



# RENDVÉDELEM

VII. évfolyam  
2018/különszám



BELÜGYMINISZTERIUM



## **IMPRESSZUM**

**KIADJA:**

Belügyi Tudományos Tanács

**FELELŐS KIADÓ:**

Dr. Dános Valér ny. r. vezérőrnagy, a Belügyi Tudományos Tanács ügyvezető alelnöke

**SZERKESZTŐ:**

Dr. Sabjanics István, a Belügyi Tudományos Tanács titkára

**KIADÓ:**

Cím: 2090 Remeteszőlős, Nagykovácsi út 3.

Postacím: 1903 Budapest, Pf. 314.

E-mail: titkar@bm-tt.hu

Telefon: +36 26 795 911, BM: 24-592

Fax: +36 26 795 919, BM: 24-650

HU ISSN 2560-2349

**A kiadványban megjelenő tanulmányok nem tükrözik a kiadó álláspontját.**

**TARTALOMJEGYZÉK**

Szerzők .....	3
Szerkesztői előszó .....	4
Fehér Judit: Információbiztonsági események kezelése egy belügyi szervnél .....	5
Tózsér Erzsébet: A pszichológia szerepe a rendőrségi szervezeti kultúrában .....	20

## SZERZŐK

**FEHÉR JUDIT** doktorjelölt, Óbudai Egyetem,  
Biztonságtudományi Doktori Iskola

**TÓZSÉR ERZSÉBET** PhD hallgató, Nemzeti Közszolgálati Egyetem,  
Rendészettudományi Doktori Iskola

## SZERKESZTŐI ELŐSZÓ

A Belügyminisztérium – szakmai tevékenységének elméleti segítése, valamint doktori iskolák és hallgatóik munkájának gyakorlati támogatása érdekében – együttműködési megállapodást írt alá 2014 őszén nyolc állam- és jogtudományi doktori iskolával, valamint a Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskolájával.

A gyakornoki rendszer valamennyi tudományterületre történő kiterjesztése céljából a Belügyminisztérium együttműködést kötött 2015 májusában az Országos Doktori Tanáccsal és a Doktoranduszok Országos Szövetségével.

Az együttműködési megállapodásokban foglaltak a Belügyminisztérium gyakornoki rendszerének működtetése által valósulnak meg, melynek keretében a Belügyminisztérium feladatköréhez kutatásaikkal kapcsolódó doktoranduszoknak, doktorjelölteknek lehetőséget biztosít a kapcsolódó belügyi szervnél kutatásuk lefolytatásához.

A Belügyminisztérium közigazgatási államtitkára, a Belügyi Tudományos Tanács elnöke 2017 márciusában, immár második alkalommal hirdette meg pályázatát a Belügyminisztériumot érintő közszolgálati témában – doktoranduszok, abszolutóriumot szerzett és fokozatszerzési eljárás alatt álló – kutatók számára gyakornoki rendszer keretében tudományos kutatás folytatására.

A Belügyminisztérium gyakornoki rendszerének 2017. évi periódusában 12 kutató vett részt sikerrel; egy fő tudományos fokozatot szerzett, egy fő doktorjelölti státuszban van.

A Belügyi Tudományos Tanács 2018. évi különszámában lehetőséget biztosított a gyakornok számára kutatási eredményeik publikálására. Jelen számunkban a programban résztvevő két gyakornok beszámolója válik elérhetővé a téma iránt érdeklődők számára.

Az értékes tanulmányokhoz hasznos olvasást kívánunk!

FEHÉR JUDIT<sup>1</sup>

## INFORMÁCIÓBIZTONSÁGI ESEMÉNYEK KEZELÉSE EGY BELÜGYI SZERVNÉL

### Absztrakt

Nem minden információbiztonsági esemény incidens. Hajlamosak vagyunk arra, hogy incidensként detektáljunk az információs rendszerünkben történő működésbeli elakadást. Holott, ha jól, megfelelően szabályozott környezetben kezelnénk, akkor a biztonsági eseményt okozó problémának a felfedéséből, kivizsgálásából egyértelműen kiderülne, hogy történt-e károkozás azaz olyan incidens, amit kezelni kell. Sok esetben csak elfedjük a probléma okozóját, „tűzoltással” helyre állítjuk a működést és nem veszünk tudomást az okokról. Ami ismételt biztonsági eseményt fog okozni később, mind addig amíg meg nem szüntetjük a probléma okát. Ezzel önmagunknak és a szervezetünknek még nagyobb kárt okozunk. Valószínűleg a probléma megoldásának és megszüntetésébe fektetett energia már az első jelenségnél kevesebb lenne, mint később a nagyobb, szélesebb károkozás megszüntetése.

**Kulcsszavak:** biztonsági esemény, incidens, probléma, kárelhárítás

### Bevezetés

„Tökéletes biztonságot akkor tudunk elérni, ha beszüntetjük az összes tevékenység végzését, azaz nem csinálunk semmit. Belátható, hogy ez ritkán választható megoldás. Azonban a veszélyek és lehetőségek ismeretében eredményesen kezelhetjük a tevékenységek végzéséből fakadó kockázatokat a szükséges kontrollok kialakításával, és működtetésével. A belső kontroll rendszer kialakítása során különféle védelmi intézkedések kombinációjaként alakítják ki a biztonsági szakemberek azt a kontroll rendszert, amely a felső vezetés által felvállalt kockázat vállalási szintnek megfelelő védelmet biztosítja a szervezet számára.

Egy szervezetnél akkor jó a biztonsági kultúra, ha a munkatársak ismerik jogaikat és kötelezettségeiket, és érvényesítik is azokat. Azoknak a munkatársaknak, akik tudatlanságból, hanyagságból, vagy szándékosan nem biztonságtudatosan viselkednek, ismételt biztonságtudatosági oktatáson kell részt venniük, illetve el is maraszthatják őket. A biztonsági kultúrát tehát az egyének biztonságtudatos magatartása alakítja ki, ahol kialakult, ott a munkatársak tudják, mi veszélyeztet(het)i a biztonságot, és ennek megfelelően cselekszenek is. „[1]

---

<sup>1</sup> doktorjelölt, Óbudai Egyetem, Biztonságtudományi Doktori Iskola

„Az információs rendszer szempontjából fenyegetésnek tekintünk minden olyan körülményt vagy eseményt, amely az adatok, vagy információs rendszerek biztonságát fenyegetheti. Ide soroljuk például a személyektől eredő támadásokat (pl. számítógépes betörés), és a külső behatásokat (pl. földrengés).”[1]

Egy belügyi szervnél minden esetben érzékeny kérdésként jelentkezik az információbiztonság területén a biztonsági események kezelése. Minden esetben az a cél, hogy minél kisebb területet érintsen, minél alacsonyabb kárértékkel, minél rövidebb időn belül megszűnjön a biztonsági esemény és helyre álljon az eredeti állapot.

Mindenkinek más és mást jelent a biztonsági esemény az információbiztonság világában. Mit is nevezünk biztonsági eseménynek? Sok szakember hajlamos a biztonsági eseményeket incidensként vagy problémaként detektálni. Ez a három kifejezés, három különböző jelentéstartalommal bíró szakmai meghatározása az események kezelésének sorában. A fogalmak értelmezésében segítségül vannak a szakmát meghatározó útmutatók.

### 1. A biztonsági esemény az Ibv tv szerint

„*biztonsági esemény*: nem kívánt vagy nem várt egyedi esemény vagy eseménysorozat, amely az elektronikus információs rendszerben kedvezőtlen változást vagy egy előzőleg ismeretlen helyzetet idéz elő, és amelynek hatására az elektronikus információs rendszer által hordozott információ bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása elvész, illetve megsérül;” [2]

Ebből következik, hogy a biztonsági eseménynek még a gyanúját is komolyan kell venni, nem lehet eltekintetni tőle, ki kell vizsgálni.

Összegezve biztonsági eseménynek tekintjük az elektronikus információs rendszer biztonságában beállt olyan kedvezőtlen változást, melynek hatására az informatikai rendszerben kezelt adatok bizalmassága, sértetlensége, hitelessége, funkcionalitása vagy rendelkezésre állása megsérült vagy megsérülhet.

2. Az incidenst az ITIL informatikai szolgáltatás módszertana az alábbiakban határozza meg:

„Incidens (Incident) – Olyan esemény, amely nem része az informatikaszolgáltatás normális működésének és a szolgáltatás kiesését vagy minőségének romlását eredményezi.”

Ebből az következik, hogy az események mögött általában valamilyen incidensek állnak. Az incidens lehet hiba egy kérdés vagy új kérés is, tehát valamilyen információval már rendelkezünk róla és kárt okozott.

Összegezve az incidens egy bekövetkezett biztonsági esemény, amely azonnali beavatkozást igényel.

3. A problémát az ITIL informatikai szolgáltatás módszertana az alábbiakban határozza meg:

„Probléma (Problem) - Az incidens(ek) valódi, még fel nem tárt oka. Ez lehet egy meghibásodott konfigurációs elem vagy ismeretlen hiba.”

Ebből az következik, hogy ez lehet ismert, amelyre létezik megkerülő vagy igazi megoldás, vagy ismeretlen, amelyre még nincs megoldás, ezért mindaddig fennállnak, amíg egy változtatással végleg meg nem oldjuk a problémát.

Összegezve a probléma egy incidens kiváltó oka, amelyet ha megoldunk, megszűnik az incidens, megkezdhetjük a károk elhárítását, minimalizálását, csökkentését és lezárásra kerül a biztonsági esemény.

### A biztonsági esemény szabályozása

„A közigazgatási információs rendszerek működésében tapasztalt tipikus biztonsági kockázatok:

- egy új rendszer a beüzemelés követő néhány héten belül több napra megbénul;
- vezető munkatársak adathordozói illetéktelenek kezébe kerülnek a rajta levő személyes levelezéssel, nem nyilvános adatokkal;
- a munkájában el nem ismert rendszergazda az üzemeltetési feladatok naprakész pontos dokumentálása nélkül távozik;
- a munkatársak áthelyezésüket követően is hozzáférnek a korábbi szervezeti egységük anyagaihoz.

Mi okozza a biztonsági kockázatok növekedését:

- • az informatikai szolgáltatásoktól és az adatkapcsolat folyamatosságától való függés;
- • a szándékos károkozás megnövekedett motivációja;
- • a nagy informatikai beruházást is tartalmazó projektek kudarcai;
- • a hardver, illetve szoftver eszközök meghibásodása;
- • a virtuális vállalatok terjedése;
- • az időjárás változása.

Az információbiztonsági kockázatok kezelésének négy alapszere van:

- a tevékenységek beszüntetése (kockázat megszűnik);
- a tevékenység kockázataira biztosítás kötése (kockázatot áthárítottuk a biztosítóra);
- a felelős vezető a kockázatot megismeri és nem tart további intézkedést szükségesnek (kockázatot a szervezet felvállalta);
- a felelős vezető védelmi intézkedéseket (kontroll) valósít meg, vagy szüntet meg (kockázati válasz meghatározása és megvalósítása).”[1]

A biztonsági eseményt minden esetben kezelni kell. Még az Ibvtv is kiterjed erre a feladatra:

„A biztonsági esemény kezelése: az elektronikus információs rendszerben bekövetkezett biztonsági esemény dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység;”[3]

Hogyan is kezdünk neki egy ilyen esemény kezelésének?

Célszerű egy szervezetenél eljárásrendet kidolgozni a biztonsági esemény kezelésére. Álláspontom szerint egy ilyen eljárásrendnek célja, hogy az adott szervezetenél az elektronikus információs rendszerei tekintetében egységes módon definiálja az alapelveket, rögzítse a keretrendszert és szabályozza azokat a munkafolyamatokat, amelyekkel a legkisebb kárértékkel elháríthatja a működést befolyásoló tényezőket. Az alábbiakban összegzem azokat a javaslatokat, amit egy belügyi szervezetnek feltétlenül rögzítenie kell egy biztonsági eseményt kezelő eljárásrendben.

Egy ilyen eljárásrendben meg kell határozni a szervezeti hatályát, hogy a szervezeten belül és kívül kik érintettek benne. Azaz a szervezettel más módon kapcsolatba kerülő természetes és jogi személyekre, jogi személyiséggel nem rendelkező szervezetekre (külső személy). A szervezeti hatályban feltétlenül meg kell határozni a hatály mértékét. Például a külső személyek tekintetében a velük kötött szerződésben rögzített mértékben, illetve a titoktartási nyilatkozat alapján kötelesek eljárni biztonsági eseménykor.

A szervezeti hatályt követően ki kell térni a területi hatály tekintetében. Meg kell határozni azon telephelyeket, egymástól elkülönülő épület egységeket, vagy alszervezetek objektumait, amelyek adott esetben akár földrajzilag is elkülönülnek a szervezettől, de szervezesen részét képezik.

A következő szabályozandó terület a tárgyi hatálya. Itt javasolt meghatározni a szervezet általa üzemeltetett valamennyi meglévő és a jövőben fejlesztendő informatikai rendszert, illetve azok környezetét alkotó rendszerelemeket azok teljes életciklusában (az előkészítéstől a rendszerből történő kivonásig). A tárgyi hatálynál egy kormányzati szervnél megfontolandó a minősített adatokat rendszerek kérdésköre, és a vezeték nélküli Internet hozzáférés használatra és a nyilvános prezentáció megjelenítő rendszerek. Ezek viszont olyan speciális területeket fednek le, hogy javasolt őket külön szabályozni.

Egy biztonsági esemény kezelő eljárásrendnek álláspontom szerint feltétlenül figyelembe kell vennie és hivatkoznia, az alábbi normatívákra:

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- A hivatkozások között mindenképpen meg kell említeni az adott szervezet Informatikai Biztonsági Szabályzatát.

A hivatkozásokat követően az alapfogalmak között definiálni kell a biztonsági eseményeket, hogy mit minősítünk annak, ezért javaslok néhányat az eddigi tapasztalataim alapján:

- a biztonság megsértésének lehetősége,
- a bizalmasság megsértésének lehetősége,
- a sérthetlenség megsértésének lehetősége,
- a rendelkezésre állás megsértésének lehetősége,
- az adatokkal való visszaélés lehetősége,
- jogosulatlan hozzáférés az adatokhoz,
- jogosulatlan adatkezelés,
- jogosulatlan adatfeldolgozás,
- tudatos vagy gondatlan károkozás az informatikai rendszerben, a rendszerek által kezelt adatok körében,
- tudatos vagy gondatlan károkozás az informatikai eszközökben.

Az eljárásrendben meg kell határozni biztonsági események kezelésével kapcsolatos azon alapelveket, melyek a szervezet céljait szolgálják. Az alábbiak meghatározóak lehetnek egy belügyi szerv esetében:

- a normál szolgáltatásüzemeltetés mielőbbi helyreállításra kerüljön, és az események folyamatokra gyakorolt káros hatása a lehető legkisebbre legyen csökkenthető,
- bármilyen biztonsági esemény hatékonyan felderíthető és kezelhető legyen, különösen abban a tekintetben, hogy egy eseményt incidensként kell-e kezelni vagy sem,
- az azonosított incidensek kiértékelése és a rájuk adott válasz a legmegfelelőbb és leghatékonyabb módon történjen,
- a szolgáltatás lehető legjobb minőségi és elérhetőségi szintje valósulhasson meg,
- a biztonsági eseményekből és azok kezeléséből gyorsan levonhatók legyenek a megfelelő következtetések, hogy a jövőbeli biztonsági események megakadályozásának az esélyei növekedjenek.

A biztonsági eseményeket minősíteni kell, rangsorolni kell. A minősítésekor meg kell állapítani, hogy az eseményben érintett alkalmazások, eszközök, illetve szolgáltatások mennyire fontosak, fennáll-e szolgáltatás-kiesés. Ha van szolgáltatás-kiesés, az mekkora anyagi vagy egyéb kárt okoz, illetve fel kell mérni az érintett felhasználók számát, körét, összetételét.

A biztonsági esemény súlyozását a következő tényezők összességének figyelembe vételével kell meghatározni a szervezetnek:

- alkalmazás kritikussága
- az érintett felhasználók száma
- alkalmazás(ok)ban a hiba által érintett funkciók jellege
- érintett alkalmazások száma
- a szakrendszerek közti kommunikáció működése;
- rendészeti szerv érintettsége,

Tekintettel a fentiekre a biztonsági esemény súlyozása az alábbiak szerint alakulhat:

1. alacsony: az esemény gyanúja, kéretlen levél, kismennyiségű adathalász levél,
2. közepes: vírusfertőzés adatvesztés és adatkompromittálódás nélkül,
3. magas: működés biztonsági esemény, kis mennyiségű adat szivárgás, tudatos személyes adat kiszivárogtatás, bűncselekmény,
4. kritikus: nagy mennyiségű személyes adat szivárgás, az informatikai rendszerek kompromittálódása, az informatikai rendszer működésének megakadályozása, leállítása.

A biztonsági esemény kezelése során meg kell határozni az eljárásban érintettek körét, a felelőseket. Egy belügyi szervnél az alábbi felelős személyek lehetnek érintettek:

- A szervezet Információbiztonsági Felelőse (a továbbiakban: IBF), vagy helyettese,
- az üzemeltető szervezet Biztonsági Vezetője,
- az ügyben érintett külső személyek Biztonsági Vezetője
- az ügyben érintett szerv vagy szervezeti egység vezetője,
- az informatikai szakterület vezetője,
- a szervezet ellenőrzési szakterületének vezetője,
- a szervezet Adatvédelmi Felelőse,
- az érintett rendszer Adatgazdája.

Az eljárásrendben rögzíteni kell az értesítendő Hatóságok körét, melyeket az alábbiakban rendszereztem egy belügyi szervezet esetében:

- NEIH - Nemzeti Elektronikus Információbiztonsági Hatóság
- NAIH - Nemzeti Adatvédelmi és Információszabadság Hatóság
- NMHH - Nemzeti Média- és Hírközlési Hatóság
- Országos Informatikai és Hírközlési Főügyelet
- NKI - Nemzeti Kibervédelmi Intézet
- EÜF – Elektronikus Ügyintézési Felügyelet
- Nyomozó Hatóság
- Nemzetbiztonsági Szolgálatok

A definíciók rögzítését követően meg kell határozni a keretrendszerét az eljárásrendnek, ez azt jelenti, hogy számba kell venni a biztonsági esemény eseteit. Néhányat felsorolok, amelyek egy belügyi szerv esetében a szervezeti felépítéséből fakadóan előfordulhatnak:

- I. Hatósági megkeresés alapján kezelendő biztonsági események
- II. Házkutatási parancs alapján kezelendő biztonsági események
- III. Vezetői megkeresés alapján kezelendő biztonsági események
- IV. Biztonsági esemény észlelése az üzemeltetői szervezet által
- V. A szervezet IBF megkeresése alapján végezendő feladatkör
- VI. Az Iktató rendszerben történt biztonsági esemény kezelése
- VII. A szervezet munkatársa által bejelentett biztonsági esemény kezelése

A szabályozásnak ki kell térnie az eseményt alátámasztó adatok kinyerésének módjára, és azok átadására az érintett hatóságok részére.

Az adatokat minden esetben úgy kell kinyerni az adott érintett elektronikus információs rendszerből vagy az azt monitorozó rendszerből, hogy a későbbiekben más eljárásban bizonyító erőként felhasználhatóak legyenek. Kiemelt figyelmet kell fordítani ezen adatok tárolására, a bizalmasság, sérthetlenség és rendelkezésre állás szavatolására. Ennek megfelelően az alábbi követelmények elengedhetetlenek:

1. a mentéseket külső elektronikus adathordozóra kell másolni, amit biztosíthat a szervezet, vagy az érintett Hatóságis. Ha az adatok átadása online módon történik, a folyamatot alá kell támasztani igazoló log file-okkal, offline mód esetében az átadás-átvételt aláírással kell igazolni.
2. a sérthetlenség garantálása érdekében minden egyes file-ról valamilyen fajta algoritmussal kell lenyomatokat készíteni,
3. nagy mennyiségű file-ok esetében a könyvtárak tartalmáról készült lenyomatokból egy összegző lenyomatot kell generálni,
4. a külső elektronikus adathordozó mellé kell tenni papír alapon a rögzített állományok listáját könyvtárszerkezettel, valamint a lenyomatokkal,
5. nagy mennyiségű file-ok esetén a kísérő lapon csak a főkönyvtárak listáját, azok leírásait, továbbá az összegző lenyomatot kell megjeleníteni,
6. az átadandó eszközöket és listákat lepecsételt zárt borítékban kell a Hatóság, illetve az igénylő számára átadni.

### A biztonsági esemény kezelésének folyamata

A biztonsági események megjelenését két alapvető részre oszthatjuk.

- működés közben minőségi hiba történik
- hatósági megkeresés keretében keressük az esemény jelenlétét

Amennyiben az elektronikus információs rendszerek működése közben minőségi hiba történik, akkor az kihatással van a rendszerek üzemeltetésének céljára. Bekövetkezik egy úgy nevezett esemény. Az esemény egyszerűen egy külső vagy belső hatás, amely miatt az elektronikus információs rendszerek működésének minőségében változás történik.

Ezt a működés változást lehet emberi erőforrással ellenőrizni vagy monitorozni az elektronikus információs rendszerek működését. Az esemény detektálása akkor történik meg, amikor a normális aktivitást megváltozik. Ezt a változás érzékelheti maga a felhasználó, vagy üzemeltető egyaránt:

- megjelennek bizonyos jelenségek, az elektronikus monitorozás közben,
- egy adott időpontban többen hívták az üzemeltetőket ugyanazon eseménynek a megjelenésével,
- többen keresték a helpdesket szerteágazó működési fennakadással,
- izolált esemény történt egy felhasználónál.

Az események bekövetkezésekor a következő feladatokat kell végrehajtani:

1. Esemény észlelése. Ez a legfőbb cél, hogy egyáltalán észlelni tudjuk az eseményeket. Ezért fontos az elektronikus információs rendszerek monitorozása mind monitorozó alkalmazásokkal, mind emberi erőforrás segítségével.
2. Események csoportosítani tudjuk. Többnyire határfoka és rendszeressége szerint. Itt fontos megjegyezni, hogy nem minden eseményből lesz incidens vagy probléma. Lehetnek olyan események is, amelyek csak a gyanúját vetik fel egy létező problémának, de még nem okoztak incidenst, csak biztonsági eseményként jelentek meg. Vannak események, amelyek csak informatív jellegűek, tudnunk kell róluk, de azonnali beavatkozást nem igényelnek. Be kell tudnunk sorolni az eseményt a szabályzóban meghatározottak szerint.
3. Meg kell tudni állapítani, hogy bekövetkezett-e a biztonsági esemény, azaz történt-e incidens és ha igen, az milyen fokú.
4. Előzetes diagnózist kell felállítani, hogy igényel-e az esemény beavatkozást. Ha nem akkor le kell zárni az esetet.
5. Ha igényel beavatkozást, akkor át kell tekinteni, hogy mekkora kört érint az esemény.
6. Meg kell vizsgálni, hogy mi lehetett az esemény kiváltó oka, a probléma.
7. Események közti összefüggések vizsgálatát kell lefolytatni. Meg kell keresni a probléma forrását.
8. Több alternatív intézkedést kell megfontolni, felsorakoztatni.
9. Meg kell kezdeni az intézkedést a probléma megszüntetésére.
10. Vissza kell térni az eredeti normális működési rendre.
11. Fel kell mérni a károkat, és intézkedéseket kell tenni a kárenyhítésre.
12. Az esemény észlelője felé ki kell dolgozni a válaszadási procedúrát, melyen keresztül meg kell történnie a visszacsatolásnak, hogy az esemény megszűnt.

13. Meg kell vizsgálni, hogy hogyan keletkezett a probléma, és megelőző intézkedéseket kell tenni az újbóli megjelenése előtt. Tehát okulni kell az esetből, le kell vonni a konzekvenciákat.

### **Az incidens kezelése**

Az incidens kezeléséről szakmai egyeztetést folytattam a Belügyminisztérium Információbiztonsági szakterület vezetőivel, és mind az igazgatás, mind az ágazathoz tartozó szervek esetében megállapításra került, hogy sok helyen kapkodnak egy valóban megállapított incidens kezelése kapcsán. Megpróbálják minél előbb helyre állítani a működést, helyre állítani az adatokat. Legtöbb esetben figyelmen kívül hagyják az okozó problémát.

Ennek fényében az általuk elmondottak alapján, azokat összegezve felállítottam egy incidenskezelési modellt. Próbáltam olyan nagy adatfeldolgozó szervezeteket megkeresni, ahol az ilyen esetek kezelése mindennapos tevékenységnek minősült. Az alábbi modellt a KEKKH, a Belügyminisztérium és a Rendőrség gyakorlati elemeiből, továbbá a jogszabályok feldolgozásából építettem fel.

A megállapított incidens bejelentését fogadó elsődleges feladata az incidens hatása és sürgőssége alapján annak besorolása. Erre javasolt egy incidens kezelési rendszert létrehozni.

#### *Az incidensek kezelésével kapcsolatos alapfeladatok*

1. Felelősségek és eljárások: meg kell fogalmazni és dokumentálni kell a vezetői felelősségeket, valamint azokat az eljárásokat, amik révén biztosítható a gyors, hatásos és rendezett válaszadás az incidensekre.
2. Események jelentése: meg kell követelni, hogy az események, amilyen gyorsan csak lehet, jelentésre kerüljenek a megfelelő csatornákon keresztül.
3. Gyengeségek jelentése: meg kell követelni az elektronikus információs rendszerrel kapcsolatban álló valamennyi személytől – beleértve a felhasználókat, adminisztrátorokat, rendszergazdákat stb. – hogy jelentsék, ha bármilyen gyengeséget (biztonsági rést) észlelnek vagy gyanítanak az elektronikus információs rendszerekben vagy szolgáltatásokban, vagy a rendszerekhez, a rendszerek biztonságához kapcsolódó szabályzatokban, munkautasításokban.
4. Felmérés és döntéshozatal: a gyengeségeket és az eseményeket fel kell mérni, és el kell dönteni róluk, hogy incidensnek minősülnek-e.
5. Reagálás az incidensekre: a dokumentált eljárások szerint kell reagálni az incidensekre.
6. Tényekre vonatkozó adatok összegyűjtése: meg kell fogalmazni, dokumentálni és alkalmazni kell az incidensekkel kapcsolatos adatok azonosítására, gyűjtésére, beszerzésére és megőrzésére szolgáló eljárásokat.
7. Tanulás az incidensekből: az incidensek elemzéséből és megoldásából szerzett ismereteket fel kell használni arra, hogy csökkenjen a jövőbeni incidensek bekövetkezésének valószínűsége és hatása, illetve, hogy növekedjen az incidenskezelési rendszer hatékonysága.

#### *Az incidenskezelési rendszerrel kapcsolatos használati feladatok*

Ahhoz, hogy viszonylag gyorsan tudjuk kezelni az incidenseket, egy elektronikus információs rendszerrel érdemes a folyamatokat megtámogatni. Az incidenskezelési rendszerbe javaslom az alábbi alapadatokat és folyamatokat rögzíteni:

- a. az események, incidensek észlelése és bejelentése (emberi és/vagy automatikus eszközök útján);
- b. a bejelentéssel kapcsolatos információk összegyűjtése, majd kiértékelése annak megállapítására, hogy mely bejelentéseket kell incidensnek minősíteni;
- c. az incidensek megválaszolása a tevékenységek időkorlátainak megfelelően:
  - azonnal, valós- vagy majdnem valós időben;
  - ahol az incidensek ellenőrzés alatt állnak, ott a nem sürgős tevékenységek levezetése;
  - ahol az incidensek nem állnak ellenőrzés alatt, akkor a krízis tevékenységek indítása – mint például a tűzoltóság kihívása vagy egy üzletmenet folytonossági terv (Business Continuity Plan, a továbbiakban: BCP) aktiválása;
  - az incidens kommunikálása a meghatározott belső és külső partnerek felé.
- d. meghatározott minősítésű incidensek minőségügyi vizsgálata;
- e. valamennyi tevékenység és döntés megfelelő naplózása a további elemzések számára;
- f. az incidens döntéssel történő lezárása.<sup>2</sup>

Az incidenskezelési rendszerrel kapcsolatos felülvizsgálati feladatok

Ki kell alakítani az incidensek lezárását követő felülvizsgálati tevékenységeket, ennek keretében:

- a tevékenységek elemzéséből, a vizsgálatok eredményéből le kell vonni a tanulságokat
- meg kell határozni az intézkedésekkel kapcsolatos fejlesztéseket, függetlenül attól, hogy a tanulságokat egy vagy több incidensből vonták-e le
- meg kell határozni az incidenskezelési rendszer egészére vonatkozó fejlesztéseket.

*Az incidenskezelési rendszerrel kapcsolatos fejlesztési feladatok*

Az incidenskezeléshez kapcsolódó folyamatok fejlesztésének magában kell foglalnia a következőket:

- a szervezet kockázatelemzési és kockázatkezelés folyamatainak felülvizsgálata;
- az incidenskezelési rendszer és a kapcsolódó dokumentáció fejlesztése;
- az információbiztonságra vonatkozó fejlesztések kezdeményezése, amely magában foglalhatja új és/vagy javított biztonsági ellenintézkedések bevezetését is.

### **A probléma kezelése, az okok felderítése**

Ha megvizsgáltuk a problémát, rádöbbenünk, hogy a probléma az incidens mögötti ok, amit egy incidensből nem is feltétlenül lehet kideríteni. Sok esetben az informatikai szolgáltatást nyújtó üzemeltető, a fellépő hibát javítja rögtön, de nem tudják garantálni, hogy máskor nem fog előfordulni. Ennek az az oka, hogy rögtön tűzoltási tevékenységeket kell végezni, hogy a működés helyre álljon, de nincs idő kivizsgálni, hogy mi okozta az incidenst, tehát a problémát. És mivel nem sikerült feltárni az okát az incidensek, elfedik így az üzemeltetők a következményt, azaz kijavították a hibát, de lehet, másnap újra előjön. Ebből fakad, hogy egy adott probléma felderítéséhez nagyon sok körülményt kell ismerni, amit hiába is vizsgálunk ki közel sem biztos, hogy a probléma teljesen feltárható. Miért is ilyen nagyon fontos, hogy a problémát felfedjük? A problémák feltárásának van egy másodlagos

---

<sup>2</sup> A KEKKH nyomán

haszna is, létrejön egy adatbázis az ún. ismert hibákról, amelyek segítséget nyújthatnak az üzemeltetők számára, tehát ki lehet belőle alakítani egy incidens kezelési eljárást, ezzel az incidensekre még gyorsabb választ tudnak adni, és már ki is küszöbölhető a hiba. Ez a tapasztalat szerzés. Ha ezt a tudást az adott szerv üzemeltetői egy másik hasonló belügyi szerv üzemeltetőivel meg tudnák osztani, létre lehetne hozni egy közös „probléma adatbázist”, annak érdekében, hogy az incidenseket elkerülhessék az üzemeltetők, vagy azonnal elháríthassák az azokat okozó problémákat. A probléma kezelését két fajta féle képen tehetjük meg:

- „Reactive (visszaható) Problem Management: amikor a rendelkezésre információk alapján utólag tárjuk fel és elemezzük a problémát.
- Proactive (kezdeményező) Problem Management: előzetes elemzése a lehetséges problémáknak.”[4]

Mindkét megoldás következménye lehet a kárenyhítésnek.

### **Biztonsági Esemény Kezelési Eljárásrend általános rendelkezései**

Az előző fejezetekben azt taglalhattam, hogy milyen sorra jelentkező feladatokat kell ellátni egy biztonsági esemény kapcsán. Ezeket a feladatokat eljárásokba rendszerezni, amelyek mindenkor minden körülmény felett betarthatóak. A fenti eljárások hogyan is jelennek meg a gyakorlatban? Lássunk rá egy általános példát:

1. Biztonsági esemény gyanúját vagy észlelését követően az észlelő szervezet vagy személy értesíti a szervezet IBF-ét,
2. a szervezet IBF megteszi az elsődleges intézkedéseket az esemény kivizsgálására,
3. a szervezet IBF-e felméri az esemény körülményeit, valamint súlyozza azt, valamint megállapítja, hogy történt- e incidens,
4. a súlyozási rend szerint magas és kritikus besorolású biztonsági eseménynél a szervezet IBF értesíti a szervezet vezetőjét és az ügyben érintett felelős személyeket,
5. a szervezet IBF intézkedéseket tesz a biztonsági esemény vagy adott esetben az incidens elhárítására,
6. a súlyozási rend szerint magas és kritikus besorolású biztonsági eseménynél a szervezet IBF értesíti a megfelelő Hatóságokat a biztonsági eseményről, annak körülményeiről és a megtett intézkedésekről,
7. a szervezet IBF együttműködik az eljárásban résztvevő hatósággal és képviseli szervezet érdekeit, adott esetben átadja az érintett adatállomány az arra illetékesek számára,
8. a szervezet IBF felméri a károkat, összegzi a károk enyhítésére teendő intézkedéseket,
9. a szervezet IBF kivizsgálja az esemény körülményeit és levonja a következtetéseket, melynek keretében megelőző intézkedéseket fogalmaz meg a hasonló biztonsági események elkerülése érdekében,
10. a súlyozási rend szerint magas és kritikus besorolású biztonsági eseményről az eljárás végén a szervezet IBF elkészíti a jelentést és átadja a szervezet vezetőjének,
11. a szervezet IBF minden hónap utolsó munkanapján összefoglaló jelentést készít az adott hónap biztonsági eseményeiről.

### Az IBF feladatai a biztonsági esemény kezelése során

Amint az előzőekben is láttuk az IBF-nek rendkívül sok feladata van a szervezetnél, a szervezet képviselése során, és a biztonsági esemény kezelése során. Az alábbiakban rendszereztem ezen feladatokat:

- a nyilvántartásokból az érintett személy nevén lévő számítástechnikai eszközök listája,
- az érintett szerv postafiók (levelezés) mentése,
- az érintett számítógépben található adathordozók a mentése,
- mobil számítástechnikai eszközök mentése,
- mobil adathordozók mentése,
- a hálózati file szerver szervezeti közös meghajtójának a mentése,
- az érintett hálózati tárhelyeinek a mentése,
- az érintetthez köthető városi és szervezeti telefonszám híváslistája,
- az érintett szolgálati mobil telefon híváslistája,
- az érintett személy vagy szervezet, különböző rendszerekhez történő jogosultságainak feltalálása,
- az érintett személy által kezelt rendszerek naplói,
- az érintett személy által kezelt, iktatórendszerben rögzített irat állomány listája,
- és minden más, ami a biztonsági esemény vizsgálatához, illetve elhárításához szükséges.

Biztonsági esemény során a kárelhárítás, vagy intézkedés keretében az eljárásban érintett személy tekintetében az alábbi hozzáférések vagy jogosultságok felfüggesztéséről vagy megszüntetéséről gondoskodhat az IBF:

- hálózati hozzáférés,
- hálózati közös meghajtóhoz történő hozzáférés,
- levelezési postafiókhoz történő hozzáférés,
- különböző levelezési csoportokhoz történő hozzáférés,
- az érintett rendszerekhez történő hozzáférés,
- szolgálati mobiltelefon korlátozása,
- szervezeti és városi telefon korlátozása.

Az üzemeltető szervezet Biztonsági Vezetőjének feladatai az érintett szervezet IBF megkeresése alapján:

- a szervezet által biztosított felhasználói postafiók (levelezés) mentése és azok átadása, tiltása, felfüggesztése,
- az üzemeltett számítógép adathordozóinak a mentése és azok átadása,
- a szervezeten nyilvántartott mobil számítástechnikai eszközök mentése és azok átadása,
- a szervezet által nyilvántartott mobil adathordozók mentése és azok átadása,
- a hálózati file szerver szervezeti közös meghajtójának a mentése és azok átadása,
- az érintett személy vagy szervezet hálózati tárhelyeinek a mentése és azok átadása, tiltása, felfüggesztése,

- az érintett személyhez köthető városi és a szervezeti telefonszám, szolgálati mobiltelefon híváslistájának elkészítése és azok átadása, az eszközök használatának tiltása, felfüggesztése,
- az érintett személy az üzemeltett különböző rendszerekhez történő jogosultságainak feltalálása és azok átadása,
- az üzemeltett rendszerek tekintetében, az érintett személy által kezelt rendszerek naplójának mentése és azok átadása,
- minden elvégzett feladatról visszajelzés küldése,
- minden online vagy off line átadott adatállományhoz mellékelni kell valamely titkosított eljárással készített HASH lenyomatot.

Biztonsági Esemény Kezelése során az IBF-nek értesítenie kell az alábbi Hatóságokat

- NEIH - Nemzeti Elektronikus Információbiztonsági Hatóság
- NAIH - Nemzeti Adatvédelmi és Információszabadság Hatóság
- NKI - Nemzeti Kibervédelmi Intézet

Összefoglalva, a fenti elemzésben sorra vettem, hogy mit tekinthetünk biztonsági eseménynek, incidensnek és problémának. E három fogalom egymásból következtek. Ezen kifejezéseket próbáltam körülhatárolni, meghatározni.

Egyértelműen kitűnt az elemzésekből, hogy nem minden biztonsági esemény incidens. Bizonyos biztonsági események az általunk végzett vizsgálatok alapján lehetnek megvalósult incidensek, amelyek minden esetben intézkedést igényelnek, továbbá a legtöbb esetben károkozással járnak, vagy problémák, amelyek eseményt váltanak ki. Viszont azt is sikerült megállapítani, hogy minden incidenst valamilyen probléma okozza. A probléma egy vagy több incidens eredő oka is lehet.

Ha az incidenst okozó problémát megtaláltuk, akkor azt kezelni is kell. „A problémakezelés fő célja az incidensek hatásának minimalizálása. Reaktív módon a hiba okának megkeresésével foglalkozik és megelőző, proaktív módon az incidensek jövőbeni előfordulásának megakadályozását végzi.”[4] Tehát, egyértelművé vált, hogy az incidens és a probléma nem azonos fogalmak, egymásból következnek és igen szoros a kapcsolat közöttük. A problémának a feltárása és megoldása maga után vonzza azt a tényt is, hogy az incidenst megszüntettük, azaz a biztonsági eseményt kezeltük.

Annak érdekében, hogy a probléma többször ne jelenjen meg szervezetünknel és okozzon biztonsági eseményt létre kell hozni, a saját, illetve más szervezetek tapasztalásaiból egy tudásbázist, egy adattárat, melyben modellezzük a biztonsági esemény megjelenésétől a probléma megoldásán át a kárenyhítésig a teljes folyamatot. Így lehetőséget adunk saját magunk és azon szervezetek számára, akikkel ezen tudást megosztjuk, hogy időben észlelhessük és el is háríthassuk a fenyegető veszélyeket.

**Felhasznált Irodalom**

[1] Horváth Gergely Krisztián, CISA CISM: Közérthetően (nem csak) az IT biztonságról, Információ és IT biztonsági kultúra fejlesztése a közigazgatásban, KIFŰ, Széchenyi terv, Budapest, 2013, 1-2.

[2] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 9. pont

[3] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 10. pont

[4] ITIL - az informatikaszolgáltatás módszertana KFKI Számítástechnikai Rt Verzió: 3.1 2002. Széchenyi-terv, 10-15

**Feldolgozott irodalom**

- 2003. évi C. törvény az elektronikus hírközlésről
- 2010. évi CXLVII. törvény egyes rendészeti tárgyú és az azokkal összefüggő törvények módosításáról
- 222/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás működtetéséről
- 276/2006. (XII. 23.) Korm. rendelet a Közigazgatási és Elektronikus Közszolgáltatások Központi Hivatala létrehozásáról, feladatairól és hatásköréről
- 30/2011. (IX. 22.) BM rendelet a Rendőrség szolgálati szabályzatáról
- 346/2010. (XII. 28.) Korm. rendelet a kormányzati célú hálózatokról Köteles Bernadett (összeállította): A kormányzati intézmények informatikai stratégiájának készítése - A Közigazgatási Informatikai Bizottság 22/1. számú (2.0 verzió) ajánlása – 2009.
- Sebestyén Attila: Stációk és determinánsok a rendvédelmi szervek informatikai működésének fejlődésében - doktori (PhD) értekezés (28. oldal) - Zrínyi Miklós Nemzetvédelmi Egyetem, Egyetemi Könyvtár, Budapest - 2009.- p.17-28.
- Rajnai Zoltán - Mógor Tamásné: Elektronikus adatkezelő rendszerek kockázatelemzése, a kockázati módszerek bemutatása - Bolyai Szemle XXIII. évfolyam, 2014/2. szám - Nemzeti Közszerzői Egyetem - ISSN 1416-1443 - p.43-59.
- Pándi Erik: A magyar kormányzati távközlés egységesítésének hatása a rendvédelmi-katonai-, és közigazgatási kommunikációs rendszerek megszervezésére és irányítására - doktori (PhD) értekezés - Zrínyi Miklós Nemzetvédelmi Egyetem, Egyetemi

Könyvtár, Budapest - 2005. - p. 21-68.

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) Az Európai Unió Hivatalos Lapja, 2016.5.4., L 119/1-88pp.
- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről
- 2000. évi IV. törvény az információ biztonságáról szóló, Brüsszelben, 1997. március 6-án kelt NATO Megállapodás megerősítéséről és kihirdetéséről,
- 2011. évi CXII. tv az információs önrendelkezési jogról és az információszabadságról,
- 2003. évi C. tv. az elektronikus hírközlésről,
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról,
- a 301/2013. (VII. 29.) Korm. rendelet „a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról”,
- 233/2013. (VI. 30.) Korm. rendelet „az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről,
- 36/2013. (VII. 17.) BM rendelet „a zárt célú elektronikus információs rendszerek biztonságának felügyeletével és ellenőrzésével kapcsolatos ágazati szabályokról”,
- 77/2013. (XII. 19.) NFM rendelet az „állami és önkormányzati szervek elektronikus

információbiztonságáról szóló 2013. évi L. törvényben, illetve a módosításáról szóló 2015. évi CXXX. törvényben, meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről.

- 12/2012. BM utasítás a Belügyminisztérium Informatikai Stratégiájáról,
- 21/2011. BM utasítás a Belügyminisztérium Informatikai Biztonság Politikájáról,
- 94/2009. HM utasítása a honvédelmi tárca információbiztonság politikájáról,
- 23/2013. (V.17.) ORFK utasítást a belső adatvédelmi és adatbiztonsági szabályzatról,
- 45/2013. (XI.15.) ORFK utasítást az internethálózat működtetéséről, valamint az Internet és elektronikus levelezési rendszer Rendőrségi igénybevételének szabályairól.
- 25. számú Ajánlása Magyar Informatikai Biztonsági Ajánlások (MIBA),
- 25/1. Magyar Informatikai Biztonsági Keretrendszer (MIBIK),
- 25/1-3. kötet Az Informatikai Biztonság Irányításának Vizsgálata (IBIV),
- 25/1-1. kötet Informatikai Biztonság Irányítási Rendszer (IBIR),
- 25/2. Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma (MIBÉTS).
- ISO/IEC 27002:2005 és az ISO/IEC TR 13335 nemzetközi szabványok,
- ISO/IEC 27001:2005,
- ISO/IEC 27001:2013.
- a 185/2015. (VII. 13.) Korm. rendelet „a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenység vizsgálat lefolytatásának szabályairól”

TÓZSÉR ERZSÉBET<sup>3</sup>A PSZICHOLÓGIA SZEREPE  
A RENDŐRSÉGI SZERVEZETI KULTÚRÁBAN

A Rendőrség munkáját már a '80-as évek közepe óta segíti a pszichológia. Az első néhány pszichológus a bűnügyi vonalat erősítve, klinikai szaktudásukkal, helyi igényeknek megfelelően kerültek be a szervezetbe. Ekkor a rendőrökkel való pszichológiai, illetve pszichológusi munka nem képezte munkakörük szerves részét, ám fokozatosan a kezdetben csak személyes kapcsolatokon keresztül, az adott pszichológus önszorgalmából megvalósuló beszélgetések, foglalkozások révén egyre erősödő igény jelent meg arra, hogy ne csupán a rendőri munka segítségét végezzék el, de az állománnyal kapcsolatosan egyéb teendőket is végrehajtsanak. A pszichés gondoskodás fontosságának központi felismerése és törvényi szabályozása *a fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról szóló* 1996. évi XLIII. törvény 75. paragrafusában<sup>4</sup> jelent meg először. Ezt követte a 33/1997. IM-BM-TNM együttes rendelet, mely ötéves türelmi idővel írta elő a Rendőrségen ellátandó pszichológiai feladatokat. A szervek hathatós intézkedéseit megelőzően kiadásra került a 21/2000. (VIII.23.) IM-BM-TNM együttes rendelet *a fegyveres szervek hivatásos, közalkalmazotti és köztisztviselői állományának munkaköri egészségi, pszichikai és fizikai alkalmasságáról, a szolgálat-, illetve keresőképtelenség megállapításáról, valamint a belügyi egészségügyi szolgálat igénybevételéről*. Ebben részletesen szabályozásra kerültek az alkalmassági vizsgálatok és ez alapján hozták létre és töltötték fel az egyes szervezeti egységeknél a pszichológus státuszokat (Szabó, 2010).

Így került sor a Rendőrség Hivatalain belül az Egészségügyi Alosztályok megalakítására, melyeknek már része volt a pszichológiai alapellátás is. A Humánigazgatási Szolgálat alá 2008-ban került az Egészségügyi és Pszichológiai Alosztály, mely a későbbiekben a 2012-es „tipizálás” során csak a „nagy megyékben” maradt meg, a többi helyen csoporttá alakult. A jelenleg meglévő csoportok, vagy alosztályok szakmai vezetése az ORFK Személyügyi Főigazgatóság Egészségügyi Szakirányító és Hatósági Főosztályának vezetői révén történik. A pszichológusok szakmai koordinációjáért a szakirányító szakpszichológus a felelős, ugyanakkor a területi szervek szempontjából a munkahelyi vezetőjük vagy a csoportvezető/alosztályvezető, vagy pedig közvetlenül a humánigazgatási szolgálat vezetője, mivel az orvosokkal, fogorvosokkal, azok asszisztenseivel, illetve a pszichológusi asszisztensekkel mind egységesen tagozódnak be a megyei HISZ részlegébe.

A pszichológiai tevékenység jelenleg a Rendőrség, illetve a tágabb értelemben vett rendvédelem és honvédelem integráns része (Fridrich, 2015), amely vélhetően egyfajta

<sup>3</sup> PhD hallgató, Nemzeti Közszolgálati Egyetem, Rendészettudományi Doktori Iskola

<sup>4</sup> „A hivatásos állomány tagjának meg kell felelnie a miniszter által meghatározott, a beosztásának és életkorának megfelelő egészségi, pszichikai és fizikai alkalmassági követelményeknek. Az alkalmasság elérésének és szinten tartásának feltételeit a fegyveres szerv biztosítja.” (1996. évi XLIII. törvény 75.§)

reakció is arra vonatkozóan, hogy a dolgozóknak nem csupán a testi-, de a lelki egészségének védelme, ezáltal pedig a hatékonyság elősegítése és az ilyen értelemben vett biztonságos munkafeltételek megteremtése is a szervezet feladatát képezi (Futóné Kartai, Vizinger és András, 2009; Malét-Szabó és Szatmári, 2012; Szatmári, 2013).

A 21/2000. (VIII.23.) IM-BM-TNM együttes rendelet csaknem egy évtizeden keresztül volt meghatározó az alapellátói pszichológiai munkában, egészen az 57/2009. (X. 30.) IRM-ÖM-PTNM együttes rendelet megjelenéséig, amely napjainkig hatályos (bár köztudott, hogy modernizálásán a Belügyminisztérium Egészségügyi Koordinációs Osztálya nagy erővel dolgozik, kikérve és beépítve a területen dolgozó szakemberek véleményét és javaslatait).

Belső szabályzóként 2009-ben megjelent a pszichológiai szakterület által elkészített legelső protokoll (Virág, 2009), mely az összes felmerülő feladatkört igyekezett keretbe foglalni. Fő célkitűzés a pszichológus szakmai munka szakszerűsítésén, egységesítésén túl, a hétköznapi feladatok végrehajtásának tudományos szintre emelése, a pszichológia tudományának gyakorlati felhasználásának facilitálása és egy szervezeti és egyéni igényekre reagáló szolgáltatói pszichológiai szakterület kialakítása voltak, és nem elhanyagolható módon a vezetői állomány tájékoztatása a szakterület alkalmazási területeiről és módszereiről (Virág és Vajger, 2009). Nagyon hasonló céllal jött létre 2014-ben szintén a szakterületen dolgozó szakemberek tollából a parancsnoki állománynak szánt „kézikönyv”, mely egyben a pszichológiai szakterület munkájának szélesebb körű ismertetését és lehetőségeit is ismertetni kívánta (Szeles, 2014a).

A rendvédelemben, illetve a rendőrségen dolgozó pszichológusok feladatait a hatályos protokollok (Szeles, 2016), a vonatkozó jogszabályok és a mindenkor érvényes pszichológusi etika szabályozza. A rendőrségi pszichológiai munkát öt fő tevékenységi területre (Szeles, 2015) lehet csoportosítani:

1. az alkalmassági vizsgálatok
2. a mentálhigiénés ellátás
3. a képzések
4. a rendőr szakmai feladatokat támogató pszichológiai tevékenységek
5. a szervezetfejlesztés és szervezetpszichológiai vizsgálatok

Az (1.) **alkalmassági vizsgálatok** végzéséhez soroljuk a hivatásos állományba vételt megelőző, a rendészeti tanintézetbe történő felvétel előtti, beosztás változást megelőző, közlekedépszichológiai, illetve a kétévente esedékes időszakos pszichikai alkalmassági vizsgálatokat, valamint meghatározott esetekben soron kívüli vizsgálatokat.

A (2.) **mentálhigiénés ellátás** az egyszerű tanácsadástól akár a terápiás jellegű gondozási tevékenységig is mélyülhet, a problémától, valamint a szakember képzettségétől és kompetenciáitól függően. De ide sorolható a pszichés egyensúlyvesztések korai felismerése esetén adekvát ellátórendszerbe irányítás, a rendkívüli események prevenciója, és kezelése, az egyéni és csoportos krízisintervenció, az utánkövetés és az utógondozás. 2014-ben a rendkívüli események kezeléséhez is készült útmutató a szakterületi vezetés részéről (Szeles, 2014b).

A (3.) **képzések** tekintetében két fő területtel kell számoljunk. Az egyik a (a.) **tréningek** tartása, amelyek a sztrész- és konfliktus-kezeléstől, a kommunikáció- és önismereti fejlesztésen át, a csapatépítő foglalkozásokig változatos képet mutatnak. A másik a

(b.) szakmai képzésekhez kapcsolódó pszichológiai témájú előadások, mint pl. az intézkedés lélektan.

A (4.) **rendőr szakmai feladatokat támogató** pszichológiai tevékenységek több alterületre sorolhatóak be. A rendőrségi fogdák és őrzött szállások ellátása speciális terület, a rendőrségi fogdán és az őrzött szállásokon fogvatartottak pszichológiai ellátásáról készült protokoll (Csizmadia et. al., 2012) szabályozza a pszichológus ilyen jellegű tevékenységét, amely leginkább krízisintervenciós beavatkozást jelent. A csapaterős tevékenység pszichológiai támogatására és a katasztrófa-helyzetek és különleges jogrend időszakában során végzendő pszichológiai feladatokra jó példa a migrációs válsághelyzet idején a szakterület munkatársai által végzett feladatellátás (Borbély, Farkas és Tózsér, 2017; Borbély, Fridrich és Tózsér, 2018), mely végrehajtására az ORFK külön feladattervet készített Szeles E. (2015b). A nyomozati és bűnmegelőzési munka támogatása, illetve a rendészeti feladatellátás támogatása feladatok szempontjából nagyon színesek lehetnek, akár szaktanácsadóként van jelen egy-egy kihallgatáson, vagy éppen a kihallgatás pszichológiai aspektusairól tart képzést, előadást az érintett állomány számára (Farkas, 2017).

A (5.) **szervezetfejlesztési** feladatok közé tartoznak a különböző felmérések elkészítései a felmerülő vezetői kérdések alapján, vagy egy adott időszak alatt felmerülő tendenciák alapján a szükséges jelentések megtétele, esetleges javaslattevés a vezetők számára (Malét-Szabó és Szatmári, 2012). Ezen területen különösen nagy felelősség hárul a pszichológusra, mivel ez az a terület, amely révén a szervezet egészére közvetlen is hatást gyakorolhat. Egyben elmondhatjuk azt is, hogy a szervezetfejlesztéssel kapcsolatos feladatok óhatatlanul hatást gyakorolnak a szervezeti kultúra egészére is.

A szervezeti kultúra minden szervezet esetében egyedi, az adott szervezet tagjai által létrehozott és fenntartott jelenség, mely a tagok által vallott értékek és hiedelmek, illetve normák és szabályok szövevényes rendszere. Ez a Rendőrségen egy nagyon speciális foglalkozási kultúrába ágyazottan jelenik meg, melynek sajátosságai áthatnak mindent a szervezeten belül (Kovács, 2009, Finszter, 2016).

A szervezet – amely a társadalomban is egy különleges pozíciót és feladatkört képvisel – bizonyos sajátosságai (mint például a jellegéből adódó, szigorú hierarchia és parancsuralmi rendszer, vagy az uniformizáltság, illetve a specifikus hivatás együttesen) egy szükségszerűen sajátos szervezeti kultúrát teremtenek. Ennek fontos eleme a konzervativizmus (Finszter, 2003) és az állandóság (Finszter, 2013) – ezt a „rendőr”, mint foglalkozás is tükrözi, hiszen igen stabil munkaként tekintenek rá, amelyre mindig is szükség volt és mindig szükség lesz. Ugyanakkor a rendőrséggel foglalkozó szakirodalmak alapján megjelenik a tartózkodás, bizalmatlanság (Csányi, 2008; Bali, 2011), valamint a gyanakvás (Finszter, 2003; Paoline, 2003) is. Ennek oka talán a fentebb már említett sajátos feladatellátásban keresendő, amely bizonyos értelemben fekete-fehér gondolkodásmódot kényszerít ki. Összességében tény, hogy a szervezeti kultúra ezen jellemzői nehezítik a szervezetpszichológia működtetését a hétköznapi alapellátó pszichológusi gyakorlatban.

Ennek ellenére – talán a vezetői képzések pozitív hatásaiból következően is – a modern vezetők egyre inkább igénylik a szervezetfejlesztést a pszichológiai szakterületek részéről. Előfordul, hogy csak egy-egy szervezeti egység esetében észlelt probléma hátterének feltárására kéri fel a szakterületet, illetve azzal kapcsolatos megoldási javaslatot várnak a pszichológustól. 2009-ben, pályafutásom elején, az állományilletékes parancsnok a szervezeti egységek közötti fluktuációbeli és hangulati eltérések hátterére kereste a választ. Így lett lehetőségem egy egész megyét érintő elégedettség-felmérés elvégzésére, és ezzel

párhuzamosan a vezetők vezetői stílusának és attitűdjének vizsgálatára. Az elégedettség-felmérés megmutatta a különbségeket a „problémásnak” ítélt szervezeti egységek és a többi között, és az is jól kimutatható volt, hogy nem a fizikai vagy anyagi tényezők befolyásolták azt, sokkal nagyobb szerepet játszottak a „szociális” tényezők, vagyis a kapcsolatok – a közvetlen vezetővel és a munkatársakkal való kapcsolat (Kovács és Tózsér, 2017).

Ez a vizsgálat erősítette meg bennem, hogy a szervezeti kultúra alakítása kulcsfontosságú feladatunk a szervezetfejlesztés során, és a Nemzeti Közszerológiai Egyetem Rendészettudományi Doktori Iskolájába jelentkezéskor ezért választottam kutatási témámnak a rendészeti szervezeti kultúrát. Az is egyértelművé vált ugyanakkor, hogy egyetlen vizsgálattal, vagy célzott beavatkozással még nem változtatjuk meg alapjaiban a szervezetet – ez nem feladatunk és természetesen nem is célunk. Ugyanakkor a pszichológia tudománya, ha lehetőséget kap rá, olyan rezdülésekre, olyan összefüggésekre hívhatja fel a figyelmet, amelyek messze nem magától értetődőek, és amelyek a mindennapokra jelentős hatással bírnak. A szervezetfejlesztési eszközök segítségével, a szervezeti kultúra kutatásával a vezetők számára olyan, a szervezet számukra láthatatlan aspektusairól jelezhet vissza a pszichológiai szakterület, mely fontos információ lehet számukra döntéseik meghozatala előtt, és melyre csak a legérettebb és legelkötelezettebb vezetők nyitottak (Horváth, 2014). Magyarországon azonban viszonylag szűk a szakirodalma ennek a témakörnek, tehát a rendészeti szerveknél zajló szervezetfejlesztési vizsgálatok szélesebb körben való publikálását érdemes lehet facilitálnia szakmánknak.

A szervezeti kultúra vizsgálata és alakítása a leghatékonyabb belső eszköz, illetve lehetőség a szervezet stratégiai céljainak eléréséhez, valamint ahhoz, hogy a szervezet tagjait a szükséges gondolkodás-, és cselekvésmódokra hangoljuk rá – olyan szemléletet adjunk nekik, amely a mindennapok szintjén bír pozitív értelemben vett újító hatással. Egy olyan szervezet esetében, mint a Rendőrség, mely alapvetően a közjót szolgálja, egy megfelelő, erős szervezeti kultúra megléte és fejlesztése alapvető társadalmi érdeke minden állampolgárnak, hiszen a szervezeti kultúra hatással van a szervezet presztízsére, a szervezet tagjainak elégedettségére és a szervezettel való azonosulásukra is (Bakacsi, 1996).

Éppen ezért releváns az olyan nagy egységek vizsgálata, mint amilyen egy megyei rendőr-főkapitányság. A célzott kutatás mind a megyei, mind pedig az országos szervezet szintjén is szerencsésen érdeklődésre és támogatásra talált, így alakulhatott meg egy kutatócsoport a Nemzeti Közszerológiai Egyetemen az „Egy megyei rendőr-főkapitányság szervezeti kultúrájának vizsgálata” címmel 2016 őszén (Tózsér, Fridrich és Borbély, 2018). A kutatócsoport az egy éves időtartamra tervezett munkáját 2017. június 1-én kezdhette meg. Kutatócsoportunk célkitűzése a megye szervezeti kultúrájának átfogó feltérképezése, kvantitatív és kvalitatív módszerek alkalmazásával. A vizsgálat egész megyére kiterjedő meghirdetése után a csoport által kialakított szervezeti kultúra kérdőívek kitöltésére biztosítottunk lehetőséget.

Összességében az előzetes adatok alapján 269 db megfelelően kitöltött kérdőív érkezett vissza – s ez alapján elmondhatjuk, hogy reprezentatív, nagy elemszámú minta révén fogunk releváns eredményekhez jutni, amelyekről nem túlzás azt feltételezni, hogy az országos átlagra vonatkozóan is levonhatunk következtetéseket. Természetesen az adatok nagysága miatt a kapott kérdőívek feldolgozása jelenleg is folyamatban van. A kutatócsoportunk szervezettől független tagjai strukturált interjúkat készítettek a megye vezetőivel, melyek feldolgozása ugyancsak zajlik aktuálisan is. Reményeink szerint az adatok feldolgozását követően olyan megfontolásokat és javaslatokat leszünk képesek megfogalmazni helyi és országos viszonylatban is, amellyel a szervezet és a benne dolgozó

egyének javát egyaránt szolgálni leszünk képesek, és egyben kielégítő választ tudunk adni a vezetők által megfogalmazott kérdésekre is.

A rendőrségi pszichológiai szakterületnek rendkívül nagy a felelőssége a szervezetpszichológiai elemzések során – a kapott eredmények megfelelő interpretálása, és a szakterületi javaslatok megfogalmazása meghatározóak lehetnek a szervezet jövőjére nézve. Izgalmas kihívás ez, amely ugyanakkor gondos odafigyelést igényel. Ám a kutatás adatfelvétele során tapasztaltak miatt fontos, hogy a pszichológia szervezetben betöltött, szervezeti kultúra-alakító hatásáról – ha csak röviden is –, de értekezzek, mivel a nyílt véleménynyilvánítás elől alapvetően elzárkózni hajlamos, bizalmatlan és konzervatív szervezetben körülbelül 30%-os válaszadási arányt sikerült elérni egy viszonylag rövid határidő alatt, vélhetően a pszichológiai szakterület korábbi szervezfejlesztési tevékenységének is köszönhető. A magam részéről a szakterület irányába mutatott bizalomként könyveltem el, és a kutatócsoporttal igyekszünk ezt központilag is hasznosítható eredményekkel meghálálni.

Az ORFK 2016-os intézkedése révén a pszichológiai szakterületet megerősítették, vagyis kibővítették a szakterületen dolgozó személyek létszámát, és a szakterület munkafeltételeinek javítására is központi intézkedések történtek. Mindez vélelmezhetően azt mutatja, hogy a szervezet is felismerte a pszichológia tudományában rejlő lehetőségeket – és ebben igen nagy szerep hárult a szakirányításra.

A szakirányítás alapvető törekvése az, hogy minden szervnél szakmailag magasan kvalifikált, egyúttal gyakorlatias tapasztalatokkal rendelkező, szervezet iránt elkötelezett kollégák dolgozzanak. Ezen törekvést szolgálja az is, hogy a pszichológusok számára előre tervezetten, negyed évente esetmegbeszélő munkaértekezletek kerülnek megtartásra, ahol lehetősége van a kollégáknak egymástól tanulni, illetve a gyakorlatban problémásnak talált helyzetekről a szakirányítás révén közös álláspontot kialakítani. Mindez fontos a pszichológusok közti személyes kapcsolatok kialakításának támogatása szempontjából is – elvégre egy újonnan a szervezetbe érkező kollégának hamar alkalmat kínál arra, hogy megismerje pszichológus kollégáit, a hosszabb ideje a szervezetben dolgozók pedig átadhatják tapasztalataikat, és így a közös gondolkodásra is megnyílik az út. A pszichológusok szakmai felkészültségét erősítendő a szakirányítás ugyancsak támogatja a szakképzettség megszerzését, illetve a módszerspecifikus továbbképzéseken való részvételt is. Ugyancsak ennek jegyében a Nemzeti Közsolgálati Egyetemen a Rendészettudományi Doktori Iskola több rendőrségi pszichológus doktorandusz hallgatónak teremt lehetőséget szakmai munkájuk tudományos szintre emelésére, kutatásuk megvalósítására és tudományos fokozat szerzésére. Mindezekon felül az ORFK közreműködik a Belügyminisztérium tehetséggondozási programjának keretein belül létrejött gyakornoki programban is – ebből a pszichológiai szakirányítás is komoly részt vállal a tudományos munkát segítőben.

Ugyanakkor nem tagadható le az sem, hogy a személyes tapasztalat, a pszichológusra közvetlenül rábízott állomány ismerete alapvető fontosságú – elvégre az állandó szakember jelenléte, aki kongruensen képvisel egy adott szakterületet – egyfajta biztonságot is ad. Egyúttal az állandóság, a „kipróbáltság” az, amely révén egy alapvetően bizalmatlan (Szabó, 2010), gyanakvással terhes (Finszter, 2003; Paoline, 2003), konzervatív (Finszter, 2003) és állandóságot (Finszter, 2013) mutató szervezeti légkörben kialakítható a pszichológia, mint újdonság, irányába vetett bizalom.

A pszichológus ilyen értelemben maga is egyetlen személyben képviseli hivatásának egészét – akárcsak az egyetlen rendőr a testület egészét -, következésként csak akkor tud

hitelesen tenni a szervezet pozitív irányába történő változtatásáért, ha szakmai kompetenciájának birtokában, kongruensen képviseli a szakmai szempontokat és meglátásokat.

## Felhasznált irodalom

1996. évi XLIII. törvény - *A fegyveres szervek hivatásos állományú tagjainak szolgálati viszonyáról*

33/1997. (V. 13.) BM-IM-TNM együttes rendelet - *A fegyveres szervek hivatásos és szerződéses állományának egészségi, pszichikai és fizikai alkalmassága, az ideiglenes szolgálat-, keresőképtelenség, illetve az állomány megváltozott egészségi állapotú tagjai egészségügyi felülvizsgálatának elbírálásáról és a belügyi egészségügyi intézmények igénybevételéről*

21/2000. (VIII. 23.) IM-BM-TNM együttes rendelet - *A fegyveres szervek hivatásos, közalkalmazotti és köztisztviselői állományának munkaköri egészségi, pszichikai és fizikai alkalmasságáról, a szolgálat-, illetve keresőképtelenség megállapításáról, valamint a belügyi egészségügyi szolgálat igénybevételéről*

57/2009. (X. 30.) IRM-ÖM-PTNM együttes rendelet – *Az egyes rendvédelmi szervek hivatásos állományú tagjai egészségi, pszichikai és fizikai alkalmasságáról, közalkalmazottai és köztisztviselői munkaköri egészségi alkalmasságáról, a szolgálat-, illetve keresőképtelenség megállapításáról, valamint az egészségügyi alapellátásról*

Bakacsi Gy. (1996). *Szervezeti magatartás és vezetés*. Budapest, Közgazdasági és Jogi Könyvkiadó

Bali M. (2011). A rendőrkép és a rendőrségkép. *Magyar Rendészet, (XI.) 2*, 13-33.

Borbély Zs., Farkas J. és Tózsér E. (2017): A tömeges méretű illegális migráció pszichés következményei a rendészeti feladatellátás során. *Hadtudományi Szemle, X. évfolyam, 3. szám.*, 288-304.

Borbély Zs., Fridrich A. C. és Tózsér E. (2018): Az ideiglenes biztonsági határzár menti feladatellátás hatása a határzár védők magánéletére. *Honvédség és társadalom konferencia – tanulmánykötet (megjelenés alatt)*

Csányi Cs. (2008). A rendőrség morális „válságának” értelmezése. *Rendészeti Szemle, (56) 1*, 89-95.

Csizmadia É., Erdélyi Sz., Szeles E., Hajdú N., Nagy T., és Balogh J. T. (2012) *Módszertani útmutató – a rendőrségi fogdákon és az őrzöttszállításokon fogvatartott személyek egészségügyi és pszichológiai ellátásához*. ORFK Humánigazgatási Szolgálat Egészségügyi Szakirányító és Hatósági Főosztály, Budapest

Farkas J. (2017): Psychological Assessment of Children by Forensic Experts. *Ünnepi kötet dr. Zakar András c. egyetemi tanár 70. születésnapjára. Acta Universitatis Szegediensis. Acta Juridica et Politica; Tom. 80*. Szeged, Szegedi Tudományegyetem Állam- és Jogtudományi Kar, 55-64.

Finszter G. (2003). A rendőrség elmélete és a kormányzat gyakorlata. *Belügyi Szemle, (1)*, 91-110.

Finszter, G. (2013). A változó rendészet és a rendészettudomány. *Pécsi Határőr Tudományos Közlemények, XIV*, 5-12.

Finszter G. (2016): *A rendészet és a rendészeti igazgatás elmélete*, egyetemi jegyzet, Nemzeti Közsolgálati Egyetem, Budapest

Fridrich A. C. (2015) *Az eltérő szakterületen dolgozó rendőrök teszteredményeinek vizsgálata – Hasonlóságok és különbségek az RMSK tükrében*. ELTE PPK TPI, Budapest

Futóné Kartai Zs., Vizinger E. és András Zs. (2009). *Lelki egészségvédelem a kulturált rendészetért. Pécsi Határőr Tudományos Közlemények, X, 257-264.*

Horváth J. (2014): A rendészeti szerveknél elvárt vezetői magatartás. In: szerk. Horváth József – Kovács Gábor: *A rendészeti szervek vezetés- és szervezésmélete*, Nemzeti Közszolgálati Egyetem, Budapest, 133–158.

Kovács G. (2009): A rendészeti szervek szervezeti kultúrájának összetevői és sajátosságai, a téma feldolgozása a Rendőrtiszti Főiskola vezetésméleti oktatásában. *Pécsi Határőr Tudományos Közlemények, X, 223-234.*

Kovács G. és Tózsér E. (2017): A vezetői attitűdök, vezetői stílusok és a dolgozói elégedettség összefüggéseinek vizsgálata egy megyei rendőr-főkapitányságon. *Pro Publico Bono – Magyar Közigazgatás, 2. szám, 138-157.*

Malét-Szabó E. és Szatmári A. (2012). A rendőr lelki biztonsága – avagy a biztonság megőrzésének egyik alappillére a rendőr lelki biztonsága. *Pécsi Határőr Tudományos Közlemények, XIII, 399-412.*

Paoline, E. A. (2003). Taking stock: Toward a richer understanding of police culture. *Journal of Criminal Justice, 31, 199– 214.*

Szabó E. (2010): *A munkahelyi egészségpszichológia és egészségfejlesztés rendszere a Magyar Köztársaság Rendőrségén, valamint a szubjektíve észlelt munkahelyi stresszterheltség jellegzetességei – különös tekintettel az idői tényezőre – a hivatásos állományú rendőrök körében*. Doktori értekezés, Debreceni Egyetem.

Szatmári A. (2013). A problémamegoldás pszichés szempontú vizsgálata, mint alkalmassági kritérium. *Pécsi Határőr Tudományos Közlemények, XIV. 151-160.*

Szeles E. (szerk.) (2014a) *Kézikönyv a vezetői/ parancsnoki állomány számára a pszichológiai szakterület munkaformáinak megismerésére, az állománnyal való bánásmód hatékonyságának növelésére* ORFK Humánigazgatási Szolgálat Egészségügyi Szakirányító és Hatósági Főosztály, Budapest

Szeles E. (2014b) *A rendkívüli események kezelésének pszichológiai protokollja*. ORFK Humánigazgatási Szolgálat Egészségügyi Szakirányító és Hatósági Főosztály, Budapest

Szeles E. (2015a) *Pszichológiai tevékenység a Rendőrségen (belső anyag)*

Szeles E. (2015b) *Feladatterv – A migrációval kapcsolatos feladatok végrehajtására vezényelt állomány pszichésstabilitásának megőrzésére, valamint az akut és poszttraumás stressz betegség kialakulásának megelőzése érdekében*. ORFK Humánigazgatási Szolgálat Egészségügyi Szakirányító és Hatósági Főosztály, Budapest

Szeles E. (2016) *Módszertani útmutató – a Rendőrségnél végzett pszichikai alkalmassági vizsgálatok és az ahhoz kapcsolódó gondozási tevékenység szakmai protokollja*. ORFK Személyügyi Főigazgatóság Egészségügyi Szakirányító és Hatósági Főosztály, Budapest

Tózsér E., Fridrich A. C. és Borbély Zs. (2018) *Ügyfélszolgálati szemlélet a szervezeti kultúrában*. II. Turizmus és biztonság konferencia kiadványkötet (megjelenés alatt)

Virág L. (szerk.) (2009) *A rendvédelmi pszichológiai tevékenység szakmai protokollja*  
Rendőrség Tudományos, Technológiai és Innovációs Tanács, Budapest

Virág L. és Vajger É. (2009) Paradigmaváltás – a rendvédelmi pszichológiai tevékenység szakmai protokollja, mint a szervezeti kultúra egy lehetséges formálója. *Pécsi Határőr Tudományos Közlemények*, X, 245-249.