

NEMZETI KÖZSZOLGÁLATI EGYETEM
ÁLLAMTUDOMÁNYI ÉS NEMZETKÖZI TANULMÁNYOK KAR

TUDOMÁNYOS DIÁKKÖRI KONFERENCIA
2022. ÉVI TAVASZI FORDULÓ

A KÖZSZOLGÁLATI ÁLLOMÁNY ADAT- ÉS
INFORMÁCIÓBIZTONSÁGI FELKÉSZÜLTSEGE

Szerző:
Szabó Dorina Barbara

Témavezető:
Dr. Bányász Péter, adjunktus

Budapest
04.14.
2022

A KÖZSZOLGÁLATI ÁLLOMÁNY ADAT- ÉS INFORMÁCIÓBIZTONSÁGI FELKÉSZÜLTSEGE

04.14.

2022

Tartalomjegyzék

BEVEZETÉS	6
A téma aktualitása.....	6
A tudományos probléma megfogalmazása	7
Kutatási célkitűzések.....	8
Kutatási hipotézisek megfogalmazása	8
Kutatási módszerek.....	9
1. FEJEZET: AZ ÁLLAMPOLGÁROK SZEMÉLYES ADATAINAK KEZELÉSE, AZ ÁLLAMI NYILVÁNTARTÓ RENDSZEREK BEMUTATÁSA.....	10
1.1 Fejezet: A személyes adatok általános jellemzése, azok védelmének jelentősége... 10	
1.2.fejezet: A személyes adatok szerepe az állam működése szempontjából: a személyi nyilvántartások; a közigazgatás, mint adatkezelő.....	13
1.3 fejezet: Az anyakönyvi igazgatás háttéralkalmazásai.....	14
1.3.1.fejezet: Személyi adat- és lakcímnnyilvántartó rendszer.....	14
1.3.2.fejezet: Elektronikus Anyakönyvi Rendszer.....	15
2. FEJEZET: A KÖZSZOLGÁLATI ÁLLOMÁNY, AVAGY A KÖZIGAZGATÁS HUMÁN-ERŐFORRÁSA, VALAMINT A RÁJUK VONATKOZÓ INFORMÁCIÓBIZTONSÁGI SZABÁLYOK ISMERTETÉSE.....	17
2.1. fejezet: Az anyakönyvvezetők jogállása	18
2. 2. fejezet: Információbiztonsági- tudatosság Magyarország helyi önkormányzataiban	20
2.3. Fejezet: A helyi önkormányzatok információbiztonsági előírásainak ismertetése az Ibtv. alapján.....	22
3.FEJEZET: AZ ANYAKÖNYVVEZETŐK ADAT- ÉS INFORMÁCIÓBIZTONSÁGI FELKÉSZÜLTSGÉNEK FELMÉRÉSE	27

3. 1. fejezet: A kitöltők nemének, illetve az azokkal kapcsolatos összefüggések vizsgálata	27
3.2. fejezet: Az információbiztonsággal kapcsolatos válaszok elemzése	32
4. FEJEZET: INFORMÁCIÓBIZTONSÁGI KÉPZÉSI KERETRENDSZER ANYAKÖNYVVEZETŐK SZÁMÁRA	44
4.1. fejezet: Az információbiztonsági tudatosító program jogosultságának indoklása	44
4.2 fejezet: Az információbiztonsági tudatosító program keretrendszer	49
4.3. fejezet Az információbiztonsági tudatosító program kialakítását befolyásoló tényezők	51
4.4. fejezet Az információbiztonsági tudatosító program tematikája	54
4.5. fejezet: Javaslatok a jelenlegi működési rendre vonatkozóan	58
4.5.1.fejezet: Logikai védelmi intézkedések javaslata	59
4.5.2.fejezet: Adminisztratív védelmi intézkedések javaslata	59
4.5.3.fejezet: Fizikai védelmi intézkedések javaslata	61
ÖSSZEGZETT EREDMÉNYEK	63
FELHASZNÁLT IRODALOM	64
ÁBRÁK JEGYZÉKE	66
RÖVIDÍTÉSEK JEGYZÉKE	67
FÜGGELÉKEK/MELLÉKLETEK	69
1.számú melléklet (Kérdőíves felmérés kérdései)	69
2.számú melléklet (Kérdőív kiértékelése)	70

„A közigazgatás élet és az élet szakadatlan cselekvést kíván. Cselekvést akkor is, ha a cselekvésben a tudomány nem ad útbaigazítást. Az átmeneti korok tragikuma az, hogy a tudomány régi igazságait már nem tudják használni, az újak pedig még nem állnak rendelkezésre. Az átmenet éppen ezt a tudomány irányítása nélküli bolyongás korszakát jelenti....És célunk az, hogy elősegítsük e fontos területen a tudomány új orientációját: a keresés helyett a haladás útjának megnyitását.”(Magyary Zoltán)¹

„Attól függetlenül, hogy városon vagy falun zajlik, minden ember életének közös fonala van: születés – házasság – halál.”(Ismeretlen szerző)²

¹ Zoltán Magyary, „A közigazgatás legfőbb vezetése szervezési szempontból”, *Statistikai Közlemények Budapest Székesfőváros Statisztikai Hivatala*, 1936, 4.

² Szatmár Megyei Múzeum honlapja:

<http://www.muzeusm.ro/hu/expozitii/civiliyatie-identitate-multiculturalitate/firul-vietii/>

BEVEZETÉS

A téma aktualitása

A XXI. század elején a kormányzati igazgatás jelentős változásokon ment keresztül. A közigazgatás -paradigmaváltásának eredményeként- alapvetően a szolgáltató állam képében igyekszik megfelelni a felé támasztott elvárásoknak azáltal, hogy az állampolgárok igényeit figyelembevéve alakítja, szervezi folyamatait.

Korunkat gyakran illetik az információs társadalom jelzővel, amely az információk szabad áramlásán, illetve az információk nyitottságán alapul.³ Az információs társadalom igényeinek való megfelelés, valamint az Európai Unió által is megfogalmazott követelmények hazánkban is életre keltették az e-közigazgatás intézményét. Ez alapvetően egy szemléletváltást jelentett, amely során a közigazgatás szervezetrendszerét új alapokra szervezték, miközben elkezdték rendszeresíteni az infokommunikációs eszközök használatát. Az e-közigazgatás elterjedésével elkerülhetetlenné vált az informatikai újítások és az azok nyújtotta lehetőségek alkalmazása, amely által a közigazgatás eddig külön kezelt szervezetei egy egységként képesek működni összekapcsolt rendszerek formájában, valamint ennek eredményeképp lehetővé vált, hogy a közigazgatás alkalmazkodjon a társadalom elvárásaihoz: az ügyintézés folyamata egyszerűbbé, átláthatóbbá és gyorsabbá vált. Az e-közigazgatás különböző szolgáltatásai hozzájárulnak a hatékony közigazgatáshoz.⁴ Hazánkban ez a kormányzati törekvés 2018. január 1-jével teljesedett be, amikor hivatalosan is elindult Magyarországon az elektronikus közigazgatás, amely kötelezővé tette a különböző állami szervek számára az elektronikus ügyintézés biztosítását.

Ezzel párhuzamosan -pontosabban ennek előzményeként- megkezdődött a papíralapú ügyintézés digitalizálása, vagyis elektronikussá alakítása. Ennek egyik aspektusa volt a 2014-ben bevezetett Elektronikus Anyakönyvi Rendszer (továbbiakban: EAK), amely a több, mint 100 éves papíralapú anyakönyvezés intézményét helyezte új alapokra.

Az információs társadalom korában a legnagyobb érték az adat, azon belül is a személyes adat. Tudatos felhasználóként igyekszünk becsben tartani minden velünk kapcsolatos adatot, követjük a jelszóalkotási trendeket, törekszünk azok rendszeres cseréjére, frissítünk és patchelünk. Tesszük ezt mind azért, hogy adataink, dokumentumaink, fájljaink biztonságban

³ Péter Bányász, „A közösségi média szerepe a 21. század hadseregeiben”, *Hadtudomány* 22. évfolyam, sz. 1–2: 2012.

⁴ Tamás Kaiser, „Jó Állam Jelentés 2016” (Budapest, 2016).

maradjanak, vagyis, hogy ne válhassunk egy kibertámadás célpontjává. Azonban adatainkat nem csak mi kezeljük. Az Európai Unió Általános Adatvédelmi Rendelete (továbbiakban: GDPR) garanciális biztosítékokat vezetett be annak érdekében, hogy az Európai Unió állampolgárainak adatai biztonságban legyenek, azok felhasználása szigorúan célhoz kötött és átlátható módon valósulhasson meg. Az állampolgárok felől egy jogos elvárás, hogy adataikat biztonságos módon kezeljék, tárolják, illetve azokhoz olyanok férjenek hozzá, akik megfelelnek az általuk támasztott követelményeknek. *„Az információs társadalom információbiztonsága szempontjából tehát a fő cél a kritikus információk megóvása.”*⁵

De vajon hol tart most ebben a folyamatban a hazai közigazgatás? A jogszabályi keret megteremtése és folyamatos fejlődése mellett a személyi állomány is képes volt az aktualitásokhoz való alkalmazkodásra? Diplomamunkám célja egy helyzetjelentés a jelenlegi, hazai közigazgatás működéséről, különösképpen az állami anyakönyvezésről.

A tudományos probléma megfogalmazása

Az e-közigazgatás számos lehetőség mellett, azonban számos biztonsági kockázatot is megteremtett. Az összekapcsolt rendszerként működő központi adatbázisok, valamint az azokban kezelt adatoknak a közigazgatás -funkcióiból fakadóan- nem csak használója, de tulajdonosa is lett.

A kibertámadások jelentős gazdasági, politikai, nemzetbiztonsági -és nem melleleg- a társadalom egészére is kiterjedő káros következményeket idézhetnek elő. Az elmúlt évek kibertámadással kapcsolatos tapasztalatai alapján elmondható, hogy az állami -közhatalmi- szervek és maga a közigazgatás is kiemelt célpontjaivá váltak a kibertámadásoknak. Az általam vizsgált csoport -az anyakönyvvezetők- véleményem szerint kiemelt kockázati réteg, hiszen az állam zavartalan működéséhez szükséges legtöbb állami nyilvántartáshoz jogosultsággal rendelkeznek. Az új technológiák bevezetése és alkalmazása egyben olyan biztonsági rés(ek)e)t is megteremtett, amely az anyakönyvvezetők által kezelt hatalmas mennyiségű -állampolgári- személyes adatok magas szintű védelmét feltételeznék. Tekintve az általuk kezelt adatbázisok fontosságát, felkészültnek kell(ene) lenniük az újabb és újabb kiberbiztonsági támadások, támadási alternatívák megismerésére, felismerésére, valamint az azokra való reagálásra, a hatékony védelem kialakítására.

⁵ „AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)”

Emellett nem szabad megfeledkeznünk az IoT eszközök elterjedéséről sem, ami szintén alapjaiban változtatta meg az egyének életét. Ezek használata azonban a közigazgatás személyi állományán belül -véleményem szerint szintén- biztonsági kockázatként értékelhető a felhasználói tudatosság hiányának okán. A Magyar Kormánytisztviselői és Állami Tisztviselői Kar Hivatásetikai Kódexe is kiemeli, hogy az érintettek magánéletükben sem kerülhetnek olyan helyzetbe, amely alkalmat adhat arra, hogy mások befolyásolják őket. Éppen ezért is tartom kiemelten fontosnak, hogy a közigazgatás rendelkezzen egy átfogó információbiztonsággal kapcsolatos tudatosító programmal, amely garantálni tudja annak megvalósulását, hogy a különböző technikai és technológiai újdonságok tudatos felhasználójaként, az általános kiberbiztonsági higiénia elvárásainak megfeleljenek.

Kutatási célkitűzések

Kutatásom során három célt fogalmaztam meg:

1. Célként fogalmaztam meg, hogy javaslatot teszek a kiberbiztonság területén a helyi önkormányzatok keretein belül megvalósuló állami anyakönyvvezetés működésére, az állampolgárok személyes adatainak védelme, valamint az állami élet zavartalan működésének érdekében.
2. Célként fogalmaztam meg az anyakönyvvezetők kiberbiztonsági tudatosságának és a reziliencia javításának érdekében egy információbiztonsági tudatosítási program keretrendszerét
3. Célként fogalmaztam meg az információbiztonság növelése érdekében általános működési ajánlások megfogalmazását az anyakönyvvezetők részére.

Kutatási hipotézisek megfogalmazása

Kutatásom során az alábbi hipotéziseket fogalmaztam meg:

- H1. A közszolgálati személyi állomány teljes egésze a kibertámadások potenciális célpontja.
- H2. Az anyakönyvvezetők számára szükség van egy szakmaspecifikus információbiztonsági tudatosító képzés kialakítására, megszervezésére és a gyakorlatba történő megvalósítására is.
- H3. A közigazgatásban eltöltött idő és az egyén adat-és információbiztonsági felkészültsége között nincs szignifikancia
- H4. Releváns információbiztonsági tudatosítási program hiányában, valamint az azokon megszerezhető kompetenciákat és attitűdöket kikényszerítő szabályozók hiányában a közszolgálati állomány információbiztonsággal kapcsolatos magatartása önkéntes és esetleges

lesz, amely nem feltétlen fog megfelelni az állampolgárok személyes adatainak védelmének érdekében elvárt szintnek.

Kutatási módszerek

Diplomamunkám készítése során az anyakönyvvezetők mindennapi munkavégzése kapcsán túl, vizsgáltam a szabályozottság kérdését a kiberbiztonság tekintetében. Kutatómunkám során törekedtem az elméleti összefüggések és a gyakorlati alkalmazás komplex vizsgálatára. A jelenlegi szabályozási keretet bemutató jogszabályok elemzésének fő feladata a kutatás megalapozása és az esetleges következtetések megfogalmazása volt. Dolgozatom alapját egy empirikus kutatás jelenti, amit az információbiztonsági tudatosság ötlépcsős modellje alapján végeztem kérdőív formájában. A kérdőív eredményeit statisztikai módszertan segítségével értékeltem ki keresztábra-elemzéssel, valamint Fisher- egzakt teszttel. Emellett Kruskal-Wallis tesztet végeztem.

1. FEJEZET: AZ ÁLLAMPOLGÁROK SZEMÉLYES ADATAINAK KEZELÉSE, AZ ÁLLAMI NYILVÁNTARTÓ RENDSZEREK BEMUTATÁSA

Jelen fejezetben szeretném ismertetni a személyes adatok általános jellemzőit, annak definícióját, valamint a személyes adatok védelmére vonatkozó szabályozási rendszert. Emellett szeretném felhívni a figyelmet az állami szervek -különösképp a helyi önkormányzatok- által kezelt nyilvántartórendszerek fontosságára, valamint azok információbiztonsági szabályaira az állami és önkormányzati szervek adatkezelésére vonatkozó szabályozást az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény alapján⁶ (továbbiakban: Ibtv).

1.1 Fejezet: A személyes adatok általános jellemzése, azok védelmének jelentősége

Az elmúlt évtizedben mind az európai uniós jogrendben, mind pedig a hazai jogalkotásban is egyre hangsúlyosabb szerepet kapott az állampolgárok személyes adatainak védelme. Olyannyira, hogy Magyarországon a legmagasabb szintű jogforrás, az Alaptörvény⁷ is rögzíti, hogy mindenkinek joga van a személyes adatainak a védelméhez.

A személyes adat fogalmát -hazánkban- az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Infotv.)⁸ határozza meg. A törvény értelmében személyes adat, az érintettre vonatkozó bármely információ. A jogszabály alapján az érintett pedig, a bármely információ alapján azonosított vagy azonosítható természetes személy. Ez alapján megállapítható, hogy a személyes adatok védelme természetes személyekre vonatkozó jog, aki több információ alapján azonosítható közvetlen vagy közvetett módon, úgymint a név, azonosító szám, helymeghatározó adat, online azonosító vagy egy, vagy több tényező alapján.

Az információs társadalomban a legnagyobb érték az adat, éppen ezért kiemelkedően fontos, hogyan kezeljük azokat. A GDPR is megfogalmazza, hogy a gyors technológiai fejlődés és a globalizáció új kihívások elé állította a személyes adatok védelmét. A személyes adatok gyűjtése és megosztása jelentős mértékben megnőtt. A technológia a vállalkozások és a közhatalmi szervek számára tevékenységük folytatásához a személyes adatok felhasználását

⁶ „2013. Évi L. Törvény Az Állami És Önkormányzati Szervek Elektronikus Információbiztonságáról”

⁷ „Magyarország Alaptörvénye” (2012).

⁸ „2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról”

minden eddiginél nagyobb mértékben lehetővé teszi.⁹ Vagyis, adatainkhoz nem csak mi férhetünk hozzá, hanem a különböző globális vállalkozásokon túl az állami közhatalmi szervek is. De mit is tehetünk legnagyobbnak titulált értékeink védelme érdekében?

A természetes személyek személyes adataik kezelésével összefüggő védelme alapvető jog.¹⁰ Ebből következően a magánszféra védelme alkotmányos alapjognak tekinthető, azonban mégsem tartozik az abszolút alapjogok körébe, hiszen más alapjog védelme érdekében lehetőség nyílik a korlátozására – például a közbiztonság védelme jegyében.¹¹ Magánszféránk védelmének tartalmi oldalát az információs önrendelkezési jog képezi, amely az érintett azon képessége, amellyel megadja, vagy éppen megtagadja az adatkezeléshez való hozzájárulást.

Ez a jogunk garantálja, hogy adataink kezelése célhoz kötötten, átlátható módon történjen és kizárólag azok férhessenek hozzá, akiknek erre engedélyük, felhatalmazásuk van. A GDPR hatálya kiterjed az online -vagyis a kibertérben végzett- tevékenységeinkre is. A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.¹² Az adatkezelők kötelezettségei megsokszorozódtak, ma már -a kibertérben- szinte lehetetlen a weboldalak elérése anélkül, hogy rendelkezünk a sütik (cookie-k) engedélyezéséről -vagy azok felhasználásának korlátozásáról-, illetve, hogy regisztrációnk során ne fogadjunk el adatkezelési nyilatkozatot. Azonban a közhatalmi szervek vonatkozásában, ügyeink intézése során nem írunk alá Adatvédelmi Nyilatkozatot. Éppen ezért születtek meg az információbiztonsági szabályzatok, a helyi önkormányzatok és az állami szervek esetében kötelező jelleggel.

Az információbiztonság(i szabályzatok) célja az elektronikus információs rendszerekben tárolt adatok védelme a bizalmasság, sértetlenség és a rendelkezésre állás kritériumainak megfelelően (CIA-elv)¹³.

Az e-közigazgatás elterjedésével a közigazgatásban megindult a digitalizáció, aminek hatására

⁹ AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet).

¹⁰ AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet).

¹¹ Péter Bányász, *Közösségi média és közszolgálat* (Budapest: Nemzeti Közszolgálati Egyetem, 2018).

¹² 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

¹³ nem a Központi Hírszerző Ügynökség

a papíralapú adatkezeléssel szemben elsődlegessé vált az elektronikus adatkezelés: a közigazgatás elektronikus információs rendszerekbe kezdte kezelni adatait. Az állami élet zavartalan működése szempontjából az közigazgatási szervek által kezelt-elektronikus információs rendszerek -illetve az azokban tárolt, kezelt adatok-nélkülözhetetlenek. A kibertér tehát egyértelmű előnyt hordoz magában az állampolgárok és az állam interakcióinak viszonyában is.¹⁴

A bizalmasság garantálja, hogy az elektronikus információs rendszerben tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.¹⁵ A sértetlenség az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható.¹⁶ A rendelkezésre állás pedig annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.¹⁷

Mindezek alapján elmondható, hogy a személyes adataink védelme nem csak saját felelősségünk, hanem az azokat kezelő globális vállalatok és állami közhatalmi szerveké is. Információs önrendelkezési jogunk garantálja, hogy rendelkezessünk ezek felhasználásának, kezelésének korlátozásáról, azonban az állam által kezelt elektronikus információs rendszerek esetében ez a jogunk kevésbé gyakorolható. Jelenleg az utóbbi esetben bízunk kell az állami adatkezelés jogszabály szerinti működésében.

¹⁴ László Kovács, *A kibertér védelme* (Budapest: Dialóg Campus, 2018).

¹⁵ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

¹⁶ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

¹⁷ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

1.2.fejezet: A személyes adatok szerepe az állam működése szempontjából: a személyi nyilvántartások; a közigazgatás, mint adatkezelő

„Az anyakönyvektől is – miként minden nyilvántárást illetően – azt követeljük, hogy olyanok legyenek, mint a jó tükrök, mely tisztán és hiven mutatja a valóságot, összes és jellemző tulajdonságaival együtt.”¹⁸

A személyi nyilvántartások iránti –uralkodói- igény már az ókorban felmerült. Ekkoriban a személyi nyilvántartások egyrészt az állami adóztatáshoz, pontosabban az adóalanyok számáról tájékoztatta az államot, emellett pedig a hadsereg felállításához is segítséget nyújtott. A középkorban már a katolikus egyház is felismerte a személyi nyilvántartások jelentőségét. IV. Pius pápa 1563-ban, a Tridenti-zsinaton rendelte el az egyházi anyakönyvezés bevezetését. Ahogyan az ókorban vezetett állami személyi nyilvántartások segítették az állam működését, úgy az egyházi felekezetek által vezetett személyi nyilvántartások is megbízható adatot biztosítottak a felekezet számára híveikről. Ez azért volt fontos, mert a hívek jelentős mennyiségű adót fizettek, illetve szolgáltatottak termény formájában az adott egyházi felekezetnek. Az egyház által vezetett anyakönyvek ezáltal lehetővé tették az egyház számára adót fizetők nyilvántartását, miközben akarva- akaratlanul megalapozták az anyakönyvvezetés alapjait.¹⁹

A személyi nyilvántartások képezik az állam működésének alapját. Ahhoz, hogy egy kormányzat hatékonyan legyen képes ellátni funkcióját, megbízható információkra van szüksége, hiszen ezekből tud olyan döntéseket meghozni, ami a társadalom javát szolgálja. Éppen ezért a kormányzatok mindig is törekedtek arra, hogy minél szélesebb körből legyenek képesek információt gyűjteni, és igyekeztek kiterjeszteni a megfigyeléshez kapcsolódó képességüket – mind technikai-technológiai, mind szabályozási oldalról.²⁰ Többek között a titkosszolgálatok ereje is a nyilvántartásokba rejlik, de napjainkban az is elképzelhetetlen lenne, hogy az állam -pontosabban az állami szervezetek például a NAV- ne tudná a nyilvántartásai alapján kinek mely kötelezettségei vagy éppen jogosultságai vannak az állam felé vagy éppen az államtól. Ebből kifolyólag mondhatjuk, hogy hazánk legnagyobb adatkezelője az állam.

¹⁸ József Dolencz, *Az anyakönyvek államosítása* (Budapest: Grill Károly CS. és Kir. Udv. Könyvkereskedése, 1893).

¹⁹ Dorina Barbara Szabó, „A képviselő-testület szervezetalakítása, szabadsága és annak korlátai, különös tekintettel az anyakönyvi hivatalra” (Budapest, Nemzeti Községi Szolgálati Egyetem, 2020).

²⁰ Bányász, *Közösségi média és községi szolgálat*.

Adatkezelésnek nevezzük a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely műveletet vagy műveletek összességét, így a gyűjtést, rögzítést, rendszerezést, tagolást, tárolást, átalakítást vagy megváltoztatást, lekérdezést, betekintést, felhasználást, közlést, továbbítást, terjesztést vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolást vagy összekapcsolást, korlátozást, törlést, illetve megsemmisítést.²¹

1.3 fejezet: Az anyakönyvi igazgatás háttéralkalmazásai

Jelen alfejezetben szeretném ismertetni az általam választott csoport, az anyakönyvvezetők által kezelt nyilvántartásokat, amelyek nélkülözhetetlen szerepet töltenek be az anyakönyvi eljárások intézése során.

1.3.1.fejezet: Személyi adat- és lakcímnyilvántartó rendszer

A közigazgatási tevékenységek alanya a nyilvántartott személy. A népesség-nyilvántartási rendszerek nélkül elképzelhetetlen lenne bármely hatóság vagy közigazgatási szerv feladatellátása, hiszen minden önkormányzati, illetve államigazgatási feladat ellátás alanya a nyilvántartott személy. Az állami nyilvántartó rendszerekkel szemben támasztott követelmény az aktualitás, naprakészség. Hatékonysági okokból így a nyilvántartó rendszerek kezelése nem központi, hanem alsóbb (megyei, járási) szinteken valósul meg, illetve sok esetben a helyi önkormányzatok gondoskodnak azok kezeléséről.

Az ENSZ Statisztikai Bizottsága 1956-ban tette kötelezővé a tagországaiban a népesség-nyilvántartó rendszerek működtetését. Magyarországon manuálisan 1974-ben indult el az állampolgárok nyilvántartása. Már ekkor is jelentős szerepe volt az anyakönyveknek, hiszen az állampolgárok összeírásának alapját az anyakönyvi bejegyzések képezték. 1975-ig megtörtént az állampolgárok összeírása, amely biztosította egy közhiteles rendszer felállításának alapjait. A népesség-nyilvántartás segédeszköze a személyi szám lett, amelyből kitűnik az állampolgár születési dátuma, illetve neme is. 1986-ban indult el a személyi adat- és lakcímnyilvántartó rendszer (továbbiakban: SZL- nyilvántartás). Az anyakönyvvezetők jogosultak, mi több kötelesek minden olyan változást rögzíteni (születés, családi állapot változás, elhalálozás) amely tudomásukra jutott, ezzel biztosítva a rendszer közhitelességét, aktualitását. Az állampolgárok személyes adatainak védelme érdekében minden SZL-nyilvántartásban végzett

²¹ AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet).

keresést indokolni kell, amire a keresés indításával párhuzamosan kerül sor, jellemzően a keresést indokoló anyakönyvi folyószám ismertetésével.²²

1.3.2.fejezet: Elektronikus Anyakönyvi Rendszer

Magyarországon az e-közigazgatás kialakításának egyik fő aspektusaként, a Magyar Zoltán Közigazgatás-fejlesztési Program részeként valósult meg elektronikus anyakönyvezés. Az induláshoz szükséges feltételeket az Anyakönyvi eljárásról szóló 2010. évi I. törvény (továbbiakban: Aktv.) teremtette meg. E törvény alapján az EAK 2014. július 1-jén kezdte meg működését. A törvény értelmében, 2014. június 30-án a papíralapú anyakönyveket lezárták, azokba új esemény nem rögzíthető. Az EAK működéséért a Belügyminisztérium háttérintézményeként működő Nemzeti Infokommunikációs Szolgáltató Zrt (továbbiakban: NISZ), mint nyilvántartó szerv felelős, míg az adatfeldolgozó és az üzemeltető IdomSoft Informatikai Zártkörűen Működő Részvénytársaság. Kiemelendő, hogy az anyakönyvvezetők csupán végponti felhasználói a rendszernek.

A papíralapú nyilvántartás alapvetően eseményközpontú nyilvántartás volt, az EAK azonban már személyközpontú nyilvántartás, amely határidő nélkül tartja nyilván a nyilvántartás alanyának személyazonosító adatait, valamint a személyazonosító adatokhoz rendelt az alany anyakönyvi eseményeit. Aki a nyilvántartásba kerül, azt a rendszer egy egyedi azonosítóval, úgynevezett EAK azonosítóval látja el. Törvényi előírás, hogy minden nyilvántartásba vett személy csak egy EAK azonosítóval rendelkezhet a nyilvántartás átláthatóságának érdekében. Emellett a bejegyzett anyakönyvi eseményeknek is saját azonosítója van, amit EAK eseményazonosítónak nevezünk. Az EAK rendszernek köszönhetően az ország bármely pontján lévő hivatalban lehetőség van az egyes anyakönyvi eljárások intézésére, anyakönyvi események rögzíttetésére, kérelmek benyújtására. Ebben a tekintetben megszűntek a területi korlátok, az ügyfél bármely települési anyakönyvvezetőnél jogosult ügyet indítani, nem csupán az adott anyakönyvi esemény szerinti illetékes anyakönyvvezetőnél, ahogy az korábban, a rendszer bevezetése előtt szükséges volt.

Az EAK rendszer lehetőséget biztosít arra, hogy azon személyek, akik egymás anyakönyvi bejegyzéseiben érintettek automatikusan megjelennek egymás anyakönyvi bejegyzéseiben. Vagyis, egy gyermek születésekor, annak szülei is rögzítésre kerülnek az EAK-rendszerben. Amennyiben a gyermek házasságban élő szülő gyermeke, úgy a szülők házassága, ellenkező

²² Szabó, „A képviselő-testület szervezetalakítása, szabadsága és annak korlátai, különös tekintettel az anyakönyvi hivatalra”.

esetben az apai elismerő nyilatkozat is rögzítésre kerül. Ezzel párhuzamosan a gyermek születése, mint anyakönyvi esemény a szülők bejegyzéseiben is megjelenik. A rendszer e funkciójának köszönhetően a jövőben családok, generációk történelme lesz felkutatható egy-egy anyakönyvi bejegyzés segítségével. Fontos kiemelni, hogy az EAK rendszer közvetlen hozzáférést biztosít az SZL-keresőhöz, amelynek segítségével a személyazonosító adatok átemelhetők az EAK rendszerbe. Vagyis, az EAK és az SZL esetében összekapcsolt, interdependenciában lévő rendszerekről beszélünk. Információbiztonsági szempontból így kiemelten fontos lenne az anyakönyvvezetők tudatos felhasználásán túl a különböző védelmi intézkedések megvalósítása is.

Fontos kiemelni, hogy a rendszer elindításának nem volt előfeltétele a papíralapú anyakönyvek eseményeinek rögzítése, vagyis 2014. július 1-jén egy üres, események nélküli adatbázis kezdte meg működését. A papíralapú anyakönyvekben található események rögzítése azóta is folyamatban van, külön ügyként szerepel az EAK rendszerben. Vagyis, a papíralapú anyakönyvek bizonyos esetekben még mindig az anyakönyvi eljárások részét képezik. Bár már ezekbe az anyakönyvekbe új bejegyzés nem jegyezhető, a papíralapú anyakönyvből az elektronikus anyakönyvbe történő rögzítést az utólagos bejegyzés rovatban fel kell tüntetni, és „*Az elektronikus anyakönyvben rögzítve.*” szöveggel le kell zárni. A bejegyzést a bejegyzés dátumával és a bejegyző aláírásával kell ellátni, továbbá a betűrendes névmutatóban is fel kell tüntetni.

A fentiek alapján az anyakönyvvezetők hozzáférése kettős: egyrészt hozzáférnek a papír alapú nyilvántartásokhoz, másrészt pedig az állami nyilvántartó rendszerekhez. Ezekben az esetekben a hozzáférés magában foglalja az egyes nyilvántartási rendszerek adattartalmának megismeréséhez való jogot is.²³

Összefoglalva, az állam -mint adatkezelő- számára nélkülözhetetlenek a központi nyilvántartórendszerek, amelyek az állampolgárok személyes adataiból épülnek fel. Éppen ezért ezen nyilvántartórendszerek kezelése, kiemelt fontosságú, főleg az egymással interdependenciában lévő rendszerek esetében. A nyilvántartórendszerek közül kiemelkedik az EAK, amely egy közel 120 éves eljárás digitális alternatívájaként jelent meg és vált az anyakönyvvezetők munkavégzésének legfőbb elemévé.

²³ Szabó.

2. FEJEZET: A KÖZSZOLGÁLATI ÁLLOMÁNY, AVAGY A KÖZIGAZGATÁS HUMÁN-ERŐFORRÁSA, VALAMINT A RÁJUK VONATKOZÓ INFORMÁCIÓBIZTONSÁGI SZABÁLYOK ISMERTETÉSE

Ebben a fejezetben szeretném bemutatni a közszerolgalati állományt, annak működését kiemelt hangsúlyt fektetve a dolgozatom fókuszcsortját képező anyakönyvvezetőkre, valamint a rájuk vonatkozó információbiztonsági előírásokra.

2.1 Fejezet: A közigazgatás személyi állományára vonatkozó jogállási törvények

A közszerolgalati jogviszony alapvető jellemzője, hogy az egyik jogalany minden esetben az állam, míg a másik a közszerolgalati dolgozó. Vagyis egy, a munkavégzés céljából létesített különleges jogviszony, amely alapvetően többletjogokkal, de emellett többletkötelezettségekkel is rendelkezik.

A közszerolgalatban való alkalmazás olyan alapvető állampolgári jog, amely hazánkban is alkotmányi szinten kerül deklarálásra. Az Alaptörvény XXIII. cikk (8) bekezdésének rendelkezése szerint: „Minden magyar állampolgárnak joga van ahhoz, hogy rátermettségének, képzettségének és szakmai tudásának megfelelően közhivatalt viseljen.”²⁴ Vagyis, a közhivatal viseléséhez való jog, alapjog minden magyar állampolgár számára.

A közigazgatásban dolgozók jogállását korábban, a közszerolgalati tisztviselőkről szóló 2011. évi CXCI. törvény (továbbiakban: Kttv) rendezte. 2019. január 1-jétől, azonban egy új jogszabály hatálybalépésével a közszerolgalati állomány két részre bomlott. Amíg a Kttv hatálya a helyi önkormányzat képviselő-testületének polgármesteri hivatala, közterület-felügyelete, a közös önkormányzati hivatala köztisztviselőjének és közszerolgalati ügykezelőjének közszerolgalati jogviszonyára, a VII/A. Fejezet rendelkezései szerint a polgármesterre és az alpolgármesterre, továbbá a Kormány által intézményfenntartásra kijelölt szerv kormánytisztviselőjének és kormányzati ügykezelőjének kormányzati szolgalati jogviszonyára terjed ki²⁵, addig ezzel szemben a kormányzati igazgatásról szóló 2018. évi CXXV. törvény (továbbiakban: Kit) kormányzati igazgatási szervek tisztségviselőinek szolgalati jogviszonyát²⁶ rendezi. A Kit megalkotásakor a jogalkotó céljai között szerepelt, a közigazgatásban dolgozók anyagi

²⁴ Magyarország Alaptörvénye.

²⁵ 2011. évi CXCI. törvény a közszerolgalati tisztviselőkről

²⁶ 2018. évi CXXV. törvény a kormányzati igazgatásról

megbecsültségén javítása, egy hatékonyabb kormányzati igazgatási szervezetrendszer kialakítása, valamint a közszolgálat és a családi élet összeegyeztethetőségének elősegítése.

Fontos különbség, és a témám szempontjából kiemelendő, hogy a két jogállási törvény alapjaiban tér el egymástól, hiszen a Kttv. egy zárt, míg a Kit. egy nyitottabb közigazgatási életpályamodellt vázol fel. Véleményem szerint mindkét pályamodell védelmi szempontból egyenértékű, nem tudom határozottan kijelenteni melyik biztonságosabb az információbiztonság tekintetében. Hiszen, amíg a Kttv. esetében a tisztviselőktől egy élethosszig tartó hivatás az elvárt, amely által a szakmaiság és a felhalmozódott tapasztalat kétségtelen, addig előfordulhat, hogy az idő előrehaladtával, a technológiai kihívásokat nem követve könnyebb célponttá válhat az, aki régebb óta a pályán van. Egyrészt, az előmeneteli rendszer is feltételezheti ezt, hiszen minél több időt tölt valaki a közigazgatásban, annál magasabb beosztást tölthet be, amivel párhuzamosan a hozzáférési jogosultságai is tágabbak lehetnek. Másrészt, a közigazgatásban eltöltött évek -főleg ebben a jogviszonyban- egyfajta kényelmet, kvázi biztonságérzetet nyújt a hosszabb ideje pályán lévők számára. Ebből kifolyólag, bezárva a közigazgatás burkába, a monoton munkavégzés során, nem érintkezve mindennap biztonsági kihívásokkal könnyen előfordulhat, hogy már az olyan alapelvek, mint például a tiszta asztal politikája is feledésbe merül -amennyiben ismerik azt.

A Kit. ezzel szemben egy nyitottabb pályát vázol fel, lehetőséget biztosítva a fiatalabb generációknak, vagyis a pályakezdőknek is. Az előmenetel esetében nem mérvadó a közigazgatásban eltöltött évek száma, így könnyen előfordulhat, hogy egy fiatalabb kerül vezető pozícióba egy idősebb -a Kttv. szemléletében egy tapasztaltabb- kollégával szemben. A legfontosabb különbség azonban, hogy ez a nyílt modell nem vár el élethosszig tartó közszolgálatot, vagyis előfordulhat, hogy valaki olyan rövid időt tölt a köz szolgálatában, hogy nem alakul ki benne a hivatástudat, vagy az ügyfelek és a szervezet iránti elkötelezettség.

2.1. fejezet: Az anyakönyvvezetők jogállása

A továbbiakban a helyi önkormányzatok tisztviselőivel, azon belül is az anyakönyvvezetőkkel szeretnék foglalkozni. A fentiek alapján megállapítható, hogy az anyakönyvvezetők jogállásukat tekintve -a dolgozat írásakor- a Kttv. hatálya alá esnek. Az anyakönyvvezetők által végzett közigazgatási feladatellátás rendkívül speciális, hiszen alapvetően egy állami feladatellátást valósítanak meg a helyi önkormányzatok falain belül. A számukra előírt képesítési feltételeket a közszolgálati tisztviselők képesítési előírásairól szóló 29/2012. (III. 7.) Korm. rendelet tartalmazza.

A kormányrendelet értelmében két besorolási osztály különböztetünk meg. I. besorolási osztályba tartoznak azok az anyakönyvvezetők, akik felsőfokú szakképzettséggel és anyakönyvi szakvizsgával rendelkeznek, II. besorolási osztályba pedig a középfokú végzettséggel és anyakönyvi szakvizsgával rendelkezők. A besorolási osztályokon belül besorolási fokozatokat különböztetünk meg. Az I. besorolási osztályba tartozik a gyakornoki, forgalmazói, tanácsosi, vezető tanácsosi, főtanácsosi és a vezető főtanácsosi fokozat. A II. besorolási osztályon belül gyakornoki, előadói, főelőadói és főmunkatársi fokozatokat különböztetünk meg. A besorolási osztályokon belül a köztisztviselő abban az esetben tud előrelépni, ha megszerzi a felsőfokú végzettségét. A fokozatok jelentősége, hogy a fokozatokhoz tartozó szorzószámmal kerül megállapításra a tisztviselő illetménye. Minél magasabb a besorolási fokozat annál nagyobb a hozzá tartozó szorzószám. Vagyis, a köztisztviselő illetménye az illetményalap (38.650.- Ft), valamint az egyes fokozatokhoz tartozó szorzószám szorzataként állapítható meg.

A besorolási fokozatok között az előmenetelnek több feltétele is van.

1. a következő besorolási fokozat eléréséhez szükséges a várakozási idő letelte,
2. az előírt szakmai követelmények teljesítése,
3. a jogszabályban előírt feltételek teljesítése,
4. legalább „megfelelő” minősítés,
5. a közigazgatási szerv által meghatározott feltételek teljesítése²⁷

Az anyakönyvi szakvizsga nélkülözhetetlen ahhoz, hogy valaki anyakönyvvezetőként dolgozzon. A tanfolyamon belül 100 órás gyakorlati és 60 órás elméleti képzésen kell részt venniük a leendő anyakönyvvezetőknek. A tanfolyam egy elméleti és egy gyakorlati vizsgával zárul. A szakvizsga sikeres teljesítése mellett a Kttv. előírja, hogy a helyi önkormányzat képviselő-testületének polgármesteri hivatalában, közterület-felügyeletében, a közös önkormányzati hivatalban foglalkoztatott köztisztviselőknek (...) közigazgatási szakvizsgával kell rendelkezniük.²⁸

²⁷ „29/2012 (III.7.) Korm. rendelet a közszolgálati tisztviselők képesítési előírásairól”

²⁸ „Kttv. - 2011. évi CXCV. törvény a közszolgálati tisztviselőkről

2. 2. fejezet: Információbiztonsági- tudatosság Magyarország helyi

önkormányzataiban

Az információbiztonsági-tudatosság (továbbiakban: ISA) úgy definiálható, mint az alkalmazott egyéni felfogása a saját információbiztonsági tudásáról és a szervezetének információbiztonsági politikáinak ismeretéről.²⁹ Azáltal, hogy az emberek döntéseket hoznak és felelősséget vállalnak, az emberi tényező jelentős mértékben hozzájárul az információbiztonság aspektusához.³⁰ Az ISA azért is kiemelten fontos, mert ennek szintje határozza meg, hogy az adott szervezet mennyire hatékonyan tudja megvédeni információs vagyonát.

Egy 2014-es felmérés szerint-amely a SANS kérdőív alapján zajlott-, az önkormányzatok és az önkormányzati tulajdonú profitorientált szervezetek egyes tagjai nincsenek tisztában a biztonsági alapelvekkel és veszélyekkel, sem pedig munkaszervezetük biztonsági szabályzatával.³¹

Alapvetően 1-5-ig tartó skálán az önkormányzatok az utolsó előtti helyen végeztek. Emellett a fent említett kutatás 2014-ben kimondta, hogy az önkormányzatoknál dolgozók ötödének szintén továbbképzésre volna szüksége az információbiztonság-tudatosság területén.

A kutatás eredményeként elmondható, hogy alacsony színvonalúnak volt mondható az információbiztonság-tudatosság a közszférában az önkormányzati tulajdonú nonprofit szervezeteknél. Azok a munkavállalók tartoznak ide, akik részben tisztában vannak a veszélyekkel és az esetek túlnyomórésztében tudják, hogy bizonyos biztonsági alapelveket be kellene tartaniuk, de továbbképzésre szorulnak a témában. Egyesek nincsenek tisztában a biztonsági alapelvekkel és veszélyekkel, sem pedig munkaszervezetük biztonsági szabályzatával. Az itt dolgozók harmada nem venné észre, hogy a számítógépét feltörték, tizede odaadta céges jelszavát másnak, az alkalmazottak harmada nem elégedett a korábbi képzésekkel, tizede pedig nem tudja, mi az a spam, és nem tudja megmondani, hogy van-e telepítve víruskereső program a számítógépén. A harmada meg van győződve arról, a számítógépén tárolt adatok nem értékesek a hackerek számára, sokan közülük nem hallottak a felhő szolgáltatásokról, harmada céges adatokat tárol a mobiltelefonján, fele személyes fájlok

²⁹ Rocha Flores W, Ekstedt M. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security* 2016;59:26–44.

³⁰ Rocha Flores W, Ekstedt M. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security* 2016;59:26–44..

³¹ András Nemeslaki és Péter Sasvári, „Az információbiztonság-tudatosság empirikus vizsgálata a magyar üzleti és közszférában”, *Infokommunikáció és jog* 11. évfolyam, sz. 4 (2014): 169–77.

letöltésére is használja a munkahelyi számítógépét. A szervezetek felénél nincs informatikai biztonsággal foglalkozó részleg, kétharmadánál nincs előírás a levelezőrendszer használatára és szabály a weboldalak látogatására. Mint említettem ez a kutatás 2014-ben készült. Pontosan abban az évben, amikor bevezetésre került az Elektronikus Anyakönyvi rendszer. Ez a témám szempontjából azért is megkérdőjelezhető, mert Kárpáti Orsolya szerint 3 tényező biztosítja az EAK rendszer adatvédelmi és adatbiztonsági követelményeknek megfelelő működését. Ez a 3 tényező a t a megfelelő szabályozás, az informatikai biztonság gyakorlati megvalósulása és a tudatos felhasználók.³² Elgondolkodtató, hogy ilyen visszajelzések alapján mi indokolta a rendszer bevezetését, miért nem előzte meg azt egy információbiztonsági tudatosító program, amely jelen tanulmány alapján indokolt lett volna, illetve figyelembe véve azt a tényt, hogy a biztonsági incidensek legtöbb esetben a biztonságtudatosság hiánya miatt következnek be.

A tanulmány felmérései alapján 7 évvel digitális gazdaság és társadalom fejlettségét mérő 2021. évi mutató (DESI) alapján Magyarország a 27 uniós tagállam közül még mindig a 23. helyen áll.³³

A kutatás eredményeinek összefoglalásaként megállapítom, hogy az anyakönyvvezetők olyan elektronikus információs rendszerekhez rendelkeznek hozzáféréssel, illetve kezelik azokat - ebbe beleértve az adatok rögzítését, azok módosítását, illetve törlését is-, amelyek rendkívül fontos szerepet töltenek be az állami adminisztráció tekintetében. Teszik mindezt úgy, hogy az adat- illetve információbiztonsággal, az azokra való előírásokkal a pályára lépéshez szükséges szakvizsga során sem érintkeznek.

³² Orsolya dr. Kárpáti, „Az elektronikus anyakönyvezés helye és szerepe a magyar közigazgatásban” (PhD értekezés, Miskolc, 2020).

³³ A digitális gazdaság és társadalom fejlettségét mérő mutató (DESI), 2021

2.3. Fejezet: A helyi önkormányzatok információbiztonsági előírásainak ismertetése az Ibtv. alapján

Általánosságban elmondható, hogy az Ibtv. alapjaiban változtatta meg az állami szervek és helyi önkormányzatok működését, illetve az adatkezelésre vonatkozó szabályait. Új szabályozók jelentek meg a szervezetek életében, amelyek célja az adat-és információbiztonság garantálása az állami ügyintézés során. Jelen alfejezetben az általam választott csoport, az anyakönyvvezetők feladatellátásának helyet adó helyi önkormányzatokra vonatkozó jogszabályi előírásokat szeretném röviden ismertetni.

A helyi önkormányzatok elektronikus információs rendszereiben kezelt adatok és információk tekintetében, az Ibtv három kulcsfontosságú alapelvet követel meg, mégpedig a bizalmasság, sértetlenség és rendelkezésre állás köré. Annak érdekében, hogy a helyi önkormányzatok által használt és kezelt elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs rendszereket be kell sorolni egy-egy biztonsági osztályba bizalmasság, sértetlenség és rendelkezésre állás szempontjából.³⁴

Összességében, az Ibtv. két nagyon fontos folyamatot különít el: a biztonsági szintbe, valamint a biztonsági osztályba sorolást. A biztonsági osztályba sorolás alkalmával - az érintett elektronikus információs rendszer vagy az általa kezelt adat bizalmasságának, sértetlenségének vagy rendelkezésre állásának kockázata alapján - 1-től 5-ig számozott fokozatot kell alkalmazni, a számozás emelkedésével párhuzamosan szigorodó védelmi előírásokkal együtt.³⁵ A biztonsági osztályba sorolást a szervezet vezetője hagyja jóvá- helyi önkormányzatok esetében a jegyző-, és felel annak a jogszabályoknak és kockázatoknak való megfeleléséért, a felhasznált adatok teljességéért és időszerűségéért. A biztonsági osztályba sorolást a szervezet informatikai biztonsági szabályzatában kell rögzíteni.³⁶ Az elektronikus információs rendszere biztonsági osztályba sorolásakor az elektronikus információs rendszerben kezelt adatok bizalmasságának, sértetlenségének és rendelkezésre állásának követelményeit a rendszer funkcióira tekintettel, és azokhoz igazodó súllyal érvényesíti, jelen esetben a nemzeti adatvagyonot kezelő rendszerek esetében a sértetlenség követelményét emeli ki.³⁷

³⁴ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

³⁵ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

³⁶ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

³⁷ „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”

Emellett, a kockázatokkal arányos, költséghatékony védelem kialakítása érdekében a szervezetet az elektronikus információs rendszerek védelmére való felkészültsége alapján a szervezetnek biztonsági szintekbe kell sorolni a jogszabályban meghatározott szempontok szerint.³⁸

Az elektronikus információs rendszerrel rendelkező szervezetek biztonsági szintjének kezdeti kötelező besorolása a szervezeteket olyan biztonsági követelmények elé állította, amelyek végrehajtása a teljes szervezetre nézve esetenként indokolatlan volt és aránytalan terhet jelentett, ezért 2015-ben módosították a rendelkezést. A törvénymódosítás előtt a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói, az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemek esetén legalább az 5. biztonsági szint volt az elvárt. 5. biztonsági szintként kell megállapítani, ha az érintett szervezetnél van 5. biztonsági osztályba sorolt rendszer.³⁹ Az új szabályozás értelmében azonban ez megszűnt, ezért is van lehetőség a helyi önkormányzatok számára eltérő biztonsági szintek megállapítására. Tekintve, hogy a 3-as biztonsági szint is csupán akkor kötelező, ha az érintett szerv a szakfeladatait támogató elektronikus információs rendszert használ, de nem üzemelteti azt, így megállapítható, hogy az a szervezet, amely központi szolgáltatótól veszi igénybe az elektronikus információs rendszerek szolgáltatásait annak alacsonyabb lesz a biztonsági szintje, mint annak, aki önállóan üzemelteti azokat. A módosított szabály lehetővé tette, hogy az elektronikus információs rendszer fejlesztését vagy üzemeltetését végző, illetve üzemeltetéséért vagy információbiztonságáért felelős szervezeti egységeit a szervezettől elvárt, eltérő biztonsági szintekbe lehessen sorolni. Ez a szabály könnyebb végrehajtást eredményezett a szervezetek részére, és biztosította, hogy az elvárt védelemi intézkedések megvalósítására ott kerüljön sor, ahol azt a kockázatok indokolják, úgy, hogy a szervezet védelemre való felkészültsége továbbra is az irányadó legyen.⁴⁰ Ebből kifolyólag, míg korábban az Ibtv. minimum követelményként legalább 2-es biztonsági osztályba sorolta a helyi önkormányzatokat, valamint azok társulásait, ma már erről saját hatáskörben dönthetnek. Ez azt eredményezte, hogy bár azonos rendszereket használnak minden helyi önkormányzatban, mégis eltérő besorolást tapasztalhatunk a különböző helyi önkormányzatok Informatikai Biztonsági Szabályzatában (továbbiakban: IBSZ).

³⁸ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

³⁹ Bodó: Információbiztonsági jogi ismeretek vezetőknak

⁴⁰ Bodó: Ibtv gyakorlata

Az IBSZ jogszabály alapján előírt szabályzat⁴¹, amely többek közt tartalmazza a szervezet biztonsági szintbe- illetve osztályba sorolását, valamint mindazon előírásokat, amelyek az adott szervezet vonatkozásában az infokommunikációs eszközök rendeltetésszerű és biztonságos használatához szükségesek. Vagyis, egy jogszabály által előírt szabályzat, amelyben meg kell határozni a célokat, a szabályzat tárgyi és személyi (a szervezet jellegétől függően területi) hatályát, az elektronikus információbiztonsággal kapcsolatos szerepköröket, a szerepkörhöz rendelt tevékenységet, a tevékenységhez kapcsolódó felelősséget, az információbiztonság szervezetrendszerének belső együttműködését.⁴² A törvény értelmében minden helyi önkormányzatnak meg kell bíznia vagy ki kell neveznie egy személyt, aki az elektronikus információs rendszer védelméért, valamint a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért felelős.⁴³

Az anyakönyvvezetők munkavégzésük során adatkezelőként végzik az állampolgárok adatainak kezelését. Teszik ezt azért, hogy az állam naprakész alapnyilvántartásokkal rendelkezzen, amelyek a későbbiekben kerülnek ismertetésre. Visszaulva a korábbiakra, olyan elektronikus információs rendszerekhez férnek hozzá, valamint rendelkeznek azokban nem csak az olvasás, de az írás képességével is, amelyek nélkülözhetetlenek az állam megszokott működésének szempontjából.

Ibtv már a preambulumban kiemeli, hogy a nemzet érdekében kiemelten fontos - napjaink információs társadalmát érő fenyegetések miatt - a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon. A nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról szóló 38/2011. (III. 22.) Korm. rendelet értelmében az anyakönyvvezetők által kezelt EAK a nemzeti adatvagyon része.

Általánosságban elmondható, hogy a helyi önkormányzatok IBSZ-e nem egységes. Maradva a korábbi szabályozásnál, a legtöbb önkormányzat mai napig 2-es biztonsági szintbe sorolással rendelkezik.

Ha a korábbi szabályozás lenne érvényben -vagyis a nemzeti adatvagyon okán az 5-ös biztonsági szint lenne érvényes az anyakönyvvezetőkre- több kritérium sem teljesülne, amely véleményem szerint jelenleg szabályozás mellett is szükséges lenne.

⁴¹ Nagyné Takács Veronika, „Hogyan írjunk informatikai biztonsági szabályzatot?”, *Hadmérnök* 14, sz. 3 (2019): 113–28, <https://doi.org/10.32567/hm.2019.3.10>.

⁴² 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

⁴³ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

Ilyen feltétel, hogy

- a szervezetnek rendelkeznie kell átfogó információbiztonsági programmal, amely szerves része a szervezet feladatellátásnak és biztosítja a személyi állomány biztonság tudatosságának növelését;
- a szervezet személyi állományának rendelkeznie kell információbiztonsági operatív képességgel és a feladat elvégzéséhez szükséges szaktudással;
- a biztonsági sérülékenységek felismerésének és kezelésének képességét a szervezet egésze tekintetében meg kell valósítani;⁴⁴

Jelenleg, a 41/2015 (VII.15.) BM rendelet értelmében 5-ös biztonsági osztályba kell sorolni azokat az elektronikus információs rendszereket, melyek esetében kiemelkedően nagy káresemény következhet be, mivel a nemzeti adatvagyon helyreállíthatatlanul megsérülhet, valamint az ország, a társadalom működőképességének fenntartását biztosító létfontosságú információs rendszer rendelkezésre állása nem biztosított; illetve a lehetséges társadalmi-politikai hatás: súlyos bizalomvesztés az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek.⁴⁵ Az EAK a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról szóló 38/2011. (III. 22.) Korm. rendelet értelmében nemzeti adatvagyonnak minősül. Emellett, egy esetleges támadás, amely érintené az anyakönyvvezetők által szinte legtöbb folyamatban használt SZL nyilvántartás⁴⁶ -amely egyébként össze van kapcsolva az EAK-kal- veszélyeztetné az országot, a társadalom működőképességének fenntartását. Ezáltal egy sikeres kibertámadás pedig súlyos bizalomvesztéssel járna az állampolgárok részéről, amely veszélyeztetné hazánk demokratikus berendezkedését is. Az adatok védelme érdekében az Ibtv. a helyi önkormányzatoktól az alábbiakat várja el. Meg kell bízni, vagy ki kell jelölni az elektronikus információs rendszer biztonságáért felelős személyt.

Meg kell határozni a szervezet elektronikus információs rendszerei védelmének felelőseire (továbbiakban: IBF), feladataira és az ehhez szükséges hatáskörökre, felhasználókra vonatkozó szabályokat.

Ki kell adni az informatikai biztonsági szabályzatot, amely tartalmazza a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását és a szervezet biztonsági szintbe történő besorolását, az elektronikus információs rendszerek kockázatelemzésének elvégzése

⁴⁴ „2. melléklet a 41/2015 (VII.15.) BM rendelethez”

⁴⁵ 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.

⁴⁶ személyiadat- és lakcímnnyilvántartás

alapján, valamint biztosítani kell ezek tekintetében a jogszabályban meghatározott követelmények teljesülését. Emellett rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén kell meggyőződni arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a vonatkozó jogszabályoknak és a kockázatoknak.

Gondoskodni kell az elektronikus információs rendszer eseményeinek nyomon követhetőségéről, biztonsági esemény bekövetkezésekor pedig a biztonsági eseményre történő gyors és hatékony reagálásról, és ezt követően a biztonsági események kezeléséről az érintettek haladéktalan tájékoztatása mellett. Végül pedig -ami a témám szempontjából legfontosabb-, meg kell valósítani az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatását, a szervezet vezetője és a szervezet munkatársai információbiztonsági ismereteinek szinten tartását.⁴⁷

Ebben a fejezetben ismertettem az anyakönyvvezetők jogállására vonatkozó szabályokat, előírásokat. Összegeztem egy 2014-es, a hazai közszféra információbiztonságára vonatkozó eredményeit, illetve az állami szervek és helyi önkormányzatok információbiztonságára vonatkozó legfontosabb előírásokat, előrevetítve az egyes hiányosságokat e terület vonatkozásában.

⁴⁷ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

3.FEJEZET: AZ ANYAKÖNYVVEZETŐK ADAT- ÉS INFORMÁCIÓBIZTONSÁGI FELKÉSZÜLTSGÉNEK FELMÉRÉSE

Jelen fejezetben kutatásomat megalapozó, kérdőíves felméréssel és annak elemzésével próbálok képet adni az anyakönyvvezetők jelenlegi adat-és információbiztonsági felkészültségéről.

A korábbi fejezetekben többször utaltam arra, hogy az anyakönyvvezetők milyen -az állami működés szempontjából- kiemelkedő elektronikus információs rendszerek felhasználói, ezzel párhuzamosan pedig az állampolgárok személyes adatainak kezelői. Az Ibtv. kijelenti, hogy a társadalom részéről jogos elvárás, hogy a nemzeti elektronikus információs rendszerekben kezelt adatok és információk bizalmosságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerlemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelmének garantálása. Vagyis, az állampolgárok jogosan várják el, hogy adataik kezelése során garantálva legyen az adatbiztonság. Az adatbiztonság alatt az adatok jogosulatlan megszerzése, módosítása, továbbá megsemmisítése ellen tett műszaki és szervezési megoldások összességét kell érteni.⁴⁸ Ebből kifolyólag az anyakönyvvezetők -mint adatkezelők- felé is elvárásként támasztják a biztonságos adat-és információkezelés követelményét.

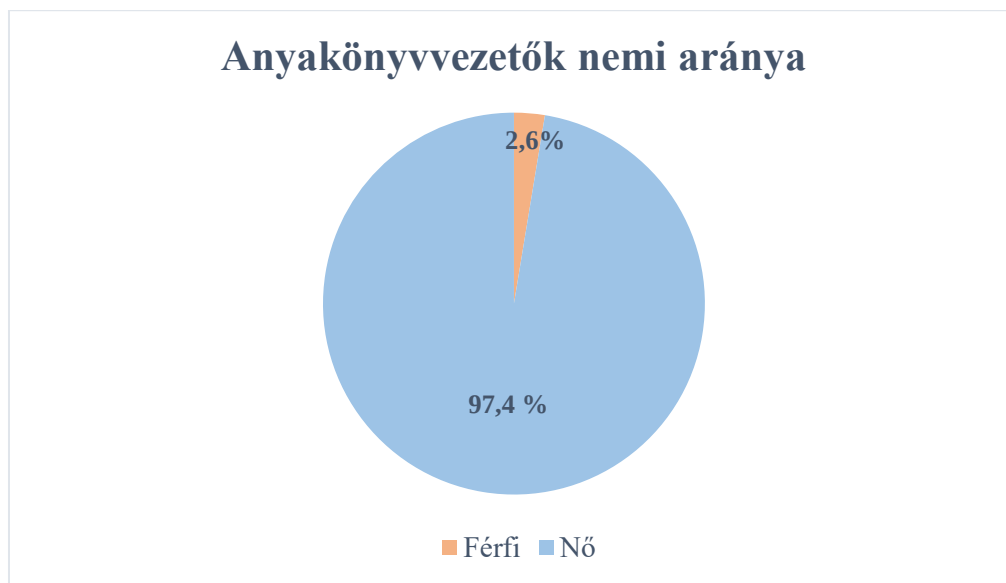
A továbbiakban a kérdőíves felmérést ismertetném. A sokaság tisztasága okán a kérdőív egy olyan zártkörű Facebook csoportba vált elérhetővé, amely kizárólag anyakönyvvezetőkől áll. Az abból származó adatokat az IBM SPSS Statistics 25 programcsomag segítségével értékeltem ki a kutatási módszertanban meghatározott elemzési eljárásokkal. A kérdőív kérdéseit az 1. számú melléklet tartalmazza.

3. 1. fejezet: A kitöltők nemének, illetve az azokkal kapcsolatos összefüggések vizsgálata

Kutatásom során először is a kitöltők nemi összetettségét vizsgáltam.

⁴⁸ Attila Pál Bodó, Tamás Joó, és Tamás Palicz, *AZ IBTV. GYAKORLATA*, szerk. Veronika Deák (Budapest: Nemzeti Közszerológiai Egyetem, 2020).

Az állami anyakönyvvezetés kezdetekor⁴⁹ kizárólag a megfelelő képesítéssel⁵⁰, illetve magyar állampolgársággal rendelkező 24 évet betöltött férfiak tölthettek be (a rabbik és a lelkészek kivételével) anyakönyvvezetői tisztséget, azonban a női emancipáció során a hölgyek számára is elérhetővé váltak a hivatali pozíciók. Olyannyira, hogy ma már az anyakönyvvezetői szakmai kifejezetten „elnőiesedett”. Ezt a tényt igazolja az alábbi ábra, amely alapján megállapítható, hogy a kitöltők 97,4% nő, míg csupán 2,6%-a férfi.



1. ábra Anyakönyvvezetők nemi aránya (Saját szerkesztés)

A nemek közötti különbségek szerepét az információbiztonsági magatartásokban és tudatosságban korlátozott számú tanulmány vizsgálta. A vizsgálatok során tanulmányozták a férfiak és nők közötti különbségeket a technológia és a digitális eszközök használatában, és megállapították, hogy a nők jobban aggódnak a digitális eszközök és az információs technológia használata miatt. Emellett felfedezték, hogy a férfiak jobb információs technológiai készségekkel, tudással rendelkeznek és hatékonyabban használják a számítógépet.⁵¹ Egy másik tanulmányban szintén különbségeket fedeztek fel a férfiak és a nők között az információbiztonság és a kiberbiztonság területén. Kiderült, hogy a nők nagyobb

⁴⁹ 1895. október 1

⁵⁰ gymnasium, reáltanoda, vagy polgári iskola hat osztályát avagy egyenrendű katonai tanfolyamot vagy kereskedelmi iskolát végzett, vagy tanítói oklevéllel bír, vagy pedig ha ezen minősítéssel nem bír is, de oly hivatali vagy állást viselt, mely az itt felsorolt képesítések valamelyikéhez van kötve;

⁵¹ Jun He és L. Freeman, „Are Men More Technology-Oriented Than Women? The Role of Gender on the Development of General Computer Self-Efficacy of College Students”, *AMCIS*, 2009.

valószínűséggel válnak adathalász támadások áldozataivá, mint a férfiak.⁵² A tanulmányok és eredmények azt mutatják, hogy a nemek közötti különbségek hatással lehetnek az információbiztonsági magatartásra, valamint, hogy a férfiak valószínűleg jobb információbiztonsági magatartást tanúsítanak, ezáltal jobban védettek az kibertérben, mint a nők.⁵³ A tanulmányok eredményei alapján megállapítható, hogy az anyakönyvvezetői réteg információbiztonsági felkészültségének erősítése kiemelkedően fontos, hiszen a nők nagyobb számban képviseltetik magukat a szakmán belül.

A H1 okán azt vizsgáltam, hogy a felmérésben részt vevő anyakönyvvezetők véleményük szerint lehetnek-e kibertámadás célpontjai, vagyis a kitöltők önmagukkal, illetve a munkavégzésükkel kapcsolatos percepcióját vizsgáltam. Keresztábra elemzéssel azt vizsgáltam, hogy a H1 hipotézisben megfogalmazott kritériumok befolyásolják-e a kitöltők önmagukról alkotott képét.

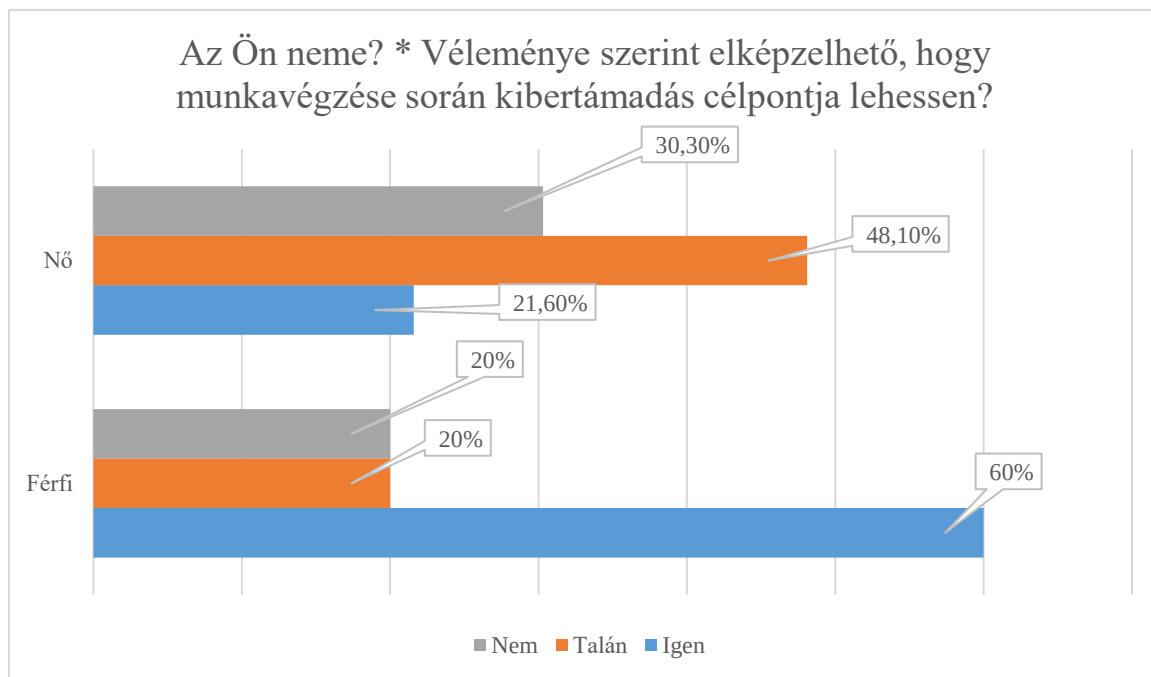
Az Ön neme? * Véleménye szerint elképzelhető, hogy munkavégzése során kibertámadás célpontja lehessen? Crosstabulation

			Véleménye szerint elképzelhető, hogy munkavégzése során kibertámadás célpontja lehessen?			Total
			Igen	Nem	Talán	
Az Ön neme?	Férfi	Count	3	1	1	5
		% within Az Ön neme?	60,0%	20,0%	20,0%	100,0%
	Nő	Count	40	56	89	185
		% within Az Ön neme?	21,6%	30,3%	48,1%	100,0%
Total	Count		43	57	90	190
	% within Az Ön neme?		22,6%	30,0%	47,4%	100,0%

A nemek közötti válaszok megoszlását a 2. ábrán illusztráltam.

⁵² Steve Sheng és mtsai., „Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions”, köt. 1, 2010, 373–82, <https://doi.org/10.1145/1753326.1753383>.

⁵³ Faye Alotaibi és Aziz Alshehri, „Gender Differences in Information Security Management”, *Journal of Computer and Communications* 8, sz. 3



2. ábra Az Ön neme? Véleménye szerint elképzelhető, hogy munkavégzése során kibertámadás célpontja lehessen?

A táblázat alapján megállapítom, hogy a férfiak 60%-a, még a nőknek csupán 21,6 %-a gondolja úgy, hogy potenciális célpont lehet egy kibertámadás során.

Correlations

		Az Ön neme?	Véleménye szerint elképzelhető, hogy munkavégzése során kibertámadás célpontja lehessen?
Az Ön neme?	Pearson Correlation	1	,133
	Sig. (2-tailed)		,067
	N	190	190
Véleménye szerint elképzelhető, hogy munkavégzése során kibertámadás célpontja lehessen?	Pearson Correlation	,133	1
	Sig. (2-tailed)	,067	
	N	190	190

A két változó közötti összefüggést Pearson korrelációval vizsgáltam, amely a változók közötti kapcsolat meglétét, szorosságát és annak irányát értékeli. Ezáltal megállapítottam, hogy a korrelációs együttható értéke 0,133 ($p=0,133$), amely a pozitív előjel alapján azt jelenti, hogy a

két változó közötti kapcsolat egyenes arányú. Tekintve, hogy ez az érték 0-hoz közelít, így a szignifikancia szintje közepesnél alacsonyabb szintű. Önmagában a 2 változó közötti szignifikanciát azért tartom fontos eredménynek, mert ha a kitöltők magukra egy kibertámadás potenciális célpontjaként tekintenek a munkavégzésükkel kapcsolatban, az jelentősen befolyásolja információbiztonsági magatartásukat. Továbbá, ezt az eredményt kockázatként értékelem, hiszen az anyakönyvvezetők 97,4%-a nő, akik -a diagramm alapján- magukra többségében nem, vagy csak esetlegesen (talán) tekintenek kibertámadás célpontjaként. Amennyiben nem érzi magát valaki veszélyben a munkavégzése során, úgy nem várható el tőle, hogy kövesse az irányadó szabályokat a saját -és ügyfeleinek- biztonsága érdekében.

3.2. fejezet: Az információbiztonsággal kapcsolatos válaszok elemzése

Ebben az alfejezetben azt igyekszem bizonyítani, hogy a közigazgatásban eltöltött idő és az egyén adat-és információbiztonsági felkészültsége között van-e összefüggés (H3). Megjegyezném, hogy a közigazgatásban eltöltött évek száma bizonyos esetekben alulreprezentáltságot eredményezett egyes csoportokban, aminek okán az SPSS-ben végzett keresztábra-elemzéseim Fisher-tesztel egészítettem ki, amely megmutatja, hogy van-e szignifikáns kapcsolat két nominális mérési szintű változó között, amellett, hogy nem érzékeny az eloszlásra és a mintanagyságra, vagyis nem szükséges, hogy minden adatcella meghatározott számú kitöltővel rendelkezzen.

Elsőként azt vizsgáltam, hogy van-e összefüggés az anyakönyvvezetőként eltöltött idő és a szervezet IBSZ-ének ismerete között.

Mióta dolgozik anyakönyvvezetőként? * Ismeri-e az Ön szervezetének Informatikai Biztonsági Szabályzata (IBSZ) adatvédelemre vonatkozó előírásait? Crosstabulation

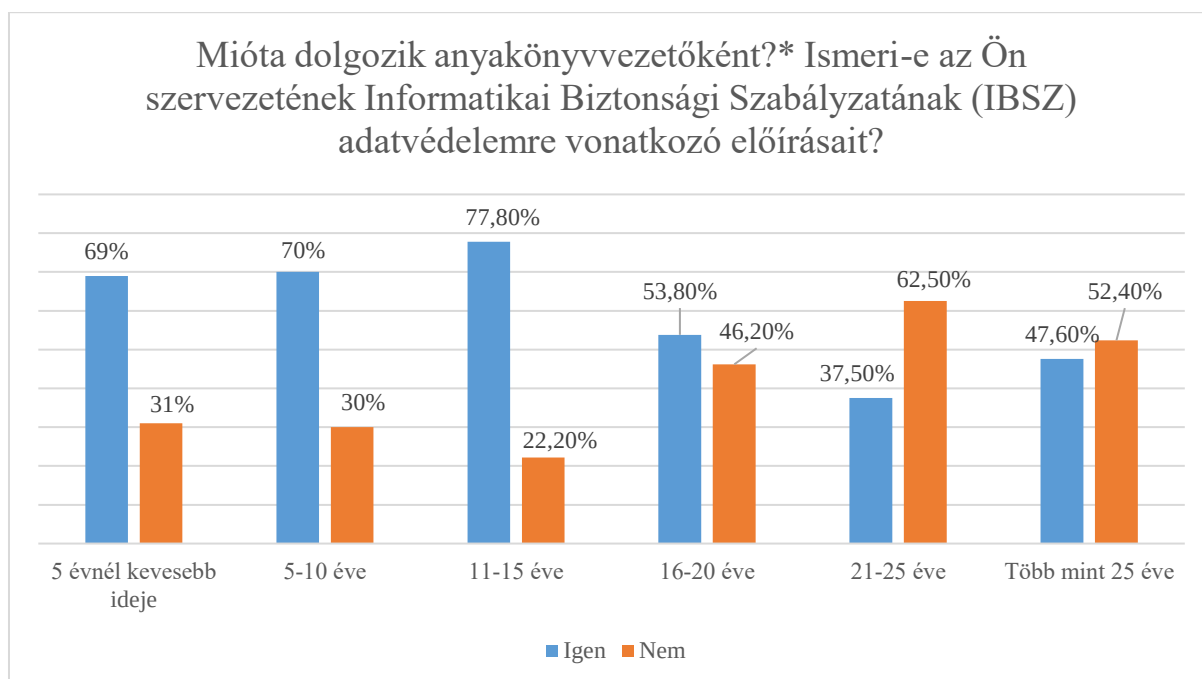
			Ismeri-e az Ön szervezetének Informatikai Biztonsági Szabályzata (IBSZ) adatvédelemre vonatkozó előírásait?		Total
			Igen	Nem	
Mióta dolgozik anyakönyvvezetőként?	5 évnél kevesebb ideje	Count	49	22	71
		% within Mióta dolgozik anyakönyvvezetőként?	69,0%	31,0%	100,0%
	5-10 éve	Count	35	15	50
		% within Mióta dolgozik anyakönyvvezetőként?	70,0%	30,0%	100,0%
	11-15 éve	Count	21	6	27
		% within Mióta dolgozik anyakönyvvezetőként?	77,8%	22,2%	100,0%
	16-20 éve	Count	7	6	13
		% within Mióta dolgozik anyakönyvvezetőként?	53,8%	46,2%	100,0%
	21-25 éve	Count	3	5	8
		% within Mióta dolgozik anyakönyvvezetőként?	37,5%	62,5%	100,0%
	25 évnél több ideje	Count	10	11	21
		% within Mióta dolgozik anyakönyvvezetőként?	47,6%	52,4%	100,0%
	Total	Count	125	65	190
		% within Mióta dolgozik anyakönyvvezetőként?	65,8%	34,2%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2- sided)	Exact Sig. (1- sided)	Point Probability
Pearson Chi-Square	9,195 ^a	5	,102	,100		
Likelihood Ratio	8,939	5	,112	,132		
Fisher's Exact Test	8,975			,104		
Linear-by-Linear Association	5,027 ^b	1	,025	,026	,015	,003
N of Valid Cases	190					

a. 2 cells (16,7%) have expected count less than 5. The minimum expected count is 2,74.

b. The standardized statistic is 2,242.



3. ábra Mióta dolgozik anyakönyvvezetőként? Ismeri-e az Ön szervezetének Informatikai Biztonsági Szabályzatának adatvédelemre vonatkozó előírásait?

A Fisher-teszt esetében, akkor állítjuk azt, hogy a két változó között szignifikáns kapcsolat van, ha ez az érték, kisebb, mint 0,05. A táblázat alapján megállapítható, hogy ez az érték 0,104 ($p=0,104$), amely alapján nincs szignifikancia a vizsgált kérdések tekintetében, vagyis a kitöltésben részt vevők anyakönyvvezetőként eltöltött ideje nem befolyásolja az IBSZ ismeretét. Ez több szempontból is kritikus. Egyrészt azért, mert az IBF gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról⁵⁴,

⁵⁴ „2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról”

amely megkérdőjelezi ennek a jogszabályi kötelezettségnek a teljesülését. Emellett pedig az IBSZ be nem tartása jogkövetkezményt von maga után⁵⁵, tehát ha a munkavállaló nem tartja be az abban foglaltakat, akkor különböző szankciók sújthatják, ám hogyan tartsa be azokat, ha nem is ismeri őket?!

A közigazgatáson belül az egyik legnehezebben kivitelezhető információbiztonsági előírás: a tiszta asztal politikája. A tiszta asztal politika olyan irányelv, amely olyan ajánlásokat fogalmaz meg a munkavállalók számára, amelyek által az adat-és információbiztonsági kockázat csökkenthetővé válik olyan módszerek alkalmazásával, mint az érzékeny adatokat tartalmazó iratok és dokumentumok zárható szekrénybe való tárolásával, vagy például a belépési jelszavakat/ vagy azokra utaló fényképek, feljegyzések (post-itek) betiltása a munkavégzés helyszínéül szolgáló asztalon, számítógépen.

Mióta dolgozik anyakönyvvezetőként? * Hallott-e már a tiszta asztal elvéről? Amennyiben igen, alkalmazza-e?
Crosstabulation

			Hallott-e már a tiszta asztal elvéről? Amennyiben igen, alkalmazza-e?			Total
			Igen, hallottam és alkalmazom is a munkavégzés em során	Igen, hallottam, de nem alkalmazom a munkavégzés em során	Nem	
Mióta dolgozik anyakönyvvezetőként?	5 évnél kevesebb ideje	Count	21	7	43	71
		% within Mióta dolgozik anyakönyvvezetőként?	29,6%	9,9%	60,6%	100,0%
	5-10 éve	Count	11	8	31	50
		% within Mióta dolgozik anyakönyvvezetőként?	22,0%	16,0%	62,0%	100,0%
	11-15 éve	Count	10	4	13	27
		% within Mióta dolgozik anyakönyvvezetőként?	37,0%	14,8%	48,1%	100,0%
	16-20 éve	Count	1	1	11	13
		% within Mióta dolgozik anyakönyvvezetőként?	7,7%	7,7%	84,6%	100,0%
	21-25 éve	Count	1	0	7	8
		% within Mióta dolgozik anyakönyvvezetőként?	12,5%	0,0%	87,5%	100,0%
	25 évnél több ideje	Count	6	2	13	21
		% within Mióta dolgozik anyakönyvvezetőként?	28,6%	9,5%	61,9%	100,0%
	Total	Count	50	22	118	190
		% within Mióta dolgozik anyakönyvvezetőként?	26,3%	11,6%	62,1%	100,0%

⁵⁵ „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”

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2- sided)	Exact Sig. (1- sided)	Point Probability
Pearson Chi-Square	9,362 ^a	10	,498	,504		
Likelihood Ratio	10,769	10	,376	,459		
Fisher's Exact Test	8,299			,579		
Linear-by-Linear Association	,558 ^b	1	,455	,466	,237	,016
N of Valid Cases	190					

a. 7 cells (38,9%) have expected count less than 5. The minimum expected count is ,93.

b. The standardized statistic is ,747.

A Fisher teszt segítségével megállapítom, hogy nincs szignifikancia a tiszta asztal elv és az anyakönyvvezetőként eltöltött idő között a válaszadók esetében, vagyis az anyakönyvvezetőként eltöltött idő nem feltételezi az alapelv ismeretét és annak alkalmazását.

Az alábbiakban az anyakönyvvezetőként eltöltött idő és a biztonságos jelszóalkotási ajánlások ismeretét, illetve annak alkalmazását vizsgáltam.

Mióta dolgozik anyakönyvvezetőként? * Ismer-e biztonságos jelszóalkotásra vonatkozó ajánlásokat? Amennyiben igen, alkalmazza-e azokat? Crosstabulation

			Ismer-e biztonságos jelszóalkotásra vonatkozó ajánlásokat? Amennyiben igen, alkalmazza-e azokat?			Total
			Igen, de nem alkalmazom azokat	Igen, és alkalmazom is azokat	Nem	
Mióta dolgozik anyakönyvvezetőként?	5 évnél kevesebb ideje	Count	17	37	17	71
		% within Mióta dolgozik anyakönyvvezetőként?	23,9%	52,1%	23,9%	100,0%
	5-10 éve	Count	10	31	9	50
		% within Mióta dolgozik anyakönyvvezetőként?	20,0%	62,0%	18,0%	100,0%
	11-15 éve	Count	9	13	5	27
		% within Mióta dolgozik anyakönyvvezetőként?	33,3%	48,1%	18,5%	100,0%
	16-20 éve	Count	5	4	4	13
		% within Mióta dolgozik anyakönyvvezetőként?	38,5%	30,8%	30,8%	100,0%
	21-25 éve	Count	4	2	2	8
		% within Mióta dolgozik anyakönyvvezetőként?	50,0%	25,0%	25,0%	100,0%
	25 évnél több ideje	Count	1	6	14	21
		% within Mióta dolgozik anyakönyvvezetőként?	4,8%	28,6%	66,7%	100,0%
	Total	Count	46	93	51	190
		% within Mióta dolgozik anyakönyvvezetőként?	24,2%	48,9%	26,8%	100,0%

Symmetric Measures

		Value	Approximate Significance	Exact Significance
Nominal by Nominal	Phi	,385	,002	. ^c
	Cramer's V	,273	,002	. ^c
N of Valid Cases		190		

c. Cannot be computed because there is insufficient memory.

Azonban a Cramer's V^{56} együtttható értéke alapján megállapítom, hogy a 2 változó közötti szorosság csekély, $p=0,002$. Maga a szignifikancia úgy gondolom, abból fakad, hogy azok a kitöltők, akik vettek részt információbiztonsággal kapcsolatos képzésen nagyobb arányban ismerik és használják a biztonságos jelszavakra vonatkozó iránymutatásokat. Ezt az alábbi keresztábra elemzés igazolja.

Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető? * Ismer-e biztonságos jelszóalkotásra vonatkozó ajánlásokat? Amennyiben igen, alkalmazza-e azokat? Crosstabulation

			Ismer-e biztonságos jelszóalkotásra vonatkozó ajánlásokat? Amennyiben igen, alkalmazza-e azokat?			Total
			Igen, de nem alkalmazom azokat	Igen, és alkalmazom is azokat	Nem	
Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető?	Igen	Count	17	39	10	66
		% within Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető?	25,8%	59,1%	15,2%	100,0%
	Nem	Count	29	54	41	124
		% within Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető?	23,4%	43,5%	33,1%	100,0%
Total	Count		46	93	51	190
	% within Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető?		24,2%	48,9%	26,8%	100,0%

⁵⁶ asszociációs együtttható, amely két nominális változó közötti kapcsolat szorosságát mutatja meg.

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	7,375 ^a	2	,025
Likelihood Ratio	7,825	2	,020
Linear-by-Linear Association	3,458	1	,063
N of Valid Cases	190		

a. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 15,98.

A Kí- négyzet próbával megállapítom, hogy az, ha valaki részt vett információbiztonsági képzésen, befolyásolja a biztonságos jelszóalkotásra vonatkozó ismereteit, azok alkalmazását.

Az alábbi táblázatban azt vizsgáltam, hogy van-e összefüggés az anyakönyvvezetőként eltöltött idő és az információbiztonsági tudatossággal kapcsolatos képzésen való részvétel között.

Mióta dolgozik anyakönyvvezetőként? * Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető? Crosstabulation

			Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető?		Total
			Igen	Nem	
Mióta dolgozik anyakönyvvezetőként?	5 évnél kevesebb ideje	Count	22	49	71
		% within Mióta dolgozik anyakönyvvezetőként?	31,0%	69,0%	100,0%
	5-10 éve	Count	21	29	50
		% within Mióta dolgozik anyakönyvvezetőként?	42,0%	58,0%	100,0%
	11-15 éve	Count	11	16	27
		% within Mióta dolgozik anyakönyvvezetőként?	40,7%	59,3%	100,0%
	16-20 éve	Count	4	9	13
		% within Mióta dolgozik anyakönyvvezetőként?	30,8%	69,2%	100,0%
	21-25 éve	Count	1	7	8
		% within Mióta dolgozik anyakönyvvezetőként?	12,5%	87,5%	100,0%
	25 évnél több ideje	Count	7	14	21
		% within Mióta dolgozik anyakönyvvezetőként?	33,3%	66,7%	100,0%
	Total	Count	66	124	190
		% within Mióta dolgozik anyakönyvvezetőként?	34,7%	65,3%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2- sided)	Exact Sig. (1- sided)	Point Probability
Pearson Chi-Square	3,887 ^a	5	,566	,575		
Likelihood Ratio	4,171	5	,525	,545		
Fisher's Exact Test	3,711			,598		
Linear-by-Linear Association	,091 ^b	1	,763	,783	,403	,035
N of Valid Cases	190					

a. 2 cells (16,7%) have expected count less than 5. The minimum expected count is 2,78.

b. The standardized statistic is ,301.

Ezek alapján megállapítottam, hogy nincs szignifikáns összefüggés az információbiztonsági képzésen való részvétel és az anyakönyvvezetőként eltöltött idő között. Ez alapvetően probléma, hiszen normál esetben minél régebb óta dolgozik valaki anyakönyvvezetőként, annál több információbiztonsági képzésen kellett volna részt vennie.

Emellett azt is vizsgáltam, hogy van-e összefüggés a között, hogy a válaszadók vettek-e rész információbiztonsági képzésen. Ennek szignifikanciaelemzését Khí-négyzet teszttel végeztem, amely arra ad álaszt, hogy a két változó között van-e szignifikáns kapcsolat. Csakúgy, mint a Fisher-teszt esetében akkor beszélhetünk szignifikanciáról, ha az érték 0,05-nél kisebb.

Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető? *
Véleménye szerint elképzelhető, hogy munkavégzése során kibertámadás célpontja lehessen?
Crosstabulation

			Véleménye szerint elképzelhető, hogy munkavégzése során kibertámadás célpontja lehessen?			Total
			Igen	Nem	Talán	
Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető?	Igen	Count	20	17	29	66
		% within Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető?	30,3%	25,8%	43,9%	100,0%
	Nem	Count	23	40	61	124
		% within Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető?	18,5%	32,3%	49,2%	100,0%
Total	Count		43	57	90	190
	% within Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető?		22,6%	30,0%	47,4%	100,0%

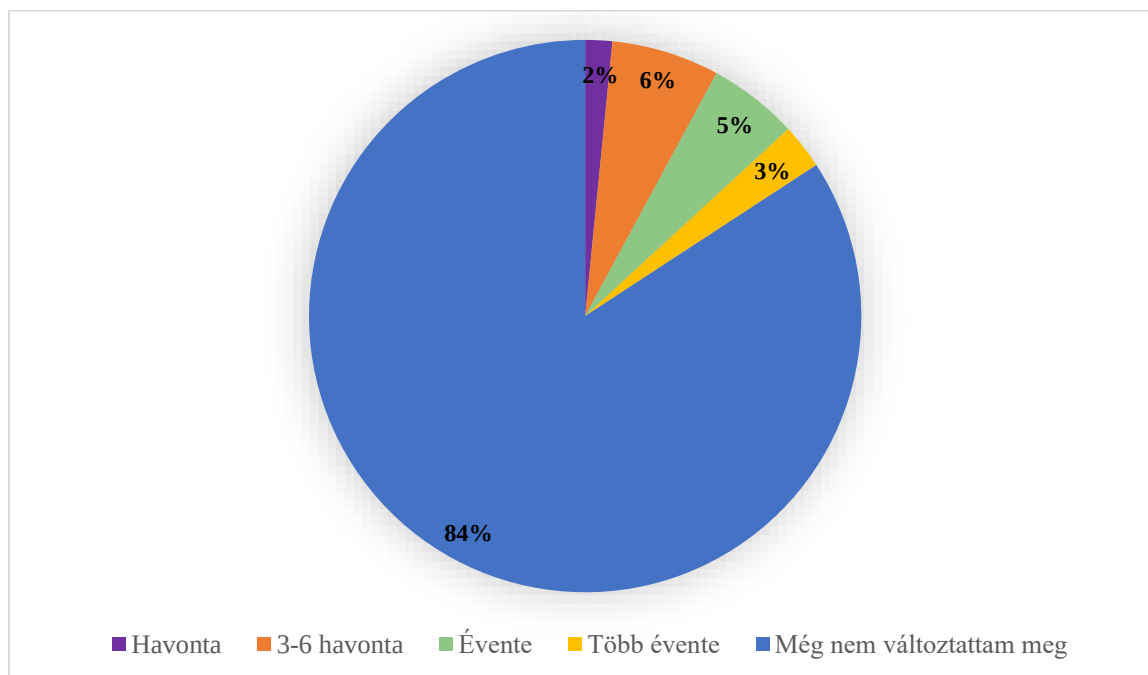
Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	3,488 ^a	2	,175
Likelihood Ratio	3,400	2	,183
Linear-by-Linear Association	1,940	1	,164
N of Valid Cases	190		

a. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 14,94.

Tekintve, hogy a Khí- négyzet próbára kapott érték 0,175 ($p=0,175$) így nem áll fent szignifikancia a kitöltők körében a között, hogy vettek-e részt információbiztonsági képzésen és a között, hogy saját magukat potenciális kibertámadás célpontjaként tekintik. Véleményem szerint ez azt jelenti, hogy a számukra jelenleg rendelkezésre álló tananyag nem készíti fel őket a kibertérben várható veszélyekre, hiszen akkor tisztában lennének azzal, hogy munkavégzésük okán potenciális kibertámadási célcsoport részei. Emellett, a pályára lépés feltételeként előírt szakvizsga sem foglalkozik sem az adat, sem pedig az információbiztonságra való előírások ismertetésével.

A továbbiakban a jelszóhasználattal kapcsolatos információbiztonsági attitűdöket vizsgáltam.



4. ábra Milyen gyakran változtatja meg az EAK-hoz tartozó jelszavát? (Saját szerkesztés)

A diagramm alapján megállapítom, hogy a kitöltők 84%-a nem változtatta meg még a jelszavát. A következő táblázat azt vizsgálja, hogy azok a kitöltők, aki nem változtatták meg az EAK-hoz tartozó jelszavukat, mióta képezik az anyakönyvvezetői állomány részét.

Mióta használja az Elektronikus Anyakönyvi Rendszert (EAK-ot)? * Milyen gyakran változtatja meg az EAK-hoz tartozó jelszavát? Crosstabulation

		Milyen gyakran változtatja meg az EAK-hoz tartozó jelszavát?					Total
		Havonta	3-6 havonta	Évente	Több évente	Nem változtattam	
Mióta használja az Elektronikus Anyakönyvi Rendszert (EAK-ot)?	Bevezetésétől kezdve (2014. 07. 01.)	3	4	3	2	82	94
		3,2%	4,3%	3,2%	2,1%	87,2%	100,0%
	2015	0	0	0	0	8	8
		0,0%	0,0%	0,0%	0,0%	100,0%	100,0%
	2016	0	0	0	1	15	16
		0,0%	0,0%	0,0%	6,3%	93,8%	100,0%
	2017	0	1	1	0	12	14
		0,0%	7,1%	7,1%	0,0%	85,7%	100,0%
	2018	0	2	3	0	15	20
		0,0%	10,0%	15,0%	0,0%	75,0%	100,0%
	2019	2	2	0	2	10	16
		12,5%	12,5%	0,0%	12,5%	62,5%	100,0%
	2020	0	3	0	0	12	15
		0,0%	20,0%	0,0%	0,0%	80,0%	100,0%
	2021	0	0	0	0	5	5
		0,0%	0,0%	0,0%	0,0%	100,0%	100,0%
Total		5	12	7	5	161	190
		2,6%	6,3%	3,7%	2,6%	84,7%	100,0%

A táblázat alapján megállapítom, hogy azon válaszadók, akik az EAK-ot bevezetésétől kezdődően használják 87,2%-uk nem változtatta meg a felhasználói fiókjukhoz tartozó jelszavát. Hogyan lehetséges ez? Úgy, hogy az EAK jelenleg nem rendelkezik jelszóprotokollal, vagyis a felhasználóktól nem követeli meg a rendszeres jelszócserét. Ebből kiindulva megállapítom, az adminisztratív előírásoknak a hiányát, amely által igazolom a H4 hipotézisem azon részét, amely szerint az információbiztonsági képzéseken megszerzett kompetenciák és attitűdök kikényszerítő szabályozók hiányában a kitöltők információbiztonsággal kapcsolatos magatartása esetleges és önkéntes.

Az alábbiakban Kruskal-Wallis tesztel vizsgáltam, hogy van-e összefüggés a jelszóváltoztatás gyakorisága és az információbiztonsági képzéseken való részvétel között. A Kruskal-Wallis teszt egy nemparaméteres próba, amely azt vizsgálja, hogy minden minta azonos eloszlású sokaságból származik-e.

Kruskal-Wallis Test

Ranks			
Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvezető?		N	Mean Rank
Milyen gyakran változtatja meg az EAK-hoz tartozó jelszavát?	Igen	66	93,85
	Nem	124	96,38
	Total	190	

Test Statistics^{a,b}

Milyen gyakran változtatja meg az EAK-hoz tartozó jelszavát?	
Kruskal-Wallis H	,227
df	1
Asymp. Sig.	,634

a. Kruskal Wallis Test

b. Grouping Variable: Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvezető?

A kitöltők körében a jelszóváltoztatás gyakorisága nem állt szignifikáns összefüggésben az információbiztonsági képzésen való részvétellel.

Jelen alfejezet alapján igazoltam, hogy az általam vizsgált információbiztonsági attitűddel kapcsolatos kérdések során nem állt jelentős szignifikancia az információbiztonság és az anyakönyvvezetőként eltöltött idő között a kitöltők körében. (H3) Ez azonban azért probléma, mert a korábbi fejezetekben ismertetett IBSZ alapjaiban határozza meg a biztonságos működés feltételeit a kitöltők körében. Ennek nem ismerete azonban nem mentesít a felelősség alól.

Emellett megállapítom, hogy azon kitöltők, akik vettek részt valamilyen információbiztonsági képzésen nem rendelkeznek nagyobb tudatossággal, amely a jelenleg, számukra elérhető képzés tartalmán túl, az ott megszerzett ismeretek gyakorlatba való átültetését kérdőjelezi meg. (H2, H4)

A kérdőíves felmérés alapján megállapítottam, hogy az anyakönyvvezetői szakma alapvetően hölgyekből áll, amely az említett tanulmányok alapján információbiztonsági kockázatként értékelhető. Emellett igazoltam, hogy nincs szignifikancia a hivatali pályán eltöltött idő és a biztonság tudatos magatartások között. Azokban az esetekben, amelyek korrelációt mutattak a képzések és az ott megszerzett gyakorlatok alkalmazása között -véleményem szerint-, azt igazolják, hogy nem a jelenleg elérhető képzéssel van probléma, hanem az ott megszerzett tudás alkalmazásával, valamint annak a biztonsági kultúrába, a mindennapi munkavégzésbe való beépítésével. A jelenleg elérhető képzéseken megszerzett ismereteket jelenleg önkéntes alapon követik a kitöltők, hiszen nem állnak rendelkezésre olyan kontrolltényezők, amelyek lehetővé tennék az információbiztonsággal kapcsolatos magatartásszabályok megkövetelését, azok alkalmazásának kikényszeríthetőségét. Mindezek alapján igazoltam, hogy szükséges van az anyakönyvvezetőknek szóló információbiztonsági képzés kialakítására az állampolgárok adat- és információvédelmének garantálhatósága okán.

4. FEJEZET: INFORMÁCIÓBIZTONSÁGI KÉPZÉSI KERETRENDSZER ANYAKÖNYVVEZETŐK SZÁMÁRA

A korábbi fejezetek összegzése alapján, különböző szempontokat figyelembevéve ismertetném az anyakönyvvezetők információbiztonságára irányuló tudatosítás program keretrendszerét. Jelen fejezet arra a hipotézisre épít, hogy az anyakönyvvezetők számára jelenleg nem érhető el egy olyan információbiztonsági tudatosító program, ami kifejezetten az anyakönyvi munkavégzésre, a munkavégzés során használt elektronikus információs rendszerekre - valamint azok felhasználói tudatossággal megvalósítható védelmére- irányul, ezáltal által nem feltétlen rendelkeznek információbiztonsági operatív képességgel és az e feladatok elvégzéséhez szükséges szaktudással, valamint a biztonsági sérülékenységek felismerésének és kezelésének képessége sem valósul meg a szervezet egészének tekintetében. A tudatosság megteremtésének célja, hogy az alkalmazottakat felvértesse az információbiztonsági kockázatokkal kapcsolatban, és felvilágosítsa őket szerepükről és felelősségükről⁵⁷, vagyis, hogy az anyakönyvvezetők humán tűzfalként⁵⁸ képesek legyenek észlelni és kezelni az esetleges kibertérből érkező támadásokat.

4.1. fejezet: Az információbiztonsági tudatosító program jogosultságának indoklása

Az infokommunikációs eszközök és az internet biztonságos használatát tanulni kell.⁵⁹ Amint azt már a korábbi fejezetekben említettem, az anyakönyvvezetők mindennapi munkavégzésük során olyan nyilvántartásokat -elektronikus információs rendszereket- kezelnek, illetve férnek hozzá, amelyek egy része a nemzeti adatvagyon részét képezi, vagy pedig nélkülözhetetlen az állam megszokott, zavartalan működésének szempontjából. Az anyakönyvvezetői pályára lépés feltétele egy sikeres anyakönyvvezetői szakvizsga, azonban felhívnom a figyelmet arra, hogy a hatályos anyakönyvvezetői szakvizsga nem foglalkozik az adat-és információbiztonság témaköreivel. Ez alapján megállapítom, hogy a pályára lépés feltételeként nem jelenik meg a

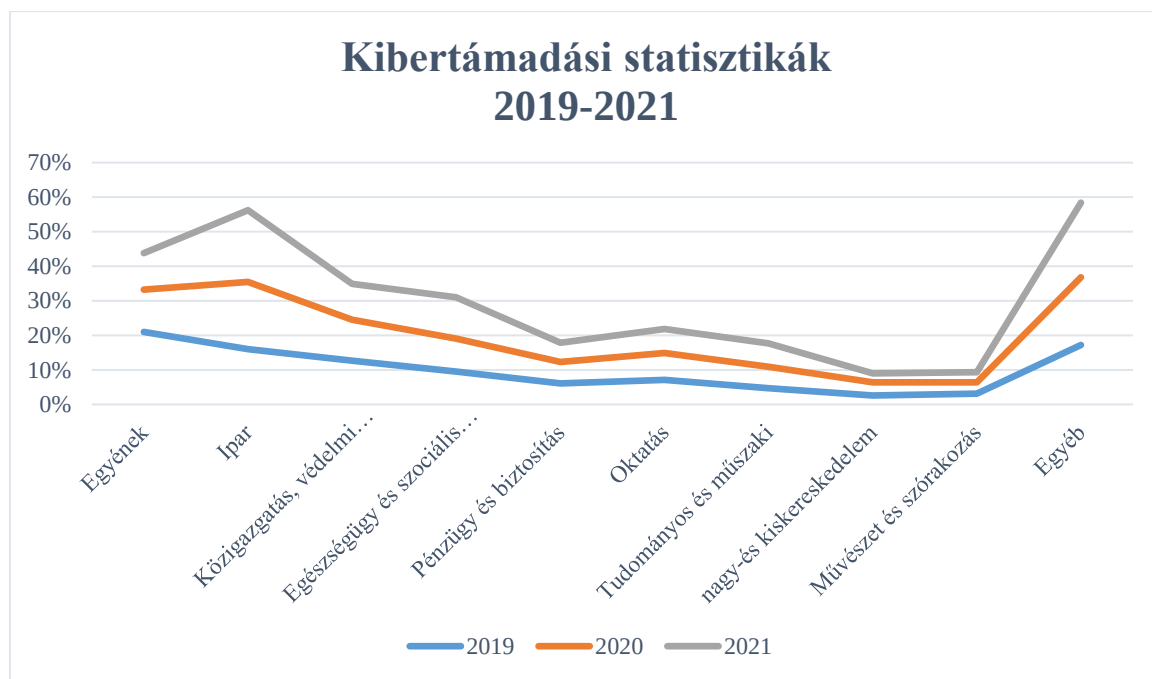
⁵⁷ Tanja Grassegger és Dietmar Nedbal, „The Role of Employees’ Information Security Awareness on the Intention to Resist Social Engineering”, *Procedia Computer Science*, CENTERIS 2020 - International Conference on ENTERprise Information Systems / ProjMAN 2020 - International Conference on Project MANagement / HCist 2020 - International Conference on Health and Social Care Information Systems and Technologies 2020, CENTERIS/ProjMAN/HCist 2020, 181 (2021. január 1.): 59–66, <https://doi.org/10.1016/j.procs.2021.01.103>.

⁵⁸ Az emberi tűzfal kifejezést olyan emberek leírására használják, akik követik a bevált gyakorlatokat az adatsértések vagy gyanús tevékenységek megelőzése és bejelentése érdekében. Fred Rica: Human firewalling, KPMG Advisory, <https://advisory.kpmg.us/articles/2021/human-firewalling.html>, letöltés dátuma: 2022.02.08.

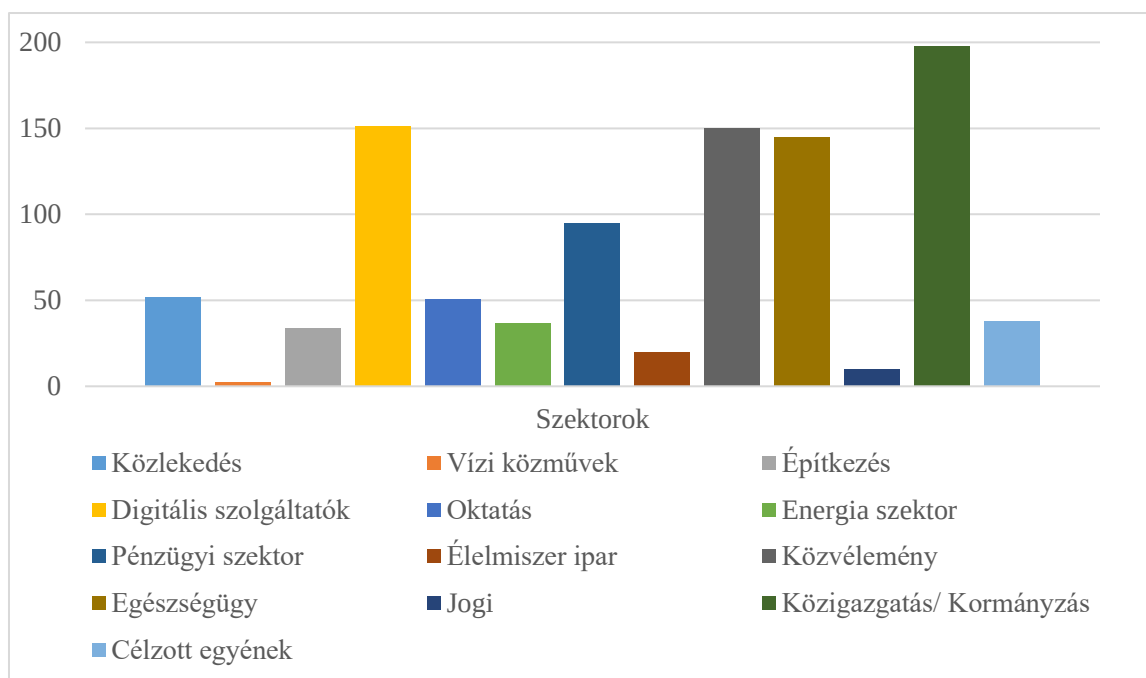
⁵⁹ Kovács, *A kibertér védelme*.

biztonságos adat-és információkezelésre vonatkozó szabályzatok, valamint az abban foglaltak elsajátítása, mint követelmény

A program aktualitásai közé sorolom azt a tényt, hogy az anyakönyvvezetők -mint a közigazgatási személyi állomány részei- potenciális célpontjai lehetnek a kibertámadásoknak. Az alábbi ábra rámutat arra, hogy az elmúlt évben (2021) a közigazgatás kiemelkedő, 4. helyen állt a kibertámadások célpontjaként. A korábbi években jellemzően a 3. legtámadottabb terület volt azonban az egészségügy -a COVID járványból kifolyólag- felértékelődött a támadók tekintetében.



5. ábra Cyber Attacks Statistics 2019-2021 (Saját szerkesztés, forrás: Hackmagaddon)



6. ábra Megcélzott szektorok az események száma szerint 2020. április-2021. július (Saját szerkesztés, forrás: ENISA THREAT LANDSCAPE 2021)

A diagrammok alapján megállapítható, hogy a közigazgatás a kibertámadások kiemelt potenciális célpontja. Ezt a tényt támasztja alá, a fentiekben ismertetett állami nyilvántartó rendszerek összessége is, amelyek tökéletes eszközként szolgálhatnak egy állam ellen irányuló támadás kivitelezése szempontjából. Gondoljunk csak bele, mi történne, ha ezek a nyilvántartások nem frissülnének. Mi alapján valósulna meg az állampolgárok nyilvántartása? Hogyan tudná az adóhatóság⁶⁰ kik az adóalanyok? Ezáltal felborulna a központi költségvetés teljesíthetősége is. Mindezek alapján kijelenthető, hogy azok, akik a közigazgatás szervezetrendszerébe dolgoznak -a támadók szempontjából- rendkívül értékes információk birtokában vannak. (H1) Többek közül ezért a felhasználót fel kell készíteni ezen kihívások kezelésére, természetesen a rájuk vonatkozó szintig. Megjegyzem, ez a kibertámadásoknak való kitettség a teljes közszolgálati állományra, valamint minden olyan személyre igaz, aki akár a Munka törvénykönyve szerinti, vagy egyéb szerződéses munkaviszonyban áll a közigazgatás szervezetrendszerével.

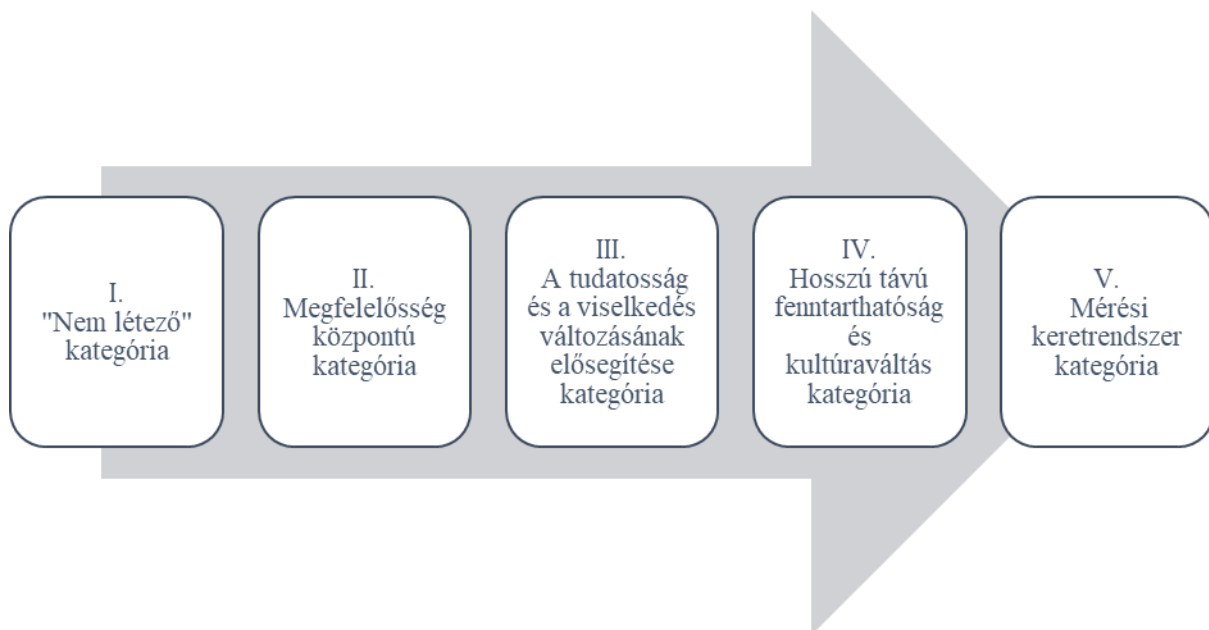
A program aktualitását igazolja, hogy az anyakönyvvezetők által használt elektronikus információs rendszerek összekapcsolt rendszerek, vagyis teljesen mindegy, hogy egy fővárosban, vagy egy -példának okáért- Borsod-Abaúj-Zemplén megyei településen működő

⁶⁰ Nemzeti Adó-és Vámhivatal

anyakönyvvezető válik célponttá, az okozott kár nagysága azonos mértékű lesz. Emellett -szintén az aktualitást igazolva- ha nem rendelkeznek kellő felkészültséggel, illetve tudással ahhoz, hogy felismerjenek egy esetleges kibertámadást, úgy az arra való reagálás sem várható el.

A biztonságtudatosság hiánya az elektronikus információs rendszer -jelen esetben az EAK-bizalmasságára hat, vagyis arra, hogy az adott elektronikus rendszerhez kizárólag az arra jogosultak férhetnek hozzá a jogosultsági szintüknek megfelelő mértékig. Hogyha a bizalmasság megszűnik, úgy alapjaiban válik megkérdőjelezhetővé az állami működés. Valamint szintén megemlíteném az egységes önkormányzati IBSZ hiányát, amely által jelenleg előfordulhat, hogy az ugyanazon elektronikus információs rendszereket használó helyi önkormányzatok biztonsági szintje eltérő. Emellett kutatások kimutatták, hogy a megnövekedett ISA pozitív hatással van az attitűdre, mivel segít az alkalmazottaknak jobban megérteni az információbiztonsági intézkedések fontosságát⁶¹ A cél olyan szemléletmód kialakítása, amely egy egészséges bizalmatlanságot gerjeszt a felhasználókba, mindazon által felkészíti őket egy esetleges incidens kezelésére, az arra való reagálásra. Ennek kulcsa a tudatosság, vagyis, hogy a felhasználók tisztába legyenek a rájuk leselkedő veszélyekkel. Ez társadalmi érdek. Ha egy szervezet -jelen esetben az állam- számára egy projekt nem fontos, vagyis nem tulajdonít kellő erőforrást és energiát egy kezdeményezés mögé, úgy az nehezen, vagy sehogy sem valósítható meg. Ugyanez a helyzet a biztonságtudatosítással is: ha nincs meg a vezetői támogatás és a szervezet érettsége -jelen esetben az állami finanszírozással társulva- nem elvárható, hogy ez a probléma magától oldódjon meg. Ha a nemzetközi környezetben szeretnénk értékelni a jelenlegi helyzetet, akkor a 2011-ben létrehozott SANS Institute Információbiztonsági Tudatosság Érettségi Modellje tökéletes modellként szolgál. Ez a modell alapvetően 5 kategóriát különít el egy szervezet biztonsági érettsége alapján.

⁶¹ Yuryna Connolly L, Lang M, Gathegi J, Tygar DJ. Organisational culture, procedural countermeasures, and employee security behaviour. Information and Computer Security 2017;25(2):118–36. <https://doi.org/10.1108/ICS-03-2017-0013>.



7. ábra Security Awareness Maturity Model (Saját szerkesztés, forrás: www.sans.org)

Ez az 5 kategória alapvetően egy fejlődési görbeként is értelmezhető, amely iránymutatásként szolgálhat a szervezet számára. Mára már nemzetközi szabvánnyá vált, amelyet a szervezetek érettségének összehasonlítására is használnak. Az első kategória a nem létező kategória, amelyben nem létezik semmilyen biztonságnövelő program a szervezetben. Ezáltal az alkalmazottak nem is sejtik, hogy célpontok, cselekedeteik közvetlen hatással vannak a szervezet biztonságára, nem ismerik és nem tartják be a szervezeti szabályzatot, és könnyen esnek támadások áldozataivá. Úgy gondolom ez a kategória az, ahova jelenleg az anyakönyvvezetők, de csaknem a teljes hazai közigazgatás tartozik. A második kategória a megfelelőségközpontú kategória, amely során már vannak olyan szabályozók, illetve követelmények(auditok) amelyeknek meg kell felelnie az adott szervezetnek, szervezeti egységnek. Ezen a szinten már megjelenik a képzés, azonban csak eseti (éves) alapon. A harmadik kategória -amely a tudatosság és a viselkedés változásának elősegítése-leírásaként szolgál az alábbi fejezet. Ebben az esetben a program túlmutat az éves képzésen, és egész évben folyamatos megerősítést tartalmaz, aminek eredményeként az emberek megértik és követik a szervezeti szabályzatokat, valamint aktívan felismerik, megelőzik és jelentik az incidenseket. Ennek megvalósulása szolgálhat tökéletes alapként a negyedik kategóriához, amely hosszútávon fenntartható kultúraváltozásként említhető. Ebben a fázisban a program rendelkezik a folyamatokkal, az erőforrásokkal és a vezetői támogatással

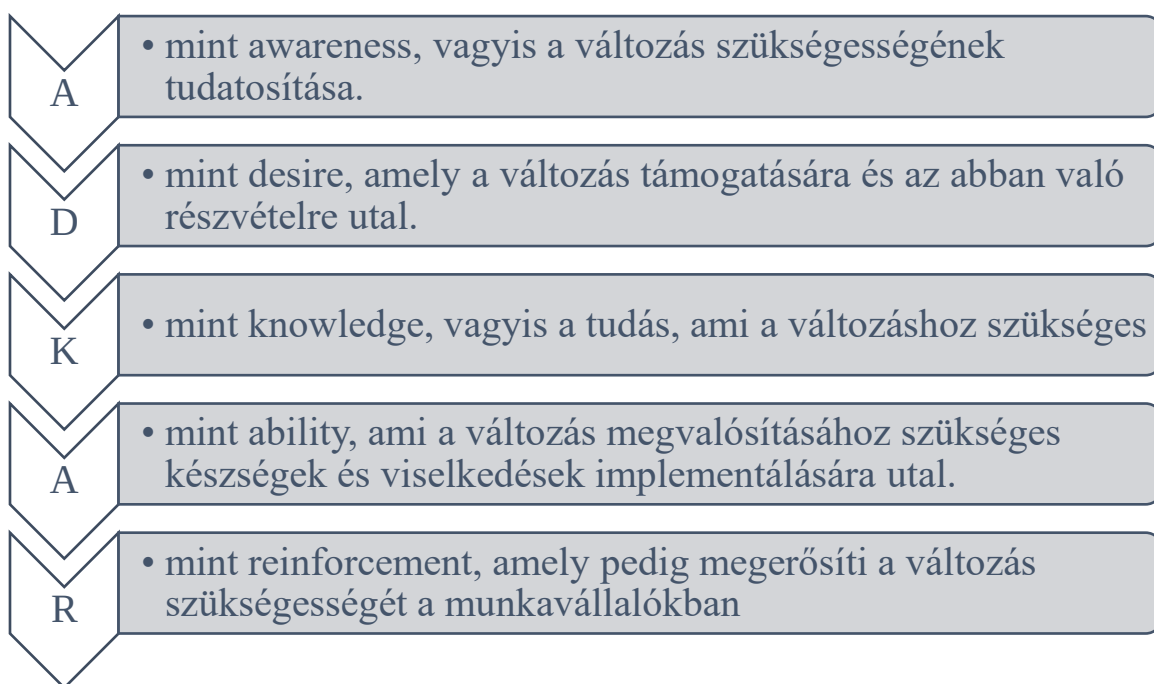
egy hosszú távú életciklushoz, beleértve (legalább) a program éves felülvizsgálatát és frissítését.

Ennek eredményeként a program a szervezet kultúrájának bevált része, aktuális és vonzó, túlmutat a viselkedés megváltoztatásán, és megváltoztatja az emberek hiedelmeit, attitűdjeit és biztonságfelfogását.⁶²

4.2 fejezet: Az információbiztonsági tudatosító program keretrendszere

Az általam megoldásként kínált képzési keret alapja az úgynevezett ADKAR modell, amely alapvetően egy változásmenedzsment modell. Vagyis, véleményem szerint ez a tudatosítási program egy változásként jelenne meg az anyakönyvvezetők mindennapjaiba, amit menedzselni szükséges.

Az ADKAR modell szerint a változás emberi sikertényezői az alábbiak.⁶³



8. ábra ADKAR modell (Saját szerkesztés, forrás: Hiatt Jeffrey M. ADKAR: A model for change in business, government and our community)

Elsőként is tehát fel kell hívni a figyelmet, illetve meg kell értetni az anyakönyvvezetőkkel miért is fontos, hogy részt vegyenek egy információbiztonsággal kapcsolatos tudatosítási képzésen. Fel kell hívni a figyelmüket arra, milyen veszélyek leselkedhetnek rájuk, és hogy

⁶² Security Awareness Maturity Model, issued 2011, <https://www.sans.org/security-awareness-training/resources/maturity-model/>.

⁶³ Hiatt Jeffrey M., „ADKAR: A model for change in business, government and our community”, Prosci Learning Center Publications, 2006.

milyen elektronikus információs rendszerekhez is rendelkeznek hozzáféréssel, ami potenciális célponttá avanszálja őket. Magukénak kell, hogy érezzék a problémát. Ehhez nulladik pontként említeném a már többször említett vezetői támogatást (engedélyt) ami a változásmenedzsment egészében jelen kell, hogy legyen. Hiszen, ha a szervezet vezetője elkötelezett egy változás mellett, úgy annak relevanciája is megalapozottabb lesz az állomány számára. Emellett fontos, hogy az alkalmazottak és a vezetők közös értékeket valljanak, és személyes felelősséget érezzenek szervezetük sikeréért.⁶⁴ Összességében, a változásra való tudatosság a legfontosabb tényező a sikeres változtatási kezdeményezés létrehozásában.

Ezt követően szorgalmazni kell, hogy az alkalmazottak aktív részesévé is váljanak a változásnak. Ehhez szükséges a képzésen megszerzett tudás, amely tartalmazza a munkavégzésükhöz szükséges biztonságtudatos készségek és biztonságtudatos magatartás megszerzését, hogy azokat a mindennapi munkavégzésük során is alkalmazni tudják. Végül pedig meg kell erősíteni bennük, hogy a technológiai fejlődés okán folyamatosan újabb lehetőségekkel bővül a támadók tárháza, így a képzést nem elég egyszer elvégezni, folyamatosan reagálni kell az újabb és újabb támadástípusokra.

A tudás, mint harmadik pont talán a legösszetettebb. Ehhez elsőként meg kell határozni a célcsoportot, akik a változás magját alkotják. A célcsoport meghatározása bár azt hinnénk könnyű, hiszen többször említettem, hogy kifejezetten az anyakönyvvezetői rétegre koncentrálódna, azonban maga az anyakönyvvezetők elég tág fogalom. Alapvetően azért gondolom így, mert sokan mások pl. egyes miniszterek, nagykövetségek munkatársai és a polgármesterek legtöbbje is rendelkezik anyakönyvi szakvizsgával, amely feltételezi, hogy az EAK-hoz is hozzáféréssel rendelkeznek. Éppen ezért a célcsoport az EAK-hoz felhasználói fiókkal rendelkezők. Jelen dolgozat írója azonban kizárólag az anyakönyvvezetőkre fókuszál.

A célcsoport már önmagában a területi megoszlás, a szakmai tapasztalat, illetve az eltérő szervezeti kultúrákból kifolyólag is széleskörű, nem koherens, hiszen tagjai eltérő információbiztonsági kompetenciákkal és magatartásokkal rendelkeznek, ráadásul a helyi önkormányzatok védelmi szintje sem összehasonlítható. Azonban, mindenkire azonos szintű veszélyek leselkednek. A támadók szempontjából nézve pedig nyilván érdemesebb egy olyan helyszínen próbálkozni, ahol feltehetően kisebb a védelmi intézkedések szintje. Éppen ezért van az anyakönyvvezetőkön, mint humán tűzfalon a legnagyobb hangsúly, hiszen ha a fizikai

⁶⁴ A. Yuryna Connolly és mtsai., „Organisational Culture, Procedural Countermeasures, and Employee Security Behaviour: A Qualitative Study”, *Information and Computer Security* 25, sz. 2 (2017. július): 118–36.

védelmi rendszerek nem is állnak feltétlen rendelkezésre (pl. beléptető kapu, kamerák) akkor ők tudják felismerni, vagy legalább ellehetetleníteni egy támadás kivitelezését a felkészültségükkel és a már említett egészséges bizalmatlansággal. Ehhez azonban folyamatos képzésekre lenne szükség, hiszen a technológiai újdonságokkal párhuzamosan a támadások is egyre szofisztikáltabbak lesznek. Ezért is szükséges -negyedik pontként- az anyakönyvvezetőket olyan kompetenciákkal, illetve biztonságtudatos magatartással kell felruházni, amely alkalmas arra, hogy a változás része legyen a szervezet életének hosszú távon. Végül pedig -ötödik pontként- erősíteni kell a munkavállalókban, hogy a változás valóban a szervezet részévé váljon, vagyis nem szabad, hogy a megszerzett tudás és a jó gyakorlatok csak rövid ideig legyenek jelen a szervezet életében.

Mindezek alapján, tehát szükség lenne egy állapotfelmérésre, hogy hol is tartanak jelenleg az anyakönyvvezetők információbiztonsági tudatosság terén. Az eltérő alapok okán -a képzést megelőzően- szükség lenne egy általános információbiztonsági tudatosságot felmérő tesztre, ami alapján kategorizálhatóak lennének az anyakönyvvezetők a felkészültségük szerint. Az előzetes teszt alapján 3 kategóriába sorolhatnánk őket: kezdő, közép-haladó, illetve haladó szintre.

4.3. fejezet Az információbiztonsági tudatosító program kialakítását befolyásoló tényezők

A továbbiakban a program megvalósíthatóságának szempontjait figyelembe véve szeretném bemutatni a szakma sajátosságait, amelyek meghatározzák az oktatás kivitelezésének, felépítésének módját.

A program időtávja nehezen meghatározható, ugyanis az IT biztonságban a tudás nagyon hamar elévül, éppen ezért fontos, hogy a képzés folytonos, továbbképzésszerű legyen, hogy értékálló, naprakész tudással rendelkezzenek. A kiberbiztonsági tudatosítási program egy hosszú távú befektetés -jelen esetben az állam részéről-, amely kizárólag folyamatos képzés esetén segíthet a kiberbiztonsági kultúra kialakításában.

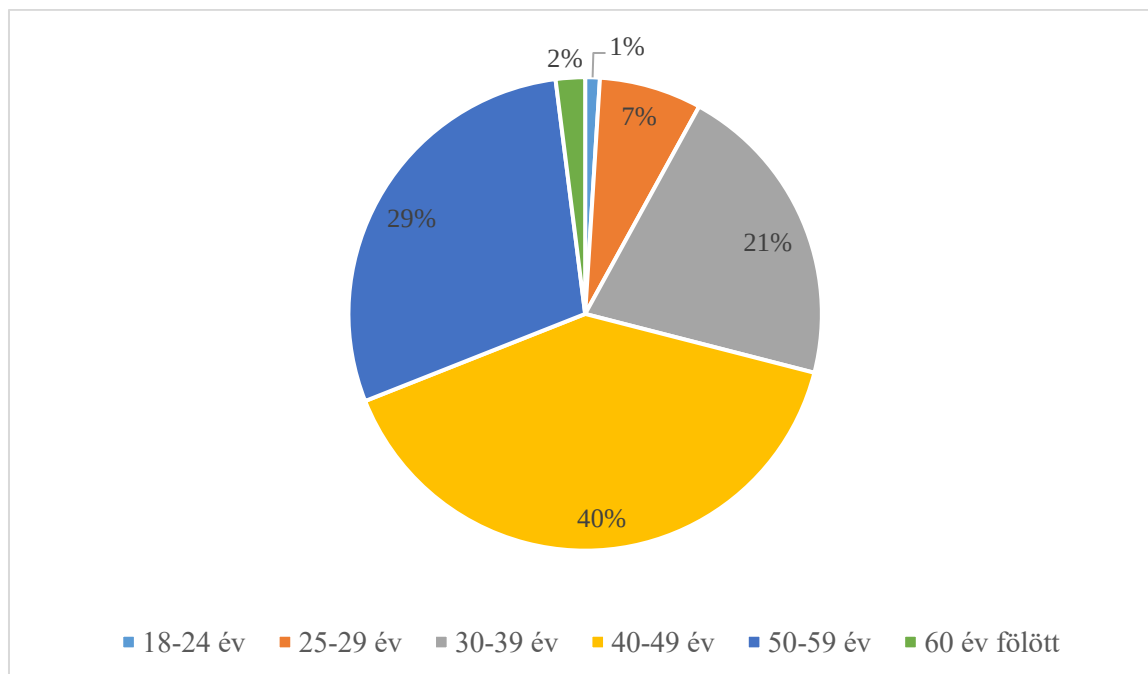
Az információs csatorna kiválasztása kulcsfontosságú. Ennek kiválasztásához elsőként szükséges az anyakönyvvezetők átlagéletkorát meghatározni. Ez azért fontos, mert az eltérő korosztályok eltérő digitális kompetenciákkal is rendelkeznek.

Marc Prensky már 2001-ben megkülönböztetett két eltérő csoportot a digitális kompetenciák szerint: e a digitális bevándorlókat és a digitális bennszülötteket.⁶⁵



9. ábra Átlagéletkor változása az állam- és önkormányzati igazgatásban 2014-2018 (Saját szerkesztés, forrás: Szakács Gábor: *A közszolgálati tisztviselők élet-és munkakörülményei, társadalmi helyzete Magyarországon*)

Egy 2018-ban készült felmérés szerint az átlagéletkor az államigazgatásban 41,09 évről 44,26 évre, az önkormányzati igazgatásban 40,8 évről 45,8 évre emelkedett 2014-hez képest.⁶⁶ Az általam készült felmérés adatai alapján készített diagramm is hasonló adatot igazol: a kérdőíves felmérésben résztvevők átlagéletkora 44,7 év volt.



10. ábra Anyakönyvvezetők életkori megoszlása

⁶⁵ Digital Natives, Digital Immigrants, Marc Prensky, On the Horizon MCB University Press, Vol. 9 No. 5, October 2001

⁶⁶ Gábor Szakács és Georgina Stréhl-Klotz, szerk., *A közszolgálati tisztviselők élet-és munkakörülményei, társadalmi helyzete Magyarországon* (Budapest: Nemzeti Közszolgálati Egyetem, 2018).

Ezáltal kijelenthető, hogy a közszolgálati állomány többségében digitális bennszülöttekből áll. Prensky értelmezésében ők az 1990-es évek előtt születtek, vagyis azelőtt, hogy a digitális technológia megjelent, illetve elterjedt. Azonban kiemelném, hogy az ISA nem generációfüggő, az egyén életkora nincs összefüggésben az információbiztonságának a szintjével. 2020-ban egy tanulmány⁶⁷ kimutatta, hogy a digitális bevándorlók korosztálya alapvetően emberi interakciót igényel az e-learning tanulási folyamatokhoz is, vagyis esetükben a tisztán e-learning formában megvalósuló képzés szinte elképzelhetetlen. Számukra egy olyan köztes megoldásról beszélhetünk, amely -ha akár e-learning keretek között valósul is meg- közvetlen interakciót biztosít. A tanulmány rámutat arra, hogy a virtuális térben folytatott interakció is kielégítőnek bizonyult az e korosztályhoz tartozók körében. Az anyakönyvvezetők működésének tekintetében azonban jelenleg is kritikus pont az anyakönyvi osztály költségvetésének megszervezése, hiszen -ahogy többször említettem- állami feladatot valósítanak meg, helyi önkormányzatok falain és -ami még lényegesebb- költségein belül. Ebben az kontextusban azonban úgy gondolom nem elvárható, hogy a sok esetben amúgy is kis költségvetéssel rendelkező helyi önkormányzatok még egy kiadási tétellel szembesüljenek az anyakönyvvezetők továbbképzése kapcsán. Vagyis, véleményem szerint ennek a projektnek alapvetően a központi költségvetésből kellene megvalósulnia. Azonban, egy a kibertérben zajló -online- oktatás költséghatékony megoldás lehetne mind az állam, mind pedig az önkormányzatok részéről is, hiszen elkerülhetőek lennének a frontális oktatással járó jelentős költségek (utazás költségei, helyszínbérlés, catering), ellenben mégis személyesebb lenne egy hagyományos e-learning képzésnél, biztosítva az interakciót a felek között.

Ami szintén indokolja az információs csatorna választását, az -a korábbi fejezetben ismertetett- anyakönyvvezetői személyi állomány nemi összetétele, vagyis a nők felülreprezentáltsága a szakmán belül. Úgy gondolom, hogy ennek okán, a képzésnek a teljesítését munkaidőben lenne szükséges abszolválhatóvá tenni. Ezt a fentiekben ismertetett átlagéletkor és a szakmabeliek nemi aránya indokolja: úgy gondolom nem elvárható egy középkorú hölgytől -akinek feltehetően családja van, hogy munka után, a mindennapi teendők mellett/helyett- e-learning képzésen vegyen részt, illetve a munkaidő utáni tanulás, vagy a szabadnapokon teljesítendő

⁶⁷Ch'ng Lay Kee: Face-to-Face Tutorial, Learning Management System and WhatsApp Group: How Digital Immigrants Interact and Engage in E-learning?

képzés elvonja a pihenő idejét, amely az újbóli munkavégzéshez szükséges regenerálódást garantálja.

A módszerrel kapcsolatban úgy gondolom, hogy rendkívül fontos -mint minden képzés esetén- hogy az aktualitásokra reagáljon, vagyis beemelhetők lennének már bekövetkezett esettanulmányok is, amelyek rámutatnának arra, hogy milyen fontos szerepe van az egyénnek a szervezet biztonságos működésének szempontjából, azok közös megvitatásának és a tapasztalatok levonásának segítségével. Az interakció által, azonban lehetőség lenne arra, hogy a képzés az anyakönyvvezetők érdeklődése szerint alakuljon, ha esetleg ők érdeklődnek egy-egy téma iránt, akkor azt is figyelembe lehetne venni. Szintén költséghatékony alternatíva lehetne, ha az oktatást az IBF tartaná. Ezáltal közvetlenebb viszony is kialakulhatna az anyakönyvvezetők és az IBF között, így nagyobb bizalommal fordulnának hozzá hosszabb távon is.

4.4. fejezet Az információbiztonsági tudatosító program tematikája

A tematika kidolgozásánál egy olyan képzés összeállítása a cél, amelyben a hangsúly a kiberbiztonsági tudatosság növelésére irányul, az anyakönyvvezetők mindennapi munkavégzése során -amely által közvetve garantálható lenne az állampolgárok személyes adatainak védelme. A program célja, hogy a résztvevők a program teljesítése után rendelkezzenek megfelelő digitális kompetenciával és szakmaspecifikus digitális készségekkel, a médiatudatosság, a biztonságos internethasználat, valamint a digitális technológia hatékony alkalmazása terén.

A képzés során elérendő kompetenciák:

1. Tudás: Az anyakönyvvezető ismerje meg azokat a fontosabb előírásokat az adatvédelmi és információbiztonsági szabályozásokból, amelyek a mindennapi munkáját befolyásolják. Legyen tisztában az állami adat- és kibervédelmi rendszerrel. Értse meg a szervezeti feladatokat az adat- és kibervédelemben, valamint ismerje a kibertámadás esetén alkalmazandó eljárásokat. Képes legyen felismerni és azonosítani az esetlegesen ellene irányuló támadásokat, valamint megelőzni, hogy ilyen jellegű támadások célpontjává váljon. Ezeken túl átlátja a munkáltatók által meghatározott belső szabályzatok megalkotásának szükségességét az információs rendszerekben tárolt adatok sértetlensége és a rendelkezésre állás tekintetében és tisztában van az emberi tényező szerepével a kibertámadások kivitelezése során.

2. Képességei: Az anyakönyvvezető legyen képes értelmezni az adat-és információbiztonsággal kapcsolatos jogszabályokból, szabályzatokból eredő követelményeket és átlátni a kibertér speciális jogállását.
3. Attitűdje: Az anyakönyvvezető munkavégzése során figyelembe veszi és alkalmazza az adatvédelemmel és kiberbiztonsággal kapcsolatos jogszabályokat, a szervezetének belső szabályzóit, így garantálja az állampolgárok személyes adatainak kezelésének biztonságát. Emellett partner abban, hogy se a szervezete, se ő maga ne váljon kibertámadás áldozatává.
4. Autonómiája és felelőssége: Munkavégzése során gyakorlatába beépíti és alkalmazza a képzésen megszerzett tudást.

Úgy gondolom, hogy elsősorban az anyakönyvvezetőkre potenciális leselkedő támadásformákat lenne érdemes bemutatni, úgymint a social engineering⁶⁸, a phishing⁶⁹, a malwarekkel⁷⁰ való visszaélés vagy a clickbait⁷¹ támadástípusokat. Szorgalmaznám továbbá a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (továbbiakban: NBSZ NKI) podcastjának releváns részeinek (pl: jelszavakkal kapcsolatos, online térben történt csalásokkal kapcsolatos anyagok) meghallgatását is. Tehát alapvetően inkább gyakorlatias, mintsem elméleti programról lenne szó, hiszen a cél a tudatos felhasználásnak a növelése. Ebből fakadóan nem kizárólag teszt formájában lenne ellenőrizve az anyakönyvvezetők információbiztonsággal kapcsolatos tudása, hanem a mindennapi munkavégzés keretei között is. Például, egy kreált phishing e-maillal(phishing szimuláció), ami által releváns statisztika is készíthető lenne arról, hányan kattintottak rá a program előtt, illetve az azon való részvétel után az abban található linkre, csatolmányokra.

Mindemellett érdemes lenne az NBSZ NKI által nyújtott sérülékenységvizsgálati szolgáltatás pszichológiai manipuláció (social engineering) vizsgálat lefolytatása is, amelyek mind a gyakorlati, vagyis a megszerzett tudás megfelelő alkalmazását vizsgálná. Az ezekből szerzett jó, illetve rossz tapasztalatok ismertetése szintén alkalmas lenne arra, hogy kifejezetten az e területről származó példákon keresztül -minél közelebb hozva az anyakönyvvezetőket a témához, prezentálva milyen veszélyeknek vannak kitéve a munkavégzésükkel kapcsolatban- mutassanak be eseteket, így is tovább növelve a tapasztalati úton történő információátadás. Amit ezzel kapcsolatban még fontosnak tartok, hogy nem

⁶⁸ olyan támadásforma, amely során a támadó az emberi tényező kihasználható tulajdonságait használja fel, hogy ily módon férjen hozzá megtevesztéssel, zsarolással a védett információkhoz, rendszerekhez.

⁶⁹ adathalászat

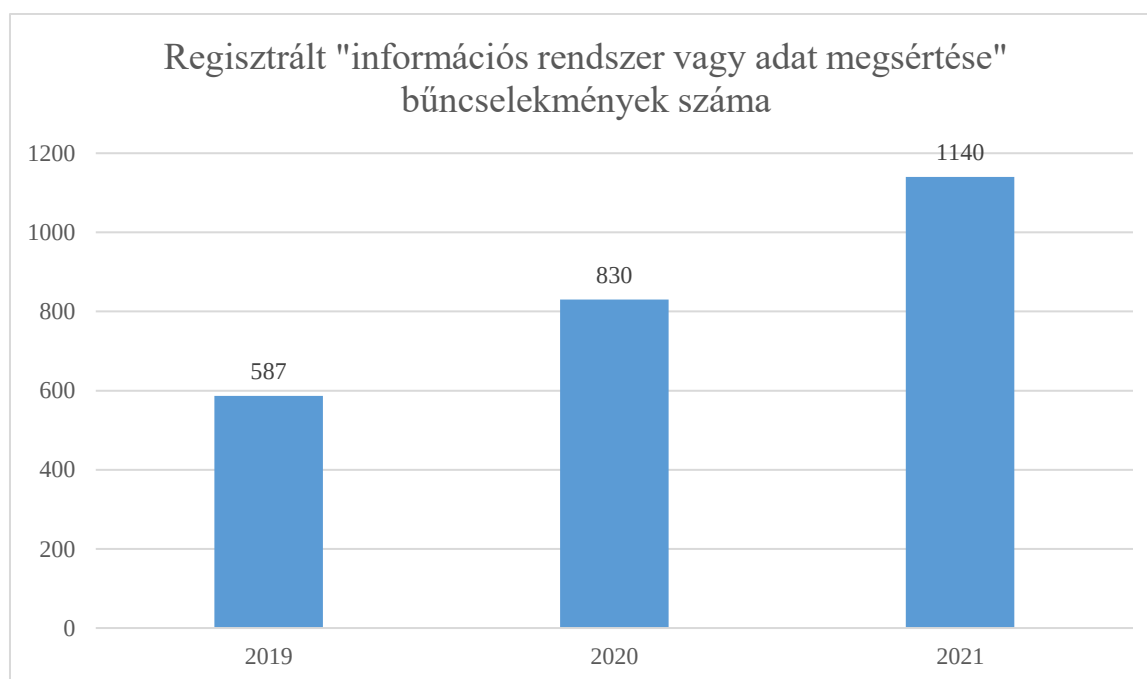
⁷⁰ rosszindulatú/ kártékony szoftver

⁷¹ kattintásvadász internetes tartalom

szabad erősíteni a jelenleg is érvényes gondolkodásmódot, miszerint kellemetlen, ha valakit támadást ért. Minden elismert és felvállalt támadás segítség lehet egy következő támadás megakadályozásában.

Ismerniük kell, hogy kihez fordulhatnak és úgy gondolom érdemes lenne az NBSZ NKI-t is bevonni a tudatosítási programba, hogy még közelebb kerülhessenek az anyakönyvvezetőkhez, ezzel is bizalmat erősítve bennük.

A kiberbűnözés formáinak ismertetése szintén a képzés egy fontos részét képezné, hiszen a kiberbűnözés célja informatikai rendszerek felhasználásával az anyagi haszonszerzés, célpontjaik között az üzleti és politikai világ szereplői egyaránt megtalálhatóak.⁷² Ezt azért tartom fontosnak, mert évről évre egyre nagyobb számban fordulnak elő a kibertérben elkövetett bűncselekmények, és feltételezhetően ez az arány a jövőben továbbra is nőni fog a hagyományos -nem a kibertérben elkövetett- bűncselekményekkel szemben.



11. ábra Regisztrált "információs rendszer vagy adat megsértése" bűncselekmények száma 2019- 2021(Saját szerkesztés, forrás:bsr.bm.hu)

Az diagramm alapján megállapítható, hogy a SARS-CoV-2 (COVID-19) (továbbiakban: COVID) okozta járvány után a kibertérben elkövetett, információs rendszer vagy adat megsértésére irányuló bűncselekmények száma 2021-re csaknem megduplázódott a járvány

⁷² Moskowitz, Sanford L.: The Global Cybercrime Industry. In: Cybercrime and Business, Strategies for Global Corporate Security, 2017, pp. 3–22.

előtti időszakhoz képest. Az oktatás relevanciáját ez a tény szintén megalapozza, hiszen a jövőben is bármikor előfordulhat olyan esemény, amennyiben az érintettek számára home office munkavégzés írható elő, amely során szintén szükséges a vonatkozó információbiztonsági képzéseken megszerzett kompetenciák és ismeretek alkalmazása. Azáltal, hogy a támadásokat bizonyos jellemzők segítségével felismerik, az alkalmazottak nagyobb valószínűséggel azonosítják a fenyegetést⁷³

A képzés időtartamakor aktuális statisztikák alapján illusztrálható lenne az aktuális kibertámadási trendek iránya, vagyis, hogy mi a legnépszerűbb támadási forma abban az időszakban és arra még nagyobb figyelmet fordítani. Mindez pedig kiegészülne egy jogszabályi keret ismertetéssel is, amely által elvárható lenne az Infotv. és a GDPR szerinti működés is. Végezetül szükséges lenne egy végső teszt kitöltése, amely a programra irányulva választ adhatna a szervezőknek, fejlesztőknek, az érintettek igényei által formálhatóvá válna.

Emellé szükség lenne e-learning tananyagok fejlesztése, amely kifejezetten az anyakönyvvezetéssel kapcsolatos információbiztonsági kérdésekre fókuszálna. A különböző szintekhez eltérő mélységű és mennyiségű modulok tartoznának, amelyek egyik legfontosabb tulajdonsága az lenne, hogy folyamatosan frissüljenek. Úgy gondolom, az e-learning anyagok által elsajátított ismeretek a mindennapi életben is hasznosíthatóak lennének, hiszen olyan ismeretekkel is szolgálna, ami munkaidőn kívül is biztosíthatja, hogy az egyének elkerülhessék a különböző, kibertérből érkező támadásokat.

A kibertérben megjelenő, jól felkészült, az ott lévő eszközöket, rendszereket és szolgáltatásokat biztonság tudatosan használni tudó felhasználók számára lehetőséget biztosító szakirányú oktatáson kívül meg kell teremteni annak a felkészítésnek és oktatásnak a rendszerszintű alapjait is, amelyek során a felhasználók valóban tisztában lesznek azokkal a legalapvetőbb ismeretekkel, amelyek segítenek számukra eligazodni a kibertérben megjelenő veszélyforrások között.⁷⁴ A tudatosság egy folyamat, nem pedig egy állapot. Az elérendő cél adott, már csak az ahhoz szükséges utat kell kikövezni. Bízom abban, hogy jelen dolgozat hasznos alapul szolgálhat az érintettek számára.

⁷³ Smith A, Papadaki M, Furnell SM. Improving Awareness of Social Engineering Attacks. In: Dodge RC, Futcher L, editors. Information Assurance and Security Education and Training. Berlin, Heidelberg: Springer; 2013, p. 249–256.

⁷⁴ Kovács, *A kibertér védelme*.

4.5. fejezet: Javaslatok a jelenlegi működési rendre vonatkozóan

Jelen fejezetben -a korábbi fejezetek megállapításai alapján- igyekszem javaslatokat megfogalmazni a jelenlegi működési rend megváltoztatására, olyan -kockázatokkal arányos- védelem kialakítására, amely egy információbiztonsági tudatosító programmal párhuzamosan kellő feltételeket biztosítana az általam vizsgált fókuszcsoporthoz megfelelő adat- és információbiztonsági tudatosságának és felkészültségének növeléséhez.

A védelem – a magyar nyelvben – tevékenység, illetve tevékenységek sorozata, amely arra irányul, hogy megteremtse, fejlessze, vagy szinten tartsa azt az állapotot, amit biztonságnak nevezünk.⁷⁵

A cél az állampolgárok személyes adatainak védelme. Ehhez kiindulópont, hogy a védelem alapvető tárgya az adat, de az adatot kezelő rendszerelemek is védendőek, hiszen ezek megfelelő állapota feltétele az adat védelmének.⁷⁶ A kockázatokkal arányos védelem kialakításának kapcsán szeretném megemlíteni az „elmaradt kár az haszon” tételt, vagyis azt, hogy a kár az veszteség, és a meghatározható valószínűségű veszteség elkerülése haszonként fogható fel. Ebből egyenesen következik, hogy a potenciálisan bekövetkező károk elkerülésére tett intézkedés nem „pénzkidobás”, hanem olyan beruházás, amely hasznot hoz.⁷⁷ Az anyakönyvvezetés tekintetében ez a haszon politikai, illetve társadalmi haszon is, hiszen a nemzeti adatvagyon részét képező EAK esetleges elérhetetlenné válása, vagy az abban tárolt adatok elvesztése politikai és társadalmi veszteségekkel is járhat.

Jó gyakorlatként szeretném megemlíteni a Magyar Államkincstár példáját, amely az Agrár-és Vidékfejlesztési támogatások kifizető ügynökségeként, a folyósításhoz szükséges ISO/IEC 27001:2013 tanúsítvány megszerzését nem a Fővárosi- és Megyei Kormányablakok egészére, hanem kizárólag az Agrár- és Vidékfejlesztést Támogató Főosztályokra (továbbiakban: AVTF) írta elő. Az anyakönyvi osztályok esetében is -tekintve, hogy az Ibtv is lehetőséget biztosít arra, hogy egyes szervezeti egységek eltérő biztonsági szintbe legyenek sorolhatóak- kialakítható lenne egy hasonló gyakorlati megoldás, amely keretében az anyakönyvi osztályok tekintetében megvalósítható lenne a kockázatokkal arányos védelem kialakítása. A védelem költségeiből származó haszon nyilvánvalóan eltérő az említett szervek esetében, hiszen az anyakönyvi

⁷⁵ Muha Lajos (2007): A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, PhD értekezés, ZMNE, Budapest, 127 p.

⁷⁶ Muha Lajos (2008): Az informatikai biztonság egy lehetséges rendszertana, In: Bolyai Szemle, XVII. évfolyam, 4. szám, Budapest.

⁷⁷ Muha Lajos (2007): A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, PhD értekezés, ZMNE, Budapest, 127 p.

hivatalok kvázi láthatatlan tevékenységet végeznek, míg a példaként szolgáló AVTF-ek évi több ezer milliárd euró folyósításáról gondoskodnak. Mégis úgy gondolom, hogy az állami élet zavartalan működésének szempontjából elkerülhetetlen -már csak a nemzeti adatvagyon részét képező EAK okán is- az anyakönyvvezetők információbiztonsági szintjének növelése a szükséges fizikai, logikai, illetve adminisztratív védelmi intézkedések bevezetése mellett. Az alábbiakban különböző védelmi intézkedések tekintetében fogalmazok meg javaslatokat.

4.5.1.fejezet: Logikai védelmi intézkedések javaslata

A logikai védelem az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem.⁷⁸ Diplomamunkámban igazoltam, hogy jelenleg nincs egy olyan kontrolltényező, amely az anyakönyvvezetők jelszóprotokolljára irányul. A kutatásomból megállapítható, hogy vannak olyan anyakönyvvezetők, akik az EAK bevezetése óta (2014), azaz 8 éve nem változtattak jelszó. Ebből kifolyólag azonnali logikai védelmi intézkedést javasolnék a jelszó-rendszerre vonatkozóan. Ennek okán mind az EAK fiókhoz, mind pedig a helyi önkormányzati számítógépeken olyan jelszóprotokollt javasolnék, amely megfelel a jelenlegi, nemzetközi jelszótrendeknek, úgymint a kis-és nagybetűk, számok, valamint speciális karakterek alkalmazásának előírásában, emellett pedig változtatása havonta kötelező lenne. A megváltoztatott jelszó továbbá nem egyezhetne meg a korábbi 5 jelszóval. Javasolnám ennek tekintetében egy állami jelszómenedzser létrehozását, amelyben a közigazgatási személyi állomány egy helyen kezelhetné jelszavait, ami által megvalósulhatna a tiszta asztal elv és eltűnhetnének a manuális jelszófeljegyzések az asztalokról, monitorokról.

4.5.2.fejezet: Adminisztratív védelmi intézkedések javaslata

Az adminisztratív védelem a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás.⁷⁹ Elsőként is szükséges lenne a változásmenedzsment stábjának felállítása, akik a folyamat egészének kialakításáért, megvalósításáért és a későbbiekben az ellenőrzésért is felelősek lennének. Tekintve, hogy véleményem szerint ez az állam részéről kezelendő probléma, így mindenféleképp központi szinten kerülne felállításra a stáb, amelynek a jelenleg működő anyakönyvi felügyelők is aktív tagjai lehetnének szakmai tapasztalatuk okán. A szabályozás tekintetében elsőként is egy, a helyi önkormányzatok IBSZ-ére vonatkozó egységes keretrendszer megalkotására tennék javaslatot, amellyel elkerülhetővé válna, hogy eltérő

⁷⁸ „2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról”

⁷⁹ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

biztonsági szintek és osztályok jelenjenek meg az önkormányzatok IBSZ-ébe. Ennek felülvizsgálata során fontosnak tartom a helyi önkormányzatok biztonsági szintjének, pontosabban az anyakönyvi szervezeti egység magasabb szintű besorolását. Indokoltnak tartanám a 3. besorolási szintet, hiszen a szakfeladatait támogató elektronikus információs rendszert használnak, de nem üzemeltetik azt. A szervezet kritikus adatot, nem minősített, de nem közérdekű, vagy közérdekből nyilvános adatot kezel, központi üzemeltetésű, és több szervezetre érvényes biztonsági megoldásokkal védett elektronikus információs rendszerek vagy zárt célú elektronikus információs rendszer felhasználója, illetve feladatai támogatására más külső szolgáltatót vesz igénybe. Ehhez a szinthez, már kapcsolódna, hogy a biztonsági kontroll folyamatokat az érintett szervezet vagy szervezeti egység tekintetében szabályozottan és ellenőrizhető módon kell bevezetni, az érintett személyek számára oktatás tárgyává tenni. Ez jogszabályi alapot jelenthetne az anyakönyvvezetők képzésének megvalósításához. Bár sok helyi önkormányzat IBSZ tartalmaz bizonyos adminisztratív védelmi előírásokat, úgy gondolom az anyakönyvi osztályok esetében minden esetben meg kellene valósulnia bizonyos szabályzatok megalkotásának. Ilyen például a kulcskezelési nyilvántartás, amely által dokumentálható lenne, hogy az adott irodába ki(k)nek van belépési jogosultsága, távollét esetén pedig ki(k) helyettesítheti(k). Mindemellett szükségesnek tartom az okoseszközök hivatali használatának korlátozását -amelyet már szintén sok IBSZ már tartalmaz. A szabályozásnak mindenekelőtt korlátoznia kell az állományba tartozás tényének nyilvános közzétételét. Ennek megalkotása során azonban érdemes a minősített információkhoz való hozzáférés függvényében kialakított kockázati profilok esetén más-más követelményt megfogalmazni.⁸⁰

A korábbi fejezetek alapján megállapítom, hogy az anyakönyvvezetők jelenleg nem rendelkeznek kellő adat-és információbiztonsági felkészültséggel a mindennapi munkavégzésükkel kapcsolatos potenciális -kiber- támadásokkal szemben. Mindemellett olyan elektronikus információs rendszereket kezelnek, illetve férnek hozzá, ami viszont szükségessé tenné egy információbiztonsággal kapcsolatos tudatosító képzés bevezetését kifejezetten erre a szakterületre fókuszálva, figyelembe véve az állomány sajátosságait. Ezáltal javaslom továbbá, hogy az anyakönyvvezetők szakvizsgájába kerüljön beépítésre, a nemzeti adatvagyon részét képező elektronikus információs rendszerek használatával kapcsolatos, valamint egy általános biztonságtudatosító tananyag, amely már a pályára lépés előtt biztonságtudatosítási alapot biztosít számukra. Emellett a pályán lévőknek is szükséges lenne egy információbiztonsággal kapcsolatos tudatosító program bevezetése, akár

⁸⁰ NBSZ NKI, „Közösségi hálózatok hivatali használata”, 2018.

továbbképzés jelleggel is, hiszen napról napra újabb és fejlettebb kihívások elé állíthatja őket a kibertér, ezért nem tartom elegendőnek egy egyszeri képzés elvégzését.

4.5.3.fejezet: Fizikai védelmi intézkedések javaslata

A fizikai védelem a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem.⁸¹

A beléptetés kapcsán elkülöníteném az épületbe való belépést az anyakönyvi irodákba való belépéstől.

A helyi önkormányzatok esetében -ahol nem épült ki 24 órás megfigyelésre alkalmas kamerarendszer- elterjedt az élőerős védelem alkalmazása az objektum tekintetében. Az így megvalósuló védelem mellett, általában a szolgálatban lévők gondoskodnak a portaszolgálat ellátásáról is, az ügyfelek útbaigazításáról és az esetleges csomagok átvételéről is 24 órában. Javaslatot tennék, hogy az ily módon megvalósuló védelem egészüljön ki a kulcsok- illetve a kulcskezelési nyilvántartás kezelésével is, hogy a kulcsok felvétele ellenőrizhetővé, a dokumentációk pedig az érintett dolgozók számára is optimális helyszínen -belépéskor- valósuljon meg.

Az anyakönyvi alapiratok tárolására szolgáló irattárak esetében beléptetőkártya használatát javasolnám. emellett pedig látogatói jegyzőkönyv vezetését is. A belépőkártya alkalmazása okán nyomon követhetővé válna ki, mikor lépett be az irattárba, a látogatási naplóból pedig az is látszana milyen célból. Komplex kamerarendszer kiépítésére tennék javaslatot, tekintve, hogy az ügyfélfogadás helyszíne jellemzően nem különül el a munkavégzés helyszínétől- jellemzően az irattárhoz való közelség, a papíralapú anyakönyvek, illetve az alapiratok elérhetősége okán-. Ennek kialakításához szükséges egy érdekmérlegelési teszt, hogy pontosan mennyi ideig tárolják a rögzített felvételeket. Emellett a látogatói nyilvántartást az ügyintézés folyamatára is kiterjeszteném, ami alapján dokumentálható lenne, hogy ki és milyen célból kereste fel az anyakönyvi hivatalt. Ez akár elektronikus formában is megvalósulhatna, de akár egy excel táblában is vezethető lenne, ki, milyen időpontban és milyen anyakönyvi eljárással kapcsolatban kereste fel az anyakönyvvezetőt. Ez a dokumentáció kiegészülve a kamerarendszerrel egy social engineering támadás esetén -természetesen, ha a hivatalban

⁸¹ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

személyes érintkezés során valósul meg-, megalapozhatná a nyomozás, illetve a támadás felderítésének sikerességét.

Preventív védelmi intézkedésként javasolnám a földszintről könnyen elérhető ablakok -főként az irattár esetében- azok ráccsal való ellátását, illetve munkaidőt követően mozgásérzékelő riasztóval való ellátását.

Az irattár tekintetében -a már fentebb említett mágneses beléptetőkártya kiépítésén túl- szükséges lenne füstérzékelők és a vízmentes oltószer kialakítása tűzesetekre, illetve az elektromos radiátorra való átállás is. Ezen védelmi intézkedések által elkerülhető lenne egy esetleges tűzeset, annak oltásával, illetve egy csőtörés általi károkozás az alapíratokban. Az alapíratok megőrzése kapcsán fontosnak tartanám a szellőzés, szükség esetben a klimatizálás megoldását is, hiszen nem megfelelő páratartalom esetén könnyen roncsolódhatnak, amelyek adatvesztéssel járnak a még az EAK-ba nem rögzített anyakönyvi események kapcsán. Emellett javasolnám a salgó polcrendszer kialakítását, illetve azok földelésbe kötését, elkerülve az esetleges feszültség alá kerülésből származó károkat.

Összességében, mindhárom védelmi intézkedés tekintetében jelentős változtatásokat kellene eszközölni a megfelelő biztonsági szint kialakításának érdekében, azonban meglátásom szerint egy megfelelő kockázatelemzés során az általam javasolt intézkedések száma optimalizálható lenne az állami költségvetéshez -esetleg a helyi önkormányzatok költségvetéséhez-. Fontosnak tartom hangsúlyozni, hogy a felsorolt védelmi intézkedések kizárólag megfelelő szintű felkészültséggel kiegészülve alkalmasak az előírányzott védelmi szint megvalósításához, amely tény szintén indokolja az információbiztonsági tudatosító program szükségességét a közszolgálati állomány adat-és információbiztonsági felkészültségének növelésének okán. Még a legerősebb technikai védelmiintézkedések sem elegendőek, ha a támadó sikeresen befolyásolja a munkavállalót.⁸²

⁸² Stirnimann S. Der Mensch als Risikofaktor bei Wirtschaftskriminalität. Wiesbaden: Springer Fachmedien Wiesbaden; 2018.

ÖSSZEGZETT EREDMÉNYEK

Diplomamunkámban igazoltam, hogy a közszeroláati személyi állomány teljes egésze a kibertámadások potenciális célpontja. Alátámasztottam, hogy a közigazgatásban eltöltött idő és az egyén adat- és információbiztonságának szintje között nincs szignifikancia. Felhívtam a figyelmet arra, hogy az anyakönyvvezetők számára szükség van egy szakmaspecifikus információbiztonsági tudatosító képzés kialakítására, megszervezésére és a gyakorlatba történő megvalósítására is. Ennek létjogosultsága abban rejlik, hogy releváns információbiztonsági tudatosítási program hiányában, valamint az azokon megszerezhető kompetenciákat és attitűdöket kikényszerítő szabályozók hiányában a közszeroláati állomány információbiztonsággal kapcsolatos magatartása önkéntes és esetleges lesz, amely nem feltétlen fog megfelelni az állampolgárok személyes adatainak védelmének érdekében elvárt szintnek. Ezek megvalósítása érdekében különböző védelmi intézkedések javaslatát fogalmaztam meg.

Fenti vizsgálatok alapján dolgozatomban az alábbi eredményeket értem el:

T1: Bizonyítottam, hogy a közszeroláati személyi állomány teljes egésze a kibertámadások potenciális célpontját képezi.

T2: Igazoltam, hogy az anyakönyvvezetők számára mielőbb szükséges egy szakmaspecifikus információbiztonsági tudatosító program kialakítása, megszervezése, illetve annak gyakorlati kivitelezése.

T3: Megállapítottam, hogy a közigazgatásban eltöltött idő és az információbiztonsági tudatosság között nincs mérhető összefüggés.

T4: Meghatároztam azokat az elérendő kompetenciákat és attitűdöket, amelyek megfelelő -azok kikényszerítésére alkalmas- szabályozókkal, illetve védelmi intézkedésekkel kiegészülve garantálhatják az állampolgárok személyes adatainak védelmét a közszeroláati személyi állomány adat-és információbiztonsági felkészültsége révén.

FELHASZNÁLT IRODALOM

Magyarország Alaptörvénye (2012).

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

Kttv. - 2011. évi CXCV. törvény a közszolgálati tisztviselőkről

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679

RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)

2018. évi CXXV. törvény a kormányzati igazgatásról

29/2012 (III.7.) Korm. rendelet a közszolgálati tisztviselők képesítési előírásairól

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

2. melléklet a 41/2015 (VII.15.) BM rendelethez

Alotaibi, Fayez, és Aziz Alshehri. „Gender Differences in Information Security Management”. *Journal of Computer and Communications* 8, sz. 3 (2020. március 4.): 53–60.

Bányász, Péter. „A közösségi média szerepe a 21. század hadseregeiben”. *Hadtudomány* 22. évfolyam, sz. 1–2: 2012.

Bányász, Péter. *Közösségi média és közszolgálat*. Budapest: Nemzeti Közszolgálati Egyetem, 2018.

Bodó, Attila Pál, Tamás Joó, és Tamás Palicz. *AZ IBTV. GYAKORLATA*. Szerkesztette Veronika Deák. Budapest: Nemzeti Közszolgálati Egyetem, 2020.

Dolenecz, József. *Az anyakönyvek államosítása*. Budapest: Grill Károly CS. és Kir. Udv. Könyvkereskedése, 1893.

Grassegger, Tanja, és Dietmar Nedbal. „The Role of Employees’ Information Security Awareness on the Intention to Resist Social Engineering”. *Procedia Computer Science*, CENTERIS 2020 - International Conference on ENTERprise Information Systems / ProjMAN 2020 - International Conference on Project MANagement / HCist 2020 - International Conference on Health and Social Care Information Systems and Technologies 2020, CENTERIS/ProjMAN/HCist 2020, 181 (2021. január 1.): 59–66.

He, Jun, és L. Freeman. „Are Men More Technology-Oriented Than Women? The Role of Gender on the Development of General Computer Self-Efficacy of College Students”. *AMCIS*, 2009.

Jeffrey M., Hiatt. „ADKAR: A model for change in business, government and our community”. *Prosci Learning Center Publications*, 2006.

Kaiser, Tamás. „Jó Állam Jelentés 2016”. Budapest, 2016.

Kárpáti, Orsolya dr. „Az elektronikus anyakönyvezés helye és szerepe a magyar közigazgatásban”. PhD értekezés, 2020.

Kovács, László. *A kibertér védelme*. Budapest: Dialóg Campus, 2018.

Magyary, Zoltán. „A közigazgatás legfőbb vezetése szervezési szempontból”. *Statisztikai Közlemények Budapest Székesfőváros Statisztikai Hivatala*, 1936, 4.

Nagyné Takács Veronika. „Hogyan írjunk informatikai biztonsági szabályzatot?” *Hadmérnök* 14, sz. 3 (2019): 113–28.

NBSZ NKI. „Közösségi hálózatok hivatali használata”, 2018.

Nemeslaki, András, és Péter Sasvári. „Az információbiztonság-tudatosság empirikus vizsgálata a magyar üzleti és közsférában”. *Infokommunikáció és jog* 11. évfolyam, sz. 4 (2014): 169–77.

Security Awareness Maturity Model, issued 2011. <https://www.sans.org/security-awareness-training/resources/maturity-model/>.

Sheng, Steve, Mandy Lanyon, Ponnurangam Kumaraguru, Lorrie Cranor, és Julie Downs. „Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions”, 1:373–82, 2010.

Szabó, Dorina Barbara. „A képviselő-testület szervezetalakítása, szabadsága és annak korlátai, különös tekintettel az anyakönyvi hivatalra”. Nemzeti Közszerológati Egyetem, 2020.

Szakács, Gábor, és Georgina Stréhli-Klotz, szerk. *A közszerológati tisztviselők élet-és munkakörülményei, társadalmi helyzete Magyarországon*. Budapest: Nemzeti Közszerológati Egyetem, 2018.

Yuryna Connolly, A., M. Lang, J. Gathegi, és D. J. Tygar. „Organisational Culture, Procedural Countermeasures, and Employee Security Behaviour: A Qualitative Study”. *Information and Computer Security* 25, sz. 2 (2017. július): 118–36.

ÁBRÁK JEGYZÉKE

1. ábra Anyakönyvvezetők nemi aránya (Saját szerkesztés)	28
2. ábra Az Ön neme? Véleménye szerint elképzelhető, hogy munkavégzése során kibertámadás célpontja lehessen?	30
3. ábra Mióta dolgozik anyakönyvvezetőként? Ismeri-e az Ön szervezetének Informatikai Biztonsági Szabályzatának adatvédelemre vonatkozó előírásait?	33
4. ábra Milyen gyakran változtatja meg az EAK-hoz tartozó jelszavát? (Saját szerkesztés) ...	40
5. ábra Cyber Attacks Statistics 2019-2021 (Saját szerkesztés, forrás: Hackmagaddon)	45
6. ábra Megcélzott szektorok az események száma szerint 2020. április-2021. július (forrás:ENISA THREAT LANDSCAPE 2021)	46
7. ábra Security Awareness Maturity Model (Saját szerkesztés, forrás: www.sans.org)	48
8. ábra ADKAR modell (Saját szerkesztés, forrás: Hiatt Jeffrey M. ADKAR:A model for change in business, government and our community	49
9. ábra Átlagéletkor változása az állam- és önkormányzati igazgatásban 2014-2018 (Saját szerkesztés, forrás: Szakács Gábor: A közszolgálati tisztviselők élet-és munkakörülményei, társadalmi helyzete Magyarországon)	52
10. ábra Anyakönyvvezetők életkori megoszlása	52
11. ábra Regisztrált "információs rendszer vagy adat megsértése" bűncselekmények száma 2019- 2021(Saját szerkesztés, forrás:bsr.bm.hu)	56

RÖVIDÍTÉSEK JEGYZÉKE

Rövidítés	Magyar nyelvű magyarázat	Angol nyelvű magyarázat
Aktv	2010. évi I. törvény (továbbiakban: Aktv.)	
Alaptörvény	Magyarország Alaptörvénye	
AVTF	Agrár- és Vidékfejlesztést Támogató Főosztályok	
COVID	SARS-CoV-2 (COVID-19)	
Eak	Elektronikus Anyakönyvi Rendszer	
ENISA	Európai Unió Kiberbiztonsági Ügynökség	European Union Agency for Cybersecurity
GDPR	Európai Unió Általános Adatvédelmi Rendelete	General Data Protection Regulation
IBF	A szervezet elektronikus információs rendszerei védelmének felelőse	
IBSZ	Informatikai Biztonsági Szabályzatában	
Ibtv	Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény	
Infotv	Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény	
ISA	Információbiztonsági-tudatosság	Information Security Awareness
Kit	A kormányzati igazgatásról szóló 2018. évi CXXV. törvény	
Kttv	A közszolgálati tisztviselőkről szóló 2011. évi CXCV törvény	
NBSZ NKI	Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet	

NISZ

Nemzeti Infokommunikációs
Szolgáltató Zrt

NKE

Nemzeti Közszerológati Egyetem

FÜGGELÉKEK/MELLÉKLETEK

1.számú melléklet (Kérdőíves felmérés kérdései)

A kitöltésben résztvevőkre vonatkozó kérdések
Az Ön neve?
Az Ön életkora?
Mióta dolgozik anyakönyvvezetőként?
Szakma specifikus kérdések
Mióta használja az Elektronikus Anyakönyvi Rendszert (EAK-ot)?
Véleménye szerint elképzelhető, hogy munkavégzése során kibertámadás célpontja lehessen?
Jelszó használatra vonatkozó kérdések
Milyen gyakran változtatja a munkahelyi (nem az EAK eléréséhez szükséges) számítógépéhez tartozó jelszavát?
Milyen gyakran változtatja meg az EAK-hoz tartozó jelszavát?
Információbiztonsággal kapcsolatos kérdések
Ismeri-e az Ön szervezetének Informatikai Biztonsági Szabályzata (IBSZ) adatvédelemre vonatkozó előírásait?
Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető?
Ismer-e biztonságos jelszóalkotásra vonatkozó ajánlásokat? Amennyiben igen, alkalmazza-e azokat?
Használ-e az EAK eléréséhez szükséges számítógépén képernyőzárolást, ha elhagyja a munkaterületét?
Hallott-e már a tiszta asztal elvéről? Amennyiben igen, alkalmazza-e?

2.számú melléklet (Kérdőív kiértékelése)

Az Ön neme? * Véleménye szerint elképzelhető, hogy munkavégzése során kibertámadás célpontja lehessen? Crosstabulation

		Véleménye szerint elképzelhető, hogy munkavégzése során kibertámadás célpontja lehessen?			Total
		Igen	Nem	Talán	
Az Ön neme?	Férfi	Count	3	1	5
		% within Az Ön neme?	60,0%	20,0%	100,0%
	Nő	Count	40	56	89
		% within Az Ön neme?	21,6%	30,3%	48,1%
Total	Count	43	57	90	190
	% within Az Ön neme?	22,6%	30,0%	47,4%	100,0%

Correlations

		Az Ön neme?	Véleménye szerint elképzelhető, hogy munkavégzése során kibertámadás célpontja lehessen?
Az Ön neme?	Pearson Correlation	1	,133
	Sig. (2-tailed)		,067
	N	190	190
Véleménye szerint elképzelhető, hogy munkavégzése során kibertámadás célpontja lehessen?	Pearson Correlation	,133	1
	Sig. (2-tailed)	,067	
	N	190	190

Mióta dolgozik anyakönyvvezetőként? * Ismeri-e az Ön szervezetének Informatikai Biztonsági Szabályzata (IBSZ) adatvédelemre vonatkozó előírásait? Crosstabulation

			Ismeri-e az Ön szervezetének Informatikai Biztonsági Szabályzata (IBSZ) adatvédelemre vonatkozó előírásait?		
			Igen	Nem	Total
Mióta dolgozik anyakönyvvezetőként?	5 évnél kevesebb ideje	Count	49	22	71
		% within Mióta dolgozik anyakönyvvezetőként?	69,0%	31,0%	100,0%
	5-10 éve	Count	35	15	50
		% within Mióta dolgozik anyakönyvvezetőként?	70,0%	30,0%	100,0%
	11-15 éve	Count	21	6	27
		% within Mióta dolgozik anyakönyvvezetőként?	77,8%	22,2%	100,0%
	16-20 éve	Count	7	6	13
		% within Mióta dolgozik anyakönyvvezetőként?	53,8%	46,2%	100,0%
	21-25 éve	Count	3	5	8
		% within Mióta dolgozik anyakönyvvezetőként?	37,5%	62,5%	100,0%
	25 évnél több ideje	Count	10	11	21
		% within Mióta dolgozik anyakönyvvezetőként?	47,6%	52,4%	100,0%
	Total	Count	125	65	190
		% within Mióta dolgozik anyakönyvvezetőként?	65,8%	34,2%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability
Pearson Chi-Square	9,195 ^a	5	,102	,100		
Likelihood Ratio	8,939	5	,112	,132		
Fisher's Exact Test	8,975			,104		
Linear-by-Linear Association	5,027 ^b	1	,025	,026	,015	,003
N of Valid Cases	190					

a. 2 cells (16,7%) have expected count less than 5. The minimum expected count is 2,74.

b. The standardized statistic is 2,242.

Mióta dolgozik anyakönyvvezetőként? * Hallott-e már a tiszta asztal elvéről? Amennyiben igen, alkalmazza-e?
Crosstabulation

			Hallott-e már a tiszta asztal elvéről? Amennyiben igen, alkalmazza-e?			
			Igen, hallottam és alkalmazom is a munkavégzés em során	Igen, hallottam, de nem alkalmazom a munkavégzés em során	Nem	Total
Mióta dolgozik anyakönyvvezetőként?	5 évnél kevesebb ideje	Count	21	7	43	71
		% within Mióta dolgozik anyakönyvvezetőként?	29,6%	9,9%	60,6%	100,0%
	5-10 éve	Count	11	8	31	50
		% within Mióta dolgozik anyakönyvvezetőként?	22,0%	16,0%	62,0%	100,0%
	11-15 éve	Count	10	4	13	27
		% within Mióta dolgozik anyakönyvvezetőként?	37,0%	14,8%	48,1%	100,0%
	16-20 éve	Count	1	1	11	13
		% within Mióta dolgozik anyakönyvvezetőként?	7,7%	7,7%	84,6%	100,0%
	21-25 éve	Count	1	0	7	8
		% within Mióta dolgozik anyakönyvvezetőként?	12,5%	0,0%	87,5%	100,0%
	25 évnél több ideje	Count	6	2	13	21
		% within Mióta dolgozik anyakönyvvezetőként?	28,6%	9,5%	61,9%	100,0%
Total	Count	50	22	118	190	
	% within Mióta dolgozik anyakönyvvezetőként?	26,3%	11,6%	62,1%	100,0%	

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability
Pearson Chi-Square	9,362 ^a	10	,498	,504		
Likelihood Ratio	10,769	10	,376	,459		
Fisher's Exact Test	8,299			,579		
Linear-by-Linear Association	,558 ^b	1	,455	,466	,237	,016
N of Valid Cases	190					

a. 7 cells (38,9%) have expected count less than 5. The minimum expected count is ,93.

b. The standardized statistic is ,747.

Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető? *
Ismer-e biztonságos jelszóalkotásra vonatkozó ajánlásokat? Amennyiben igen, alkalmazza-e azokat? Crosstabulation

			Ismer-e biztonságos jelszóalkotásra vonatkozó ajánlásokat? Amennyiben igen, alkalmazza-e azokat?			Total
			Igen, de nem alkalmazom azokat	Igen, és alkalmazom is azokat	Nem	
Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető?	Igen	Count	17	39	10	66
		% within Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető?	25,8%	59,1%	15,2%	100,0%
	Nem	Count	29	54	41	124
		% within Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető?	23,4%	43,5%	33,1%	100,0%
Total	Count		46	93	51	190
	% within Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető?		24,2%	48,9%	26,8%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	7,375 ^a	2	,025
Likelihood Ratio	7,825	2	,020
Linear-by-Linear Association	3,458	1	,063
N of Valid Cases	190		

a. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 15,98.

Mióta dolgozik anyakönyvvezetőként? * Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető? Crosstabulation

			Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető?		Total
			Igen	Nem	
Mióta dolgozik anyakönyvvezetőként?	5 évnél kevesebb ideje	Count	22	49	71
		% within Mióta dolgozik anyakönyvvezetőként?	31,0%	69,0%	100,0%
	5-10 éve	Count	21	29	50
		% within Mióta dolgozik anyakönyvvezetőként?	42,0%	58,0%	100,0%
	11-15 éve	Count	11	16	27
		% within Mióta dolgozik anyakönyvvezetőként?	40,7%	59,3%	100,0%
	16-20 éve	Count	4	9	13
		% within Mióta dolgozik anyakönyvvezetőként?	30,8%	69,2%	100,0%
	21-25 éve	Count	1	7	8
		% within Mióta dolgozik anyakönyvvezetőként?	12,5%	87,5%	100,0%
	25 évnél több ideje	Count	7	14	21
		% within Mióta dolgozik anyakönyvvezetőként?	33,3%	66,7%	100,0%
	Total	Count	66	124	190
		% within Mióta dolgozik anyakönyvvezetőként?	34,7%	65,3%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)	Point Probability
Pearson Chi-Square	3,887 ^a	5	,566	,575		
Likelihood Ratio	4,171	5	,525	,545		
Fisher's Exact Test	3,711			,598		
Linear-by-Linear Association	,091 ^b	1	,763	,783	,403	,035
N of Valid Cases	190					

a. 2 cells (16,7%) have expected count less than 5. The minimum expected count is 2,78.

b. The standardized statistic is ,301.

Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető? *
Véleménye szerint elképzelhető, hogy munkavégzése során kibertámadás célpontja lehessen?
Crosstabulation

			Véleménye szerint elképzelhető, hogy munkavégzése során kibertámadás célpontja lehessen?			Total
			Igen	Nem	Talán	
Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető?	Igen	Count	20	17	29	66
		% within Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető?	30,3%	25,8%	43,9%	100,0%
	Nem	Count	23	40	61	124
		% within Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető?	18,5%	32,3%	49,2%	100,0%
Total	Count		43	57	90	190
	% within Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvvezető?		22,6%	30,0%	47,4%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	3,488 ^a	2	,175
Likelihood Ratio	3,400	2	,183
Linear-by-Linear Association	1,940	1	,164
N of Valid Cases	190		

a. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 14,94.

Mióta használja az Elektronikus Anyakönyvi Rendszert (EAK-ot)? * Milyen gyakran változtatja meg az EAK-hoz tartozó jelszavát? Crosstabulation

		Milyen gyakran változtatja meg az EAK-hoz tartozó jelszavát?					Total
		Havonta	3-6 havonta	Évente	Több évente	Nem változtattam	
Mióta használja az Elektronikus Anyakönyvi Rendszert (EAK-ot)?	Bevezetésétől kezdve (2014. 07. 01.)	3	4	3	2	82	94
		3,2%	4,3%	3,2%	2,1%	87,2%	100,0%
	2015	0	0	0	0	8	8
		0,0%	0,0%	0,0%	0,0%	100,0%	100,0%
	2016	0	0	0	1	15	16
		0,0%	0,0%	0,0%	6,3%	93,8%	100,0%
	2017	0	1	1	0	12	14
		0,0%	7,1%	7,1%	0,0%	85,7%	100,0%
	2018	0	2	3	0	15	20
		0,0%	10,0%	15,0%	0,0%	75,0%	100,0%
	2019	2	2	0	2	10	16
		12,5%	12,5%	0,0%	12,5%	62,5%	100,0%
	2020	0	3	0	0	12	15
		0,0%	20,0%	0,0%	0,0%	80,0%	100,0%
	2021	0	0	0	0	5	5
		0,0%	0,0%	0,0%	0,0%	100,0%	100,0%
Total		5	12	7	5	161	190
		2,6%	6,3%	3,7%	2,6%	84,7%	100,0%

Kruskal-Wallis Test

Ranks			
		Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvezető?	
		N	Mean Rank
Milyen gyakran változtatja meg az EAK-hoz tartozó jelszavát?	Igen	66	93,85
	Nem	124	96,38
	Total	190	

Test Statistics^{a,b}

Milyen gyakran változtatja meg az EAK- hoz tartozó jelszavát?	
Kruskal-Wallis H	,227
df	1
Asymp. Sig.	,634

a. Kruskal Wallis Test

b. Grouping Variable: Vett-e részt információbiztonsági tudatossággal kapcsolatos képzésen mióta anyakönyvezető?

