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

Héder Klára[1]

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

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

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

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

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

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

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

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

1. Bevezetés

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

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

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

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

2. Információbiztonság, kiberbiztonság és biztonságtudatosság: nehézségek és problémák

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

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

---

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

3 Kiss–Krasznay (2017): i. m. 56.

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

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

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

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

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

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

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

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

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

---

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

7 Kiss–Krasznay (2017): i. m.

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

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

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

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

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

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

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

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

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

---

11 Kiemelés: H.K.

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

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

14 Krasznay (2017): i. m.

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

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

2.2. A gyenge információbiztonság-tudatosság lehetséges okai

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

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

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

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

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

---

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

18 Kiss–Krasznay (2017): i. m.

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

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

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

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

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

3. A felhasználó mint ismeretlen faktor

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

3.1. Tulajdonságkutatás: célcsoportra szabott programok – jobb eredmények?

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

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

[22] Bányász–Bóta–Zágon (2019): i. m.

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

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

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

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

---

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

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

3.2. Problémás célcsoport: a felhasználók hibáztatása

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

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

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

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

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

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

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

---

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

26 Légárd (2021): i. m. 358.

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

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

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

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

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

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

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

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

4. A biztonságtudatosítás pszichés gátjai

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

4.3. Szubjektív veszélypercepció a digitális térben: a veszély alulbecslése

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

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

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

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

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

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

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

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

37 Csépe (2017): i. m. 278.

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

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

4.4. Szubjektív veszélypercepció a digitális térben: a veszély túlbecslése

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

5. Összefoglalás

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

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

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

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

Felhasznált irodalom

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Tartalom