NEMZETBIZTONSÁGI SZEMLE
13. évfolyam (2025) 3. szám 108–126. | DOI: 10.32561/nsz.2025.3.7

Drusza Tamás,[1] Mezei József,[2]
Solti István,[3] Regényi Kund[4]

A biztonság tudatosítása mint titkosszolgálati funkció

Nemzetközi példák alapján

Security Awareness as a Secret Intelligence Function,

Based on International Examples

A titkosszolgálatok alapvető funkciói egyes szakértői vélemények szerint: az információgyűjtés, az információ menedzselése, a kémelhárítás és a fedett műveletek. Ezt akár el is fogadhatjuk, habár a különböző feladatrendszerekkel bíró, speciális szolgálatok kivételt képeznek, nem lehet e felsorolás minden elemét értelmezni esetükben. Az azonban egyértelmű, hogy azon szolgálatok közül, amelyek elhárító feladatokat látnak el, egyre nagyobb számban találunk olyanokat, amelyek a feladatellátásuk eredményessége érdekében awareness programokat folytatnak. Ennek célja a társadalom tagjai biztonságtudatosságának fokozása. Azon állampolgároké, akiket a nemzetbiztonsági kockázatok érinthetnek. A tevékenység fontosságának jelentősége megkérdőjelezhetetlen, olyannyira, hogy napjainkban erre akár – ahogyan a címben is utalunk rá – olyan önálló funkcióként tekinthetünk, amelyet érdemes és kell is vizsgálni, illetve a folyamatosan változó működési környezethez igazítani. Ezen írás célja, hogy egy áttekintő elméleti háttér felvázolását követően bepillantást engedjen néhány európai, illetve az Amerikai Egyesült Államok egyes hírszerző szervei által folytatott biztonságtudatossági programokba.

Kulcsszavak: *nemzetbiztonság, biztonságtudatosítás, elmélet, módszertan*

[1] Tanársegéd, NBI Rendészettudományi Kar Polgári Nemzetbiztonsági Tanszék, e-mail: drusza.tamas@uni-nke.hu
[2] Adjunktus, NBI Rendészettudományi Kar Polgári Nemzetbiztonsági Tanszék, e-mail: mezei.jozsef@uni-nke.hu
[3] Adjunktus, NBI Rendészettudományi Kar Polgári Nemzetbiztonsági Tanszék, e-mail: solti.istvan@uni-nke.hu
[4] Egyetemi docens, NBI Rendészettudományi Kar Polgári Nemzetbiztonsági Tanszék, e-mail: regenyi.kund@uni-nke.hu

According to some experts, the basic functions of intelligence services are: information gathering; information management, counter-intelligence and covert operations. This may be accepted, although specialised services with different systems of tasks are an exception, not all elements of this list can be interpreted in their case. However, it is clear that there are an increasing number of services that perform counter-intelligence tasks and that are running awareness programmes to ensure the effectiveness of their tasks. The aim is to raise the security awareness of members of society. Citizens who may be affected by national security risks. The importance of this activity is unquestionable, so much so that today it can even be seen, as the title suggests, as a function in its own right, which should and must be examined and adapted to the constantly changing operational environment. The purpose of this paper is to provide an overview of the theoretical background and to give an insight into the security awareness programmes of some European and US intelligence agencies.

Keywords: *national security, security awareness, theory, methodology*

Bevezetés

A titkosszolgálatok tevékenységének, azon belül is funkcióinak, feladatainak vizsgálata komoly tudományos probléma. A különböző kutatói álláspontok eltérő módon közelítik meg azt a kérdést, hogy ezen szervezeteknek milyen szerepük van a társadalmi működésben. Az alábbiakban a titkosszolgálati működés egy olyan aspektusát járjuk körbe, amelyet viszonylag ritkán sorolnak a titkosszolgálatok alapvető feladatai közé. Nevezetesen a biztonságos, biztonságtudatos viselkedés fejlesztését.

Ez azért fontos, mert a nemzetbiztonsági fenyegetések egy jelentős része személyekre hat, tőlük igyekszik érzékeny információt beszerezni, az ő viselkedésüket igyekszik befolyásolni. Ezek lehetnek egyszerű állampolgárok vagy egy fontos állami szervezet magas beosztású munkatársai. Ebben az esetben sok múlik azon, hogy az adott személy hogyan viselkedik. Motivált és képes-e aktívan tenni a fenyegetések felismerése és elhárítása érdekében, jelentős mértékben elősegítve ezzel a titkosszolgálatok vagy a rendészeti szervek védelmi tevékenységét és ezzel az ország és a társadalom biztonságát és megfelelő működését.

A titkosszolgálatok szerepe azért fontos, mert az említett fenyegetések egy jelentős része titkos módon tevékenykedő szervezetektől származik, például más országok hírszerző szerveitől, terrorista csoportoktól vagy szervezett bűnözői köröktől. A titkosszolgálatok olyan szervezetek, amelyek a legjobban ismerik ezen tevékenységek jellemzőit, amiből az is következik, hogy az ezekkel szembeni felkészítést ők tudják a leginkább kompetens módon végrehajtani. Az alábbi tanulmány a nemzetközi gyakorlatot áttekintve vizsgálja meg a kérdés hátterét.

A tanulmány három részre oszlik. Egyrészt a titkosszolgátok által végzett biztonságtudatosításról szóló elméleti háttérre. E rész célja, hogy segítse e biztonságtudatosítási tevékenység elméleti rendszerének megfogalmazását, lehetővé téve a külföldi példák hatékonyabb elemzését, értelmezését. Másrészt áll azokból az adatokból, amelyeket a külföldi szolgálatok *awareness* tevékenységéről nyílt forrásokból összegyűjtöttünk. A harmadik részben pedig elvégezzük az első két fejezetben rögzített adatok, ismeretek elemzését és

értelmezését, és megfogalmazunk néhány elméleti következtetést, illetve ezekből fakadó gyakorlati következtetést.

A biztonságtudatosítás rövid elméleti háttere

Mivel a személyes biztonság egy, a maslow-i hierarchiában alacsonyan található, azaz fontos emberi szükséglet,[5] azt gondolhatnánk, hogy ennek tudatosítása nem lényeges: az emberek a biztonságukra maguktól figyelnek. A biztonság azonban összetett fogalom, számos aspektusa van, amelyekhez egyes egyének nem azonos módon viszonyulnak. Egyik csoportosítási lehetőség a fizikai és az absztrakt biztonság.

Fizikai vs. absztrakt biztonság

A *fizikai biztonság* a biztonság olyan formája, amelynek tárgya az adott személy élete és testi épsége, illetve a birtokában lévő „kézzelfogható", azaz érzékszervekkel érzékelhető tárgyak. Ezek védelmére az ember ösztönösen figyel, biológiai determináltsága, valamint érzékszervei révén. A fizikai biztonságot veszélyeztető fenyegetéseket nevezhetjük *fizikai fenyegetéseknek*.

Az *absztrakt biztonság* a biztonság olyan formája, amelynek tárgya nem az adott személy testi épsége vagy a birtokában lévő tárgy, hanem valamilyen ezektől elvonatkoztatható dolog. Ennek fenyegetése – az úgynevezett *absztrakt fenyegetés* – ebben az esetben valamilyen elvont, nehezen, vagy nem érzékelhető tárgyra irányul. E tárgyak legtöbbször olyan adatok, amelyek révén az adott egyénnek vagy – tovább növelve az absztrakció mértékét – valaki másnak kárt lehet okozni. Ezek fenyegetése azért nem váltja ki a biztonságérzet automatikus csökkenését, mert védelmük kívül esik az érzékszervi észlelésen, és mivel csak az utóbbi néhány évezred társadalmi termékei, biológiai ösztönök által sem meghatározottak. Ezen túlmenően a fenyegetés tárgyai sokszor nem az adott személy biztonságát fenyegetik, hanem egy szervezet vagy egy annál is nagyobb csoport ismeretlen tagjait, így a fenyegetés csak áttételes. Ezen absztrakció nem ösztönzi az egyéneket arra, hogy változtassanak viselkedésükön ahhoz képest, amikor még nem voltak kitéve az absztrakt fenyegetéseknek.

Ezen absztrakt fenyegetések célpontjai igen tágan értelmezhetők. Jelenthetik például a bankkártyaadatok, PIN-kódok, jelszavak, gépjárműnyitó vagy -indító kódok, illetve személyes, bizalmas adatok megszerzését. Emellett jelentheti például az ember tevékenységének titokban történő megfigyelését. Az absztrakt fenyegetések egy külön csoportja a kiberfenyegetések, amelyek a kibertéren mint absztrakt téren keresztül fenyegetik az egyént. Külön csoportját képezik ezen körnek a fontos és bizalmas adatok, mivel azok sérülése az adott személyre nagy eséllyel csak áttételes hatással nem bír, ugyanakkor egy ország biztonságára komoly negatív hatást gyakorol.

[5] Maslow 1943: 370–396.

A biztonságtudatosítás szakirodalmi háttere

Erős szakirodalmi álláspont, hogy a biztonság megfelelő kialakításának leggyengébb láncszeme az ember.[6] Ennek következtében a biztonság fokozása leginkább az emberi tényező fejlesztésén keresztül valósítható meg. Ebből adódóan kiterjedt kutatások folynak arról, hogy milyen módon lehet a biztonságtudatos viselkedést eredményesen és hatékonyan javítani.

A biztonságtudatosítás kérdésköréről adandó tudományos összefoglaló során nem kerülhető meg az a kérdés, hogy mit értünk e fogalom alatt. E kérdésben a szakirodalom sem nevezhető egységesnek. Egy 2022-es áttekintő jellegű cikk alapján az alábbiak szerint összegezhető az ezzel kapcsolatos tudományos helyzet.[7]

Fontos kiindulópont, hogy mit értünk a biztonságtudatosítás fogalmán. Valójában ez esetben azt keressük, hogy mit értünk a biztonságos viselkedés fejlesztésén. A szakirodalom alapján a témakörrel kapcsolatosan három összefüggő, egymásra épülő fogalmat lehet elkülöníteni:[8]

1. *Biztonságtudatosítás (security awareness):* Olyan programok, amelyek célja a munkavállalók biztonsági tanulásának elősegítése, az információbiztonság fontosságának tudatosítása, valamint folyamatos erőfeszítések a biztonsági magatartás megváltoztatására. *Ezen általánosnak mondható szinten általában olyan tevékenységeket értenek, amelyek keretében rövid idő alatt, egyszerű eszközökkel igyekeznek felhívni az alanyok figyelmét a biztonságos viselkedés fontosságára.*
2. *Biztonsági tréning (security training):* Oktatási eszközök és kommunikációs alagutak, amelyek aktiválják az alkalmazottak gondolkodási folyamatait, ráveszik őket a megfelelő cselekvésre, és lehetővé teszik számukra a biztonsági politikák és eljárások jobb megértését. *Ezen a szinten a cél a biztonságos gondolkodás fejlesztése és a biztonságos viselkedés elsajátítása.*
3. *Biztonsági oktatás (security education):* Erőfeszítések, amelyek célja, hogy javítsák az alkalmazottak tudatát a biztonsági politikákkal, irányelvekkel és a biztonsági környezettel kapcsolatban, hogy javítsák az alkalmazottak biztonsággal kapcsolatos viselkedését. *Ezen a szinten a cél a komplex biztonsági környezet megértése és a tudatosság magas fokának elérése.*

E három fogalmat a SETA betűösszetétellel szokták jelölni, amely a *security, education, training, awareness* szavakat/tevékenységeket takarja. Megfigyelhető, hogy a három meghatározás között nem könnyű különbséget tenni, a szakirodalmi alkalmazásuk sem egységes. Az ilyen fajta lehatárolásnak mégis van egy olyan előnye, hogy lehetővé teszi a differenciálást egy folyamat különböző szintjei, fokozatai között. Ezen elkülönítésre a következők miatt is szükség van:

- A biztonságos viselkedés tanult magatartásforma, amelynek elsajátítási folyamata – összetettségtől függően – kifejezetten hosszadalmas is lehet. Így e folyamat sikerét különböző módokon, eszközökkel lehet elősegíteni.

[6] Hu–Hsu–Zhou 2022: 752–754.
[7] Hu–Hsu–Zhou 2022.
[8] Merritt 2024; Hu–Hsu–Zhou 2022.

- Különböző szervezeteknek különböző mértékben van szükségük a dolgozóik biztonságtudatos viselkedésére. Az is előfordul, hogy egy szervezeten belül a különböző részterületeken dolgozóknak eltérő szintű tudásra van szükségük e téren.

A fentiek vizsgálatára a szakirodalomban két nagy kutatási megközelítés létezik.[9] Az elsőben a SETA-programok hatását vizsgálják a munkavállalók viselkedésére, azaz azt, hogy mi változik a viselkedésben ezen programok hatására, van-e eredménye ezen programoknak, és ha igen, milyen. Általánosságban elmondható, hogy ezen vizsgálatok túlnyomó többsége szerint a SETA-programok javítják a szabályok betartását, a biztonsági teljesítményt és az általános biztonságos viselkedést, ezért az alkalmazásuknak van létjogosultsága.

A tanulmányok másik csoportjában – különböző elméleti alapokon állva – a SETA-programok hatásmechanizmusát vizsgálják, azaz azt, hogy miként hatnak ezek a programok a munkavállalói viselkedésre. E kutatások alapvetően számos további csoportra oszthatók:

1. A védelmi motiváció elméletén alapuló megközelítések.[10] Ezen elgondolás alapja az, hogy a fenyegetéssel való megküzdés három tényezőn múlik elsősorban:
   - A veszély észlelt mértéke: annak mértéke, hogy valaki mennyire érez fenyegetőnek egy adott jelenséget.
   - Válaszhatékonyság: abban való bizalom mértéke, hogy a veszélyre adott cselekvéses válasz megfelelő, az tényleg képes elhárítani a veszély negatív hatásait.
   - Énhatékonyság (önbizalom): abban való bizalom, hogy a cselekvést végre tudja hajtani az illető.

2. A tervezett viselkedés elméletén alapuló megközelítés.[11] Ezen elmélet szerint a viselkedést az alábbi tényezők befolyásolják. Minden tényező egy hiedelemrendszeren alapul, amelynek pozitív irányú megváltoztatása pozitív hatással van az elvárt viselkedésre is.
   - A viselkedési attitűd, amely azt mutatja meg, hogy az egyén pozitívan vagy negatívan értékeli az adott cselekvésben való részvételét, azaz hogyan viszonyul hozzá. Az attitűd definiálható az egyén hitein, hiedelmein keresztül (például úgy véli, hogy a biztonság nem fontos, ennek megváltoztatása javítja a biztonságos viselkedés esélyét).
   - A szubjektív norma azt jelenti, amelyet a társadalom helyez az adott személyre, hogy az adott cselekvést végezze el (például annak elmagyarázása, hogy a vezetés számára miért fontos a biztonság, fokozhatja a beosztottak biztonságos viselkedésének valószínűségét).
   - Az észlelt viselkedési kontroll mutatja meg, hogy az adott személynek mekkora befolyása van azon külső és belső tényezőkre, amelyek akadályozzák őt a viselkedés végrehajtásában (például hogyan lehetséges bonyolult jelszavak megjegyzése, ezáltal javítva az erős jelszavak alkalmazásának valószínűségét).

[9] Hu–Hsu–Zhou 2022: 756.
[10] Burns et al. 2018; Hina–Selvam–Lowry 2019; Posey–Roberts–Lowry 2015; Hovav–Putri 2016.
[11] Jenkins–Durcikova 2013.

3. Az elrettentés elméletén alapuló cselekvés,[12] amely arra a feltételezésre épül, hogy az alkalmazottak megfelelő viselkedését a büntetéstől, szankciótól való félelem fenntartásával lehet kiváltani. Minél kisebb ez a félelem, annál nagyobb az úgynevezett morális leválasztás esélye, azaz hogy az egyén igazolni tudja maga számára a felelőtlen viselkedést, vagy át tudja hárítani a felelősséget, esetleg torzítani tudja a következményeket. Az elrettentés két tényezőn nyugszik:

- a büntetés mértékén: érdekes módon az egyik empirikus kutatás arra jutott, hogy a büntetés mértéke nagyobb elrettentő erővel bír, mint a valószínűsége;
- a büntetés valószínűségén.

4. Méltányossági elméletek szerint[13] az alkalmazottak cégbe vetett bizalma jelentősen növeli a biztonságot. A biztonsági korlátozásokat az alapján ítélik meg, hogy

- a korlátozások számukra milyen hatással bírnak;
- a korlátozásokat mennyire indokolja külső kényszer;
- az etikai normákkal mennyire van összhangban.

Ezen kutatások eredményei alapján nem a büntetés, hanem a tiszteletteljes kommunikáció, a biztonsági oktatási programok, valamint az alkalmazottak jogainak maximalizálása révén a bizalom előmozdítása hatékonyabb eszköz a biztonság növelésére, mint a büntetés, különösen szigorított IT-biztonságú szervezetekben.

5. Az elszámoltathatósági elmélet alapján[14] végzett kutatások arra a következtetésre jutottak, hogy a biztonság növelhető, ha az elszámoltathatóság megvalósul a szervezeti folyamatok tekintetében. Ez azt jelenti, hogy az egyénnek a cselekvéseiről be kell számolnia egy másik személynek, aki pozitív vagy negatív következményeket rendel azokhoz. Például a jelszavak megváltoztatásának gyakorisága vagy a jelszavak erősségének fokozása lehet ilyen cselekedet, amelyre visszajelzést kap a másik személytől.

6. A kapcsolatok elmélete alapján folytatott kutatások[15] szerint a munkaadók és munkavállalók közötti kapcsolatok társadalmi cserekapcsolatokként definiálhatók, amelyek képesek javítani a szervezeti kultúrát és növelni az alkalmazottak elkötelezettségét. Az alkalmazotti kapcsolatok erősítése elősegítheti a bizalmat és a nyitott kommunikációt a szervezetben, ami növeli az alkalmazottak hajlandóságát a biztonsági szabályok betartására és az információbiztonság iránti felelősségvállalásra.

A bemutatottakon kívül még több kevésbé releváns megközelítés is létezik. Az elméletek sokfélesége arra mutat rá, hogy számos tényező befolyásolhatja a biztonságos viselkedést.[16] Mi magunk úgy látjuk, hogy a titkosszolgálatok szerepét, lehetőségeit az első két elmélet alapján lehet a legjobban megragadni. Meglátásunk szerint a biztonsághoz, ezen belül is az absztrakt fenyegetésekhez való viszonyulás döntő faktor abban, hogy az adott személy milyen mértékben viselkedik biztonságosan. Ebből fakadóan az attitűd fogalmát látjuk

12 D'Arcy–Hovav–Galletta 2009; Herath et al. 2018.
13 Lowry et al. 2015.
14 Yaokumah–Walker–Kumah 2019.
15 Yaokumah–Walker–Kumah 2019.
16 A témában lásd még például: Dobák–Babos 2021.

célszerűnek kiemelni, mivel a viszonyulást a szociálpszichológiában e fogalom[17] fejezi ki a legjobban, ahogy erre a tervezett viselkedés elmélete is utal. Az attitűdöt leggyakrabban három fő komponens mentén figyelhetjük meg:

- Érzelmi komponens, avagy egy adott személynek milyen érzései vannak az absztrakt veszélyek kapcsán. Kialakul-e benne a félelemérzet ezzel kapcsolatosan, mennyire érzi fenyegetőnek, illetve hogyan viszonyul az esetleges károkozáshoz. Hasznosnak érzi-e a biztonság fokozására tett lépéseket.
- Kognitív komponens, ami az alany tudatosan meglevő ismereteit jelenti az absztrakt veszélyekkel kapcsolatosan. Mennyire van tisztában az ilyen tényezők létezésével, működésével. Ezek alapján mennyire van tudatában annak, hogy e veszélyek kit és hogyan veszélyeztetnek, milyen károkat okozhatnak a társadalomnak, és így miért racionális, hogy tenni kell ezek kivédése érdekében.
- Cselekvéses komponens, ami ez esetben az absztrakt fenyegetések megismerésével, felismerésével, kivédésével kapcsolatos múltbéli és tervezett cselekvéseket jelenti. Tett-e már lépéseket korábban, és hajlandó lenne-e a jövőben tenni, illetve fokozni az ilyen jellegű tevékenységét. A cselekvés magában foglalja az erre vonatkozó motivációt és képességet is.

Az attitűd e három komponense olyan módon függ össze egymással, hogy az érzelmi és kognitív komponens meghatározó a cselekvéses komponens tekintetében, mivel az emberek a kognitív disszonancia elkerülése érdekében hosszú távon igyekeznek cselekedeteiket érzelmeikkel és tudásukkal összhangba hozni, elkerülve az összhang hiányából fakadó belső feszültségérzetet, szorongást (kognitív disszonancia). Így ha az érzelmi és a kognitív komponens nem pozitív a tudatos biztonságos cselekvés irányába, akkor ilyet nem várhatunk az egyéntől.

Fontos továbbá, hogy akitől elvárják a biztonságos viselkedést, annak lehetőséget kell adni arra, hogy megtanulja, begyakorolja és alkalmazza e magatartási formákat. Ez utóbbiba bele kell érteni a megfelelő eszközökkel végrehajtott tréningezést is.

A fentiekből az következik, hogy a biztonság tudatosítása során nem kizárólag a tudás átadására kell fókuszálni. A biztonságtudatosítás során fontos mindhárom komponensre hangsúlyt fektetni. Ennek során az alanyokban ki kell alakítani a veszélyeztetettség vagy a biztonság hasznossága, illetve fontossága érzésének olyan mértékét, amely motiválttá teszi őket a biztonságos viselkedés elsajátítására és alkalmazására. Erre megfelelő eszköz például a kiszolgáltatottság, a lehetséges erkölcsi és anyagi kár mértékének bemutatása, illetve annak hangsúlyozása, hogy – különösen a titkosszolgálatok tevékenysége szempontjából – senki sincs biztonságban.

Összefoglalásképpen a biztonságtudatosítás rendeltetését az alábbiak szerint fogalmazhatjuk meg: olyan fejlesztő tevékenység, amelynek célja az absztrakt veszélyekkel szembeni tudatos cselekvésre való képesség és motiváció növelése. Így a biztonságtudatosítás

[17] Rosenberg–Hovland 1960. Az attitűd háromtényezős modelljét 1960-ban alkották meg, azóta számos fejlesztésen és pontosításon esett át, de az eredeti gondolatmenet a mai napig relevánsnak mondható.

rendeltetése a biztonságos viselkedés kialakítása és ösztönzése, amelynek érdekében az alábbiakra szükséges hatni:

1. Az absztrakt fenyegetésekkel kapcsolatos attitűd érzelmi, kognitív és cselekvéses komponense.
2. Motiváció a viselkedés megtanulására és alkalmazására.
3. Lehetőség a helyes magatartás elsajátítására és alkalmazására.

A titkosszolgálatok szerepe a biztonságtudatosításban

A fenti kutatások közös pontja, hogy leginkább a szervezeti működésre fókuszálnak, ahol a résztvevők a munkaadó és a munkavállaló. Emellett a kutatások jelentős része az IT-biztonságra koncentrál, kevésbé helyezve fókuszt például a *social engineering* kérdésére. A titkosszolgálatok ebből a szempontból egy harmadik szereplőnek tekinthetők, akik elsősorban nem saját alkalmazottjaikat kívánják felkészíteni, hanem más szervezetekét, illetve az állampolgárok bizonyos csoportjait. Emellett a biztonság jellege is túlmutat egy adott szervezet működési keretein. Így a titkosszolgálatok biztonságtudatosításban játszott szerepének, lehetőségeinek, feladatainak megítéléséhez további szempontok elemzésére van szükség.[18]

A titkosszolgálati biztonságtudatosítás célközönségének közös pontja nem egy szervezethez való tartozás, hanem a nemzetbiztonsági relevancia. Ilyen módon e személyi kör meglehetősen heterogén mind fenyegetettség, mind előzetes felkészültség, mind a szükséges tudás tekintetében.

Tágan értelmezve a körbe beletartozik minden olyan állampolgár, aki külföldi ellenérdekelt akció célpontja lehet, illetve aki segíthet e tevékenységek (például szabotázs) elhárításában. Szűkebben értelmezve: e személyi kör jelentős részét a nemzetbiztonsági ellenőrzéshez kötött beosztást betöltők vagy minősített, szenzitív adatokhoz hozzáféréssel rendelkezők alkotják. Ők többnyire állami szolgálatban állnak, de a magánszféra szervezeteiben is dolgoznak ilyen személyek. E személyi kör a birtokukban lévő adatok értékéből, illetve hatáskörükből adódó döntési lehetőségeikből fakadóan nagyobb eséllyel kitettek a nemzetbiztonságot veszélyeztető absztrakt fenyegetéseknek. Esetükben a fenyegetések köre is szélesebb, intenzitásuk mélyebb, mert az ellenérdekelt feleknek megéri több erőforrást áldozni összetettebb támadásokra.

Ennek leggyakoribb módja az ilyen adatokat hordozó személyek titkos vagy leplezett megfigyelése, csapdába csalása, illetve esetlegesen kompromittálása. E tevékenységek legtöbbször rejtettek, vagy azért nem érzékelhetők, mert hétköznapi tevékenységnek vannak álcázva, így nem tűnnek kockázatot hordozónak. Másrészt ha az alanyok észlelnek is valami szokatlant, akkor sem tudják, mi és miért történik, és hogy erre mit kellene reagálniuk. Ennek leginkább az az oka, hogy a hétköznapi élet nem készít fel speciális tevékenységekkel szembeni válaszokra. Ráadásul az adatok megszerzése a személynek közvetlenül nem feltétlenül okoz kárt, így kevésbé érezheti magát motiváltnak a megvédésükkel kapcsolatosan.

[18] Regényi–Jasenszky–Lippai 2022.

A nemzetbiztonsági fenyegetésekből fakadóan a titkosszolgálati *awareness* célja nemcsak a biztonságos viselkedés általános szintjének (lásd például információbiztonság) javítása, hanem a speciális fenyegetésekkel szembeni különleges attitűd és ismeretek kialakítása kell hogy legyen. Példának okáért az IT-biztonsági szabályok betartása önmagában nem garantálja a *social engineering* technikákkal vagy a kompromittálással szembeni védelmet. Ezért szükséges a biztonsági környezet komplex megközelítése és speciális tudásanyag (például ellenérdekelt szolgálatok céljai és beszervezési módszerei) átadása.

E személyi kör fölött a nemzetbiztonsági szolgálatok nem rendelkeznek olyan direkt kontrollal, mint amivel egy munkaadó rendelkezik a munkatársai felett, így nehezebben tudja kényszeríteni a biztonságos viselkedésre ezen egyéneket, illetve kisebb eséllyel tudja kiszűrni közülük azokat, akik nem így tesznek. Ezért fontos, hogy a személyek önként akarják és önállóan tudják alkalmazni a biztonságos viselkedés szabályait, módszereit, ehhez megfelelő motivációval és tudással rendelkezzenek.

Összefoglalásként elmondható, hogy e személyi kör biztonságos viselkedése nemcsak közvetlenül a munkaadó számára fontos, hanem más közérdek, példának okáért a nemzetbiztonság szempontjából is. Így a biztonságos viselkedés ösztönzésének, az erre való felkészítésnek a miként je is túl kell hogy mutasson az általános munkavégzéshez szükséges mértéken és módszeren.

Külföldi titkosszolgálatok biztonságtudatosítási *(awareness)* tevékenysége

Ebben a fejezetben megvizsgáljuk a külföldi titkosszolgálatok biztonságtudatosítással kapcsolatos tevékenységéről az interneten fellelhető adatokat. Számba vettük az interneten általunk talált ezzel kapcsolatos adatokat, amelyeket a mellékletben szedtünk össze, kiegészítve további adalékokkal. A vizsgálatunk az Európai Unió 26 országára, valamint az USA-ra, az Egyesült Királyságra, Norvégiára, Svájcra és Ukrajnára terjedt ki. A vizsgált 31 országból 12-ben találtunk nyílt forrásokban releváns, megjelenítésre érdemes információt, ezekből készítettük az alábbi összefoglalót.

Fontos megjegyezni, hogy az alábbiakban kifejezetten a titkosszolgálatok által végzett vagy kifejezetten titkosszolgálati fenyegetések elhárításával kapcsolatos *awareness* tevékenységre fókuszáltunk. Ennek megfelelően az általános, gyakran más szervezetek által is végzett terror- és kiberbiztonsági tudatosító tevékenységeket nem vizsgáltuk.

A téma kutatása eleve nem könnyű a titkosszolgálatokat körülvevő konspiráció miatt. Valószínűsíthető, hogy lényegesen több szolgálat végez ilyen tevékenységet, mint amennyi ezt publikusan felvállalja, illetve az is, hogy a tevékenység kiterjedtebb, mint amit nyílt forrásból meg lehet ismerni. Ezen túlmenően fontos megjegyezni, hogy biztonságtudatosítási tevékenységet nem csak titkosszolgálatok folytatnak. Ezek alapján az alábbiakban leírtak az elérhető nyílt adatokon alapulnak, és értelemszerűen nem veszik figyelembe a nem nyilvános adatokat. Ebből fakadóan a vázolt helyzetkép feltehetően nem teljes, ugyanakkor alkalmas a téma áttekintésére.

A különböző országok szolgálatai különböző módokon közelítik meg a biztonságtudatosítás kérdéskörét. Anyagunk mellékletében részletesen közöljük az alábbi adatok

forrásaiként szolgáló webhelyeket. A továbbiakban országonként vesszük számba az általunk fellelt adatokat.

Ausztria esetében a DSN (Direktion Staatsschutz und Nachrichtendienst, polgári elhárító és hírszerző szolgálat) kapcsán találtunk biztonságtudatosítással kapcsolatos információkat. Ezek azonban nem önmagukban, hanem a kiberbiztonsággal összefüggésben vannak bemutatva, jóllehet számos olyan információt tartalmaznak, amelyek túlmutatnak a kiberbiztonságon, és inkább az általános biztonságtudatos viselkedéshez tartoznak. A jelzett honlapon a Kiberkalauz menüpontban ezzel kapcsolatos letölthető brosúrák találhatók, amelyek viselkedési alapelvek, tanácsok formájában nyújtanak ismereteket, szöveges módon. Jól látható, hogy e tájékoztató anyagok elsősorban az attitűd kognitív részét célozzák meg, nem alkalmasak az érzelmi komponens befolyásolására.

Bulgária esetében a DANS (Állami Nemzetbiztonsági Ügynökség, polgári elhárító szolgálat) tevékenységi körében találhatók információk az *awareness* tevékenységről. E szervezet a kémelhárítással és a radikalizációval kapcsolatosan tett közzé az állampolgárokat célzó ismereteket. Mindkét csoportban letölthető brosúrák állnak az érdeklődők rendelkezésére, amelyek részletesen beszámolnak a fenyegetések mibenlétéről és a velük szembeni védekezés teendőiről. E brosúrák inkább a tudásátadásra fókuszálnak, az attitűd kognitív komponensére hatnak.

Csehországgal kapcsolatosan nem találtunk konkrét adatokat a titkosszolgálatok biztonságtudatosítási tevékenységéről. Egyetlen cikk lelhető fel, amely szerint a BIA (Biztonsági Információs Szolgálat, polgári elhárító szolgálat) olyan programot készít elő, amely széles körű képzési programot nyújt privát és állami szervezeteknek a kémkedés elleni fellépés erősítése érdekében. E programról további információ nem áll rendelkezésre, de figyelemre méltó az, hogy a BIA-nál egy civilek számára is elérhető képzési programban gondolkoznak, amely magában foglalhatja az attitűd komplex formálását is.

Dániában az adatok alapján kifejezetten nagy hangsúlyt helyeznek az *awareness* tevékenységre. Ezt jól mutatja, hogy a dán titkosszolgálat (PET, Dán Rendőrségi Hírszerző Szolgálat, polgári elhárító szolgálat) honlapján a nyitólapon szerepel a biztonsági tanácsadás menüpont. E menüpontban az érdeklődők tájékozódhatnak a biztonságtudatos viselkedésről, a kémkedés, a szabotázs és a hibrid fenyegetés elhárításával, valamint a biztonságos tudományos kutatómunkával kapcsolatos tudnivalókról.

Ezen túlmenően elérhető egy kifejezetten tanácsadásra szakosodott rész is, ahol az ország szempontjából kritikus személyi körhöz tartozók (királyi család, politikusok, üzletemberek, követségek, diplomaták) képzéseket rendelhetnek meg. A tanácsadás lehet személyes vagy online, kiterjed konkrét fenyegetettségértékelésre is. Figyelmet érdemel az úgynevezett jó biztonsági kultúra megteremtését támogató kurzus. Az ismertető anyagból jól látszik, hogy komplex szemléletről van szó, amely segíti a biztonságtudatos szervezeti kultúra kialakítását. Itt nemcsak hagyományos frontális oktatásról van szó, hanem lehetőség van az attitűd komplex formálására is audiovizuális tartalmak és csoportos tréning révén. A többi területről is általánosan elmondható, hogy részletes leírásokkal és letölthető brosúrákkal támogatják a biztonságtudatosítást. Összességében a nyílt adatokból úgy tűnik, hogy az európai országok közül a dán szolgálatnál fektetik a legnagyobb hangsúlyt a biztonságtudatosításra.

Franciaországban a várakozásunkkal ellentétben nem találtunk külön a biztonságtudatosítási tevékenységre vonatkozó adatot. Az egyetlen ilyen témájú oldalt a DGSI (Belső

Biztonsági Főigazgatóság, polgári elhárító szolgálat) weblapján találtunk. Ez egy rövid összefoglaló szöveget tartalmaz az állampolgárok számára arról, hogy miért fontos a radikalizáció felismerése a társadalmi szereplők által, melyek ennek a vázlatos támpontjai, illetve hogy mit lehet tenni ennek gyanúja esetén.

Németországban elsősorban a Szövetségi Alkotmányvédelmi Hivatal (polgári elhárító szolgálat) foglalkozik a biztonságtudatosítás témakörével. A honlapjukon a Gazdaság és tudományos védelem menüpontban utalnak a civil szférával való együttműködésre, a biztonságtudatosság, a biztonságtudatos kultúra kialakításának fontosságára. A menüpontban letölthető néhány brosúra a kémkedés és a szabotázs, illetve a gazdasági és a tudományos élet kapcsolatáról, továbbá a szolgálat oldalán elérhető az általános biztonsági helyzettel kapcsolatos tájékoztatás, amelyek az attitűd kognitív komponensét célozzák. Konkrét biztonságtudatosítási programra vonatkozó adatot nem találtunk.

Norvégiában a titkosszolgálatok közül a PST (Rendőrségi Biztonsági Szolgálat, polgári elhárító szerv) foglalkozik biztonságtudatosítással. Ez alapvetően három szinten ragadható meg. Az első szinten található a nemzetbiztonsággal kapcsolatos ügyeket érintő általános tájékoztatás. Ez ugyan a legtöbb szolgálatnál megjelenik valamilyen formában, de a norvég szolgálat esetében kifejezetten részletes és alapos. Formája szerint megtalálható egy részletes szöveges dokumentum az ország biztonsági helyzetéről, valamint cikkek, fenyegetésértékelések, tanácsok a legfontosabb kihívásokkal összefüggésben, mindezek nyilvánosan elérhető online formában. A második szinten áll egy online nyilvánosan elérhető biztonsági kézikönyv. Ebben a tisztviselők és más releváns személyek számára alaposan bemutatják a biztonsággal, a kockázatokkal és a biztonságtudatos viselkedéssel kapcsolatos legfontosabb tudnivalókat, konkrét viselkedési példákkal illusztrálva. A könyv többek között kitér a személyes fizikai biztonságra, a lakóhely biztonságára, az online tér biztonságára, a vészhelyzeti biztonságra, a nyilvános szereplésekre, az utazással kapcsolatos biztonságra. A harmadik szint a személyes biztonsági tanácsadás, amely a tisztviselőkön kívül kiterjed a kulcsfontosságú gazdasági szereplőkre is, ennek pontos részletei azonban nem ismertek.

Értékelésünk szerint a norvég szolgálat biztonságtudatosító tevékenysége viszonylag kiterjedtnek mondható. A releváns személyeken túl a norvég társadalom egészét is megcélozzák, és a különböző eszközök alkalmazásával nemcsak a biztonságtudatos attitűd kognitív részét helyezik a középpontba, de igyekeznek hatást gyakorolni az érzelmi és a cselekvési komponensre is.

Olaszországban a Biztonsági Információs Minisztérium keretein belül, de a titkosszolgálatok tevékenységére építve működik a biztonságtudatosítás, elsősorban a kémelhárítás, illetve a gazdaság és a tudomány területén *(ECOFIN prevention)*. A fellelt ismeretek szerint fontosnak tartják a hírszerző szolgálatok és a gazdasági-tudományos szféra együttműködését, elsősorban a gazdasági versenyképesség fenntartása érdekében. A gazdasági szervezetek esetén hangsúlyozzák a fejlett biztonsági kultúra kialakításának fontosságát. Jóllehet a honlapon promotálják a kapcsolatfelvétel lehetőségét, e kapcsolat és a szolgálat által nyújtott támogatás mibenlétéről több információ nem érhető el. Az oldalon röviden bemutatják a lehetséges veszélyforrásokat, illetve megtalálható még két nagyon rövid, letölthető szöveges brosúra, amelyek megelőzési tippeket és az utazások során tanúsítandó viselkedéssel kapcsolatos információkat nyújtanak. Általánosságban megállapítható, hogy Olaszországban a titkosszolgálatok figyelmet fordítanak a biztonságtudatosításra, de ezzel kapcsolatos konkrét intézkedések nehezen azonosíthatók.

Portugáliában a Biztonsági Információs Szolgálat (polgári elhárító szerv) végez biztonságtudatosító tevékenységet. Ennek két pillére van: egyrészt az úgynevezett Tudásvédelmi Program (PPC), másrészt a Kritika Program. Előbbinek a célja a portugál polgárok és vállalkozások figyelmének felhívása a gazdasági kémkedés veszélyeire, a gazdasági érdekek védelme céljából. E programban 2023-ban 348 szervezet (kutatószervezetek, magánvállalkozások, közigazgatás) 1988 tagja vett részt. A leginkább képviselt területek az energia-, a technológiai, a védelmi és a közigazgatási szektorok voltak. A Kritikai Program célja a létfontosságú infrastruktúrák, érzékeny pontok és más releváns nemzeti infrastruktúrák védelmének javítása a fizikai biztonságukat fenyegető lehetséges fenyegetések, elsősorban a terrorizmus és a szabotázs ellen. A 2015-ös bevezetésétől 2023-ig összesen 648 tanácskozásra, illetve egyéb tevékenységre került sor a biztonságtudatosítás javítása érdekében. Úgy tűnik, hogy a portugál szolgálat nagy figyelmet fordít a biztonságtudatosságra, de ennek pontos módjára vonatkozóan nem közölnek adatokat.

Romániában az elhárításért felelős SRI (Román Információs Szolgálat, polgári elhárító szerv) folytat külső szereplők számára biztonságtudatossági tevékenységet. A honlapjukon kérdezz-felelek formában elérhető egy szöveges tájékoztató az online biztonsággal, a terrorizmussal, illetve az idegen hírszerző szolgálatok tevékenységének kivédésével kapcsolatosan. Ezen túlmenően az SRI egy online folyóiratot üzemeltet weblapján *Intelligence Magazin* címmel. A kiadványban mindenféle titkosszolgálati témában találhatók írások, erős fókusszal a biztonságtudatosság fejlesztésére. Az utóbbi időben úgy tűnik, hogy az online biztonság kapta a legnagyobb hangsúlyt. A témába vágó fontos – 2016. évi, így nem naprakész – sajtóhír, hogy az SRI kérésre kihelyezett képzéseket tart vállalatok számára kémelhárítás témakörében. A cikkben az SRI vezetői úgy nyilatkoztak, fontos részét képezi e tevékenységnek, hogy segítenek kialakítani egy megfelelő információbiztonsági rendszert, de az SRI csak tanácsadóként van jelen, minden döntést a szervezetek hoznak. Véleményük szerint akkoriban ez még a nyugati világban is egyedülállónak számító kezdeményezés volt. Úgy tűnik, hogy az SRI-nél igyekeznek az attitűd érzelmi és kognitív komponensére is hatni.

Ukrajnában az Ukrán Biztonsági Szolgálat (SZBU, polgári elhárító szerv) oldalán találhatók biztonságtudatosítással kapcsolatos információk *Hasznos információk* címmel. E cím alatt három további kategória található: A *Viselkedés vészhelyzetben* című rész a legtágabb, itt kiberbiztonsági, közösségi médiás támadással, gyanús tárgyakkal, túszhelyzetekkel, információszivárogtatással, illetve ellenérdekelt szolgálat beszervezési kísérletével kapcsolatos helyzetekben követendő teendők rövid leírása található. A másik két menüpont (*Orosz agresszióval szembeni fellépés,* illetve *Titokvédelem*) a címe ellenére nem tartalmaz releváns információt. Az említett teendők leírása viszonylag rövid és tömör, a lényeg bemutatására szorítkozik, ugyanakkor a témák sokszínűsége figyelemre méltó. A közölt információk körén és tartalmán megfigyelhető a háború hatása is, több helyen is említik mint a lehetséges fenyegetéseket kiváltó tényezőt.

Az *Egyesült Államokban* számos példa található a titkosszolgálatok vagy hasonló szervezetek biztonságtudatosító munkájára. Ennek legjobb példája a Védelmi Minisztérium (DoD) alá tartozó Defense Counterintelligence and Security Agency (DCSA) által végzett részletes biztonságtudatosítási programok és ehhez kapcsolódó internetes felületek. A DCSA ugyan nem titkosszolgálat, azonban olyan hivatalos szerv, amelynek tevékenységét más országokban jellemzően titkosszolgálatok végzik, és munkatársai között bevallottan jelentős

számban vannak titkosszolgálati szakemberek. Tevékenységi köre kiterjed a biztonsági (lásd nemzetbiztonsági ellenőrzés Magyarországon) és iparbiztonsági ellenőrzésekre, valamint titkosszolgálati és más biztonsági fenyegetések megelőzésére és kivédésére készíti fel az állampolgárok releváns csoportjait. Ebben kiemelt figyelmet szentelnek a belső fenyegetéseknek *(insider threat),* elsősorban a minisztérium szempontjából, de általánosságban is.

A biztonságtudatosság fejlesztése érdekében az ügynökség két internetes felületet működtet. A Center for Development of Security Excellence (CDSE) feladata képzések szervezése az 1. táblázatban foglaltak szerint.

1. táblázat: A Center for Development of Security Excellence feladatai

Képzési területek	Képzési eszközök	Képzések
Kémelhárítás	Esettanulmányok	Éves kötelező oktatás
Kibervédelem	Gyakorlati útmutatók	Nem minősített információs képzés
Iparbiztonság	Játékok	Minősített információs képzés
Információbiztonság	Útmutatók	Minősített információvédelmi képzés
Műveleti biztonság	Poszterek	Műveleti biztonsági képzés
Személyi biztonság	Rövid biztonsági oktatóvideók	Személyes adatok védelmével kapcsolatos képzés
Fizikai biztonság	Biztonsági oktatóvideók	SPED-tanúsítványt nyújtó képzés
Általános biztonság	Eszköztárak	
Minősítettinformáció-hozzáférési programok	Webinárok és konferenciák	

Forrás: a szerzők szerkesztése a kutatás során fellelt adatok alapján

A táblázatban foglalt lehetőségek mindegyikéhez elérhetők legalább rövid tananyagok vagy a téma összefoglalói, a legtöbb esetben az információk, ismeretek jelentős része bárki számára elérhető a táblázatban megadott formákban. Az offline kurzusokra a STEPP nevű *(Security, Training, Education and Professionalization Portal),* e célra létrehozott portálon keresztül lehet jelentkezni. Az éves kötelező képzés tananyaga a *security awareness hub* (biztonságtudatosító központ) felületen található, kémelhárítási, kiberbiztonsági, általános biztonsági, információbiztonsági, belső (szervezeti) biztonsági, műveleti biztonsági információk és online kurzusok érhetők el mindenki számára. Egy külön menüpontban (Kémelhárítás és belső fenyegetések) elérhetők brosúrák és jelentések. Előbbiek a felismerendő magatartásformákról és az ezzel kapcsolatos teendőkről szólnak részletes magyarázatokkal. A jelentések anonimizált és összegzett formában tartalmazzák egy adott pénzügyi év adatait a tekintetben, hogy milyen területeket, milyen módon, honnan ért támadás. Egyértelműen elmondható, hogy az USA *awareness* rendszere a leginkább komplex, és az attitűd mindhárom komponensére hatni kíván.

Következtetések, lehetőségek

Az alábbi következtetéseket fogalmaztuk meg:

1. A titkosszolgálatok által végzett biztonságtudatosító tevékenységre szükség van. Egyrészt mivel a biztonsági fenyegetések a társadalmi működés és így az állampolgárok egyre szélesebb körét érintik, másrészt mivel – különösen a virtuális tér gyors bővülésével és az MI megjelenésével – egyre változatosabb módon fenyegetnek. Továbbá az absztrakt fenyegetésekkel szembeni tudatos védekezés nem ösztönös, hanem tanult magatartásforma, így ennek befolyásolása is célirányos tevékenységet igényel. A titkosszolgálatok rendelkeznek azokkal a tapasztalatokkal, amelyek alapján ezt a leghatékonyabban tudják kivitelezni az összes állami szerv közül.
2. A biztonságtudatos viselkedés feltétele a biztonsággal, fenyegetésekkel szembeni megfelelő attitűd kialakítása. Ennek érdekében szükséges hatni az attitűd érzelmi, kognitív és cselekvési összetevőire is.
3. A biztonságtudatos viselkedés kialakítása többlépcsős, ismétléses folyamat. Mivel a szolgálatok ritkán találkoznak az adott személyekkel, nem csak a személyes ismeretátadásra kell fókuszálniuk. Segíteni kell a szervezeteket abban, hogy megfelelő biztonsági szabályrendszert és kultúrát alakítsanak ki. Célszerű továbbá online képzések alkalmazása is, hogy minél szélesebb kör számára minél gyakrabban legyen lehetőség tájékozódni.
4. A biztonságtudatos viselkedésnek több szintje van. Az állampolgárok teljes köre szóba jöhet a nemzetbiztonsági fenyegetés érintettjeként, jóllehet a különböző csoportok különböző mértékben. Alapesetben mindenki kitett például az ellenérdekelt manipulációs tevékenységnek, így egy alapszintű társadalmi felvilágosító, tudatosító tevékenység az egész társadalom ellenálló képeségét növelni tudja. Ezen túlmenően vannak azok a szervezetek, amelyek kiemelt helyet foglalnak el a társadalmi működés szempontjából (például érzékeny infrastruktúrát, adatokat kezelnek). E kör feltehetően tovább bontható például állami és nem állami szektorra, illetve rangsorolható fontosság szerint. Ezek alapján a különböző csoportokat különböző jellegű és módszerű képzésben célszerű részesíteni.
5. A külföldi elhárító szolgálatok bő egyharmad része bizonyosan folytat valamilyen biztonságtudatosítási tevékenységet. Ezek az általános tájékoztatástól, a személyes és online képzésen át, a szervezeti tanácsadásig számos formát öltenek. Az online elérhető adatok alapján világszinten az Egyesült Államok végezheti ezt a tevékenységet a legmagasabb szinten. Európában Dánia tűnik az élenjárónak, de általában elmondható, hogy a skandináv országok nagy hangsúlyt fektetnek erre a tevékenységre.
6. A leggyakrabban alkalmazott eszköz a nemzetbiztonsági helyzet és fenyegetések általános bemutatása, ez szinte minden vizsgált szolgálatnál megjelenik minden formában. Szintén gyakran használnak különböző brosúrákat, amelyek röviden bemutatják a fenyegetéseket és az esetleges teendőket. Komplexebb eszközök alkalmazására (videók, esettanulmányok, tréningezés, tanácsadás) kevesebb adatot találtunk.

Az *awareness* tevékenység fejlesztésének lehetséges lépései

A fentiek alapján egy teljes körű titkosszolgálati *awareness* rendszer kialakítása az alábbi lépések mentén látszik célszerűnek.

Tapasztalatok, módszerek megismerése: A külföldi partnerszolgálatokkal történő kapcsolatfelvétel tapasztalatok, módszertanok, képzési anyagok megismerése érdekében. A tanulmányunkban jeleztük, mely országokban látjuk kifejezetten fejlettnek az *awereness* tevékenységet.

Felmérés: A biztonságtudatos viselkedés kialakításának elősegítése érdekében célszerű lehet az absztrakt biztonsággal kapcsolatos ismeretek felmérése a releváns szervezeteknél, illetve személyeknél. Egy ilyen felmérés segítene megismerni az igényeket és a hiányosságokat, és lehetővé tenné a titkosszolgálati *awareness* tevékenység hatékonyságának fokozását.

Komplex módszertan kidolgozása: Fontos, hogy a biztonság tudatosítása olyan összetett folyamat, amelyet a leghatékonyabban akkor lehet végrehajtani, ha komplex módszertan áll rendelkezésre. Ennek során egyszerre célszerű hatni az attitűd mindhárom komponensére, javítani kell a motiváció szintjét, átadni és begyakoroltatni a szükséges ismereteket, valamint támogatni az ezt elősegítő biztonsági kultúra kialakítását és fenntartását. Ennek lehetséges elemei:

- Általános nemzetbiztonsági helyzettel kapcsolatos tájékoztató: A nemzetbiztonságot fenyegető tényezők a legtöbb ember számára absztrakt fenyegetések. Akkor várható tőlük a tudatos viselkedés, ha megismerik ezen absztrakt fenyegetések mibenlétét.
- Alapvető nemzetbiztonsági (titkosszolgálati) ismeretek: A releváns személyi kört, mint a támadások potenciális célpontjait, fontos lenne megismertetni az ellenérdekelt felek (például hírszerző szolgálatok) *modus operandijával,* különös tekintettel a beszervezési és *social engineering* technikákra.
- Biztonsági ismeretek: A biztonságos viselkedés kiváltásához értelemszerűen szükség van az ehhez nélkülözhetetlen ismeretek átadására.
- Esettanulmányok: Ezek révén lehetőség van közelebb hozni a személyekhez a biztonságos viselkedés előnyeit, elmaradásának hátrányait, valamint jó gyakorlatait. A valóságos példákra épülő esettanulmányok a leghatékonyabbak.
- Online tér alkalmazása: Az online eszközök alkalmazása több előnnyel is járna. Egyrészt lehetővé teszi a széles körű elérést, másrészt a képzés ismétlését, rendszeressé tételét, ami javíthatja annak eredményességét. Az online eszközök lehetnek videós anyagok, weblap, e-learning vagy akár online folyóirat.

Biztonsági kultúra fejlesztésének támogatása: A szervezetek biztonságorientált kultúrája nagymértékben elő tudja segíteni a hosszú távú biztonságtudatos viselkedést. Ehhez azonban szükséges a szervezetek támogatása a biztonságtudatos szervezeti kultúra kialakítása érdekében, különösen nemzetbiztonsági szempontból. Ez azonban a legtöbb szervezet számára nehézséget jelent, így számukra hasznos lehet a kultúra kialakításának és fenntartásának támogatása.

Tanácsadás: A biztonság tudatosítása összetett folyamat, amely során a szervezetek számos nehézséggel szembesülhetnek, különösen abban az esetben, ha kifejezetten kitettek biztonsági fenyegetéseknek. Ebben az esetben sokat segíthet a gyors és szervezetre, személyre szabott biztonsági tanácsadás. Mindez továbbfejleszthető, akár profitorientált

szervezetek számára történő – például az ipari kémkedés okozta károk csökkentésére irányuló –, akár anyagi ellentételezésért nyújtott nemzetbiztonsági jellegű tanácsadássá.

Felhasznált irodalom

Burns, A. J. et al. (2018): Intentions to Comply Versus Intentions to Protect: A VIE Theory Approach to Understanding the Influence of Insiders' Awareness of Organizational SETA Efforts. *Decision Sciences,* 49(6), 1187–1228. Online: https://doi.org/10.1111/deci.12304

D'Arcy, John – Hovav, Anat – Galletta, Dennis (2009): User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research,* 20(1), 79–98. Online: https://doi.org/10.1287/isre.1070.0160

Dobák Imre – Babos Sándor (2021): A biztonságtudatosítás lehetőségei a 21. századi platformok fényében. *Nemzetbiztonsági Szemle,* 9(4), 18–34. Online: https://doi.org/10.32561/nsz.2021.4.2

Herath, Tejaswini et al. (2018): Examining Employee Security Violations: Moral Disengagement and Its Environmental Influences. *Information Technology & People,* 31(6), 1135–1162. Online: https://doi.org/10.1108/ITP-10-2017-0322

Hina, Sadaf – Selvam, Dhanapal Durai Dominic Panneer – Lowry, Paul Benjamin (2019): Institutional Governance and Protection Motivation: Theoretical Insights Into Shaping Employees' Security Compliance Behavior in Higher Education Institutions in the Developing World. *Computers & Security,* 87, 101594. Online: https://doi.org/10.1016/j.cose.2019.101594

Hovav, Anat – Putri, Frida Ferdani (2016): This Is My Device! Why Should I Follow Your Rules? Employees' Compliance with BYOD Security Policy. *Pervasive and Mobile Computing,* 32, 35–49. Online: https://doi.org/10.1016/j.pmcj.2016.06.007

Hu, Siqi – Hsu, Carol – Zhou, Zhongyun (2022): Security Education, Training, and Awareness Programs: Literature Review. *Journal of Computer Information Systems,* 62(4), 752–764. Online: https://doi.org/10.1080/08874417.2021.1913671

Jenkins, Jeffrey – Durcikova, Alexandra (2013): What, I Shouldn't Have Done That? The Influence of Training and Just-In-Time Reminders on Secure Behavior. In *Proceedings of 34th International Conference on Information Systems*. Milánó.

Lowry, Paul Benjamin et al. (2015): Leveraging Fairness and Reactance Theories to Deter Reactive Computer Abuse Following Enhanced Organisational Information Security Policies: An Empirical Study of the Influence of Counterfactual Reasoning and Organisational Trust. *Information Systems Journal,* 25(3), 193–273. Online: https://doi.org/10.1111/isj.12063

Maslow, Abraham H. (1943): A Theory of Human Motivation. *Psychological Review,* 50(4), 370–396. Online: https://doi.org/10.1037/h0054346

Merritt, Marian et al. (2024): Building a Cybersecurity and Privacy Learning Program. Gaithersburg: National Institute of Standards and Technology. Online: https://doi.org/10.6028/NIST.SP.800-50r1

Posey, Clay – Roberts, Tom L. – Lowry, Paul Benjamin (2015): The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. *Journal of Management Information Systems,* 32(4), 179–214. Online: https://doi.org/10.1080/07421222.2015.1138374

Regényi, Kund – Jasenszky, Nándor – Lippai, Zsolt (2022): The Concept of Security Awareness, Its Development From the Point of View of National Security, Counter-Terrorism, and Private Security. *Belügyi Szemle,* 70(1. ksz.), 123–137. Online: https://doi.org/10.38146/BSZ.SPEC.2022.1.7

Rosenberg, Milton J. – Hovland, Carl I. (1960): Cognitive, Affective and Behavioral Components of Attitude. In Rosenberg, Milton J. – Hovland, Carl I. (szerk.): *Attitude Organization and Change: An Analysis of Consistency among Attitude Components.* New Haven: Yale University Press, 1–14.

Yaokumah, Winfred – Walker, Daniel Okyere – Kumah, Peace (2019): SETA and Security Behavior: Mediating Role of Employee Relations, Monitoring, and Accountability. *Journal of Global Information Management,* 27(2), 102–121. Online: https://doi.org/10.4018/JGIM.2019040106

Melléklet

Ország	Szolgálat	Van-e nyilvánosan elérhető *awareness* programja, anyaga?	Ha van, milyen területen (általános, kiber, terror, kémelhárítás, gazdaságbiz.)?	Milyen formában (online tájékoztató, papír brosúra, tanfolyam, reklámkampány stb.)?	Ki a célcsoport (állampolgárok, gazdasági szereplők, rendészeti szervek stb.)?	Online elérhetőség (link)	Egyéb megjegyzés, körülmény
Ausztria	Belügyminisztérium (Direktion Staatsschutz und Nachrichtendienst)	Van	Általános kiberbiztonság	Rövid tájékoztató, letölthető anyagok	Állampolgárok	https://www.dsn.gv.at/501/start.aspx#uebersicht https://www.dsn.gv.at/501/files/Cyber_Ratgeber/Schriftenreihe_Cybersicherheit_Cyber-Sicherheit_auf_Dienstreisen_Februar2022_BF_20220216.pdf	A biztonságtudatosítás a kiberbiztonság kérdéskörével együtt van kezelve
Bulgária	DANS	Van	Kémelhárítás, radikalizáció	Letölthető tájékoztató	Állampolgárok	https://www.dans.bg/en/awareness	
Cseh Köztársaság	BIA	Nincs	Kémelhárítás	Oktatás	Gazdasági, tudományos szféra	https://www.mpo.cz/en/guidepost/for-the-media/press-releases/security-information-service-and-mit-will-offer-training-to-companies-to-fight-spying--240321/	A cikk szerint a privát szféra számára is elérhető képzéseket vezet be a BIA

Dánia	PET	Igen	Általános	Online, oktatás, személyes tanácsadás	Állami alkalmazottak, gazdasági, ipari ágazatok munkatársai, illetve állampolgárok	https://pet.dk/raadgivning-om-sikkerhed https://pet.dk/-/media/mediefiler/pet/dokumenter/vejledninger/pet_kursusark_god_sikkerhedskultur_2022.pdf	Tájékoztatók, animációs kisfilmek, online/offline tanfolyamok és személyre szabott tanácsadás is elérhető, amelyet meg lehet rendelni
Franciaország	DGSI	Igen	Terrorelhárítás	Online tájékoztató	Állampolgárok	https://www.dgsi.interieur.gouv.fr/english/recognizing-the-signs-of-violent-radicalization	Radikalizálódás felismerése
Németország	Bundesnachrichtendienst (BND)	Igen	Kiber + hibrid	Rövid tájékoztató és letölthető anyagok	Állampolgárok	https://www.bnd.bund.de/DE/Die_Themen/Cybersicherheit/cybersicherheit_node.html	
Németország	Bundesamt für Verfassungsschutz	Igen	Gazdaságbiztonság	Rövid tájékoztató, letölthető anyagok	Állampolgárok, gazdasági élet szereplői	https://www.verfassungsschutz.de/EN/topics/economic-and-scientific-protection/economic-and-scientific-protection_node.html	A szolgálat honlapja szinte mindenütt utal az állampolgárok közreműködésére a biztonság terén
Norvégia	Politiets Sikkerhetstjeneste (PST)	Igen	Általános	Online tájékoztató	Állampolgárok	https://politietstryggingsteneste.no/globalassets/2024/ntv2024/nasjonal-trusselvurdering-2024_engelsk_web_.pdf https://pst.no/psts-podcast/ https://pst.no/alle-artikler/	Nemzeti kockázatok bemutatása az állampolgárok számára, írásos tanácsok
Norvégia	Politiets Sikkerhetstjeneste	Igen	Általános	Biztonsági tanácsadás, online kézikönyv	Kormányzati személyek, veszélyeztetett személyek	https://pst.no/alle-artikler/artikler/dette-gjor-vi/tryggleiksradgiving/ https://pst.no/alle-artikler/artikler/psts-sikkerhetshandbok-2024/	Biztonsági kézikönyv
Olaszország	Információbiztonsági Minisztérium, illetve Belső Biztonsági és Információs Ügynökség	Igen	Ipari kémkedés, gazdasági-pénzügyi biztonság	Letölthető brosúra, tanfolyam	Államigazgatási szereplők, gazdasági szereplők	https://www.sicurezzanazionale.gov.it/prevenzione-ecofin/tips-prevenzione	
Portugália	SIS	Igen	Gazdasági hírszerzés, létfontosságú infrastruktúrák védelme, terrorizmus	Nincs	Állami szervek, magánszervezetek, egyetemek, kutatóközpontok	https://www.sis.pt/pagina/117/programas-de-sensibilizacao	Meghirdetett programok vannak, amelyeknek a részletei közvetlenül a portugál szolgálatoktól ismerhetők meg
Románia	SRI	Igen	Kém- és terrorelhárítási és kiberbiztonsági	Online tájékoztató	Állampolgárok	https://www.sri.ro/security-advice	Az SRI oldalán van egy alapvető tájékoztató az állampolgárok számára
Románia	SRI	Igen	Általános	Online újság	Állampolgárok	https://intelligence.sri.ro/	Az oldalnak van egy kifejezett *awareness* rovata, ahol a biztonságtudatosságra helyezik a fő hangsúlyt

Románia	SRI	Igen	Kémelhárítás	Személyes oktatás	Gazdasági szereplők	https://www.profit.ro/stiri/exclusiv-sri-face-instructaje-contraspionaj-si-in-companiile-private-doar-la-cerere-si-gratuit-15041993	
Ukrajna	SZBU	Igen	Általános, kémelhárítási, kibervédelmi, egyéb	Online tájékoztató	Állampolgárok	https://ssu.gov.ua/en/yak-diiaty-v-ekstremalnykh-sytuatsiiakh	
USA	Defense Counterintelligence and Security Agency					https://securityawareness.usalearning.gov/	
USA	Defense Counterintelligence and Security Agency					https://www.dcsa.mil/Counterintelligence-Insider-Threat/	
USA						https://www.cdse.edu/	
USA						https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-videos	
USA	Belbiztonsági Minisztérium (DHS)	Igen	Terrorizmus	Többféle formában: papír, videó	Állampolgárok	https://www.dhs.gov/see-something-say-something	*If You See Something, Say Something* Rendelkezik egy prevenciós programokkal és partnerséggel foglalkozó központtal: https://www.dhs.gov/CP3
USA	Szövetségi Nyomozó Iroda (FBI) Közösségi Kapcsolatok Osztálya	Igen	Információbiztonság	Online	Állampolgárok	https://www.fbi.gov/how-we-can-help-you/outreach	