetőségei:

- minden olyan megosztható információ eljuttatása az állampolgárokhoz, amely alapján mindazt elvárhatjuk, amit az előző „tudati" részben leírtunk;
- a hatóságok mindenkori felelőssége, hogy az állampolgárok részéről érkező információkról legyen visszacsatolás a forrás irányába.

Magatartási ajánlások:

- mire kell figyelned a mindennapi életedben a jobb túlélési esélyekért;
- mit tegyél, ha belekerültél egy ilyen szituációba;
- mik a túlélés legjobb esélyei.

E gondolatok jegyében adta ki a TEK 2019-ben a *Mindennapi biztonság* című kézikönyvet,[10] amelyben a megelőző védelmi ajánlásainkat igyekeztünk összefoglalni. A cél olyan gyakorlati, a mindennapokban használható ajánláscsomag összeállítása volt, amelynek felhasználásával javulhat az azt alkalmazó biztonsági szintje, és eredményesebbé válik a munkája.

Az anyagot rendelkezésére bocsátottuk együttműködő partnereinknek, a szakmai és érintett kamaráknak, továbbá e-könyv-formátumban elérhetővé és letölthetővé tettük a TEK honlapján az aktuális menüpont alatt.

Az eredményesség érdekében elemeztük a Magyarországra jellemző jelenlegi állapotokat a biztonságtudatosítás területén. Meg kell állapítani, hogy több érintett szervezet (TEK, AH, ORFK, BRFK, NBT) folytat ilyen jellegű munkát. Ezek koordinálatlanok, nincsenek egyeztetve, sok esetben átfedések tapasztalhatók, és mint afféle párhuzamosok, soha nem, vagy csak a végtelenben találkoznak. A szigetszerűen végrehajtott programoknak is köszönhető, hogy a hatékonyság meglehetősen alacsony. Csak példaként ragadnám ki, hogy adósak vagyunk egy közös oktatási csomag megalkotásával – összehangoltan a rendvédelem, terrorelhárítás, nemzetbiztonság –, amely célirányosan tudna megjelenni a különböző szintű és korosztályú oktatási intézményekben az általános iskolától a felsőoktatásig.

A nemzetközi tapasztalatok azt mutatják, hogy a terrorizmus megelőzésére, visszaszorítására irányuló nemzeti kezdeményezésekben vannak hasonlóságok. Ugyanakkor látni kell, hogy a munka hatékonyságát befolyásoló tényezők, mint például a társadalmi berendezkedés, a társadalmi szerkezet, a nemzetgazdaságok színvonala, az eltérő biztonsági kihívások teszik az adott helyen egyedivé a küzdelmet.

A terrorizmus elleni harc elmúlt évtizedeinek alapvető tanulsága, hogy a konkrét terrorelhárítási feladattal megbízott állami szerv vagy szervezetrendszer önmagában nem képes hatékonyan fellépni. Komplex, össztársadalmi együttműködésre van szükség, így alakulhatnak ki azok az intézményi, együttműködési és kommunikációs csatornák, amelyek segíthetik a megelőzést és a detektálást.

[10] Jasenszky Nándor (szerk.): *Mindennapi biztonság*. Budapest, Terrorelhárítási Központ, 2019.

A jövő feladatainak lényege abban látható, hogy a részt vevő szakmai szervezetek részéről alkalmazott szigetszerű felvilágosítási, tájékoztatási rendszereket meg kell változtatni. Célszerű lenne országos hatáskörű, megfelelő humán és anyagi erőforrásokkal ellátott szervezetet létrehozni, amely képes partnerként fellépni, adott esetben különböző minisztériumok által irányított területeken is.

A politikai szándék egyértelműen levezethető *Magyarország Nemzeti Biztonsági Stratégiájá*ból,[11] amely megfogalmazza a kormányzati elvárásokat: „126. pont: A biztonság szavatolása érdekében elsődleges cél a nemzeti intézkedések hatékonyságának és rugalmasságának, valamint a nemzeti együttműködés szilárdságának erősítése." Az irány és a célok adottak, innen már az „aprópénzre váltásé" kell, hogy legyen a jövő.

3. Befejezés

A titkosszolgálatokat és a Terrorelhárítási Központot vizsgálva látható, hogy aktuálisan két területen folytatnak biztonságtudatosító tevékenységet a szolgálatok, a terrorelhárítás és az adatvédelem területén. A szervezetek közel egy időben kezdték el ezt a tevékenységet, hasonló úton járnak, de az intenzitásban az alkalmazott eszközök és módszerek tekintetében egyes területeken jelentős eltérések tapasztalhatók. Ez irányú tevékenységeikben vannak kisebb-nagyobb átfedések, azonban nyilvánosan nem látszik, hogy együttműködnének egymással, ami pedig tovább növelhetné a hatékonyságot.

Az AH és a TEK tekintetében hiányzik az az egyértelmű jogszabályi felhatalmazás, amely a Nemzetbiztonsági Szakszolgálat esetében megvan, habár a *Nemzeti Biztonsági Stratégiá*ban foglaltak közvetetten megadják ezt.

Zárásként elmondható, hogy a biztonságtudatosság fokozása széles körű és hatékony segítséget jelenthet a nemzetbiztonsági szolgálatok részére feladataik ellátásához, ezért az ez irányú képességek fejlesztése mindenképpen indokolt.

Felhasznált irodalom

Jasenszky Nándor (szerk.): *Mindennapi biztonság.* Budapest, Terrorelhárítási Központ, 2019. Online: http://tek.gov.hu/pdf/mindennapi_biztonsag_kezikonyv.pdf

Internetes források

Cyberkriminalität – die Gefahr aus dem Home Office. Online: https://www2.deloitte.com/ch/de/pages/risk/articles/covid-19-cyber-crime-working-from-home.html

Ki robbantgat itt 25 éve? Nem tudjuk. *Origo,* 2014. január. 13. Online: www.origo.hu/itthon/20140113-robbantasos-merenyletek-magyarorszagon-a-rendszervaltas-ota.html

[11] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.

Túszdráma is volt az 5. „Terrorelhárítási Központ a bíróságok biztonságáért” szimpóziumon. *Magyarország bíróságai,* 2018. szeptember 26. Online: https://birosag.hu/hirek/kategoria/tudomanykultura/tuszdrama-volt-az-5-terrorelharitasi-kozpont-birosagok

Ajánlott irodalom

Szalai Flóra: A terrorizmus és a terrorelhárítás törzsfejlődése – A TEK előadása az ÁJK-n. *Jurátus,* 2017. március 13. Online: https://juratus.elte.hu/a-terrorizmus-es-a-terrorelharitas-torzsfejlodese-a-tek-eloadasa-az-ajk-n/

Hamvas Intézet: TEK megnyitó. Megalakult a Terrorelhárítási Központ (2010. szeptember 1.). Online: www.hamvasintezet.hu/hankiss-agnes-munkadokumentumai-az-europai-parlamentbol-2009-2014/konferenciak-esemenyek-eloadasok/tek-megnyito/

„A TEK – mint koncepció – szerintem jó”. Nagyinterjú a TEK kommunikációs vezetőjével. Első rész. *lemil.blog.hu,* 2017. május 23. Online: https://lemil.blog.hu/2017/05/23/_a_tek_mint_koncepcio_szerintem_jo

„Párhuzamosság, ez a kulcsszó”. Nagyinterjú a TEK kommunikációs vezetőjével. Befejező rész. *lemil.blog.hu,* 2017. május 26. Online: https://lemil.blog.hu/2017/05/26/_parhuzamossag_ez_a_kulcsszo

Jogi forrás

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

NEMZETBIZTONSÁGI SZEMLE
9. évfolyam (2021) 4. szám 62–78. • DOI: 10.32561/nsz.2021.4.5

Héder Klára[1]

A biztonságtudatosítás pszichés gátjai: szubjektív veszély- és kontrollpercepció a digitális térben

Psychological Barriers to Security Awareness: Subjective Danger and Control Perception in the Digital Space

Az információbiztonság-tudatosítás sikere össztársadalmi érdek. E hosszú távú folyamat eredményességének biztosításához mind a programok készítői oldalán, mind pedig a célcsoporti oldalon fontos, hogy megismerjük és kivédjük azokat a gátakat, amelyek a kimeneti eredményességet befolyásolhatják. A cikk bemutatja azokat a kérdéseket, amelyeket az információbiztonság-tudatosítás „technokrata megközelítése" vet fel. Bemutatja a képzések kialakítása mögött megbújó rejtett feltételezéseket, a felhasználói oldalon tapasztalható pszichés hárítások és ellenállási pontok mögött húzódó fontosabb okokat, a szubjektív veszély- és kontrollpercepció hatását a programokban való hosszú távú részvételi szándékra.

Kulcsszavak: *információbiztonság-tudatosság, biztonságtudatosítás, kiberbiztonság, adatvédelem, pszichológiai hárítás*

The success of raising information security awareness is in the public interest. To ensure the effectiveness of this long-term process, both on the program developer side and on the target group side, it is important to be aware of and overcome the psychological barriers that can affect output results. The article presents the issues raised by the "technocratic approach" to raising awareness of information security. It presents the hidden assumptions behind the design of the programs, the reasons behind defence mechanisms and resistance points experienced on the user side, and the impact of the

[1] Pszichológus, doktori hallgató, Nemzeti Közszolgálati Egyetem Rendészettudományi Doktori Iskola; e-mail: hederklara@gmail.com

subjective perception of danger and control on the long-term intention to participate in the programs.

Keywords: *information security awareness, cybersecurity, data protection, defence mechanisms*

1. Bevezetés

> „A fegyverként használható tartalmak három leginkább elterjedt célbajuttatási módszere a Lockheed Martin Computer Incident Response Team (LM-CIRT) 2004–2010 közötti megfigyelései alapján az e-mail csatolmányok, a weboldalak és a hordozható USB eszközök."[2]

De miért? Hogyan lehetséges, hogy hatalmas port felvert adatlopási botrányok, személyes rossz tapasztalatok, világméretű zsarolóvírus-támadások után, a rengeteg kiberbiztonsággal, biztonságtudatosítással kapcsolatos erőfeszítések ellenére még napjainkban is áldozatul esünk ilyen közismert trükköknek? Miért van az, hogy:

> „A támadó és a célpont közötti elsődleges kapcsolat egy, a szervezet infrastruktúrájához hozzáféréssel rendelkező személy."[3]

A jelentős biztonságtudatosítási erőfeszítése ellenére miért emelkedik ki még mindig az emberi tényező[4] mint az egyik legjelentősebb kiberbiztonsági kockázati faktor?

2. Információbiztonság, kiberbiztonság és biztonságtudatosság: nehézségek és problémák

A kibertámadások okozta károk napjainkban dollármilliárdokban mérhető összegeket érnek el. Egy elemzés 2019-ben egyedül az egészségügyben globálisan 11,5 milliárd USD-ra becsülte a zsarolóvírusok által okozott károk költségét, 2021-re pedig 20 milliárd USD-ra teszi a várható károkat a szakterületen,[5] és akkor még nem beszéltünk az egyéb szektorokban fellépő veszteségekről.

A nagy társadalmi struktúrákra, fontos szervezetekre, kritikus infrastruktúrákra mért csapások sokszor gazdasági vagy biztonsági okok miatt a nagyközönség számára

---

2 Kiss Attila – Krasznay Csaba: A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai. *Információs Társadalom,* 17. (2017), 1. 55–71.

3 Kiss–Krasznay (2017): i. m. 56.

4 „Még az egyre összetettebb támadások megjelenése ellenére is az adathalászat és a közösségi manipuláció *(social engeneering)* továbbra is igen gyakori fertőzési vektorok a legtöbb rosszindulatú szereplő számára – a tapasztalatlan amatőröktől a legképzettebb csoportokig." Lásd Trend Micro: *A Constant State of Flux Trend Micro 2020 Annual Cybersecurity Report* (2021). 35.

5 Palicz Tamás et al.: „Pénzt vagy életet!". Zsarolóvírusok az egészségügyi informatikai rendszerekben. *Orvosi Hetilap,* 161. (2020), 36. 1503.

„láthatatlanok" vagy kevésbé transzparensek. Azt azonban korántsem állíthatjuk, hogy a kibertámadások az átlagfelhasználó számára ismeretlen problémát jelentenének.

A zsarolóvírus-támadások nagy port felvert, széles sajtónyilvánossággal érintett eseményeivel kapcsolatban sokaknak van személyes rossz tapasztalata is. Azt a személyt pedig, aki maga vagy ismerőse által érintett volt kibertámadásban, esetleg zsarolóvírus miatt vesztette el akár többéves munkájának eredményét, aligha kell a továbbiakban győzködni az információbiztonság fontosságáról. Az ilyen támadások pedig éppen „jövedelmezőségük"[6] miatt egyre gyakoribbá válnak, s így a jelenséggel, valamint összes káros hatásával egyre több hétköznapi felhasználó találkozik.

A kiberbiztonság objektív mutatói mellett tehát a szubjektív percepció is romlik,[7] csakhogy a helyzet mindezek ellenére nem látszik javulni. A gyakori kibertámadások, az információbiztonsági kockázatok növekedése ellenére az információbiztonság-tudatosság nem nőtt jelentősen, és ma sem mondható el, hogy a problémát teljesen magunk mögött hagytuk. De miért nem javul a biztonságtudatosság, amikor a veszély valós, jelentős vagy éppen fokozódó, és ezzel már igen sok érintett szervezet és személy is tisztában van?

2.1. A biztonságtudatosítás „technokrata"[8] megközelítése: jobb szakértők – jobb programok – jobb eredmények (?)

A magyarországi eseményeket tekintve elmondható, hogy erőfeszítésből nincs hiány. Jobbnál jobb szakemberek próbálják a veszély nagyságára, jelentőségére, a kritikus helyzetek felismerésére és elkerülésére felhívni a felhasználók figyelmét. Megközelítésükben a szakszerűség, a hatékonyság, sikeresség és a megelőzés kapja a legfontosabb szerepet. A programok egyaránt kiterjednek az információbiztonság-tudatosság szervezeti, infrastrukturális és egyéni dimenzióinak[9] fejlesztésére is.

A szakértői szemléletet kockázati megközelítés jellemzi, amely a kiberbiztonsági kockázatokkal szembeni kitettségre, érzékenységre, a támadások gyakoriságára és a sikeres támadások által okozott kárra, valamint ezek kivédésére helyezi a hangsúlyt, és ezeknek a szempontoknak a figyelembevételével építi fel stratégiáját.[10]

Ezt a szemléletet jobb híján „technokrata" megközelítésnek is nevezhetjük, amelyben a hatékonyságalapú, tudáson és szakértelmen alapuló, sikerorientált, eszköz- és kimenetközpontú hozzáállás a domináns.

---

6 A számítástechnikai bűnözés miatti globális veszteségeket 2020-ban 1 billió USD-ról 2021-re 6 billió USD-ra becsülik. Lásd: ITU Global Cybersecurity Index 2020.

7 Kiss–Krasznay (2017): i. m.

8 A *„technokrata"* kifejezés sarkított; a hatékonyságalapú, tudáson és szakértelmen alapuló, megoldáskereső nézőpontra alkalmazom.

9 Nemeslaki András – Sasvári Péter László: Az információbiztonság-tudatosság empirikus vizsgálata a magyar üzleti és közszférában. *Infokommunikáció és Jog,* 10. (2014), 60. 169–177.

10 Bányász Péter – Bóta Bettina – Csaba Zágon: Social engineering jelentette veszélyek napjainkban. In *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében.* Budapest, Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 2019. 12–37.

> „Az államoknak, így Magyarországnak is biztosítania kell kiberterének védelmét, amely megkívánja az egyes közszolgálati hivatásnemekben olyan szakértők[11] jelenlétét, akik a szükséges és elégséges mértékben értik az információbiztonság műszaki megközelítését, de saját szakterületükön is magas szintű hozzáértésről tesznek tanúbizonyságot."[12]

A biztonságtudatosítás „technokrata" megközelítése alapján a hatékonyságnövelő célokat jobb szakemberekkel, jobb képzési anyagokkal, szélesebb körben elérhető biztonságtudatosítási programokkal, összefoglalva: jobb szakértőkkel és nagyobb szakszerűséggel lehetne elérni.

Az így felépített programok, képzések általában jól strukturáltak, szakszerűek, effektívek és a legtöbb esetben sikeresek és mérhetően csökkentik a kiberbiztonsági kitettséget. Az elért eredmények pedig Magyarországon sem maradtak el. Mind az információbiztonság, mind pedig a tágabb fogalmi kört magában foglaló kiberbiztonság témakörében számos kiváló szakanyag, képzés, e-learning-tananyag érhető el jelenleg is az érdeklődők, illetve a szervezetek által képzésre kötelezettek[13] számára.[14]

E programok hatékonysága pedig kézzelfoghatóan is megjelenik: Magyarország, az ITU Global Cybersecurity Index 2020 felmérésében igen magas pontszámokat ért el mind a jogi és technikai lépések megtétele, mind a kiberbiztonság irányítási és koordinációs mechanizmusainak kialakítása és összehangolása, mind pedig a kiberbiztonsági kapacitás fejlesztése és a kiberbiztonsági kihívások kollektív kezelésének terén; s így az összesített eredményekben is.[15]

Rendszerszintű kiberbiztonsági elmaradásokról ezért hazánkban a fenti eredmények fényében tehát nem beszélhetünk; a „technokrata megközelítés" lényegében eredményesnek bizonyult. A kiváló szakértők és a valóban elért eredmények ellenére azonban a személyes tapasztalatok mégis azt mutatják, hogy a felhasználók információbiztonság-tudatosságán azért még mindig lehetne mit javítani.[16]

A szakszerűség-orientált megközelítések ilyenkor elsőként általában a már sok szempontból sikeresnek bizonyult módszerek esetleges hibáinak megkeresését, a hibát okozó okok feltárását és kiküszöbölését, valamint a módszerek, eszközök javítását/fejlesztését tűzik ki célul. (Nem pedig egy teljesen új megközelítés alkalmazását.) Melyek lehetnek tehát azok a tényezők, amelyek még mindig gátolják az információbiztonság-tudatosság fejlesztését?

---

11 Kiemelés: H.K.

12 Krasznay Csaba: A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban. *Nemzet és Biztonság,* 10. (2017), 3. 40.

13 Például 2021 novemberében a Probono közigazgatási továbbképzési portálon az „információbiztonság" kifejezésre keresve 18 darab e-learning-képzés, a „kiberbiztonság" kifejezésre keresve pedig 46 elektronikus tananyag érhető el köztisztviselők számára. (A két témakörben végzett keresés eredményei között természetesen van átfedés).

14 Krasznay (2017): i. m.

15 Pontszámok: Jogi intézkedések: 18,16/20; Technikai intézkedések: 16.82/20; Szervezeti intézkedések: 18.29/20; Kapacitásfejlesztési intézkedések: 18,6/20; Együttműködési intézkedések: 19.41; Összpontszám: 91.28/100; Regionális rang: (EU) 22; Minősítés: fejlett ország. Forrás: ITU Global Cybersecurity Index 2020.

16 Például Nemeslaki–Sasvári (2014): i. m. kutatásában az állami intézményeknél és a nagyvállalatoknál a felhasználók 40%-a mondta, hogy megadnák céges jelszavukat valaki másnak.

2.2. A gyenge információbiztonság-tudatosság lehetséges okai

A hagyományos magyarázatok több tényezőt is figyelembe vesznek a biztonságtudatosság hiányosságainak magyarázatára. A biztonsági problémák legjelentősebb okaként első helyen a felhasználók képesség és/vagy ismerethiányát[17] szokták feltüntetni.[18] Ezért az első kézenfekvő magyarázat az, hogy a felhasználók nem ismerik a veszély nagyságát, jellegét, vagy éppen nem rendelkeznek a kivédéséhez szükséges tudással, eszközökkel, esetleg nem állnak a digitális műveltség és az információtudatosság megfelelő érettségi szintjén.[19] A második lehetséges magyarázati kör, hogy a tágabb társadalmi környezet, szervezet nem teszi lehetővé vagy éppen nem támogatja valamilyen módon eléggé az egyének információbiztonság-tudatosságának erősödését.

Harmadik magyarázatként elképzelhető, hogy a biztonsági problémák mögött az áll, hogy a kiberbűnözéssel foglalkozó csoportok „szakmai tudása", intellektuális tőkekoncentrációja magasan meghaladja az átlagfelhasználó lehetőségeit. Így a támadók lépéselőnybe kerülve újabb és újabb – a megtámadottak számára még ismeretlen – „trükkökkel" állnak elő, amelyek kivédésére az érintettek még nem képesek. Nem elhanyagolható magyarázati lehetőség az sem, hogy a kiberbiztonsági előírások, protokollok, egyéni és szervezeti gyakorlatok terén mutatkoznak rések, amelyeket a kiberbiztonsággal foglalkozó szakembereknek kell rövidre zárniuk.

Mindegyik fenti esetben kézenfekvőnek tűnik nagy tudású technikai és képzési szakemberek bevonása, a kiberbiztonsággal kapcsolatos ismeretek és skillek szakmai és felhasználói fejlesztése, biztonságtudatosítással kapcsolatos programok indítása és ezáltal a felhasználók úgynevezett biztonsági megfelelőségének *(security compliance)* és biztonságtudatosságának *(security awareness)* növelése.[20]

2.3. Egy rejtett feltételezés: képzésfejlesztés = jobb programok érdeklődő felhasználóknak

A fenti fejlesztő szándékkal azonban az a probléma, hogy a technokrata megközelítés folyamatos javító szándékának hátterében egy burkolt feltevés figyelhető meg. Az, hogy a biztonságtudatosítási képzések azért nem tökéletesen sikeresek (még), mert az eddig kialakított programok nem érték el a felhasználókat, vagy ha már elérték, akkor esetleg nem voltak megfelelően magas színvonalúak. A fenti logika mentén ezért szakmai továbbfejlesztésük mindenképpen javíthatna a kimeneti eredményességen.

---

17 A tudás, a kognitív ismeretek elsőbbsége még a fogalom meghatározásában is több esetben megjelenik: például „Az általános információbiztonsági tudatosság (information security awareness, ISA) egy munkavállalónak az információbiztonsággal kapcsolatos kérdések és azok következményeinek átfogó ismerete és a potenciál megértése." (Burcu Bulgurcu – Hasan Cavusoglu – Izak Benbasat: Information Security Policy Compliance: An Empirical Study Of Rationality-Based Beliefs And Information Security Awareness. *Management Information Systems Quarterly,* 34. [2010], 3. 532.)

18 Kiss–Krasznay (2017): i. m.

19 Az információbiztonság-tudatosság érettségi modelljeiről részletesebben lásd Tarján Gábor: *Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben.* Doktori (PhD-) értekezés. Budapest, Budapesti Corvinus Egyetem, 2020.

20 Bulgurcu–Cavusoglu–Benbasat (2010): i. m.; Illéssy Miklós – Nemeslaki András – Som Zoltán: Elektronikus információbiztonság-tudatosság a magyar közigazgatásban. *Információs Társadalom*, 14. (2014), 1. 52–73.

E modell rejtett feltételezése az, hogy a megcélzott felhasználók mindegyike egyformán érdekelt abban, hogy megismerje a számára potenciálisan káros információbiztonsági vagy kiberbiztonsági kockázatokat, és igyekeznek, hogy megtanulják ezek felismerését, és hogy képesek legyenek kivédésükre. A biztonságtudatosítás technokrata megközelítésében implicit előfeltétel, hogy a felhasználók szeretnék megszerezni ezeket az információkat, és motiváltak saját vagy szervezetük digitális javainak védelmére. Mivel az érintettek motiváltak a probléma megoldására, szeretnének többet megtudni saját információbiztonságuk javításához. Ehhez pedig szívesen veszik igénybe a szakterület kompetens, nagy tudású szakértői által kialakított képzési, információs lehetőségeket. A felhasználók esetleg lehetnek digitálisan kevésbé képzettek vagy tájékozatlanok a kiberbiztonság területén, de ha egy program felhívja a figyelmet az őket fenyegető digitális veszélyekre, akkor szeretnének fejlődni, megismerni, hogy hogyan védhetik ki a felmerülő veszélyeket, és végül – a biztonságtudatosítási erőfeszítéseknek hála – a képzéseken kialakított, megfelelő skillek birtokában ezt meg is fogják tenni.

A gondolat logikus: jobb/több területről érkező szakemberek → jobb képzési és információs anyagok és programok → szélesebb körben informált + motivált felhasználók → növekvő információbiztonság-tudatosság.[21] A biztonságtudatosítás technokrata megközelítése szerint tehát nincs más teendő, mint az érdeklődő hallgatóság számára jobb szakemberekkel, jobb programokat készíteni, azokat szélesebb körhöz eljuttatni, a felhasználókat jobban felkészíteni a várható veszélyekre és kivédésükre, az eredmények pedig nem maradnak majd el.

Ez az írás azonban arról szól, hogy miért nem igaz minden esetben a fenti logikus feltételezés.

3. A felhasználó mint ismeretlen faktor

Mivel a szakszerűségen és hatékonyságon alapuló eddigi fejlesztések többségében sikeresnek mutatkoznak, a biztonságtudatosságon azonban még mindig lehetne mit fejleszteni, logikus felvetésként felmerül, hogy esetleg a befogadó oldalon kell keresni a probléma forrását.

3.1. Tulajdonságkutatás: célcsoportra szabott programok – jobb eredmények?

Az információbiztonág technokrata megközelítésében gyakran megjelenik az érintettek valamilyen jellemzőjének, tulajdonságának, hosszú távon állandó attribútumának vizsgálata. Sok tényező egyértelműen befolyásoló hatással bír az információbiztonság-tudatosságra. A személyiségjegy, nem, kor, kulturális háttér,[22] de rengeteg más

[21] Például Képességfejlesztés, szélesebb, jobban átgondolt képzési struktúra a témában a közigazgatásban (Krasznay [2017]: i. m.)

[22] Bányász–Bóta–Zágon (2019): i. m.

tényező is megjelenik, amelyek hosszú távon befolyásolják, hogy az adott személy mennyire tudatosan és milyen sikeresen küzd meg a kiberbiztonsági kihívásokkal, mennyire hajlandó az információbiztonsági előírásoknak megfelelni.[23]

A szakszerűségen és hatékonyságon alapuló technokrata megközelítés szerint, ha a befogadói oldal jellemzői pontosan ismertekké válnak, akkor számukra sokkal jobban testre lehet szabni a képzéseket és tájékoztató anyagokat. Ez alapján, ha a célcsoport számára fontosabb problémákat dolgozunk fel a számukra érthetőbb módon, vagy szükség esetén interaktívabb képzést alkotunk, esetleg gamifikáljuk a tartalmat, vagy a befogadók igényeihez pontosabban igazodó képzésmódszertani eszközt alkalmazunk, akkor jobban megragadhatjuk a célcsoport figyelmét, jobb és tartósabb eredményeket érhetünk el, így végül sikeresebb lesz a kidolgozott program. Az ilyen szakszerű erőfeszítések pedig mindig elérnek valamilyen eredményt.

Egy jobb, szakszerűbb, a célcsoport igényeit jobban figyelembe vevő és ahhoz jobban illeszkedő képzés/program mindig eredményesebb, mint az, amely nem vesz figyelembe ilyen szempontokat. A baj csak az, hogy még mindig ott tartunk, hogy ugyanazon a paradigmán belül javítgatjuk a már meglévő eszközöket. Még mindig azt a rejtett feltételezést érvényesítjük, hogy a felhasználó motivált vagy – kevésbé szerencsés esetben – ugyan még most nem motivált, de ha megismeri a veszély nagyságát, akkor mindenképpen motiválttá válik. Ha a fenti feltételezés igaz, akkor a szakszerűbb, személyre szabottabb program kialakítása biztos, hogy eredményesebb lesz. De amíg a felhasználókat passzív – de érdeklődő – befogadónak tekintjük, addig nehezen magyarázható az a hatás, hogy a meglévő jelentős erőfeszítések, elérhető információk, folyamatosan javuló és egyre jobban elérhető képzések ellenére az információbiztonság-tudatosság sok esetben még mindig nem éri el a kívánt szintet.[24]

Mivel a technokrata megközelítés nagy hangsúlyt fektet a képzések, programok szakszerűségére és hatékonyságára, a bizonyítottan hatékony eszközök birtokában az elégtelen eredmények okainak keresésekor a következő logikus feltételezés az, hogy valamilyen szempontból a célcsoport a problémás (a nagy szaktudással, nagy gondossággal kialakított eszközök nem lehetnek azok, hiszen ezek már eddig is bizonyították eredményességüket.)

---

[23] Rendkívül részletes irodalmi áttekintés a témában Rao Faizan Ali et al.: Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. *Applied Sciences,* (2021), illetve Rodrigo Hickmann Klein – Luciano Mezzomo Edimara: What Influences Information Security Behavior? A Study with Brazilian Users. *Journal of Information Systems and Technology Management,* 13. (2016), 3. 479–496.

[24] A szerző egy régebbi saját kérdőíves kutatásában (2018), egy – nagyrészben magasan képzett, döntően erős felhasználói IKT-kompetenciával rendelkező fővárosi, döntően értelmiségi nőkből álló – 96 fős minta tagjai közül egyetlen egy személy sem(!) állította, hogy az internetes oldalakon felugró cookie-kat minden esetben elolvassa, és 67 fő (69,9%) pedig a „Lényegében soha", vagy pedig az „Általában nem, vagy csak nagyon ritkán" választ választotta.

3.2. Problémás célcsoport: a felhasználók hibáztatása

Az első és egyben leggyakoribb „vádpont" a felhasználókkal szemben, hogy nem megfelelően cselekednek: elővigyázatlanok, nem fordítanak elég figyelmet a kérdésre, vagy éppen kényelmességből nem követik az előírásokat.

> „Hiába védjük rendszereinket a legmodernebb és legerősebb fizikai és logikai védelmi intézkedésekkel, ha az elektronikus információs rendszereket használók nem tartanak lépést a technológiai fejlődéssel, illetve nem kellően tudatosak és elővigyázatosak a rendszerek használata során."[25]

Ez az érvelés nem tulajdonít mélyebb, hosszú távon ható háttérokokat a megjelenő viselkedés mögött: a felhasználók így viselkednek, és kész. Megoldásként a szerző a következő mondatban – a technokrata megközelítés szellemében – jobb képzéseket ajánl:

> „A felhasználók digitális és információbiztonsági tudásának, kompetenciáinak fejlesztésére a tudatosítási programok nyújtják a leghatékonyabb megoldást." [26]

Légárd cikkében később részletezi, hogy a szimuláción, gamifikáción alapuló képzések miért sikeresebbek, mint az elsősorban kognitív ismeretátadásra épülő egyéb módszerek, de egyéb tekintetben nem tér ki arra, hogy mi okozza az általa alapproblémaként megnevezett nehézséget: nevezetesen, hogy a felhasználók miért nem tartanak lépést a technológiai fejlődéssel, miért nem kellően tudatosak, és miért elővigyázatlanok.

Más kutatók azonban nemcsak a tényleges viselkedést vizsgálják, hanem keresik a jelenség hátterében meghúzódó mozgatórugókat is. Sok esetben – okfeltárásként, jobbító szándékkal, de – felmerül a felhasználók személyes tulajdonságainak elemzése, „kárhoztatása" is az alacsony információbiztonság-tudatosság okainak keresésekor. Ha azzal a feltételezéssel élünk, hogy a célcsoport a problémás, akkor eszerint feltételezhetően olyan tulajdonságok jellemzik, amelyek általában is gátolják a biztonságtudatosság erősödését. Esetleg feltételezhetjük, hogy a sikertelenség oka, hogy a felhasználók egyszerűen „nem elég jók": nem elég felkészültek, nem eléggé tájékozottak, nem megfelelő az IKT-kompetenciájuk, alacsony a digitális műveltségük, digitális írástudásuk korlátozott,[27] túl kockázatkeresők, nem kellően informáltak (még), esetleg félreinformáltak, nem állnak az információbiztonság-tudatosság érettségének megfelelő szintjén, és hiányosságként felróható tulajdonságaik még hosszan sorolhatók tovább.

A 2020-ban elfogadott *Nemzeti Biztonsági Stratégia* például így fogalmaz: „Általános jelenség továbbá a felhasználók információbiztonsági tudatosságának

---

25 Légárd Ildikó: Játék a jövőért 3. Az információbiztonsági tudatosság fejlesztési lehetősége egy gamifikált applikáció segítségével. *Polgári Szemle,* 17. (2021), 1–3. 358.

26 Légárd (2021): i. m. 358.

27 „Ennek okaként *(*mármint annak, hogy a felhasználó nem veszi észre folyamatban lévő social engineering támadást*)* elsősorban a biztonságtudatosság hiányát, a digitális írástudatlanságot azonosíthatjuk." (Bányász–Bóta–Zágon [2019]: i. m. 13.)

alacsony szintje,[28] holott a felhasználók megfelelő információbiztonsági tudatossága a kiberincidensek megelőzésének egyik kulcseleme."[29]

A fenti állítás pedig valóban megalapozott. A 2012-ben amerikai információbiztonsági szakemberek által kidolgozott SANS-kérdőív információbiztonság-tudatosság koncepcionális modellje szerint a felhasználók 5 nagyobb kockázati csoportra oszthatók, de csoportosíthatók digitális műveltség szerint is a rendkívül tudatos és szabálykövető csoporttól, a tájékozatlan és az előírásokat be nem tartó személyekig. Nemeslaki és Sasvári (2014)[30] kutatási eredményei alapján e két kategorizáció között van korreláció: az információbiztonság-tudatosság és az alkalmazottak digitális műveltsége között jól látható kapcsolat figyelhető meg. A nagyon alacsony vagy rossz digitális műveltséggel rendelkezők magasabb valószínűséggel kerülnek a nagyobb kockázati kategóriák valamelyikébe.

Amennyiben pedig a felhasználók speciális tulajdonságai, alacsony IKT-kompetenciája, digitális műveltségének korlátozottsága vagy más tényező áll az alacsony információbiztonság-tudatosság hátterében, akkor pedig a megoldás ismét csak a „technokrata" szemléletben már megjelent érvelés: Fejlesszük a felhasználókat, csináljunk jobb programokat, szabjuk jobban testre a célcsoport számára, és az eredmények nem fognak elmaradni! Ha problémás célcsoporttal találkozunk, akkor nagyobb szakértői erőfeszítés szükséges, de a módszer sikeres lesz.

A fenti érvelés pszichés előnyei a képzéseket/programokat előkészítő, abba mindent beleadó és azt gondosan kivitelező szakértők számára, hogy saját szakterületükön határozzák meg a beavatkozási területet, a minőség javítására helyezik a hangsúlyt, ugyanakkor nem kell szembesülniük módszereik korlátaival sem (például hogy valamilyen fontos szempontot nem vettek figyelembe). A felhasználók elmarasztalása, esetleges hibáztatása pedig csökkenti a lehetséges kudarcokból fakadó kellemetlen érzéseket („Nem a program volt sikertelen, hanem a felhasználók érdektelenek/motiválatlanok/stb."), és növeli a további erőfeszítések sikerébe vetett hitet.

A programkészítők oldaláról tehát a biztonságtudatosítás sikerének egyik pszichés gátja a saját szaktudásba vetett feltétlen bizalom, a problémákra kizárólagosan a saját szakterületen keresett megoldási mód preferálása; az a hit, hogy ugyanazzal a módszerrel, csak jobban kivitelezve el lehet azt az eredményt érni, amelyet eddig még nem sikerült (a felhasználók alkalmatlansága miatt).

Ez a hatás pedig csak ront a helyzeten, hogyha a felhasználók nem csupán valamilyen tulajdonságaik, jellemzőjük miatt sikertelen, jóindulatú passzív érdeklődők, akik várják a rájuk szabott, kiváló szakmai programokat, hanem kifejezetten ellen is állnak az ilyen szakmai erőfeszítéseknek.

[28] Kiemelés: H.K.
[29] Lásd: https://net.jogtar.hu/jogszabaly?docid=A20H1163.KOR&txtreferer=00000001.txt
[30] Nemeslaki–Sasvári (2014): i. m.

4. A biztonságtudatosítás pszichés gátjai

4.1. Amikor a célcsoport ellenáll: hárítás, távolítás és bagatellizálás

Az ellenállás első védvonala az érdektelenség. Az a gondolat, hogy egy nyilvánvalóan valid – magánéleti és munkahelyi – információbiztonsági kockázattal/veszéllyel szembesülve az érintettek nemhogy nem mutatnak érdeklődést a helyzet jobb megértésére, az adott problémával való megküzdési lehetőségek megismerésére, saját skilljeik javítására, hanem az ilyen erőfeszítéseknek esetleg még aktívan ellen is állnak, elsőre igen furcsa feltételezésnek tűnhet.

E gondolat logikátlanságának ellenére mégis gyakori az a tapasztalat, hogy a felhasználók sokszor meglehetős érdektelenséget mutatnak a témában: nem tájékozódnak a lehetséges veszélyekről és ezek kivédési lehetőségeiről, ha lehetséges „ellógják" az információbiztonsággal kapcsolatos programokon való részvételt, vagy ha esetleg részt is vesznek ezeken, akkor azt ímmel-ámmal teszik, önként nem keresnek képzési, fejlesztési lehetőségeket, és csak a minimális információbiztonsági szervezeti elvárásoknak tesznek eleget. Miért?

E jelenség egyik oka a hárítás, gyakori módszerei: a távolítás, bagatellizálás. A hárítások olyan tudattalan énvédelmi szabályozó mechanizmusok, amelyekkel a számunkra kellemetlen, elfogadhatatlan vagy éppen fájdalmas lelki tartalmak tudatba való betörését szabályozzuk (korlátozzuk).

Az információbiztonsággal kapcsolatos kérdésekben a felhasználók elvileg ismerik az olyan fontosabb kiberbiztonsági kockázatokat, mint a zsarolóvírusok, jelszófeltörések, adathalászati eszközök és társaik; tisztában vannak a szervezeti előírásokkal és elvárásokkal, és azt is tudják, hogy saját jól felfogott önérdekük is azt kívánja, hogy tájékozottak legyenek a rájuk leselkedő legújabb veszélyekkel kapcsolatban. Ennek ellenére gyakran mégsem mutatnak érdeklődést az ilyen képzések, oktatási programok iránt. A kifogások tárháza rendkívül változatos: a „Nem érdekel annyira az informatiká"-tól, az „Ez minket úgysem érint"-ig.

Ez a jelenség a probléma távolítása; az érintettek a lehetséges információbiztonsági veszélyekkel szembesülve kellemetlen érzéseket élnek át, amelyek zavaró hatását aktív pszichés hárításokkal csökkentik. A felhasználók bár általában elismerik a védekezés elvi fontosságát, de saját maguk és szervezetük szempontjából nem minősítik jelentősnek a veszélyt. A tennivalók fontosságát és sürgősségét bagatellizálják, hárításaiknak ellentmondó információkat elfojtják, racionalizálják. (Például Nemeslaki és Sasvári [2014] kutatásában a közszféra vizsgálatánál az önkormányzatoknál dolgozók 55%-a úgy nyilatkozott, hogy szerinte az adataik nem érdekesek mások számára.)

A kiberbiztonsági veszélyekkel kapcsolatos kellemetlen tudattartalmak távolítása csökkenti a személyek szorongását, „megkíméli" a felhasználókat attól, hogy számukra kényelmetlen, vagy éppen aggasztó veszélytényezőkkel kelljen foglalkozniuk mindennapi (munka)tevékenységeik során. A mechanizmus olyan személyes előnyei, mint a szubjektív biztonságérzet növelése vagy a már megszokott munkarutin fenntartása pedig kellő megerősítő hatással bírnak a hárítások hosszú távú fennmaradásához,

de – nem elhanyagolható mellékhatásként – az információbiztonsággal kapcsolatos érdeklődés és motiváció csökkenéséhez vezethetnek.

A célcsoport tagjai tehát saját pszichés integritásuk védelmében aktív hárításokkal élnek, amelyek csökkentik a szubjektív veszélyérzetet, növelik a biztonságos világba vetett hitet, ugyanakkor az információtudatosítási erőfeszítésekkel szemben érdektelenné teszik az adott személyt. („Nem érdekel a képzés, mert nálunk úgysincs ilyen probléma.")

4.2. Kognitív torzítások a hárítások, az „érdektelenség" hátterében

Az informatikai kockázatokkal kapcsolatos hárítás, távolítás, alulbecslés mögött gyakran pszichológiai háttérmechanizmusok miatt kialakuló kognitív torzítások állnak. A heurisztikák, következtetési ugrások, tévedések, torzítások *(cognitive biases)* alapvetően jellemzők az emberi gondolkodásra.[31] A kognitív torzítások olyan szisztematikus, minden emberre jellemző rendszeres hibák, amelyek megjelennek az emberek ítélet- és döntéshozatalában, s amelyeket kognitív korlátok, motivációs tényezők és/vagy a természetes környezethez való alkalmazkodás hozott létre.[32]

Ilyen kognitív torzítás, távolító hatás a „személyes sérthetetlenség illúziója"[33] és a „harmadikszemély-hatás".[34] Mindkét elmélet szerint a személyek magukat és a hozzájuk hasonlókat pozitívabb színben, a veszélyeknek kevésbé kitetteknek és kevésbé befolyásolhatónak látják, mint a „többieket" (mindenki mást). Úgy gondolják, hogy a negatív kimenetelű, veszélyes események valószínűleg más személyekkel fognak megtörténni, mint velük. Ez a mechanizmus fenntartja a biztonságos, kiszámítható, igazságos világ illúzióját, ugyanakkor valós veszélyek esetében a probléma kockázatos elfedéséhez, hárításához vezethet, amely elősegíti az áldozati ignorancia, a sérthetetlenség, a „velem nem fordulhat elő" érzésének kialakulását.

E kognitív torzítások csökkentik a kialakuló szubjektív veszélyészlelést és ennek következtében a motivációt is a lehetséges kiberbiztonsági kockázatok kivédésére és információtudatosabb viselkedés kialakítására (hiszen ez „Másvalaki Problémája"[35]).

---

31 Amos Tversky – Daniel Kahneman: Judgment under Uncertainty: Heuristics and Biases. *Science*, 185. (1974), 4157. 1124–1133; Eldar Shafir – Robin A. LeBoeuf: Rationality. *Annual Review of Psychology,* 53. (2002). 491–517.

32 „Systematic error in judgment and decision-making common to all human beings which can be due to cognitive limitations, motivational factors, and/or adaptations to natural environments." Andreas Wilke – Mata Rui: Cognitive Bias. In V. S. Ramachandran (szerk.): *The Encyclopedia of Human Behavior,* 1. Academic Press, 2012. 531.

33 Fogalom: Philip G. Zimbardo – Ebbe B. Ebbesen – Christina Maslach: *Influencing attitudes and changing behavior.* London, Addison-Wesley, 1977.

34 A harmadikszemély-hatás: az egyén önmagát és azokat, akiket magához hasonlónak tart vagy feltételez, védettnek vél az – elsősorban a média által okozott – káros hatásokkal szemben. Úgy gondolja, hogy e káros hatások nagyobb valószínűséggel fognak másokat sújtani. W. Phillips Davison: The Third-Person Effect in Communication. *Public Opinion Quarterly,* 47. (1983), 1. 1–15.

35 „Az MVP-pajzs a Galaxis útikalauz stopposoknak sorozat harmadik kötetében, »Az élet, a világmindenség, meg minden« című Douglas Adams regény egyik módszere tárgyak álcázására. Lényege, hogy a tárgyat nem lehet láthatatlanná tenni, sem eltakarni, de ha meggyőzzük a szemlélőt, hogy a tárgy Másvalaki Problémája (MVP), akkor egész egyszerűen nem vesz tudomást a létezéséről. A szeme látja, de az agya nem hajlandó

Az eredmény pedig: a kognitív torzítások hatására a felhasználók túlzónak érzik a kiberbiztonsággal kapcsolatos veszélyek hangoztatását. Úgy látják, hogyha vannak is ilyen problémák, akkor az ezzel kapcsolatos tájékoztatások indokolatlanul felnagyítottak, hiszen ezek a veszélyek főleg másokat érintenek. Mivel kevésbé érzik magukat személyesen érintettnek a kérdésben, motivációjuk a képzéseken/programokon való részvételre csökken: a célcsoport érdektelenné válik.

4.3. Szubjektív veszélypercepció a digitális térben: a veszély alulbecslése

A biztonságtudatosítási intézkedések, képzések és eljárások nem egy passzív, jóindulatúan elnéző vagy feltétlenül lelkes befogadói közeget érnek el. A felhasználói magatartást és a biztonságtudatossági erőfeszítésekhez való hozzáállást ugyanis nagyban befolyásolja a felhasználók veszélypercepciója, saját lehetőségeihez kapcsolódó kontrollérzete és a biztonságtudatossághoz, információbiztonsághoz kapcsolódó már meglévő attitűdje.[36]

Az információbiztonsági problémák hárításának másik oka az informatikai veszélyek viszonylag magas látenciája és sok esetben „láthatatlansága". Az események rejtve maradnak a felhasználók elől, nem szembesülnek azonnal a következményekkel, az okozott kárral, gyakran sem magát az eseményt, sem pedig annak veszélyességét, néha még magát az okozott kárt sem ismerik fel.

Az így kialakuló hamis szubjektív biztonságérzet oka, hogy: „Az internet világában evolúciós viselkedéskészletünk nem, vagy nem jól működik."[37] A fenyegetettség szubjektív megéléséhez, az áldozattá válás lehetőségének kiértékeléséhez a digitális térben ugyanis gyakran hiányoznak a szubjektív veszély érzékeléséhez evolúciósan előhúrozottan szükséges affektív komponensek és látható jelek: a veszély nem nyilvánvaló, a lehetséges károk és következmények elővételezése gyakran nehézségekbe ütközik, az esemény bekövetkezésének valószínűsége pedig nem megbecsülhető.

A nem jól felismerhető veszélyek pedig megerősítik a már említett „személyes sérthetetlenség illúziója", illetve a „harmadiszemély-hatás" következtében létrejött téves vélekedést: azt, hogy a veszélyre vonatkozó tájékoztatások túlzók, a helyzet nem igényel azonnali beavatkozást, nem szükséges személyes erőfeszítés a kérdésben, nincs szükség a képzéseken való részvételre.

Az eredmény: a célcsoport a veszélyek alulbecslése esetén motiválatlanná, érdektelenné válik.

Amennyiben a programok készítői tisztában vannak a fenti problémával, a veszély alulbecslése esetén a biztonságtudatosítás klasszikus megközelítése a veszélytudat erősítése: a lehetséges kockázatok hangsúlyozása, a személyes érintettség érzésének

felfogni és értelmezni a látványt, hiszen az nem rá tartozik, nem az ő dolga." Forrás: https://hu.wikipedia.org/wiki/A_Galaxis_%C3%BAtikalauz_stopposoknak_technol%C3%B3gi%C3%A1ja

36 Klein–Edimara (2016): i. m.; Csépe Valéria: A szubjektív biztonság pszichológiai dimenziói. In Finszter Géza – Sabjanics István (szerk.): *Biztonsági kihívások a 21. században*. Budapest, Dialóg Campus, 2017. 275–288; Ali et al. (2021): i. m.

37 Csépe (2017): i. m. 278.

növelése. („Erősítsük bennük, hogy őket személyesen is érinti a veszély, akkor majd motiváltabbak lesznek a programokban való részvételre.")

Sajnos nem, vagy nem mindig. A felhasználók oldaláról ugyanis ezekkel a módszerekkel is gond lehet.

4.4. Szubjektív veszélypercepció a digitális térben: a veszély túlbecslése

Mint ahogy arról már szó esett, a felhasználók megkerülhetetlenül találkoznak az információbiztonság árnyoldalaival (például zsarolóvírusok, adatlopások), de ezekkel kapcsolatos veszélyérzetüket aktív hárításokkal csökkentik az élhetőbb élet érdekében.

A biztonságtudatosítással foglalkozó programok nagy erőfeszítést tesznek azért, hogy ezt a hárítást lebontsák, a személyeket szembesítsék a valós veszély sokszínűségével, jelentőségével és lehetséges személyes káraival. Ilyen esetben az addig „boldog tudatlanságban" (aktív hárításban) lévő személy dömpingszerűen szembesül a lehetséges problémák rendkívül széles tárházával, olyan veszélyek elkerüléséhez kap tanácsokat, amelyek létezéséről eddig esetleg még csak nem is hallott.

Egy kidolgozott, a kiberbiztonsági veszélyekre és károkra fókuszáló, rendkívül szakszerű és esetleg az érzelmekre (félelem, aggodalom) is sikeresen ható képzés/program pedig előfordulhat, hogy túlterheli a célcsoportot. Ha a képzés/program (túl) sikeresen bontja le az addig felépített hárítási mechanizmusokat, az addig féken tartott negatív érzelmek, aggasztó gondolatok elönthetik a célszemélyeket. Ha az érintettek a tájékoztatás után a veszély valós mértékével szembesülnek, a lebontott hárítások és az új információk következményeként esetleg a valóságosnál sokkal nagyobbnak látják a személyes veszélyeztetettség lehetőségét.

A veszély túlértékelése viszont újabb negatív érzelmeket generálhat, és megjelenhet a személyes alkalmatlanság érzése. („Én túl keveset tudok ezeknek a veszélyeknek a kivédéséhez.") Kialakulhat a veszélyes esemény valószínűségének túlbecslése és a saját hatékonyság alulbecslése is. („Mit csináljak, aki el akarja lopni az adataimat, az el is fogja lopni. Úgyse tudok tenni ellene semmit.")

Az informatika területén járatlan célszemély pedig úgy érezheti, hogy olyan területen szembesül – a számára rendkívül veszélyes eseményekkel – amelyeknek sem kialakulását, sem kivédését nem érti, a megakadályozásra ajánlott eszközöket túl bonyolultnak látja. Következményként a személyes hatékonyságba vetett hit gyöngül, a felhasználók a veszélyeket kivédhetetlennek, vagy csak nagyon korlátozottan megakadályozhatónak ítélhetik. Az eredmény: a felhasználó önbizalma csökken, a problémák megakadályozását lehetetlennek, magát tehetetlennek és kétségbeesettnek érzi.

Mivel a biztonságtudatosítás nem egy elemből álló esemény, hanem folyamat, a veszélyek túlhangsúlyozása miatt elbizonytalanított felhasználók kerülni kezdik a további hasonló helyzeteket. Aktívan ellenállnak, hogy részt vegyenek további olyan programokon, amelyeken esetleg még több informatikai nehézséggel, kiberbiztonsági veszéllyel szembesülnének, s amelyek hatására még inkább tehetetlennek éreznék magukat.

Összefoglalva: a képzésekben/programokban a veszélyek (túl)hangsúlyozása a felhasználókban erős negatív érzelmeket (például aggodalmakat) generálhatnak, amelyek tehetetlenségérzéshez, haraghoz, hárításhoz vezethetnek. Az eredmény: a felhasználók hosszú távon aktívan ellenállhatnak a programoknak, leértékelhetik az erőfeszítéseket, kerülhetik a részvételt a következő eseményeken/képzéseken. („Ha túl nagy a veszély, ami ellen nem tudok semmit sem tenni, akkor inkább nem is akarom tudni, nem is akarok vele foglalkozni.")

4.5. Szubjektív kontrollpercepció a digitális térben: a kontroll túl- és alulbecslése

Másik gond, hogy a harmadik generációs informatikai bűncselekmények legtöbbször „nagy valószínűségű és kis kárt okozó" *(high possibility – low impact)* jellegűek. Az ilyen események esetén az érintettek gyakran „tanult tehetetlenséget"[38] mutatnak: úgy gondolják, hogy nem tudnak szinte semmit tenni az ilyen esetek ellen, ezzel kár is próbálkozni, az úgyis bekövetkezik. Mivel a veszély és az okozott kár nem azonnal jelenik meg, sok esetben teljesen láthatatlan marad az érintett számára, a felhasználók motiváltsága az információbiztonság-tudatos viselkedés növelésére, a veszélyek kivédésére alacsony maradhat.

A veszélyek kivédésével kapcsolatos szubjektív kontroll érzete („Ezt meg tudom akadályozni, ezt ki tudom védeni") nagyban befolyásolja, hogy a felhasználók hogyan értékelik az adott információbiztonsági problémát. A lehetséges személyes kontrollszint szempontjából a kiberbiztonsági veszélyek pedig igen széles skálán mozoghatnak: a jól látható, könnyen kivédhető eseményektől a szinte láthatatlan, rendkívül szofisztikált, nehezen kivédhető, nagy károkat okozó kiberbiztonsági támadásokig.

A személyes kontroll és hatékonyság túlbecslése nem túl gyakori esemény, de következményeként kialakulhat a veszélyek alulbecslése és a biztonságtudatosítási programok iránti motiválatlanság is. („Minek menjek el, ez nekem a kisujjamban van.")

Sokkal nagyobb gondot jelent azonban a személyes hatékonyság alulbecslése: az hogy a felhasználók a veszélyt túl nagynak, saját lehetőségeiket, IKT-kompetenciáikat túl korlátozottnak és nehezen fejleszthetőnek ítélik meg. („Minek menjek el, úgyse tudok ellene tenni semmit. Minek menjek el, ez nekem túl bonyolult, úgysem tudom megtanulni.")

Az eddig felsorolt pszichés gátak, mind a hárítások, kognitív torzítások, mind pedig a veszélyek alul-, illetve túlbecslése, valamint a szubjektív személyes kontroll nem megfelelő megítélése nagyban befolyásolja, hogy az érintettek hosszú távon mennyire motiváltak az információbiztonság-tudatosságuk fejlesztésében és az ilyen programokon/képzéseken való részvételben.

---

38 A „tanult tehetetlenség" *(learned helplessness)* az a jelenség, amikor a személy az addig őt ért kiszámíthatatlan negatív hatások eredményeképpen azt a meggyőződést alakítja ki, hogy tehetetlen a fellépő eseményekkel szemben, még akkor is, ha valójában lehetősége lenne a probléma megoldására. A tanult tehetetlenség kialakulása után a cselekvés lehetőségét feladja, lemond a helyzettel való megbirkózás lehetőségéről. Steven F. Maier – Martin E. Seligman: Learned helplessness: Theory and evidence. *Journal of Experimental Psychology: General,* 105. (1976), 1. 3–46.

Az információbiztonság-tudatosság sikeres fejlesztéséhez a felhasználóoldali pszichés gátak felismerése és figyelembevétele elengedhetetlenül szükséges. Az eredményes programok feltétele a reális veszélypercepció és információbiztonsági skillek kialakítása mellett a hangsúly áthelyezése a felhasználói önbizalom és a személyes hatékonyság erősítésére.

5. Összefoglalás

A 21. században az információbiztonság-tudatosítással kapcsolatos programok szerepe és jelentősége jelentősen felértékelődött. A sikeres beavatkozáshoz azonban elengedhetetlen, hogy mind a készítők, mind pedig a felhasználók tisztában legyenek azokkal a pszichés gátakkal, amelyek kiváló programok esetén is csökkenthetik a kimeneti eredményességet.

A biztonságtudatosítás „technokrata megközelítése" rendkívül sikeres a jól megtervezett és kiválóan kivitelezett programok megalkotásában, de kérdéseket vet fel az olyan változó tényezők figyelembevételében, mint a résztvevők pszichológiai hárításainak, kognitív torzításainak, a veszélyek szubjektív percepciójának és a személyes hatékonysággal kapcsolatos célcsoporti vélekedéseknek a figyelembevétele.

Ahhoz, hogy egy célcsoportba tartozók az információbiztonság-tudatosítás hosszan tartó folyamatában hosszú távon is motiváltak maradjanak, a tervezőknek a programok/képzések sorozata közben kell biztosítania, hogy a felhasználók motiváltak maradjanak a következő szakaszba lépésre, a folyamatos továbbfejlődésre. Mindehhez nagy segítséget jelenthet a felhasználói félelmek, nehézségek, ellenállási pontok és okok megismerése, a veszélypercepció erősítése helyett a személyes hatékonyság erősítésére áthelyezett képzési hangsúly.

A biztonságtudatosítás hosszú távú folyamat. Sikeressége össztársadalmi érdek, amelynek elérésében a készítői és felhasználói nehézségek, pszichológiai gátak megismerése és az eredmények felhasználása csak egy újabb feladat a kiberbiztonsági veszélyek csökkentése felé vezető úton.

Felhasznált irodalom

163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Online: https://net.jogtar.hu/jogszabaly?docid=A20H1163.KOR&txtreferer=00000001.txt

Ali, Rao Faizan – Panneer Selvam – Dhanapal Durai Dominic – Emad Azhar – Mobashar Rehman – Abid Sohail: Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. *Applied Sciences,* (2021). Online: https://doi.org/10.3390/app11083383

Bányász Péter – Bóta Bettina – Csaba Zágon: Social engineering jelentette veszélyek napjainkban. In *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében.* Budapest, Magyar Rendészettudományi Társaság

Vám- és Pénzügyőri Tagozat, 2019. 12–37. Online: https://doi.org/10.37372/mrttvpt.2019.1.1

Bulgurcu, Burcu – Hasan Cavusoglu – Izak Benbasat: Information Security Policy Compliance: An Empirical Study Of Rationality-Based Beliefs And Information Security Awareness. *Management Information Systems Quarterly,* 34. (2010), 3. 523–548. Online: https://doi.org/10.2307/25750690

Csépe Valéria: A szubjektív biztonság pszichológiai dimenziói. In Finszter Géza – Sabjanics István (szerk.): *Biztonsági kihívások a 21. században*. Budapest, Dialóg Campus, 2017. 275–288.

Davison, W. Phillips: The Third-Person Effect in Communication. *Public Opinion Quarterly,* 47. (1983), 1. 1–15. Online: https://doi.org/10.1086/268763

Illéssy Miklós – Nemeslaki András – Som Zoltán: Elektronikus információbiztonság tudatosság a magyar közigazgatásban. *Információs Társadalom,* 14. (2014), 1. 52–73. Online: https://doi.org/10.22503/inftars.XIV.2014.1.3

International Telecommunication Union (ITU): Global Cybersecurity Index 2020. Online: www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Kiss Attila – Krasznay Csaba: A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai. *Információs Társadalom,* 17. (2017), 1. 55–71. Online: https://doi.org/10.22503/inftars.XVII.2017.1.4

Klein, Rodrigo Hickmann – Luciano Mezzomo Edimara: What Influences Information Security Behavior? A Study with Brazilian Users. *Journal of Information Systems and Technology Management,* 13. (2016), 3. 479–496. Online: https://doi.org/10.4301/S1807-17752016000300007

Krasznay Csaba: A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban. *Nemzet* és *Biztonság,* 10. (2017), 3. 38–53. Online: https://doi.org/10.32576/nb.2017.3.4

Légárd Ildikó: Játék a jövőért 3. Az információbiztonsági tudatosság fejlesztési lehetősége egy gamifikált applikáció segítségével. *Polgári Szemle,* 17. (2021), 1–3. 358–373. Online: https://doi.org/10.24307/psz.2021.0726

Maier, Steven F. – Martin E. Seligman: Learned helplessness: Theory and evidence. *Journal of Experimental Psychology: General,* 105. (1976), 1. 3–46. Online: https://doi.org/10.1037/0096-3445.105.1.3

Nemeslaki András – Sasvári Péter László: Az információbiztonság-tudatosság empirikus vizsgálata a magyar üzleti és közszférában. *Infokommunikáció* és *Jog*, 10. (2014), 60. 169–177. Online: https://infojog.hu/wp-content/uploads/pdf/201460_NemeslakiAndras_SasvariPeter.pdf

Palicz Tamás – Sas Tibor – Tisóczki József – Bencsik Balázs – Joó Tamás: „Pénzt vagy életet!" Zsarolóvírusok az egészségügyi informatikai rendszerekben. *Orvosi Hetilap,* 161. (2020), 36. 1498–1505. Online: https://doi.org/10.1556/650.2020.31788

Shafir, Eldar – Robin A. LeBoeuf: Rationality. *Annual Review of Psychology,* 53. (2002). 491–517. Online: https://doi.org/10.1146/annurev.psych.53.100901.135213

Tarján Gábor: *Az információbiztonsági tudatosság* érettségi *szintjének mérése szervezetekben.* Doktori (PhD-) értekezés. Budapest, Budapesti Corvinus Egyetem, 2020. Online: http://phd.lib.uni-corvinus.hu/1090/1/Tarjan_Gabor_dhu.pdf

Trend Micro: *A Constant State of Flux Trend Micro 2020 Annual Cybersecurity Report* (2021). Online: https://documents.trendmicro.com/assets/rpt/rpt-a-constant-state-of-flux.pdf

Tversky, Amos – Daniel Kahneman: Judgment under Uncertainty: Heuristics and Biases. *Science*, 185. (1974), 4157. 1124–1133. Online: https://doi.org/10.1126/science.185.4157.1124

Wilke, Andreas – Mata Rui: Cognitive Bias. In V. S. Ramachandran (szerk.): *The Encyclopedia of Human Behavior,* 1. 531. Academic Press, 2012. Online: https://s3.amazonaws.com/arena-attachments/557491/b16d97da35ed37a0a022e806c-c931a0d.pdf

Zimbardo, Philip G. – Ebbe B. Ebbesen – Christina Maslach: *Influencing attitudes and changing behavior.* London, Addison-Wesley, 1977.

Tartalom