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