Illéssy Miklós – Nemeslaki András – Som Zoltán

# Elektronikus információbiztonság-tudatosság a magyar közigazgatásban

## Bevezetés

Magyarország Országgyűlése 2013. április 15-én elfogadta az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényt (a továbbiakban információbiztonsági törvény, Ibtv.), amely kiemelkedő csúcspontja annak az összetett kormányzati stratégiának, amely szerint a magyar állam kezelni kívánja azokat a modern kihívásokat és fenyegetéseket, amelyeket az egyre jobban elterjedő digitális infrastruktúra és a kibertér jelent. A nemzetközi trendek is alátámasztják, hogy az információbiztonság nem csak technológiai (melyet több magyar egyetemen, illetve képzőhelyen kiválóan tanítanak), hanem elsősorban szervezetirányítási kérdés erős jogi-közigazgatási fókusszal. Éppen ezért az Ibtv. számos képzési követelményt határoz meg a törvény hatálya alá tartozó vezetőkkel és az elektronikus információs rendszerek biztonságáért felelős személyekkel szemben.

Az információbiztonság multidiszciplináris szemléletű megközelítése speciális vezetőképzési programok kidolgozását igényli, amelyek a résztvevőket megismertetik a munkájuk során felmerülő jogi, igazgatási, biztonsági, minőségi, vezetési alapokkal, valamint képessé teszi őket az előírt kockázatértékelések elvégzésére, eszközöket ad nekik biztonsági rendszereket irányítani, képessé teszi őket a felmerülő incidensek kezelésére. Mindezek mellett, a felelős személyek munkája kudarcra ítélt, ha nem tudják vezető társaikat, kollégáikat és beosztottaikat segíteni abban, hogy együttesen alakítsák ki az információs társadalom kihívásainak megfelelő szervezeti kultúrát, szemléletet és munkastílust.

Tanulmányunk ehhez a problémakörhöz kapcsolódik oly módon, hogy eredményeivel az elektronikus információrendszerek biztonságával kapcsolatos képzésfejlesztéshez járuljon hozzá, amelyet az AROP 2.2.19 projektben kialakított eTanulás Módszertani Központ végez eLearning anyagok előkészítése és gyártása formájában számos egyetem részvételével. Dolgozatunkban a magyar közigazgatás információbiztonsággal kapcsolatos tudatosságát térképeztük fel két módszertannal a) egy szakértői interjú sorozattal, és b) egy köztisztviselői kérdőíves megkérdezéssel, amelyet leíró statisztikai módszerekkel elemeztünk. A kutatás eredeti célkitűzése konkrét ajánlatok és javaslatok megfogalmazása volt megbízóinktól a képzés fejlesztők felé, amely ajánlások az AROP 2.2.17. Humánerőforrás fejlesztési program keretében kerültek dokumentálásra és prezentálásra.

Kutatási jelentésünknek ez a változata az általános eredményeket, a kutatók és oktatók számára hasznosítható információkat, a vizsgálatok továbbfejlesztésének irányait és természetesen a gyakorló szakemberek és átlagos informatikai felhasználók számára tanulságos következtetéseket foglalja össze. Felépítése öt szakaszra tagozódik az alábbi szerkezetben.

A bevezető után a kutatás koncepcionális és elméleti hátterét, majd a konkrét kutatási kérdéseket foglalja össze. A második pontban az információbiztonság szabályozási és stratégiai helyzetét mutatjuk be Magyarországon, kiemelve a miniszteri rendelet szintjén szabályozott képzési struktúrát a résztvevők, információbiztonsági vezetők és szervezeti vezetők vonatkozásában. Az ezt követő pontban a szakértői interjúk eredményeit foglaljuk össze 15 interjú alapján, amelyeket a magyar közigazgatás különböző érintettjeivel és szintjein folytattunk. A negyedik szakaszban azt az on-line kérdőívet elemezzük leíró statisztikai és néhány egyszerűbb összefüggés vizsgálattal, amit közel 300 köztisztviselő töltött ki önkéntes alapon. Végül a záró ötödik fejezetbe összegezzük következtetéseinket, és javaslatot teszünk a kutatás kiterjesztésére illetve a magyar közszolgálat információbiztonság-tudatosságának összetettebb megismerésére.

## Elméleti háttér és kutatási kérdések

Kutatásunk kiindulópontja Magyarország információbiztonságának meghatározó koncepcionális dokumentuma a kiberbiztonság részletes kifejtését tartalmazó „Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat” (kihirdetve: Magyar Közlöny 2013. évi 47. szám), a továbbiakban Stratégia. A Stratégia célja „a szabad és biztonságos kibertér kialakítása és a nemzeti szuverenitás védelme”. Ezen belül a stratégia kiemeli, hogy a magyar kibertér, mint a gazdasági és társadalmi élet meghatározó területe, egyszerre legyen szabad, biztonságos és innovatív.

A Stratégia a magyar kiberteret a globálisan összekapcsolt információs rendszerek azon részeként definiálja, amelyekben a keletkező adatok és információk vonatkozásában Magyarország valamilyen formában érintett. A Stratégia részletesen leírja azokat a célokat, irányokat, feladatokat és eszközöket, amelyeken keresztül a magyar kormányzat biztosíthatja a magyar kibertér védelmét, a technológiai innovációk adaptálását és a szorosabb nemzetközi együttműködést. Az egész stratégia egyik legfontosabb üzenete a megelőzés, az oktatás és képzés, valamint a biztonsággal kapcsolatos tudatosság fontosságának hangsúlyozása, mely az egész dokumentumban visszatérő elem.

Kutatásunk ebbe a környezetbe ágyazódik, és annak a kérdéskörnek az alátámasztását tűzi ki célul, amely szerint a Kiberstratégia és az azt követő rendelkezések végrehajtása nagymértékben a kormányzati szervezetek humán erőforrásainak ismereteitől, motivációjától, képességeitől függ. Ezek a tényezők meghatározó elemei az ún. biztonsági megfelelőségnek (security complience), amely alapvetően biztosítja a biztonságpolitika hatékony működését, esetünkben különös tekintettel annak információbiztonsági területén.

A tapasztalatok és a legújabb elméleti kutatások szerint ugyanakkor bizonyítható összefüggés van a biztonsági megfelelőség és a biztonságtudatosság (security awareness) között, azaz abban, hogy a munkavállalók/köztisztviselők/kormánytisztviselők motivá-

cióját, információbiztonsági megfelelőségét úgy lehet növelni, ha rendszeres keretek között fejlesztjük biztonságtudatosságukat, mind a technológia, mind a szervezet működése vonatkozásában (Bulgurcu et.al., 2010).

Mivel olyan adatok nem állnak rendelkezésünkre, amelyek alapján meg tudnánk határozni a magyar közszolgálat biztonságtudatossági szintjét, ezért kutatási kérdésünk rendkívül egyszerű: annak az alapvető ismeretkörnek a feltárása és azonosítása, amelyek a magyar közszolgálat alkalmazottainak információbiztonsággal kapcsolatos tudatosságát jellemzik. Pragmatikus szempontból a kutatás a képzésfejlesztésre összpontosít azért, hogy a kapott eredmények alapján tudatosságfejlesztést biztosító programokat lehessen indítani. Feltáró jelleggel tehát olyan empirikus kutatássorozat megindítását kezdjük meg ezzel a tanulmányunkkal, amely lehetővé teszi a magyar közszolgálat információtudatossági megfelelőségének folyamatos felmérését, fejlődési irányainak kijelölését, annak nyomon követését.

Kutatásunk középpontjában tehát az információbiztonság tudatosság és a köztisztviselő áll. Természetesen közelítésünk és eredményeink kiterjeszthetők a kormányzati szerveken kívül is a tágabb közalkalmazotti, vállalati illetve akár vállalkozói vagy magán szférákra is azok sajátosságainak figyelembevételével.

Az információbiztonság-tudatosságot (IBT) vizsgálatunk kérdéseinek összeállításához úgy definiáljuk, mint a munkavállaló általános ismereteinek és attitűdjének halmazát az információrendszerek használatával kapcsolatban úgy, ahogy azt a szervezeti környezetében értelmezi (Bulgurcu et. al., 2010, 532). Az IBT ebben a vonatkozásban két fő területből áll, egyrészt az általános szintű információbiztonsággal kapcsolatos tájékozottságból, másrészt az információbiztonsági szabályozások és stratégiák ismeretéből.

Az IBT fejlesztése azoknak az akadályozó tényezőknek az eltávolításával valósítható meg, amelyek annak elsajátításának és elmélyítésének útjában állnak. Ilyenek például az IKT felhasználói készségek, általános biztonsági ismeretek, a szervezeti költségvetési korlátok, vagy a különböző felelősségi körökben való tájékozottság (Knapp et. al., 2012). A szakmai körökben keringő történetek és empirikus vizsgálatok is abba az irányba mutatnak, hogy sem a szabályzatok önmagukban, sem az IBT-vel kapcsolatos kampány-szerű figyelemfelhívások nem eredményeznek tartós és lényeges javulást ezen a területen (Knapp et. al, 2012; Burgulcu. et al., 2010), ezért érvelünk amellett, hogy az IBT összetevőinek és mozgatóinak ismerete a Stratégia és az abból származó törvényi szabályozás végrehajtásának kulcseleme.

## Az elektronikus információbiztonság stratégiai szerepe és jogszabályi háttere

A Kormány e-kormányzati stratégiájában kiemelt szerepet szánt a nemzetbiztonság és ezen belül is a kibervédelem szempontjainak. Ebbéli szándékának megfelelő törvényi háttért is teremtett, mely figyelemreméltó szisztematikussággal alapozza meg e szempontok érvényesülését. Elsőként a „Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozatot" fogadták el, amelynek 31. pontja szól a kiberbiztonságról (kihirdetve: Magyar Közlöny 2012. évi 19. szám). Ezt követte a kiber-

biztonság részletesebb kifejtését tartalmazó dokumentum, a „Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat" (kihirdetve: Magyar Közlöny 2013. évi 47. szám). E stratégiai dokumentumok kimunkálását és elfogadását követte az első jogalkotási lépés, „Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény" (a továbbiakban: Ibtv.) elfogadása (kihirdetve: Magyar Közlöny 2013. évi 69. szám). A törvényben meghatározott célok és feladatok végrehajtását részterületenként határozta meg még részletesebben egy sor rendelet, melyek közül témánk szempontjából a legfontosabb, „Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet" (kihirdetve: Magyar Közlöny 2013. évi 173. szám).

Az előző szakaszban bemutattuk a Kiberstratégia oktatással kapcsolatos irányelveit, hangsúlyoznunk kell ugyanakkor, hogy természetesen a közigazgatást és az e-kormányzati rendszereket is, mint a kibervédelem elsődleges prioritással rendelkező területeit említi a dokumentum:

> „Magyarország kiemelt figyelmet fordít arra, hogy az általános, a közép- és felsőoktatásban, a kormányzati tisztviselők képzésében és a szakmai továbbképzéseken a kiberbiztonság szakterülete integrálódjon az informatikai oktatásba. Magyarország stratégiai együttműködés kialakítására törekszik azon egyetemi és tudományos kutatóhelyekkel, melyek a kiberbiztonsági kutatás-fejlesztésben kiemelkedő és nemzetközileg is elismert eredményeket mutatnak fel, és segítik a kiberbiztonsági kiválósági központok kialakulását – fogalmaz a Stratégia".

A Kiberbiztonsági Stratégiában elfogadott célok és elvek mentén született meg Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.), amely a közigazgatás szinte minden szintjén új feladatokat határozott meg. A törvény alapvető célja a „nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonságának" védelme. A törvény, miután tisztázta a kiberbiztonsággal kapcsolatos legfontosabb fogalmakat, a törvény intézményi hatályát határozta meg. Eszerint a kormányzati elektronikus információbiztonság az alábbi intézményeket érinti:

- a központi államigazgatás szerveit, a Kormány és a kormánybizottságok kivételével;
- a Köztársasági Elnöki Hivatalt;
- az Országgyűlés Hivatalát;
- az Alkotmánybíróság Hivatalát;
- az Országos Bírósági Hivatalát és a bíróságokat;
- az ügyészségeket;
- az Alapvető Jogok Biztosának Hivatalát;
- az Állami Számvevőszéket;
- a Magyar Nemzeti Bankot;
- a fővárosi és megyei kormányhivatalokat;

- a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatalait;
- a hatósági igazgatási társulásokat;
- a Magyar Honvédséget.

A törvény hatálya alá tartoznak a felsorolt intézmények számára adatkezelést végzők is csakúgy, mint a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói, valamint az európai és nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt részei. A törvény alapján tehát ez az a szervezeti kör, amelynek munkatársait elektronikus információbiztonsági képzésben kell részesíteni. A törvény és annak nyomán megszületett 26/2013. (X. 21.) KIM rendelet három szinten nevezi meg azokat a közigazgatásban dolgozó alkalmazottakat, akiknek képzéséről gondoskodni kell IB (információbiztonsági) felelős vezető, IB résztvevő és IB felelős. A rendelet szerint e három szinten a Nemzeti Közszolgálati Egyetem köteles gondoskodni a továbbképzés tananyagainak kidolgozásáról az alábbiak szerint:

1. táblázat
*Az IB továbbképzés és éves továbbképzés programjainak szerkezete*

| | *Továbbképzés* | | *Éves továbbképzés* | |
|---|---|---|---|---|
| | *Idő (óra)* | *Tárgykörök* | *Idő (óra)* | *Tárgykörök* |
| IB felelős | 300 | Két féléves ASZTK*<br>80% elmélet<br>20% gyakorlat<br>Elektronikus IB vezető képesítés | 50 | IB technológia<br>IB stratégia, szabályozás<br>Incidenskezelés (kockázat)<br>Jog és szervezetirányítás |
| IB résztvevő | 50 | IB technológia<br>IB stratégia, szabályozás<br>Incidenskezelés (kockázat)<br>Jog és közigazgatás | 25 | IB technológia<br>IB stratégia, szabályozás<br>Incidenskezelés (kockázat)<br>Jog és szervezetirányítás |
| Felelős vezető | 8 | Jog, közigazgatás, vezetés<br>IB technológia<br>IB stratégia, szabályozás | 8 | Jog, közigazgatás, vezetés<br>IB technológia<br>IB stratégia, szabályozás |

**ASZTK:* Akkreditált Szakirányú Továbbképzés

A következőkben bemutatott szakértői interjú sorozat illetve kérdőíves lekérdezés, konkrét célja az 1. Táblázatban bemutatott képzésekhez való ajánlások kidolgozása volt.

## A szakértői interjúk tapasztalatai: az információbiztonság területei

A 15 interjú során két nagyobb kérdéscsoportra kerestünk válaszokat: milyen igényeket és elvárásokat támasztanak alanyaink a továbbképzésekkel kapcsolatban, illetve mi jellemzi az IB-felelősök kijelölésének közigazgatási folyamatát. Ennek érdekében nem

csak azok véleményére és tudására voltunk kíváncsiak, akik központi szerepet játszanak és játszottak az IB-vel kapcsolatos kormányzati programok kidolgozásában és végrehajtásában, hanem arra is válaszokat kerestünk, hogy mindebből mi és hogyan szivárog le a „végeken", vagyis a közigazgatás nem országos intézményeiben. Ezért a szakértői interjúkat két csoportra osztottuk, az első csoportba azok a szakértők kerültek, akik kisebb vagy nagyobb befolyással bírnak az IB fejlesztését célzó országos politikák kialakítására, ezeket neveztük úgynevezett „szakértői interjúknak". A másik csoportba azok kerültek, akik ilyen befolyással nem rendelkeznek, viszont van rálátásuk arra, hogy milyen pozitív és negatív folyamatok kísérik például a törvény végrehajtását. Ezeket a típusú interjúkat úgynevezett „felhasználói interjúknak" neveztük el. A következő 2. táblázat mutatja az interjúk fontosabb adatait.

2. táblázat
*A kutatás során elvégzett szakértői interjúk*

| *Szervezet típusa* | *Interjúalany beosztása* | *Interjúkészítés ideje* | *Interjú típusa* |
|---|---|---|---|
| Minisztérium | IB-felelős | 2014. 01. 13. | Szakértői |
| Egyetem | IB-szakértő | 2014. 01. 15 | Szakértői |
| Egyetem | IB-szakértő | 2014. 01. 16. | Szakértői |
| Országos hatóság | elnökhelyettes | 2014. 01. 30. | Szakértői |
| Minisztériumi háttérintézmény | IB-szakértő | 2014. 01. 31. | Szakértői |
| Informatikai szolgáltató | IB-igazgató | 2014. 02. 05. | Szakértői |
| Informatikai szolgáltató | IB-szakértő | 2014. 02. 05. | Szakértői |
| Informatikai szolgáltató | IB-szakértő | 2014. 02. 05. | Szakértői |
| Minisztériumi szervezet | informatikai főosztályvezető | 2014. 02. 06. | Szakértői |
| Országos IB-szerv | képzési felelős | 2014. 02. 25. | Szakértői |
| Vidéki kisváros önkormányzata | HR-szakértő | 2014. 01. 30. | Felhasználói |
| Vidéki kisváros önkormányzata | informatikus | 2014. 01. 30. | Felhasználói |
| Vidéki nagyváros bírósága | informatikai osztályvezető-helyettes | 2014. 01. 31. | Felhasználói |
| Megyei adóigazgatóság | humánigazgatási főreferens | 2014. 01. 31. | Felhasználói |
| Vidéki nagyváros bírósága | IB-szakértő | 2014. 02. 04. | Felhasználói |

Mint látható, az interjúk során a megkérdezett 15 interjúalany közel kétharmada a szakértői csoportból került ki, míg a fennmaradó kicsit több mint egyharmad képviselte a felhasználói csoportot. Ezeket az arányokat azért alakítottuk ki, mivel a kutatás célja a képzés tartalmával kapcsolatban megfogalmazott szakértői és munkáltatói vélemények feltárása volt, ebben pedig a felhasználói csoport kompetenciája korlátozott. Általánosságban is elmondható, hogy a közigazgatás alsóbb szintjein dolgozók között a témával

kapcsolatban nagy a bizonytalanság, általában keveset tudnak arról, mi, miért és hogyan történik. Ez jelenleg nem biztos, hogy baj, hiszen egy olyan új ügy beemelése és fontosságának elismertetése, mint amilyen az információbiztonság is, általában felülről lefelé történő kezdeményezések útján történik, különösen a bürokratikus szervezetek esetében. Ez a bizonytalanság a képzések beindulásával, az IB személyi struktúrájának felállításával és napi szintű működtetésével önmagában is csökkeni fog.

A kutatás során a kiszemelt és nyilatkozni hajlandó szakértőkkel félig strukturált mélyinterjúkat készítettünk. A szakértői és felhasználói csoport számára némileg eltérő vezérfonalat dolgoztunk ki. Mindkét vezérfonal a következő három nagyobb területre koncentrált: az információbiztonság kérdése a közigazgatásban, a képzendők körének kiválasztásának folyamata és a képzés tartalmával összefüggő kérdések, vélemények, elvárások. A szakértői csoport tagjaival készített interjúk során országos vagy nemzetközi tendenciákat igyekeztünk megragadni, míg a felhasználói csoport tagjaival a már elindult folyamatok kapcsán szerzett tapasztalatokra voltunk kíváncsiak, illetve hogy helyben milyen igények keletkeznek, amik esetleg eltérnek az országos szinten felmerülő igényekről.

A kutatás 2014. január elején indult, a szakértői lista összeállítására, a vezérfonalak elkészítésére, az interjúk leszervezésére és lefolytatására, valamint az eredmények kiértékelésére két hónap állt rendelkezésre a kutatócsoport tagjai számára, ami jelentős korlátokat szabott a célok kitűzésekor. A kutatás rövid idő ellenére arra mindenképpen alkalmas volt, hogy azonosítsuk azokat a legfontosabb pozitív és negatív tendenciákat, melyeket az elektronikus információbiztonság növelését célzó közigazgatási törekvéseket jellemzik, és amelyek hasznos útmutatóul szolgálhatnak az ehhez kapcsolódó képzések fejlesztéséhez.

Az interjúalanyok által elmondottakat négy nagyobb témakör szerint csoportosítva mutatjuk be: az IB szabályozási háttere és szervezeti struktúrája a közigazgatásban, az informatikai infrastruktúrával kapcsolatos legfontosabb kérdések és problémák, az IB-vezetők, az IB-felelősök és az IB-résztvevők kiválasztásának folyamata, valamint a képzésekkel kapcsolatban megfogalmazott legfontosabb igények és elvárások.

## Az információbiztonsággal kapcsolatos szabályozás és szervezeti struktúra

A megkérdezett szakértők többsége szerint a magyar IB-szabályozás nemzetközileg is élenjáró színvonalú, egyes vélemények szerint jóval előrébb tart, mint azt az informatikai infrastruktúra használatának fejlettsége indokolná. A stratégia, a törvény és a végrehajtási rendeletek logikusan épülnek egymásra, ezek elfogadását széleskörű egyeztetés előzte meg a szakmán belül. Mindez azonban nem feledtetheti el, hogy Magyarország nagy lemaradásból indult ezen a téren. Hiába indultak tehát be az elmúlt években, a szakértők szerint, egyértelműen pozitív folyamatok, ahhoz hogy ennek érezhető hatása legyen, még időre lesz szükség. A pozitívumok között említették a párbeszédet az állam, a privát szektor és az oktatási/akadémiai szféra között, a preventív szemlélet és a tudatosítás fontosságának elismerése, valamint a holisztikus szemlélet, vagyis annak fel-

ismerése, hogy az információbiztonság szintjének emelése nemcsak a közigazgatásban, de a magánszektorban és az állampolgárok körében is ugyanolyan fontos.

Ezzel együtt a múlt öröksége még jó időre korlátokat szab a fejlődésnek. Legjobban ezt az alábbi vélemény illusztrálta:

> „A legnagyobb probléma, hogy a kezdetektől fogva nem rendszerezetten és nem megfelelő szemlélettel lettek megtervezve a rendszerek, majd átadva és üzemeltetve. Így ez többszörös munkát jelent, amikor szeretné ezeket a rendszereket azonos szisztéma, rendszer szerint üzemeltetni, vagy akár csak amikor egyáltalán elvárásokat szeretne megfogalmazni e rendszerek irányába, működésével szemben; és ez nagyon lassú folyamat. Olyan, mint egy város elfoglalása, mintha mindent házról-házra miden egyes eszközért, szolgáltatásért gyakorlatilag megküzdve minden egyes üzemeltetővel." (informatikai szolgáltató információbiztonságért felelős igazgatója)

Az IB egész szervezeti struktúrája 1-2 éve épült ki a közigazgatáson belül, egyelőre sok a párhuzamosság, az átfedés a hatáskörökben és a munkavégzésben egyaránt, ráadásul – több interjú alany szerint is – e szervezeti egységek között alacsony a koordináció és a kooperáció, a rivalizálás ezzel szemben néha eléri a kontraproduktív szintet. Jelenleg a szervezeti struktúra tetején a Nemzeti Kiberbiztonsági Tanács (KBKT) található, melynek elnöke a Miniszterelnökséget vezető államtitkár, tagjai az államtitkárok és a tagszervezetek elnökei. Ezen belül – a második szinten – különböző kiberbiztonsági munkacsoportok (KBMCS) alakultak, illetve a szélesebb társadalmi egyeztetésnek teret adó Kiberbiztonsági Fórum (KBF), amelyben a kormányzaton kívül képviseltetik magukat az üzleti, a tudományos és a civil szféra képviselői. A harmadik szinten találhatók az ágazati CERT-ek (Computer Emergency Response Team), a Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja, a Kormányzati Eseménykezelő Központ (govCert Magyarország), a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) és Nemzeti Biztonsági Felügyelet (NBF). A CERT-ek feladata a felderítés, az utólagos kárelhárítás az, hogy minél hatékonyabban legyen adott incidens elhárítva, összefogva az adott intézményeket egy jól járható metodika szerint. A NEIH és az NBF (szak)hatóságként működnek; a NEIH elvárásokat fogalmaz meg a különböző kormányzati intézmények és szervek felé, elvárja, hogy legyen szabályzat, meglegyen a biztonságért felelős személy, valamint ellenőrzést gyakorol felettük. Emellett szakhatóságként fordulhat az NBF-hez, amennyiben valamilyen minősített adattal kapcsolatos az ügy vagy szakmailag nem tud ellátni. Ebben a struktúrában a legalsó, negyedik szinten az egyes intézményeknél kinevezett IB-felelősök állnak.

A szakértők többségének véleménye szerint az egyik legfontosabb tennivaló a harmadik szinten lévő szervezetek közötti együttműködés erősítése, illetve a negyedik és a harmadik szint közötti információáramlás megfelelő csatornáinak megteremtése lesz. A szakértők egy része szerint jelenleg nem világos, hogy adott esetben kinek, milyen szervezet felé kell vagy lehet fordulnia, melyik intézmény mivel foglalkozik és mivel nem. Egy másik interjúalanyunk türelmesebben fogalmazott:

„Az egész stratégia nagyon fontos, de a legfontosabb, hogy legyen koordináció. Több száz ágazat van, amit össze kell fogni. Több háttérintézmény van, ezeket koordinálni kell. A stratégiának a legfontosabb eleme az, hogy egyáltalán van, az már jó, hogy létezik. Van összefogás, koordinálás, de ezen még lehet javítani. Meg fog alakulni szépen sorban az összes ágazati munkacsoport, akik felméréseket készítenek, megmutatják, hol állnak és merre kellene haladni. A lényeg az, hogy felállnak ezek a munkacsoportok, legyen együttműködés a szervezetek között." (minisztériumi háttérintézmény, IB-szakértő)

A képzés azért kiemelten fontos, mert ezzel a negyedik szinten, vagyis a közigazgatás munkahelyeinek a szintjén teremtődik meg az információbiztonság egy olyan szakmai alapja, amelyeken keresztül a felsőbb szinteken elindított folyamatok sokkal gyorsabban és hatékonyabban tudnak beszivárogni a mindennapi munkavégzés rutinjába. Létező probléma, hogy ha fel is tárnak valamilyen biztonsági hiányosságot egy adott munkahelyen, évekig nem javítják ki, mert nem tudják, miért fontos, nem érzik magukénak. Az IB-felelősök feladata lesz az IB ügyének képviselete a munkahelyeken. Szintén fontos, hogy a különböző intézményeknél dolgozó IB-felelősök között kialakuljon a szakmai párbeszéd, de erről a későbbiekben szólunk majd.

## IT-infrastruktúra helyzete a közigazgatásban

Az elektronikus információbiztonság egyik fontos eleme az IT-infrastruktúra állapota. Ezzel kapcsolatban az egyik legnagyobb probléma, hogy nem ismerjük a magyar közigazgatásban jelenleg használt informatikai rendszereket. Egyik szakértő becslése szerint jelenleg 50-100 ezer informatikai rendszert használhatnak a magyar közigazgatásban, de a becslés tág határai is jól jelzik azt a bizonytalanságot, amellyel ezen a területen számolnunk kell. A törvény és a végrehajtási rendeletek kapcsán elindult ezek feltérképezése, de ez még nagyon korai stádiumban tart. Több megkérdezett szakértő is amellett érvelt, hogy egy informatikai kataszteri térkép nélkül nagyon nehéz továbblépni, ennek megfelelően ez az egyik első feladat, amelyet a már említett jogszabályok elő is írnak. Ilyen nyilvántartás alapján megoldható lesz az informatikai rendszerek biztonsági osztályokba sorolása, majd az ehhez szükséges, kockázat-arányos védelem megtervezése.

Az mindenesetre az informatikai biztonság növelését nagyban megkönnyíti, hogy ma már az informatikai beszerzések központilag, például a Nemzeti Infokommunikációs Szolgáltató (NISZ) Zrt.-n keresztül történnek. A beszerzések központosításával egyszerűbb, és ami ugyanilyen fontos, olcsóbb az alapvető biztonsági szempontokat érvényesíteni. Erről egyik interjúalanyunk a következőképpen számolt be:

„A jelenlegi rendszerek fejlesztése során nem vették figyelembe az IB szempontjait. Rengeteg sérülékeny rendszer van, nincs mögöttük support szerződés; ami kezelné a feltárt hibákat. Vannak olyan rendszerek, ahol 3 éve nem ismert a fejlesztő személye, már se a fejlesztő, se a megrendelő nem érhető el, nem dolgozik a

kormányzatnál. Jó esetben legalább a NISZ-ben van a rendszer, és kap valamilyen védelmet, rosszabb esetben valami külső szolgáltatónál, ahol kérdéses a védelme." (informatikai szolgáltató, IB-igazgató)

A költségek kapcsán az egyik szakértő arra hívta fel a figyelmet az információbiztonság egyik sajátossága, hogy ha jól működik, a kívülálló számára láthatatlan. Nem látható, nem vagy nehezen mutatható ki, nem lesz tőle a szolgáltatás jobb, gyorsabb, színesebb, szagosabb és az egyszerű felhasználó nem is igen tudja megfogni. Jelenleg nincsenek elterjedve olyan szabványok, amivel ezt mérni lehetne, bár a szakma elemi érdeke lenne, hogy bemutassa, a biztonság növelésével mennyit lehet megtakarítani.

Egyes vélemények szerint maga az infrastruktúra is nagyon decentralizált, ami növeli a költségeket és biztonsági kockázatokat is rejt. Egyik megkérdezett szakértőnk szerint:

„Nemrég volt egy felmérés, hogy hány gépterem van az állam kezében. 900-nál is nagyobb szám jött ki. Japánban ezzel szemben van 50 prefektúra, és minden prefektúrában egy alkalmazás-szolgáltatási központ, az szolgálja ki az összes állami intézményt abban a prefektúrában. Ezek redundanciában össze vannak kötve. Magyarországon a teljes védelmet végigvinni 900 géptermen szinte lehetetlen." (informatikai szolgáltató, IB-szakértő)

Belátható, hogy 900 helyen nehezebb érvényesíteni ugyanazokat az alapelveket, eljárásokat és előírásokat, mint például 50 helyen. Emellett lényegesen olcsóbb is biztosítani a biztonsághoz elengedhetetlen infrastrukturális feltételeket és a megfelelő szakértelmet.

Ezzel kapcsolatban egy érdekes problémára is felhívták a figyelmet a szakértők. Hatalmas fejlesztések indultak be az elmúlt pár évben az informatikai infrastruktúrák fejlesztésére, ami mindenképpen pozitív fejlemény. Azonban e fejlesztések finanszírozása jórészt EU-s forrásokból történt, amelyek nem teszik lehetővé e rendszerek üzemeltetését, fejlesztését vagy a folyamatos támogatás biztosítását. Ezekre külön forrást kell találni, különben a fejlesztések nem lesznek fenntarthatók. Visszatérve az IB szűkebb területére, további probléma, hogy jelenleg nehezen vagy egyáltalán nem számszerűsíthető, hogy éves szinten mennyibe kerülnek a közelmúltban meghozott információbiztonsági intézkedések.

További lendületet adhat az infóbiztonsági szempontok érvényesítésének, ha az állam konkrét ajánlásokat fogalmaz meg a fejlesztésekkel kapcsolatban, így az IB szempontjai már a tervezés szakaszában érvényesülhetnének. Jelenleg a törvény az üzemeltetési elvekre vonatkozóan tartalmaz előírásokat, de nincs olyan egységes fejlesztési ajánlás, amely arra vonatkozóan szolgálna iránymutatóul, hogy mi az a biztonsági követelményrendszer, amihez minden fejlesztő, cégmérettől függetlenül, alkalmazkodni tudna, és ezek szerint fejleszthetné információs rendszereit az állam részére. Ilyen ajánlások megfogalmazása a fejlesztők egyfajta képzéseként is értelmezhető.

## Kinevezések közigazgatási folyamata

A törvény három szinten határozza meg azok körét, akiket valamilyen információbiztonsági képzésben kell részesíteni: felelős vezető, IB-felelős és IB-résztvevő. Az egyes szinteken megjelenő feladatokkal kapcsolatban nagyjából egyetértés mutatkozik a megkérdezett szakértők között. A három szinten különböző típusú problémák jelentkeznek. Elvileg a Nemzeti Elektronikus Információbiztonsági Hatóságnak kell regisztrálnia az IB által érintett személyeket, az érintett intézmények jelzései alapján. Ahhoz azonban, hogy ellenőrizni lehessen, mely szervezetek mulasztották el a törvény végrehajtását, egy alacsonyabb szintű jogszabályban taxatíve fel kellett volna sorolni az érintett intézmények nevét. Így viszont szinte lehetetlen ellenőrizni, hogy mely intézmény tett eleget törvényben előírt kötelezettségeinek és mely nem.

A IB vezetőkkel kapcsolatban legtöbbször elhangzott aggály az volt, hogy elvileg ennek a személynek minden szervezet esetében a munkáltatói jogokat gyakorló vezetőnek kell lennie. Egy minisztérium esetében azonban felmerül a kérdés, hogy ki számít vezetőnek, maga a miniszter vagy a közigazgatási államtitkár? Elvileg a miniszter lesz ez a személy, az azonban kétséges, hogy a valóságban a miniszterek hogyan fogják ezt a plusz feladatot kezelni, mit, hogyan és kinek delegálnak tovább, beülnek-e majd a kötelező képzésekre? A vezetők képzése több szempontból is kritikus fontosságú. Egyrészt ők jelenítik meg az információbiztonság ügyének fontosságát az egész szervezeten belül. Másrészt a vezetők nevezik ki az IB-felelős személyeket. Ahhoz, hogy a legmegfelelőbb emberek kerüljenek erre a posztra, elengedhetetlen, hogy a kinevező személyek is pontosan értsék a terület fontosságát és a konkrét feladatokat.

Az IB-felelősök kinevezésével kapcsolatban még nagyobb a bizonytalanság. A megkérdezett szakértők szerint ugyanis a jogszabályok nem adnak kellően pontos iránymutatást arra vonatkozóan, hogy milyen szervezeti egységenként lehet ilyen személyt kinevezni. Feltehetően ez előre nem is határozható meg pontosan. Volt olyan szakértő, aki nem is feltétlenül alkalmazotti létszám szerint határozná meg, hogy milyen szinteken kell kijelölni IB-felelősöket:

> „Nem létszámban, hanem adat függvényében határoznám meg ezt. Ha például egy önkormányzat nem kezel nemzeti adatvagyon körében kritikus dolgokat, nem kezel nagyon érzékeny adatot, ott akár járásonként lehetne egy referens. Ahol viszont keletkezik ilyen információ, oda mindenképpen kellene." (minisztériumi szervezet, informatikai osztályvezető)

Volt olyan megkérdezett minisztériumi háttérintézmény, ahol a kinevezések pontos menetéről és szintjeiről a minisztérium saját rendeletet alkotott a törvény alapján. Ezzel az a probléma, hogy a jogszabályok értelmezése nem minden esetben egységes, előfordulhat, hogy egyes belső rendelkezések nincsenek összhangban a jogalkotó szándékával, rosszabb esetben pedig még a törvény betűjével sem. E rendeletek külső szakmai kontrollja általában elmaradt. Ez felveti annak problémáját, hogy a törvény végrehajtásáért felelős hatóság rendelkezik-e azokkal a jogosultságokkal, amelyek segítségével feladatát kellő hatékonysággal el tudja-e látni, érvényt tud-e szerezni a törvényben leírtaknak.

Majdnem minden megkérdezett megemlítette, hogy szükséges volna az egyes intézményekben működő információbiztonsági szervezeti egységek megerősítésére, anyagi eszközökkel és humán erőforrással egyaránt, egy bizonyos méret fölött például külön adminisztrátorral és vezetővel. Abban a legtöbb szakértő egyetértett, hogy kulcskérdés lesz, rendelnek-e majd a megnövekedett feladatokhoz kiegészítő erőforrásokat, mert ha változatlan büdzséből kell több feladatot megoldani, az nem segíti a színvonalas munkavégzést.

A hatósági szakértők szerint fontos, hogy IB-felelősnek olyan embereket válaszszanak ki, akik jól ismerik belülről a szervezetet, hiszen nekik tudásbrókeri szerepet is be kell majd tölteniük a szakhatóságok és az adott közigazgatási intézmény között. Ez azt jelenti, hogy nekik kell majd a NEIH, az NBF, a NISZ és más szakmai szervezetek elvárásait közvetíteni az intézmények felé, és megfordítva: a munkahelyek szintjén keletkező problémákat „lefordítani" arra a nyelvre, amit az információbiztonsági szakemberek is értenek. Ők lesznek azok, akik: „beszélik mind a két nyelvet, ismerik a helyi viszonyokat, tudják a felmerülő problémákat helyben, lokálisan kezelni esetleg, másrészt ami nem oldható meg azon a szinten, azt műszaki tartalomra fordítva tudják az üzemeltetőnek továbbküldeni. Jellemzően az üzemeltető nem érti meg, amit a felhasználó mond, visszakérdez, amit viszont a felhasználó nem ért". Ebből az is következik, hogy az IB-felelősöknek nem elsősorban a technikai hátteret kell minél mélyebben megérteni, hanem a szakmai alapok elsajátítása után olyan puha vagy társadalmi tudások terén is jól kell teljesíteni, mint a kommunikációs vagy együttműködési készség.

## Képzés

A képzéssel kapcsolatban az egyik legnagyobb kihívás, amivel a képzési anyag kidolgozása során a fejlesztőknek szembe kell nézniük, az a rendkívül heterogén szintű tudás, ami a közigazgatásban dolgozókat jellemzi az IB terén. A képzendők nagyon eltérő szakmai és kulturális háttérrel rendelkeznek, valahol egy jogász lett az IB-felelős, más helyen a fizikai infrastruktúra biztonságáért felelős részlegen dolgozó munkatárs, ennek figyelembe vétele oktatás módszertanilag is komoly feladat lesz.

Egyöntetű volt a megkérdezett szakemberek véleménye arról, hogy a képzés során gyökeresen szakítani kell a hagyományos képzésekkel, mind azok tartalmát, mind pedig módját vagy formáját illetően. Az általános tárgyak és ismeretek mennyiségét minimalizálni szükséges, a képzési tartalmakat minél szorosabban a mindennapi munkába ágyazottan kell megjeleníteni – mondták szakértőink, akik között IB-oktatással foglalkozó szakember is akadt. Szintén fontosnak érezték, hogy az IB-t nem lehet egy vagy két szakmára redukálni, sem az informatikára, sem pedig a jogra, inkább egyfajta gondolkodásmód, logika átadására kellene törekedni:

> „Nem kell mindenkit rendszergazdává, fejlesztővé képezni. Olyannak kell lennie a képzésnek, hogy gondolkodásmódot tanítson, hogy meglegyen a hozzáállása, az elvárása bizonyos eszközökkel, szolgáltatásokkal szemben, igénye legyen arra, hogy ő és az adatai is biztonságban legyenek. Aztán mindenki a maga szintéjén várja ezt el és mindenki a maga szintjén tegyen érte."

Azokra az elemekre kell tehát helyezni a hangsúlyt, amelyeket a napi rutin során közvetlenül használni tudnak majd a képzésben résztvevők. Ebben kitüntetett szerepe van a folyamatok, eljárások, szabványok, ajánlások ismeretének. Egy megkérdezettünk tapasztalata az, hogy megtörtént incidensek esettanulmány-alapú feldolgozásával mind a szabályok, mind pedig az eljárások, folyamatok sokkal könnyebben átadhatók:

> „Erre kíváncsiak az emberek. Nem elég elmondani a szabályzatot, az esetre fog emlékezni nem a szabályzatra, illetve az eseten keresztül a szabályzatra, az elkerülhető hibákra és a helyes megoldásokra."

Legtöbben szívesen látnák, ha az alapvizsgában és a szakvizsgákban, önálló, választható modulként megjelenne az információs és elektronikus közigazgatás biztonság oktatása. Szintén nagyon fontos, hogy az újonnan érkezők egy gyorstalpalón elsajátítsák a legalapvetőbb ismereteket, különösen azokban az intézményekben, ahol magas a fluktuáció. A képzés tartalmának kidolgozása során szintén érdemes figyelembe venni, hogy a közigazgatásban dolgozók rendkívül leterheltek, így a kiegészítő képzéseket többnyire felesleges pluszfeladatként élik meg. Ezért, ha nem érdekes módon tálalják a tananyagot, az oktatás hatékonysága hatványozottan visszaesik. Ebben nagy segítség lehet az eLearning mint oktatási módszer részleges alkalmazása, mely lehetőséget teremt arra, hogy mindenki rugalmasan, a saját tempójában tanuljon, koncentráltan és rövidebb idő alatt jusson célba az átadni kívánt tudást, figyelembe véve az egyéni tanulási szokásokat.

Visszatérő motívum volt, hogy a három az elektronikus információbiztonság szervezetének szintjén különböző dolgokat kell oktatni, amit egyébként a rendelet is így szabályoz. A megkérdezettek szerint az IB-vezetőknek elsősorban tudatosításra és holisztikus ismeretekre van szüksége. Tudatosítani kell bennük a felelősséget, hogy ha kikerül az adat, az az ő felelősségük. A törvény ismerete, a képesség kialakítása a legfontosabb, és az, hogy vezetőként tudja kontrollálni és irányítani a folyamatokat: mit kell kérdezni a biztonsági felelőstől, mit kell kérdeznie a beosztottjaitól, mit kell tennie egy hatósági ellenőrzés során, a hibákat, hogyan tudja orvosolni stb.

A megfogalmazott elvárások szerint az IB-felelősöknek a vezetőkhöz képest sokkal gyakorlat-orientáltabb képzésben kell részesülniük, összhangban a rendeletben megfogalmazottakkal. Esetükben is fontos azonban, hogy a tananyag elrugaszkodjon a hagyományos oktatási anyagoktól: támadás szimulálása, folyamatábra, amely azt ábrázolja, hogy ilyen esetben mi a teendő. Mások szerint nem kell nagyon mély technológiai ismeretekkel rendelkezniük, hiszen ennek megszerzése nem várható el mindenkitől. Ehelyett inkább a szakmai alapokat kellene megtanítani a felelősöknek és azt, hogy fel tudják ismerni, ha baj van vagy baj lehet és tudják, hogy kikhez fordulhatnak szakmai segítségért vagy meg tudják keresni, hogy ki a szakmailag kompetens partner, aki a segítségükre lehet. Szintén nagyon fontos, hogy a továbbképzések és az éves továbbképzések mellett legalább az IB-felelősök szintjén felálljon egy komplett tudásmenedzsment rendszer. Szakértőink szerint biztosítani kell az információ szervezett módon történő megosztását az IB-felelősök között. Fontos, hogy legyen olyan szakmai fórumuk, ahol egymás között tudják megbeszélni a felmerülő problémákat és azokat a megoldásokat, amelyekkel ezeket elhárították. Ebbe a szakmai közösségbe integrálni lehetne a CERT-eket, a NEIH-t és az NBF-et is. Így létrejöhetne egy közvetlen kapcsolat

az információbiztonsági szervezeti struktúrájának harmadik és negyedik szintje között, amelynek alapja egy gyorsan és közvetlenül elérhető kollektív tudásbázis volna. A vállalati szférában ez már bevett módon alkalmazott megoldás, általában külön erőforrásokat is allokálnak azon dolgozók részére, akik az ilyen felületek működtetésében, életben tartásában aktívan közreműködnek, mert ez még így is olcsóbb és gyorsabb megoldás, mintha mindenki a legegyszerűbb problémákkal is a hivatalos utakat próbálná bejárni.

## A kérdőíves felmérés tapasztalatai: az általános információbiztonság tudatosság helyzete

A kutatásunk második szakaszában a közigazgatásban dolgozók IB-tudatosságának szintjét térképeztük fel. Tudomásunk szerint eddig szisztematikusan felépített adatgyűjtésből származó, empirikusan alátámasztott felmérés nem született még ebben a tárgyban Magyarországon. Ennek érdekében online kérdőívet tettünk ki a Nemzeti Közszolgálati Egyetem Tanulmányi és Vizsgaportáljára, amely a képzésben és továbbképzésben részesülő közigazgatási dolgozók számára kikerülhetetlen online felület. A kérdőívet 379 fő töltötte ki, de az online kérdőívek egyik sajátossága eredményeként, minden kérdésre értékelhető módon ennél kevesebben, 285-en válaszoltak.

A kérdőív kidolgozásánál az úgynevezett Security Awareness Survey (SANS) kérdőívét használtuk mintának, mert a feltáró jellegű vizsgálat miatt igyekeztünk a lehető legegyszerűbb és legrövidebb kérdéssort összeállítani.

A SANS kérdőívét az USA-ban dolgozó információbiztonsági szakértők dolgozták ki, a hétköznapi felhasználói szokásokat méri fel és azokhoz rendel 1-5-ig terjedő skálán egy értéket, majd az összesített értékek alapján öt kockázati kategóriába sorolja a válaszadókat.

A legalacsonyabb kockázati kategóriába tartozó munkavállalók jellemzője, hogy tisztában vannak a biztonsági alapelvekkel és veszélyekkel, jól képzettek, mindennapi viselkedésük megfelel a munkahelyi biztonsági szabályoknak és irányelveknek.

A második legkisebb kockázatot jelentő csoportba tartozó munkavállalók már vettek részt valamilyen IB-képzésen, tisztában vannak a veszélyekkel, de mégsem követik teljes mértékben a vonatkozó biztonsági alapelveket és szabványokat.

Az átlagos veszélyt jelentő kockázati csoportba azok a munkavállalók tartoznak, akik tisztában vannak a veszélyekkel és tudják, hogy bizonyos biztonsági alapelveket be kellene tartaniuk, de továbbképzésre szorulnak a témában. Esetükben különösen az jelent veszélyforrást, hogy nem ismerik fel biztosan az incidenseket és nem tudják, mi a teendő ilyen esetben.

A jelentős kockázati tényezőt jelentő csoportba tartozók nincsenek tisztában a biztonsági alapelvekkel és veszélyekkel, sem pedig munkaszervezetük biztonsági szabályzatával.

A kimondottan magas kockázati tényezőt jelentő csoportba tartozó munkavállalók nincsenek tisztában a veszélyekkel és nincsenek tekintettel a biztonsági szabályzatokra sem. Tevékenységük folytán a munkahelyi informatikai rendszer könnyen támadhatóvá válik a behatolók által.

A kérdőív 25 kérdésből állt, amelyek a következő nagyobb témákat érintették: munkaszervezet és szabályozás (7 kérdés), információbiztonsággal kapcsolatos tudások és ismeretek mindennapi felhasználói környezetben (8 kérdés), informatikai eszközök használata és adatkezelés (3 kérdés), általános számítógép használati szokások, különös tekintettel a jelszavak kezelésére (7 kérdés). A beérkezett válaszokat az SPSS statisztikai programcsomag segítségével dolgoztuk fel.

## A minta bemutatása és kritikai értékelése

A minta statisztikai értelemben nem reprezentatív a lebonyolításra rendelkezésre álló szűk időkeret miatt. Ugyanakkor azonban a reprezentativitás koncepcionálisan is nehéz kérdés, hiszen kérdéses az, hogy ismerjük-e az alapsokaság, tehát a közigazgatásban dolgozó állomány fontosabb szocio-demográfiai adatait kellő pontossággal ahhoz, hogy statisztikai értelemben mintavételi eljárásról beszélhessünk egyáltalán. A válaszokból kitűnik, hogy a kérdőívet kitöltők valamivel több, mint fele (54%) nő, 46%-a férfi. Túlnyomó többségük (85%) budapesti lakos, a főiskolai vagy egyetemi végzettséggel rendelkezők aránya 90%. A válaszolók több mint kétharmada (68%) 45 évesnél fiatalabb volt, 32%-uk a 35 éves kort sem érte el. A 45–54 éves kor közöttiek aránya 23%, míg az 55 éves vagy annál idősebbeké 9% volt. Mindezek alapján tehát megállapítható, hogy a mintában valós súlyuknál feltehetően nagyobb arányban képviseltetik magukat a budapestiek és a fiatalok.

## Globális, egyéni, szervezeti és infrastrukturális információbiztonság tudatosság

A globális képet tekintve megállapíthatjuk, hogy a válaszolók jól teljesítettek, hiszen 87%-uk a második legalacsonyabb kockázati besorolású csoportba került, mindössze 13% teljesített ennél rosszabbul, és ők sem kaptak közepesnél gyengébb osztályzatot. Figyelembe kell azonban vennünk a minta torzító hatásait.

A válaszadók megoszlása életkor szerint nem mutat különbségeket, a jó értékelést kapók között ugyanolyan arányban találunk fiatalokat, középkorúakat és időseket, mint a teljes mintában. Sőt, ha a közepes kockázati osztályba sorolt válaszadókat vizsgáljuk meg életkor szerint, akkor azt látjuk, hogy közöttük kevesebb 35 év alattit és 45–54 évest találunk, mint a mintában, míg a középgeneráció, vagyis a 35–44 éves korosztály felülreprezentált a mintában képviselt súlyukhoz képest (43%, illetve 36%). Ezeket a következtetéseket azonban óvatosan kell kezelni az alacsony elemszámok miatt.

Annak érdekében, hogy a globális értékelésen túl részletesebb képet kapjunk azokról a területekről, ahol a válaszadók jól vagy rosszabbul teljesítenek, a kérdéseket három nagyobb dimenzió mentén különítettük el.

A szervezeti dimenzióba olyan kérdések kerültek, amelyek a céges szokásokat és eljárásokat mérték: pl. Van-e IB-részleg a munkahelyén?, Tudja-e kihez kell fordulnia,

ha számítógépét feltörték?, Szokott-e céges adatokat lemásolni és hazavinni?, Részesült-e munkahelyén IB-képzésben? stb.

Egyéni dimenziónak neveztük el azokat a kérdéseket, amelyek általános ismereteket és szokásokat tükröznek a felhasználó szintjén: pl. Észrevenné-e, ha gépét feltörnék?, Megadta-e már céges jelszavát másnak is?, Milyenek a levelek csatolmányainak megnyitásával kapcsolatos szokások? stb.

Végül infrastrukturális dimenzióba soroltuk az olyan kérdésekre adott válaszokat, amelyek a munkahelyi informatikai infrastruktúra állapotáról alkotott válaszadói percepciókat mérték, vagyis azt, hogy a válaszadók szerint mennyire biztonságosak a munkahelyi rendszereik: pl. Telepítve van-e vírusirtó a gépén?, Számítógépe automatikusan végzi-e el a frissítéseket?, Talált-e már vírust vagy trójai programot a céges gépén? stb.

3. táblázat
*Az IB-tudatosság szintje globálisan és a mért dimenziók szerint*

| | *Globális* | *Szervezeti* | *Egyéni* | *Infrastrukturális* |
|---|---|---|---|---|
| | | *dimenzió* | | |
| Jeles | 0% | 7% | 0% | 67,5% |
| Jó | 87% | 92% | 77% | 29% |
| Közepes | 13% | 1% | 23% | 3,5% |
| Összesen | 100% | 100% | 100% | 100% |

Mint a 3. táblázat adataiból látható, az infrastrukturális dimenziómérő válaszok értékei haladják meg legjelentősebb mértékben a globális képet: 67,5%-uk az e dimenziókra számított értékek szerint „jelesre vizsgázott", további közel 30% ért el jó eredményt és mindössze 3,5%-uk kapott közepes kockázati besorolást. Itt újra fel kell hívnunk a figyelmet arra a torzító hatásra, amelyet a földrajzi egyenlőtlenség jelentett a mintán belül. További kritikus észrevételeket is teszünk még az átfogó értékelés után, amelynek során a válaszok belső ellentmondásait elemezzük.

A szervezeti dimenzió kockázati besorolását mérő válaszok szintén kiugróan jó eredményt mutatnak: 7%-uk a legjobb kategóriába került, 92%-uk a második legjobb kategóriába és ebben a dimenzióban mértük a közepes értékek legalacsonyabb arányát, a válaszadók mindössze 1%-a sorolódott a közepes szintű kockázatot jelentő csoportba. Érdekes módon az egyéni dimenziót mérő kérdésekre adott válaszok mutatják a relatíve legrosszabb értékeket: 77% kapott jó minősítést és 23% közepest, szemben a globális szinten mért 87 és 13%-kal. Ennek a dimenziónak a megoszlásait alaposabban is megnéztük a két releváns háttérváltozó, vagyis az életkor és a nem szerint. Ezeket a megoszlásokat mutatja a 4. táblázat.

4. táblázat
*Az egyéni dimenzió értékei életkor és nem szerint*

| | *Jó osztályzat* | *Közepes osztályzat* | *Átlag a mintán belül* |
|---|---|---|---|
| *Életkor szerint* | | | |
| 35 év alattiak | 34,5% | 21,5% | 31,5% |
| 35–44 év között | 34% | 43% | 36% |
| 45–54 év között | 23% | 24,5% | 23% |
| 55 év felettiek | 8,5% | 11% | 9% |
| *Nem* | | | |
| Nő | 57% | 46% | 54,5% |
| Férfi | 43% | 54% | 45,5% |

A 4. táblázat azt mutatja, hogy a különböző életkori kategóriák, illetve nemek képviselői milyen arányban fordulnak elő a jó és a közepes kategóriában, illetve ehhez képest mekkora a súlyuk a teljes mintán belül. Az értékek egyrészt megerősítik a korábban elmondottakat, vagyis hogy életkor szerint a legfiatalabbak teljesítenek ugyan a legjobban, azonban a 35–44 éves korosztály törést mutat, a mintában képviselt súlyukhoz képest jelentősen nagyobb arányban találunk relatíve rosszabb értékeket, mint akár a náluk fiatalabbaknál, akár a náluk idősebbeknél. Új elem azonban, hogy nemek szerint is jelentős eltérések mutathatók ki. Ezek szerint a közepes osztályzatot kapott válaszadók körében közel 10%-kal kisebb a nők aránya, mint a teljes mintán belül, míg a férfiaknál ugyanez fordítva igaz, vagyis jelentősen több férfit találunk a közepesre értékeltek között, mint a teljes mintában.

## Az információbiztonság tudatosság összetevőinek részletes elemzése

Bármely kérdőíves felmérésnél megvan annak a veszélye, hogy a kérdőívnek szeretnének megfelelni a válaszadók. Ezen kívül az sem hagyható figyelmen kívül, hogy egy online (számítógéppel segített) kérdőív kitöltése feltételezhetően csak azoktól várható el jobbára, akik munkájukhoz rendszeresen (napi szinten) használják a számítógépet, valamint nincs az informatikai eszközökkel kapcsolatban negatív attitűdjük. Ilyen, kellő távolságról szemlélve a kitöltéssel kapcsolatos felhasználói szokásokat láthatóvá válik, hogy a kérdések megválaszolása során monoton növekvő tendenciát mutat a kihagyott kérdések száma. Azaz minél hátrébb helyezkedett el a kérdés a kérdőívben, annál nagyobb eséllyel, illetve egész pontosan annál több válaszadó által került kihagyásra.

A kérdőívre adott válaszok értékelése előtt le kell szögezni, hogy az informatikai biztonság olyan terület amely „nem mérhető jól" kérdőívvel. Ennek két oka van. Az egyiket fentebb már említettük: sokan a kérdésfeltevés analógiájára próbálnak logikusan szándékuk szerint helyesen válaszolni. Pontos mérés tehát akkor keletkezne, ha éles helyzetben kiderülne, hogy a munkavállaló valóban úgy is cselekszik, mint ahogy elméletben tudja vagy sejti a jó választ. A másik fontos oka annak, hogy nehéz mér-

ni egy szervezet informatikai biztonsági szintjét az, hogy a kérdőíves kutatások logikájának megfelelően nem a teljes alapsokaságot szondázzuk, hanem azokból valamilyen módszer szerint mintát veszünk, ellentmondva annak, hogy az informatikai biztonság egyik legfontosabb célkitűzése mindig az „egyenszilárdság" megteremtése. Egy példával illusztrálva ez azt jelenti, hogy ha százból csak egyetlen felhasználó hagyja nyitva a munkahelyén a bejárati ajtót, akkor azon ugyanúgy be tudnak menni a (adat)tolvajok, mintha 99 hagyta volna nyitva. Tehát, ha egyetlen számítógépet sikeresen megfertőznek célzott, vagy véletlen támadás során, akkor onnan már könnyedén, de legalábbis könnyebben tudják a szervezet többi számítógépét, szervereit célba venni.

További fontos információ a kiértékelés előtt, hogy tökéletes biztonság nem létezik, de a szervezet erőforrásaihoz képest erre kell törekedni. A ráfordítások és a biztonsági szint arányban tartása és ezen arány eldöntése mindig az adott szervezet vagy intézmény feladata és felelőssége.

*A szervezet információbiztonsága*

A válaszadók 88%-a nyilatkozta, hogy van informatikai biztonsággal foglalkozó részleg a munkahelyén, amely válasz egyik jelentése, hogy 12% olyan munkaszervezetnél dolgozik, ahol nincs ilyen.

Vélhetően itt komoly informatikai biztonsági gondok lehetnek, hiszen ebből következik, hogy ott a felső vezetés sem kap valós képet az információs és informatikai biztonságról. A munkavállalók nem részesülnek semmilyen képzésben vagy felvilágosításban. Az üzemeltetés által végzett feladatokról ebben a vonatkozásban nincs visszacsatolás sem az üzemeltetés, sem a felső vezetés felé.

A magasnak tűnő 88%-ot azonban érdemes megvizsgálni további kérdések tükrében:

- 8% nem érzi biztonságosnak a számítógépét adatlopásokkal szemben.
- 14%-a a válaszadóknak talált már trójai programot a gépén.
- 25% inkább úgy gondolja, hogy csak az IT-részleg feladata a biztonság garantálása.
- 26%-a azt mondja, hogy megadta már másnak a céges jelszavát.
- 33% nem tudja miről ismerhető fel valamilyen átverős (spam) levél.
- 40%-a állítja, hogy nem venné észre, ha feltörnék a számítógépét.
- 49% pedig mindezek ellenére úgy gondolja, hogy megfelelően elegendő informatikai biztonsági képzésben részesült. Hozzászámolva a bizonytalanokat ez az arány 61%-ra növekszik.

*A válaszadók információbiztonsági ismeretei, a képzéshez való viszonyuk*

Különösen nagy gondnak látszik az, hogy a válaszadók 61%-a úgy gondolja, hogy megfelelően képzett. Ennek a válasznak is két vonulata különböztethető meg. Az egyik a fentebb már felsorolt tényezők, másrészről pedig az a tény, hogy a biztonság nem tekinthető állapotnak, azaz nem érhető el. Technikai, hardver, szoftver, folyamat és törvényi változások naponta érik a szervezeteket. Ebből következik, hogy ezeket a változásokat nyomon kell követni, azaz az oktatási terv alapján optimális esetben negyedévente, de legalább félévente ismétlő képzésekre van szükség, amely szakmai igényre az Ibtv. intézményi választ is ad, a kötelező továbbképzések meghatározásával.

*Mobil eszközök és adatvagyon-használat*

A tudatossági oktatás (viszonylag) sűrű, rendszeres, periodikus fejlesztésének igényét támasztja alá a következő kérdéscsokor elemzése: Használhatja ön saját mobil infokommunikációs eszközeit (pl. okos telefon) céges információk tárolására és átvitelére? Azért különösen fontos ez a kérdés, mert a mobil eszközök két oldalról is veszélyforrást jelentenek: egyrészt a céges adat saját (magán) adathordozóra kerül, ahol veszélyeknek van kitéve, másrészt a magán adathordozó bekerül a céges hálózatba, amelyet megfertőzhet.

A válaszadók 17,4%-a felelt igennel erre a kérdésre. Esetükben a szoftverfrissítések és hardvercserék, illetve úgy általában a változások okán javasolt időközönként az oktatásuk, tudásuk szinten tartása és az esetleges incidensek tapasztalatainak visszacsatolása.

A válaszadók közel 43%-a nemmel felelt erre a kérdésre. Márpedig a tiltás alapvetően nem jó megoldás. Ennek oka, hogy „kerülőutak" keletkezhetnek. A munkavállaló kifejezetten kényelmetlennek érezheti a helyzetet, nem ért egyet a szabályozással és úgy érzi, hátráltatja a munkáját. Hosszútávon pedig, amennyiben megengedőbb irányba változik a céges szabályozás, akkor ezt a szegmenst teljesen nulláról kell majd oktatni.

A válaszadók 21%-a felelte azt, hogy használhatja, de csak a cég által nyújtott szolgáltatás igénybevételével. Ennek a szakmai szempontból ideálisnak tekinthető változatnak az aránya elég alacsony, a teljes használhatósággal együtt se éri el a 40%-ot. A jól körülhatárolt szolgáltatások megkönnyítik a munkavállalók életét, a munkavégzés folyamatát segítik. Ezekben az esetekben feltételezhető, hogy a visszajelzések mentén módosítják a szolgáltatásokat is.

A „Nem tudom" válaszok aránya is igen magas (18,7%), majdnem megegyezik az ideálisnak tekinthető megoldást alkalmazó munkavállalókéval. Ez a munkavállalói csoport akkor jelenik meg a biztonsági kockázat térképén, amikor megszerzi az első olyan eszközét, amely már képes a céges adatvagyonhoz csatlakozni. Vagy más módon, úgymond „hirtelen" tudomást szerez a lehetőségről.

Közel minden ötödik munkavállaló ilyen időzített bomba a céges adatvagyon szempontjából.

Biztonsági kockázatkezelés szempontjából hasonló kérdéssel arra kerestük a választ, hogy a megkérdezett munkavállalók milyen arányban töltenek le munkájukhoz különböző szoftvereket az internetről. Ez a szám elérte a 24%-ot, azaz ezeknél a szervezeteknél nincs eljárás arra nézve, hogyan kezeljenek egy olyan új alkalmazást, amely feltételezhetően ténylegesen szükséges a (napi) munkavégzéshez.

A válaszadók 40%-ánál fordult már elő, hogy a céges adatvagyon valamely elemét lemásolta és hazavitte (munkavégzés céljából, bár ez a kockázatkezelés szempontjából irreleváns). A válaszadók 56%-a állítja, hogy vagy nincs a megtekinthető weboldalakra vonatkozó előírás a munkahelyén vagy nincs vele tisztában. Ugyanez a kérdés a céges levelező rendszerre kicsit kedvezőbb, de még ebben az esetben is a válaszadók 45%-a állítja, hogy nincs szabályozás vagy nincs azokkal tisztában.

*A konkrét IT infrastruktúra biztonságának értékelése*

Számos kérdésre adott válaszban jelenik meg valamilyen tudás hiánya, vagy vélelmezhető valamilyen infrastruktúrának a túlértékelése. Ezek nagymértékben ellentmondanak a vélt biztonsági szintnek. Ez a vélt biztonsági szint, a vélt tudás túlértékelése önmagában

is nagy kockázatot jelent, azonban itt további számos tényező erősíti. Nevezetesen, a válaszadók:

- 60%-a állítja, hogy észrevenné, ha feltörnék vagy megfertőződne a számítógépe;
- 84%-a nem ért egyet azzal, hogy a vírusirtó megállít minden programot;
- 13%-a viszont nem biztos benne, hogy be van-e kapcsolva a vírusirtó a számítógépén;
- 74%-a szerint elvégzi a számítógépe a frissítések telepítését (automatikusan);
- 72%-a mondja a jelszó változtatási gyakoriságra, hogy az automata figyelmeztető üzenetekre hagyatkozik.

Ezekből a számokból nem olvasható le egyértelmű következtetés, de véleményünk szerint ezek az adatok is arra utalnak, hogy magas lehet a hamis biztonságérzet a közigazgatásban dolgozók között, túlértékelt vagy magasnak vélelmezett a munkahelyeken az információbiztonsági szint. Ilyen belső logikai ellentmondás, hogy automata frissítésekre, rendszerüzenetekre nagy számban hagyatkoznak a válaszadók. Tehát vagy a kérdésnek próbáltak megfelelni és arra pozitív, optimista választ adni, vagy a saját tudásukat értékelték túl, a többi válasz viszont megmutatta az ellentmondást. Ilyen jól látható példa, hogy több mint 70%-uk valamilyen automatikára hagyatkozik, ugyanakkor nagyságrendileg egyező számúan nem bíznak meg teljesen a vírusirtóban. Sőt, 60% még azt is észrevenné, amit a vírusirtó nem vesz észre. Talán kicsit kevésbé, de ellentmondásos az is, hogy minden nyolcadik válaszadó (13%) nem biztos benne, hogy a vírusirtó be van-e kapcsolva a gépén.

## Következtetések és lehatárolások

Tanulmányunkban áttekintettük a magyar közigazgatás információbiztonság tudatosságával kapcsolatos szabályozási keretrendszert, 15 közigazgatási szakértő szerinti meghatározó kulcsterületeit, és a közigazgatásban dolgozó 297 köztisztviselő információbiztonság tudatossági önértékelését.

Úgy véljük, eredményeink számos hasznos kiindulópontot jelentenek további kutatások számára, amelyek akár elméleti szempontból, akár a további törvényalkotás, végrehajtás vagy stratégiakészítés számára fejleszthetik tovább ismereteinket a magyar közigazgatás és az információbiztonság kérdéskörében. Ehhez mindenképp rögzítenünk kell azokat a lehatárolásokat, amelyek között eredményeink és megállapításaink érvényesek. Az első ilyen korlátozó terület az információbiztonság fogalmának elméleti feldolgozása, multidiszciplináris jellegének a közszolgálat számára lényeges kibontása. A második terület az információbiztonság ontológiai felépítéséből adódó mérhető változók meghatározása, és az empirikus vizsgálatok egyrészt ennek megfelelő modelljeinek létrehozása, másrészt reprezentativitásának biztosítása. A harmadik továbbfejlesztendő terület a kvalitatív elemzések vonatkozásában a szakértői interjúk, fókuszcsoportok vagy akár megfigyelések keresztvalidálása, akár külföldi vagy más iparágakkal való összehasonlítása.

A lehatárolások mellett kutatásunk számos olyan eredményt hozott és jelenséget mutatott meg, amelyeket célszerű figyelembe venni a magyar közszolgálat információbiztonság tudatosságának fejlesztése kapcsán.

A koncepcionális és szabályozási háttér áttekintésével megállapítottuk, hogy a magyar információbiztonsági szabályzás előbbre tart, mint azt az IT infrastruktúra illetve a közigazgatás „igény nyomása" indokolná. Nemcsak hazai körülmények között, de nemzetközi összehasonlításban is élenjáró, szisztematikus, a szinte átláthatatlanul komplex technológiai fejlődést kezelni és kézben tartani tudó szabályozási környezet alakult ki az elmúlt években Magyarország információbiztonságának stratégiai kezelésére.

Egybehangzó szakértői vélemények alapján ugyanakkor egyrészt közigazgatási rendszereink heterogenitása és decentralizáltsága, valamint a nehezen belátható költséghatékonyság javulás miatt továbbra is lemaradásban leszünk, amennyiben ezeken a területeken nem történik szisztematikus építkezés. Interjúink megerősítik, hogy ezen nagymértékben segíthet az információbiztonsággal kapcsolatos humán erőforrás-fejlesztés információbiztonsági vezetői és alkalmazotti szinteken is. Az információbiztonság vonatkozásában egyértelmű az egyetértés az egymás közötti kommunikáció hangsúlyozásában, a pontos egyéni és szervezetek közötti felelősség meghatározásában, a viselkedés és a kultúra meghonosításában; azaz nem elsősorban a technikai, hanem a humán területek húzó hatásának kihasználásában. Ez a logika egyébként nagyban összecseng azokkal az innováció befogadási paradigmákkal, amelyek megmutatják a szervezeti és human abszorpciós képességeket, amelyek nélkül nem kerülnek befogadásra a technológiai innovációk. Ebben a vonatkozásban, tanulmányukban felhívtuk a figyelmet a szereplők heterogén szakmai alapjaira, tudására és motivációjára. Kiemelt szükség lesz annak a tudáshálózatnak a kiépítésére, amely adatbázisok kiépítésével, esettanulmányok kidolgozásával, szakértői kapcsolatrendszer karbantartásával folyamatosan fejlődőképes rendszert fog alkotni az információbiztonsági elvárások megvalósítására.

A kismintás kérdőívünk kimutatta azokat a neuralgikus területeket, amelyek alapján láthatóvá váltak az ellentmondások az információbiztonság tudatosság megítélésében. A válaszadók nagyon, mondhatni talán túlzottan is magabiztosak saját tudásokban az általuk használt rendszerekben, azok automatizmusaiban. Ezzel párhuzamosan tetten érhető a kérdéseknek, a kérdőívnek való megfelelési szándék, ez a referenciakérdésekkel kimutathatóvá vált. A szervezeti tudás érzékelhetően túlértékelt, a tisztázó kérdésekre adott válaszok eredményeinek tükrében azok valós tartalma esetleges, bizonytalan. Az informatikai biztonsági egységek szervezeten belüli hierarchia szintje a javasoltnál alacsonyabb, vagy nem létezik, sok esetben keverik vagy összemossák az általános, üzemeltetési informatikával.

## Irodalom

Albrechtsen, E. 2007: A qualitative study of users' view on information security. *Computers & Security*. Vol. 26., No. 4., 276–289.

Bulgurcu, B. – Cavusoglu, H. – Benbasat, I. 2010: Information Security Policy Compliance: An Empirical Study Of Rationality-Based Beliefs And Information Security Awareness. *MIS Quarterly*. Vol. 34., No. 3., 523–548.

Knapp, K. J. – Ferrante, C. J. 2012: Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations. *Journal of Management Policy & Practice*. Vol. 13., No. 5., 66–80.

Shaw, R. S. – Chen, C. C. – HARRIS, A. L. 2009: The impact of information richness on information security awareness training effectiveness. *Computers & Education*. Vol. 52., No. 1., 92–100.

Illéssy Miklós az ELTE Szociológiai Intézetében végzett 2001-ben. 2003 óta a Magyar Tudományos Akadémia Szociológiai Intézetének munkatársa, jelenleg a Nemzeti Közszolgálati Egyetem E-közszolgálati Fejlesztési Intézetén belül működő Technológia és Innováció Kutatóközpont kutatójaként is dolgozik. 2001 óta vesz részt jellemzően az EU által támogatott nemzetközi összehasonlító kutatásokban. Legfontosabb kutatási szakterületei közé tartoznak a munkaszociológiai és szervezetszociológiai kérdések, illetve a kettő metszéspontjában álló munkaszervezeti innovációk.

Nemeslaki András, okleveles gépészmérnök (1986), a műszaki tudomány kandidátusa (1992), habilitált doktor (2011), egyetemi tanár (2013). A Nemzeti Közszolgálati Egyetem E-közszolgálati Fejlesztési Intézetének vezetője, az AROP 2.2.19. E-tanulás Módszertani Központ kutatási programjainak vezetője. Több mint húsz éve végez kutatásokat és publikál az információrendszer-menedzsment, e-business és projektmenedzsment területen.

Som Zoltán jelenleg a Nemzeti Közszolgálati Egyetem, Közigazgatás-tudományi kar, Közigazgatás-tudományi Doktori iskola és a Technológia és Innovációs Kutatóközpont PhD hallgatója, az E-közszolgálati Fejlesztési Intézet munkatársa. Kutatási területe az informatikai biztonságon belül a biztonság tudatosság, ennek mérése, növelése. Kutatásainak egyik fókuszterülete pedig a közigazgatás. Az informatikai folyamatok irányítására vonatkozó nemzetközi ITIL-F minősítéssel rendelkezik. A Szegedi Tudományegyetemen szerzett matematika–fizika főiskolai tanári, majd egyetemi informatika tanári diplomát.