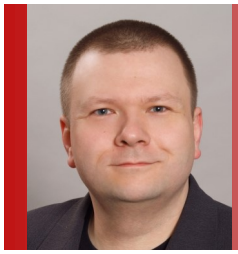
Dr. KOLLÁR Csaba



Az információbiztonság-tudatosság fejlesztése a (felső)vezetők körében

coaching és tanácsadás módszerével

Az információs társadalommal párhuzamosan futó, majd azt később leváltó digitális korban, vagy más névvel az adatok korában a korábbi korokkal ellentétben másfajta értékek kerülnek a fókuszba. A materiális világ megfogható tárgyi objektumai mellett a szimbolikus javak – értve ezalatt az adatokat, az információkat és az ezekből képzett tudást – felértékelődése figyelhető meg. A vállalatok és felsővezetőik egy része már nem csak az informatikai eszközökről, s ezek fizikai amortizációjáról, hanem az ezeken levő adatokról gyakran mint a vállalat legértékesebb erőforrásáról, az adatvagyonról is beszél. A releváns adatok és információk, illetve az ezek feldolgozása és elemzése során keletkezett vállalati tudás pénzben kifejezett értéke dinamikusan növekszik, ezzel párhuzamosan azonban a (felső)vezetők és az alkalmazottak információbiztonság-tudatossága elmarad, ami közvetve-közvetlenül hatással van a vállalatok nyereségére, folyamatos működésére, piaci helyzetére.Tanulmányomban az elméleti alapvetést követően egy, a magyarországi vezetők körében a közelmúltban végzett online nagymintás kutatás információbiztonsággal kapcsolatos saját kutatásunk megállapításait elemzem, majd az információbiztonság-tudatosságot erősítő coaching és tanácsadási módszereket, elsősorban az ISO 27000 szabványcsaládban megnevezett PDCA-modell átdolgozott, kibővített változatát mutatom be.

Elméleti alapvetés

A digitális kor legjellemzőbb tulajdonsága (Kollár, 2014), hogy a külvilágból érkező, s érzékszerveink által érzékelhető (látható, hallható, stb.), illetve nem érzékelhető jelenségek az információfeldolgozás minél előbbi fázisában digitalizálódnak. Az ilyen javak a hagyományos árukhoz képest sokkal gyorsabban és sokkal több emberrel oszthatóak meg (vírusszerű terjedés), s ha egy digitális adat/információ bekerül a hálózati környezetbe, akkor onnan gyakorlatilag kitörölhetetlen.

Az adatok, az információk, s az ezekből képzett tudások egy része szabadon hozzáférhető, felhasználásukról (elvileg) annak előállítója rendelkezik (Lessig, 2004). Egy másik része a vállalati, szervezeti, kormányzati/állami adatvagyont képezi, s többségüknél már belső

szabályzatok és/vagy szabványelőírások rendelkeznek többek között az adatok és információk előállításáról, tárolásáról, feldolgozásáról, elérhetőségéről, módosításáról, megoszthatóságáról, selejtezéséről (törléséről), valamint az adatok és az adattárolók fizikai és egyéb védelméről.

Muha (2004) szerint (3. rész, 3.2. fejezet, 2. o.) az „adatot, mint a támadások alapvető célját a következő rendszerelemek veszik körül:

- az informatikai rendszer fizikai környezete és infrastruktúrája,
- a hardverrendszer,
- a szoftverrendszer,
- a kommunikációs, hálózati rendszerek,
- az adathordozók,
- a dokumentumok és dokumentáció,
- a személyi környezet (külső és belső).”

A fentiek alapján látható, hogy az információbiztonság egy olyan komplex fogalom, ami a (1) személyi biztonság, a (2) fizikai biztonság, a (3) dokumentumbiztonság és az (4) elektronikus információbiztonság köré szerveződik. Tanulmányomban az emberi erőforrással, mint az információbiztonság kritikus tényezőjével foglalkozom, a többi területet és fogalmat csak említésszinten tárgyalom. Az emberi erőforrás a következőfontosabb tényezők miatt tekinthető kritikus területnek (Oroszi felsorolása alapján, 2008):

- Tudatlanság, szakképzetlenség
- Emberi hanyagság és figyelmetlenség
- Segítőkészség
- Hiszékenység, naivság
- Befolyásolhatóság
- Bosszúállás
- Kényelmesség

Az ember társas lény (Aronson, 2008), aki természetéből adódóan is törekszik arra, hogy társas kapcsolatokat alakítson ki és tartson fenn, akár a magánéletében, akár a munkahelyén. A munkavállalók, alkalmazottak, vezetők, tulajdonosok, beszállítók, vevők, stb. – tehát összefoglalóan a vállalat külső-belső érintettjei –személy- illetve csoportközi kommunikációja során (akár a hagyományos, akár a mediatizált kommunikációt is vizsgáljuk) a hivatalos témák mellett legalább érintőlegesen a magánélet eseményei is megjelennek. A „hogy vagy/van?” kérdésre az emberek, különösen a magyar emberek egy része rendszerint nem egy semmitmondó választ ad, hanem akár több percen keresztül is elkezd mesélni az életéről. A jó kérdező ilyen esetekben könnyen tudja úgy terelni a beszélgetés folyamát, hogy a személyes, illetve a vállalat életéből származó bizalmas információk is elhangozzanak.Nem ritka az az eset sem, amikor a munkavállaló, de akár a (felső)vezető is a közösségi oldalakon oszt meg szerinte semmitmondó tartalmakat, me-

lyeket a szakavatott, pszichológiai manipulációhoz (socialengineering) értő szakemberek kielemeznek, feldolgoznak annak érdekében, hogy a személyt, a vállalatot, illetve a vállalat bizalmas adatait tároló rendszereket érő támadásokat tudjanak megvalósítani.
Elvárható lenne a munkavállalók, de különösen a (felső)vezetők jelenleginél lényegesen tudatosabb magatartása a(z információ)biztonság területén. Azoknak a vállalati vezetőknek, akiknél az MSZ ISO 27001 bevezetésre került, elméletileg biztonságtudatosabbaknak kellene lennie.
Az említett szabvány 5.1. alfejezetében (28. o.) a vezető elkötelezettségével kapcsolatban így fogalmaz: „A vezetőségnek bizonyítania kell elkötelezettségét az ISMS (InformationSecurity Management System – információbiztonsági irányítási rendszer) kialakítása, bevezetése, működtetése, figyelemmel kisérése, átvizsgálása, fenntartása és fejlesztése iránt:

a) ISMS-szabályzat kialakításával;
b) ISMS-célok és -tervek kialakításának biztosításával;
c) az információvédelemért viselt feladat- és felelősségi körök kialakításával;
d) az információvédelmi célok teljesítése és az információvédelmi szabályzatnak való megfelelés fontosságának, a jogszabályok szerinti felelősségeknek, valamint a folyamatos fejlesztés szükségességének kinyilvánításával a szervezet felé;
e) elegendő erőforrás biztosításával az ISMS létrehozásához, bevezetéséhez, működtetéséhez és fenntartásához;
f) az elfogadható kockázati és kockázati szintű ismérvekről való döntéssel;
g) belső ISMS-auditok elvégzésének biztosításával;
h) az ISMS vezetőségi átvizsgálásainak lefolytatásával."

Az alább ismertetésre kerülő empirikus kutatás eredményei sajnos rácáfolnak arra a felvetésre, hogy a vállalatok vezetői – még azok is, akiknél az ISO 27000 szabvány bevezetésre került – a digitális korban kellő (információ)biztonság-tudatossággal rendelkeznek.

Empirikus vizsgálat

2015. decembere és 2016. januárja között egy számos kérdésből álló online kérdőívvel vizsgáltuk meg a magyarországi vezetők véleményét a digitális korral kapcsolatban, *Szervezetek a digitális korban* címmel (Kollár és Poór, 2016). Vezetőnek tekintettünk minden olyan munkavállalót, akinek van legalább egy alárendelt alkalmazottja, s önálló döntési jogkörrel is rendelkezik bizonyos kérdésekben.
Összesen 406-an töltötték ki a kérdőívet értékelhető módon. Terjedelmi korlátok miatt a kérdőív részletes elemzésétől itt eltekintek, egyedül a nyitott kérdésekre adott válaszokat ismertetem.

A digitális kort leíró mozaikszavak közül a felmérésében a CAMSSA (cloud, analytics, mo-

„ (...) az adatok korában a korábbi korokkal ellentétben másfajta értékek kerülnek a fókuszba.”

bile, socialmedia, security és augmentedreality) mozaikszóhoz tartozó fogalmakat kérdeztük meg a „Kérjük, írja le 1-2 mondatban, hogy mi jut az eszébe a következő fogalomról...” kezdetű kérdésekkel. A gyakoribb és érdekesebb válaszok elemzése során kiderült, hogy a megkérdezett vezetők egy része nem is tudja, hogy mit jelent a cloudcomputing. Többen helyesen fogalmazták meg a bárhonnani könnyű elérést, a platformfüggetlenséget, a hozzáférési jogok kérdését. Sajnos kevesebb, mint 1% írt olyan választ, ami a felhő veszélyeiről, illetve a felhő és az információbiztonság kapcsolatáról szólt. A bigdataanalytics-nél is a válaszadók negyede-ötöde írta azt, hogy nem ismeri, de szerencsére néhányan már a benne rejlő lehetőségeket is leírták (pl.: szofisztikált adatbányászat, algoritmusok használata, megalapozottabb döntések támogatása). A mobileszközök és -alkalmazások tekintetében a vezetők a többi területhez képest tájékozottabbak voltak. A közösségi médiánál a fiatalabbak konkrét alkalmazásokat és az alkalmazások lehetőségeit írták be válaszként, s ahogy az életkor szerint egyre idősebb válaszadókat vizsgálták, megjelentek a „jobban kellene ismernem”, illetve az „én már ebből kinőttem” típusú válaszok is. A közösségi média vállalati, azon belül elsősorban marketing és PR eszközként történő használatáról is többen tettek említést. Az augmentedreality-t a válaszadók zöme gyakorlatilag nem ismerte, vagy csak olyat írt, hogy a „jövő eszköze”, a „jövő lehetősége”.

A digitális kor biztonságfogalmánál szándékosan nem akartukszűkíteni a válaszadási lehetőségeket azzal, hogy csak az adatokra, informatikára, információbiztonságra fókuszáltatva kérdezzük meg a vezetőket. Ennek ellenére válaszaik szinte kivétel nélkül az adatbiztonság, a hálózati biztonság, az informatikai rendszer, a belépési kódok, a vírusvédelem köré szerveződtek, s az információbiztonság humán aspektusáról, a socialengineeringről még csak említést sem tettek.

Ugyancsak nem került említésre az alkalmazottak általános biztonságtudatosságának, illetve szűkebben értelmezett információbiztonság-tudatosságának a fejlesztése, holott több olyan, a kutatásban részt vevő vállalatról is tudunk, amelyik már több évvel ezelőtt bevezette az ISO 27000-es szabványcsaládot. Ez azért érdemel tanulmányunk szempontjából kiemelt figyelmet, mivel az MSZ ISO 27002 dokumentum 46. oldalán a 8.2.1. alfejezetben, a vezetőség felelősségénél a szabvány érthetően és egyértelműen fogalmaz: „A vezetőség követelje meg az alkalmazottaktól, szerződő felektől és a használó harmadik féltől, hogy a biztonságot a meghatározott szervezeti szabályzatokkal és eljárásokkal összhangban alkalmazzák.” A bevezetési útmutatóban pedig – tételesen felsorolva – a vezetőség felelőssége tartalmazza annak biztosítását, hogy az alkalmazottak, szerződő

felek és a használó harmadik fél:

a) „megfelelően legyenek tájékoztatva az információbiztonsági feladataikról és felelősségükről mielőtt az érzékeny információkhoz vagy információs rendszerekhez hozzáférést biztosítanak számukra;
b) legyenek ellátva irányelvekkel, hogy a feladatuk biztonsági elvárásait a szervezeten belül kinyilvánítsák;
c) legyenek ösztönözve, hogy a szervezet biztonsági szabályzatait teljesítsék;
d) egy tudatossági szintet érjenek el a biztonságra vonatkozóan a szervezeten belüli feladatukra és felelősségükre vonatkozóan;
e) alkalmazkodjanak az alkalmazás kikötéseihez és feltételeihez, amelyek tartalmazzák a szervezet információbiztonsági politikáját és megfelelő munkamódszereket;
f) folyamatosan megfelelő jártasságú és minősítésű legyen."

Az elméleti alapvetésben, illetve jelen részben leírtak alapján megállapítottam, hogy a vállalati informatikai és információbiztonsági szabályozás tekintetében

a) a vállalatok rendelkezésére állnak szabványok
b) a szabványok rendelkeznek a vezetőkre vonatkozó biztonsági előírásokkal, illetve
c) a vezetőség felelőssége tartalmazza annak biztosítását, hogy a vállalat érintettjei hogyan járjanak el helyesen az információbiztonság tekintetében, ugyanakkor
d) a szabványok gyakorlati megvalósításánál sajnos nem érvényesül megfelelő hatékonysággal a (felső)vezetők biztonság-tudatosságra nevelése/ coacholása, s ezért
e) szükség van egy olyan modell/módszer kidolgozására, amelyik a szabványban ismertetett modellre építve ezt megvalósítja.

Az információbiztonság-tudatosság fejlesztése

Munkámban többek között Vogelauer (2002), Duzmath (2014), Bates (2015) könyveiben leírt, valamint a coach képzéseim során bemutatott módszereket és modelleket használom. Ezek között az ISO 27001 szabvány 20. oldalán ismertetett PDCA (plan, do, check, act), illetve a PDCA alternatív változatai (PDSA: s – study, OPDCA: o – observation) sem szerepelnek. Azért tartom fontosnak az említett modell alkalmazását a (felső)vezetők információbiztonság-tudatosság témájú coacholása során, mert ha a vezetők ezzel a modellel a coaching-ülések alkalmával megismerkednek, majd egy másik szituációban (pl.: informatikai audit, belső információbiztonsággal kapcsolatos képzések) találkoznak, akkor eredményesebben tudnak részt venni a folyamatokban, illetve hatékonyabban

tudják vezetni/menedzselni azokat.

A szabványos PDCA-modell (szakszerűbben fogalmazva PDCA-ciklus) folyamatosan ismétlődő, négy lépésből álló menedzsment módszer. Eredeti célja szerint a termékek és folyamatok kontrolljára, illetve folyamatos fejlesztésre használják. Ez azt is jelenti coach-nyelven, hogy a coach a (felső)vezetővel bizonyos időközönként áttekinti a vállalat életében zajló, információbiztonsággal kapcsolatos eseményeket, folyamatokat, majd részint tanácsadói, részint coach szerepben újra megerősítik a vezető információbiztonság -tudatosságát. Ahogy Szilágyi (2014) fogalmaz: lista helyett PDCA, vagyis a biztonságtudatosság-coachingnál nem egy listát állítunk össze (bár lehetnek listaelemek), hogy min kellene a vezetővel dolgoznunk, hanem egy folyamatosan ismétlődő ciklust tekintünk át, s ha sikeres az együttműködésünk, akkor egy spirált tudunk realizálni (Deming, 1986), amelyik egyre magasabbra és magasabbra emeli a vezetői biztonságtudatosságot. A biztonságtudatosság így mindig tovább javítható, az ismétlések révén pedig a nevezett lépéseket egyre minőségibb, tudatosabb szinten tesszük meg.

Megjegyzem, hogy sajnos egyes vállalatok túlkorlátozzák harmadik fél (külső coach, vagy tanácsadó) bizalmas adatokhoz történő hozzáférését, illetve a biztonsági események megismerhetőségét – ami alapja az információbiztonság-tudatosság célú coachingnak– így a coach munkája a számára biztosított információk ismeretében ugyan sikeresnek mondható, de összességében sikeresebb is lehetne. A titoktartási szerződés – mely a vállalati/vezetői tanácsadás és coaching során rendszerint alapvető elvárás – kiegészítése akár az IT-vezető javaslataival hatékonyan tudja megoldani az említett problémát.

A PDCA-modellben az egyes betűk jelentése a következő:

Plan – tervezés. Általánosságban azt mondhatjuk, hogy a tervezés során az elvárt teljesítményt, vagy valamilyen teljesítmény-alapú szintet, illetve az ezek eléréséhez szükséges célokat és folyamatokat kell meghatározni. Egy másik megközelítés szerint (1) találkozunk a hibával, (2) feltárjuk a hiba okait, majd (3) megtervezzük a hibajavítást. Ebben a modellben is megfogalmazásra kerül a cél, ugyanakkor a hangsúlya – ahogy azt később látni fogjuk – nem megfelelő. A szabvány így ír a tervezésről: „Olyan ISMS-politika, -célok, -folyamatok és -eljárások kialakítása, amelyek lényegesek annak érdekében, hogy a kockázat kezelése és az információbiztonság fejlesztése a szervezet általános politikájával és céljaival összhangban lévő eredményeket tudjon felmutatni."

A coaching szempontjából fontos kulcsszavak a következők:

- tervezés
- cél
- folyamat
- kockázatkezelés

- eredmények

Do – végrehajtás, cselekvés, megvalósítás. A cselekvés általánosságban azt jelenti, hogy (1) a folyamatokat elindítják, (2) a tervet végrehajtják, (3) a terméket elkészítik. Ennél a résznél beszélhetünk a megvalósítás során összegyűjtött anyagok elsődleges elemzéséről, hiszen ezek lesznek majd a későbbi részek kiindulópontjai. A szabvány így ír a végrehajtásról: „Az ISMS-politika, -intézkedések, -folyamatok és -eljárások bevezetése és működtetése."

A coaching szempontjából fontos kulcsszavak a következők:

- adatgyűjtés
- folyamatindítás
- végrehajtás
- bevezetés
- működtetés

Check – ellenőrzés. A cselekvés részben mért és összegyűjtött adatok, illetve az ezekből képzett információ és tudás révén itt nyílik lehetőség az elvárt eredmények és az aktuális eredmények összevetésére. Ez a tervezés részben megfogalmazott célok, a cselekvés részben megvalósított eredmények összehasonlítása. Ideális esetben ezek egybeesnek, gyakorlatilag azonban mindig lesznek eltérések, ezek kiderítése a legfontosabb feladat az ellenőrzés során. Lehetőség van az adatok grafikonban történő ábrázolására, de akár saját mutatószámok képzésére is. Az itt megfogalmazott különbségek adják a megfelelő információt a beavatkozáshoz. A szabvány az ellenőrzéssel kapcsolatban így fogalmaz: „A folyamatok teljesítményének értékelése, és ahol lehetséges, mérése az ISMS-politikával, -célokkal és a gyakorlati tapasztalatokkal összevetve, továbbá az eredmények jelentése a vezetésnek átvizsgálás céljából."

A coaching szempontjából fontos kulcsszavak a következők:

- mérés
- ellenőrzés
- jelentés/tanulmány
- átvizsgálás

Act – beavatkozás (alternatív lehetőség: adjust – igazítás). A tervezett és a megvalósult állapot közötti különbségek gyakran korrekciós intézkedéseket kívánnak meg. A beavatkozás, vagy újabban igazítás során meg kell határozni (1) a különbségek okát, (2) a változtatási helyeket, (3) szükség esetén a változtatási helyek preferenciáját, sorrendiségét, valamint (4) egyéb dolgokat is (pl.: ki a felelős, mi a határidő, stb.). A szabvány a beavatkozással kapcsolatban így fogalmaz: „Helyesbítő és megelőző tevékenységek végre-

hajtása a belső ISMS-átvizsgálás (audit) és vezetőségi átvizsgálás eredményei, illetve egyéb lényeges információk alapján az ISMS folyamatos fejlesztése érdekében."

A coaching szempontjából fontos kulcsszavak a következők:

- korrekció, beavatkozás
- fejlesztés
- végrehajtás ellenőrzése

Ahogy korábban már utaltam rá, a szabványban is bemutatott és használt PDCA-modell eredeti állapotában véleményem szerint nem használható kellő hatékonysággal a coaching során, ezért célszerűnek tartottam, többek között Farmer (2014) ajánlása alapján átdolgozni a modellt, illetve kiegészíteni a problémamegoldás hét lépésével. Egy tíz lépésből álló modellt dolgoztam ki, az alábbiakban az egyes betűk magyarázata olvasható.

Tuning – ráhangolás. Ideális lenne, ha minden (felső)vezető megértené, hogy az adatok korában milyen értékkel bírnak az adatok és az adattárolók, s hogy ezek elvesztése, törlése, meghibásodása, stb. mekkora, Forintban/dollárban/stb. kifejezett veszteséget jelenthet a vállalkozásnak. A kérdés tehát nem az, hogy kell-e foglalkozni a (felső)vezetők információbiztonság-tudatosságával és az (információ)biztonság iránti elköteleződésével, hanem az, hogy milyen módon. Hogyan lehet rávezetni, ráhangolni a (felső)vezetőt arra, hogy ahogy a fizikai világban levő értékeit akár otthon, akár a vállalatnál magától értetődően védi, úgy legalább ilyen gondossággal járjon el a (bizalmas) adatok, információk tekintetében. A ráhangolás gyakoribb módszerei a következők:

- esettanulmány elmesélése
- a coach saját élményének az elmesélése
- a (felső)vezető múltjában levő információbiztonsággal kapcsolatos eset átbeszélése
- tanulmány, cikk ajánlása olvasásra
- rövidebb könyv, vagy könyvfejezet ajánlása olvasásra
- releváns film ajánlása megnézésre (pl.: Youtube)

Purpose – cél. A célok kijelölésénél és meghatározásánál a coachoknak több módszer/modell is a rendelkezésére áll, én a gyakorlatban a SMART modellt szoktam használni. A SMART röviden azt jelenti, hogy a célnak konkrétnak (Specific), mérhetőnek (measurable), megvalósíthatónak (achievable), relevánsnak (relevant) és időkerethez kötöttnek (time-bound) kell lennie. Bizonyos esetekben a SMARTER modellt is használom, ahol az utolsó két betű jelentése: eredmények értékelése (evaluated), tervek felülvizsgálata, módosítása (reviewed). A (felső)vezetők információbiztonság-tudatossága fejlesztő-

séhez azonban jobbnak látom a klasszikus SMART modellt.

A konkrét cél az információbiztonság-tudatosság fejlesztése a (felső)vezetők körében. Ahhoz, hogy ezt a célt a (felső)vezető is magáénak érezze, azonosuljon vele, szükséges konkretizálni.

A **konkretizálás** történhet a ki, mit, mikor, hol, hogyan, miért kérdésekre adott kifejtős válaszok segítségével, vagy Wehrle (2014) skálás kérdésére adott válasszal. A kérdés így hangzik: „Kérem, képzeljen el egy 1-től 10-ig terjedő skálát, amelyen a tíznél van az ön célja, hogy információbiztonság-tudatossága az elvárt szinten legyen (meghatározott időn belül). Hol áll ebben a pillanatban?" Mivel (felső)vezetőnek tesszük fel a kérdést, lehet követő kérdéseket is feltenni, mint pl.: „ha beosztottait kérdeznénk meg, ön szerint milyen választ adnának?", vagy „ha beosztottait kérdeznénk meg az ön információbiztonság-tudatosságáról, milyen választ adnának?", illetve „mit gondol, mi lehet az eltérés

„Nem ritka az az eset sem, amikor a munkavállaló, de akár a (felső)vezető is a közösségi oldalakon oszt meg szerinte semmitmondó tartalmakat, melyeket a szakavatott, pszichológiai manipulációhoz (socialengineering) értő szakemberek kielemeznek, feldolgoznak annak érdekében, hogy a személyt, a vállalatot, illetve a vállalat bizalmas adatait tároló rendszereket érő támadásokat tudjanak megvalósítani."

oka?".Érdemes olyan kérdést is feltenni, ami az eredmény elérésére vonatkozik, pl.: „milyen eredmény elérésekor lenne elégedett magával/alkalmazottaival?", illetve, ha emocionális megerősítést is szeretnénk, akkor „mit érezne ekkor?", vagy „hogyan fejezné ki örömét/elégedettségét?".

A **mérhetőség** – ahogy fentebb már utaltam a coach/tanácsadó és az üzleti partner bizalmi viszonyára –csak akkor lehetséges akár a cél meghatározásánál, akár a PDCA-modellben, ha a coach/tanácsadó hozzá tud férni az információ- és IT-biztonsággal kapcsolatos valamennyi, vagy közel valamennyi, a munkájához szükséges adathoz, jelentéshez, felméréshez, stb. Ha erre van lehetőség, akkor a különböző, az elsősorban az IT-audit során használt mérőeszközök, illetve ezek (mutató)számai segíthetnek. Ezek alapján könnyű választ adni a mi, mennyi, hány, hány százalék, stb. kérdésekre. Ha nincs, vagy csak korlátosan van lehetőség, akkor is érdemes néhány kérdést feltenni, mint pl.:

- Milyen visszajelzések alapján fogja ön tudni, hogy elérte a célját? Ez a visszajelzés objektív, vagy inkább szubjektív?

- Összehasonlítva a kiindulási állapotot (az ön információbiztonság-tudatosság szintjét) és az elért állapotot, miben tudja megfogalmazni a lényeges eltérést? Miben várja a lényeges eltérést?

Megvalósíthatóság. Ha a (felső)vezető elég sok konkrét célt fogalmaz meg, s a coach/tanácsadó úgy látja, hogy egy PDCA-cikluson belül nem lehet valamennyit megvalósítani, akkor célszerű egy rangsort felállítani a célok között, s azt mondani, hogy az is mérhetőség, hogy ezek közül csökkenő fontossági sorrendben legalább hány valósuljon meg. A megvalósíthatóság során rendszerint a „hogyan?" kérdésekre, valamint a cél realitására keresünk választ. A (felső)vezetőknél saját információbiztonság-tudatosságuk fejlesztése mellett – összhangban a szabványban leírtakkal – további cél lehet a munkavállalók, beosztottak, alkalmazottak információbiztonság-tudatosságának a fejlesztése is. Ez pedig a megvalósíthatóságnál felveti az együttműködő csoportok, illetve a csoportos megvalósíthatóság lehetőségeit is (pl.: csoport-coaching).

Azokat a célokat tekintjük **releváns**nak, amelyek a (felső)vezetőt, a csapatot, az osztályt, illetve akár az egész szervezetet előre viszik – jelen esetben fejlesztik az információbiztonság-tudatosságot. Az információbiztonság-tudatosság fejlesztése, mint cél, nem önálló, hanem szervesen kapcsolódik a vállalat és (felső)vezetőinek (stratégiai) céljaihoz, többek között a biztonságosabb és így kiszámíthatóbb működéshez, a nagyobb profithoz, a hibák/leállások minimalizálásához. Ha a spirituális menedzsment alapgondolatát idézzük, akkor a végső cél egy emberségesebb, boldogabb, nyugodtabb, biztonságosabb, jobb munkakörnyezet megteremtése, ahol mindenki tudja, hogy miért van az adott vállalatnál az adott pozícióban, illetve azt is, hogy szükség van rá, hiszen nem csak a munkája, hanem ő maga is fontos. A cél relevanciájának a vizsgálatakor meg szokták kérdezni, hogy megéri-e a cél, hogy az idő megfelelő-e, illetve, hogy megvalósítható-e a jelenlegi gazdasági-társadalmi környezetben. Határozott álláspontom, hogy az információbiztonság-tudatosságuk fejlesztése megéri, az idő elérkezett és megvalósítható kisebb-nagyobb erőfeszítések és erőforrások bevonása révén.

A cél megvalósításának **időkeret**énél a PDCA filozófiája miatt nem lehet beszélni végső cél eléréséről, hiszen a modell – ahogy fentebb írtam – spirális volta miatt egyre magasabbra és magasabbra emeli a szintet, az elkötelezettséget, a biztonságot. Ugyanakkor annak érdekében, hogy egy ciklus körbeérjen, mindenképp érdemes egy ciklus végét jelző időpontot megjelölni, illetve feltenni a következő kérdéseket:

- Mit fog csinálni legelőször annak érdekében, hogy fejlessze információbiztonság-tudatosságát?
- Mit fog csinálni az elkövetkező egy hétben annak érdekében, hogy…
- Mit fog csinálni az elkövetkező egy hónapban annak érdekében, hogy…
- Mit fog csinálni az elkövetkező második/harmadik/negyedik/stb. hónapban

annak érdekében, hogy…

Mivel ciklusról beszélünk, ezért érdemes arra a kérdésre is választ kapnunk a coacheetól, hogy „mi lesz az utolsó/utolsó előtti dolog, amit tenni fog a cikluson belül információbiztonság-tudatossága fejlesztése érdekében?”. Ez az utolsó/utolsó előtti cselekedet lehet többek között egy rossz szokás végleges feladása (pl.: minden magánéleti eseményt mérlegelés nélkül kiposztol a vezető a Facebookra), vagy egy kötetlen előadás tartása a kollégáknak, hogy a vezető mit tett az elmúlt időszakban saját információbiztonság-tudatosságának fejlesztése érdekében.

A célok meghatározása után következnek a PDCA-modell egyes részei. Fentebb már utaltam rá, hogy célszerűnek, s egyben hatékonynak tartom, ha a PDCA ciklusban megjelenik a problémamegoldás 7 lépése (Vida, 2000) is, így az alábbiakban a coaching/tanácsadás fókuszában ismertetem a ciklust, az egyes ciklusokban a problémamegoldás megfelelő lépéseit, valamint a gyakrabban alkalmazott módszereket.

Plan – tervezés. A tervezés során a problémamegoldás első négy lépése kerül meghatározásra, ezek a következők:

1) **A probléma meghatározása.** A célok ismeretében a probléma meghatározása során a coach a coachee-val közösen (vagy, ha a tanácsadói szerepet nézzük, akkor maga a tanácsadó) meghatározza, hogy melyek a lényeges dolgok, amikkel foglalkozni kell, s melyek azok, amelyek lényegtelenek.
2) **Adatgyűjtés.** Az adatgyűjtéssel már a célmeghatározás során is találkoztunk, amikor a mérhetőség kérdését vizsgáltuk. Itt a fókusz azonban a probléma megértésén, az okok megkeresésén van. Célszerű lehet adatgyűjtő lapokat tervezni. A coach munka során egyfajta adatgyűjtő lapnak fogható fel a naplózás, amikor a coachee meghatározott témában, jelen esetben az információbiztonság témájában naponta, vagy legalább hetente néhány alkalommal bejegyzi a történéseket a naplóba.
3) **Adatok elemzése.** Az adatok elemzése során a probléma súlyponti kérdéseinek a meghatározása a feladat. A coach a coachee-val közösen néhány, az információbiztonság szempontjából lényeges okot azonosít. Ilyen okok lehetnek többek között:
    - hanyagság (pl.: védelem/őrizet nélkül hagyott informatikai eszköz)
    - kényelem (pl.: egy jelszó minden alkalmazáshoz, automatikus jelszómentés)
    - szószátyárság (pl.: edzésen a coachee elkotyogja az edzőtársának a cége informatikai hibáit, sebezhető pontjait)
    - befolyásolhatóság (pl.: a coachee a gyermeke kérésére kölcsönadja „játszani” a vállalati csúcs-laptopot)
4) **Okok elemzése.** Az okok elemzésénél – egyfajta őszinte tükröt állítva a coachee

elé – arra keresünk választ, hogy mi lehet az okok gyökere. A gyökér-okok vizsgálata, a „szembesítés" az alapja a (felső)vezető információbiztonság-tudatossága fejlesztésének, feltéve természetesen, hogy a (felső)vezető valóban szembesülni akar-e a gyökér-okokkal.

A tervezés során kerül meghatározásra a cselekvési terv, a terv fontosabb lépései, a lépések egymásutánisága és/vagy egymás mellett futása, az egyes lépések időkerete. Szükség lehet (coaching) eszközökre, illetve ha egy feladat túl komplexnek tűnik, akkor allépések meghatározására, valamint a kritikus út elemzésére is. Célszerű a (felső)vezető információbiztonság-tudatossága fejlesztésének a tervét leírni, szükség esetén az IT-vezetővel is egyeztetni, s inkább irányadónak kell tekinteni, semmint egy megváltoztathatatlan, kőbevésett utasítástárnak.

A tervezés során a következő módszereket is érdemes alkalmazni, főleg ha a coach inkább tanácsadónak érzi magát ezen a területen:

- Adatgyűjtő lap
- Brainstorming
- Folyamatábra
- Hisztogram
- KJ módszer
- Napló
- Ok-okozat diagram
- Pareto-elv
- Projektterv
- Szórásdiagram
- Tükör

Do – végrehajtás, cselekvés, megvalósítás. Ennél a lépésnél a tervezés során meghatározott cselekvési terv kerül megvalósításra. Itt található a problémamegoldás ötödik lépése, melynek lényege a leghatásosabb és leghatékonyabb megoldás realizálása.

A megvalósítás során a coach-tanácsadó az alábbi módszereket is igénybe veheti:

- Fadiagram
- Hálódiagram
- Mátrixdiagram

Check+Feedback – ellenőrzés és visszacsatolás. A (felső)vezetői információbiztonság-tudatosság fejlesztése során a megvalósítás/végrehajtás az ellenőrzéssel gyakorlatilag párhuzamosan halad, mivel a megvalósítási rész coaching ülései lehetővé teszik a coachnak és a coacheenak is, hogy áttekintsék, hogy az előző ülés óta milyen változások

történtek, hogyan halad a terv végrehajtása. Célszerű lehet már a tervezés résznél olyan eszközök átbeszélése és közös elfogadása, amelyek segíthetik az ellenőrzést. A hét lépéses problémamegoldás hatodik lépésével lehet itt találkozni, ez az elért hatások értékelése. Sajnos a mérnöki/informatikai megközelítés elsősorban csak az elért eredményekre fókuszál. Az információbiztonság-tudatosság fejlesztése során természetesen a coach is kiemeli, hogy a terv mely részei működnek a gyakorlatban, ezzel segítve a pozitív visszacsatolást a coachee számára. Ez különösen akkor örömteli, ha a tervben foglaltakat a coachee túlteljesítette. Lesznek azonban olyan részei a tervnek, amelyek vagy csak részint kerülnek megvalósításra, vagy egyáltalán nem. Mivel ez a folyamat elsősorban a (felső)vezetői személyiség fejlesztését célozza meg, ezért érdemes minél puhább, humánusabb módszerek közül választani, különösen azért, mert számos esetben a vezetői coaching része a life coaching is, ami érinti a (felső)vezető privát szféráját (család, barátok). Miközben a (felső)vezető a munkatársakkal és beosztottakkal kellő következetességgel jár el az információbiztonság-tudatosság fejlesztése tekintetében, s ülésről-ülésre munkahelyi sikerekről számol(hat) be, addig a magánéletben gyakran ellágyul, így a terv egyes részei nem, vagy nehezebben teljesíthetőek. Segítő kérdés lehet a következő:
„Milyen módosításokat és változtatásokat lenne érdemes az eredeti terven tennünk annak érdekében, hogy az ön számára nehezebben teljesíthető célok is megvalósíthatóak legyenek?"

Vida (2000) a következő módszerek használatát javasolja az ellenőrzés során (megjegyzem, inkább a tanácsadó-vénájú coachoknak):

- Ellenőrző kártya
- Ellenőrző lista
- Hisztogram
- Ok-okozat diagram
- Pareto-diagram

Act – beavatkozás. A (felső)vezetői információbiztonság-tudatosság fejlesztésének legnehezebb kérdése a coachok számára az, hogy meddig engedje a megvalósítás-ellenőrzés-visszacsatolás során a folyamatot „szabadon futni", s mikor avatkozzon be akár tanácsadói/szakértői határozottsággal is. A problémamegoldás hét lépéses modelljében itt található az utolsó lépés. Vida (2000) így ír erről: „A megoldás rögzítése, vagy ha a megoldás nem járt a kívánt eredménnyel, akkor visszatérés a 3. ponthoz (adatok elemzése), vagy új probléma meghatározásához." Mivel a (felső)vezetői coaching során rendszerint a vállalati/szervezeti információbiztonság-tudatosság fejlesztésével kapcsolatos elvárásoknak kell megfelelni, ezért az igazítás/beavatkozás mértéke és miléntje nagymértékben függhet a vállalat felelős IT-vezetőjétől. Itt – védve a coach etikus viselkedését – tisztázni kell, hogy a coach nem utasításokat hajtat végre a coaching ülések során a coachee-val, hanem a vállalati információbiztonsági célokra fókuszálva legjobb

szakmai tudása szerint próbálja fejleszteni a (felső)vezető információbiztonság tudatosságát. Az IT-vezető – különösen, ha a vállalatnál az ISO 27000-es szabvány bevezetésre került – tudja, hogy a PDCA-modell egy folyamatosan meg-megújuló ciklus, ezért a szakmailag a témában felkészült coach logikus érvekkel képes elfogadtatni vele, hogy a következő ciklusban/ciklusokban, amelyek egyébként érintik a vállalati információbiztonsági fejlesztéseket is, újra lehet foglalkozni a (felső)vezetők információbiztonság tudatosságának a fejlesztésével. A coaching szakmai folyamata tehát nem itt ér véget, hanem a következő három pontban.

Change– változtatás, módosítás. Ha az előző pontban a coach a markáns beavatkozás mellett döntött, ami érinti az előzetesen meghatározott célokat, akkor ennél a pontnál van lehetőség a terv módosítására. A terv módosítását a coachok/tanácsadók egy része nem szereti, hiszen a korábban megállapodott keretek kerülnek újrarajzolásra, újrafogalmazásra. És vannak olyan coachok/tanácsadók, akik saját személyes kudarcukként élik meg a céltól, illetve a tervtől való komolyabb eltérést. Mivel folyamatmodellről beszélünk, ezért én úgy gondolom, hogy egy ésszerű keretek közötti módosítás elfogadható.

Measurement+Summary – mérés és összegzés. A coachnak érdemes elgondolkodnia azon, hogy a részéről mi lehetett az oka annak, hogy egy komolyabb módosításra volt szükség. Ezek lehetnek szubjektív és objektív okok, mint pl.:

- szimpátia/antipátia
- idealizált, teljesíthetetlen célok kijelölése
- maximális igazodási kényszer a vállalati IT-szabályokhoz
- adatgyűjtési és -elemzési hanyagság
- túl korán/későn történő beavatkozás a megvalósítás-ellenőrzés-visszacsatolás folyamatába.

Az összegzést akkor is el kell végezni, ha a terv egyébként az előzetes elvárások szerint, vagy közel azzal megegyező módon és színvonalon valósult meg. Ennek írásos formája jó visszajelzés lehet a coachee, valamint a megbízó számára is. Az összegzés formája és tartalma lehet egyedi (a coach által használt dokumentum) és lehet olyan, amelyik már tartalmazza az ISO 27000 család szerinti és/vagy az auditor által javasolt mérési pontokat/számokat is. Ez utóbbinál célszerű felhívni a coach-kollégák figyelmét arra, hogy a humán informatikai, illetve információbiztonsági ellenőrzések egy részében csupán teszteket alkalmaznak, melyeknek értékelése során számadatokat (pontok, százalékok, osztályzatok) kapnak. Természetesen ilyen tesztekkel is lehet mérni az információbiztonság-tudatosságot az egyén, a munkacsoport, illetve a vállalat egésze szempontjából, de a kiemelt pozíciókban, mint amilyen a (felső)vezetőé, ennél lényegesen részletesebb mérésre/visszacsatolásra van szükség. Az eredmények – függetlenül a használt mérési módszerektől – a következő, módosított PDCA-ciklus célmeghatározását segítik elő.

Összefoglalás

Egy közelmúltban végzett nagymintás kutatásunk erősítette meg bennem, hogy a magyarországi (felső)vezetők alulinformáltak az információbiztonság tekintetében, s az információbiztonság humán oldaláról, illetve a socialengineeringről még csak említést sem tettek kérdőívünkben. Tanulmányomban éppen ezért a saját gyakorlatomban is használt modellt ismertetem, melynek célja a (felső)vezetők információbiztonság-tudatosságának a fejlesztése. Az információbiztonsággal foglalkozó ISO 27000-es szabványcsaládban nevesített és használt PDCA-modell véleményem szerint eredeti állapotában nem alkalmas a (felső)vezetők információbiztonság-tudatosságának a fejlesztésére, ugyanakkor jó alapot szolgáltat arra, hogy további elemekkel – különösen a célmeghatározással – kiegészítve hatékony módszer legyen az executive területen dolgozó üzleti coachok kezében. A (felső)vezetők információbiztonság-tudatosságának a fejlesztése a 21. század elejének egyik kiemelt tanácsadási/coaching területe, különösen, hogy a témához való (felső)vezetői hozzáállás nem csak öncélú feladat, de komoly hatással van a vállalat pénzügyi helyzetére és anyagi biztonságára is. A vállalat fejlődése ma már szétválaszthatatlan a dolgozók és a (felső)vezetők információbiztonság-tudatosságától. Ennek része az őket ért socialengineering típusú támadások felismerése és sikeres elhárítása is.

Irodalomjegyzék

Bob Dates: *The littlebook of bigcoachingmodels.* Budapest, Pearson, 2015.
Chris Farmer: *What is PDCA?* előadás, 2014. január
Duzmath Ágnes: *Life coach tanfolyami kézikönyv.* Budapest, szerzői kiadás, 2014.
Edwards W. Deming: *Out of theCrisis.* MIT Centerfor Advanced EngineeringStudy, 1986.
Elliot Aronson: *A társas lény.* Budapest, Akadémiai Kiadó, 2008.
Kollár Csaba, Poór József:*Szervezetek a digitális korban (rövid kutatási jelentés).* Budapest, PREMA Consulting, 2016.
Kollár Csaba: *Kommunikáció a digitális korban.*Budapest, PREMA Consulting, 2014.
LawrenceLessig: *Free culture: howbigmediausestechnology and thelawtolock downculture and controlcreativity.* New York, The Penguin Press, 2004.
Martin Wehrle: *Az 500 legjobb coaching-kérdés.* Budapest, Garbo könyvkiadó, 2014.
Muha Lajos (szerk.): *Az informatikai biztonság kézikönyve.* Budapest, VerlagDashöfer, 2004.
Oroszi Eszter:*Socialengineering.* Budapest, BCE, 2008.
Szilágyi Miklós: *Lista helyett PDCA (vagy mindegy minek hívod...).*http://vezetoi-coaching.blog.hu/2014/04/21/lista_helyett_pdca_vagy_mindegy_minek_hivod letöltés: 2016.05.20.
Vida Csaba: *VÁLLALATIRÁNYÍTÁS IV. Módszerek és eszközök.* Pécs, PTE, 2000.
Werner Vogelauer: *A coaching módszertani ABC-je.* Budapest, KJK-Kerszöv, 2000.
Wikipédia releváns szócikkei

Szabványok

MSZ ISO/IEC 27001. Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények.
MSZ ISO/IEC 27002. Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve.