Óbudai Egyetem

Doktori (PhD-) értekezés

Önkormányzatok kiberbiztonságának és online képességének vizsgálata, figyelemmel az emberi tényező fejlesztésének kérdéseire

Számadó Róza

Témavezető

Prof. Dr. Rajnai Zoltán

Biztonságtudományi Doktori Iskola

Budapest, 2018

Komplex vizsga bizottság:

Elnök:

Prof. Dr. Berek Lajos, ÓE

Tagok:

Prof. Dr. Tózsa István, NKE

Prof. Dr. Rajnai Zoltán, ÓE

Nyilvános védés bizottsága:

Elnök:

Prof. Dr. Berek Lajos, ÓE

Titkár:

Dr. Szűcs Endre, ÓE

Tagok:

Prof. Dr. Makó Csaba, MTA

Dr. Dombovári Ella, ÓE

Dr. Budai Balázs, NKE

Bírálók:

Prof. Dr. Tózsa István, NKE

Prof. Dr. Bukovics István, NKE

Nyilvános védés időpontja

2018. 07. 11.

TARTALOMJEGYZÉK

Bevezetés 7

1. Információbiztonság – kiberbiztonság 11

1.1. Biztonság, biztonságtudomány 11

1.1.1. Biztonság 11

1.1.2. Kritikus infrastruktúra 13

1.1.3. Információbiztonság 16

1.2. Kiberbiztonság 18

1.2.1. A kiberbiztonság fogalmi keretei 18

1.2.2. Kiberfenyegetettség 20

1.2.3. Kiberfenyegetettség trendjei, típusai 22

1.3. Központi és helyi kormányzati rendszerek kiberbiztonsági kérdései 27

Összefoglalás 29

2. Európai és hazai Szabályozási és szervezeti keretek 31

2.1. Az európai uniós szabályozási keretek 31

2.1.1. Az Európai Parlament és az Európai Tanács koncepcionális álláspontja egy erős európai kiberbiztonság kialakításáról 31

2.1.2. Európai Unió szabályozási keretei a kiberbiztonság területén 32

2.1.3. Európai Unió szabályozási keretei az adatkezelésről (GDPR: General Data Protection Regulation) 35

2.2. Az európai nemzetek kiberbiztonsági stratégiáinak összehasonlítása 35

2.3. Hazai szabályozási és szervezeti keretek 38

2.3.1. Magyarország kiberbiztonsági stratégiája 38

2.3.2. Az állami és önkormányzati szervek elektronikus információbiztonsága 40

2.3.3. Szervezeti keretek 41

2.3.4. Kormányzati kiberkoordináció 43

2.3.5. Önkormányzati koordináció 45

2.4. Digitális állam 46

Összefoglalás 50

3. Helyi igazgatás, Önkormányzatok 52

3.1. Az önkormányzati rendszer elhelyezkedése a kormányzati rendszerben 52

3.1.1. Önkormányzás, önkormányzatiság 52
3.2. Önkormányzati feladatok és hivatali szerkezet 53
3.2.1. Önkormányzati feladatok 53
3.2.2. Településszekezet és feladatellátás 54
3.3. Elvárások és megfelelés 57
3.3.1. Az Információbiztonsági törvénynek való megfelelés 57
3.3.2. Az Infotörvény elvárásainak való megfelelés 61
3.4. Humán erőforrásfejlesztés, a tudatosság növelése 64
3.4.1. Oktatási stratégiai keretek 64
3.4.2. Kihívások, jó gyakorlatok 66
3.4.3. Képzési tapasztalatok 67
3.5. Önkormányzati vezetők feladatai a kritikus infrastruktúrák védelmében 69
Összefoglalás 70
4. Önkormányzatok kiberbiztonsági helyzetének és online képességének vizsgálata 73
4.1. Online kérdőíves felmérés 73
4.1.1. A kérdőív háttere 73
4.1.2. A kérdőív feldolgozásának módszerei 75
4.2. Az online felmérés eredményeinek elemzése 78
4.2.1. Vizsgált terület (I.): kibertér – kiberbiztonság – az önkormányzatok kiberfenyegetettsége 78
4.2.4. Vizsgált terület (II.): felkészültség – képzettség – az önkormányzatok kiberbiztonsági jellemzői 97
4.2.5 Vizsgált terület (II.): felkészültség – képzettség – védekező/reagáló képesség 104
4.2.6. Vizsgált terület (III.): működési tapasztalatok 109
4.2.7. Önkormányzatok kiberbiztonsági kérdőívének fő megállapításai 114
4.3. Az önkormányzatok online megjelenési képessége – webability 119
4.3.1. A vizsgálat háttere 119
4.3.2. Az önkormányzatok online megjelenésének statisztikai elemzése 119
4.3.3. Az önkormányzatok onlineképesség-vizsgálatának eredményei 126
4.4. Fókuszcsoportos interjú 127
4.4.1. A fókuszcsoportos interjúkészítés technikájának bemutatása 127
4.4.2. A fókuszcsoport gyakorlatának feltételei, lefolytatása 127

4.4.3. A fókuszcsoportos vizsgálat során tervezett/feltett kérdések 128
4.4.4. A fókuszcsoportos vizsgálat tanulságai 128
4.5. Az empirikus kutatás legfontosabb következtetései 134
4.5.1. Megállapítások 134
4.5.2. Következtetések, javaslatok 136
Összegzett következtetések 138
A kutatómunka összegzése 138
Új tudományos eredmények 139
Ajánlások 140
Irodalomjegyzék 141
Rövidítésjegyzék 147
Táblázatjegyzék 148
Ábrajegyzék 149
Mellékletek 152
Függelék 167
Köszönetnyilvánítás 173

BEVEZETÉS

Az önkormányzatok infraszuverén kormányzati szintként a helyi közügyekben és a helyi közszolgáltatások ellátásában önálló döntési hatáskörrel rendelkeznek. A helyi szinten alkotott politikák általában jobban megfelelnek a fejlődés követelményeinek, mert nagyobb a rálátásuk a helyi viszonyokra, ugyanakkor rendkívül nagyok a különbségek és kiegyensúlyozatlan a fejlődés az ország egyes területei között, ami köszönhető a magyar aprófalvas településszerkezetnek és az ebből fakadó különböző lokális gazdasági háttérnek. Az információs társadalom jelentős kihívást jelent számukra, mivel kettős nyomásnak kell megfelelniük. Egyrészt – az állampolgárok bizalmának fenntartása érdekében – a helyi hatóságoknak fokozott figyelmet kell fordítani a közérdekű adatok nyilvánossá tételére, másrészt a rájuk bízott információk biztonságára, így a „webability", online képesség és a kibervédelem, a reziliencia egyre fontosabb szerepet tölt be egy helyi szervezet életében.

A tudományos probléma megfogalmazása

A dolgozatom, a kutatás fókuszpontjában a helyi önkormányzatok online megjelenési és kiberbiztonsági képességének a vizsgálata áll az emberi tényező jelenőségének fokozott figyelembevételével.

Képesek-e eleget tenni a nyilvánossággal kapcsolatos állampolgári elvárásoknak? Eleget tesznek-e az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.) előírásainak? Milyen fenyegetettséggel nézhetnek szembe? Tudatában vannak-e a fenyegetettség hatásainak? Rendelkeznek-e a szükséges eszközökkel, felkészült emberi erőforrással? Eleget tesznek-e az állami és önkormányzati szervek elektronikus információbiztonságáról szóló a 2013. évi L. törvény (Ibtv.) által elvárt előírásoknak? Rendelkeznek-e az információbiztonságot támogató szabályozással?

Tanulmányaim, elméleti kutatásaim és a gyakorlati tapasztalataim mind azt támasztják alá, hogy az emberi tényező szerepe meghatározó erőforrás a szervezetek életében, és ez különösen igaz az információstársadalomban, az információbiztonsági kérdésekben. Az ember–technika–környezet komplex rendszert alkot az információs társadalomban. Véleményem és tapasztalataim szerint a technológiai, szabályozási kérdések alapos figyelmet kapnak, ám az emberi tényező változási helyzetre való reagálásának figyelembe vétele, fejlesztése, kezelése nem kap kellő hangsúlyt, nincs megfelelően a rendszerbe illesztve.[1] Szervezetfejlesztői munkám során rendszeresen igazolódott, hogy az emberi tényező fejlesztése csak komplexen, a rendszer elvárásaihoz illesztve valósítható meg. Nem elfeledkezve arról, hogy ez egy olyan folyamat, amelyben eddig soha nem tapasztalt szoros kapcsolat van az élethosszig tartó tanulás koncepciójának a való élethez.

Kutatásomban arra keresem a választ, hogy kialakítható-e olyan tudatosítási, képzési és együttműködési rendszer, ami hozzásegíti az önkormányzatokat a velük szemben támasztott állampolgári és kiberbiztonsági elvárások teljesítéséhez.

[1] A különböző szakirodalmi források, cikkek az információbiztonság humán erőforrást érintő kérdéseinek tárgyalása során összefoglalóan „emberi" tényezőként említik, ezért jelen dolgozatban én is ebben a formában használom.

A témaválasztás indoklása

A témaválasztást több tényező is indokolja. Egyrészt személyes ambíciók a szervezeti működés, szervezetfejlesztés kérdéskörében és az infokommunikáció rohamos fejlődése által generált változás okozta szervezeti átalakulás vizsgálatában. Másrészt az ezredforduló óta foglalkozom különböző szerepekben az önkormányzatokkal. Szervezetfejlesztőként, változásmenedzsment tanácsadóként és az elmúlt években mint a szakmai támogatást és felügyeletet biztosító minisztérium szakmai területének aktív részese. Szakmailag és személyesen is érdekes, fontos téma számomra az önkormányzati kötelezettségek teljesítése, teljesíthetősége, az önkormányzatok dolgozóinak információbiztonsági tudatossága, valamint ezen belül a kiberbiztonsági kérdések által felvetett felelősség és annak teljesítésére való képesség. Harmadrészt lenyűgöz az infokommunikáció (IKT)[2] által kínált lehetőségek széles tárháza, és elgondolkodtat a benne rejlő veszély.

Az önkormányzatok – az önkormányzás jogának gyakorlása során – fő felelőssége, hogy feladatvégzés közben a település lakosságának érdekeit szolgálja. Az önkormányzatok, működésük során sok szempontból állnak kettős nyomás alatt. Egyrészt azonosítható elvárás a globalitás és lokalitás kérdéseiben a nyitottság, az információ minél szélesebb körű megosztása, a XXI. század közösségi médiáinak használata. A másik oldalon pedig a kiberbiztonság biztosítása érdekében felmerülő teendők. Az önkormányzatokra a helyi igazgatás letéteményeseiként jelentős felelősség és feladatmennyiség hárul az utóbbi területen is, aminek kezelésére nem, vagy nem teljes körűen vannak felkészülve.

Az IKT rendszereire épülő, összekapcsolt infrastruktúrák által alkotott globális virtuális tér: a kibertér, aminek rosszindulatú felhasználására számtalan lehetőség kínálkozik. A kibertérből érkező kihívások és fenyegetések folyamatos, dinamikus bővülése egyre szignifikánsabb veszélyt jelent. Az állami és helyi önkormányzati hivatalok hatalmas nyomás alatt vannak az adataik, infrastruktúrájuk és szolgáltatásaik biztonságossá tételét tekintve. Nagyon fontos, hogy a mérvadó döntéshozók központi és helyi szinten is felismerjék a kockázat nagyságát, rendelkezzenek stratégiával, felkészült humán erőforrással és a megfelelő eszközökkel annak érdekében, hogy időben és elvárható hatékonysággal tudjanak reagálni, amennyiben ez szükségessé válik.

Az értekezés megközelítése, nézőpontja a szervezeti hozzáállás, tudatos működés, az emberi tényező, a humán erőforrás vizsgálata, és nem célja a technikai kérdések, a kiberfenyegetések kezelésének részletes kifejtése.

Célkitűzés(ek)

1. Célként fogalmaztam meg, hogy javaslatot teszek a kiberbiztonság területén a központi és a helyi kormányzati feladatmegosztás és együttműködés kereteire. Mindezt a hatékonyság javítása érdekében, differenciáltan az önkormányzati rendszer sajátosságaihoz igazítva.

[2] Az „information and communication technology” kifejezés az 1980-as években jelent meg. Az angol szakirodalomban ICT rövidítéssel használják, a magyar szövegekben pedig IKT-ként. Többféle módon értelmezik, jelen esetben átfogó kifejezésként kerül használatra. Jelöli mindazon számítógépeket és elektronikus rendszereket, amelyek alkalmasak adatok elektronikus gyűjtésére, tárolására, felhasználására és továbbítására, továbbá jelenti az ezekhez kapcsolódó alkalmazásokat és szolgáltatásokat is.

2. Célként fogalmaztam meg az önkormányzatok kiberbiztonsági tudatosságának és a reziliencia javításának érdekében egy javaslat előterjesztését a képzési/továbbképzési rendszerre, érintettjeire és módszereire tekintve.
3. Célként fogalmaztam meg az információbiztonság növelése érdekében általános és napi működési ajánlások megfogalmazását az önkormányzatok részére.
4. Célul tűztem ki, hogy feltérképezem, csoportosítom és jellemzem az önkormányzatokat online képességük (webability) alapján.

A téma kutatásának hipotézisei

1. Gyakorlati tapasztalataim azt mutatják, hogy a kormányzat és az önkormányzatok között nem alkalmazzák a kooperációból és koordinációból származó előnyöket. Feltételezem, hogy ennek az együttműködésnek a keretei csak hatósági szempontból kimunkáltak.
2. Feltételezem, hogy az önkormányzatok online képességének szintje alacsony és, hogy az online képesség pedig összefüggést mutat gazdasági helyzetükkel, lakosságszámukkal és hivatali struktúrájukkal.
3. Tapasztalom, hogy az önkormányzatok vezetői, munkatársai nem, vagy csak részlegesen ismerik az IT-biztonsági kockázatokat, a biztonságtudatosság az önkormányzati hivatalokban jellemzően alacsony szintű. Feltételezem, hogy az önkormányzat vezetői és tisztségviselői nincsenek a megfelelő tudás birtokában és a megfelelő tudatosítási és képzési rendszer jelentősen csökkentené a kiberbiztonsági incidensek előfordulását.
4. Az önkormányzatokkal végzett munkám tapasztalatai alapján feltételezem, hogy az önkormányzatok nem rendelkeznek megfelelő gyakorlati tervekkel, protokollokkal az esetleges események, incidensek kezelésére.
5. Feltételezem, hogy az online képesség mellett a kiberbiztonság megvalósítása területén fennálló problémák a szakember- és kapacitáshiányra vezethetők vissza.

Kutatási módszerek

Kutatásom során a kiberbiztonsági kérdéseken túl vizsgáltam a szabályozottság kérdését és szükségszerűen az önkormányzati működés sajátosságait, az önkormányzati rendszer felépítését. Kutatómunkám során törekedtem az elméleti összefüggések és a gyakorlati alkalmazás komplex vizsgálatára. A szakirodalom-elemzés és a szabályozási gyakorlatot bemutató dokumentumok elemzésének fő feladata a kutatás megalapozása és az eredmények rendszerbe illesztése volt. Jelentős számú stratégiai irányokat és szabályozási kereteket tartalmazó dokumentumot dolgoztam fel nemzetközi és hazai viszonylatban. Ez mind segítette megismerni a nemzetközi és a hazai működés elméleti és gyakorlati kereteit az európai és hazai kibertérben.

A feldolgozott szakirodalmak részint hazai forrásból származtak; esetükben – a relevancia értékelését követően – törekedtem a frissességre. A nemzetközi szakirodalmak feldolgozásánál a források nagy száma, illetve a nyelvi korlátok miatti kényszerű szelekció behatárolták a vizsgálati kört, és leszűkítették azt az angol nyelven megjelent irodalomra. Elméleti kutatásomban a hatályos

jogszabályok figyelembevételével közelítettem meg a kérdéseket, végül a gyakorlati megvalósíthatóság elvét tekintettem célnak.

A dokumentumelemzés az információbiztonság, a kiberbiztonság fogalmi meghatározásától a gyakorlati kérdések áttekintéséig terjedt, különös tekintettel a kormányzati és az önkormányzati tapasztalatokra. Az európai és hazai szabályozást és a szervezeti keretek kialakításának és változásának áttekintését jelentős számú állásfoglalás, stratégiai dokumentum és jogszabály segítette. Az egyes nemzeti kiberbiztonsági stratégiák összehasonlítása lehetőséget teremtett jó gyakorlatok megismerésére. Kormányzati megközelítések, tapasztalatok és különböző elemzések már elérhetőek, azonban az önkormányzatok kiberbiztonsági területen szerzett – nemzetközi és hazai – működési tapasztalatairól nem áll rendelkezésre jelentős számú tanulmány. A fellelhető amerikai, angol elemzések, összefoglalók és a NEIH által rendelkezésemre bocsátott információk jelentősen segítették az önkormányzatok kiberbiztonsági helyzetének, képességeinek, nehézségeinek és működésének megértését. A dokumentum- és kutatáselemzéseket minden esetben saját kutatási témámhoz kapcsolódóan végeztem. A dolgozat elkészítésével célom egy az önkormányzatok online képességeinek kiberbiztonsági kérdéseit átfogó vizsgálat megalkotása volt, különös figyelemmel az emberi tényezőre.

A megismert elméleti és szabályozási keretekre építve összeállítottam egy kérdőívet, amely kiküldésre került a teljes önkormányzati kör részére. Célja az egyes önkormányzatok kiberbiztonsággal kapcsolatos attitűdjének, képességéknek és gyakorlatának megismerése volt.

A BM országos önkormányzati adatfelvételét felhasználva faktor- és klaszteranalízist végeztem annak érdekében, hogy feltárjam az önkormányzatok online képességének jellemzőit.

Fókuszcsoportos interjút folytattam le a kutatási fázis végén a kapott eredmények értelmezése és a kérdéskörök tisztázása céljából.

Különös figyelmet fordítottam a nemzetközi és a hazai gyakorlati tapasztalatok elemzésére, az adatelemzésre és az online felmérés eredményeinek vizsgálatára, továbbá az értékelhető következtetések megfogalmazására. A kutatás lezárásra került 2018. február 15-én.

1. INFORMÁCIÓBIZTONSÁG – KIBERBIZTONSÁG

Az első fejezetben a biztonságtudomány fogalomkörét és vizsgálati területének bemutatását követően részletesen foglalkozom az információbiztonság és kiberbiztonság fogalmi kereteivel és a jelenlegi helyzetével, továbbá a kormányzati szektor információs rendszereivel kapcsolatos kérdésekkel.

1.1. Biztonság, biztonságtudomány

Az alfejezet célja a fogalmi alapozás és a biztonságtudomány vizsgálati területének bemutatása.

1.1.1. Biztonság

Az emberek, a közösségek életében a biztonság, mint elvárás mindig alapvető szükségletként volt és van jelen. Jelentését/fogalmát többen, többféleképpen határozták meg. Bukovics megfogalmazásában a biztonság olyan folyamat, amely az emberi tudatban jelenik meg és amelynek kiinduló eleme az ember életösztöne. Ebből levezethető a biztonságérzet, amely olyan tudati állapot, amikor a fenyegetettséget felismerve az ember képes szeme benézni vele, megelőzni, védekezni és helyreállítani.[1] Egy másik meghatározás szerint a biztonság valakinek a léte, vagy valaminek a működése és az azt veszélyeztető tényezők együtthatása [2 p.5.] Eszerint a biztonság kifejezés akkor nyer értelmet, ha megjelenik a valamilyen veszélyeztető tényező. A biztonság annál kisebb, minél nagyobb a létet, vagy a rendeltetésszerű működést veszélyeztető tényező.

A teljesség igénye nélkül, csak példálózó jelleggel beszélhetünk egy ország kapcsán politikai-, gazdasági- vagy szociális biztonságról, környezeti megközelítésben ökológiai biztonságról, vagy az egyén szempontjából létbiztonságról. Ebből következően állíthatjuk, hogy a biztonság egy komplex, számos területet átfogó fogalom. Megközelítés függvényében változó értelemben is használhatjuk: lehet a célunk olyan munkahely választása, ahol anyagi biztonságot teremthetünk, vagy használhatjuk arra, hogy leírjunk, minősítsünk egy ember, egy társadalom biztonsági helyzetét, állapotát. Vizsgálata önmagában nem elképzelhető.

Az elmúlt évszázadok során a biztonság értelmezése – az egyre szélesebb spektrumon ható pozitív és negatív tényezők hatásrendszere miatt – egyre komplexebben értelmezendő területté vált. A társadalmi élet változásai, a gyors technológiai fejlődés mind az állandóság és a tartósság iránti igénnyel ellentétesen hatnak, így negatívan befolyásolják az egyének, a közösségek, a nemzetállamok és akár az egész világ biztonságérzetét. A gyors technológiai fejlődés, az egyre bonyolultabb, szerteágazóbb, ugyanakkor egymással állandó kapcsolatban lévő, különböző technikai rendszerek jelenléte miatt komoly kockázati tényezőkkel kell számolni a gazdaság, a közlekedés és a védelmi funkciók területén.

A XX. század végétől még komplikáltabb, még komplexebb jelenségcsomagként értelmezhető a biztonság, a biztonságtudomány kérdésköre. Az emberiség a – társadalmi élet minden aspektusát érintő, robbanásszerű – technikai fejlődés olyan szintjére ért, amikor a világ népességének egészére egyszerre ható változások lehetőségével kell szembenézni. Olyan jelenségek, mint az automatizáció,

az infokommunikációs technikák fejlődése, a mobilizációs folyamatok még inkább generálják e változást. Ezzel párhuzamosan a világban jelentkező olyan környezeti tényezők és emberi tevékenységek következtében, mint a környezetrombolás, a természeti katasztrófák – köztük az ökológiai katasztrófa lehetősége – és a terrorizmus veszélye az egész emberiség elpusztulásának veszélyét is magában hordozza.

A biztonság koncepciójának jelentős változásához járultak hozzá a XX. század történelmi eseményei is. Az I. világháborút követően jelent meg először az igény egy globális, minden államot magában foglaló kollektív biztonsági struktúra létrehozására, ami a jövőbeli fenyegetésekre megfelelő válaszokat képes adni. A Népszövetség kudarca és a II. világháború tapasztalata a biztonság fogalmának újragondolásához és a nemzetközi együttműködés megerősítéséhez vezetett. Az államok felismerték, hogy a megerősített biztonsági együttműködés előnyei felülmúlják a teljes függetlenség elvesztésének költségeit. A hidegháború egy folyamatos fenyegetettségi állapotot hozott létre, ami további együttműködésre ösztönözte az államokat (NATO, EU létrejötte). A hidegháború megszűnését követően a katonai fenyegetettség megszűnt, azonban a helyét más, nem államokra visszavezethető fenyegetések vették át (gazdasági, humán biztonság). Az államközpontú biztonságfelfogást ezzel egy időben felváltotta az egyén biztonságának kérdése. A 2001. szeptemberi, New York-i támadást követő terror elleni háború a biztonságról való gondolkodás új korszakát hozta el, hiszen a nem-állami szereplők globális katonai fenyegetésként való megerősödése fordulópontot jelentett a nyugati államok biztonsági struktúráinak fejlesztésében. [3 pp. 36–44.]

A téma vizsgálata során a biztonságtudomány és a közszféra működését érintő kérdések vizsgálata is szükséges, így megközelítése csak multidiszciplinárias módszerekkel lehetséges. Az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának honlapján a biztonságtudomány hazai meghatározása az alábbiakat tartalmazza:

A biztonságtudomány – hazai tapasztalatok alapján – foglalkozik a kockázatelmélet, a kockázati határértékek, a kockázatelfogadás és az emberi kockázati tényezők kérdéseivel, kölcsönhatásaival. Napjaink kutatásainak leginkább meghatározó területe az integrált (komplex) biztonság, vagyis a biztonsági kockázat elemzése, valamint a megbízhatóságprognózis elveinek, módszereinek szakszerű alkalmazása, mivel azok alapján nyilvánvalóvá válik, hogy a biztonság javításának egyik lehetősége a kockázatok – mérési módszerekre és azok eredményeire épülő – elemzésének és értékelésének felhasználása azok kezelése érdekében. Ez tekinthető a biztonságtudomány legfontosabb pillérének.

A komplex biztonság megközelítése az ember–technika–környezet közös rendszerként történő értelmezéséből indul ki. A komplex biztonságra törekvő szakértők tehát mindazokat a kockázatokat fel kívánják deríteni, figyelembe kívánják venni és az egzakt tudományosság mai lehetőségeinek felhasználásával meghatározni (számszerűsíteni), amelyek a rendszer összetevőinek (ember, technika, környezet) bármelyikétől származnak.

1.1.2. Kritikus infrastruktúra

A biztonságtudomány hazai meghatározása szerint a biztonságtudomány vizsgálódási területe a kritikus infrastruktúrák biztonsága. A Fejezetek a kritikus infrastruktúra védelemből című Tanulmánykötet egyes szerzői különböző szempontok, aspektusok számbavételével kísérlik meg megfogni, meghatározni a maga komplexitásában a kritikus infrastruktúra fogalmát vagy annak kritikáját . [4] A kritikus infrastruktúra, mint fogalom meghatározása korántsem egyszerű. Azt azonban megállapíthatjuk, hogy alapvetően olyan létesítményeket, szolgáltatásokat, információs rendszereket és azok részegységeit (rendszerelemeit) értjük alatta, amelyek létfontosságúak az alapvető szolgáltatások folyamatos biztosításához, a társadalmi feladatok ellátásához, és amelyek megsemmisülése vagy működésének megzavarása, korlátozása, a területi és időbeli kiterjedtség, folytán jelentős hátrányt okozna az érintett terület működésében, lakosságának ellátásában.

Látható, hogy a kritikusság, mint tényező elsősorban az infrastruktúra potenciális kiesésének hatásában jelenik meg. Nem minden esetben a rendszer maga kritikus, hanem az, ha az adott rendszer meghibásodása a kapcsolódó rendszerek működését akadályozza, vagy lehetetleníti el, és a kiesés hatásának térbeli és időbeli kiterjedése folytán a lakosság ellátásában, a gazdaság vagy a kormányzat működésében zavarok lépnek fel.

A kritikus infrastruktúrák közé az alábbi tizenegy területet sorolják:

- Energia
- Információs és kommunikációs technológiák
- Víz
- Élelmiszer
- Egészségügy
- Pénzügy
- Közbiztonság
- Polgári adminisztráció
- Szállítás
- Vegyipar és nukleáris ipar
- Űrkutatás

A vonatkozó kormányrendelet definíciója szerint a „[k]ritikus infrastruktúra: Magyarországon található azon eszközök, rendszerek vagy ezek részei, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához, az egészségügyhöz, a biztonsághoz, az emberek gazdasági és szociális jólétéhez, valamint amelyek megzavarása vagy megsemmisítése, e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna.” [50]

„A fenti fogalmat az alábbi öt alapvető tulajdonság teszi teljessé:

- *interdependencia* – egymástól való függőség;
- *informatikai biztonság* – kiemelt terület, informatizált munkafolyamatok;
- *üzemeltetés* – sajátosságok, egyedi jelleg;
- *dominóelv* – láncreakciószerű sérülés/károsodás;

- *leggyengébb láncszem és rész–egész-elv* – összekapcsolódó hálózatok stabilitása a leggyengébb elem erősségétől függ." [5]

A XXI. század új típusú kihívásainak rendszerében megjelenő fenyegetettségek és a 2001. szeptember 11-i terrortámadások következményeképpen Európában is erőteljesebben fókuszba került a kritikus infrastruktúrák védelmének kérdésköre. A mindennapi élet zavartalanságát biztosító infrastruktúrák, vagy azok bizonyos elemei kiemelt figyelmet kívánnak meg. Védelmük – akár európai uniós, akár állami szinten – olyan feladat, ami egységes stratégiai megközelítéssel, szigorú elvárások és következetes végrehajtás útján, hosszú távú stratégiai célok meghatározásával valósítható meg.

A kritikusinfrastruktúra-védelem az Amerikai Egyesült Államokból indult, ott az 1990-es években már kutatási és tudományos szinten említik, bár ekkor még megoszlottak a vélemények az egyes területek jelentőségét illetően, és leginkább csak a téma informatikai aspektusa került előtérbe. Az európai koncepció kiindulópontját és egy átfogó program kidolgozására irányuló igényt a második évezred elején megszaporodott és súlyos következményekkel járó terrortámadások jelentették. Az Európai Bizottság 2004. október 20-án elfogadta *A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben* című közleményt [51], amelyben javaslatokat tett arra, hogy miként lehetne az európai megelőzést, felkészültséget és reagálást javítani a létfontosságú infrastruktúrákat érintő terrortámadások esetén.

2005 novemberében a Bizottság egy úgynevezett *Zöld Könyvet* fogadott el a létfontosságú infrastruktúrák védelmére vonatkozó európai programról. „Az Európai Unió szintjén kiadott Zöld Könyv elsődleges célkitűzése az volt, hogy biztosítsa a nemzeti kritikus infrastruktúrák védelméről (NKIV) szóló nemzeti program megvalósítását és egy olyan jogszabály megalkotását, amely összegzi a kormányzati szereplők NKIV-vel kapcsolatos célokat, szempontokat, alapelveket, fogalmakat és a megvalósítás alapvető formáira vonatkozó álláspontját.

„A kritikus infrastruktúrák hatékony védelme tehát megköveteli valamennyi érintett fél – az infrastruktúrák tulajdonosai és üzemeltetői, a hatóságok, szakmai szervek és érdekszövetségek – közötti kommunikációt és együttműködést. Egy széles körű, érdekazonosságon alapuló összefogás nélkül a megváltozott biztonsági környezet által jelentett új típusú veszélyek (aszimmetrikus fenyegetettség, nem hagyományos kockázati tényezők megjelenése) hatékony módon nem kezelhetőek." [6 p. 350.]

„A legfőbb cél az, hogy az érintettek között aktív kommunikáció és eredményes együttműködés alakuljon ki. Szorosan ide kapcsolódik az a kezdeti célkitűzés, hogy az érintett lakosság megfelelő képet kapjon az adott infrastruktúra működésének jelentőségéről, az alternatív lehetőségek biztosításáról, vagy a szünetelő szolgáltatás ideje alatt követendő magatartási formákról egyaránt. Az ellenálló képesség kialakításához további három összetevő szükséges. Elsődleges ezek közül az alternatívák biztosítása, a kieső szolgáltatás mielőbbi pótlásának érdekében. Ehhez kapcsolódik a bekövetkezett esemény utáni, minél rövidebb idő alatt történő visszaállítás képessége, végül pedig a sebezhető pontok számának csökkentése. Utóbbi eredményeként az infrastruktúra ellenálló képessége nő, tekintettel arra, hogy kritikusság szintjét kevesebb kockázati faktor határozza meg." [7 p. 42.]

Az NKIV három fő célkitűzést fogalmazott meg. Az első a megelőzés és a védelem érdekében a kritikus infrastruktúrák legnagyobb kockázatot képviselő elemeinek beazonosítása, a kockázatok csökkentését célzó elemzések és a szükséges védelmi intézkedések alkalmazása. A második az érintett szereplők (tulajdonosok, üzemeltetők, állam) megfelelő felkészültésének biztosítása az esetleges meghibásodás vagy működésmegszakadás esetére. A harmadik pedig – jelentős kihatású meghibásodás, kiesés vagy teljes leállás esetén – az üzemfolytonosság és ellenállóképesség fejlesztése, intézkedések tervezése, kialakítása, végrehajtása vagy helyettesítő megoldások alkalmazása annak érdekében, hogy a működés a lehető legrövidebb időn belül visszaállítására kerüljön. [6 p. 351.]

Az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK tanácsi irányelvet (továbbiakban: irányelv) Magyarországnak tagállami kötelezettsége átültetni a hazai jogrendszerbe. Ezen jogharmonizációs kötelezettség mentén tagállami szinten kell meghozni azokat az intézkedéseket, amelyek beültetik az irányelvet a magyar jogrendszerbe.

A hazai viszonylatban fontos mérföldkő, hogy az Országgyűlés 2012. november 12-én törvényt fogadott el a nemzeti és az európai kritikus infrastruktúrák védelméről [52]. A jogszabály egyébként az idegenül hangzó kifejezés helyett a *létfontosságú rendszerek és létesítmények* elnevezést használja. A törvény rendelkezik az európai és magyar kritikus rendszerek kijelöléséről, a kijelölés visszavonásáról, a nyilvántartás rendjéről, az üzemeltetői biztonsági tervek bevezetésének szükségességéről, valamint az ellenőrzés rendjéről.

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. számú törvény mellékleteiben ágazatba és alágazatokba sorolja a kritikus infrastruktúrákat.

A törvény 2016-os módosításának 3. mellékletében [53] az alábbiak szerint, mint kritikus infrastruktúrát nevesíti az infokommunikációs technológiát és a körébe tartozó alágazatokat:

- internet-infrastruktúra és internet hozzáférés szolgáltatás,
- vezetékes és vezeték nélküli elektronikus hírközlési szolgáltatások, vezetékes és vezeték nélküli hírközlő hálózatok,
- rádiós távközlés,
- űrtávközlés,
- műsorszórás,
- postai szolgáltatások,
- kormányzati informatikai, elektronikus hálózatok.

Fontos kiemelni, hogy szinte minden ágazati körben működő kritikus infrastruktúra informatikai eszközök, hálózatban lévő rendszerek segítségével üzemel, így e rendszerek a kibertámadások potenciális célpontjaivá válhatnak.

A fentieket figyelembe véve, tehát a kritikus információs infrastruktúra alatt azokat az infokommunikációs rendszereket értjük, amelyek önmagukban is a kritikus infrastruktúra elemei, vagy

lényegesek azok működése szempontjából (távközlés, számítógépek és szoftver, internet, műholdak stb.). A kritikus infrastruktúrákra vonatkozó öt alapvető tulajdonság szerint e rendszerekre az alábbiak jellemzőek:

- a kritikus infrastruktúrák nem elkülönült szigetekként biztosítanak hálózati és adatbázis-hozzáférési szolgáltatásokat, hanem összekapcsolva alakítanak ki globális kritikus hálózatokat;
- magukon hordozzák az egyes rendszerelemek sérülékenységének problémáját;
- a kritikus információs infrastruktúrák védelme széleskörű együttműködést igényel (szervezetek, ágazatok, kormányzatok);
- nem határolható be fizikailag elkülönült közegre, népre, országra vagy konkrét ágazatokra.

A kritikus információs infrastruktúrák és a kritikus infrastruktúrák védelme és biztonsága nem különíthető el egymástól. Az infrastruktúrák együttes és globális védelmét a rendszereket üzemeltetőknek közösen kell biztosítani, koordinálni.

1.1.3. Információbiztonság

Kijelenthetjük, hogy visszavonhatatlanul a digitalizáció korába léptünk. Az emberek rendelkeznek elektronikus levélcímekkel, bankszámlákkal és a hozzá tartozó elektronikus szolgáltatásokkal, van mobiltelefonjuk, használnak helymeghatározó szolgáltatásokat, és a vásárlásaik egy részét is a világháló nyújtotta lehetőségek kiaknázásával bonyolítják. Vitathatatlan, hogy ezek az eszközök és szolgáltatások jelentős mértékben megkönnyítik életüket, időt és költséget takaríthatnak meg velük, azonban ezzel párhuzamosan jelentős függést is generálnak.

Életünk részévé váltak a különböző IKT eszközök, internetes alkalmazások, az internet. Ezeket használva mindenféle információkat osztunk meg magunkról, viszont mindeközben nem feltétlenül vagyunk felkészülve arra, hogy megvédjük magunkat az internet világában lehetséges rosszindulatú támadásoktól.

Az információbiztonság kérésköre végigkíséri az emberiség történelmét. A XX. század közepéig a területszerzést és megtartást, illetve a nyersanyaghoz való hozzáférést, annak birtoklását segítő értesülések megszerzésén és védelmén volt a hangsúly. A XIX. század végétől az élet minden területén dinamikus változások kezdődtek. Az átalakulás többek között érintette a közlekedés, híradás, energetika területét, amik rendkívüli változást hoztak az emberiség életében. Azonban e változások során sérült az egyének, a közösségek, nemzetek, országok, vagyis az egész világ biztonságérzete, ami magával hozott egy az élet minden területén tapasztalható gyors fejlődést, átalakulást. A kezdetleges számítógépek megjelenésekor, később a fejlett, adatkezelő rendszerek kifejlesztésével az információ megszerzésének és védelmének jelentősége, módja is megváltozott.

Ma már nem kérdés, hogy fejlett nyugati társadalmunkat átszövik az információs technológiákra épülő infrastruktúrák. Ha e rendszerek nem működnek, akkor a gazdasági élettől kezdve a közigazgatáson át, a megszokott mindennapi életvitel is az összeomlás határára kerülne. Ez hatalmas kihívás elé állítja a jelen kort.

„Az információbiztonságot és az informatikai biztonságot – néha még a szakemberek is – gyakran összekeverik egymással, sőt időnként az adatvédelemmel, a személyes adatok védelmével is. Az adatvédelem kifejezés – érdekes módon az angol nyelvben (data protection) is kizárólag a személyes adatok védelmére van fenntartva, a személyiségi jogokkal összefüggő tevékenység. Az információbiztonság és az informatikai biztonság különbözik egymástól. Az információbiztonság értelmezésünkben a szóban, rajzban, írásban, a kommunikációs, informatikai és más elektronikus rendszerekben, vagy bármilyen más módon kezelt adatok védelmére vonatkozik. Ez alapján az informatikai biztonság »csak« az informatikai rendszerekben kezelt adatok és az azt kezelő rendszer védelmét jelenti. Mivel angolul általában az információvédelemre, illetve az informatikai védelemre, sőt néha a kommunikációs, információs és más elektronikus rendszerek védelmére is az »information security« kifejezést használják, az egyes fordítások még inkább zavarossá teszik a képet. Általában a szövegkörnyezet teszi egyértelművé, hogy információvédelemről vagy informatikai védelemről van-e ott szó.” [8 p.18.]

Jelen dolgozat az egyértelműség kedvéért a két fogalmat az alábbiak szerint használja:

„Az informatikai biztonság az informatikai rendszer olyan kedvező állapota, amelyben a kezelt adatok bizalmassága (confidentiality), sértetlensége (integrity) és rendelkezésre állása (availability) biztosított (CIA-elv), valamint a rendszer elemeinek biztonsága szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. Ahol

- bizalmasság: csak az arra jogosultak ismerhetik meg az információt;
- sértetlenség: az információ tartalma és formája az elvárttal megegyezik, beleértve az is, hogy az elvárt forrásból származik (hitelesség), igazolható, hogy megtörtént (letagadhatatlanság), egyértelműen azonosítható az információval kapcsolatos műveletek végzője (elszámoltathatóság), továbbá rendeltetésének megfelelően használható;
- rendelkezésre állás: az a tényleges állapot, amikor egy informatikai rendszer szolgáltatásai az arra jogosultak számára egy meghatározott időben rendelkezésre állnak és a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva;
- zártság: az összes releváns veszélyt (fenyegetést) figyelembe veszi;
- teljes körűség: a rendszer minden elemére kiterjed a védelem;
- folytonosság: időben folyamatosan megvalósul a védelem;
- kockázatokkal arányosság: a rendszer várható működésének időtartamában a védelem költsége arányban van a lehetséges kárral.

Az információbiztonság tágabb fogalom, mint az IT biztonság. Beleértjük az információ minden – nem csak elektronikus – megjelenési formájának, az információs szolgáltatásoknak és az ezeket biztosító információs rendszereknek a védelmét.” [9 p. 12.]

Az információbiztonság megfelelő szintje egy olyan ideális állapotban lehetne elérhető, amiben minden szereplő tisztában van azokkal a szabályokkal, eljárásrendekkel, amelyek a biztonságot befolyásolják. A társadalom által elvárt biztonsági szint egyre nő, és az ehhez szükséges tudás,

kompetencia szükséglet és a műszaki megoldások, rendszerek is egyre bonyolultabbá válnak. A kibertérből érkező különböző fenyegetések, adatvesztés, zsaroló vírusokkal és egyéb módszerekkel való támadások általában a humán-erőforrás figyelmetlenségéből, a szabályok be nem tartásából és a szükséges tudás, képességek és a biztonságtudatosság hiányából következnek be. A különböző rendszerek kockázatelemzései alapján megalapozottnak tűnik az az állítás, hogy a humán faktor (emberi tényező) a leggyengébb láncszem a legtöbb biztonsági rendszer hatékony működése szempontjából. [10 pp. 37–38.]

1.2. Kiberbiztonság

A kiberbiztonság kiemelt figyelmet kapott az elmúlt időszakban a különböző kibertámadások miatt. Az alafejezet a kiberbiztonság fogalmi kereteivel és a jelenlegi helyzetével, továbbá a kiberfenyegetettség növekedése következtében szükséges közös fellépés szükségességével és a kiberfenyegetés trendjeivel, típusaival foglalkozik.

1.2.1. A kiberbiztonság fogalmi keretei

A kiberbiztonságnak számos különböző aspektusa van. Fontos a biztonságmenedzsment rugalmas értelmezése, mivel ahhoz, hogy a munka során az összes aspektusra figyelemmel legyünk, tekintetbe kell venni az állami szintű megközelítéstől kezdve az egyéneket mint önálló biztonsági aktorokat is. A nodális, vagy többszintű kormányzásban különböző kormányzási formák, gyakorlatok keverednek, ahol a résztvevők köre az állami szereplőktől, a magánszféra vállalatain át az egyénekig terjed. A részvétel alapja a biztonsági kockázatokról szerzett speciális tudás, amivel a biztonsági kormányzásban résztvevők rendelkeznek. Ez a fajta kormányzás a hierarchikus kormányzási struktúrával szemben heterogén, és az egyes szereplői magas fokú önállósággal rendelkeznek. A többszintű kormányzás nemzetközi és cross-szektorális, aminek eredményeként egy olyan hibrid struktúra jön létre, ahol a hatóságok szorosan együttműködnek a magánszféra-menedzsment struktúráival és kormányzási formáival, a magánszféra szereplői pedig nagyobb felelősséget vállalnak a biztonság növelése érdekében. A legnagyobb kihívást az jelenti a többszintű kormányzásban, hogy nincsenek egyértelmű fékek és ellensúlyok a rendszerben, a felelősség és elszámoltathatóság problémás. [3 pp. 52–57.]

A kiberbiztonsági politikák mind az ellenálló képesség, a megelőzés és a felkészültség koncepcióira épülnek. A kiberbiztonság régóta fennálló problémáinak leküzdésében kulcsfontosságú a különböző kockázatok előrelátásának képessége, mielőtt azok valós fenyegetéssé nőnek. A 2007-es észt kibertámadás hidegzuhanyként érte az európai államokat, hiszen a történelemben először bebizonyosodott, hogy a hackerek képesek megbénítani egy ország teljes infrastruktúráját. A támadás jelentős nyomás alá helyezte a politikai döntéshozókat: szükségessé vált egy olyan biztonsági gyakorlatokat kialakítása, ami alkalmas a jövőbeli kockázatok kivédésére és a technológiai sebezhetőség csökkentésére. Ezt követően a kiberkormányzás egyre inkább a megelőzésre, a kockázatok előrelátására fókuszált. Az egyik legnagyobb kihívás, hogy a technológiai fejlődés folyamatosan új, jövőbeli kockázatokat generál, ezáltal a biztonsági folyamatok állandó újragondolása és felülvizsgálata szükséges. A biztonsági stratégiákban a megelőző intézkedések kiterjesztésének motorja a bizonytalanság. Tényleges fenyegetések helyett egyre inkább lehetséges kimenetelekben

gondolkodnak a döntéshozók, és mindig a legrosszabbra készülnek. A cél, hogy már azelőtt kezeljük a kockázatokat, mielőtt azok fenyegetéssé alakulnának. Az innováció gyorsasága azonban sok esetben lehetetlenné teszi a veszélyek kiszámítását, ezért szükséges már korai stádiumban felkészülni minden lehetséges eshetőségre. Ezért elengedhetetlen a megelőző és elővigyázatossági intézkedések beépítése a biztonsági menedzsmentbe, a jelenlegi biztonsági struktúrába. Amennyiben a kockázat valós fenyegetéssé alakul át, megelőző kockázatkezelés helyett az elrettentés mechanizmusa lép életbe. [3 pp. 71–95.]

A kiberbiztonság biztosításának módja komoly kérdéseket vet fel. Munk szerint ennek mélyebb megértését jól segíti két elméleti biztonsági iskola megközelítésének összehasonlítása. [3]

A koppenhágai és a párizsi iskola a biztonság fogalmát, a biztonsági folyamatokat, gyakorlatokat két különböző perspektívából vizsgálja. A koppenhágai iskola elméletében a kivételezettség (exceptionalism) a domináns koncepció, míg a párizsi iskola a szokásos folyamatokra (regular processes) fókuszál. A koppenhágai iskola középpontjában a biztonságiasítás (securitization) fogalma áll, aminek lényege, hogy amennyiben a kockázat tényleges fenyegetéssé válik, a döntéshozók számára lehetőség nyílik az adott politikai területen kivételes intézkedéseket hozni, amelyek más helyzetben nem lettek volna legitimálhatók az állampolgárok felé. A biztonságiasítás tipikus példája a 9/11 után meghozott biztonsági intézkedések, amelyek ugyan növelték a biztonságot, de közben megkérdőjelezték a demokratikus értékeket és jelentősen korlátozták az alapvető szabadság- és emberi jogokat. A biztonságiasítás elméletének alkalmazása a kiberbiztonság területén több szempontból is problémás. Elsőként, a koppenhágai iskola szerint a biztonságiasítás alanyai az államok, hiszen csak ők rendelkeznek legitim politikai hatalommal ahhoz, hogy egy adott politikai kérdésből biztonsági kérdést csináljanak. A kiberbiztonság többszintű, szektorokon és államhatárokon átívelő rendszerében így nem érvényesül a biztonságiasítás folyamata. A párizsi iskola ezzel szemben abból indul ki, hogy a kormányzatok és bürokráciák a bizonytalanságot kihasználva bizonyos biztonsági kérdéseket rutin módon kezelnek, szokásos folyamatokban gondolkodnak, ezáltal a különleges válik a normálissá, ami gyakran a demokratikus értékek erodálásához vezet. A párizsi iskola meggyőződése, hogy a kormányzat a félelemfaktort kihasználva képes újabb és újabb biztonsági intézkedést meghozni. Továbbá, nemcsak a kormányzat, hanem a biztonsági eszközökkel foglalkozó vállalatok, valamint a média is profitál a fokozott biztonsági helyzetből. Összefoglalva, a transznacionális és cross-szektorális fenyegetések ellen szükség van a biztonsági aktorok közötti hálózatok és együttműködések létrehozására, viszont a párizsi iskola kiemeli, hogy e hálózatok által alkalmazott gyakorlatok és technológiák lehetőséget adnak visszaélésekre. [3 pp. 96–134.] Az Európai Unió és a hazai szabályozás megközelítésének bemutatására a stratégiai és szabályozási fejezetekben kerül sor.

A továbblépéshez érdemes egyértelműsíteni, hogy mit ért a jelen dolgozat a kibertér és a kiberbiztonság fogalma alatt. Ahhoz, hogy egy tudományos diskurzus értelmezhető eredményre jusson, fontos annak biztosítása, hogy az érintett felek egyes fogalmak alatt ugyanazt a jelentéstartalmat értsék. Sajnos sok esetben ez nincs így: a kiberbiztonság témaköre sem mentes ettől a problémától sem nemzetközi, sem nemzeti, hazai szinten. Abban egyre többen értenek egyet,

hogy a kiberbiztonság a kibertér és a biztonság közötti kapcsolatot határozza meg. A kiberbiztonság kifejezés tartalmának azonosítását nem könnyíti meg, hogy a tömegtájékoztatásban is egyre gyakrabban alkalmazzák eltérő tartalmi jelentéssel.

Az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (továbbiakban: ENISA) szerint öt fő terület fedi le a kiberbiztonság fogalmát: a kommunikáció biztonsága (a rendszer technikai infrastruktúrájának védelme); a működés biztonsága (a munkafolyamatok szándékos megzavarása, megváltoztatása elleni védelem); az információ biztonsága (a rendszerben tárolt vagy továbbított adat megváltoztatásával szembeni védelem); a fizikai biztonság (a rendszer védelme a fizikai veszélyektől); közbiztonsági/nemzetbiztonsági védelem (kibertérből származó olyan fenyegetések elleni védekezés, amelyek egyaránt veszélyeztethetik a fizikai rendszereket és a kiberteret – például: Stuxnet, vagy kiterjedt szolgáltatásmegtagadással járó támadás egy kritikus információs infrastruktúra ellen). [11 pp. 2–3.]

A 2013-ban kiadott Nemzeti Kiberbiztonsági Stratégia [54] az alábbi hazai meghatározást adja a kibertérre és a kiberbiztonságra:

„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.” [54 3. pont]

„A kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.” [54 5. pont]

1.2.2. Kiberfenyegetettség

Az internet világa komplex, decentralizált, és átszövi a köz- és magánszféra minden egyes aspektusát. Ahogy növekszik a társadalom függősége a kibertértől, úgy válik egyre sebezhetőbbé. A kiterjedt kiberfenyegetések leküzdése érdekében olyan biztonsági keretrendszerre van szükség, amely rugalmas, és a biztonsági együttműködés széles spektrumát valósítja meg. Az eddigi biztonsági stratégiák, kormányzási módok és gyakorlatok teljes újragondolására van szükség az ellenálló képesség fejlesztése és a hatékony felkészültség érdekében.

A kiberbiztonság egy olyan növekvő fenyegetés a posztmodern világban, ami kihat a teljes biztonsági paradigmára. A XXI. századig a fenyegetéseket az államok elsősorban katonai vonatkozásban értelmezték. Ez mára megváltozott, mivel a fenyegetések köre jelentősen kibővült. Ezzel egy időben a fenyegetések meghaladták az országhatárokat, és már nem értelmezhetők a hagyományos nemzetállami keretek között. Az egyes államok már nem képesek önállóan fellépni az újfajta fenyegetésekkel szemben, így a biztonsági intézkedéseknek és kormányzási módszereknek is változniuk kell. A biztonság ma már csak tágan értelmezhető, egy többszintű fenyegetésstruktúrában. Ez azonban felveti azt a problémát, hogy a túl sok biztonsági előírás alááshatja az egyéni szabadságot. E konfliktus abban rejlik, hogy a biztonság koncepciója nem egységesen értelmezett:

különböző biztonsági szereplők eltérő jelentőséget tulajdonítanak egyes fenyegetéseknek, így nem megfelelő az információcsere, illetve az erőforrás-allokáció.

A nemzetközi együttműködés egyik legnagyobb gátja, hogy nem létezik globális konszenzus a kiberbiztonságról való gondolkodásban. Számos államhoz köthetők olyan kibertevékenységek, amelyek gyengítik a hajlandóságot az együttműködésre, hiszen stratégiai előnyük származik a védett információk megszerzéséből (például Kína és Oroszország). Az együttműködéstől való elzárkózás azonban ezeket az államokat is sebezhetővé teszi, hiszen az ellentámadás vagy megtorlás kockázata rendkívül magas. A köz- és magánszféra közötti partnerségi viszonyok is nehezítő tényezőnek bizonyulnak, hiszen a legtöbb esetben a vállalatok elutasítják az együttműködési kezdeményezéseket a kormányzati ellenőrzéstől való félelem okán. Az állami szereplők oldaláról a legnagyobb problémát a privát partnerek felé történő információvisszatartás okozza, ami egyrészt bizalmatlansághoz vezet, másrészt nem motiválja a biztonsági szereplőket az együttműködésben való részvételre.

Az Európai Unió helyzetéről szóló értékelő beszédében Jean-Claude Juncker 2017-ben a kiberbiztonságot kiemelt területként nevezte meg [12]. Az Európai Bizottság és a Külügyi és Biztonságpolitikai Főképviselő konkrét intézkedések széles körét javasolta az EU kiberbiztonsági struktúráinak és képességeinek erősítése érdekében. A felmérések alapján az európai állampolgárok és vállalatok nagymértékben függnek a digitális szolgáltatásoktól és technológiáktól, míg a kiberbűnözésnek való kitettség folyamatosan növekszik. Példának hozható néhány adat:

- 4000-nél is több zsarolóvírus-támadás 2016-ban;
- Néhány tagállamban a bűncselekmények 50%-a kiberbűncselekmény volt;
- A biztonsági incidensek minden iparágban 38%-kal növekedtek 2015 óta;
- Az európai vállalatok 80%-a átélt kiberbiztonsági incidenst az utóbbi évben.

Az emberek többsége a más országokból indított kibertámadást azonosítják a nemzetbiztonság legnagyobb veszélyeként.

Mindezek ellenére a kiberbiztonsági tudatosság csekély szintű. A vállalatok 69%-a nem rendelkezik megfelelő rálátással a kiberkockázatoknak való kitettségére. A vállalatok 60%-a nem becsülte fel a lehetséges pénzügyi veszteséget egy kibertámadást követően. Az európai polgárok 51%-a egyáltalán nem érzi magát jól informáltnak a kiberkockázatokkal szemben.

A különböző felmérések évek óta hangsúlyozzák, hogy a „leggyengébb láncszem” a kiberbiztonsági kérdések kapcsán az emberi tényező. Az Institute of Information Security Professionals (IISP) IT biztonsági felmérése alapján a vezető kockázati tényező 2017-ben is a humán erőforrás (81%), míg a technológiai és a folyamatokból adódó kockázatok jóval kevésbé mérvadóak. [13]

Az Európai Bizottság három nagy cselekvési területet azonosított be a kiberbiztonság erősítése érdekében:

- reziliencia (rugalmas ellenállási képesség) erősítése és a kiberbiztonsági kapacitások növelése,

- hatékony bűnügyi válaszadás,
- fokozott nemzetközi együttműködés.

A Bizottság továbbá az alábbi intézkedések meghozatalát javasolta:

- megerősített Európai Kiberbiztonsági Ügynökség létrehozása (az ENISA utódjaként);
- európai kiberbiztonsági tanúsítványok alkalmazása, amelyek biztosítják a digitális termékek és szolgáltatások biztonságát;
- cselekvési terv létrehozása nagy léptékű kibertámadás esetére egy gyors, összehangolt válasz érdekében;
- tagállami kompetencia-központok hálózatának létrehozása, és az Európai Kiberbiztonsági Kutató és Kompetencia Központ felállítása;
- rgy új, a csalás és a nem pénzbeli fizetőeszközök hamisítása elleni irányelv létrehozása;
- nemzetközi együttműködés erősítése;
- kibervédelmi oktatási platform létrehozása. [14]

1.2.3. Kiberfenyegetettség trendjei, típusai

A kiberfenyegetés különböző típusainak részletes bemutatása nem célja jelen értekezésnek, azonban a fenyegetettség mértékének és kiterjedtségének érzékeltetése érdekében az EU ügynökségének jelentése alapján áttekintést adok a trendekről, típusokról.

Az Európai Hálózat- és Információbiztonsági Ügynökség által 2017-ben kiadott jelentés [15] számba veszi a kiberfenyegetések legjelentősebb trendjeit, és rangsort állít fel a legveszélyesebbnek tekintett fenyegetésekről. A tapasztalatok azt mutatják, hogy a növekvő kiberbiztonsági tudatosság és a megnövekedett védelmi kiadások ellenére a kiberfenyegetettség nem csökkent. 2017-ben jelentősen megnövekedett a kibertámadásokról szóló hírek és beszámolók száma, ami érzékelteti a jelenlegi trendet, vagyis a média kiemelt figyelmet fordít a kiberbiztonság kérdésére. 2017 legfontosabb kiberbiztonság trendjei a következők:

- a támadások és az elkövetők módszereinek komplexitása egyre növekszik;
- az elkövetők egyre könnyebben tudják elfedni a nyomaikat, így a felfedésük egyre nehézkesebbé válik;
- a kártékony infrastruktúrák átalakulása többcélú, konfigurálható funkciókká, amelyek anonimizálhatók, titkosítottak és nehezebben észlelhetők;
- a kiberbűnözés monetizálása figyelhető meg;
- a kibertérre a legnagyobb fenyegetést az államok által támogatott szereplők (kémek) jelentik;
- a kiberháború mint fogalom egyre dinamikusabban jelenik meg a köztudatban, és fokozott fenyegetettséget jelent a kritikus infrastruktúra operátorai felé.
- a szervezetek számára kiemelt fontosságú, hogy megfelelő készségekkel és képességekkel rendelkezzenek alkalmazottaik, azonban a képzésre és oktatásra még mindig kevés hangsúlyt fektetnek.

Az ENISA jelentése a politika szereplői számára kettős célkitűzést ír elő: egyrészt a jogos beavatkozáshoz szükséges jogalkotási lépések meghozatalát, másrészt a kiberfenyegetésekkel

kapcsolatos információk és a védelemhez szükséges készségek kibővítését oktatási és kutatási programokon keresztül. A vállalatok számára a jelentés a következő javaslatokat teszi: elsőként szükség van a kiberfenyegetésekkel kapcsolatos információszerzés hatékonyságának újraértékelésére, hatékonyabb módszerek, eszközök kidolgozására. Továbbá szükséges az információszerzés automatizálásának fejlesztése annak érdekében, hogy az a későbbiekben magában foglalja a stratégiai és a taktikai információszerzést is. Végezetül a jelentés kiemeli a kutatás fontosságát olyan főként új módszerek, mechanizmusok kidolgozásában, amelyek a jogszerű beavatkozást szolgálják.

A jelentés ezt követően számba veszi a 2017-ben legnagyobb kiberfenyegetést jelentő módszereket, amelyek az alábbiak:

- Rosszindulatú programok (Malware):

A leggyakrabban előforduló fenyegetés, ami folyamatos fejlődésen megy keresztül, így 2017-ben már egyre gyakoribbá váltak a kattintás nélküli fertőzések, valamint a fájl nélküli támadások, amelyek tovább nehezítik a rosszindulatú programok észlelését. A leggyakoribb vírusgazda (vector) az úgynevezett phishing, amely elsősorban a szervezetnél dolgozó emberek biztonsági tudatlanságára épít, például e-mailen keresztül küldött linkeken aktiválódik.

- Webbázisú támadások:

Leggyakoribb formája a böngésző vagy bizonyos weboldalak megfertőzése, azonban ezeknek a fenyegetéseknek az enyhítése viszonylag egyszerű a böngésző frissítésével és biztonságos beállítások használatával.

- Webes applikációs támadások:

A támadások főként kormányzati intézmények weboldalaira, valamint IT cégekre irányulnak.

- Phishing:

A phishing támadások továbbra is az egyik leggyakoribb fenyegetést jelentik, azonban egyre bonyolultabbá és célzottabbá váltak, ami megnehezíti az ellenük való védekezést. Míg korábban jellemzőek voltak a spam kampányok, mára egyre inkább az úgynevezett spear-phishing, azaz egy-egy személy vagy embercsoport célzott támadása történik. A cél lehet például a szervezet vagyonának ellopása vagy kiberkémkedés. Jellemző, hogy a phishing általában valamilyen rosszindulatú programot juttat a felhasználó gépébe egy linken keresztül (például trójai vírust vagy zsarolóvírust), jelentős mértékben épít az emberek figyelmetlenségére és tájékozatlanságára. A legjobb védekezési mechanizmus a munkatársak tájékoztatása, oktatása a gyanús e-mailek és csatolmányok kiszűrésére.

- Spam:

A spam már régóta a legelterjedtebb és legkitartóbb formája a kiberfenyegetésnek. Az e-mailek kb. felét teszi ki, és habár ez a szám az utóbbi időben csökkent, a spamet tartalmazó e-mailek minősége (jobb álcázási képességek) miatt veszélyesebbé váltak. Az egyik legújabb trend, hogy a támadók

valós cégeknek és személyeknek álcázzák magukat, így „kényszerítve” az áldozatot például egy gyanús csatolmány megnyitására. Továbbá, az e-mailekről egyre inkább áthelyeződik a hangsúly a közösségi hálózatokra, így a támadók kikerülhetik az e-mail-fiók szolgáltatók szűrőit és szélesebb kört érhetnek el.

- Szolgáltatásmegtagadással járó támadás (Denial of Service Attack):

Ezeknek a támadásoknak célja egy rendszer teljes megbénítása, amit általában túlterheléssel érnek el.

- Zsarolóvírus:

A zsarolóvírust alkalmazó támadások rendkívül jövedelmezők, ezért népszerűségük töretlen. Új trend, hogy egyre gyakoribbá válnak a célzott támadások egyes vállalatok ellen. Új fenyegetésként jelent meg a zsarolóvírusok elterjedése az egészségügyi rendszerekben és egészségügyi eszközökben. E támadások enyhítésének legjobb módja a biztonsági mentés, a rések befoltozása (amennyiben nyilvánvalóvá válik, hogy a rendszer sebezhető), valamint a felhasználók oktatása a gyanús elemek kiszűrésére.

- Botnet:

Egy új trend van kibontakozóban, miszerint a támadók most már képesek virtuális gépeket botnetekké alakítani, például a felhőalapú szolgáltatókat gazdatestként megtámadni és parazitához, élősködőhöz hasonlóan használva őket egyéb károkat okozni.

- Belső fenyegetés:

Mindegy, hogy szándékosan vagy gondatlanságból elkövetett hibáról beszélünk, a belső dolgozók jó potenciális támadási vektorként azonosíthatók. Legfőképpen a kiterjedt hozzáféréssel rendelkezők, például menedzserek jelentenek fokozott veszélyt, hiszen ők számos érzékeny információ birtokában vannak. A legnagyobb kihívást a belső fenyegetésekkel szemben a nehezen felismerhetőség jelenti.

- Fizikai manipuláció/károkozás/lopás:

Habár mindig technikai kiberfenyegetésről beszélünk, a fizikai támadások is jelentős károkat képesek okozni a digitális infrastruktúrában. Növekvő trend például a lopott telefonok tulajdonosainak átverése, és személyes adatok kicsalása a telefon megtalálása érdekében. Ugyanakkor a lopott telefonok piaca csökkenőben van, mivel az okostelefonok biztonsági intézkedései már nem teszik túl nyereségessé az eltulajdonított telefonok felhasználását.

- Adatokhoz való hozzáférés (Data Breach):

Önmagában nem értelmezhető fenyegetésként, inkább egy gyűjtőfogalom a sikeresen végrehajtott kiberfenyegetésre. Leggyakrabban a gyenge, ellopott vagy feltört jelszavak okozzák a sikeres támadásokat.

- Személyazonosság-lopás:

A személyes információ továbbra is értékes árucikk marad az online piactéren. Ennek ellenére kevés az információ az EU-n belüli személyazonosság-lopás mértékéről, és talán emiatt a legtöbb ember még mindig alulértékeli a személyazonosságára leselkedő fenyegetéseket.

- Információ kiszivárogtatás:

A legtöbb esetben belsős tevékenység vagy hiba idézi elő. A legfontosabb megelőzési tényező az érzékeny adatok/információk védelme, valamint a munkatársak tudatosságának növelése, hiszen az esetek legnagyobb részében emberi hiba okozza az információk kijutását.

- Kihasználás/kiaknázás (Exploit-kit):

Az exploit-kit egy olyan program, amely a már fertőzött weboldalba ágyazva alkalmas a felhasználó böngészőjében a biztonsági rés megtalálására, illetve hibájának kihasználására.

- Kiberkémkedés:

A legtöbb globális vállalat a kiberkémkedést tartja a legkomolyabb fenyegetésnek, amit alátámaszt az is, hogy a média is kiemelt figyelmet fordít ezekre a tevékenységekre. A következő periódusra vonatkozóan a szakértők a kiberkémkedés növekedését jósolják, amelyek geopolitikai okokra, gazdasági szankciókra, valamint nemzetállami stratégiai célokra vezethetők vissza.

A jelentés végül kitér a kiberfenyegetések leggyakoribb szereplőire és a leggyakoribb motivációkra. A szereplőket tekintve megállapítható, hogy egyre komplexebbé és hatékonyabbá váltak az utóbbi időben, aminek következtében egyre nehezebben megállapítható, hogy ki melyik oldalt szolgálja. A felhasználói közösség számára ez fokozott bizalomvesztést okoz mind a kereskedelmi, mind az intézményes szereplőkkel szemben. A kiberfenyegetések szereplői továbbá egyre jobb képességekkel rendelkeznek a tevékenységük elrejtését illetően, így egy-egy kibertámadást nehéz visszavezetni a tetteshez. A kiberbűnözők az incidensek kb. kétharmadáért felelősek. A legjellemzőbb, hogy tevékenységük valamilyen anyagi haszon szerzésére irányul, ezért leggyakrabban a magas értékkel bíró áldozatokat tűzik ki támadásuk célpontjának.

A belső fenyegetések okozói egyrészt olyan munkatársak, akik saját haszonszerzés céljából követnek el ilyen tevékenységeket, de gyakori a gondatlanságból elkövetett támadás, ami gyakran kívülről irányított, és oka a belső dolgozók hanyag hozzáállása a cég biztonságpolitikájához.

A nemzetállamok a kiberfenyegetések harmadik legaktívabb szereplői, céljuk az ipari kémkedés, valamint államtitkok megszerzése. Tevékenységüket fokozottan nehéz nyomon követni és megakadályozni.

A *hacktivisták* olyan egyének, akik valamilyen politikai esemény hatására lejáró kampányt végeznek, vagy információt szivárogtatnak ki elsősorban kormányzati szervezetekhez kapcsolódóan.

A *kiberharcosok* (Cyber-fighters) olyan nemzeti vagy vallási radikális csoportok, amelyek a kibertérben működve okoznak feszültséget az etnikai közösségeken belül. Példának hozható az Iráni Kiber Hadsereg, ami hosszú idő óta működik a kibertérben. A kiberterrorizmus mint fenyegetés jelentősége csökken, mivel a terrorista csoportok kiberkapacitásai rendkívül csekélynek mutatkoztak:

elsősorban a kriptovalutákkal való kereskedésre és a sötét piacokon való kereskedelemre korlátozódnak.

A Panda Security [16] által készített, a 2017. évet értékelő és a 2018-as év előrejelzését tartalmazó éves jelentésében arra hívja fel a figyelmet, hogy a támadók ma már sokkal precízebben tervezik meg támadásaikat: aprólékosan tanulmányozzák áldozataikat, hozzájuk igazítják stratégiájukat, ezzel javítva saját esélyeiket. 2017-ben 75 millió különböző rosszindulatú program jött létre az év eleje és októbere között. Arra kell felkészülni, hogy az adaptív elterelő hadműveletekkel operáló rejtőzködő támadások válnak gyakoribbakká. A sebezhetőségek kihasználására szolgáló eszközök új támadási vektorokat hoztak létre, amelyek nem igényelnek emberi beavatkozást. A mobilitás általános lett, így a különböző szervezetek rendszerei fenyegetettebbek mint valaha.

A Panda Security előrejelzése szerint 2018-ra a mobileszközökre és az IoT-ra (Internet of Things – dolgok internete) írt kártevők további térnyerése várható. „Az IoT-n belül olyan intelligens eszközökről beszélünk, amelyek valamilyen, legtöbbször a személyes használathoz kötődő lényeges információt osztanak meg más eszközökkel egy internetalapú hálózaton keresztül a felhasználó legnagyobb megelégedettségére. A kommunikáció két végén gyakorlatilag bármilyen kapcsolódni képes dolog állhat, a viselhető technológiai megoldásoktól kezdve a háztartási gépeken át a biztonsági berendezéseken keresztül akár az egészségügyi infrastruktúra egyes elemeivel bezárólag.” [17 p. 17.] Ezek nem támadási célpontok, hanem újabb behatolási pontok lehetnek, amelyeken keresztül be lehet törni a különböző hálózatokra. A GDPR[3] szabályozásnak köszönhetően a nyilvánosság tudatossága növekedni fog, mivel az adatainak tárolásához minden esetben a hozzájárulását kell adnia. Ez felhívja a figyelmet a lehetséges veszélyekre, ami szükséges is a hatékony tudatosság védelmi módszere tekintetében.

A biztonsági frissítéseket minden szervezetnek prioritásként kell kezelnie. Az olyan esetek, mint az Equifax[4] vagy a WannaCry[5] alátámasztják, hogy minden egyes nap, amikor egy sebezhető rendszert nem frissítenek, növekszik a vállalat biztonsági kockázata, veszélyeztetve mind a felhasználói, mind a beszállítói adatok sértetlenségét.

A 2018-as év az előzőknél veszélyesebb helyzetet vetít előre, ezért a védekezés tekintetében a képzés és a tudatosság a két kulcsmomentum, majd ezt követi a kiberbiztonság gyakorlata.

E megváltozott rendszerben a vírusdefiníciós adatbázisfájlok rendszere többé már nem működik. A kutatási számok önmagukért beszélnek: az összes rosszindulatú kód 99%-a soha többé nem jelenik meg máshol.

---

[3] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete, vagyis a General Data Protection Regulation.

[4] 2017 nyarán az atlantai központú Equifax hitelbíráló sikeres hackertámadás áldozata lett. A megtámadott Apache Struts webalkalmazás keretrendszer biztonsági frissítéseit a cég nem telepítette időben, így május közepétől júliusig a behatolók mintegy 143 millió amerikai polgár személyes adatait szerezték meg.

[5] 2017 májusában felbukkant számítógépes zsaroló vírus komoly fennakadásokat okozott többek között Nagy-Britanniában, ahol kórházak számítógépes rendszereit tette elérhetetlenné rövid időn belül, ezáltal megbénítva az adott intézmények működését. A május közepén végrehajtott támadásban 150 ország 200 ezer szervezetének körülbelül 300 ezer számítógépe volt érintett. A zsarolóvírus egy olyan Windows-hibát használt ki, amit a Microsoft már két hónapja befoltozott, azonban a felhasználók jelentős része a hibajavítást nem telepítette. Az USA szakértői szerint a támadás a feltételezetten észak-koreai Lazarus csoport követte el.

1.3. Központi és helyi kormányzati rendszerek kiberbiztonsági kérdései

A kibertámadások jellege az utóbbi évtizedben jelentős változásokon ment át. Kezdetben azért hackelték meg a számítógépes rendszereket, hogy az elkövetők megmutassák: lehetséges. Manapság azonban a hackertámadások sok esetben valamilyen anyagi haszon szerzésére irányulnak, és mára már egy egész piac épült ki az illegálisan megszerzett adatokra. Időközben a rosszindulatú programok (malware) piaca is exponenciálisan növekedett, ami megnehezíti a támadások kivédését. Tulajdonképpen napjainkra szinte lehetetlenné vált a teljes biztonság megteremtése, így a szervezeteknek elsősorban a megelőzésre és az ellenálló képességük javítására kell koncentrálniuk.

Eggers megállapítása szerint a közszféra minden más szektornál jobban ki van téve a kibertámadásoknak, egyrészt, mert általában több és érzékenyebb adatot halmoz fel, másrészt pedig az adattárolás sokszor elavult módon, és korszerűtlen eszközökön történik. A digitális stratégiák (felhőalapú rendszerek használata, közösségi média megnyitása a kormányzati szféra előtt) sebezhetőbbé tették a kormányzati rendszereket, azonban ezt a fajta kockázatot kénytelenek elfogadni a fejlődés érdekében. A teljes biztonság nem valósítható meg, így a cél inkább az, hogy a szervezet felkészült legyen egy támadásra, és képes legyen minimalizálni a támadás okozta károkat. Mindezeket figyelembe véve, elengedhetetlen, hogy a kormányzat elegendő emberi és pénzügyi erőforrást fektessen a kiberbiztonság kiépítésébe. Ezzel szemben az erőforrás- és szakemberhiány általános probléma a kormányzati szervek kiberbizontonsági gyakorlatában. A legnagyobb problémát az okozza, hogy a kormányzati szektor nem tud versenyezni a magánszféra által kínált keresetekkel, így a kormányzati szervezetekből hiányzik a jól képzett IT szakember. [18]

Az állami és helyi önkormányzati hivatalok hatalmas nyomás alatt vannak az adataik, infrastruktúrájuk és szolgáltatásaik biztonságossá tételét tekintve. A folyamatos incidensek hatására természetesen növekszik a szervezeteken belüli tudatosság az adatok és a digitális infrastruktúra védelmével kapcsolatban. E szervezetekben dolgozó IT szakemberek azonban számos kihívással szembesülnek. Egyrészt azzal, hogy a fenyegetések komplexitása és intenzitása növekszik; leginkább a zsarolóvírusok jelentenek veszélyt, mivel képesek egyszerre nagyszámú áldozatot célba venni, és jelentős adatvesztést okozni. Másrészt a kiberfenyegetések egy jelentős része olyan konkrét szervezetet vagy szervezeten belüli egyént megcélzó fenyegetés, amit rendkívül nehéz a hagyományos védelemi struktúrával kiszűrni.

Lippman például az USA-ra nézve további problémának tartotta a kiberbiztonsági kezdeményezésekre fordított források csekély mértékét. Az amerikai önkormányzati szervezetek a költségvetésük kevesebb, mint 5%-át fordítják kiberbiztonságra, szemben a magánszféra vállalataival, ahol ez az arány 10%. Problémát jelent továbbá a biztonságiszakember-hiány, valamint a tudáshiány eme állami szervezeteken belül. A kormányzati szektor nehezen tudja felvenni a versenyt a magánszférával, így jelentős a magánszféra szakemberelszívó hatása. További problémát jelent, hogy a kiberbiztonsági termékek proliferációja a folyamatos riasztásokon keresztül túlterhelést okoz az IT rendszerekben, tehát kontraproduktív folyamatot eredményez. Az egyre komplexebbé váló szabályozásnak és fokozott biztonsági feltételeknek való megfelelés elsősorban a kis létszámú

szervezetekben okoz kapacitáshiányt. A növekvő számú és komplexitású fenyegetésekkel szemben elengedhetetlen az integrált, automatizált, rugalmas, valamint skálázható megoldások megtalálása annak érdekében, hogy a szervezetek képesek legyenek a pénzügyi és humán erőforrásaikat a lehető leghatékonyabban felhasználni a kiberbiztonságuk növelésére. Mivel a kormányzati szervezetekben korlátozott a szakértelem, egyszerű, de hatékony megoldásokra van szükség (például az IT szakértő egy ablakon keresztül képes legyen átlátni az egész hálózatot) [19].

Lou Romero is az USA-beli helyi önkormányzatok IT gyakorlatait vette górcső alá. Vizsgálata eredményeként megállapította, hogy az amerikai önkormányzatok többsége nem rendelkezik vészhelyzet esetére helyreállítási tervvel, így azok rendkívül kitettek az adatvesztésnek és a zsarolóvírusos támadásoknak. Néhány önkormányzat esetén létezik valamiféle háttértár, de ennek kapacitása nem elegendő a teljes működés helyreállításához. Romero azt találta, hogy míg az önkormányzatok jelentős része (60%) kiszervezi szolgáltatásai egy részét, csak kis részük gondoskodik kockázatkezelésről, ami egy harmadik fél részére történő kiszervezés kockázatait vonja maga után. Példának hozza a bérszámfejtés kiszervezését, ami egy esetleges támadás esetén veszélyeztetheti a munkatársak személyes adatainak védelmét. Megállapítja, hogy az önkormányzatok jelentős részénél nem megfelelő a jelszókezelési szabályzat, amit tovább súlyosbít az önkormányzati munkatársak információbiztonsági tudatosságának alacsony szintje és a tudatosságnövelő tréningek hiánya. Ugyancsak biztonsági kockázatként értelmezhető, hogy a helyi önkormányzati levelezés sok esetben nincs titkosítva, így akár az érzékeny információt tartalmazó csatolmányok is befoghatók. További kockázati tényező a régi számítógépek nem megfelelő újrahasznosítása: a leselejtezett gépeken tárolt adatok nem megfelelő kezelése, átmentése [20].

A Socitm Insight hírlevelében megjelent cikk [21] a helyi kiberbiztonság és reziliencia kérdéskörét járja körbe angol tapasztalatok alapján. Az állampolgárok bizalmának fenntartása érdekében a helyi hatóságoknak fokozott figyelmet kell fordítani a rájuk bízott információk biztonságára, így a kibervédelem és reziliencia egyre fontosabb szerepet tölt be egy szervezet életében. A Socitm tanulmánya a következő veszélyforrásokat azonosította be:

- érzékeny információ megszerzése gazdasági, diplomáciai vagy katonai előny szerzése érdekében,
- gazdasági-pénzügyi haszon,
- politikai nyilvánosság keltése,
- központi vagy helyi kormányzat lejáratása,
- számítógépes infrastruktúra irányítása kártékony célok elérése érdekében, vagy önmagában a számítógépes infrastruktúra megzavarása vagy megsemmisítése.

A digitális szolgáltatásoktól való függőség jelentősen növeli a sebezhetőséget például tűz, árvíz vagy más természeti katasztrófa esetén. A helyi hatóságok nagymértékben növelhetik ellenálló képességüket az egyes rendszerek összekapcsolásával és közös szolgáltatások nyújtásával.

A kiberbiztonság további fontos kérdése, hogy a biztonsági intézkedések a kormányzati szereplők részéről milyen politikai vitákat váltanak ki az állampolgárokból, a nyomásgyakorló csoportokból. A politikai szereplők feladata, hogy olyan intézkedéseket hozzanak, amelyek egyrészt hatékonyan fel tudják venni a versenyt a rosszindulatú tevékenységekkel szemben, másrészt tiszteletben tartják az állampolgárok jogait a kibertérben is. Az átláthatóság kritikus szempont az állampolgárok bizalmának fenntartása érdekében.

Összefoglalás

A biztonságra törekvés az emberek alapvető szükségletét képezi, viszont tökéletes állapota sosem érhető el. A biztonságtudomány fejlődésének a 2001-es New York-i terrortámadás jelentős lendületet adott, mivel szembesítette a kormányzatokat a nem állami szereplők jelentette potenciális fenyegetéssel. A biztonságtudomány és részei csak multidiszciplinárisan, komplexen közelíthetők meg, mivel az érintett ember–technika–környezet tényezőcsoport csak közös rendszerként értelmezhető. A biztonságtudomány vizsgálódási területe a kritikus infrastruktúrákra terjed ki, aminek kiemelt területe az információbiztonság. A kritikus infrastruktúrákat szintén az egymástól való kölcsönös függés és informatizáltság jellemzi.

Az Európai Bizottság által 2005-ben kiadott *Zöld könyv* célja a nemzeti kritikus infrastruktúrák védelméről (NKIV) szóló nemzeti programok megalkotásának támogatása volt. A NKIV három fő célkitűzést fogalmazott meg a megelőzés és a védelem, az érintettek felkészültségének biztosítása és az ellenálló képesség fejlesztése érdekében. E nemzetközi kezdeményezés hatására 2012-ben megszületett a hazai szabályozás a létfontosságú rendszerek és létesítmények kijelöléséről és védelméről.

A kritikus információs infrastruktúrák különös figyelmet érdemelnek, hiszen nem különülnek el a létfontosságú infrastruktúráktól; védelmüket, biztonságukat együttesen szükséges biztosítani.

Az információs társadalom fejlődése nagyon rövid idő alatt alakította át ismert világunkat. A webtechnológia szabaddá válása óta alig húsz év telt el, és ma már a gépek által vezérelt együttműködő hálózatokról, mesterséges intelligenciáról beszélünk. A 2007-es észt kibertámadás új nézőpontba helyezte a kiberbiztonsági kérdéseket. Az ilyen szintű kiberfenyegetettség és az erre adott hatalmi válasz jelentősen megosztják a különböző biztonságtudományi iskolákat annak kérdésében, hogy hol van az a határ, ameddig a biztonság érdekében a hatalom korlátozhatja az egyén jogait. A kiberbiztonsági kérdések kezelésére az Európai Unió 2004-ben létrehozta az Európai Uniós Hálózat- és Információbiztonsági Ügynökséget, az ENISA-t, aminek keretében, 2017-ben kiemelt területeként került azonosításra a kiberbiztonság kérdésköre, tekintettel a kiberfenyegetettség növekedésére.

Az Európai Bizottság három cselekvési területet határozott meg a kiberbiztosnság biztosítása érdekében: reziliencia erősítése és kiberbiztonsági kapacitások növelése, hatékony bűnügyi válaszadás, fokozott nemzetközi koordináció és együttműködés. Az ENISA a 2017-es jelentésében tételesen felsorolta a kiberfenyegetési trendeket, és számba vette a legveszélyesebb fenyegetéseket. Ilyen irányvonal a kibertámadások komplexitásának növekedése, a támadók rejtőzködési képessége, a kártékony infrastruktúrák adaptálódása és nehéz azonosítása. Különös figyelmet érdemel, hogy a

szervezetek – bár kiemelt fontosságú – nem fordítanak kellő figyelmet arra, hogy munkatársaik megfelelő készségekkel, képességekkel rendelkezzenek a kiberbiztonság kérdéskörében. A két kiemelt célkitűzés a védekezés optimalizálása érdekében: a szabályozás és a kompetenciafejlesztés.

A szakértők véleménye szerint a közszféra minden más szektornál jobban kitett a kibertámadásoknak, mivel sok érzékeny adatot tárol és erőforrásai (emberi és technológiai) sokszor nem felkészültek, tudatosak vagy korszerűek. További probléma a kiberfenyegettség egyre komplexebbé válása, miközben általános a szakemberhiány, továbbá az (ön)kormányzati terület nem képes versenyezni a forprofit szféra kereseti kínálatával.

Az amerikai önkormányzatok esetében azonosított hátrányok és nehezítő tényezők a területre fordított források alacsony volta, a szakemberhiány, a nem megfelelően védelmi rendszerek okozta túlterhelés, a feladatok növekedése miatti – különösen a kis szervezetek esetében – kapacitáshiány. Az USA önkormányzatai esetében több kockázatot is azonosítottak: nem rendelkeznek helyreállítási tervvel, jelentős részük kiszervezi szolgáltatásai egy részét, viszont nem rendelkezik kockázatkezelési tervvel sem egy harmadik fél részére történő adatkiszolgáltatás kezelésére, többségüknél nincs jelszókezelési szabályzat, amit tovább súlyosbít a munkatársak alacsony információbiztonság-tudatossági szintje, illetve a mobil eszközök használatára és a leselejtezett eszközök kezelésére vonatkozó szabályozás hiánya.

2. EURÓPAI ÉS HAZAI SZABÁLYOZÁSI ÉS SZERVEZETI KERETEK

Az Európai Unió irányelveit a nemzetállamok jogharmonizációs kötelezettségüknek megfelelően ültetik át jogrendjükbe. Az EU szabályozása a kötelező kereteket határozza meg, a részletszabályokat, szervezeti felépítést a nemzeti sajátosságoknak megfelelően a tagállamok határozzák meg.

2.1. Az európai uniós szabályozási keretek

Ahogyan az előzőekben láthattuk az Európai Unió prioritásként kezeli a kiberbiztonsági kérdéseket. Az alfejezetben bemutatásra kerül az EU kiberbiztonsági álláspontja, szabályozási keretei.

2.1.1. Az Európai Parlament és az Európai Tanács koncepcionális álláspontja egy erős európai kiberbiztonság kialakításáról

Az Európai Parlament és a Tanács [22] 2017 őszén közös állásfoglalást adott ki. A reziliencia, elrettentés és védelem témakörében részletesen kifejti az EU előtt álló kihívásokat, és megjelöli a legfontosabb cselekvési területeket. Megállapításai között szerepel, hogy a tradicionális bűnözés és a kiberbűnözés közötti határvonal elmosódása fokozott problémát jelent, hiszen a kibertérben sokkal nehezebb az elkövetőt beazonosítani és előállítani. Ugyanakkor gyakran állami szereplők is élnek kibereszközökkel a geopolitikai céljaik elérése érdekében, például a demokratikus folyamatokba való beavatkozás, hamis információ keltés vagy a kritikus infrastruktúra megzavarása által. Habár a tagállamok önállóan felelősek a saját nemzeti biztonságukért, a kiberfenyegetések mértéke és határon átnyúló természete következtében indokolt az uniós szintű fellépés a kibervédelmi tevékenységek összehangolása érdekében.

A dokumentum elsőként az ENISA mandátumának kiterjesztését és megerősítését tűzte ki célul. Álláspontjuk szerint az ENISA a jövőben kiemelt tanácsadó szerepet kapna a kiberbiztonsági politika végrehajtásában, valamint közreműködne az európai kiberbiztonsági tanúsítványok létrehozásában, műveleti együttműködésekben és válságkezelésben. A kiberbiztonsági piac növekedése szükségessé teszi a kiberbiztonsági termékek piacán magasabb szintű standardok bevezetését. Ennek érdekében az Európai Bizottság kezdeményezte az *Európai kiberbiztonsági tanúsítványok keretrendszerének* kidolgozását. A *Hálózatok és információs rendszerek biztonságáról szóló irányelv* végrehajtása a tagállamok kiberbiztonsági képességeinek erősítését, valamint a tagállamok közötti együttműködés hatékonyságát szolgálja. Az irányelv implementációjának kritikus pontja az információ áramlása, ami egyelőre számos akadályba ütközik, főként a köz- és magánszféra között. A megoldást a köz- és magánszféra együttműködésének (PPP: public private partnership) erősítése és a szélesebb körű információmegosztás jelentené.

A tagállami gyakorlatban a reziliencia jelentősen növelhető a felkészültség erősítésével, valamint a támadásokra való gyors és hatékony reagálás érvényesítésével. Továbbá szükséges a tagállami kiberbiztonsági kompetenciák összehangolása és egy szintre hozása, aminek érdekében egy Európai Kiberbiztonsági Kutató és Kompetencia Központ felállítására tettek javaslatot.

A kiberbiztonság egyik fontos területe a tudatosság elérése az oktatás által. Ennek nem kizárólag az IT szakemberek képzésében kell nagyobb szerepet kapina, hanem egységesen meg kell jelennie más tudományterületek tananyagában is. A reziliencia növelése érdekében a szervezeteknek képezniük kell munkavállalóikat annak érdekében, hogy azok tudatosabban végezzék munkájukat, és tisztában legyenek a kiberhigiénia fogalmával és gyakorlatával. A tagállamok feladata a lehető legteljesebb körben biztosítani a kibervédelmi eszközök elérhetőségét a vállalkozások és egyének számára, valamint az ország vezető szervei figyelmét felhívni az e-kormányzat terén alkalmazandó biztonsági előírásokra. Továbbá a tagállamoknak különböző tudatosságnövelő kampányokon keresztül kell felkészíteni a lakosságot a kiberkockázatokra.

A kibervédelem egyik meghatározó eleme az elrettentés, aminek kapcsán a dokumentum a bűnüldözés hatékonyságának növelését tűzte ki célul, elsősorban az elkövetők felkutatása, nyomon követése és előállítása terén. Mindezek kapcsán fokozottan előtérbe kerül a tagállamok bűnüldöző szervei közötti együttműködés ösztönzése, például az elektronikus bizonyítékok kölcsönös elérhetősége vagy az egységes igazságügyi standardok bevezetése terén. A kiberbiztonság egyre fontosabb részét képezi a *közös biztonság és védelempolitikának,* mivel annak keretein belül egységesített folyamatok és technikai képességek kerülnek kidolgozásra, amelyek tovább növelik az unió ellenálló képességét.

Végezetül megfogalmazták, hogy a kiberfenyegetettség (annak globális természete miatt) elleni fellépés a nemzetközi együttműködés és partnerség elengedhetetlen része az EU és a harmadik országok között. Az EU mindenekelőtt az ENSZ-el szorosan együttműködve előmozdítja a nemzetközi jog érvényesülését a kibertérben is, miközben támogatja a regionális bizalomépítő intézkedések fejlesztését és végrehajtását. Bilaterális kapcsolataiban hangsúlyozza a dialógus fontosságát, valamint az állami felelősségvállalás szerepét, ugyanakkor biztosítja a nemzetközi közösséget arról, hogy a kiberbiztonság kiépítése nem szolgál a belső piac protekciójának indokaként, se az alapvető jogok és szabadságok korlátozásaként. Továbbá a NATO-val szorosan együttműködve segíti a kiberbiztonsági standardok interoperabilitását is.

2.1.2. Európai Unió szabályozási keretei a kiberbiztonság területén

Az európai kiberbiztonsági keretrendszer a kivételezettség logikájával szemben egy preventív, megelőző logikát alkalmaz. A biztonsági szereplők célja, hogy olyan technológiákat és stratégiákat alakítsanak ki, amelyek által a jövő kiszámíthatóbbá és könnyebben kezelhetővé válik, így még azelőtt sor kerüljön a beavatkozásra, hogy az adott szituáció kivételes intézkedéseket követelne. Az európai biztonsági rendszerekben egyre nagyobb hangsúllyal jelenik meg a kiberbiztonság kérdése. Az Európa Tanács, a NATO, valamint az Európai Unió is egyre átfogóbb kiberbiztonsági struktúrát alakított ki egyes intézményekkel szemben. Az EU hangsúlyozza az összes releváns érdekelt fél felelősségét a kiberbiztonsági együttműködésben. Ennek érdekében szükség van arra, hogy az érdekeltek normákat és viselkedési formákat határozzanak meg a kibertérre vonatkozóan, betartsák a létező jogszabályokat, valamint bizalomnövelő intézkedéseket alakítsanak ki, amelyek által növelik az átláthatóságot és csökkentik az állami viselkedés téves észlelését. Habár alapjaiban véve az európai kiberstratégiák inkább államközpontúak, egyre nagyobb jelentőséget kap a nemzetközi, valamint a

magánszféra szereplőivel való együttműködés. Az európai kiberbiztonság további kritikus pontja a jogalkotás nehézkessége. Az Európai Unió tagállamainak hajlandósága a nemzeti jogszabályok harmonizációjára továbbra is alacsony, holott a kiberkockázatok növekvő száma gyors reakciót tenne szükségessé [3 pp. 141–157.]

A 2013-ban készült el az Európai Unió kiberbiztonsági stratégiája, majd az Európai Bizottság számos további kezdeményezést fogadott el az európai kiberbiztonság növelésére vonatkozóan. A kiberbiztonság kérdése a politikai prioritások előterébe került, és mind az EU új, *digitális egységes piaci stratégiájának* [23], mind *Az európai digitális menetrendnek* [24] szerves részét képezi. Legutóbb a 2016-ban elfogadott *hálózati és információs rendszerek biztonságáról szóló irányelv* (NIS: Network and Information Security) [55] jelentett fontos mérföldkövet a biztonságos európai kibertér megteremtésében.

A kiberbiztonság fontosságát alátámasztja, hogy manapság a kritikus infrastruktúra (például víz- és villamosenergia ellátás) legnagyobb része digitális hálózatokon keresztül működik, így egy kibertámadás valós veszélyforrást jelenthet a mindennapi életre is. A kiberbiztonság a digitális közös piac létrehozása szempontjából is fontos, hiszen az emberek digitális platformokba vetett bizalma nélkül az online szolgáltatások nem tudnak hatékonyan működni.

Az Európai Bizottság fő célként a kiberbiztonsági képességek és az együttműködés növelését, az EU globális szerepének erősítését, valamint a tagállami politikák egységesítését tűzte ki.

A kiberbiztonsági stratégia öt prioritást határozott meg:

- kiberreziliencia növelése,
- kiberbűnözés csökkentése,
- uniós kiberbiztonság-politika és ellenálló képességek (védekezés, fejlesztés, elrettentés, tudatosság) kialakítása a közös biztonság és védelempolitika keretein belül,
- ipari és technológiai erőforrások fejlesztése,
- koherens nemzetközi kibertér-politika létrehozása.

A 2015–2020 közötti időszakra kiterjedő európai biztonsági stratégia az alábbi cselekvési területeket azonosítja:

- a meglévő politikák végrehajtása a kiberbiztonság, az információs rendszerek elleni támadások, gyermekek szexuális kihasználása elleni küzdelem területein;
- a meglévő szabályozás felülvizsgálata és lehetséges kiterjesztése a nem készpénzzel történő visszaélés és csalás elleni küzdelem terén;
- a kiberbűnözés elleni bűnügyi nyomozással szemben fennálló akadályok felülvizsgálata, kiemelt figyelemmel a joghatóságra és az információhoz való hozzáférésre;
- kiberkapacitás-építő tevékenységek fejlesztése.

Az Európai Digitális Egységes Piac Stratégia [25] középpontjában az európai versenyképesség ösztönzése, és a kiberbiztonsági piac töredezettségének leküzdése áll. A stratégia célja a köz- és magánszféra együttműködésének megteremtése (PPP) a kiberbiztonság terén.

A tagállamoknak a NIS irányelvének saját igazgatási rendszerükbe való integrálására 21 hónap áll rendelkezésre. Az irányelv három pillérre épül:

- a tagállami készenlét biztosítása,
- a tagállamok közötti együttműködés erősítése,
- a biztonság kultúrájának megteremtése, fokozott figyelemmel a kritikus szolgáltatásokra (energia, közlekedés, vízügy, bankszektor, pénzügyi-piaci infrastruktúra, egészségügy, digitális infrastruktúra).

A megvalósítás érdekében a NIS-irányelv valamennyi tagállam számára kötelezettségeket állapít meg a hálózati és információs rendszerek biztonsága nemzeti stratégiájának elfogadására vonatkozóan, ami meghatározza a stratégiai célokat és a végrehajtandó konkrét szakpolitikai intézkedéseket. Az irányelv 4. cikke szerint a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia olyan keret, amelyben a hálózati és információs rendszerek biztonságára vonatkozóan nemzeti szinten stratégiai célkitűzéseket és prioritásokat állapítanak meg.

Az irányelv 7. cikke rendelkezik a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiáról. Eszerint valamennyi tagállam elfogad egy hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiát, amiben meghatározza a stratégiai célokat, valamint a hálózati és információs rendszerek magas szintű biztonságának megteremtéséhez és fenntartásához szükséges megfelelő szakpolitikai és szabályozási intézkedéseket. A hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia különösen a következő témákkal foglalkozik:

- a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia céljai és prioritásai;
- a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia céljainak és prioritásainak teljesítését szolgáló irányítási keretrendszer, ideértve a kormányzati szervek és egyéb érintett szereplők szerepkörét és felelősségét is;
- a felkészültségre, a reagálásra és a helyreállításra vonatkozó intézkedések azonosítása, ideértve a köz- és a magánszféra közötti együttműködést is;
- a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiához kapcsolódó oktatási, tájékoztató és képzési programok megjelölése;
- a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiához kapcsolódó kutatási és fejlesztési tervek megjelölése;
- a kockázatok feltárására szolgáló kockázatértékelési terv;
- a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégia végrehajtásába bevont különböző szereplők jegyzéke.

Az irányelv 25. cikk (1) bekezdése alapján a tagállamoknak 2018. május 9-ig szükséges elfogadniuk és kihirdetniük azokat a törvényi, rendeleti és közigazgatási rendelkezéseket, amelyek szükségesek ahhoz, hogy az irányelv előírásainak megfeleljenek.

2.1.3. Európai Unió szabályozási keretei az adatkezelésről (GDPR: General Data Protection Regulation)

A 2018 májusában hatályba lépő adatvédelmi szabályok [56] előtt érvényben lévő általános adatvédelmi rendelet több, mint 20 éve került kihirdetésre, ami az elmúlt évek infokommunikációs változásaihoz viszonyítva rendkívül hosszú időszaknak számít. Az elmúlt két évtizedben létrejött digitális, vezeték nélküli és vezetékes kommunikációs módok lényegesen hozzájárulnak ahhoz, hogy az emberek személyes adataikat, információikat napi rendszerességgel és bátrabban osztják meg, mint korábban, ami ugyanakkor komoly kockázatokat is magában hordoz. Az új rendelet megszületése maga után vonja, hogy minden tagállamban a személyes adatok védelméhez kapcsolódó szabályozást felül kell vizsgálni, és a jogharmonizációs kötelezettségeknek megfelelően módosítani az uniós szabályozásnak megfelelően.

Az új szabályok megerősítik a személyes adatok tárolásának megszüntetéséhez való jogot. Az internetes kereskedőknek és szolgáltatóknak szem előtt kell tartaniuk az alapértelmezett adatvédelem elvét, vagyis a társaságok kötelesek a lehető legvilágosabban, legérthetőbben és legátláthatóbban tájékoztatni látogatóikat személyes adataik felhasználásának módjáról annak érdekében, hogy azok könnyebben eldönthessék, mely adataikat osztják meg. A nemzeti adatvédelmi felügyeleti hatóságok feladata lesz, hogy ezeket a jogokat tudatosítsák, valamint iránymutatást adjanak arról, milyen módon kell velük a leghatékonyabban élni.

A személyes adatok tárolása megszüntetésének lehetősége az állampolgárok számára lehetővé teszi online adataik kezelését a védelméhez kapcsolódó kockázatok figyelembevételével. A szabályok célja az emberek jogainak erősítése. A magas szintű adatvédelem elengedhetetlen ahhoz, hogy nagyobb bizalom alakuljon ki az internetes szolgáltatások és általában a digitális gazdaság iránt. Mivel az európai fejlődés motorja az IKT területéhez kapcsolódik (az ágazat közvetlenül 20%-kal járul hozzá az általános növekedéséhez, továbbá az összes gazdasági beruházás 40%-a erre az ágazatra irányul), az EU gazdasági növekedésének élénkítése szempontjából rendkívül fontos az emberek bizalma az online szolgáltatások iránt. Az adatáramlás mindinkább globalizálódik, a felhőalapú szolgáltatások pedig egyre gyakoribbak. Kiemelt fontosságú az egyéni ellenőrzés lehetősége a személyes adatok kezelése felett. [26]

Az európai rendelet szükségessé teszi a hazai szabályozás felülvizsgálatát is.

2.2. Az európai nemzetek kiberbiztonsági stratégiáinak összehasonlítása

Az egyes országok kiberbiztonsági stratégiái között jelentős átfedések és eltérések tapasztalhatók, amik több okra vezethetők vissza. Attól függően, hogy mennyire követték a nemzetközi ajánlásokat, több részletben is mutatnak hasonlóságot, sőt azonosságot is. Vannak azonban olyan részek, ahol az egyes országok nézőpontjának megfelelően helyeznek hangsúlyt az egyes ajánlásokra, vagy hagyják

figyelmen kívül azokat. A CECSP[6] országok kiberbiztonsági stratégiáját három pillér (európai uniós elvárások, NATO által megszabott feltételek, kiberbiztonsági stratégiákat összehasonlító elemzés, módszertan) mentén hat területet vizsgálva elemezték [24 pp. 130–136.]. Az öt CECSP ország stratégiájának kialakítása során e három pillér alapján, az alábbi területeken kerestek azonosságokat és eltéréseket:

- alkalmazott terminológia;
- stratégia beágyazottsága;
- a kiberbiztonsági környezet értékelése és a fenyegetések számbavétele;
- célkitűzések pontos meghatározása és prioritások felállítása;
- cselekvési terv meghatározása;
- kockázatelemzési és -értékelési szemléletmód érvényesülése.

1. táblázat

A CECSP országok első kiberbiztonsági stratégiáinak összehasonlítása [27 pp. 130-136] saját szerkesztés

	Ausztria	**Csehország**	**Lengyelország**	**Magyarország**	**Szlovákia**
Terminológia	Részletesen tartalmaz.	Nem tartalmaz.	Az elején tartalmaz néhány definíciót.	Törzsszövegében tartalmaz: kibertér, kiberbiztonság.	Mellékletében tartalmaz.
Beágyazottság	Mindegyik figyelembe veszi az EU és a NATO elvárásait, és hivatkozik a nemzeti felsőbb szintű stratégiákra (például nemzetbiztonsági). Mindegyik meghatározza a frissítés és felülvizsgálat időpontját. Az egyes szereplők felelőssége és érintettsége meghatározott.				
Helyzetelemzés	van[7]	van	van	van	van
Célkitűzések/ prioriátások	Mindegyik stratégia meghatározza a célokat (közel azonosakat). Prioritási sorrendet egyik sem állított fel.				
Cselekvési terv	Komplex cselekvési tervet tartalmaz.	Célkitűzésekkel együtt szerepelnek az intézkedések.	Az intézkedésekhez rendeltek prioritást és mindegyikhez évente kockázatelemzést készítenek.	Kormányzati koordináció területén jelöl ki feladatokat.	Célkitűzésekkel együtt szerepelnek az intézkedések.
Értékelési útvonal	Folyamatos és rendszeres.	Általános jelleggel.	Folyamatos és rendszeres.	Általános jelleggel.	Általános jelleggel.

Az Európai Unión belüli országok első kiberbiztonsági stratégiáik kialakítása során elsősorban arra koncentráltak, hogy felmérjék a legfontosabb kormányzati feladatokat, kijelöljék a szükséges kormányzati szerepeket, kifejlesszék a koncepciókat, és létrehozzák azokat a szervezeteket, amelyek szükségesek a kibertérből érkező kihívások a nemzeti szintű kezelésére.

A dokumentumok vizsgálata egy folyamat, ami során fény derülhet hasznosítható módszerekre. Ezt szokták mint jó gyakorlatot, best practiset vagy mint bechmarkingot emlegetni.

[6] Ausztria és Csehország kezdeményezésére – Lengyelország, Szlovákia és hazánk részvételével – 2013-ban hozták létre a Közép-európai Kiberbiztonsági Platformot (Central European Cyber Security Platform).
[7] Része a kiberkockázati mátrix.

Ilyen jó gyakorlat az a komplex megközelítés, amit az osztrák és lengyel stratégia tartalmaz: a beépített folyamatos és rendszeres kockázatelemzési és értékelési módszertan. Jó példaként azonosítható – Molnár által bemutatott [28] – az Egyesült Királyság által megvalósított első és – a tapasztalatokat és a várható trendeket figyelembe vevő – második generációs kiberbiztonsági stratégiája.

A 2011-től 2015-ig tartó időszakra vonatkozó brit kiberbiztonsági stratégia víziójában egy gazdasági és társadalmi szempontból értéket képviselő biztonságos és rugalmas kibertér elérése fogalmazódott meg négy célkitűzés mentén. A stratégia céljainak elérésére 650 millió font anyagi erőforrást allokáltak, azonban felismerve a terület fontosságát, végül a négy év alatt 860 millió fontot költöttek a stratégia megvalósítására.

Az elért releváns eredmények röviden:

- Széleskörű partnerségi hálózat[8] létrehozása, aminek célja biztosítani az információ-megosztást a piac és a kormányzat érintett szereplői között.
- Cyber Essentials[9] kormányzati program, ami alapvető biztonsági intézkedéseket követel meg a vállalatoktól annak érdekében, hogy könnyen és eredményesen tudják felvenni a harcot az internetes bűnözéssel szemben.
- A CERT-UK[10] létrehozása, ami a hálózatbiztonsági kérdésekben érintett szervezetek központi fórumaként szolgál és havonta három gyakorlat segítségével teszteli a kiberbiztonsági reagáló képességet. Emellett 2013-ban elindították az egyedülálló kibertartalékos programot (Cyber Resesrve), és hatékony kezdeményezésnek bizonyult a Kibervédelmi Partnerség (Defence Cyber Protection Partnership) és az Összhaderőnemi Kibercsoport (Joint Forces Cyber Group) is.
- A harmadik célkitűzés a nyitott társadalmakat támogató nyitott, vibráló és stabil kibertér megteremtésére irányul, aminek keretében kiemelt figyelmet szentelnek a kiberbiztonsági ismeretek és tudás széles körben való terjesztésére.[11]
- A tudatosítás, képzés kiemelt fókuszterület. 2012-től kezdve alapvető kiberismeretek oktatása indult az általános iskolákban, a felsőoktatásban pedig valamennyi alapképzésben bevezetésre került egy közös kiberbiztonsági modul, a mesterképzésben pedig már több, mint egy tucat akkreditált mesterképzés indult el. Több kutatóintézet is rendelkezik kiberbiztonsági profillal, akik célul tűzték ki, hogy a már működő kiberbiztonsági doktori iskolák 2019-re száz doktoranduszt tudnak majd magukénak [28 pp. 137–141.].

A britek új kiberbiztonsági stratégiája 2021-ig tervez. Az öt éves időszakra a szükséges kiberbiztonsági reformok és intézkedések megvalósítására 1,9 milliárd fontot irányoztak elő annak

[8] Kiberbiztonsági Információmegosztási Partnerség – Cyber Security Information Sharing Partnerhip –, ami 10 regionális csoportot, több, mint 1750 szervezetet és 5000 magánszemélyt fog össze.
[9] A követelményeket teljesítő vállalatok tanúsító oklevelet kapnak, és felkerülnek a kormányzati listára mint képesített vállalatok, amivel egyúttal teljesítik az előfeltételt ahhoz, hogy kormányzati beszállítók lehessenek.
[10] Computer Emergency Response Team.
[11] Fórumai: a Londoni Folyamat (London Process) keretében megrendezett konferenciák mellett az Egyesült Királyság évente harminc nemzetközi projektben vesz részt.

érdekében, hogy céljaik szerint a kiberfenyegetésekre magabiztosan, rugalmasan tudjanak reagálni, miközben biztonságosan és hatékonyan prosperálnak a digitális világban.

Hármas célrendszert fogalmaztak meg:

- védelem (defend),
- elrettentés (deter) és
- fejlesztés (develop).

Ezek elérésére három stratégiai cél mentén terveznek beavatkozásokat. Az első az aktív kibervédelem annak érdekében, hogy a brit IKT kevésbé legyen sérülékeny. Eszközeik: beépített védelemmel rendelkező eszközök, kormányzat és kritikus infrastruktúrák kiemelt védelme. Az elrettentés keretében deklaráltan támadó kiberképességeket kívánnak fejleszteni annak érdekében, hogy meg tudják védeni a saját kiberterüket, és visszavágni abban az esetben, ha támadás éri azt. Mindemellett szorgalmazzák egy globális kiberszövetség létrehozását. A harmadik fókuszterület a fejlesztés, ezen belül is kiemelten a humánerőforrások fejlesztése.

2.3. Hazai szabályozási és szervezeti keretek

Az alfejezetben összefoglalásra kerülnek a kiberbiztonság hazai szabályozási és szervezeti keretei. Áttekintésre kerül a kormányzati kiberkoordináció és az önkormányzati koordináció szükségessége.

2.3.1. Magyarország kiberbiztonsági stratégiája

A Digitális Jólét program (DJP) 2.0 [57] hivatott a kormányzati infokommunikációs és digitális fejlesztési programokat összehangolni annak érdekében, hogy Magyarország minél felkészültebb legyen az elkerülhetetlen és egyre gyorsuló digitális átalakulásra. Célként fogalmazódott meg az oktatási rendszer digitális átalakítása, a digitális kompetenciák fejlesztése, a hazai vállalkozások és a közigazgatás digitális transzformációjának segítése. A DJP 2.0 [29] komplex megközelítést céloz meg, és a horizontális területek között kiemelten szerepelteti az információbiztonságot és az kibervédelmet. Javasolt intézkedései között kiemelten szerepel a Nemzeti Kiberbiztonsági Stratégia felülvizsgálata a kibervédelmi képességek fejlesztése érdekében.

A Magyary Zoltán Közigazgatás-fejlesztési Program keretében 2012 elején sor került a stratégiai tervezés és irányítás teljes hazai rendszerének átalakítására. A stratégiaalkotási és irányítási tevékenység megújítását és a stratégiák tartalmi összehangolásához szükséges keretek kialakítását a 38/2012. (III. 12.) Kormányrendelet a kormányzati stratégiai irányításról [58] valósította meg. A rendelet egyik célja hozzájárulni ahhoz, hogy a stratégiai szemlélet a kormányzati tervezés részévé váljon, a stratégiai dokumentumok pedig egy átlátható, hierarchikus rendszerbe illeszkedjenek. A Nemzeti Kiberbiztonsági Stratégia már az új stratégiai tervezési rendszer kialakítását és hatálybalépését követően, 2013-ban került kiadásra, annak szabályait és elvárásait azonban részben figyelmen kívül hagyta. A stratégia nem hivatkozik a stratégiai tervezési rendszerről szóló rendeletre, és jelenlegi állapotában nem feleltethető meg egyetlen, a rendeletben említett stratégiai dokumentumtípusnak sem. Annak ellenére, hogy a 2013-as stratégia a stratégiák elkészítésére vonatkozó hazai szempontrendszernek nem felel meg, és nemzetközi összehasonlításban is számos hiányossága felróható, a dokumentum rámutatott számos olyan területre és kérdésre a kiberbiztonság kapcsán, amelyek napjainkban már nem csak a szakembereket, hanem egyre inkább

a közvéleményt is foglalkoztatják. A 2013-as stratégiával együtt elfogadott információbiztonsági törvény (Ibtv.) [59] megteremtette azt a jogszabályi környezetet, amely elősegítette a kiberbiztonság területén működő állami szervezetek kialakítását és megszilárdítását [11 p. 5.].

A stratégia célja a szabad, biztonságos és innovatív kibertér megteremtése, Magyarország versenyképességének növelése, az új technológiai innovációk, megoldások biztonságos módon történő bevezetése, illetve adaptálása a digitalizálódott államigazgatási, kormányzati és gazdasági területeken, a biztonságos elektronikus közigazgatási rendszer létrehozása, illetve az állami szolgáltatások innovatív fejlesztése, valamint a kiberbiztonság, a tudatosság növelése, a felkészültség szintjének emelése a társadalom minden területén.

„A 2016. július 19-én az Európai Unió a hálózatbiztonság és információbiztonság területén egységes törekvéseként megjelentette az úgynevezett NIS irányelveket, amelyben a tagállamok részére előírta, hogy rendelkezzenek az irányelvben bemutatott területeken kiberbiztonsági stratégiával. Ennek megfelelően Magyarország előtt két lehetőség adódott. Vagy módosítja a már meglévő, 2013-ban kormányhatározattal elfogadott kiberbiztonsági stratégiát, vagy az irányelveknek megfelelően új stratégiát alkot. A szakemberek egységes álláspontja egy új stratégia megalkotását célozta meg, így megkezdődött a jogszabály előkészítése.” [30 p. 352.]

A stratégiával együtt elfogadott és azóta többször módosított Ibtv. megteremtette azt a jogszabályi környezetet, ami elsősorban az állami, közigazgatási elektronikus információs rendszerek tekintetében elősegítette a kiberbiztonság területén működő állami szervezetek kialakítását és megszilárdítását.

A hazánkban működő kiberbiztonsági szabályozás és gyakorlat hiányossága, hogy a szabályok és kötelezettségek szigetszerűen, csak az állami és önkormányzati rendszerekre, illetve a létfontosságú infrastruktúrákra vonatkozóan kerültek megfogalmazásra, másrészt a kiberbiztonsági szakosított intézményrendszer – részben a hírközlési és oktatási-kutatási ágazatot kivéve – is csak e területeken, e szabályok mentén jött létre. A Nemzeti Közszolgálati Egyetem Stratégiai Védelmi Kutatóközpontja elkészítette a *Kiberbiztonsági Stratégia 2.0 – A kiberbiztonság stratégiai irányításának kérdései* [11] című tanulmányt, amelyben a nemzeti, európai uniós és nemzetközi szabályok és normák alapján vizsgálta meg Magyarország Nemzeti Kiberbiztonsági Stratégiáját. A tanulmány azonosította a kiberbiztonsági stratégia hiányzó elemeit, illetve ajánlásokat fogalmazott meg a felülvizsgálat során szükségszerű változtatásokra. Például az új stratégiának szükséges figyelemmel lennie a kormányzati stratégiaalkotási elvárásokra, a nemzetközi ajánlások érvényre juttatására, akciók és cselekvési tervek megfogalmazására úgy, hogy ezekhez rendel indikátorokat, területi mutatókat.

A Nemzeti Kibervédelmi Intézet szervezésében és informatikai biztonsági szakértők bevonásával a 2017 elején megalakult Információbiztonsági Stratégiai Bizottság a rendelkezésre álló elemzések, illetve a Digitális Jólét Programban megfogalmazott helyzetértékelés és SWOT elemzés figyelembevételével iránymutatásokat fogalmazott meg a stratégia felülvizsgálatára és az újonnan létrejövő stratégia célkitűzéseire vonatkozóan.

Ezen célok elérése érdekében – az irányelv előírásainak figyelembevételével – a meghatározott célterületek, illetve feladatok az alábbiak:

- hatékony hazai és nemzetközi együttműködések,
- tudatosság növelése,
- oktatás, képzés – versenyképes hazai tudásbázis,
- gyermek és ifjúságvédelem – biztonságos, tudatos, értékteremtő internethasználat,
- kutatóközpontokkal való együttműködés, a kutatás és fejlesztés szerepének erősítése,
- a NIS irányelvének átültetése a magyar jogrendbe, és egy nemzeti szabályozás kidolgozása,
- az állami és önkormányzati, kormányzati szervek szolgáltatásainak, biztonságának, valamint az e-közigazgatás biztonságának növelése (a Nemzeti Infokommunikációs Stratégia 2014–2020 program végrehajtása, a digitális állam megvalósítása),
- védelempolitika – elhárító és támadó képesség,
- kritikus infrastruktúrák és szolgáltatásai védelme,
- bűnüldözés – kiberbűnüldözés,
- intézményrendszer fejlesztése.

A jelenleg hatályos stratégia 2013-ban először határozta meg a globális kibertér részeként a magyar kibertér gazdasági és társadalmi életben betöltött meghatározó szerepét.

2.3.2. Az állami és önkormányzati szervek elektronikus információbiztonsága

A Nemzeti Kiberbiztonsági Stratégiában elfogadott célok és elvek mentén született meg az Ibtv., amiben a közigazgatás minden szintje számára fogalmazódtak meg új feladatok. Egy 2014-ben lefolytatott kutatás [31] során megkérdezett szakértők többsége szerint a kialakított szabályozás az információbiztonság területén, nemzetközi szinten is élenjáró. Véleményük szerint egyes esetekben még meg is előzi a szükségleteket, mivel előrébb tart a szabályozásban, mint ahogyan ezt az informatikai infrastruktúra fejlettsége indokolná.

A törvény 2. § (1) pontja szerint az Ibtv. előírásait az alábbi szervezetekre kell alkalmazni:

„a) a központi államigazgatási szervekre, a Kormány és a kormánybizottságok kivételével,

b) a Köztársasági Elnöki Hivatalra,

c) az Országgyűlés Hivatalára,

d) az Alkotmánybíróság Hivatalára,

e) az Országos Bírósági Hivatalra és a bíróságokra,

f) az ügyészségekre,

g) az Alapvető Jogok Biztosának Hivatalára,

h) az Állami Számvevőszékre,

i) a Magyar Nemzeti Bankra,

j) a fővárosi és megyei kormányhivatalokra,

k) a helyi és a nemzetiségi önkormányzatok képviselő-testületének hivatalaira, a hatósági igazgatási társulásokra,

l) a Magyar Honvédségre." [59]

A törvény és annak nyomán megszületett 26/2013. (X. 21.) KIM [60] rendelet alapján e szervezeti kör munkatársai részére szükséges – három szinten – információbiztonsági képzést biztosítani: felelős vezető, résztvevő és információbiztonsági (továbbiakban IB) felelős.

Az információbiztonság megvalósítása érdekében szükséges multidiszciplináris szemléletű képzési programok indítására a közszféra keretein belül a Nemzeti Közszolgálati Egyetem (NKE) tett kísérletet. Az Ibtv. konkrétan megfogalmaz képzési követelményeket a törvény hatálya alá tartozó szervezetek vezetőivel és az elektronikus információs rendszerek biztonságáért felelős személyekkel szemben (1. melléklet).

A képzési keretek adottak, így – elméletileg – az állam és az önkormányzatok számára hosszú távon biztosítottá válik az információ biztonságát támogatni képes szakember.

Az NKE-n 2014-ben lefolytatott kutatás szakértői megkérdezéssel vizsgálta az IB felelősök képzésével szembeni elvárásokat. Megállapításuk szerint az információbiztonság területén a közigazgatásban dolgozókat rendkívül heterogén szintű tudás jellemzi. Az IB felelősök kinevezésekor volt, hogy jogász, volt, hogy a műszaki területért felelős tisztviselőt választottak. A szakértők az alábbi elvárásokat fogalmazták meg IB felelősök képzésével kapcsolatosan:

- a képzés tudatosítsa a tanulóval a feladattal járó felelősség tekintetében;
- legyen gyakorlatorientáltabb mint egy, a szervezetek vezetői számára összeállított tananyag;
- ne hagyományos képzési módszerek kerüljenek alkalmazásra, hanem esettanulmányok – feldolgozás, támadások – incidensek szimulálása, beavatkozási-cselekvési terv, folyamatábra készítése stb.
- legyen rendszeres továbbképzés és
- jöjjön létre egy tudásmegosztó, tudásmenedzsment rendszer, szakmai fórum [31 p. 63–65.].

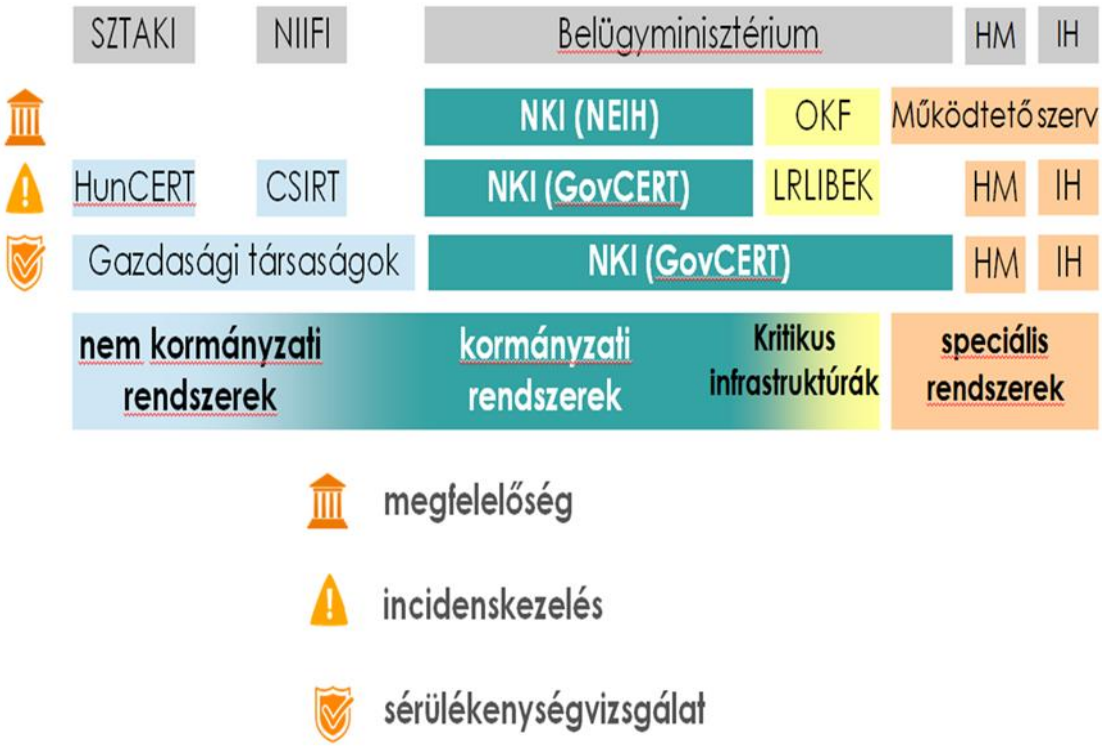
2.3.3. Szervezeti keretek

A hazánkban működő kiberbiztonsági szabályozás és intézményrendszer nem komplexen közelítette meg a szervezeti felépítés kérdését, hanem első körben az állami és önkormányzati rendszerekre, illetve a létfontosságú infrastruktúrákra vonatkozóan fogalmazta meg a szabályokat és kötelezettségeket, így a szakosított intézményrendszer is csak ezen a területen jött létre. Az állami és önkormányzati szervezetekben a változások hamarabb mennek végbe, ha erre jogszabály is kötelez (persze szerencsés, ha egyben útmutatást is ad a megvalósításhoz). A kérdéskör által megkívánt komplexitás, multidiszciplináris megközelítés nem elég hangsúlyos a szabályozásban, így a horizontális megközelítés sok esetben elmaradt. Az Ibtv. hatálya alá tartozó állami és önkormányzati szervezetek általános biztonsági eseményeinek vonatkozásában kezelési hatáskörrel a Kormányzati

Eseménykezelő Központ (GovCERT), hatósági jogkörrel pedig a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) rendelkezik. Mindkét szervezet működtetésére a Nemzetbiztonsági Szakszolgálat került kijelölésre.

A Nemzetbiztonsági Szakszolgálaton belül megalakításra került a Nemzeti Kibervédelmi Intézet (NKI). Az NKI rendelkezésre álló kapacitásainak minőségi és mennyiségi fejlesztését indokolja az elektronikus információbiztonsági felügyeleti és támogatási feladatok iránti igények növekedése.

A honvédelmi igazgatás információs rendszerei vonatkozásában a katonai nemzetbiztonsági tevékenységet ellátó szervezet saját rendszerei tekintetében önállóan látja el az incidenskezelési és felügyeleti feladatokat. *Az európai vagy nemzeti létfontosságú rendszerelemmé a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény* [52] alapján kijelölt rendszerelemek elektronikus információs rendszerei esetében az Ibtv. szerinti hatósági feladatokat a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság (BM OKF) látja el. *A kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól szóló 185/2015. (VII. 13.) Korm. rendelet* [61] alapján a létfontosságú létesítmény, rendszer elektronikus információs rendszereit érintő biztonsági események és fenyegetések kezelését és az egyéb információbiztonsági funkciókat a BM OKF Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ (LRLIBEK) látja el.



1. ábra

Információbiztonsági funkciók és szervezetek [32]

Az elektronikus információs rendszerek sérülékenységvizsgálatát a jelenlegi szabályozás szerint a Nemzetbiztonsági Szakszolgálat, az Információs Hivatal és a Katonai Nemzetbiztonsági Szolgálat (a saját rendszerei tekintetében), valamint telephely biztonsági tanúsítvánnyal, továbbá a feladat ellátásához szükséges – jogszabályban meghatározott – szakértelemmel és infrastrukturális feltételekkel rendelkező gazdasági társaságok végezhetik.

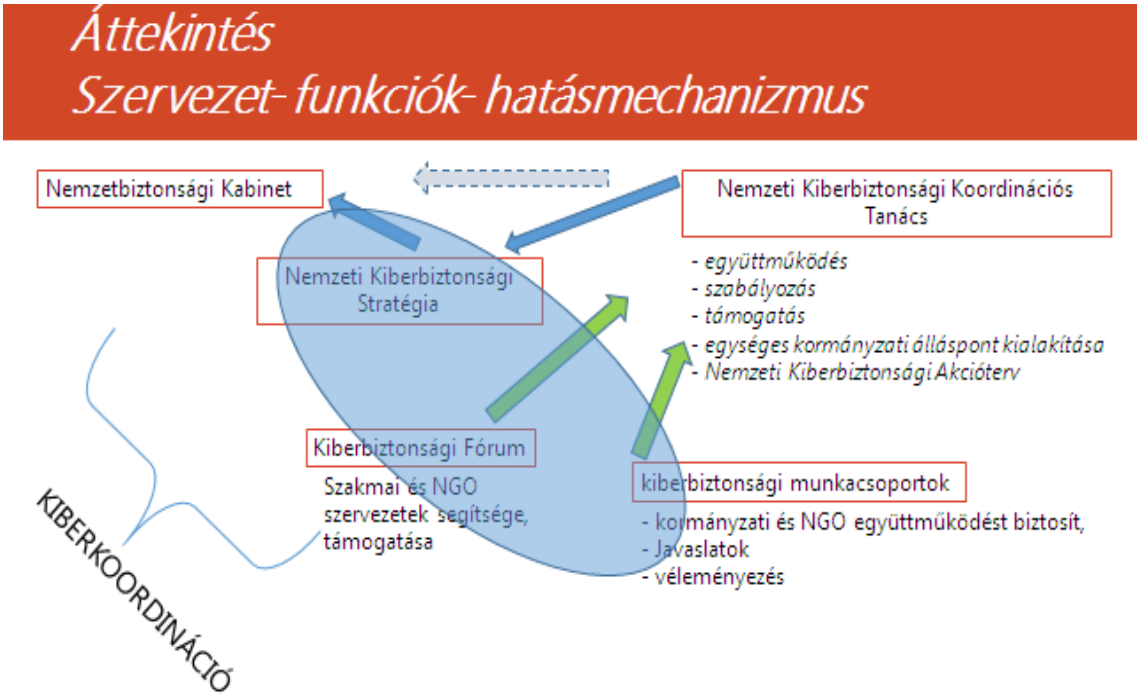
Az Ibtv. hatálya alá nem tartozó elektronikus információs rendszerek, hírközlési szolgáltatók tekintetében az MTA–SZTAKI működtet információbiztonsági eseménykezelő szervezetet (HunCERT). A Nemzeti Információs Infrastruktúra Fejlesztési Program (NIIF) megvalósítása keretében a Kormányzati Informatikai Fejlesztési Ügynökség működtet számítógépes biztonsági eseménykezelő szervezetet (NIIF CSIRT). Az NIIF CSIRT a magyar köznevelés, felsőoktatás, kutatás és közgyűjtemények szolgáltatójához, az NIIF-hez tartozó IT biztonsági és biztonsági eseménykezelő csoport. A csoport célja segíteni a számítógépes és hálózati biztonsági események kezelését és koordinációját minden olyan esetben, amelyben a NIIF legalább egy tagintézménye érintett. Az NIIF CSIRT munkacsoportja ezen kívül fontos, biztonsággal, megelőzéssel, illetve elhárítással kapcsolatos információkat is továbbít az NIIF tagintézményeinek.

2.3.4. Kormányzati kiberkoordináció

A koordináció fogalma kapcsán két különböző tudományos megközelítésről beszélhetünk: amikor a koordinációt mint a folyamatok összehangolását, és a koordinációt mint végállapotot közelítjük meg. A folyamatok összehangolására akkor van szükség, ha az adott feladat elvégzéséhez sok szereplő összehangolt tevékenységére van szükség. Tehát a közszféra koordinációjára akkor van szükség, ha egy meghatározott cél érdekében több közpolitikai szereplő együttműködésben cselekszik. Figyelmet kell szentelni a koordinációs mechanizmusoknak annak érdekében, hogy létrejöjjenek olyan együttműködési formációk, amelyek képesek koordinációs hatást kifejteni. A végállapotként értelmezett koordináció célja egy olyan állapot létrehozása, ahol a rendszerben a felesleges átfedések minimálisan vannak jelen. A közigazgatásban ez a hatáskörök és illetékességi területek megfelelő meghatározásával érhető el. A közszféra koordinációjában – a folyamatos változást is figyelembe véve – a folyamatelvű megközelítés a mérvadó, de tekintettel kell lenni a végállapot-központú megközelítésre is. A közigazgatási koordináció akkor valósul meg, ha egy adott területen, a célok elérése több egymástól kölcsönösen függő szervezet erőfeszítése szükséges és ezen erőfeszítések hatására csökkennek a redundanciák és hatékonyabbá válik a feladatvégzés. A kereteket a kialakított koordinációs mechanizmus biztosítja és különböző koordinációs eszközökkel kerül végrehajtásra [33 pp.20–21.].

Az információbiztonsági kérdések önmagukban komplexek és szerteágazóak, mivel minden területet érintenek. Ezért ennek a feladatnak az összehangolására, a kormányzati koordináció biztosítására az Ibtv. [62 III/11.] rendelkezése és a 484/2013-as kormányrendelet előírásainak megfelelően létrehozásra került a Nemzeti Kiberbiztonsági Koordinációs Tanács (a továbbiakban: Tanács) [61] mint a Kormány javaslattevő, véleményező szerve.

A Tanács tevékenységét az e-közigazgatásért felelős miniszter által delegált kiberkoordinátor, valamint a nem kormányzati szereplőkkel való együttműködésnek keretet biztosító kiberbiztonsági munkacsoportok és a Nemzeti Kiberbiztonsági Fórum (a továbbiakban: Fórum) támogatja.



2. ábra

A kormányzati kiberkoordináció szervezetei [34]

A kiberkoordináció célja, hogy az információbiztonság kérdéseinek mint a kritikus infrastruktúrák e horizontális elemének kormányzati szinten megfelelő hangsúlyt adjon. Feladata, hogy interminiszteriális szinten biztosítsa a koordinációt, működtesse a koordinációs mechanizmust és kidolgozza a koordinációs eszközöket.

A kormányzati koordináció azért szükséges, hogy hatékony, redundanciamentes, szakmailag megalapozott összehangolt kormányzati kibervédelmet valósítson meg. A szakmai területeken belül létrejöttek a minisztériumokban a kiberbiztonsági munkacsoportok, azonban ezek működését az integrált működés hiánya és a szétaprózottság jellemzi, továbbá nem terjed ki a teljes igazgatási rendszerre sem.

Ahogyan 2. ábrán láthatjuk, továbbá ahogy a neve is mutatja, a kordináció csak kormányzati szinten került létrehozásra. A koordinációba az önkormányzatok sem horizontálisan – az államigazgatás alrendszere – sem vertikálisan – a területi és települési kormányzati szereplők – nem kerültek bevonásra. Az önkormányzatok nem partnerként, hanem csak kötelezettként jelennek meg a szabályozásban. A helyhatóságok speciális körülményei, nehézségei, lehetőségei és elvárásai nem kerültek figyelembevételre. A nemzetközi és a hazai tapasztalat is azt mutatja, hogy az ilyen esetekben, amikor országos kötelezettség teljesítéséről van szó, de mind a központi közigazgatásból, mind az önkormányzati körből nagyszámú résztvevő érintett a végrehajtásban, akkor e sokszereplős

együttműködés nehézkes. További tapasztalat, hogy ezekben az esetekben a horizontális és vertikális információáramlás is részleges.

2.3.5. Önkormányzati koordináció

A helyi közszolgáltatások elérhetősége és működésének színvonala egyszerre függ a központi kormányzati szakpolitikai irányítástól és a szolgáltatások helyi igényekhez, lehetőségekhez történő illeszkedésétől. A keretek, standardok és az ajánlások a kormányzati szintneken, míg a helyi szinthez való illesztés biztosítása elsősorban a helyi önkormányzatok felkészültségén múlik, és a szubszidiaritás elve alapján az alacsonyabb szervezési szinten hatékonyabban is valósítható meg. Az információbiztonság kérdéskörében sem kerülhető meg egy valós koordinációs mechanizmus kialakítása a központi közigazgatás és az önkormányzati szektor között.

Az ivóvízminőség-javító programok (IMJP) végrehajtása során felmerült nehézségek kapcsán kialakított koordinációs mechanizmus és alkalmazott eszközök ugyanezen kört érintették, ezért az alkalmas koordinációs minta lehet. Az IMJP végrehajtása 2001-ben indult és 2011 nyarán a vizsgálatok azt mutatták, hogy az emberi fogyasztásra szánt víz minőségéről szóló 1998. november 3-i 98/83/EK tanácsi irányelv előírásainak [63] az érintett 365 településből még 312 esetében nem felelt meg az ivóvíz minősége az irányelv előírásainak.

A helyzet speciális volt, hiszen 2004-ben a csatlakozási szerződésben vállalt (halasztással érintett) kötelezettséget az ország vállalta, azonban a kötelezettség végrehajtásáért az önkormányzatok voltak felelősek. A vizsgálat azt mutatta, hogy az országos szint és a helyi önkormányzati szint közötti kommunikáció jórészt csak szabályozási dokumentumokon, hatósági aktusokon keresztül valósult meg. 2012-ben jól látszott, hogy a kötelezettségszegési eljárás elkerülése érdekében szükséges a kormányzati beavatkozás a központi kormányzati szint és a helyi önkormányzati szint közötti együttműködés, koordináció és információáramlás biztosítása érdekében. A feladat végrehajtására a kormányzat létrehozta a Belügyminisztérium mint önkormányzatokért felelős minisztérium keretei között a feladatért felelős szervezeti egységet: az Önkormányzati Koordinációs Irodát (ÖKI). Az ÖKI feladatai közé tartozott az önkormányzati ivóvízminőség-javító projektek figyelemmel kísérése, a problémák feltárása, becsatornázása, megoldási javaslatok megfogalmazása, kockázatok követése, értékelése, kommunikáció és kooperáció javítása az érintettek között a derogációs kötelezettséggel érintett önkormányzati ivóvízminőség-javító projektek eredményes megvalósítása érdekében. A feladat megvalósítására kialakított új típusú kormányzati ügykezelési módszer középpontjában a közvetítés és a koordináció állt. Pilot jelleggel kialakításra és működtetésre, tesztelésre került a horizontális és vertikális együttműködési és koordinációs mechanizmus. Az alkalmazott koordinációs eszközök támogatták az információáramlást, a jó gyakorlatok terjesztését a központi és helyi megvalósítók között. A rendszeres adatszolgáltatás, a monitoring látogatások és személyes kapcsolattartás lehetővé tették, hogy a felmerülő nehézségek többsége még a kockázati szinten kezelhetőkké váljanak. A kormányzati beavatkozásokat értékelő hatásvizsgálat alapján a sikerességet elősegítő eszközök a következők voltak: partnerség, közös platform, azonnali reakciók, az ügyek közös képviselete, hatékony információ- és tapasztalatcsere.

Az egészséges ivóvíz biztosítása érdekében kialakított koordinációs mechanizmus és alkalmazott koordinációs eszközök egyfajta, esettanulmányként, jó gyakorlatként szolgálhatnak a kiberkoordináció esetében. Az országos érdek és elvárás teljesítéséhez az önkormányzati alrendszer megfelelése elengedhetetlen, aminek a tagjai jelentős számossággal bírnak. Eközben a tapasztalatok azt mutatják, hogy a jelentős számú központi kormányzati aktorok között sem jött még létre olyan koordinált állapot, amit integrált együttműködés, zökkenőmentes információcsere és információáramlás jellemezne. Országos érdekében szükség van a folyamatok összehangolására, hogy a feladat elvégzéséhez a sok szint és sok szereplő tevékenysége összehangolásra kerüljön.

2.4. Digitális állam

Kimondhatjuk, hogy keresleti oldalról a mennyiségi és minőségi szempontból egyaránt egyre magasabb szintű felhasználói igények, kínálati oldalról pedig a folyamatos technológiai fejlődés és innováció eredményeként Magyarországon is kialakult a digitális ökoszisztéma,[12] ami már jelenleg is felhasználók millióit és eszközök tízmillióit köti össze egyre nagyobb kapacitású hálózatokkal és egyre összetettebb elektronikus szolgáltatásokkal.

Az infokommunikációs szektor mind gazdasági, mind társadalmi értelemben jelentős szerepet játszik Magyarországon. Az IKT mint ipar a magyar GDP mintegy 12%-át adja, az ebben az iparágban foglalkoztatottak száma pedig az OECD országainak többségével összevetve is kiemelkedően magas. Az ágazat további lendületes fejlődését fékező tényezők lebontását célzó, jól átgondolt és precízen megvalósított lépések nélkül Magyarország nem lesz képes kiaknázni az IKT gazdasági szektorában rejlő potenciált, így félő, hogy lemarad az európai országok közötti már ma is rendkívül intenzív versenyben.

A Nemzeti Infokommunikációs Stratégia azzal a céllal került megalkotásra, hogy koherens képet adjon a magyar információs társadalom jelenlegi viszonyairól, majd ez alapján a 2014–2020-as uniós tervezési ciklussal egybeeső időtávra meghatározza az infokommunikációs területre vonatkozó fejlesztési irányokat, közpolitikai, szabályozási és támogatási teendőket, továbbá számba vegye az ezek megvalósításához szükséges eszközöket és erőforrásokat.

[12] Digitális ökoszisztéma alatt a NIS vonatkozásában egy olyan elosztó, alkalmazkodó, nyílt társadalmi-technikai rendszert értünk, amelyet az önszerveződés, skálán való mérhetőség és a fenntarthatóság jellemez, illetve amelyben felhasználók (lakosság, vállalkozások, kormányzat) milliói és eszközök tízmilliói kommunikálnak egymással, tartalmak és alkalmazások tízezreit igénybe véve a nagy adatforgalmat biztosító szélessávú hálózatok segítségével.

3. ábra

A Nemzeti Infokommunikációs Stratégia pillérszerkezete [35 p.6.]

A kiemelt célok közt szerepel egy interoperabilitás megvalósítását támogató szabályozási környezet létrejötte annak érdekében, hogy 2020-ra az adatbázisok szintjén megvalósuljon a jelentősebb állami nyilvántartások közötti interoperabilitás. A digitális állam fejlődésének alapfeltétele az elektronikus közigazgatás biztosításához szükséges kiszámítható és stabil infrastrukturális és informatikai háttér, a közigazgatás belső folyamatainak átgondolt és az interoperabilitás elvét követő elektronizálása, illetve a lakosságnak és a vállalkozásoknak nyújtott fejlett e-közigazgatási szolgáltatások kialakítása és működtetése. Mind a közigazgatás megbízható és stabil működése, mind az elektronikus közigazgatási szolgáltatások, illetve elektronikus közszolgáltatások biztosítása szempontjából kulcsfontosságú, hogy a kormányzati elektronikus információs rendszerek biztonságosan, interoperábilis módon és valamennyi alrendszert, intézményt és felhasználói kört kiszolgálva működjenek. Ennek feltétele egy olyan kormányzati IT-háttér szisztematikus felépítése, ami mind infrastrukturális, mind üzemeltetési, mind pedig fejlesztési szempontból képes a hagyományos IT-szolgáltatások és a várhatóan egyre több területen elterjedő felhőalapú megoldások, illetve ASP és SaaS szolgáltatások stabil és megbízható biztosítására.

Az elektronikus kormányzati szolgáltatások esetében kiemelten fontos, hogy a közigazgatás oldalán maximálisan garantálható legyen a hálózatok, rendszerek, folyamatok és felhasználói adatok biztonsága. Az e-közigazgatási szolgáltatások egyik sikerkritériuma épp annak a biztosítása, hogy az állampolgárok és a vállalkozások biztosak lehessenek a rendszerek folyamatosan működőképesében, a szolgáltatások elérhetőségében, és adataik illetéktelenek számára való hozzáférhetetlenségében.

Az Ibtv. és végrehajtási rendeletei megfelelő alapot nyújtanak az állami és önkormányzati szervek kibervédelmi és információbiztonsági tevékenységéhez. A technika fejlődésével párhuzamosan az állami és önkormányzati szerveknek lépést kell tartaniuk az információbiztonság folyamatosan változó követelményeivel.

Az ISA (Interoperability Solutions for European Public Administrations Work Programme) kulcsfaktorként határozta meg az interoperabilitás biztosítása érdekében a közös keretrendszer

létrehozását, aminek elérése érdekében 2015 áprilisában megalkotásra került a hazai *E-közigazgatás keretrendszer koncepció* [36]. A keretrendszer kialakítását azonban alapvetően nem technológiai kérdésként kell kezelni, hiszen ma már technológiai oldalról több lehetséges megközelítéssel is biztosítható a közigazgatási feladatok egységes szemléletű ellátása. A kérdést abból a szempontból kell rendezni, hogy az új feltételrendszerben milyen módon lehet érvényre juttatni a közszolgáltatások alapértékeit úgy, hogy a megoldás

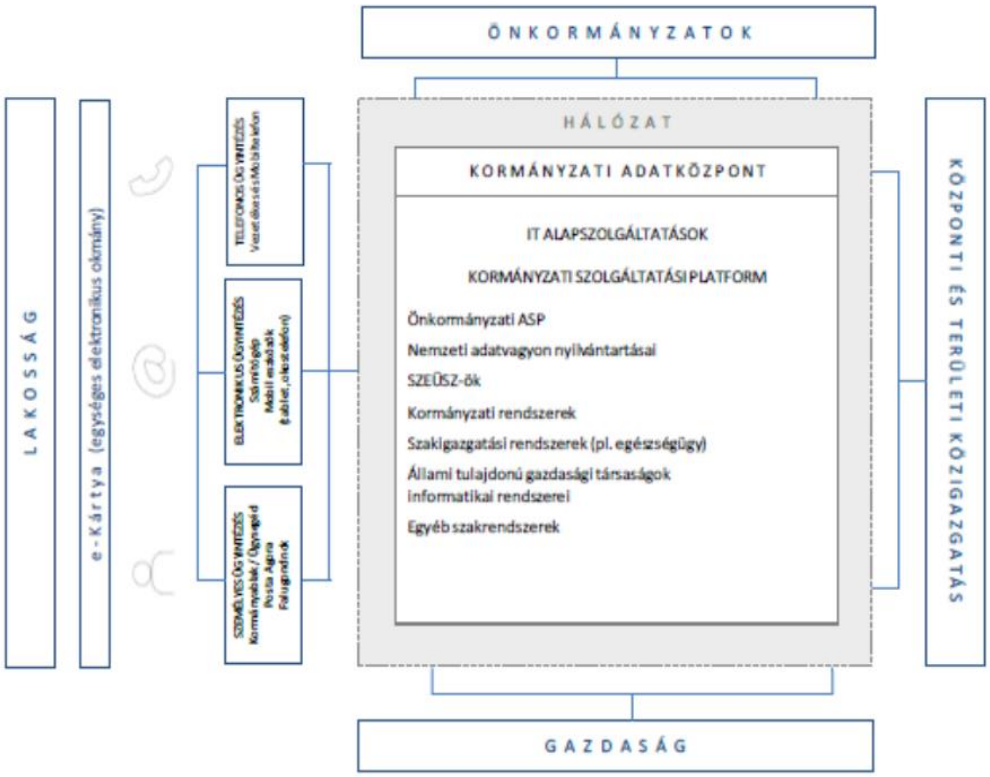
- maximálisan szolgálja a folyamatok költséghatékonyságát, gyorsaságát,
- lehetővé tegye a meglévő infrastruktúra lehető legjobb kihasználását,
- kezelhető követelményeket írjon elő a változásmenedzsment felé,
- az ügyfelek lehetőségeivel és igényeivel találkozó, az adatvédelem és az adatbiztonság követelményeit alapként kielégítő megoldásokat biztosítson.

A platform kialakítása során fontos figyelembe venni az európai tendenciákat, amelyek esetében az elektronikus ügyintézés infrastruktúráját egyre inkább egységesen, egységes megoldások (de természetesen szigorúan elkülönített, célhoz kötött adatbázisok, eljárások) mentén használják, ezáltal létrehozva azt a kritikus szolgáltatástömeget, amelyért már az állampolgároknak is érdemes megtanulni új eljárásokat, szabályokat, továbbá beszerezni újabb eszközöket.

A NIS négy digitális alappillére (infrastruktúra, kompetencia, gazdaság, állam) mentén történő digitális fejlesztés központi eleme egy

- minden szereplő számára egységes logikai keretrendszerben kiépült,
- hálózati és kormányzati adatközponti infrastruktúrát,
- szabványosított kapcsolórendszereken keresztül elérhető csatlakozott szakrendszereket,
- szabályozott elektronikus szolgáltatások igénybevételét biztosító kormányzati szolgáltatási platform.

Az infokommunikációt is magába foglaló elektronikus közigazgatás elemeit és összefüggéseit az alábbi ábra mutatja be:



4. ábra

Kormányzati szolgáltatási platform [36 p.17.]

Egyértelmű törekvésként azonosítható, hogy az uniós irányelvekben, stratégiákban kitűzött célokat Magyarország is teljesítse, ugyanakkor az is látható, hogy többségében csak koncepció, stratégia és tervek szintjén teljesültek az elvárások. Az elkövetkezendő évek programjait és eredményeinek teljesülését – azok vizsgálatát – követően lehet megállapítani, hogy mi teljesült hazánkban az interoperabilitás területén. Az eredmény kritikus tényező, hiszen az infokommunikációs interoperabilitás hatása az ország versenyképességére vonatkozóan nem megkérdőjelezhető.

A koncepcióban, elsősorban az interoperabilitás magasabb szintjein – sajnálatosan – több hiány is azonosításra került. Hiányok mutatkoznak szemantikai szinteken, és jelentős elmaradások szervezeti, jogi és politikai területeken.

A célok elérése érdekében van még néhány konkrét tennivaló, ami a hazai fejlesztők és érintettek előtt nehézségként, kihívásként vagy feladatként áll a kitűzött 2020-as dátumig:

Az ügyfélközpontú szemlélet hangoztatása gyakran csak hívó szónak maradt meg, de a jogi szabályozásban tett előrelépések ellenére (például a Ket. előírta [64], hogy az ügyféltől nem kérhető olyan adat igazolása, ami más hatóság nyilvántartásában fellelhető) érdemi előrelépés általánosságban nem történt. Kérdés, hogy az Ákr. [65] által elvárt egyablakos eljárás hoz-e érdemi előrelépést.

A fentiek okán az elektronikus közigazgatás kialakításának egyik elengedhetetlen feltétele és óriási feladata az állami adatbázisok felmérése és együttműködési képességének megteremtése, az adatok keletkezéséért elsődlegesen felelős adatgazdák feladat- és hatáskörének definiálása. Ennek jogi kereteit az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól szóló 2013. évi CCXX. törvény [66] fektette le. A következő időszak feladata a tényleges interoperabilitás megvalósítása.

Az interoperabilitási célkitűzések megvalósítása, a különböző rendszerek és szolgáltatások együttműködési képességének erősítése is kulcskérdés az elektronikus közigazgatási szolgáltatások fejlesztése, kiterjesztése szempontjából.

A NIS előírásainak megfelelően szükséges a következő években az elektronikus szolgáltatások infrastrukturális hátterének (informatikai, back-office) biztosítása, az e-közigazgatási szolgáltatások fejlesztése és megfelelő szintű összekapcsolása a lehető legteljesebb interoperabilitás mellett.

A szervezeti interoperabilitás eléréséhez pedig szükséges a szervezetek (és munkatársaik, vezetőik) kompetenciafejlesztése, a tudatosítás. Az IKT már szerves része a szervezeti hálózatnak, hatékony és eredményes működés ma már elképzelhetetlen ezek nélkül az eszközök, rendszerek és hálózatok nélkül. Ugyanakkor a hozzá kapcsolódó információbiztonsági kérdések, a kiberbiztonsági tudatosság még nem vált a szervezeti kultúra megkerülhetetlen részévé.

A GDPR és az információsszabadság

Az Alaptörvény VI. cikkének 2. bekezdése rögzíti a személyes adatok védelméhez és a közérdekű adatok megismeréséhez kapcsolódó jogokat.

Ahogyan az uniós szabályozást bemutató fejezetben már láthattuk, az újonnan kialakuló egységes európai szabályozás második pillére az Európai Unió általános adatvédelmi rendelete, a GDPR. A korábbi adatvédelmi irányelv nem tudta elérni azon célját, hogy „a tagállami szabályozásokat közös nevezőre hozza, így mára 28 különféle adatvédelmi szabályozás jött létre az Unión belül. Ez azzal járt, hogy a felhasználók egészen más védelemben részesülnek az egyik tagállamban, mint adatfeldolgozás helyén, mint egy másik országban. Többek között ezt a helyzetet hivatott orvosolni az új szabályozás, amelyet egy hosszas, mintegy négy éves előkészítő munka előzött meg. A Bizottság már 2012-ben útjára indította a reformkezdeményezést, amely az EU főszervei között létrejött kompromisszumot követően nyerte el végleges formáját. A rendelet legnagyobb jelentősége ezért abban rejlik, hogy az Unió igen nagy lépést tehet a digitális egységes piac kialakulása felé.” [37 p. 263.]

Összegzés

Az Európai Parlament és a Tanács közös állásfoglalásában a kiberbiztonsági kérdések fontosságát hangsúlyozta és jelölt ki cselekvési területeket. Ezek közé tartozik az ENISA mandátumának kiterjesztése és megerősítése, a kiberbiztonsági termékek standardizálása, a tagállamok kiberbiztonsági képességének növelése, a tagállamok közötti együttműködés hatékonyságának javítása. A resiliencia jelentősen növelhető a felkészültség javításával, a tudatosság elérése pedig oktatással. Fontos szempont, hogy nem elégséges az IT szakemberek képzése, hanem az

információbiztonsági, kiberbiztonsági kérdéseknek be kell épülniük más tudományágak oktatási anyagába is. Ezen túl a tagállamoknak tudatosságnövelő kampányok keretében kell felhívniuk a szervezetek és az állampolgárok figyelemét a kiberkockázatok széles körére.

Az EU a szabályozásában a teljeskörűségre törekszik. A tagállamokban jelenleg a 2016-os NIS-irányelv saját jogrendükbe való illesztése zajlik. A Bizottság fő célként a kiberbiztonsági képességek és együttműködés növelését, az EU globális szerepének erősítését, valamint a tagállami politikák egységesítését tűzte ki.

A NIS irányelve három pillérre épül: a tagállami készenlét biztosítása, a tagállamok közötti együttműködés erősítése és a biztonság kultúrájának megteremtése. Az uniós célok teljesítése érdekében minden tagállam elfogad egy a hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiát, amiben meghatározza a célokat, a végrehajtási keretrendszert és azok szereplőit a hozzájuk rendelt felelősség meghatározásával, továbbá a felkészültség biztosításához szükséges intézkedéseket, a kapcsolódó oktatási, tájékoztatási és képzési programokat és kutatási fejlesztési terveket, végül a kockázatkezelést.

Az egyes nemzetek kiberbiztonsági stratégiáinak összehasonlítása kiváló alapot nyújt a jó gyakorlatok megismerésére (osztrák, lengyel és a brit stratégiák). Ilyen jó gyakorlatok a komplex megközelítés intézményrendszerei, a különböző kiberbiztonsági folyamatok menedzsmentje, módszertana, illetve a tudatosítás, a képzés programjai.

A kiberbiztonság hazai szabályozási rendszere magyar és külföldi szakértők szerint is élenjáró. Továbbá jelenleg is zajlik a NIS irányelvének és a hazai elvárásoknak megfelelő új kiberbiztonsági stratégia kidolgozása. Az Ibtv. pedig pontos elvárásokat fogalmaz meg mind az állami, mind az önkormányzati szereplők részére. A törvény rendelkezik a kormányzati kiberkoordinációról is. A kormányzati kiberkordinációba azonban az önkormányzatok nem kerültek bekapcsolásra. A kormányzat és az önkormányzatok közötti koordináció és együttműködés az adminisztratív szabályozási keretekre és a kormányzati szervek hatósági eljárására korlátozódik. A feladat jellege, az érintettek nagy száma és többszintű kormányzás keretein belül az eltérő szintek miatt elengedhetetlen az önkormányzatokat is bevonó koordinációs mechanizmus kialakítása és működtetése. Ezen túl az Ibtv. által adott feladatok kiterjednek a rendszerek biztonsági osztályba sorolására és az érintett szervezetek információbiztonsági felelősének képzési kötelezettségére is. Egy 2014-es kutatás már akkor jelezte, hogy ennek a képzésnek gyakorlatorientáltan kell megvalósulnia, az egyes érintett szervezetek funkciójának, szükségleteinek figyelembevételével és az IB felelősöktől elvártaknak megfelelően.

A kiberbiztonsági szabályozás és intézményrendszer első körben a kritikus infrastruktúrákra, az állami és önkormányzati körre fogalmazta meg a szabályokat és kötelezettségeket, így a megközelítés nem alkalmazkodott a komplexitás elvárásához, továbbá elsősorban hatósági szempontból volt kidolgozott. A 2014–2020-as időszakra vonatkozó *Nemzeti Infokommunikációs Stratégia* viszont négyes pillérszerkezetével lefedi a teljes spektrumot.

3. HELYI IGAZGATÁS, ÖNKORMÁNYZATOK

A harmadik fejezet az önkormányzatok kormányzati rendszerben betöltött helyét, mutatja be az önkormányzatok feladatait és az önkormányzati hivatalok típusait. Az értekezés szempontjából kiemelten fontos részként kerül ebben a részben tárgyalásra az elektronikus információs rendszerekhez kapcsolódó képzések jelenlegi helyzete. A fejezet másik jelentős elem az önkormányzatok megfelelése (illetve nem megfelelése) az Ibtv. és az Infotv. elvárásainak.

3.1. Az önkormányzati rendszer elhelyezkedése a kormányzati rendszerben

„Ha elfogadjuk továbbá azt a közkeletű definíciót, hogy az állam egy adott földrajzi terület feletti legfőbb hatalommal bíró politikai egyesülés, akkor a helyi önkormányzatot definiálhatjuk a közhatalom demokratikus decentralizációját megtestesítő helyi közhatalom-gyakorlás szervezeti kereteként. A helyi önkormányzat az állam, mint szuverén hatalmának vertikális megosztása, amely a horizontális hatalommegosztásból – törvényhozó, végrehajtó, igazságszolgáltatási – következő három hatalmi ág mellett egy további negyedik hatalmi ágként is felfogható.

A helyi önkormányzat tehát az ún. infraszuverén kormányzati szinten elhelyezkedő autonómia. /Az infraszuverén kormányzati szinten nem csak önkormányzatok, hanem kormányzati – állami – szervek is működnek, működhetnek./ Az önkormányzatok sajátossága és ez különbözteti meg a kormányzati szervek területi szerveitől (az államigazgatástól), hogy képviseleti jellegűek (választással jönnek létre) és komplexek, hiszen saját döntéseiket saját maguk hajtják végre. Az infraszuverén szint az államok többségében egyébként jellemzően nem egy, hanem két-három szintet is jelenthet. Ezt a területi tagoltságot hívjuk az állam területi beosztásának. Hazánkban ilyen szint a megye, a járás és a település szintje.” [38 p. 12.]

3.1.1. Önkormányzás, önkormányzatiság

„Az önkormányzás fogalma a gyakorlatban azt jelenti, hogy az adott helyi közösség függetlenül működik, saját ügyeiben önálló döntési jogosultsággal rendelkezik. A helyi önkormányzatok esetében a fent említetteken túl ez abban nyilvánul meg, hogy a kormány csak ellenőrzési (felügyeleti) jogkört gyakorolhat felettük. Helyi közügyet csak kivételesen és csak törvény utalhat más szervezet feladat és hatáskörébe.” [39]

A helyi önkormányzatok a kormánynak nincsenek alárendelve, csak az Országgyűlés állapíthat meg rájuk nézve kötelező szabályt. Az önkormányzatok az államszervezet integráns, de annak nem alárendelt részei. Az állam azáltal szabályozza az önkormányzatok szervezetét, hogy lefekteti a választás szabályait, de az állam meg is szüntetheti azt azzal, hogy az alaptörvény-ellenesen működő képviselő-testületet feloszlatja. A közfeladatok, közszolgáltatások nagy része kötelező feladat, amit szintén az állam határoz meg. A feladatellátáshoz szükséges pénzeszközöket, illetve a hozzájutás lehetőségét is az állam biztosítja.

A helyi önkormányzatok az állami szervezetrendszer részei, így szerepük meghatározó a közfeladatok ellátásában.

Az Alaptörvény [67] 31. cikke a helyi önkormányzatok működésének kettős célját nevesíti: a helyi közügyek intézése és a helyi közhatalom gyakorlása. Az Alaptörvény szerint a helyhatóságok elsődleges feladatköre a helyi közügyek intézése. Magyarország helyi önkormányzatairól szóló 2011. évi CLXXXIX. törvény (Mötv. [68]) 4. §-a szerint a helyi közügyek alapvetően a lakosság közszolgáltatásokkal való ellátásához, valamint a helyi önkormányzás és a lakossággal való együttműködés szervezeti, személyi és anyagi feltételeinek megteremtéséhez kapcsolódnak.

A modern társadalom kihívásai paradigmaváltást kívánnak meg a helyi irányítás terén is. Hiszen annak érdekében, hogy az önkormányzat a közszolgáltatásokat hatékonyan tudja megszervezni és ellátni, e mellett pedig fejlesztési célokra is tudjon összpontosítani merőben új irányítási stílusra, gazdaság-, és társadalom-szervezésre, technológiaalkalmazási képességre van szükség.

3.2. Önkormányzati feladatok és hivatali szerkezet

A teljes közjogi rendszer átfogó megújításának, a közigazgatási rendszer átalakításának, fejlesztésének meghatározó elemeként fogadta el az Országgyűlés az Mötv.-t. Az önkormányzati reform egy költséghatékony feladatorientált önkormányzati rendszer kiépítését célozta. Egyúttal újradefiniálta az állam és a helyi önkormányzatok közötti munkamegosztást. [40 p. 29.]

3.2.1. Önkormányzati feladatok

A helyhatóságok által ellátandó helyi közfeladatokat elsődlegesen a jogalkotó telepíti a helyhatóságokra, többnyire kötelező jelleggel. Ennek szükségességét az alapozza meg, hogy az állampolgárok számára biztosítottak legyenek az alapvető közszolgáltatások.

„Mindezeket figyelembe véve helyben intézendő közügynek az minősül, melyet a törvényalkotó határozott meg ekként (kötelező önkormányzati feladatok), továbbá az, melyet a helyi önkormányzat képviselő-testülete önként felvállalt (fakultatív önkormányzati feladatok). Az Alaptörvény 34. cikk (1) bekezdése a jogforrási szintet is meghatározza, amikor rögzíti, hogy helyi önkormányzat számára kötelező feladat- és hatáskört kizárólag törvény állapíthat meg. E cikk rendelkezik a kötelező feladat telepítésének másik fontos követelményéről, mely szerint a helyi önkormányzat kötelező feladat- és hatásköreinek ellátásához, azokkal arányban álló költségvetési, illetve más vagyoni támogatásra jogosult.” [40 p. 30.]

A kötelezően ellátandó feladatcsoportokat az Mötv. 13. § (1) bekezdése tartalmazza az alábbiak szerint:

„A helyi közügyek, valamint a helyben biztosítható közfeladatok körében ellátandó helyi önkormányzati feladatok különösen:

a. településfejlesztés, településrendezés;

b. településüzemeltetés (köztemetők kialakítása és fenntartása, a közvilágításról való gondoskodás, kéményseprő-ipari szolgáltatás biztosítása, a helyi közutak és tartozékainak kialakítása és fenntartása, közparkok és egyéb közterületek kialakítása és fenntartása, gépjárművek parkolásának biztosítása);

c. a közterületek, valamint az önkormányzat tulajdonában álló közintézmény elnevezése;

d. egészségügyi alapellátás, az egészséges életmód segítését célzó szolgáltatások;

e. környezet-egészségügy (köztisztaság, települési környezet tisztaságának biztosítása, rovar- és rágcsálóirtás);

f. óvodai ellátás;

g. kulturális szolgáltatás, különösen a nyilvános könyvtári ellátás biztosítása; filmszínház, előadó-művészeti szervezet támogatása, a kulturális örökség helyi védelme; a helyi közművelődési tevékenység támogatása;

h. gyermekjóléti szolgáltatások és ellátások, 8a. szociális szolgáltatások és ellátások, amelyek keretében települési támogatás állapítható meg;

i. lakás- és helyiséggazdálkodás;

j. a területén hajléktalanná vált személyek ellátásának és rehabilitációjának, valamint a hajléktalanná válás megelőzésének biztosítása;

k. helyi környezet- és természetvédelem, vízgazdálkodás, vízkárelhárítás;

l. honvédelem, polgári védelem, katasztrófavédelem, helyi közfoglalkoztatás;

m. helyi adóval, gazdaságszervezéssel és a turizmussal kapcsolatos feladatok;

n. a kistermelők, őstermelők számára – jogszabályban meghatározott termékeik – értékesítési lehetőségeinek biztosítása, ideértve a hétvégi árusítás lehetőségét is;

o. sport, ifjúsági ügyek;

p. nemzetiségi ügyek;

q. közreműködés a település közbiztonságának biztosításában;

r. helyi közösségi közlekedés biztosítása;

s. hulladékgazdálkodás;

t. távhőszolgáltatás;

u. víziközmű-szolgáltatás, amennyiben a víziközmű-szolgáltatásról szóló törvény rendelkezései szerint a helyi önkormányzat ellátásért felelősnek minősül.”

Ha áttekintjük a fent felsorolt feladatcsoportokat, akkor látható, hogy jelentős részük tartozik a kritikus infrasturktúrák körébe, amelyekhez természetesen kritikus információs infrstruktúrák kapcsolódnak.

3.2.2. Településszekezet és feladatellátás

Az 1990-ben létrejött önkormányzati rendszer kiemelt jelentőségű eleme volt, és az új alaptörvényi szabályozás és az Mötv. is a megőrzendő alapértékek közé sorolta, hogy minden település számára lélekszámtól függetlenül biztosította a helyi önkormányzás jogát. A közfeladatok ellátásához érdemi kompetenciákkal rendelkező önkormányzati rendszer szükséges, aminek meghatározó elemei a települési önkormányzatok. A helyhatóságok állnak a legközvetlenebb kapcsolatban választópolgáraikkal, ezért a helyben biztosítható közszolgáltatásokat – ide értve az alapvető

közigazgatási ügyek intézését is – a települési önkormányzatokhoz indokolt telepíteni. Ugyanakkor tény, hogy Magyarország településszerkezete jellemzően aprófalvas. Így bár minden település rendelkezik a helyi önkormányzás jogával, minden településen választanak képviselő-testületet, polgármestert, azonban nem minden esetben biztosítottak a helyi hatalomgyakorlás feltételei. A 2016. január 1-jei KSH adatai szerint Magyarországon 3155 település (a fővárosi kerületekkel együtt 3178) található, a lakosságszám pedig 10 023 061 fő.

A települési önkormányzatok elsődlegességére építkező rendszerben nem lehet figyelmen kívül hagyni azt, hogy településszerkezetünk elaprózott jellegű, és jelentős számban vannak alacsony lélekszámú települések.

5. ábra

Települések számának megoszlása lakosságszám szerint (2016.01.01.)

Forrás: a KSH adatai alapján saját szerkesztés.

A községek több, mint fele az aprófalvak kategóriájába tartozik, ennek ellenére lakosságuk az ország népességének csak mintegy 7%-át adja, továbbá a települések több, mint 75%-a 2000 fő lakosságszám alatti.

Nyilvánvaló, hogy az alacsony lélekszámú települések gazdasági teljesítőképessége korlátozott, ezért nem képesek minden közszolgáltatás önálló, hatékony biztosítására. A fenti adottságokra tekintettel a kötelező önkormányzati hatáskörök meghatározásánál figyelemmel kell lenni az egyes önkormányzatok teherbíró képességére. Erre elvi alapot a Mötv. 11. § (1) bekezdése teremt, amikor rögzíti, hogy az egyes önkormányzati típusoknak – a községnek, a városnak, a járásszékhely városnak, a megyei jogú városnak, a fővárosnak és kerületeinek, valamint a megyei önkormányzatnak – egymástól eltérő feladat és hatáskörei lehetnek. Az Mötv. 11. § (2) és (3) bekezdésében megjelenik a differenciált feladattelepítés.

„[A t]örvény a kötelező feladat- és hatáskör megállapításánál differenciálni köteles, figyelembe véve a feladat- és hatáskör jellegét, a helyi önkormányzatok eltérő adottságait, különösen

a) a gazdasági teljesítőképességet;

b) a lakosságszámot;

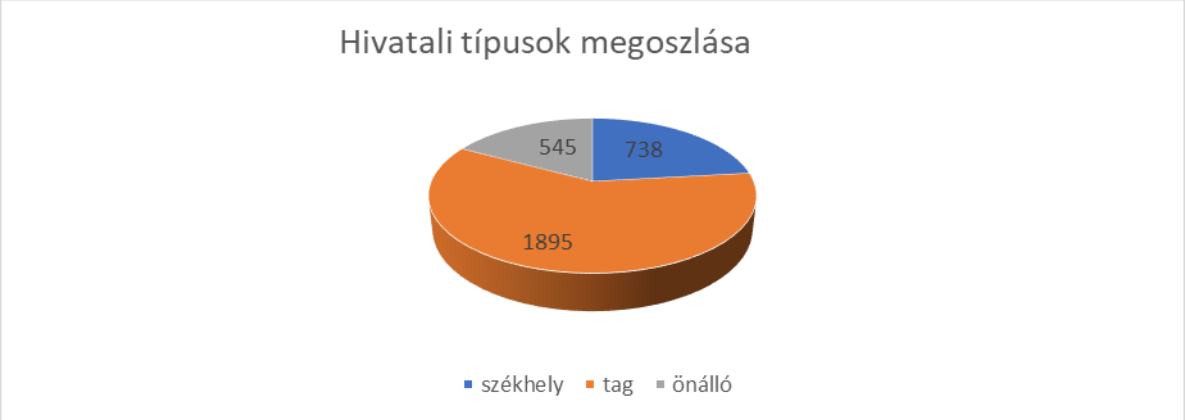
c) a közigazgatási terület nagyságát.

Jogszabály a hatáskör telepítésével egyidejűleg meghatározza a feladat- és hatáskörellátáshoz szükséges minimális szakmai, személyi, tárgyi és gazdasági feltételeket." [68]

Az ágazati jogszabályok többségében figyelembe veszik a differenciált feladattelepítés elvárását, azonban sok esetben – az önkormányzati működés ismeretének hiányában – az ágazati feladat telepítésekor a tervezés elnagyolt, nem eléggé kidolgozott.3.2.3. Hivatali szerkezet

A polgármesteri hivatalok tekintetében az Mötv. csak keretszabályozást tartalmaz, biztosítva ezzel azt, hogy a képviselő-testület a helyi sajátosságok figyelembe vételével alakíthassa ki hivatali szervezetét, határozhassa meg működését. A hivatali feladatok ellátása két módon lehetséges: önálló polgármesteri hivatal (települési, megyei önkormányzati hivatal, főpolgármesteri hivatal) működtetésével, illetve több önkormányzat által létrehozott közös önkormányzati hivatal útján.

Közös önkormányzati hivatalt azon községeknek kellett létrehoznia, amelyek lakosságszáma nem érte el a 2000 főt. Esetükben nem tartható fenn önálló polgármesteri hivatal. Azonban a 2000 fő lakosságszámot meghaladó településnek választási lehetősége van, hogy önálló hivatalt hoz-e létre, vagy közös hivatal keretében más településsel együtt gondoskodik a hivatali teendők ellátásáról.



6. ábra

Az önkormányzati hivatalok típus szerinti megoszlása (2016)

Forrás: a KSH adatai alapján saját szerkesztés.

A hivatal (mind az önálló, mind a közös hivatal) az önkormányzat operatív munkaszervezete. Fő feladata, hogy a döntéseket előkészítse és a képviselőtestület(ek) által meghozott döntéseket megvalósítsa. A polgármesteri hivataloknak nincs döntési hatásköre, azonban az önkormányzat szempontjából működése meghatározó. A közszolgáltatások színvonalas biztosításának záloga a felkészült, magas szakmai szinten működő apparátus.

3.3. Elvárások és megfelelés

Az előzőekben már többször került említésre, hogy az önkormányzatokkal szembeni állampolgári elvárások jelentősen megváltoztak és közben átalakult az önkormányzatok működési környezete is. Az önkormányzatok számára ma már nincs választási lehetőség, hogy részesei lesznek-e az információs társadalomnak, hiszen végérvényesen annak részeseivé váltak, ami jelentős szabályozási megfelelési kötelezettséget is jelent a hivatalok számára.

3.3.1. Az Információbiztonsági törvénynek való megfelelés

Az információs társadalmat érő fenyegetések miatt napjainkban kiemelten fontos az önkormányzatok vagyonát képező elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, rendszerelemek biztonsága.

Az adatok védelme érdekében az Ibtv. az alábbi feladatok ellátást várja el az önkormányzatoktól:

- Információbiztonsági felelős kijelölése.
- Elektronikus információs rendszerek biztonsági osztályba sorolása.
- Informatikai biztonsági szabályzat készítése.
- Biztonsági szabályzatok létrehozatala.
- Az elektronikus információs rendszerek kockázatelemzésének elvégzése.
- Az elektronikus információs rendszerek kockázatkezelésére intézkedések megtétele.
- A felhasználók felelősségi köreinek megállapítása, kijelölése.
- A felhasználók rendszeres képzése, biztonság tudatosságának növelése.
- A biztonsági események kezelése, eljárások kidolgozása a saját szervezeten belül.

Az Ibtv. három szereplőt azonosít az információbiztonság területén: a szervezeti vezetőt és a rendszer használóját mint a folyamat résztvevőit, továbbá az információbiztonsági felelőst.

A polgármester vagy a jegyző nem feltétlenül van tisztában az információbiztonsági kérdések fontosságával, miközben a tisztviselői állomány szükséges kompetenciafejlesztéséről dönt, és kinevezi az információbiztonsági felelőst. Ahhoz, hogy a munkatársak rendelkezzenek a szükséges képességekkel, tudatosak legyenek az eszközök, rendszerek használata során, illetve IB felelősnek a megfelelő ember legyen kinevezve, elengedhetetlen, hogy a vezetők – önkormányzatok esetében a polgármester és jegyző – értsék és tisztában legyenek a terület fontosságával és az elvégzendő feladatokkal.

A szakértők szerint az IB felelősöknek tudásbrókernek is kell lenniük. Így képesnek kell lenniük közvetíteni az önkormányzat és a hatóságok (például a NEIH) között. Általánosan ismert probléma, hogy a felhasználók nem értik az informatikus elvárásait, és az informatikus nem érti a szakmai folyamatokat. Ez a konfliktus a biztonsági előírások betartása ellen hat. Olyan IB felelőst érdemes választani, aki képes „fordítani”, beszéli mindkét nyelvet, és közvetíteni tud a műszaki üzemeltető és a szakmai feladatokért felelős szakértők között.

A NEIH adatai alapján a központi és az önkormányzati szereplők Ibtv. által elvárt kötelezettségeiknek az alábbiak szerint tettek eleget:

2. táblázat

Ibtv. elvárásainak való önkormányzati megfelelés Forrás: NEIH 2017. június 6-ai adatai alapján saját szerkesztés.

	Összesen (db)	Ebből önkormányzati hivatal (db)	Önkormányzati arány a regisztrált körhöz képest (%)	Önkormányzati megfelelés regisztrált önkormányzati körhöz képest (%)	Önkormányzati megfelelés az adott adatszolgáltatást benyújtókhoz képest (%)
Regisztrált szervezetek:	1570	1316	84%		
Adatszolgáltatást tett:	991	872	56%	66%	88%
Információbiztonsági felelőst regisztrált:	878	776	49%	59%	88%
Informatikai biztonsági szabályzatot benyújtott:	808	713	45%	54%	88%
Osztályba sorolást benyújtott:	643	577	37%	44%	90%
Osztályba sorolást benyújtott:	643	577	37%	44%	90%
Szintbe sorolást küldött:	408	368	23%	28%	90%

A táblázatból kiolvasható, hogy a regisztráltak többsége az önkormányzati hivatalok közül kerül ki: a teljes kör 84%-a. Ha megvizsgáljuk a teljesítéseket, akkor az utolsó oszlop mutatja, hogy az önkormányzati kör a teljes regisztrálti körhöz képest – ha kis mértékben is –, de szabálykövetőbb az egyéb kormányzati körből kikerülő érintetteknél: törekszik a szabálykövetére. Például az adatszolgáltatás teljesítői közül 88% önkormányzati hivatal, ami az eredeti aránynál 4%-kal magasabb. Ugyanakkor az is látszik, hogy az önkormányzatok alig valamivel több, mint fele tett eleget adatszolgáltatási kötelezettségeinek a teljes körhöz viszonyítva. A többi tényező esetében ez az arány 50% alatt van, ami nagyon alacsony érték, és egyben kiberbiztonsági szempontból is kritikus.

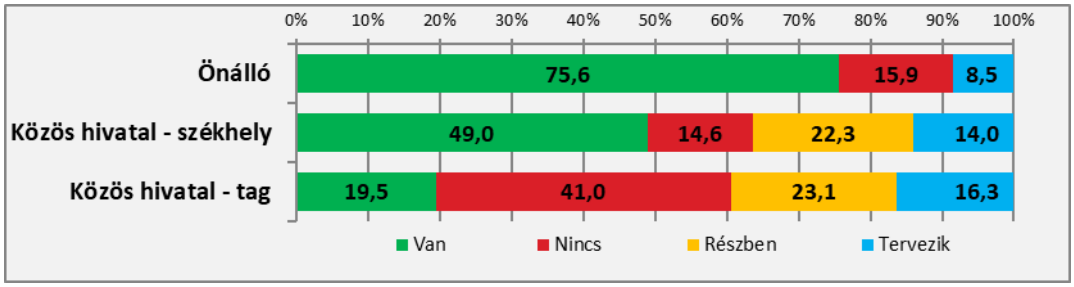
A NEIH tapasztalatai szerint [32] több probléma adódott az önkormányzatokkal végzett munka során:

- ASP (Application Service Provider: alkalmazásszolgáltató – a szerző kiegészítése) vonatkozásában, az önkormányzatok hivatalai az általuk kezelt közadatok kezelésére szerződött partnerekkel kötött együttműködéséből adódó problémák (adatmigrálás ASP-be);
- központi szolgáltatók, intézmények által az IT biztonsági követelmények előírásainak, az elvárások ismertetésének, tájékoztatásának elmaradása az ügyfelek felé (végpontok, önkormányzatok), ami komoly nehézséget okoz (például önkormányzati ASP esetében);
- a „központi" szolgáltatások, szakrendszerek fejlesztésénél a végponti védelmi intézkedések megvalósítását biztosító információk (információbiztonsági elvárások a végponti hozzáférők részére) és anyagi fedezet biztosításának elmaradása;
- mobil eszközök (például: pendrive) és internet korlátozás nélküli használata a szakrendszeri hozzáféréseket biztosító eszközökön;
- incidenskezelési együttműködés esetei és zavarai, adatszolgáltatási kötelezettség elmaradása.

Az önkormányzatok kiberbiztonsággal kapcsolatos kérdéseiről a témában lefolytatott online felmérés és fókuszcsoportos interjú eredményeit bemutató fejezetben részletesen lesz szó, jelen esetben csupán az Ibtv.-nek való megfeleléshez szorosan kapcsolódó részekre kapott válaszok eredményét mutatom be:

- Van-e az önkormányzatnak információbiztonsági stratégiája?[13]
- Van-e az önkormányzatnak adatkezeléssel foglalkozó szabályzata?
- Van-e protokoll az informatikai rendszeren elkövetett támadások esetére?

Az információbiztonsági stratégia megléte kapcsán reményt keltő, hogy bár két éve nem kötelező a készítése, az önkormányzatok jelentős része mégis rendelkezik vele. Az információbiztonsági stratégiával kapcsolatosan előzetes megállapítás, hogy átlagosan az önkormányzatok egyharmada (36,9%) rendelkezik ezzel a dokumentummal. A kép a valóságban ennél árnyaltabb, hiszen az önálló hivatalok háromnegyede, a székhelyként működő szervezetek fele és a kirendeltséghivatalok egyötöde rendelkezik ilyen alapdokumentummal. Részben elkészült stratégiákat is jeleztek, amelyeket nem fejeztek be, vagy jelenleg is azt írják. Ezek a közös hivatal tag önkormányzatokra jellemzőek.



7. ábra

Információbiztonsági stratégia rendelkezésre állása (2018.02.13.)Forrás: Online kérdőíves felmérés, saját szerkesztés.

[13] Az információbiztonsági stratégia készítésének kötelezettségét a 2015: CXXX. törvény 8. § (40) bekezdés a) pontja 2015. 07. 16-tól hatályon kívül helyezte

Az adatkezelési szabályzat tekintetében jobb eredmények a jellemzőek. Átlagosan tíz hivatal esetében hétnél található ilyen alapdokumentum (68,4%). Ezen belül az esetek több, mint 80%-ában van jelen a szabályzat az önálló (87,3%) és a székhelyhivatalok (83,4%) működésében, de a legkisebb hivatalok nagyobbik felében (51,4%) is rendelkezésre áll a dokumentum.

3. táblázat

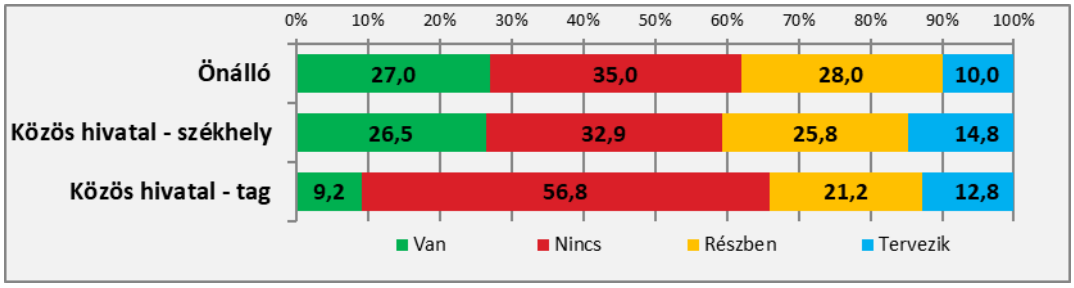
Az adatkezelési szabályzat megléte Forrás: Önkormányzatok és kiberbiztonság – online felmérés (saját szerkesztés).

Közigazgatási-feladatellátási státusz	Kötelezettségek – lehetőségek: adatkezelési szabályzat									
	Van		Nincs		Részben		Tervezik		∑	
	db	%	db	%	db	%	db	%	db	%
Önálló	89	87,3	2	2,0	9	8,8	2	2,0	102	100,0
Közös hivatal székhely	131	83,4	2	1,3	20	12,7	4	2,5	157	100,0
Közös hivatal tag	129	51,4	55	21,9	56	22,3	11	4,4	251	100,0
Összesen	349	68,4	59	11,6	85	16,7	17	3,3	510	100,0

Emellett a szabályzat hiánya leginkább a taghivatalokra jellemző, hiszen egyötödük (21,9%) nem rendelkezik ezzel, és ebben a csoportban ilyen arányban vannak a részben elkészült szakmai anyagok is (22,3%). A központi hivatalok esetében ezen arány fele, míg az önállóaknál a harmada jellemző. Végül tervezik a szabályzat megalkotását több, mint minden huszadik (4,4%) kirendeltségnél, minden negyvenedik székhelyként működő szervezetnél (2,5%), illetve minden ötvenedik (2%) önálló hivatal esetében.

A szabályozott működés kapcsán fontos még annak vizsgálata, hogy fel van-e készülve az önkormányzat egy esetleges támadásra. Ez azért is nagyon fontos, mert a reagálás idejét jelentősen lerövidítheti, ha van alkalmazandó protokoll egy informatikai rendszer ellen elkövetett támadás esetére.

Az informatikai rendszerek ellen elkövetett támadások esetére követendő protokollok kidolgozottsága területén már végképp nem kedvezőek a számok. Ezzel egyik feladatellátási státuszhoz tartozó hivataltípus sem büszkélkedhet, hiszen mindössze és átlagosan, csupán a hivatalok egyötödére jellemző a valódi „know-how" megléte (18%). A kirendeltséghivatalok 9,2%-a, míg a székhely- és önálló hivatalok 26–27%-a rendelkezik ezzel.



8. ábra

Informatikai rendszerek ellen elkövetett támadások esetén követendő protokollok kidolgozottsága

Forrás: Önkormányzatok és kiberbiztonság – online felmérés (saját szerkesztés).

A leginkább jellemző státuszok: a protokoll hiánya, vagy a részben meglévő eljárásrend kategóriái. Átlagosan a szervezetek 45%-a (a kirendeltségek 56,8%-a és a másik két hivatali csoport

egyharmada) egyáltalán nem tud felmutatni protokollt, de további egynegyedük (24%) is csupán részben kidolgozott szakmai anyaggal rendelkezik (a taghivatalok egyötöde és a másik két csoport 25,8–28%-a).

A hiányosságok pótlására átlagosan minden nyolcadik hivatalban betervezték a protokollok megalkotását, ezek közül is legnagyobb arányban a székhelyhivatalok (14,8%), a legkisebb hányadban pedig az önálló hivatalok (minden tizedik eset) szeretnék pótolni mulasztásukat.

3.3.2. Az Infotörvény elvárásainak való megfelelés

„A közérdekű és közérdekből nyilvános adatok kötelező közzétételének teljesítése nemcsak mennyiségi, hanem minőségi vetülettel is rendelkezik. Ez azt jelenti, hogy az önkormányzat nem elégedhet meg azzal, hogy az önkormányzatra vonatkozó, jogszabályok által meghatározott valamennyi közérdekű adatot – ideértve az önkormányzati döntéshozatallal összefüggő adatokat is – közzéteszi, hanem törekednie kell arra is, hogy a közzétételi kötelezettségét időszerű, pontos és hozzáférhető módon teljesítse. E két szempont együttes érvényesülése biztosítja az Infotv. való teljes körű megfelelést, a helyi lakosság tájékozottságát és részvételét a helyi közügyekben, és nem utolsósorban jelentős presztízsnövelő tényező az önkormányzatok számára is." [41 p. 3.]

Ez nem csak törvényi elvárás. Az önkormányzati működéssel szemben a XXI. század tudatos állampolgára más elvárásokat támaszt, mint azt az elmúlt században tették. Míg a XX. században az önkormányzat megengedhette magának a zárt és lassú működést, addig ma a lakosok elvárják a szolgáltató szemléletű működést. Elvárják az önkormányzattól, hogy a közérdekű adatokat megossza, megismerésüket lehetővé tegye.

További vállalása volt az országnak a Nyílt Kormányzati Együttműködésben való (a továbbiakban: OGP) részvétel.[14] A kezdeményezést 2011-ben indította útjára a nyolc alapító tagállam, és mára már dinamikusan bővülő tagsággal rendelkezik.[15] Az OGP célja a nyílt kormányzás erősítése oly módon, hogy támogatja a társadalmi részvételt, segíti a kormányzati tevékenységre vonatkozó információkhoz való jobb hozzáférést, támogatja a közigazgatás egészében történő legmagasabb szintű integritás megvalósítását.

A NAIH jelentései [42] azt mutatják, hogy a jogszabályi háttér megléte ellenére a települési önkormányzatok vagy egyáltalán nem, vagy a törvényben meghatározottakhoz képest csak részben teljesítik közzétételi kötelezettségüket, így közérdekű adatok online közzététele jelentős csorbát szenved.

Az NVSZ felmérése szerint [41 p. 7.] az önkormányzatok közzétételi kötelezettségeik maradéktalan teljesítésének akadályaként megjelölték a jegyzők és köztisztviselők, a polgármesteri hivatal alkalmazottainak kis létszámából adódó leterheltségét, valamint a csekély anyagi forrás miatti tárgyi feltételek hiányát. Nehézségként jelentkezik továbbá, hogy a közzétételi folyamatot számos önkormányzatnál egy munkatárs fogja össze, így nehéz megoldani, hogy ő az önkormányzat minden

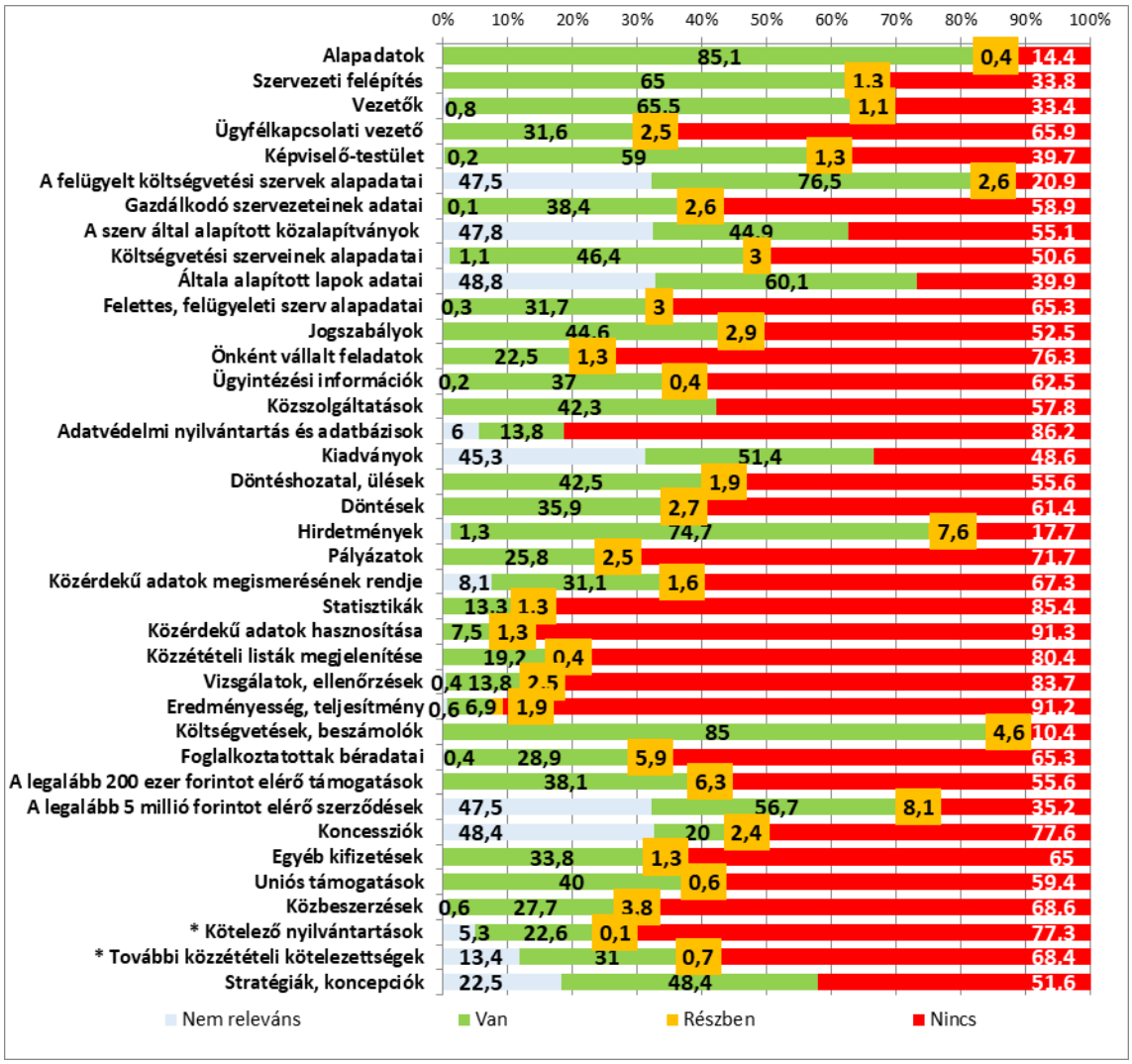
[14] 2016 decemberében Magyarország kilépett az egyezményből.
[15] 2018 februárjában több, mint 90 ország. Lásd: Participants OGP http://www.opengovpartnership.org/countries (letöltve: 2018. 03. 21.)

területére vonatkozóan rendelkezzen információval, és nyomon kövesse minden érintett szakterület adatszolgáltatásának teljesülését.

Az Infotv. 33. § (3) bekezdése lehetővé teszi az önkormányzatok számára, hogy választásuk szerint saját honlapot hozzanak létre az adatközlés céljára, vagy társulásaik által közösen működtetett, illetve a felügyeletükkel, szakmai irányításukkal vagy működésükkel kapcsolatos koordinációt ellátó szervek által fenntartott, valamint az erre a célra létrehozott központi honlapon. Ezzel egyidejűleg a honlapra, valamint az ott szereplő adatbázisokra és nyilvántartásokra vonatkozó leíró adatokat a központi közadatkereső honlapon, a *www.kozadat.hu* oldalon is közzé kell tenniük. Az Infotv. e szabálya segítséget jelenthet azoknak az önkormányzatoknak, amelyek kapacitáshiány miatt saját honlapot készíteni és üzemeltetni nem lennének képesek. Fontos ugyanakkor hangsúlyozni, hogy a www.kozadat.hu honlapon történő közzétételt nem váltja ki a saját vagy társulási honlapon történő közzététel. Kiemelendő továbbá a meglévő adatrendszerek körében egyrészt a nemzeti jogszabálytár, amelynek önkormányzati rendelettára [77] jelentős segítséget nyújt az önkormányzatok számára a rendeletek közzététele szempontjából. Emellett az önkormányzati költségvetési alapadatokról a Magyar Államkincstár törzskönyvi nyilvántartásából [78] is elérhető információk.

A Belügyminisztérium Önkormányzati államtitkárságán az Önkormányzati Koordinációs Iroda által gondozott kutatás már publikált [43 p. 10.] eredményei is azt mutatják, hogy az Infotv. által elvárt mintegy 250 adatból a nagyvárosok is csak átlagosan 80%-os mértékben tesznek eleget az online közzétételnek. A vizsgált önkormányzatok többsége 40–70% közötti eredményt tudott felmutatni.

A BM kutatása a teljes önkormányzati körre készített adatfelvétel adatait elemezte. Azokban az esetekben, amikor nem volt települési weblap, illetve – közös hivatal esetén – a székhely önkormányzati hivatal weblapján történt az analízis.



9. ábra

Összefoglaló – Az egyes közzétételi egységek előfordulási aránya (%) [43 p.11.].

Az elemzés fókuszában a weblapokon megjelenő, illetve az azokon kötelezően szereplő adatok állnak. A közzé nem tett adatok tekintetében egyértelmű a lehatárolás, hiszen ezekben az esetekben egyáltalán nincs megjelenített tartalom, ez „Nincs” kategóriája. A részleges vagy nem megfelelő tartalmú közzététel esetében a „Részben” kategóriát alkalmazták. A szerzők arra a megállapításra jutottak, hogy e két kategória között – jogkövetés szempontjából – nincs különbség. A weblapokon megjelenítendő tartalom vizsgálatánál külön elemzés készült a kötelezően megjelenítendő adatokat érintő közzétételi egységekre és magukra a konkrét adatokra, elemekre is.

Az Infotv. sajnálatos módon nem vette figyelembe a differenciált feladattelepítéssel kapcsolatos Mötv. általi elvárást. Függetlenül az egyes települések gazdasági teljesítőképességétől, lakosságszámától és a közigazgatási terület nagyságától azonos elvárásokat támaszt a településekkel szemben. Ahogyan a kutatásból is látszik, ennek az a következménye, hogy az önkormányzatok jelentős mértékben nem tesznek eleget a törvényi előírásoknak.

Az önkormányzatok online megjelenése sem biztosított teljes körűen, és a meglévő oldalak funkcionalitása, használhatósága és felhasználóbarát kialakítása rendkívül kezdetleges.

A BM kutatásának egyik megállapítása, hogy a kormányzat és a közigazgatás előtt hatalmas tanulási folyamat áll, aminek során meg kell érteniük, hogy az új közpolitika-alkotási folyamatok ellentmondást nem tűrően törnek utat maguknak. Az ügyféligények könnyen igazodnak a gyorsan változó trendekhez, ami további feladatokat ró a közigazgatásra. Annak érdekében, hogy a szolgáltatások minősége képes legyen igazodni az állampolgárok növekvő elvárásaihoz, markáns szemléletváltás szükséges, aminek központi eleme az alkalmazkodás, az új funkciók ellátásához szükséges kapacitások kialakítása, valamint a kommunikációs (és közigazgatási) stratégiák újraalkotása.

Különösen aktuális ez a megállapítás annak fényében, hogy miközben a közigazgatás lassan szerzi meg az érdemi online kommunikáció folytatásának képességét, addig az állampolgárok onlinemédia-használati szokásai átalakulnak. Newman [44] a digitális kormányzati átalakulás trendjeivel foglalkozó cikkében az egyik ilyen szokásként a mobilitás növekedését azonosítja. Kiemeli, hogy a szakértők kezdeti aggodalma, miszerint az alacsony státuszú népesség a digitális társadalom vesztese lesz, téves volt. A kutatások azt mutatják, hogy a mobilitás széleskörű elterjedése ténylegesen áthidalta a digitális szakadékot. Az emberek többségének az okostelefon az egyetlen technológia, amellyel rendelkezik, ezt viszont képes használni, és használja is. Az eszköz jellegéből adódóan, azonban a statikus, egyirányú web 1.0 eszközök helyett rögtön a web 2.0-s vagy web 3.0-as alkalmazásokat kezdték használni.

3.4. Humán erőforrásfejlesztés, a tudatosság növelése

A nemzetközi és hazai szabályozás és a különböző elemzések mind arra hívják fel a figyelmet, hogy a biztonságpolitika területén, a biztonságos működés, az előnyök kiaknázása, a kompetenciák fejlesztése és a tudatosság növelése, jelentős beavatkozásokra van szükség a humánerőforrás kompetenciáinak fejlesztésében, a tudatosság növelésében.

3.4.1. Oktatási stratégiai keretek

A Nemzeti Infokommunikációs Stratégia SWOT analízise szerint [35] Magyarországon jóval uniós átlag feletti a digitális írástudatlanság, és erős negatív attitűd jellemzi az IKT használathoz való hozzáállást. A digitális írástudatlanság a nyugdíjasok, munkanélküliek körében közel 50%. Az állampolgárokra alapszintű szolgáltatások (e-mail, közösségi oldalak, információk, hírek stb.) használata jellemző, és nincsenek tisztában az IKT valós előnyeivel, kevés az e-szolgáltatásokat, e-tranzakciókat igénybe vevők aránya, számuk elmarad az uniós átlagtól is. A tudatosság, a társadalmi felelősségvállalás ezen a téren messze elmarad a kívánatos szinttől.

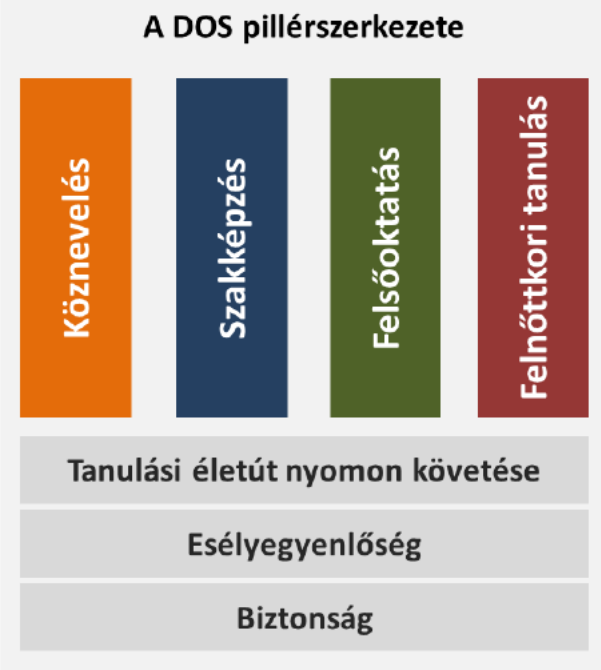
A köznevelés területén is hiányosságokat azonosítottak. Kizárólag az informatika tantárgy keretein belül fejlesztik a digitális kompetenciákat. Ezek a feladatok nem, vagy csak korlátozottan szerepelnek a fejlesztendő kompetenciák között. Továbbá a pedagógusok felkészültsége sok esetben hiányos, az eszközpark nem korszerű és/vagy nem elégséges, végül kevés az informatika tantárgy óraszáma is.

Az Itbusiness [45] 2017 végén megkérte az infokommunikációs szegmensben jelentős szerepet játszó szervezetek vezetőit, hogy értékeljék a szakmapolitika elmúlt egy évét. Többségében üdvözölték a DJP 2.0 megjelenését, azonban komoly problémaként vetették fel a digitális kompetenciák kérdéskörét. A szakértők érthetetlennek tartják a szakképzés és felnőttképzés terén tapasztalható passzivitást, miközben fejlődést akadályozó és biztonságot veszélyeztető szintet ért el

a szakemberhiány. Több meghatározó civil szervezet vezetőjének[16] elmondása szerint számos könnyen megvalósítható javaslattal éltek az állami szervek felé, azonban a szakpolitika nem tesz érdemi lépéseket. Hiányolják a kormányzat részéről annak tudomásul vételét, hogy a digitális jólét nem képzelhető el digitális kompetenciákkal felvértezett tömegek nélkül. Úgy látják, hogy bár a digitális kompetenciák fejlesztéséről örvendetesen sok szó esett, a komplex cselekvési terv kidolgozásához és megvalósításához mégsem sikerült megtalálni a célravezető lépéseket.

A nemzetközi gyakorlatok közül a brit megoldás tervez az oktatás teljes spektrumával, vertikálisan építkezve az oktatási rendszeren belül. Mindezt azért, hogy létrejöjjön a megfelelő és szükséges kibertudással, gyakorlattal és képességekkel rendelkező Egyesült Királyság. Természetesen tisztába vannak azzal, hogy ezt a szakértői kört nem lehet kiképezni egyik napról a másikra; véleményük szerint ez húsz éves időtávban érhető el reálisan. Ez túlnyúlik a jelenlegi (2016–2021) *3D* elnevezésű kibervédelmi stratégiájuk hatókörén. A most megvalósítandó programok átszövik a teljes oktatási rendszert az általános iskolától a doktori képzésig, kiegészítve azt a kibertudományi és technológiai fejlesztésekkel és együttműködésekkel [28 pp. 141–144.].

A DJP keretein belül kidolgozásra került a magyarországi Digitális Oktatási Stratégia (DOS), aminek problémamegközelítési módjai közel állnak a brit szemlélethez. Tartalmazza azt a felismerést, hogy „a digitális átalakulás gyakorlatilag semmilyen hagyományos ágazatot, vállalkozást vagy üzleti modellt sem hagy majd érintetlenül; a következő években dől el, hogy a magyar munkavállalók, s különösen a fiatalok milyen szerepet töltenek majd be az európai munkaerőpiacon, ahogy az is, hogy a magyar nemzetgazdaság milyen szerepet kaphat a nemzetközi versenyben.” [46. p. 29.]



10. ábra

Magyarország Digitális Oktatási Stratégiájának szerkezete [46.p.31.]

[16] Informatikai, Távközlési és Elektronikai Vállalkozások Szövetsége. Neumann János Számítógép-tudományi Társaság.

DOS pillérrendszerét nézve látható, hogy a stratégiai szintű akarat megvan a változtatásra; koncepcionálisan egyértelmű a megközelítés, módszertanilag tartalmazza a fontos elemeket. Azonosítja, hogy miben kell másként közelíteni a digitális kompetenciák fejlesztéséhez, azonban ezen a koncepcionális szinten marad. Nem tartalmaz a cselekvési tervhez rendelten konkrét ütemezést, felelősöket, elvárt eredményeket. A DJP 2.0 a DOS kibocsátását követő évben arról ír, hogy a felelősökkel a kidolgozás folyamatban van. Egyetértve az Itbusinessben nyilatkozó szakértőkkel, érthetetlennek tűnik a szakpolitikai passzivitás. A kompetenciafejlesztés hosszú időt igénylő feladat már az egyén esetében is, miközben itt a társadalmi szintről értekezik a stratégia.

3.4.2. Kihívások, jó gyakorlatok

Ha az angol kibervédelmi stratégia megvalósítására tervezett 1,9 milliárd fontra gondolunk (ami közel kétszerese az előző öt éves stratégiára fordított összegnek), akkor kijelenthetjük, hogy jelentősen növekszik a kibervédelemre fordított költség. Ez azonban, ha nem átgondoltan, kimunkált módon, koncepciózusan történik, akkor nem vezet a várt eredményre.

A tapasztalatok azt mutatják, hogy bár a köz- és magánszféra is egyre többet költ kibervédelmi eszközökre, a kívánt hatás elmarad. Ennek okai összetettek: a kibertámadások módszerei megváltoztak, a biztonsági megoldások kínálata is elképesztő tempóban kibővült, így egyre nehezebb eldönteni, hogy melyik megoldás lenne az adott szervezet számára hatékony. Ráadásul ezek a megoldások általában nem illeszkednek a szervezeti kultúrákba, így sok esetben a meglévő eszközök, metodikák alkalmazása nem biztosított. Tekintettel arra, hogy milyen kritikus területről van szó, milyen komoly veszteségeket okozhat az informatikai rendszerek sérülése, kiesése vagy megsemmisülése, egy kiberbiztonsági szakértő alkalmazása jelenthetne megoldást, azonban ez sem olyan egyszerű.

Az Ibtv. kötelezi az önkormányzatokat, hogy alkalmazzanak információbiztonsági felelőst, azonban egyrészt e szakemberekből van a legnagyobb hiány, másrészt az önkormányzatok anyagi eszközei sem versenyezhetnek a forprofit szervezetek ajánlataival. Önmagában a szakértő alkalmazása sem jelent megoldást, mivel a szakértői felügyeleten túl – különösen a közszférában – szükséges a lehető legmagasabb szintű vezetői elköteleződés is.

„Az információbiztonság szempontjából különlegesen fontos a szervezeti kultúra, annak okán, hogy a szervezet általános információbiztonsága valójában annak tagjain, az egyéneken, továbbá azok aktuális viselkedésén múlik. A szervezet dolgozóinak tudatos információbiztonsági magatartását – a megfelelő képzés mellett – leginkább a felsővezetői elkötelezettség és tudatosság befolyásolja pozitív irányban, melyet a dolgozóknak meg is kell tapasztalniuk (a valóságban hallaniuk kell). Vezetői elfogadás, akarat, támogatás nélkül nem lehetséges rendszert kiépíteni, működtetni.” [10 p. 38.]

David Garrett, a kaliforniai székhelyű Tensyl Security biztonsági tanácsadó cég alapítója [47] öt alapvető tényezőt számolt össze, ami miatt nem költik el a cégek a pénzüket megfelelően:

- A legtöbben a kiberbiztonságot kizárólag az IT hatáskörébe utalják, miközben az egyes incidensek leggyakrabban nem az IT-biztonság hiányosságaiból fakadnak, hanem a szervezeti kultúrából, a rossz előírásokból, vagy az azokat be nem tartó kollégákból,

vezetőkből. Önmagában a legtökéletesebb rendszer sem működik, ha a munkatársak, vezetők nem tudatosak a kiberfenyegetettség tekintetében. Rendelkezésre állhat a papíron közel tökéletes rendszer, ha a munkatársak megnyitják a spamet tartalmazó és kétes eredetű üzeneteket, valamint privát eszközöket használnak a vállalat rendszereinek eléréséhez.

- A biztonsági stratégiákkal ugyanez a probléma: mindenki azt gondolja ez az IT-ra tartozik, miközben a digitális kockázatok a legritkább esetben korlátozódnak egy területre. Jellegükből adódóan komplex megközelítést igényelnek.
- A kutatások igazolták, hogy az incidensek előfordulása szoros kapcsolatot mutat egyes munkavállalói szokásokkal. A dolgozók nem gondolják, hogy ezek a fenyegetések nagy kockázatot hordoznak, ezért a sokszor bonyolultnak, kényelmetlennek tartott biztonsági szabályokat nem tartják be: jelszóképzési szabályok, új programok telepítése, külső eszközök csatlakoztatása. A biztonsági szabályok be nem tartása a legfőbb probléma, hiszen a legjobb szabályrendszer is éppannyit ér, amennyire azt betartják, avagy betartatják.
- A biztonsági szakembereknek – a megfelelő munkavégzés érdekében – nemcsak a támadások mibenlétével kell tisztában lenniük, hanem a szervezeti működéssel, a folyamatok sajátosságaival is.
- Hozzáértés hiányában vagy az erőforrások és a bizonytalanság miatt, megfelelő védelmi rendszer kiépítése nem valósul meg. Ez főként a kisebb, forráshiányos szervezeteket, önkormányzatokat jellemzi.

A helyzetet csak komplex módon, tudatosító akciókkal, kampányokkal és rendszeres információmegosztással és képzéssel, esettanulmányok feldolgozásával, gyakorlati programok megvalósításával lehet kezelni. Jó gyakorlat a brit CERT–UK programja: ez havonta három gyakorlatot tartalmaz, amelyeknek megvalósítása a hálózatbiztonsági kérdésekben érintett szervezetek kiberreagáló képességének tesztelésére szolgál.

3.4.3. Képzési tapasztalatok

A központi és helyi kiberbiztonsági intézkedések mind az ellenálló képesség javítását, az esetleges kiberbiztonsági incidensek megelőzését és a felkészültség növelését célozták. Az elmúlt években jelentős előrelépés történt a területen, de egyrészt bőven van még tennivaló, mivel jelentős lemaradásból indultak a szervezetek. Másrészt ezeket a pozitív folyamatokat nem elég elindítani; fenn is kell tartani, rendszeresen ellenőrizni és a szükségleteknek megfelelően újratervezni. A pozitívumok közül kiemelendő, hogy elismerésre került a preventív szemlélet és a tudatosítás fontosságának elismerése, az együttműködés és a párbeszéd beindulása a kormányzat forprofit és az akadémiai/oktatási kör szereplői között. Utóbbi a holisztikus szemlélet megjelenésének köszönhető, vagyis annak a felismerésnek, hogy minden szektorban kiemelten fontos az információbiztonság szintjének emelése.

Az NKE-n 2014-ben továbbképzésben részt vevő tisztviselőket kérdeztek meg az információbiztonság témakörében. A kérdőívet 379-en töltötték ki. A kutatók tanulmányukban előre jelezték, hogy az információbiztonság kérdésköre egy szervezetnél nem mérhető jól kérdőívvel. Ennek egyik oka, hogy a válaszadók igyekeznek „jó” választ adni, így az nem tükrözi azt, ahogyan

egy valós helyzetben reagálnának. A másik ok, hogy nem a teljes sokaságot szondázzák, így a felmérés nem „egyenszilárd”.

A kutatás megállapítása szerint a kérdőívet kitöltők jelentős része (61%) gondolja úgy, hogy az információbiztonság területén kellő mértékben képzett, ami két szempontból jelez problémát. Egyrészt ez ellentmondásban van más kérdésekre adott válaszokkal, másrészt tükrözi azt a tényt, hogy a válaszadók nincsnek tisztában azzal, hogy a biztonság nem állapot, nem érhető el. A mobileszközök használata és az alkalmazások telepítése kapcsán vegyes kép került feltárásra: ez esetben is a munkatársak tudatosságának növelése lehet a megoldás. Megállapításra került, hogy az információbiztonsági szervezeti egységek a hierarchia alacsonyabb szintjén helyezkednek el (sokszor létesítményüzemeltetés), mint amit a feladat komplexitása megkíván [31 p. 68–72.].

Az önkormányzati köztisztviselők továbbképzési rendszerének kereteit a közszolgálati tisztviselők továbbképzéséről szóló 273/2012. (IX.28.) Korm. rendelet szabályozza [69]. A jogszabály értelmében a közszolgálati tisztviselők meghatározott tanulmányi pontértékű továbbképzést kötelesek elvégezni a négy éves képzési ciklus alatt. Az elektronikus információbiztonsági (EIB) továbbképzéseket az elektronikus információs rendszerek védelméért felelős vezetők, az elektronikus információs rendszerek biztonságáért felelős személyek, valamint az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek vehetik igénybe. Ezek a továbbképzések és éves továbbképzések – az NKE programismertetője szerint – az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek információbiztonsági ismereteinek frissítése, aktualizálása céljából tematikus programokat is kínálnak (célzott kibertámadások, incidenskezelés, okoseszközök), kitekintve az információbiztonsági menedzsment kérdéseire. Az e-learning képzések vizsgasorral zárulnak és ingyenesen elérhetők a közszolgák számára. A továbbképzés az információbiztonságért felelős vezetők részére nyolc, míg az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek számára 50 órásak. Az éves továbbképzések a feladatellátásban részt vevő személyek számára szintén e-learninges formában, 25 órás tanfolyamként ingyenesen rendelkezésre állnak. Az NKE releváns képzéseinek összefoglalója a 2. mellékletben található.

Az NKE-n 2014-ben lefolytatott kutatás [31] a szakértői interjúkra támaszkodva jelezte, hogy a megkérdezettek szerint az érintetti kör tudásának heterogenitása jellemző. Javaslatként fogalmazódott meg, hogy legyen része a közigazgatási alapvizsgának az információbiztonság témaköre, továbbá választható modulként szerepeljen a szakvizsgán. Az alapvizsga tananyagában megjelenik az információbiztonság témaköre. A követelményelvárás szerint azonban a minősített adatokkal kapcsolatos jogi ismeretek vannak fókuszban. Új ismeretként megjelennek a GDPR elvárásai, azonban a szakvizsga anyagai közé 2018-ban nem kerültek be. Egyértelmű ajánlásként került megfogalmazásra, hogy az eredmények elérése érdekében szakítani kellene a hagyományos tartalmakkal és oktatási módszerekkel. A megkérdezettek a gyakorlati megközelítést gondolták hatékonyabbnak. Javasolták, hogy célszerű lenne az EIB-képzés által érintett három szinten három különböző tananyagot tanítani, továbbá szakmai fórumok, szakmai párbeszéd beindítását, a

szükséges platformok létrehozását és működtetését szorgalmazták a különböző intézményekben dolgozó EIB-felelősök között.

Az NKE kutatása [31] az információbiztonsági felkészítés terültén többek között javaslatot fogalmazott meg az oktatás szereplőinek eltérő tananyaga, az oktatási módszer tekintetében. A brit kiberbiztonsági stratégia pedig a reziliens angol kibertér megvalósításához szükséges humán erőforrás kialakítására közel 20 éves időtávot prognosztizál, ezért több színtéren és módon avatkoznak be az emberi erőforrás fejlesztésébe. Célszerűnek látszik a rendszer felülvizsgálata és a szinergiák kihasználása érdekében a képzési rendszer újragondolása.

Gajduschek tanulmányában a kormányzással, közigazgatással kapcsolatban említi azt a klasszikus paradigmát, hogy a közszféra az eredményesség és a hatékonyság megállapítása alatt a közigazgatás jogszabályainak pontos, gyors és kiszámítható betartását érti. Véleménye szerint a magyar közigazgatás ezt a modellt követi: jogias jellegű közigazgatás, amelyben a meghatározó érték a jogszerűség és nem a hatékonyság [48 p. 104.]. Ez a megközelítés tetten érhető a közszolgálati képzés területén és az önkormányzatok körében is, tehát elsődleges – és sajnos sok esetben elégséges is – a jogi megfelelés ahhoz, hogy a területet eredményesnek ítéljék. Így jellemző az információbiztonsági területen is, hogy szabályozási minimum a megcélzott eredmény.

3.5. Önkormányzati vezetők feladatai a kritikus infrastruktúrák védelmében

Ahogy az első fejezetben már tárgyalásra került, a kritikus információs infrastruktúrák önmagukban és az egyéb kritikus infrastruktúra elemek információs rendszereiként ki vannak téve különböző fenyegetéseknek:

- természeti katasztrófák: (vízkárok, geológiai katasztrófák; meteorológiai jellegű károk);
- civilizációs, ipari katasztrófák: (nukleáris balesetek, veszélyes anyagok kikerülése, közlekedési balesetek);
- fegyveres konfliktusok: háborúk; fegyveres csoportok támadása, belső fegyveres konfliktusok, polgárháborúk, sztrájk;
- terrorizmus: (robbantások, támadások intézmények, távvezetékek, hírközpontok, internet szolgáltatók ellen, kulcsfontosságú személyek kiiktatása); bűnözés (adatok erőszakos megszerzése, irányítási rendszerek működésének befolyásolása, megbénítása).
- Információs támadások.

E veszélyek és támadások jellemzője, hogy szerteágazóak, komplexen jelentkeznek, hatással lehetnek nemcsak egyes infrastruktúraelemre, hanem a komplexitásból adódóan bénítani képesek kormányzati vagy nemzetközi szintű rendszerek és infrastruktúrák működését, ezért védelmükkel globálisan kell foglalkozni.

Az önkormányzatoknak a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvényben meghatározottak szerint a polgárivédelem terén a polgármesternek kiemelt feladatai vannak, és e kötelezettsége az önkormányzatok számára kötelező feladatként az Mötv. rendelkezései között is megjelenik. A települések katasztrófavédelmi

besorolásától függően a helyi kormányzásnak jelentős feladatai vannak a megelőzés, védekezés és helyreállítás során. A katasztrófavédelmi törvény egyértelműen fogalmaz: „Minden állampolgárnak, illetve személynek joga van arra, hogy megismerje a környezetében lévő katasztrófaveszélyt, elsajátítsa az irányadó védekezési szabályokat, továbbá joga és kötelessége, hogy közreműködjön a katasztrófavédelemben.” [74 1. § (2)]

A polgárivédelem terén a polgármesterek, jegyzők és közbiztonsági referensek felkészítésének pontosan kimunkált és kiérlelt rendszere működik, támaszkodva az OKF országos szervezetére és szakértelmére. Az első két veszélyességi fokozatba sorolt [69] településeken települési közbiztonsági felelősök kerülnek kijelölésre, akik kötelezettek a közbiztonsági referensi tanfolyam elvégzésére. Fő feladata, hogy segítse a polgármestert polgárivédelmi feladatainak ellátásában. A referens feladatai kiterjednek a felkészülés, a védekezés és a helyreállítás időszakára. Szakmai irányítását, felkészítését és képzését az OKF biztosítja (a közbiztonsági referensképzés kivonata a 7. melléklet).

A Katasztrófavédelmi törvény meghatározása szerint illetékességi terület és hatáskör szerint megkülönböztethető a nemzeti, a megyei és a helyi szint. A megyei védelmi bizottság elnöke évente meghatározza a polgármesterek felkészítésével kapcsolatos feladatokat. A helyi szintű igazgatás a polgármester útján valósul meg. A polgármesterek a megelőzés időszakában felelősek a veszélyelhárítási tervek elkészítéséért, valamint a helyi lehetőségek figyelembevételével a védekezés feltételeinek a biztosításáért, illetve a védekezésre való felkészülésért. [49 pp.72-84]

Az OKF megyei Polgári védelmi Főfelügyelőinek a feladata a közigazgatási vezetők, polgármesterek, jegyzők katasztrófavédelmi felkészítése, a megyei és helyi szervezetek felkészítésével kapcsolatos tevékenységek szervezése, koordinációja és szakmai felügyelete.

Az érintett önkormányzatoknak közbiztonsági felelőst kell alkalmazniuk, továbbá kötelező, gyakorlatorientált képzéseken kell részt venniük. Jelenleg a közbiztonsági referensek képzései a hagyományos katasztrófahelyzetekhez kapcsolódó védekezésre és a helyreállításra koncentrálnak, nem részük az információs társadalomból és a kibertérből érkező esetleges fenyegetésekre és kezelésükre való felkészülés.

Meglátásom szerint az információbiztonság, az információ- és kiberbiztonság biztosításához a meglévő közszolgálti képzéseket hasonló gyakorlatra koncentráló felkészítő képzésekkel lenne szükséges kiegészíteni.

Összegzés

Az önkormányzatok infraszuverén szinten elhelyezkedő autonómiák; választással jönnek létre, működésük komplex, és saját ügyekben önálló döntési jogosultsággal rendelkeznek. A kormány csak felügyeleti jogkört gyakorolhat felettük. A helyi önkormányzatok kettős céllal működnek: gyakorolják a helyi közhatalmat és intézik a helyi közügyeket.

A helyi önkormányzatok feladatait a differenciált feladattelepítés elvével összhangban az Mötv. határozza meg. A feladatok jelentős része a kritikus infrastruktúrák köréhez is kapcsolódik, amelyek egyben kritikus információs infrastruktúrák is.

Nagyon fontos szabály, hogy az önkormányzat számára feladat- és hatáskört kizárólag törvény állapíthat meg. A másik követelmény, hogy a helyi önkormányzat a kötelező feladat- és hatáskörellátáshoz, azokkal arányban álló költségvetési, illetve más vagyoni támogatásra jogosult.

A magyar településszerkezet alapvetően aprófalvas. Annak ellenére, hogy minden település rendelkezik a helyi önkormányzás jogával, nem minden esetben biztosítottak a helyi hatalomgyakorlás feltételei. Ezt a problémát hivatott orvosolni a differenciált feladattelepítés stratégiája, ami szerint a feladat- és hatáskör telepítésekor a törvény köteles figyelembe venni a feladat- és hatáskör jellegét, a helyi önkormányzatok eltérő adottságait, különösen a gazdasági teljesítőképességet, a lakosságszámot és a közigazgatási terület nagyságát.

Az ágazati jogszabályok többségében figyelembe veszik a differenciált feladattelepítés elvárását, azonban sok esetben – az önkormányzati működés nem teljes körű ismeretéből fakadóan – az ágazati feladat telepítésekor a tervezés elnagyolt, nem eléggé kidolgozott.

Az önkormányzati feladatok ellátása az önkormányzati hivatalon keresztül működik. A hivatal lehet önálló vagy több önkormányzat által létrehozott közös önkormányzati hivatal. A polgármesteri hivataloknak nincs döntési kompetenciája annak ellenére, hogy a helyi közszolgáltatások színvonalas biztosításának záloga a felkészült apparátus.

Az EIB továbbképzések a közszolgálati képzési rendszer részévé váltak, azonban elsősorban az elméleti képzési módszereket alkalmazzák, az újszerű, gyakorlatorientált módszerek térnyerése még várat magára ezen a területen. A közszolgálati alapképzés rendszerében gondolati szinten már megjelenik az információbiztonság, bár a fókusza jelenleg a minősített adatokhoz kötődik.

Az Ibtv. több kötelező feladatokat ír elő az önkormányzatok számára, továbbá nem differenciáltan telepítette a feladatokat, és nem rendelt a teljesítéshez elégséges forrást. Az Ibtv. elvárása – többek között – az IB felelős kijelölése, az információs rendszerek biztonsági osztályba sorolása, a szervezet biztonsági szintjének megállapítása és a szükséges szabályzatok létrehozása.

2017 nyaráig az önkormányzatok kevesebb, mint 30%-a szolgáltatott adatot, és alig negyede regisztrált IB felelőst, vagy nyújtot be biztonsági szabályzatot. Továbbá az információs rendszerek osztályba sorolása alig egyötödük esetében történt meg. A 2018 elején végzett online felmérés adatai e számoknál valamivel kedvezőbb képet festenek, de nem térnek el jelentősen a NEIH adataitól. A szabályozottsági kérdések vizsgálata esetében látható, hogy az információbiztonság, az adatkezelés többé-kevésbé szabályozott, azonban a legjobban teljesítő önkormányzatok esetében is alig több, mint egynegyedüktől érkezett az a válasz, hogy van egy esetleges kibertámadás bekövetkeztére protokoll. Ez arra utal, hogy a válaszadók többsége nem tartja valós veszélynek egy kibertámadás bekövetkezését.

Az önkormányzatoknak – egyéb feladataikon túl – az információs társadalomban is több elvárásnak kell megfelelniük. Az egyik az Infotv. elvárása, miszerint az önkormányzatok tegyék közzé a közérdekű és a közérdekből nyilvános adataikat honlapjukon. Mind az NVSZ, mind a BM saját kutatása szerint ennek a követelménynek az önkormányzatok nem felelnek meg. Egyrészt a

leterheltség és a kapacitáshiány miatt, másrészt azért, mert az Infotv. nem vette figyelembe a differenciált feladattelepítés előírásait.

Az uniós és a hazai stratégiákban – a reziliencia növelése és a kiberbiztonság erősítése érdekében – kiemelt helyen szerepel a kompetenciák fejlesztése, az informatikai oktatás átalakításának szükséglete és a tudatosság növelése. A különböző stratégiai dokumentumok helyzetelemzése és a szakértői vélemények egybehangzóan állítják, hogy ezen a területen még jelentős hátránnyal kell megküzdenünk. A beavatkozásra vonatkozóan csak koncepcionálisan áll rendelkezésre elképzelés, ami nem túl biztató, különös tekintettel a terület fejlesztésének időigényére.

4. ÖNKORMÁNYZATOK KIBERBIZTONSÁGI HELYZETÉNEK ÉS ONLINE KÉPESSÉGÉNEK VIZSGÁLATA

A negyedik fejezetben az empirikus kutatás eredményei kerülnek részletes bemutatásra.

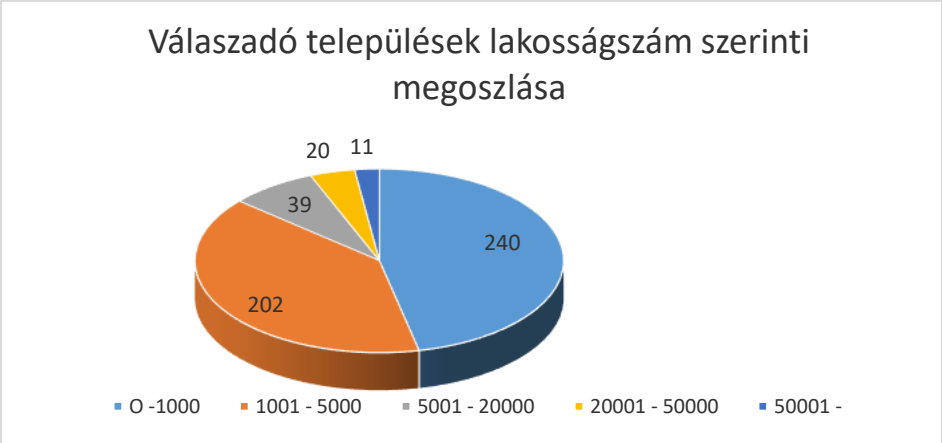
4.1. Online kérdőíves felmérés

A nemzetközi és hazai tapasztalatok, szabályozás és trendek alapján egybehangzóan és egyértelműen azonosítható, hogy az emberi tényező szerepe, felkészültsége, tudatossága meghatározó a kiberbiztonság kérdéskörében. Erre a területre vonatkozóan – tudomásom szerint – nem készült felmérés sem az egész közszférában, sem pedig önkormányzati körben. Megállapítások tételéhez javaslatok megfogalmazására van szükség; elengedhetetlennek tartottam felméri az elméleti és a szabályozási keretek felhasználásával az önkormányzati vezetők és munkatársak: az önkormányzatok kiberbiztonsággal kapcsolatos attitűdjeit, felkészültségét és gyakorlatát.

4.1.1. A kérdőív háttere

Az önkormányzatok kiberbiztonsági kérdéseinek vizsgálatához 2018. január elején – a tesztelést követően – a teljes önkormányzati kör részére elektronikus úton került kiküldésre a kérdőív, amire 2018. február 13-ig 512 válasz érkezett. A kitöltés önkéntes és anonim volt. A kérdőív kérdéseinek leírása az 3. mellékletben található. A felmérés egy adminisztratív és három tartalmi blokkra különült el. Az első blokk a kitöltőkre vonatkozó alapadatokat tartalmazza, míg a másik három az önkormányzatok kiberbiztonsági kérdéseivel foglalkozik. A szakmai blokkok összeállítása során a célom az volt, hogy átfogó képet kapjak az önkormányzatok kiberbiztonsági kérdésekhez való viszonyulásáról, felkészültségéről és működési gyakorlatáról a beérkezett válaszokon keresztül. Az anonimitás miatt a válaszadó települések adóerő-képességét nem tudtam hozzárendelni az egyes válaszokhoz, így gazdasági helyzet szerinti vizsgálatra nem volt mód. A beérkezett válaszok érékelése során vizsgáltam, hogy mi a jellemző az egyes kérdésekre adott válaszokra a települések lakosságszáma és a település hivatal típusa szerint: Ahogyan a harmadik fejezetben láthattuk a magyar település szerkezet elaprózódott, jelentős számú alacsony lélekszámú településsel. A 11. ábrán láthatjuk, hogy a válaszadók közel 40 %-a az 1000 fő lakosságszám alatti települések közül kerül ki.

Ahogy az előbbiekben már szó volt arról, hogy a magyar településszerkezet alapvetően aprófalvas és a diagrammból láthatjuk is, hogy a településszerkezeti arányok tükröződnek a válaszadó települések lakosságszám szerinti megoszlásában is.

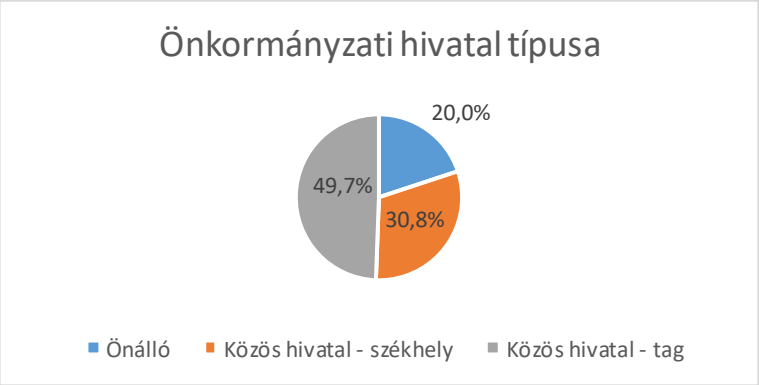


11. ábra

Válaszadó települések megoszlása lakosságszám szerint (elemszám 512)

Forrás: Önkormányzatok és kiberbiztonság – online felmérés (saját szerkesztés).

Az önkormányzatok operatív munkaszervezete a polgármesteri hivatal, ahol az információbiztonsággal kapcsolatos feladatok ellátása is történik. Ezért volt fontos a kérdőívben is rákérdezni, hogy a működést biztosító szervezetek hogyan látják, teljesítik a kiberbiztonsággal kapcsolatos elvárásokat, mennyire tartják fontosnak, mi a véleményük. A 12. ábrán láthatjuk, hogy a válaszok 50%-a közös hivatal tag önkormányzatától, 30%-a közös hivatal székhelyéből és 20%-a önálló önkormányzati hivatalból érkezett. Ez nagyságrendileg megfelel az önkormányzati hivatalok megoszlásának.

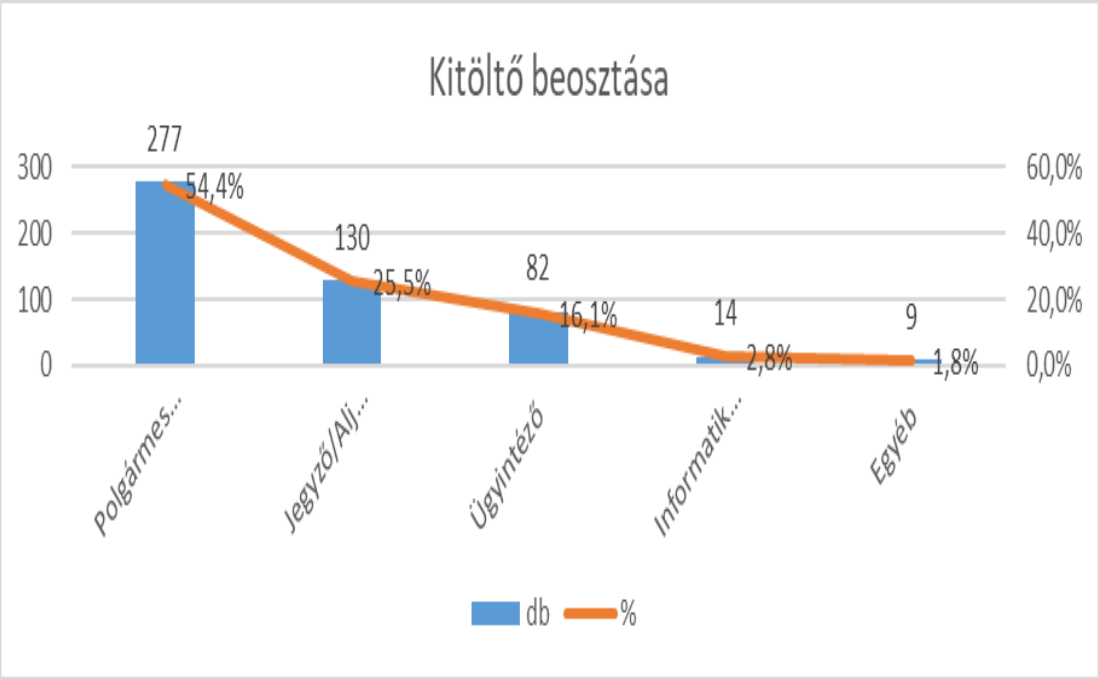


12. ábra

Válaszadó települések megoszlása önkormányzati hivatalok típusa szerint (elemszám 512)

Forrás: Önkormányzatok és kiberbiztonság – online felmérés (saját szerkesztés).

A közszféra szervezetekben a vezető szerepe elköteleződése jelentős hatással van a feladatok ellátására, motivációjára. A 13. ábrán látható, hogy a válaszadók több, mint 50 %-a tölt be vezető szerepet a válaszadó önkormányzaton belül.



13. ábra

Válaszadók megoszlása a szervezetben betöltött pozíciójuk szerint

Forrás: Önkormányzatok és kiberbiztonság – online felmérés (saját szerkesztés).

A kitöltők megoszlása azt mutatja, hogy a felmérést a legnagyobb számban a települési polgármesterek/alpolgármesterek töltötték ki, és ezt követően az önkormányzati hivatalvezető jegyzők/aljegyzők és hivatali dolgozók. Informatikai szakemberek és egyéb munkatársak elenyésző létszámban. A polgármesterek nagy száma valószínűleg a nagyszámú kistelepülési válaszadói számmal van összefüggésben.

4.1.2. A kérdőív feldolgozásának módszerei

A kérdőívre adott válaszok értékelése a kérdések jellegétől függően leíró statisztikai, matematikai statisztikai módszerekkel és a szöveges válaszok esetében egyszerű összegzéssel készült.

A három szakmai blokk az önkormányzati válaszadók véleményét, az információbiztonsággal kapcsolatos tudatosságát hivatott felmérni.

Az első szakmai blokk a kibertérrel, kiberbiztonsággal kapcsolatos vélemények összegyűjtését célozta. Arra kerestem a választ, hogy

- mennyire tartják veszélyesnek és valószínűnek egy kibertámadás bekövetkezését,
- mennyire, mely területen és milyen mértékben tartják sebezhetőnek az önkormányzati rendszereket,
- a felkészülés során milyen beavatkozásokat preferálnak.

A második szakmai blokk az önkormányzatok felkészültségéről, kiberbiztonsági kompetenciájáról alkotott vélemények feltárását tűzte ki célul. Ennek keretében arra kértem a válaszadókat, hogy nyilatkozzanak: véleményük szerint a különböző kiberbiztonsági helyzetekben mi jellemző az

önkormányzatra, illetve e rész második kérdésében a szervezet meglévő információbiztonsági képességét, felkészültségét kértem minősíteni.

A harmadik szakmai blokk a működési tapasztalatok felmérése érdekében került a kérdéssorba.

Főkomponens analízis

A kérdőív arra alkalmas részeit matematikai statisztikai elemzésnek vetettem alá, ehhez az SPSS programot használtam. A sok változóra való tekintettel a kérdőív elemezni kívánt függő változóinak a korrelációját PCA (Principal Component Analysis) segítségével elemeztem, amely során varimax rotációt használtam. Az elemzett változók többsége Likert-skálás volt, de előfordultak köztük egyszerű választásos kérdések is (PCA-ba bevont változókat az 5. melléklet tartalmazza). A főkomponensek számát a scree plot ránézeti képe alapján állapítottam meg (ahol éles törés volt a grafikonon), figyelembe véve az Eigenvalue >1 szabályt. Mivel az elemzésbe bevont változók mindegyike egyértelműen ült valamelyik főkomponensen legalább 0,484-es súllyal, ezért további szelekciós lépések használatára nem volt szükség. Ezt követően kiszámoltam főkomponensenként a Cronbach's alpha értékét, ami megmutatja, hogy mennyire erősen függenek össze az adott főkomponenshez tartozó változók. Az eredményeket 5. táblázat tartalmazza. A kapott főkomponenseket a továbbiakban általános lineáris modellel (GLM, General Linear Model) elemeztem.

GLM

A főkomponens analízis után normalitásvizsgálatot végeztem. A reziduálisok eloszlásának megállapításánál a Kolmogorov-Smirnov teszt eredményét és a Q-Q plotot vettem figyelembe. Ahol ellentmondás volt a kettő között, ott a Q-Q plot vizuális analízise alapján döntöttem (mennyire illeszkednek a pontok az egyenesre – minél jobban, annál inkább normál az eloszlás).

Mindegyik változó/reziduális normál eloszlású volt, így ezek mindegyike alkalmas volt a GLM típusú analízisre, a statisztika feltételeit teljesíti. Első lépésként minden főkomponensre kiszámoltam a faktorértékeket (factor score), ezeket tekintettem függő változónak az elemzés során. Független változóként a lakosságszámot (fő), a hivatal típusát, és a település típusát használtam (6. melléklet), emellett a lakosságszám és a településtípus interakcióját is betettem mind az öt modell esetében. A független változók esetében feltételeztem, hogy a lakosságszám növekedésével növekszik a település anyagi és szervezeti függetlensége, illetve a képessége a kiberbiztonsági kockázatok kezelésére. A települési jogállás tekintetében pedig a városi jogállás esetében is nagyobb függetlenséget és kompetenciát feltételeztem, ezért választottam ezeket a változókat. (A független változók elemszám alapján alkalmasak voltak a GLM típusú analízisre, 6. melléklet). A modellszelekció során backward szelekciós lépéseket alkalmaztam, szignifikánsnak azokat a változókat tekintettem, ahol $p \leq 0{,}05$. A végleges modellek eredményeiből boxplotokat készítettem, majd Tukey-féle post hoc tesztet végeztem.

Eredmények

Az elemzés eredményeként 5 főkomponenst kaptam. A teljes, magyarázott variancia 58,55%.

Az 4. táblázatban láthatjuk a főkomponensekhez tartozó kérdéseket és a hozzájuk tartozó súlyokat, a variancia %-át és a Cronbach's α-t.

4. táblázat

A főkomponens analízis eredményei Forrás: saját szerkesztés.

Főkomponens	Főkomponens elemei	Súly	Magyarázott variancia %	Chronbach's α
Felkészültség, képesség	jellemzo1	0,745	18,07	0,919
	jellemzo2	0,791		
	jellemzo3	0,730		
	jellemzo4	0,825		
	jellemzo5	0,767		
	jellemzo6	0,799		
	jellemzo7	0,838		
	jellemzo8	0,835		
Önkormányzatok kiberfenyegetettségének megítélése	kiber1	0,657	16,09	0,879
	kiber2	0,772		
	kiber3	0,720		
	kiber4	0,780		
	kiber5	0,680		
	kiber6	0,748		
	kiber7	0,709		
	veszelyes	0,656		
Sebezhetőség	sebezheto1	0,772	11,60	0,906
	sebezheto2	0,809		
	sebezheto3	0,780		
	sebezheto4	0,773		
	sebezheto5	0,719		
Védekező / reagáló képesség	kotelezettseg3	0,638	7,40	0,644
	kötelezettseg4	0,532		
	kötelezettseg5	0,542		
	kötelezettseg6	0,646		
	kötelezettseg7	0,655		
	protokoll	0,484		
Szabályozás rendelkezésre állása	kötelezettseg1	0,692	5,40	0,501
	kötelezettseg2	0,711		

GLM

Minden főkomponens esetén elvégeztem a GLM-et, így megtudtam, hogy a főkomponensek értékeit mely független változók befolyásolják. A GLM-ek ereményét a 5. táblázatban foglaltam össze.

5. táblázat

A GLM analízisek eredményei Forrás: saját szerkesztés.

Felkészültség, képesség			
változó	F	df, error: 505	p
lakos	3,030	4	0,017
hivatal	4,299	2	0,014
Önkormányzatok kiberfenyegetettségének megítélése			
változó	F	df, error: 507	p
lakos	3,886	4	0,004
Sebezhetőség			
változó	F	df, error:	p
-	-	-	-
Védekező / reagáló képesség			
változó	F	df, error:	p
-	-	-	-
Szabályozás rendelkezésre állása			
változó	F	df, error: 509	p
hivatal	33,055	2	0,000

4.2. Az online felmérés eredményeinek elemzése

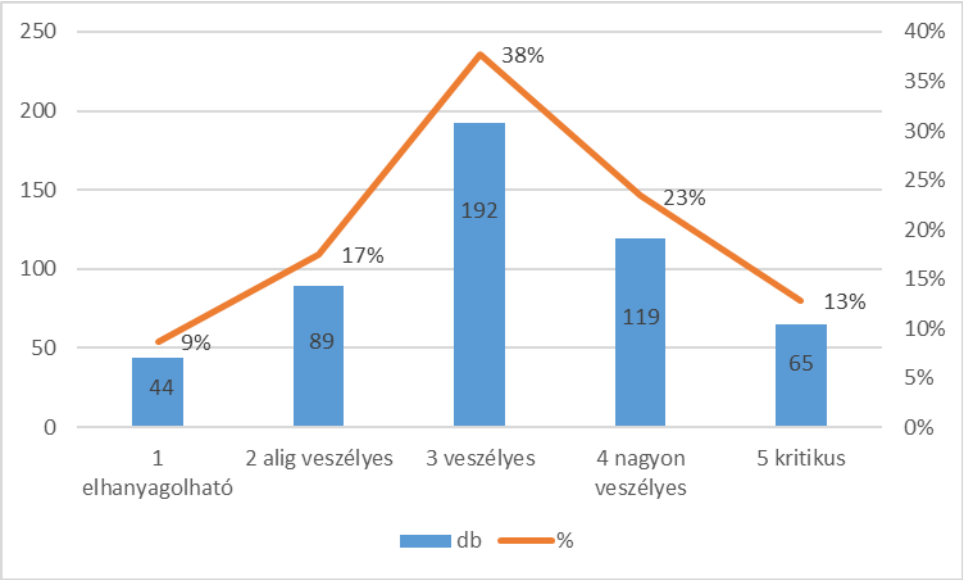
A különböző elemzési módszerek részletes eredményét nem külön-külön, hanem az alábbiakban az egyes szakmai blokkokban vegyesen mutatom be.

4.2.1. Vizsgált terület (I.): kibertér – kiberbiztonság – az önkormányzatok kiberfenyegetettsége

A kérdőív *Kibertér – kiberbiztonság* részében, a felmérés első szakmai blokkjában arra kerestem a választ, hogy a felmérést kitöltők az önkormányzat szempontjából mennyire tartják veszélyesnek egy lehetséges kibertámadást, az egyes területeken milyen valószínűséggel feltételeznek kibertámadás bekövetkezését, illetve a megadott hivatali területeket mennyire tartják sebezhetőnek. A válaszadók véleményt nyilváníthattak, hogy a kiberbiztonsági felkészülés során szerintük a védekezés, az elrettentés vagy a fejlesztés-e a legfontosabb.

Első kérdés és a válaszok eredményei:

Az első kérdés egy lehetséges kibertámadás bekövetkezésekor annak veszélyességére kérdezett rá. Az egyes hivatalok részéről kapott válaszok egy közel egyenleges eloszlást mutatnak, és a válaszadók közel kiegyenlítetten tartják jelentősen veszélyesnek, illetve közel ugyanannyian elhanyagolhatónak egy kibertámadás bekövetkezését.



14. ábra

A kibertámadás bekövetkezésének veszélyessége

Forrás: saját szerkesztés.

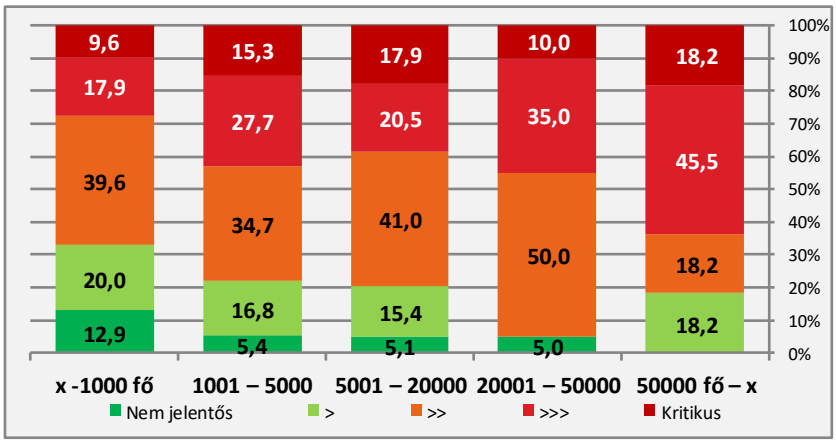
A számok további vizsgálata azt mutatja, hogy az egyenletes eloszlás csak az összes válasz egyben kezelése esetén igaz. Ha hivataltípus bontásban nézzük, akkor azt láthatjuk, hogy az önálló hivatalok 90%-a, a közös hivatal székhely önkormányzatai 70%-ban, míg a közös hivatal tagok 50%-ban tarják csak közepes vagy annál jelentősebb veszélynek. Az önkormányzati hivatalok típusa szerinti megbontásnál az önálló hivatalok és a közös székhely önkormányzatok inkább ítélték veszélyesnek, sőt közel 15%-ban kritikusnak egy ilyen incidens bekövetkezését.

6. táblázat

A kibertámadás bekövetkezésének veszélyessége Forrás: saját szerkesztés.

Közigazgatási-feladatellátási státusz	Egy kibertámadás bekövetkezésének veszélyessége (skála)											
	1. Nem jelentős		2. <		3. <<		4. <<<		5. Kritikus		Σ	
	db	%	db	%	db	%	db	%	db	%	db	%
Önálló	6	*5,9*	9	*8,8*	39	*38,2*	33	*32,4*	15	*14,7*	*102*	*100,0*
Közös hivatal	7	*4,5*	33	*21,0*	55	*35,0*	39	*24,8*	23	*14,6*	*157*	*100,0*
Közös hivatal tag	32	*12,6*	48	*19,0*	99	*39,1*	47	*18,6*	27	*10,7*	*253*	*100,0*
Összesen	*45*	*8,8*	*90*	*17,6*	*193*	*37,7*	*119*	*23,2*	*65*	*12,7*	*512*	*100,0*

A válaszokat a települések *lakosságszáma* szerint csoportosítva azt láthatjuk, hogy minél nagyobb egy település, annál kevésbé becsüli alá egy kibertámadás bekövetkezésének veszélyét.
Azon települések, amelyek alig veszélyes vagy elhanyagolható veszélynek tartják egy kibertámadás bekövetkeztét a teljes válaszadói kör 30%-a, és alapvetően közös hivatal tagjai és aprófalvas települések.



15. ábra

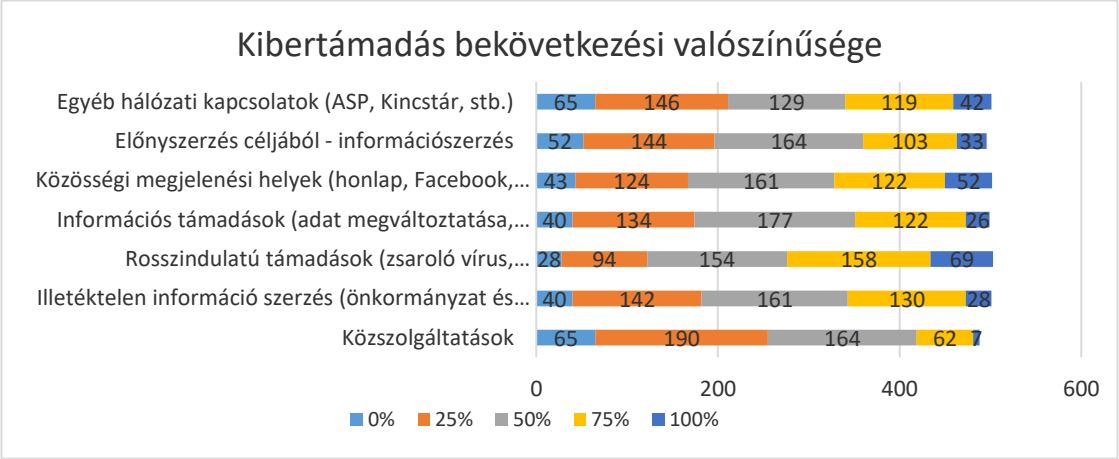
A kibertámadás bekövetkezésének veszélyessége lakosságszám-kategóriák szerint

Forrás: saját szerkesztés.

A települések lakosságszámának növekedése együtt jár a kibertámadások bekövetkezésének enyhébb veszélyt jelentő besorolásaival, és emellett fokozatosan kezd el növekedni azon vélemények aránya is, amelyek komoly problémaként, súlyos és/vagy kritikus fokú veszélyességgel társítják egy támadás bekövetkezését.

Második kérdés és a válaszok eredményei:

A következő kérdés a kibertámadások bekövetkezési valószínűségére kérdezett rá hét megjelenési terület szempontjából: közszolgáltatások, illetéktelen információszerzés (önkormányzat és a lakosok adatai), rosszindulatú támadások (zsarolóvírus, rendszerbénítás), információs támadások (adat megváltoztatása, rémhírterjesztés, egyéb), közösségi megjelenési helyek (honlap, Facebook, stb.) támadása, előnyszerzés céljából való információszerzés, egyéb hálózati kapcsolatok (ASP, Kincstár, stb.).



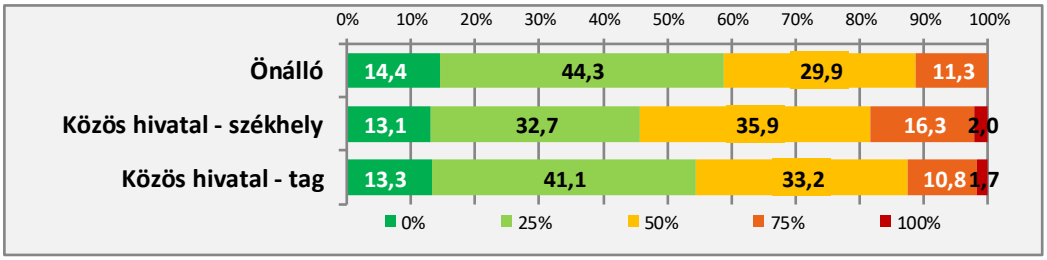
16. ábra

Adott területen egy kibertámadás bekövetkezési valószínűsége (összefoglalás)

Forrás: saját szerkesztés..

Az áttekintő ábrán jól látszik, hogy a minden elem esetében van (28–65) számos település, ahol a válaszadó kizárja, hogy ilyen típusú kibertámadás bekövetkezhetne az ő településén. A legnagyobb valószínűséggel a rosszindulatú támadások bekövetkezését jelzik, ebben az esetben a „100%-ban biztos, hogy be fog következni" válaszok száma is jelentős, de ebben az esetben is van 28 válaszadó, aki kizárja a támadás előfordulását. Érdekes képet mutatnak továbbá a közszolgáltatások elleni támadásokra vonatkozó válaszok.

A közszolgáltatások területén a kibertámadások bekövetkezésének valószínűségét a hivatali kategóriák mindegyikében elveti egy jelentős hányad (13,3–14,4%). Emellett mind a három kategóriában a hivatalok legalább 70%-a a támadás valószínűségét 25–50% közé becsülte, azaz igen alacsonynak tartja ezt a lehetőséget.

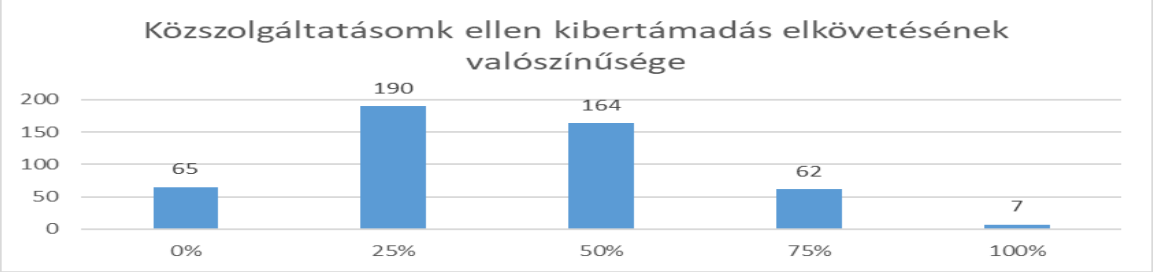


17. ábra

Kibertámadás bekövetkezésének valószínűsége a közszolgáltatások esetében

Forrás: saját szerkesztés.

A közös működésben érintett hivatalok válaszai hasonlítanak egymásra, a 25%-os bekövetkezési valószínűséget a kirendeltséghivatalok becsülték meg nagyobb arányban, míg a székhelyként funkcionáló hivatalok a legalább 75%-os előfordulási gyakoriságot jelölték meg fajsúlyosabban a tag hivataloknál. A fenti megállapítást – miszerint a közszolgáltatások területén a támadások bekövetkezésének esélye jelentősebb a közös hivatalok esetében – alátámasztja a települések lakosságszáma szerinti vizsgálódás is, hiszen a legfeljebb 5000 fős települések hivatalai azok, amelyek a szándékos incidensek bekövetkezésének lehetőségét a legnagyobb arányban becsülték meg. Függetlenül a lakosságszámtól, bármely település önkormányzati hivatalára az jellemző, hogy 10-ből legalább 7 esetben a támadások bekövetkezésének valószínűségét 25–50%-osra becsülték meg.



18. ábra

Közszolgáltatások elleni kibertámadás bekövetkezésének valószínűsége (összegezve)

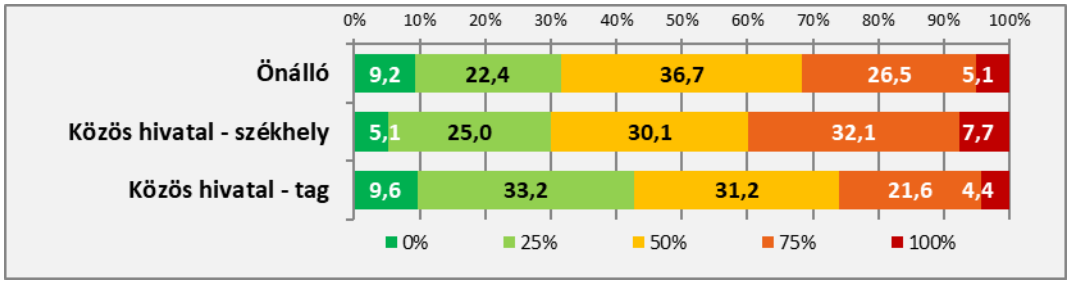
Forrás: saját szerkesztés

Az ábrán látható, hogy 65 válaszadó (hivataltípustól függetlenül, közel azonos arányban) egyáltalán nem tartja elképzelhetőnek egy, a közszolgáltatások ellen bekövetkező kibertámadást.

Ez azért érdekes – és komoly problémaként fogalmazható meg már önmagában is –, mert a válaszadók összetételét vizsgálva láthatjuk, hogy válaszok közel 80%-a településvezetőtől érkezett.

Harmadik kérdés és a válaszok eredményei:

A kibertámadások bekövetkezésének valószínűsége az *illetéktelen információszerzés* céljából a következőképpen alakult. Legkevésbé tartanak ettől a taghivatalok: minden huszadik esetben jelölték meg a 0%-os esélyt az előfordulásra. Ez az arány önállóan és a székhelyként működő hivatalok esetében ennek a duplája (9,2–9,6%). Az utóbbi kategória viszont emellett a leggyakrabban bejelölte ennek ellentétét is, vagyis teljesen biztosak annak előfordulásában.

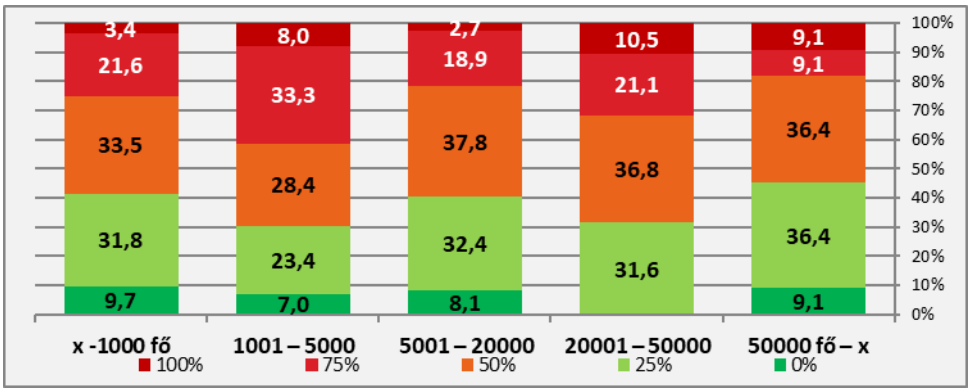


19. ábra

Kibertámadás bekövetkezésének valószínűsége illetéktelen információszerzés céljából

Forrás: saját szerkesztés.

Az önállóan működő hivatalok esetében a legmagasabb, az 50%-os bekövetkezési lehetőséget becslők aránya, emellett jelentős az ennél nagyobb mérvű előfordulással számolók aránya is.
A székhelyhivatalok rendelkeznek a legkisebb (0%), illetve legnagyobb (100%) szélsőértékekkel, illetve ebben a típusban minden harmadik hivatal jelölte meg 75%-osnak az incidens bekövetkezésének a lehetőségét.
A kirendeltségként tevékenykedő hivatalok esetében pedig megállapítható, hogy összességében a legkevésbé tartanak a bekövetkezés lehetőségétől, hiszen legnépesebb kategóriáik a 0–50%-os előfordulási szint, illetve legkevésbé jellemző kategóriáik az ennél magasabb arányú előfordulásokra illeszthetők.
A településszintű (lakosságszám szerinti) vizsgálat valamelyest más értékeket is mutat, illetve árnyalja az előbbi megállapításokat. A kisebb települések hivatalaira jellemző leginkább, hogy hisznek az incidensek legalább 75%-os előfordulási valószínűségében, ezen belül is az 1001–5000 fő közötti lakosságszámú településekre állapítható meg legfőképpen ez, ahol tízből négy hivatal nyilatkozott ehhez hasonlóan. Ez az arány duplája az 50 000 főnél népesebb települések hivatalainak adatainál (18,2%).



20. ábra

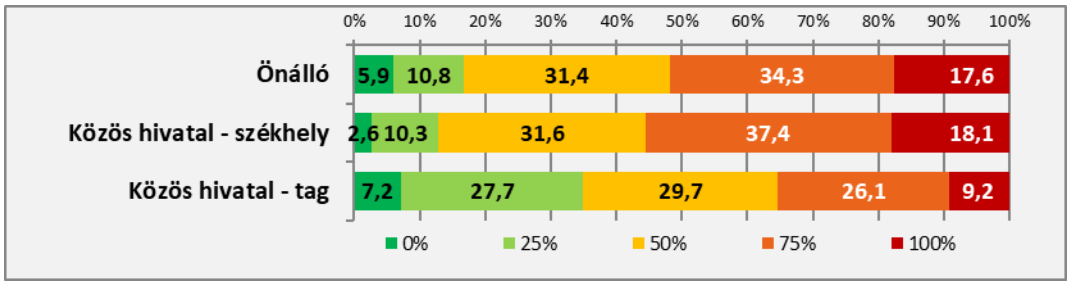
Kibertámadás bekövetkezésének valószínűsége illetéktelen információszerzés céljából lakosságszám-kategóriák szerint

Forrás: saját szerkesztés.

Az 5001–20 000 fős lakosságszám esetén pedig a települési hivatalok válaszaiból valamiféle középszerűség derül ki, inkább átlagos adatokat láthatunk, bár az 50%-os előfordulási arány itt a legjellemzőbb.

Negyedik kérdés és a válaszok eredményei:

A különböző *rosszindulatú támadások bekövetkezésének lehetősége* a legkisebb mértékű a székhelyhivatalok dolgozói szerint. Ezt támasztja alá, hogy ebben a kategóriában a legnagyobb arányú az előfordulást kizáró, illetve legalacsonyabb a 100%-os bekövetkezést prognosztizáló válaszolók aránya.



21. ábra

Kibertámadás bekövetkezésének valószínűsége rosszindulatú támadás céljából

Forrás: saját szerkesztés.

A közigazgatási feladatellátási státusz komplexitásának növekedésével párhuzamosan növekszik a nagyobb súlyú előfordulási lehetőségek aránya, az önálló és székhelyként működő hivatalok esetében is duplája a rosszindulatú támadások bekövetkezésének a kizárólagossága, mint a közös hivatali működésben tagként megjelenő hivataloknál.

A települések lakosságszáma alapján is bizonyítható egy fenti megállapítás: a kis(ebb) lélekszámú településeken tartanak legkevésbé a rosszindulatú támadások bekövetkezésétől – az 1000 fő alatti településeknek közös hivatalon belül, és nagy valószínűséggel kirendeltséghivatalként kell működniük.

7. táblázat

Kibertámadás bekövetkezésének valószínűsége rosszindulatú támadás céljából lakosságszám-kategóriák szerint Forrás: saját szerkesztés.

Lakosságszám-kategóriák (fő)	Egy kibertámadás bekövetkezési valószínűsége rosszindulatú támadások céljából/lakosságszám											
	0%		25%		50%		75%		100%		Σ	
	db	%	db	%	db	%	db	%	db	%	db	%
0 –1000	16	*6,8*	64	*27,1*	76	*32,2*	59	*25,0*	21	*8,9*	*236*	*100,0*
1001 – 5000	6	*3,0*	25	*12,5*	60	*30,0*	68	*34,0*	41	*20,5*	*200*	*100,0*
5001 – 20000	3	*7,7*	5	*12,8*	10	*25,6*	16	*41,0*	5	*12,8*	*39*	*100,0*
20001 – 50000	1	*5,0*	1	*5,0*	6	*30,0*	11	*55,0*	1	*5,0*	*20*	*100,0*
50000 – x	2	*18,2*	1	*9,1*	3	*27,3*	4	*36,4*	1	*9,1*	*11*	*100,0*
Összesen	*28*		*96*		*155*		*158*		*69*		*506*	*100,0*

A települési lakosságszám emelkedésével párhuzamosan a hivatalok feladatellátási státusza és közszolgáltatási szerepe is növekszik, emellett pedig megnő a támadások bekövetkezési valószínűségének az aránya is.

Ötödik kérdés és a válaszok eredményei:

Az információs rendszer elleni támadások esetében a bekövetkezés 50%-os aránya minden hivatal tekintetében legalább 30%-os, emellett legkevésbé tartják valószínűnek az előfordulásukat a taghivatalok, a székhelyhivatalok pedig ezzel ellentétben a leginkább látják reálisnak azt, hogy csaknem biztosan, vagy akár elkerülhetetlenül előfordul ilyen célú incidens.

8. táblázat

Kibertámadás bekövetkezésének valószínűsége az információs rendszer ellen Forrás: saját szerkesztés.

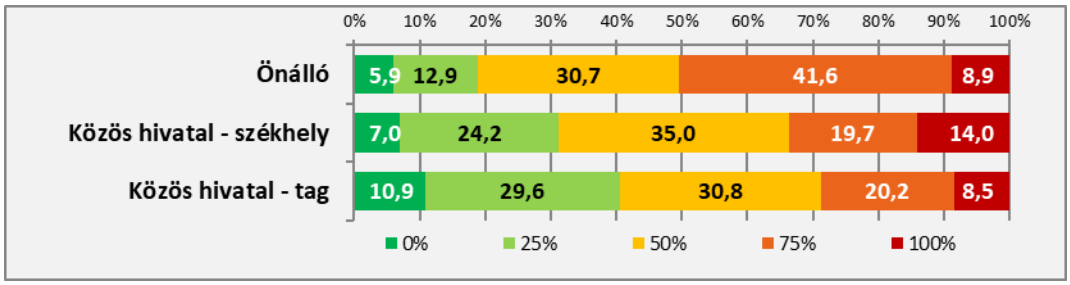
Közigazgatási feladatellátási státusz	Kibertámadás bekövetkezésének valószínűsége (%)											
	0%		25%		50%		75%		100%		Σ	
	db	%	db	%	db	%	db	%	db	%	db	%
Önálló	8	*8,0*	25	*25,0*	36	*36,0*	29	*29,0*	2	*2,0*	*100*	*100,0*
Közös hivatal	9	*5,7*	29	*18,5*	66	*42,0*	41	*26,1*	12	*7,6*	*157*	*100,0*
Közös hivatal tag	23	*9,4*	82	*33,6*	76	*31,1*	51	*20,9*	12	*4,9*	*244*	*100,0*
Összesen	*40*	*8,0*	*136*	*27,1*	*178*	*35,5*	*122*	*24,3*	*26*	*5,2*	*502*	*100,0*

A középértékekhez leginkább az önállóan működő hivatalok értékei közelítenek, gyakorlatilag minden lehetséges válasz (arány) esetében az adataik a közös hivatalok – szereptől függetlenül – mutatói közé ékelődnek.

A kistelepüléseken működő hivatalok munkatársainak becslése mutat rá leginkább a támadások mérsékelt bekövetkezésére, viszont a települések méretének növekedésével a bekövetkezések valószínűségének fokozódása figyelhető meg. Ez alól kivételt képeznek az 50 000 főnél népesebb városok, ahol a legkisebb településekre jellemző mutatók is felülíródnak, így megállapítható, hogy az itt működő hivatalok tartanak legkevésbé az információs támadások bekövetkezésétől.

Hatodik kérdés és a válaszok eredményei:

A hivatalok *közösségi megjelenési helyeit érintő kibertámadások bekövetkezése* szempontjából a válaszoló hivatalokra igaz, hogy közülük minden harmadik közepesnek, azaz 50%-osnak becsüli meg az ilyen incidensek bekövetkezését.



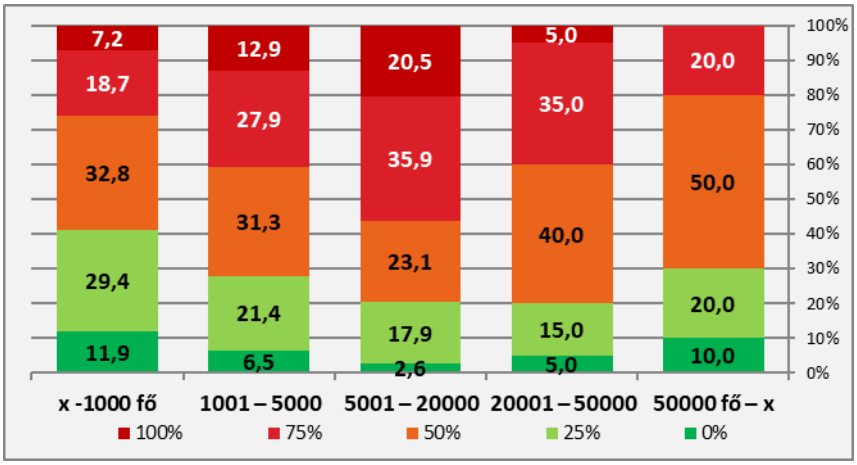
22. ábra

Kibertámadás bekövetkezésének valószínűsége a hivatal online közösségi helye elleni támadás szerint

Forrás: saját szerkesztés.

Emellett a közös hivatalok – függetlenül státuszuktól – tartanak legkevésbé egy lehetséges támadás valószínűségétől. E csoporton belül a kirendeltséghivatalok esetében látható, hogy a válaszok legalább 40%-ában szerepel a maximum 25%-os előfordulási lehetőség.
Az önállóan működő hivataloknál viszont ezzel ellentétes jelenséget rögzíthetünk, hiszen összességében itt a legnagyobb az aránya a közösségi helyek ellen irányuló becsült támadásoknak, mivel a 101 válaszadó hivatal fele (51 eset) legalább 75%-osnak ítélte meg az incidens bekövetkezésének esélyét.

A fenti megállapításokat cizellálja, hogy a lakosságszám szintjén is beigazolódnak az eredmények. Legkevésbé tartják valószínűnek a támadások bekövetkezését a legfeljebb 1000 és az ennél több, de 5000 főnél nem népesebb települések hivatalaiban, ahová a közös hivatali működésben érintett válaszadók jelentős része is sorolható. Természetesen a kisebb hivatalok esetében fordul elő leginkább, hogy nincs is közösségi megjelenése az önkormányzatnak/hivatalnak.



23. ábra

Kibertámadás bekövetkezésének valószínűsége a hivatal online közösségi helye ellen lakosságszám-kategóriák szerint

Forrás: saját szerkesztés.

A lakosságszám emelkedésével elkezd emelkedni azon válaszok aránya is, amelyek reális veszélyként látják a támadások előfordulásának lehetőségét. Emelkedik ez a tendencia egészen addig, míg a település lakosságszáma meg nem haladja az 50 000 főt. Ebben a kategóriában ugyanis

bizonyos nyugalom uralkodik: a hivatalok leginkább az 50%-os előfordulást említették, és olyan véleménnyel nem is találkozhatunk, ami szerint biztosra vehető a kibertámadás bekövetkezése.

Hetedik kérdés és a válaszok eredményei:

A kifejezetten *előnyszerzéssel járó, információszerző kibertámadások előfordulásának mértékét* leginkább az önállóan működő hivatalok dolgozói becsülik mérsékelten. Jellemző rájuk az alacsony bekövetkezési arányok megjelölése, viszont emellett az ebbe a csoportba tartozó hivatalok azok, amelyek ha mégis tartanak a támadásoktól, akkor jelentős mértékben, hiszen 9,1%-uk az elkerülhetetlen bekövetkezést is megemlítette (ez a legnagyobb arányszám a 100%-os bekövetkezés esetére).

9. táblázat

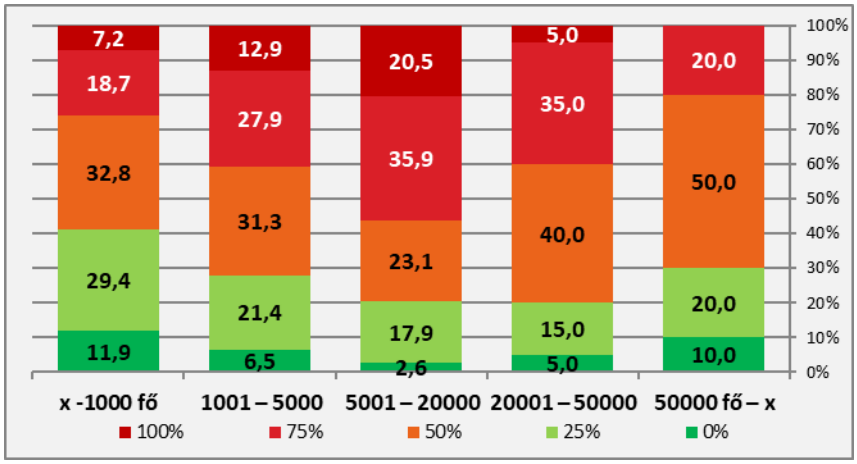
Kibertámadás bekövetkezésének valószínűsége információszerzés, előnyszerzés céljából

Közigazgatási feladatellátási státusz	Kibertámadás bekövetkezésének valószínűsége (%)											
	0%		25%		50%		75%		100%		Σ	
	db	%	db	%	db	%	db	%	db	%	db	%
Önálló	12	*12,1*	33	*33,3*	30	*30,3*	15	*15,2*	9	*9,1*	*99*	*100,0*
Közös hivatal	15	*9,7*	43	*27,7*	48	*31,0*	40	*25,8*	9	*5,8*	*155*	*100,0*
Közös hivatal tag	26	*10,6*	69	*28,2*	87	*35,5*	48	*19,6*	15	*6,1*	*245*	*100,0*
Összesen	*53*	*10,6*	*145*	*29,1*	*165*	*33,1*	*103*	*20,6*	*33*	*6,6*	*499*	*100,0*

Forrás: saját szerkesztés.

Egyébként a hivatalok közel négytizede a legfeljebb 25%-os előfordulási arányra voksolt. Ezzel ellentétben a legalább 75%-os valósínűséggel bekövetkező támadások aránya csupán 25–30% közötti.

A települési lakosságszám alapján azon hivatalok közül, amelyek az 5001–20 000 fő közötti kategóriába tartoznak, legkevesebben jelölték meg a támadások bekövetkezésének 50%-os arányát, továbbá e lakosságszámnál figyelhető meg, hogy több, mint minden második esetben elég valószínűnek tartják az incidenseket (56,4% a min. 75%-os előfordulásnál).



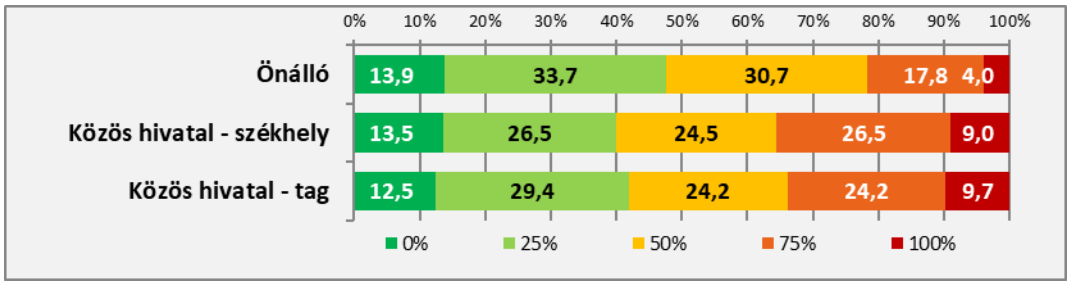
24. ábra

Kibertámadás bekövetkezésének valószínűsége információszerzés, előnyszerzés céljából lakosságszám-kategóriák szerint

Forrás: saját szerkesztés.

A települési lakosságszám növekedésével csökken – 50 000 főig – a bekövetkezéssel kapcsolatos szkeptikusok aránya, és nő az előfordulás komolyságát megemlítőké. Kivétel lehet ezek alól a legnépesebb települések csoportja, mivel ott a hivatalok a 100%-os bizonyosságban nem hisznek, viszont ugyanannyi esélyt adnak a támadások bekövetkezésének és elmaradásának.

Nyolcadik kérdés és a válaszok eredményei:
A településeken az *önkormányzati hivatalok az egyéb hálózati kapcsolatokat érő támadások tekintetében* viszonylag nyugodtak, hiszen legalább 40%-uk a legfeljebb alacsony szintű bekövetkezési valószínűséget jelölte meg (0–25%).
Köszönhető ez részben annak, hogy az önálló hivataloknak és a székhelyhivataloknak viszonylag jelentős a védettségiszint-érzése, részben pedig annak, hogy a kirendeltséghivatalok ügymeneteinek jelentős része nem rájuk, hanem a közös hivatal központjára hárul, illetve például az ASP integráció bevezetése sem teljes, nem valósult még meg teljes körűen.

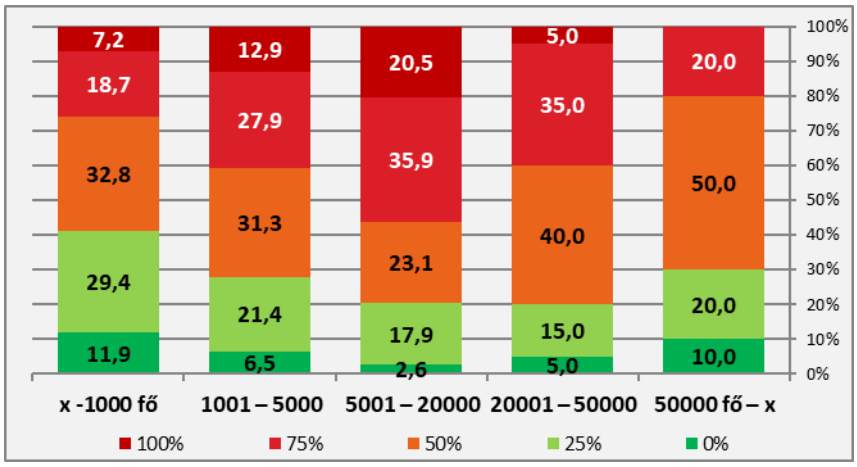


25. ábra

Kibertámadás bekövetkezésének valószínűsége egyéb hivatali hálózati kapcsolatok ellen

Forrás: saját szerkesztés.

Valamiféle bizonytalanság érzése azonban mégis felvetődik a közös hivatalok válaszadói esetében, hiszen kétszer olyan arányban jelentkeznek – az önálló hivatalokhoz mérten – csoportjukban azon hivatalok, amelyek teljes bizonyossággal fel vannak készülve az egyéb hálózati kapcsolatok megtámadására. Az említett nyugalom tehát valójában az önálló hivatalok esetében jelentkezik.
A fentieket a települések lakosságszám alapján történő vizsgálata annyiban árnyalja, hogy az 5000 főnél népesebb, de 20 000 főt meg nem haladó települések a leginkább azok, amelyek jelentős bekövetkezési valószínűséggel számolnak (min. 75%, az esetek 56,4%-a).
Emellett általánosságban azt is megállapítható, hogy a lakosságszám emelkedése nem javított az optimistább válaszok arányán, vagyis azok csökkennek, és a települési népességszám emelkedésével együtt emelkedik a támadások bekövetkezésének becsült mértéke is.
A legnagyobb lakosságszámú települési kategória (50 000 főt meghaladó) hivatalai pedig összességében a legkisebb mértékűnek vélik egy kibertámadás bekövetkezési lehetőségét.



26. ábra

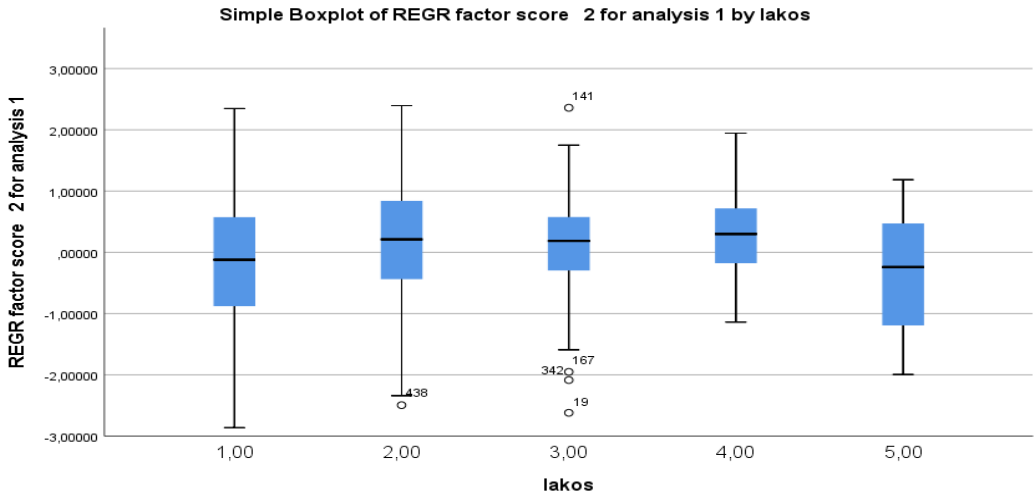
Kibertámadás bekövetkezésének valószínűsége egyéb hivatali hálózati kapcsolatok ellen a lakosságszám-kategóriák szerint

Forrás: saját szerkesztés.

Az egyes területek kibertámadásokkal történő érintettségének mértékét az összes terület esetében a középső kategóriák (25–75%) válaszokban megjelenő túlsúlya dönti el, jellemzően a válaszadók 75–85%-a ezt jelölte válaszában.

Főkomponens elemzés eredménye – az önkormányzatok kiberfenyegetettségének megítélése

A lakosságszám vált szignifikánssá.



27. ábra

Kiberfenyegetettség megítélése a különböző lakosságszám kategóriába tartozó települések esetében

Forrás: saját szerkesztés..

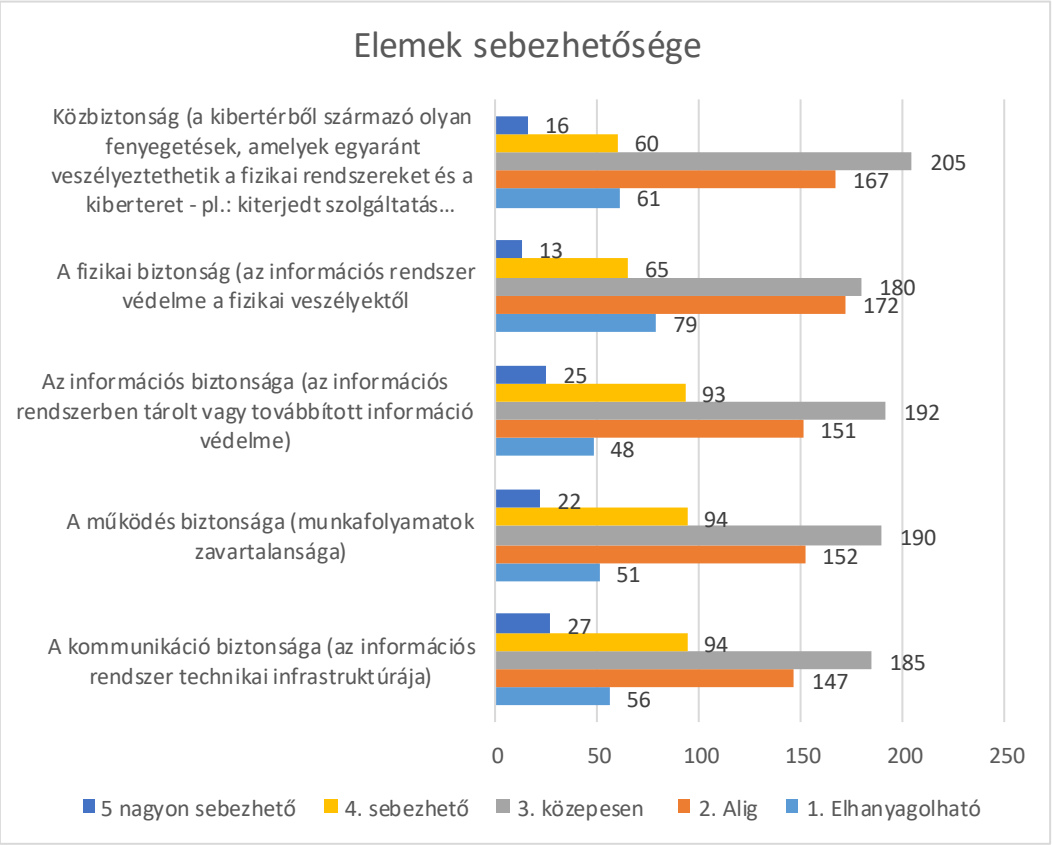
A lakosságszámot tekintve az 1-es csoport (1000 fő alatti lakosságszám) különbözik szignifikánsan a kettestől. A kiberfenyegetettséget a 2–4 kategóriákba (6. melléklet: 1001 főtől 50 000 főig) tartozó lakosságszámú önkormányzatok gondolják a legmagasabbnak. A kevés és a túl sok lakossal rendelkező települések önkormányzatai kevésbé gondolják, hogy fenyegetné őket kibertámadás.

A szakirodalom, a felmérés és a fókuszcsoportos interjú eredménye alapján ezt az okozza, hogy a kistelepülések nem érzik úgy, hogy kívül esnek a kibertámadásokat kezdeményezők érdeklődési körén; az általuk kezelt adatok, információk nem képviselnek olyan értéket, ami felkeltené az esetleges rosszindulatú támadó figyelmét. Ezekben a vélelmekben természetesen lehet igazság egészen addig, amíg a haszonszerzés a motiváció okán bekövetkező rosszindulatú támadásról vagy esetleg terrorcselekményről beszélünk, mivel akkor ezek az érvelések már nem állják meg a helyüket, hiszen az önkormányzatokon, mint könnyű célpontokon keresztül komoly nehézségeket tudnak okozni. Az 50 001 fő lakosságszámot meghaladó települések esetében pedig egy túlzott önbizalom lehet az oka a kiberfenyegetettség alacsony értékelésének.

4.2.2. Vizsgált terület (I.): kibertér – kiberbiztonság – az önkormányzatok sebezhetősége

A fontosabb önkormányzati elemek sebezhetőségének mértéke

A 28. ábra azt mutatja, hogy a válaszadók mit gondolnak az önkormányzati működés során az egyes területek, elemek sebezhetőségéről.



28. ábra

Elemek sebezhetősége (összefoglaló)

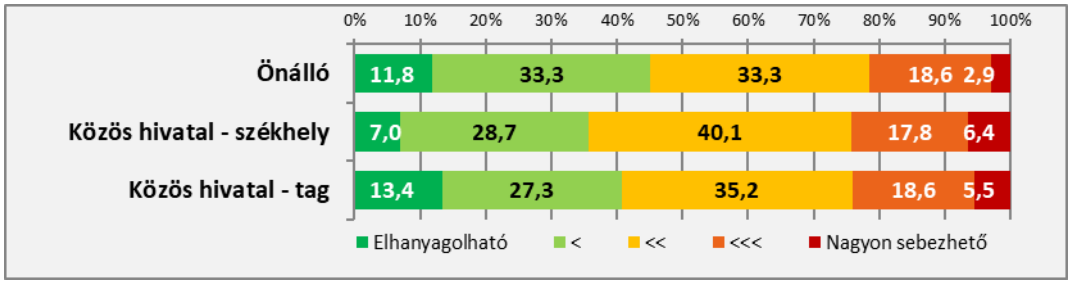
Forrás: saját szerkesztés.

Az ábrából jól látszik, hogy a válaszadók kevéssé tartják sebezhetőnek a felsorolásban szereplő elemeket.

A válaszok eredményeinek elemzése:

A kommunikáció biztonsága:

Az információs rendszerük technikai infrastruktúrájának sebezhetősége elhanyagolható, vagy nem számottevő szintű a hivatali jelzések 35–45%-ában. Emellett csaknem ilyen arányban szerepelnek azok a becslések is, amelyek szerint a sebezhetőség mértéke közepes szintűnek nevezhető (33–40%).



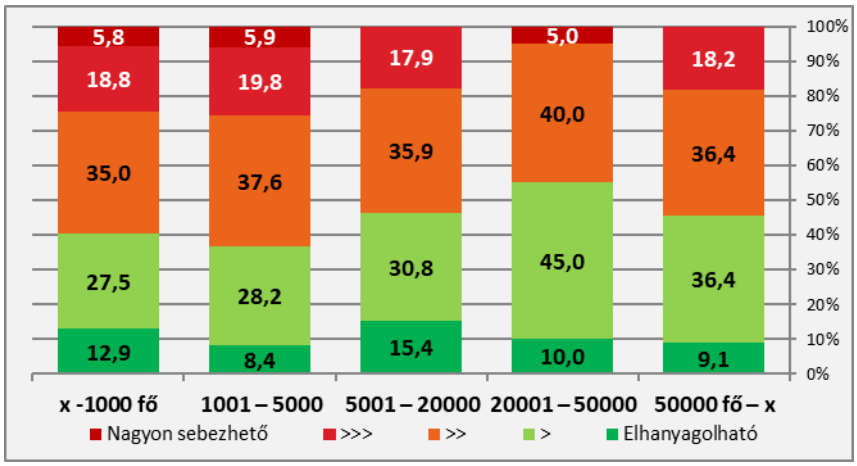
29. ábra

Az önkormányzat sebezhetőségének állapota a kommunikáció biztonsága szerint

Forrás: saját szerkesztés..

Általános megállapítás továbbá, hogy az összes hivatal közel egyötöde (17,8–18,6%) sebezhetőnek, 3–6%-a pedig kifejezetten, nagyon sebezhetőnek tartotta a saját kommunikációs rendszerét. A két válaszkomponens együttes aránya a települések közel egynegyedére igaz. Az egyes hivataltípusok mutatói egymás mellett haladnak, azonban eltérés tapasztalható a székhelyhivatalok esetében: a legkevésbé itt optimisták a sebezhetőség mértékét tekintve, és leginkább ezek a hivatalok jelölik meg közepesen sebezhetőnek a technikai infrastruktúráikat (40%).

A fenti megállapítások érzékelhetők települési lakosságszám szerinti bontásban is. Lakosságszámtól függetlenül a hivatalok 35–45%-a elhanyagolhatóan, vagy számottevően nem tartja sebezhetőnek a kommunikáció biztonságát.



30. ábra

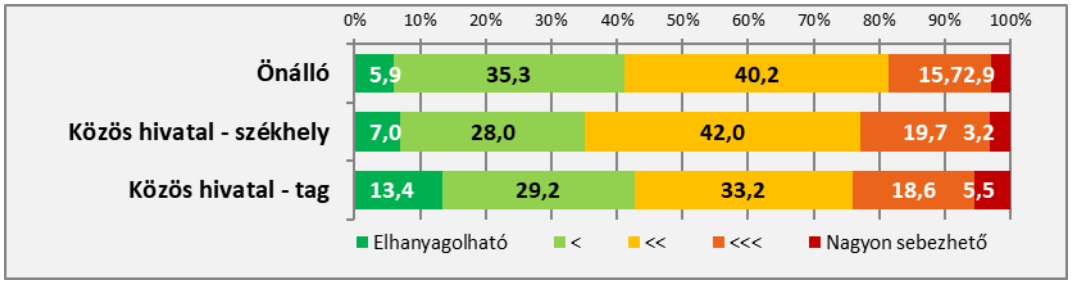
Az önkormányzat sebezhetőségének állapota a kommunikáció biztonságát tekintve lakosságszám-kategóriák szerint

Forrás: saját szerkesztés.

Legjobb a helyzet a 20 001–50 000 fős lakosságszámú települések hivatalaiban, ahol az esetek 95%-ában legfeljebb közepes mértékig tartják sebezhetőnek a rendszerüket, és csupán minden huszadik válaszban tartották úgy, hogy az nagyon sebezhető. A többi lakosságszám-kategória esetében pedig a sebezhető, vagy nagyon sebezhető állapot a hivatalok 17,9–25,7%-ára volt jellemző. Továbbá az 5000 főnél kisebb népességű települések esetében az egyes csoportokban azok mutatói együtt haladnak; ezekre a településekre jellemző a hivatali kommunikáció sebezhetőségének legnagyobb szintje (≈ 25%).

A működés biztonsága: a munkafolyamatok zavartalansága:

A települési válaszokból kiderül, hogy a hivatalok 35–45%-a jellemzően nem tartja igazán sebezhetőnek saját működését, a munkafolyamatok zavartalanok.Leginkább a kirendeltséghivatalok jelzési utalnak erre (13,4% elhanyagolható, és 29,2% alig sebezhető).



31. ábra

Az önkormányzat sebezhetőségének állapota a működés biztonsága szerint

Forrás: saját szerkesztés.

Erre a hivatali státuszra jellemző viszont az is, hogy ahol probléma lehet, ott valóban komoly a helyzet, hiszen a taghivatalok több, mint egyötöde jelezte azt is, hogy komolyan vagy nagyon sebezhető a működés biztonsága.

A lakosság szerinti településbontás is mutatja a kirendeltséghivatalok esetében a jelentős értéket az elhanyagolható és a komoly sebezhetőség eseteiben egyaránt (amelyek a legfeljebb 5000 fős településekre jellemzőek).

10. táblázat

Az önkormányzat sebezhetőségének állapota a működés biztonságát tekintve lakosságszám-kategóriák szerint

Forrás: saját szerkesztés.

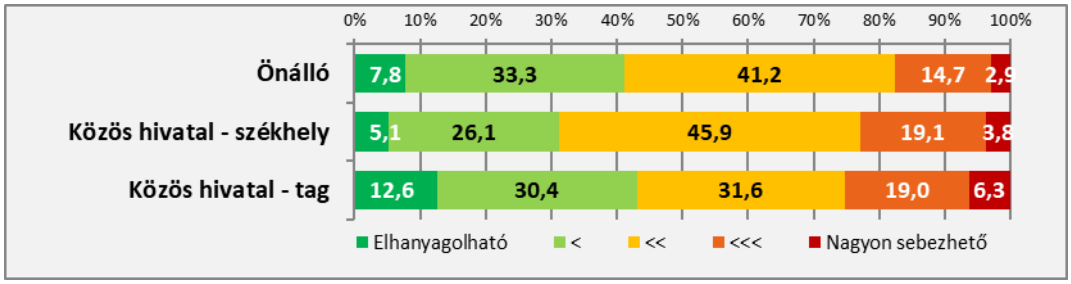
Az önkormányzat sebezhetőségének állapota a működés biztonságát tekintve lakosságszám-kategóriák	**Az egyes elemek sebezhetőségének mértéke a működés biztonságát tekintve**											
	1. Elhanyagolható		**2 . <**		**3 . <<**		**4 . <<<**		**5 . Nagyon sebezhető**		*Σ*	
	db	%	db	%	db	%	db	%	db	%	*db*	*%*
x – 1000 *(237) 46,6)*	33	*13,8*	71	*29,6*	79	*32,9*	44	*18,3*	13	*5,4*	*240*	*100*
1001 – 5000 *(202)*	15	*7,4*	52	*25,7*	85	*42,1*	43	*21,3*	7	*3,5*	*202*	*100*
5001 – 20000 *(39)*	2	*5,1*	15	*38,5*	16	*41,0*	5	*12,8*	1	*2,6*	*39*	*100*
20001 – 50000 *(20)*	1	*5,0*	10	*50,0*	8	*40,0*	0	*0,0*	1	*5,0*	*20*	*100*
50000 – x *(11)*	0	*0,0*	6	*54,5*	3	*27,3*	2	*18,2*	0	*0,0*	*11*	*100*
Összesen	*51*		*154*		*191*		*94*		*22*		*512*	*100*

A települési lakosságszám növekedésével párhuzamosan emelkedik az enyhén sebezhetőség szintje a hivatalok válaszaiban, és ezzel együtt csökken a komoly kockázatként történő megítélése is. A legnépesebb települések esetében pedig nem is beszélhetünk arról, hogy a dolgozók szerint a működés biztonsága nagyon sebezhető lenne.

Az információ biztonsága: az információs rendszerben tárolt vagy továbbított információ védelme:

A hivatalok 31,2–43%-a elégedett a tárolt, vagy továbbított információk védettségével, a sebezhetőség mértékét nagyon alacsonynak ítélték erre vonatkozóan.

Ehhez hasonló az aránya azoknak a hivataloknak is, amelyek az információs biztonságukat közepesen sebezhetőnek becsülték meg. A válaszok 17,6–26,3%-a pedig arra a kategóriára utalt, amiben komoly sebezhetőségi állapot jelentkezik az információs biztonság területén.



32. ábra

Az önkormányzat sebezhetőségének állapota az információbiztonság tekintetében

Forrás: saját szerkesztés.

Leginkább a *kirendeltségként működő hivatalok* azok, amelyek elégedettek a biztonsággal, de ide sorolhatók azok a hivatalok is, amelyeknél legnagyobb arányban merülnek fel problémák a védelem területén.

A települési lakosságszám növekedése mellett nem változik lényegesen az információbiztonsággal elégedett hivatalok aránya. Emelkedik viszont a közepesen sebezhető hivataloké, és csökken a ténylegesen komoly sebezhetőségnek kitett tárolt vagy továbbított információk aránya. Tehát legbiztonságosabbnak a helyzetet a 20 000 főt meghaladó lakosságszámú településeken ítélték.

11. táblázat

Az önkormányzat sebezhetőségének állapota az információbiztonság tekintetében lakosságszám-kategóriák szerint

Forrás: saját szerkesztés.

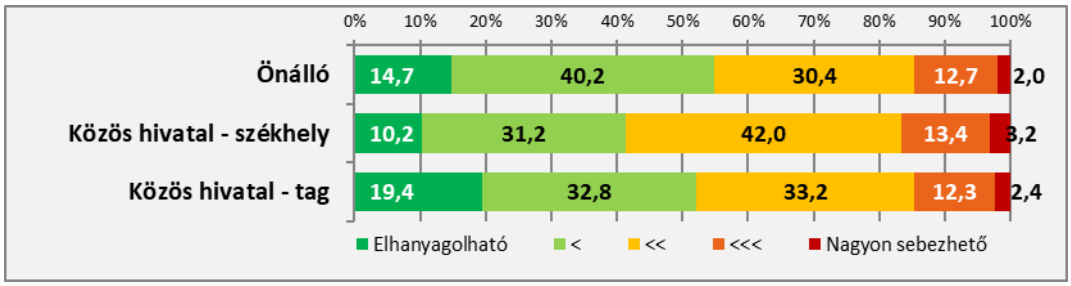
Lakosságszám-kategóriák (fő)	Az egyes elemek sebezhetőségének állapota az információbiztonság tekintetében											
	1. Elhanyagolható		2 . <		3 . <<		4 . <<<		5 . Nagyon sebezhető		Σ	
	db	%	db	%	db	%	db	%	db	%	db	%
x – 1000 *(2407) 46,6%)*	31	*12,9*	70	*29,2*	79	*32,9*	45	*18,8*	15	*6,3*	*240*	*100,0*
1001 – 5000 *(202) 39,7%)*	11	*5,4*	61	*30,2*	82	*40,6*	39	*19,3*	9	*4,5*	*202*	*100,0*
5001 – 20000 *(39) 7,7%)*	3	*7,7*	13	*33,3*	16	*41,0*	6	*15,4*	1	*2,6*	*39*	*100,0*
20001 – 50000 *(20) 3,9%)*	2	*10,0*	5	*25,0*	11	*55,0*	2	*10,0*	0	*0,0*	*20*	*100,0*
50000 – x *(11) 2,2%)*	1	*9,1*	3	*27,3*	6	*54,5*	1	*9,1*	0	*0,0*	*11*	*100,0*
Összesen	*48*		*152*		*194*		*93*		*25*		*512*	*100,0*

Ezzel ellentétben a kisebb településeken (5000 fő alatti) a komoly vagy teljes sebezhetőség jellemző a hivatalok egynegyedére, tehát a helyzetet itt érzik a legfenyegetőbbnek.

A fizikai biztonság: az információs rendszer védelme a fizikai veszélyektől:

Hasonlóan az eddig vizsgált területekhez, az információs rendszerek fizikai veszélyektől való védelmével is elégedett a hivatalok jelentős része. Összesen 41–55%-uk jelezte azt, hogy legfeljebb alacsony szintű sebezhetőségnek van kitéve a fizikai biztonságuk.

Emellett legalább minden harmadik hivatal válaszolta azt is, hogy közepes mértékben tartja sebezhetőnek (30,4–42%) az információs rendszert, viszont emellett viszonylag alacsony arányban jelölték meg a komoly sebezhetőségi kockázatok jelenlétét (≈ 15%).

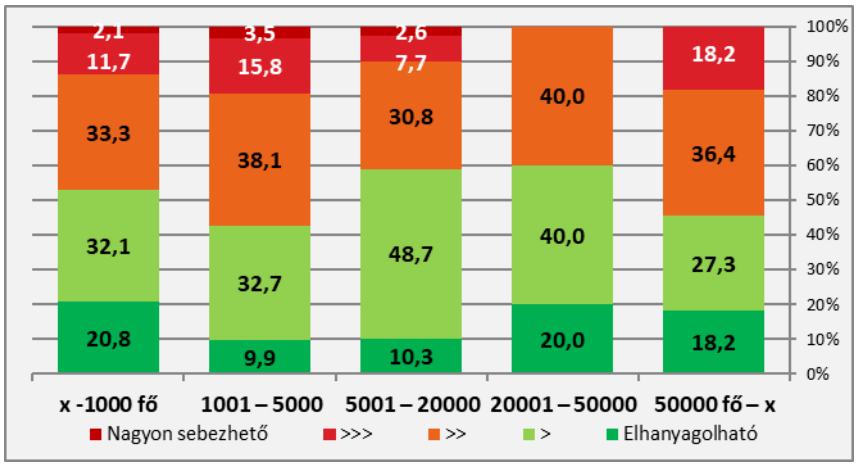


33. ábra

Az önkormányzat sebezhetőségének állapota a fizikai biztonság tekintetében

Forrás: saját szerkesztés.

A székhelyhivatalok esetében a legszolidabb azon jelzések aránya, ami a legkedvezőbb sebezhetőségi állapotokra utal, az elhanyagolható szintű sérülékenység aránya itt fele, mint a kirendeltségek, és egyharmaddal kevesebb, mint az önálló hivatalok esetében, viszont a központi hivataloknál a legjelentősebb a közepes sebezhetőség aránya (42%). A lakosságszám szerinti elemzés is mutatja a kirendeltséghivatalok magabiztosságát a sebezhetőséggel kapcsolatosan, ami leginkább az 1000 fő alatti településekre jellemző, ahol a hivatalok egyötöde biztos abban, hogy a fizikai biztonságuk szintje annyira megfelelő, hogy csupán elhanyagolható lehet annak sebezhetősége.



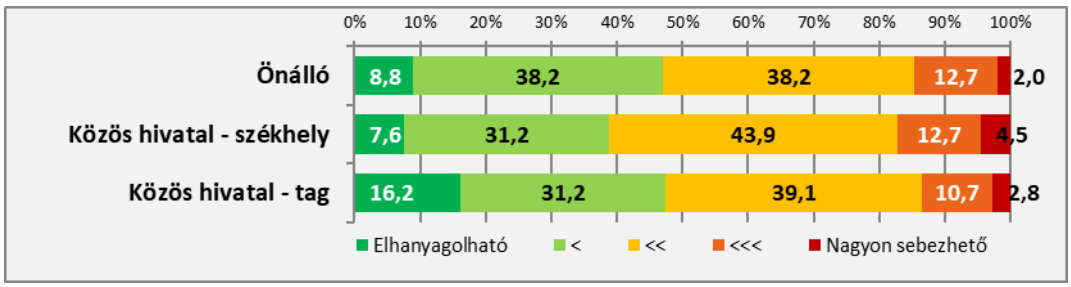
34. ábra

Az önkormányzat sebezhetőségének állapota a fizikai biztonság tekintetében lakosságszám-kategóriák szerint. Forrás: *saját szerkesztés.*

A legmegnyugtatóbb helyzetben azonban mégis azok a hivatalok válaszadói érzik magukat, amelyek 5001–50 000 fős lakosságszámú településekhez kötődnek. Ezen belül kifejezetten a kis- és középvárosok (20 001–50 000 fő), ahol a válaszok tanúsága szerint a hivatalok 60%-a legfeljebb csekély mérvű sebezhetőséget érez, és a maradék 40%-uk is csupán közepes szintű fenyegetettségben érzi magát. Az önkormányzatok komolyabb sebezhetősége pedig fel sem merül esetükben.

Közbiztonság:

Az előző vizsgált területhez hasonlóan a közbiztonság területén is a legkevésbé óvatosak a kirendeltséghivatalok, ahol dupla arányban jellemzőek azok a válaszok, amelyek a sebezhetőség elhanyagolhatóságára vonatkoznak (esetükben 16,2%, míg az önálló és székhelyhivatalok esetében 8% körüli az érték).



35. ábra

Az önkormányzat sebezhetőségének állapota a közbiztonság tekintetében

Forrás: saját szerkesztés.

A közigazgatási feladatellátási státuszok alapján kategorizált hivatalok mutatói együtt haladnak a sebezhetőség mértéke tekintetében, kisebb kiugrás a székhelyhivatalok esetében érzékelhető, mivel a nagyon sebezhető állapot megbecsülése esetében a legmagasabb az érték, de általánosságban az a jellemző, hogy a hivatalok elég kis része, mindössze 13–17%-a jelezte azt, hogy komoly sebezhetőségi lehetőség van a közbiztonság esetében.

A lakosságszámok elemzése is rámutat az 1000 fő alatti településeken a taghivatalok derűlátására az elhanyagolható sebezhetőség terén. Emellett felvillan a legnagyobb települések (50 000 fő feletti lakosságszám) leginkább önálló hivatalainak bizonytalansága is, hiszen több, mint minden negyedik hivatal komoly aggodalmát fejezte ki egy súlyos sérüléssel, támadással szemben, vagyis sebezhetőségük megítélése a legnagyobb mértékű (27,3%).

12. táblázat

Az önkormányzat sebezhetőségének állapota a közbiztonság tekintetében lakosságszám-kategóriák szerint

Forrás: saját szerkesztés.

Lakosságszám kategóriák (fő)	**Az egyes elemek sebezhetőségének állapota a közbiztonság tekintetében**											
	1. Elhanyagolható		**2 . <**		**3 . <<**		**4 . <<<**		**5 . Nagyon sebezhető**		Σ	
	db	%	db	%	db	%	db	%	db	%	db	%
x -1000 *(237) 46,6%)*	41	*17,1*	70	*29,2*	92	*38,3*	31	*12,9*	6	*2,5*	*240*	*100,0*
1001 – 5000 (*202) 39,7%*)	13	*6,4*	70	*34,7*	86	*42,6*	24	*11,9*	9	*4,5*	*202*	*100,0*
5001 – 20000 (*39) 7,7%*)	6	*15,4*	11	*28,2*	19	*48,7*	3	*7,7*	0	*0,0*	*39*	*100,0*
20001 – 50000 (*20) 3,9%*)	1	*5,0*	11	*55,0*	8	*40,0*	0	*0,0*	0	*0,0*	*20*	*100,0*
50000 – x (*11) 2,2%*)	1	*9,1*	5	*45,5*	2	*18,2*	2	*18,2*	1	*9,1*	*11*	*100,0*
Összesen	*62*		*167*		*207*		*60*		*16*		*512*	*100,0*

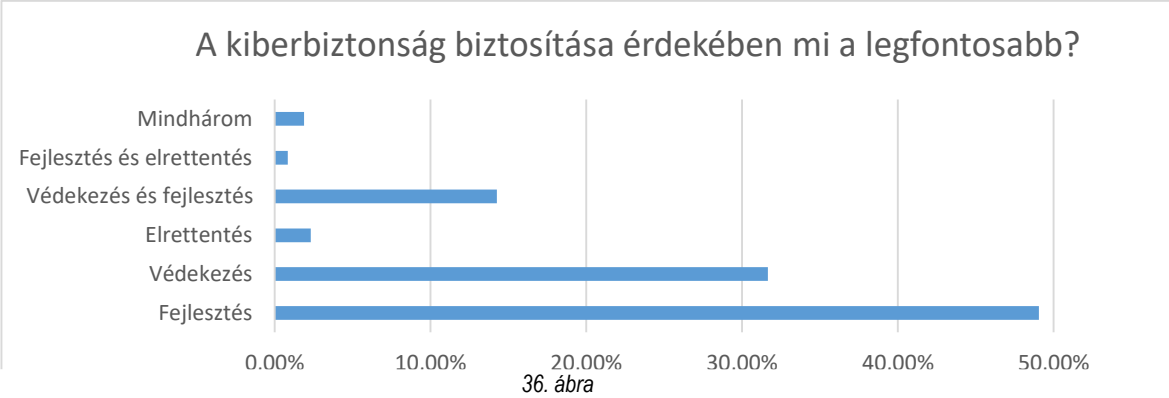
Ezzel ellentétben, a dolgozók véleménye szerint legbékésebb a helyzet ismételten a 20 000 főnél népesebb, de 50 000 lakost el nem érő települések hivatalainak esetében, ahol egyáltalán nem beszélhetünk az átlagosnál komolyabb sebezhetőségről és az esetek négytizedében közepes, míg 60%-ában legfeljebb enyhe a sérülés okozásának a lehetősége.

Főkomponens elemzés – sebezhetőség

Az elemzés a sebezhetőség tekintetében egyetlen független változóval sem jelzett szignifikáns hatást. Ez azért lehet, mert:

- vagy nagyon sok kis tényező befolyásolja;
- vagy mindentől független;
- vagy olyan változó befolyásolja, amit nem mértünk fel/nem tettünk bele az adott modellbe. Illetve a későbbi vizsgálatoknál érdemes figyelembe venni, hogy a sebezhetőség esetében vélelmezhető, hogy nincs szignifikáns kapcsolat a települési önkormányzatok esetében a lakosságszámmal, a hivatal típusával vagy a település jogállásával.4.2.3. Vizsgált terület (I.): kibertér – kiberbiztonság – a megkérdezettek válaszainak elemzése a kiberbiztonság módszereiről

A kérdés így hangzott: *A felkészülés során Ön szerint a védekezés, az elrettentés vagy a fejlesztés a legfontosabb?*



36. ábra

A válaszadók véleménye a kiberbiztonság érdekében szükséges teendőkkel/módszerekkel kapcsolatban

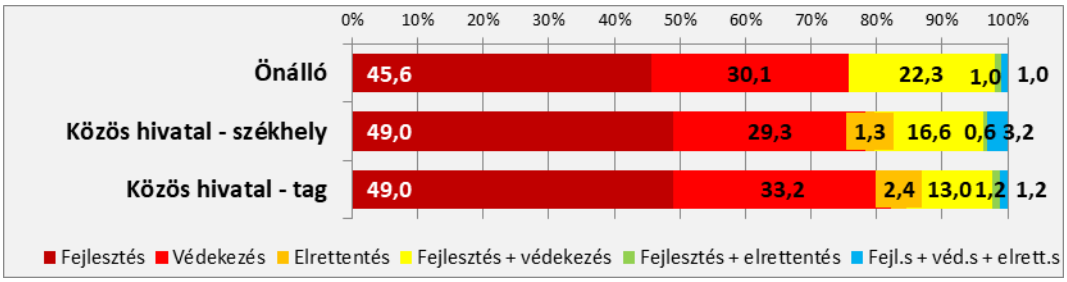
Forrás: saját szerkesztés.

A kérdésre kapott válaszok jelentős része kötött, tiszta fogalmakkal operál. Ezek teszik ki a jelzések döntő hányadát. Megemlítendők azonban azok a válaszok is, amelyek esetében több lehetőség is megjelölésre került, továbbá voltak szöveges kifejtések, magyarázatok is.

Az általános szintű megállapítások között az első, hogy feladatellátási státusztól függetlenül a hivatalok a kibertámadások elhárítása érdekében történő felkészülést leginkább a fejlesztések alkalmazásával látják biztosítottnak. Ezt a kijelentésüket az egyes hivatali kategóriák dolgozói 45–49%-ban alátámasztották válaszaikban.

A válaszadók egyharmada a tiszta védekezésre helyezi a hangsúlyt (29,3–33,2%). Emellett a fejlesztés és védekezés egyenrangú fontosságát a válaszadók további 13–22,3%-a megemlíti. Így összességében a hivatalok legfontosabb feladata a támadásokra történő felkészülés során a különböző fejlesztésekben és/vagy a védekezési technikák alkalmazásában merül ki. A két felkészülési lehetőség együtt történő említése összesen a hivatalok csaknem mindegyikére jellemző (arányuk 94,5–98% közötti).

A tiszta válaszok között az elrettentés mint felkészülési módszer egyértelműen a legkevésbé népszerű, hiszen elenyésző gyakoriságban kapott csak említést (legfeljebb 2,4%), de az önálló hivatalok dolgozóinak válaszaiban nem is szerepel a fogalom.



37. ábra

A felkészülés módszerei

Forrás: saját szerkesztés.

Az elemzés végén azok a válaszok következnek, amelyek a komplex felkészülés híveinek véleményét tükrözik. Esetükben mind a három fő módszer együtt kapott említést. Bár vélelmezhető, hogy ez a megközelítés adja a legnagyobb biztonságot, összesen kilenc válaszadó gondolt erre.

Összesítésként leszögezhetjük, hogy a három felkészülést meghatározó módszer közül az elrettentés gyakorlatilag nem adekvát lehetőség. Ezzel szemben viszont annál nyomatékosabb a fejlesztés hangsúlya, hiszen önállóan, vagy bármely másik módszerrel közösen használva is egyeduralkodó forma a sikeres felkészítésben. Összesen 344 hivatal említette meg fontosságát, ami a települések kétharmadát jelenti (67,2%).

A három válaszlehetőség mintázata a közigazgatási feladatellátási státuszon belüli kategóriák esetében hasonló mintázatot követ. Talán annyit érdemes megjegyezni, hogy a fejlesztés-védekezés szükségessége leginkább az önálló hivatalok esetében mutatkozik meg.

A *szöveges pluszinformációk* pedig magyaráznak, adalékot adnak az egyes válaszok mellé és köré, illetve a javaslatok megfogalmazásához is értékesek. Ezek közül néhány az érdekesebbek, az érdemesebbek közül:

> „A fejlesztés, a megfelelő képzés, oktatás az informatikai rendszerek használatával kapcsolatosan."
>
> „Azért a fejlesztés a legfontosabb, mert jó műszaki színvonalon és minőségi tartalommal kialakított informatikai és kibernetikai infrastruktúra biztonságosabb. A technológiai avulás gyorsan bekövetkezik az egyes technikai informatikai eszközökben – amit pótolni kell. Ezen felül a humán erőforrás fejlesztése is szinkronban kell, hogy legyen az infrastruktúra fejlesztésével."
>
> „Az esetleges támadások elleni védekezés természetes része a mindennapjainknak, tűzfal, vírusirtók használata, szerverrendszer kialakítása, információ biztonság betartása, de kiemelkedően fontos ha a fejlesztések szakmailag támogatottak is."

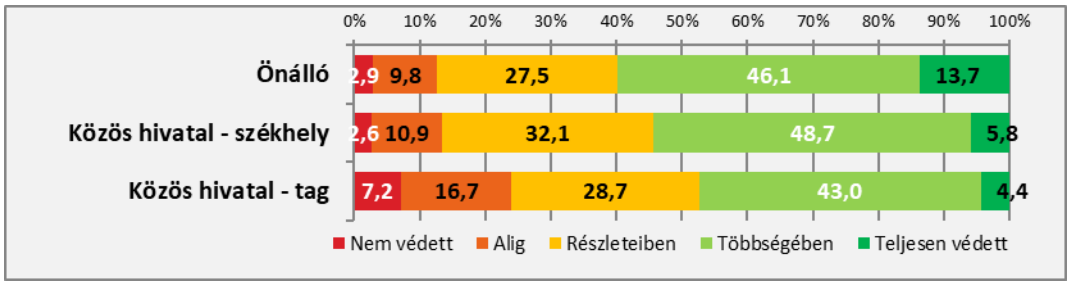
4.2.4. Vizsgált terület (II.): felkészültség – képzettség – az önkormányzatok kiberbiztonsági jellemzői

Jellemző állítások kibertámadás esetén

1. kérdés

Kibertámadás esetén rendszereink és hálózatunk védett.

Egy jövőbeli kibertámadás esetére vonatkozóan a válaszadók átlagosan 45,4%-a, vagyis kisebbik fele gondolja úgy, hogy a hivatal rendszerei és hálózata többségében védett. Emellett részleteiben védettek a jelzett egységek a hivatalok közel egyharmadában is, teljes védettségről pedig átlagosan 6,7%-os hivatali arány mellett beszélhetünk.



38. ábra

Kibertámadás esetén az önkormányzatra jellemző állítások a rendszer és a hálózat védettsége tekintetében

Forrás: saját szerkesztés.

Tehát teljes vagy részleges védettség illuziójáról beszélhetünk összességében és átlagosan a hivatalok több, mint négyötöde esetében (átlagosan 81,6%).

Emellett átlagosan minden hetedik hivatal esetében válik úgy, hogy a rendszer és hálózata csupán alig védett, és minden huszadik hivatal nem védett a kibertámadások ellen. A helyzet a kirendeltséghivatalok tekintetében a legrosszabb (7,2%), és az alig védekező hivatalok aránya is esetükben a legmagasabb.

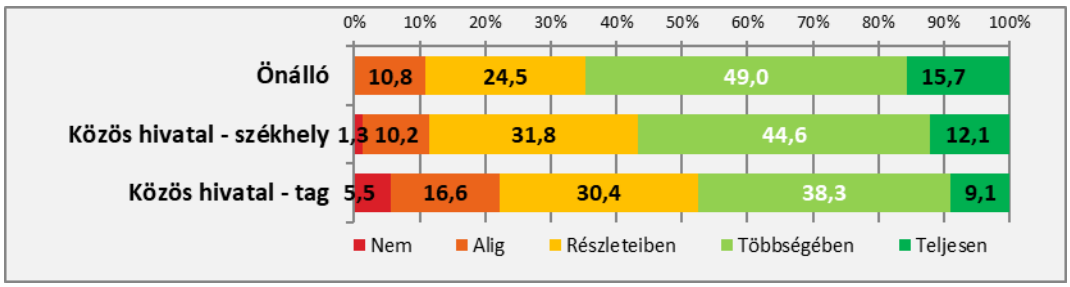
Az állítások szerint legkedvezőbb helyzetben az önálló hivatalok vannak, hiszen nem, vagy alig védettnek csupán a dolgozóik egynyolcada gondolja őket, továbbá a legalább részleteiben elérhető védettségük mértéke eléri a 87,3%-ot.

2. kérdés

Kibertámadás esetén a rendszerhasználat szabályozott.

A hivatali dolgozók véleménye a rendszerhasználatuk szabályozottságáról hasonló az előbbi kérdés eredményei esetében tapasztaltakhoz.

A válaszadók véleményének alig több, mint egytizede szerint teljes mértékben szabályozott a rendszerhasználat a hivatalokban. Leginkább az önállóan működő, míg legkevésbé a kirendeltségként működő hivataloknál beszélhetünk abszolút szabályozottságról (15,7% és 9,1%). Emellett leginkább az önálló hivatalok esetében szabályozott a rendszerhasználat (49%, vagyis az érintettek fele), illetve legkevésbé a taghivatalok esetében (38,3%).



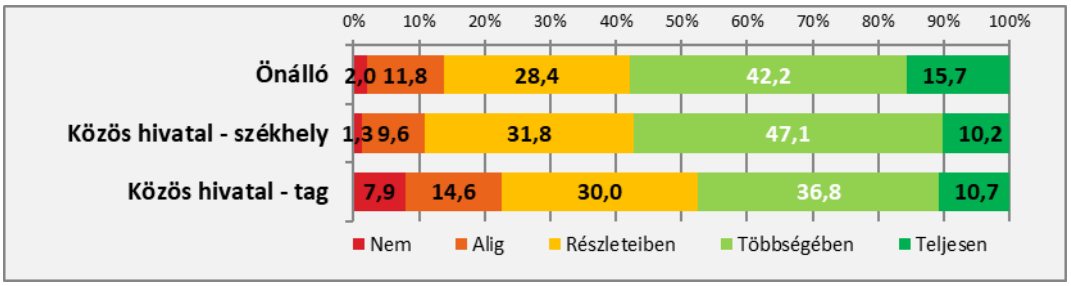
39. ábra

Kibertámadás esetén az önkormányzatra jellemző állítások a rendszerhasználat szabályozottsága tekintetében

Forrás: saját szerkesztés.

3. kérdés
A folyamatos infrastrukturális fejlesztés sokat segít a kibertámadás elleni védelemben.

Ez olvasható ki a hivatalok adataiból, hiszen a válaszok több, mint a felében (52,5%) többségében, vagy teljes mértékben segítséget nyújt a fejlesztés a védekezésben – és kifejezetten ez mondható el az önálló hivatalok esetében. Az olyan esetek, amikor csupán részleteiben hatásosak a fejlesztések, és nem minden területen érezhetők ezek a védelemben, szintén meghatározó arányt képviselnek a válaszokban. Elmondható, hogy bármely feladatellátási státusszal rendelkező hivatalok átlagosan 30%-ánál fordul ez elő.



40. ábra

Kibertámadás esetén az önkormányzatra jellemző állítások a folyamatos infrastrukturális fejlesztés tekintetében

Forrás: saját szerkesztés.

Továbbá átlagosan minden nyolcadik hivatalra jellemző, hogy a fejlesztések nem eredményesek és hatásukat csak alig lehet felfedezni a támadások elleni védekezés során. Ezek aránya legmagasabb a kirendeltséghivatalok esetében (14,6%) és legalacsonyabb a központi hivataloknál.

Végül következnek azok a hivatalok, amelyeknél nincs fejlesztés, vagy ha mégis, akkor nem releváns a védelem hatékonysága szempontjából. Átlagosan csaknem minden huszadik hivatal esik ebbe a csoportba (4,7%), amin belül egyértelműen a taghivatalok vannak a leghátrányosabb helyzetben, mivel mutatójuk értéke négyszer, illetve hatszor is gyengébb, mint az önálló vagy központi hivataloké.

4. kérdés
Kibertámadás esetében a munkatársaink tisztában vannak a fenyegetésekkel és felkészültek a tennivalók tekintetében.

Egy esetleges kibertámadás tekintetében a válaszokat elemezve kitűnik, hogy a hivatalok munkatársai összességében nincsenek tisztában a fenyegetésekkel, továbbá nem kellően felkészültek. Ez megmutatkozik abban is, hogy a többségében vagy teljes mértékben tájékozott és felkészült humánháttér csupán minden harmadik hivatalra jellemző (33,4%). Legtájékozottabbak az önálló hivatalok dolgozói, és legfelkészületlenebbek a székhelyhivatalok alkalmazottai.

Nem várt megállapítás, hogy a teljes mértékben felkészült munkatársak aránya az önálló hivatalok esetében a legalacsonyabb (5,9%) és a kirendeltségként működő szervezetek esetében a legmagasabb (9,1%). Ez nem életszerű, inkább a megfelelés érdekében adott válasz.

13. táblázat

Kibertámadás esetén az önkormányzatra jellemző állítások a dolgozók tájékozottsága és felkészültsége tekintetében
Forrás: saját szerkesztés.

Közigazgatási-feladatellátási státusz	Kibertámadás tekintetében a munkatársak tájékozottsága és felkészültsége											
	Nem		Alig		Részleteiben		Többségében		Teljesen		Σ	
	db	%	db	%	db	%	db	%	db	%	db	%
Önálló	4	4,0	28	27,7	33	32,7	30	29,7	6	5,9	101	100,0
Közös hivatal székhely	4	2,5	40	25,5	65	41,4	37	23,6	11	7,0	157	100,0
Közös hivatal tag	21	8,3	63	24,9	82	32,4	64	25,3	23	9,1	253	100,0
Összesen	29	5,7	131	25,6	180	35,2	131	25,6	40	7,8	511	100,0

Egy kibertámadás esetén az érdemben alig használható munkatársak megjelölése a hivatalok egynegyedére jellemző, és nincs számottevő különbség abban a tekintetében sem, hogy milyen státuszban működik a hivatal.

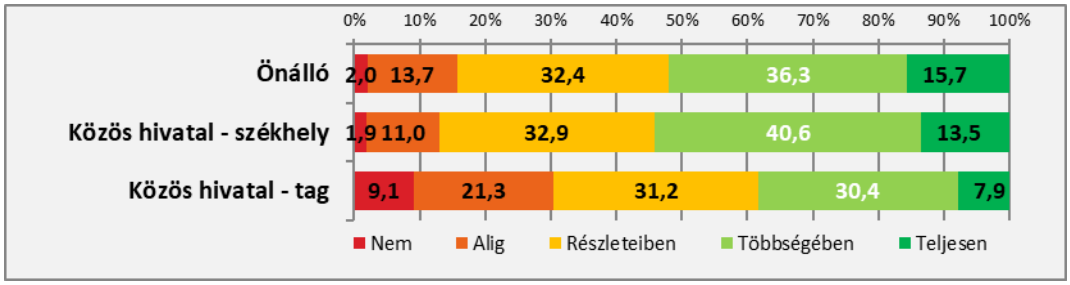
Végül és nem meglepő módon a kirendeltségként működő hivatalok esetében jellemző leginkább a tájékozatlan és fel nem készült munkatársi gárda. Arányuk 8,3%, ami kétszerese az önálló hivatalok adatainak, illetve háromszorosa a közös önkormányzati hivatalok központi egységeiben tapasztaltaknak.

5. kérdés

Számítógépeink és szoftvereink modernek és folyamatosan frissítjük őket egy esetleges kibertámadás elleni védelem elősegítése okán is.

Általános megállapításként tehető e kérdéskörrel kapcsolatos tapasztalatok esetében, hogy az önkormányzati hivatalok egy lehetséges kibertámadás esetén csupán részlegesen számíthatnak gépeik és szoftvereik védelmére, mivel a teljesen modern és folyamatosan frissített eszközpark csupán a szervezetek 11,2%-ára, vagyis minden kilencedik hivatalra jellemző – átlagosan. A legkevesebb ilyen hivatal a kirendeltségek között (7,9%), míg a legtöbb az önállóan működő hivatalok között található.

Jobb a helyzet ennél a többségében modern és frissített HW-SW környezet tekintetében, hiszen átlagosan a hivatalok egyharmada jelölte meg ezt az opciót válaszaiban. A székhelyhivatalok a leginkább, a kirendeltségként működők pedig a legkevésbé jelezték ezt a mértéket. Arányuk 40,6% és 30,4% volt.



41. ábra

Kibertámadás esetén az önkormányzatra jellemző állítások a számítógépek és szoftverek frissítése és modernizációja tekintetében

Forrás: saját szerkesztés.

A részleteiben modern és frissített gépek, szoftverek aránya hasonló az előbbi mértékhez (32%), vagyis ebben az esetben is minden harmadik hivatal válaszaiban ezt olvashattuk. Végül a

taghivatalok esetében a legmagasabb az aránya az alig modernizált és nem kellően frissített számítógépeknek és szoftvereknek. Minden ötödik kirendeltség esetében ez a helyzet, ami kétszeres mértékben meghaladja az önálló hivataloknál, illetve két és félszer a székhelyhivataloknál tapasztalt értékeket. Az elavult és nem frissített gépek, eszközök is ehhez a hivatali csoporthoz tartoznak leginkább, de összességében minden tizenegyedik szervezetre jellemzőek. Ez az arány így négy és félszer magasabb, mint az önálló vagy székhelyhivatalok esetében.

5. kérdés

Munkatársaink motiváltak és felkészültek annak érdekében, hogy védekezzek egy esetleges kibertámadás ellen.

Egy bekövetkezett kibertámadás alkalmával kevés olyan munkatársukra számíthatnak az egyes hivatalok, akik teljes mértékben felkészültek és motiváltak is arra, hogy elhárítsák a fenyegetést. Általában csupán minden huszadik hivatalnál találunk ilyen munkatársi állományt. Ez az arány megközelítőleg azonos minden önkormányzati státusz esetében.

A többségében felkészült hivatali dolgozók minden ötödik hivatalban tevékenykednek, legtöbben a székhelyszervezetek esetében.

A részleteiben motivált és felkészült, valamint a kibertámadás során az érdemben alig használható munkatársak aránya minden hivatal esetében hasonló, és mindkét, a munkatársakra vonatkozó megjelölés a szervezetek közel egyharmadát érinti (előbbi aránya 34,4%, az utóbbié pedig 30,7% volt).

14. táblázat

Az önkormányzatra jellemző állítások a kibertámadások elhárítására motivált és felkészült munkatársak tekintetében

Forrás: saját szerkesztés

Közigazgatási-feladatellátási státusz	Kibertámadás esetén motivált és a támadások elhárítására felkészült munkatársak											
	Nem		Alig		Részleteiben		Többségében		Teljesen		Σ	
	db	%	db	%	db	%	db	%	db	%	db	%
Önálló	9	*8,8*	32	*31,4*	36	*35,3*	19	*18,6*	6	*5,9*	*102*	*100,0*
Közös hivatal székhely	7	*4,5*	46	*29,3*	59	*37,6*	37	*23,6*	8	*5,1*	*157*	*100,0*
Közös hivatal tag	30	*11,9*	79	*31,3*	81	*32,1*	50	*19,8*	12	*4,8*	*252*	*100,0*
Összesen	*46*	*9,0*	*157*	*30,7*	*176*	*34,4*	*106*	*20,7*	*26*	*5,1*	*511*	*100,0*

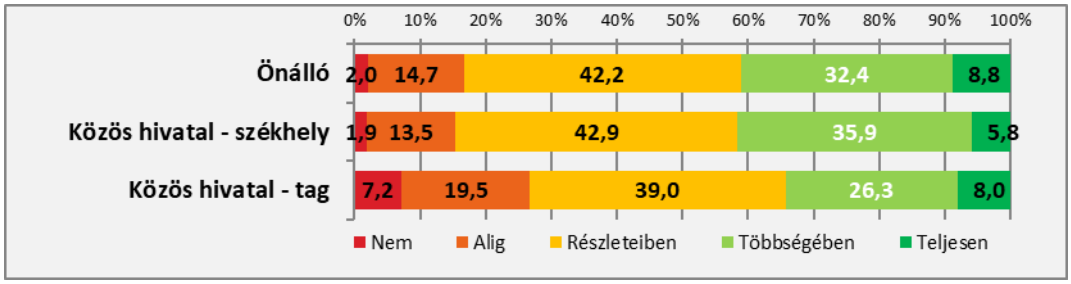
A legkevésbé vagy egyáltalán nem motivált és nem felkészült munkatársak aránya a kirendeltségként működő szervezetek esetében a legmagasabb (12,9%), ezeket követik az önálló hivatalok, és végül a központi hivatali egységek következnek, ahol csaknem harmadannyi a témában releváns dolgozók aránya, mint a kirendeltségeknél.

6. kérdés

Kibertámadás esetén adataink, online megjelenéseink megfelelően biztosítottak.

Egy kibertámadás esetén a hivatalok adatai és online megjelenései jellemzően csupán részleteiben, illetve többségében biztosítottak. A szervezetek 71,5%-ára igaz ez az állítás. A többségében biztosított tartalmak, adatok és megjelenési felületek leginkább a székhely- és az önálló hivatalokra illeszthetők elsősorban (32,4–35,9%), míg a kirendeltségek esetében csak minden negyedik szervezet jelenik meg ebben a csoportban.

A teljes mértékben biztosított adatok és megjelenések átlagosan a hivatalok 7,5%-ára jellemzőek, és a leginkább ilyenek az önállóan működő és a kirendeltség szervezetek.



42. ábra

Kibertámadás esetén az önkormányzatra jellemző állítások az adatok, online megjelenések megfelelő biztosítottsága tekintetében

Forrás: saját szerkesztés.

Az alig vagy az egyáltalában nem (megfelelően) biztosított adatok és online megjelenések leginkább a közös hivatalok kirendeltségszervezeteire jellemzőek, ahol minden negyedik hivatal ezeket az opciókat érzete sajátjának a válaszadáskor. Ez az érintettség pedig érezhetően jelentősebb, mint a másik két hivatali kategória esetében.

7. kérdés
Kibertámadás esetén történt sérülés után a helyreállítási terv alkalmazásával gyorsan működőképes a rendszerünk.

A kibertámadás okozta sérülések restaurációjának folyamatában csak nagyon komoly korlátok között számíthatnak a hivatalok a helyreállítási terv által nyújtott segítségre.

Átlagosan a hivatalok mindössze 6,5%-ában mondható teljesen kielégítőnek a helyzet, vagyis a helyreállítási terv teljes mértékben hozzájárul a rendszer gyorsan történő működőképessé tételéhez. Ez a csoport leginkább az önálló hivatalokra (minden tizedik szervezet) és legkevésbé a kistelepülések kirendeltséghivatalaira jellemző (minden huszonkettedik szervezet csupán).

Emellett többségében jellemző, hogy a helyreállítási terv a gyakorlatban is működik, a hivatalok átlagosan egynegyedében: a legnagyobb arányban – csaknem minden harmadik esetben – az önálló hivataloknál, míg legkevésbé a taghivatalok (minden ötödik szervezet) esetében.

A csupán részleteiben beszámítható helyreállítási terv a hivatalok 35–40%-ára vonatkozik, vagyis az egyes hivatali feladatellátási funkcióknak itt nincs jelentőségük.

15. táblázat

Kibertámadás esetén az önkormányzatra jellemző állítások a helyreállítási terv alkalmazhatósága tekintetében
Forrás: saját szerkesztés.

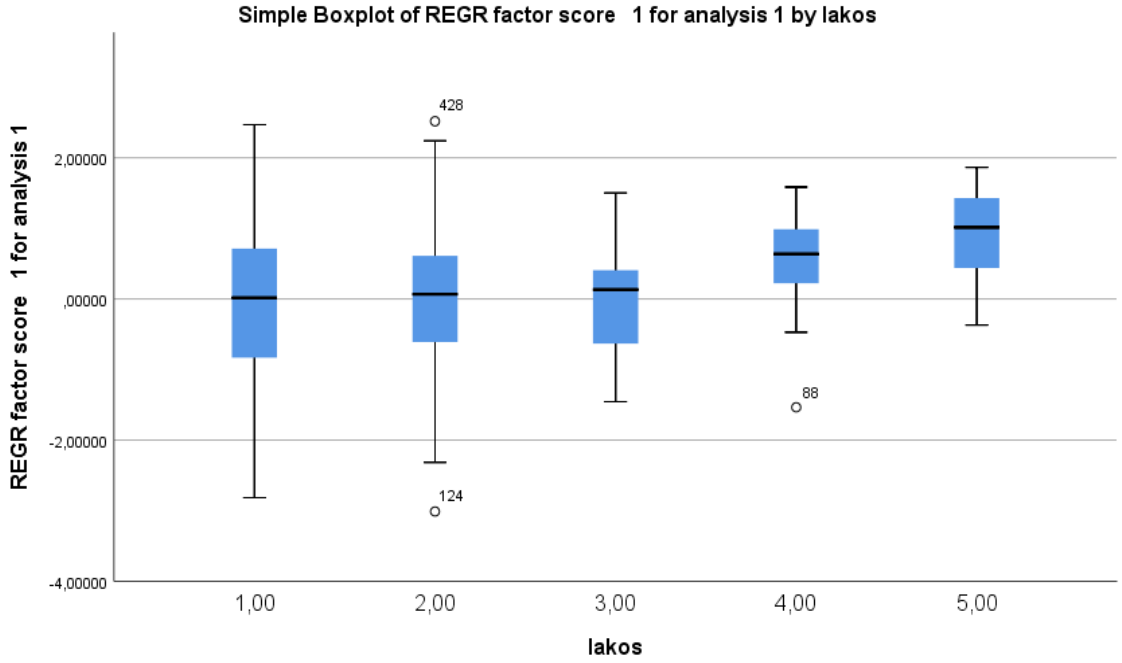
Közigazgatási-feladatellátási státusz	Kibertámadás (sérülés) esetén a helyreállítási terv által gyorsan működőképes a rendszer											
	Nem		Alig		Részleteiben		Többségében		Teljesen		Σ	
	db	%	db	%	db	%	db	%	db	%	db	%
Önálló	4	*3,9*	15	*14,7*	41	*40,2*	31	*30,4*	11	*10,8*	*102*	*100,0*
Közös hivatal székhely	12	*7,7*	40	*25,6*	56	*35,9*	37	*23,7*	11	*7,1*	*156*	*100,0*
Közös hivatal tag	43	*17,1*	64	*25,4*	86	*34,1*	48	*19,0*	11	*4,4*	*252*	*100,0*
Összesen	*59*	*11,6*	*119*	*23,3*	*183*	*35,9*	*116*	*22,7*	*33*	*6,5*	*510*	*100,0*

A csak alig, vagy egyáltalán nem hatásos helyreállítási tervek használata jellemzően a kirendeltségek esetében a legdominánsabb, mivel ezt a választási lehetőséget a érintett szervezetek több, mint 40%-a jelölte meg magára nézve jellemzőnek. Továbbá e kérdéskör tekintetében ez az a hivatali csoport, amelytől a legnagyobb arányban jöttek válaszok – csaknem minden hatodik szervezetről van szó. Esetükben lehetséges, hogy nincs is helyreállítási tervük.

A legalsó kategória megjelölése e hivatalcsoporton belül az esetek közel egyhatodában fordult elő, ami negatív irányba négyszer meghaladja az önálló hivatalok mutatóit, és egyúttal kétszer nagyobb a székhelyhivatalok értékénél is.

Főkomponens elemzés – felkészültség, képesség

Az önkormányzatok felkészültségének elemzése szignifkáns eredményt hozott mind lakosságszám, mind hivatali státusz szempontjából.

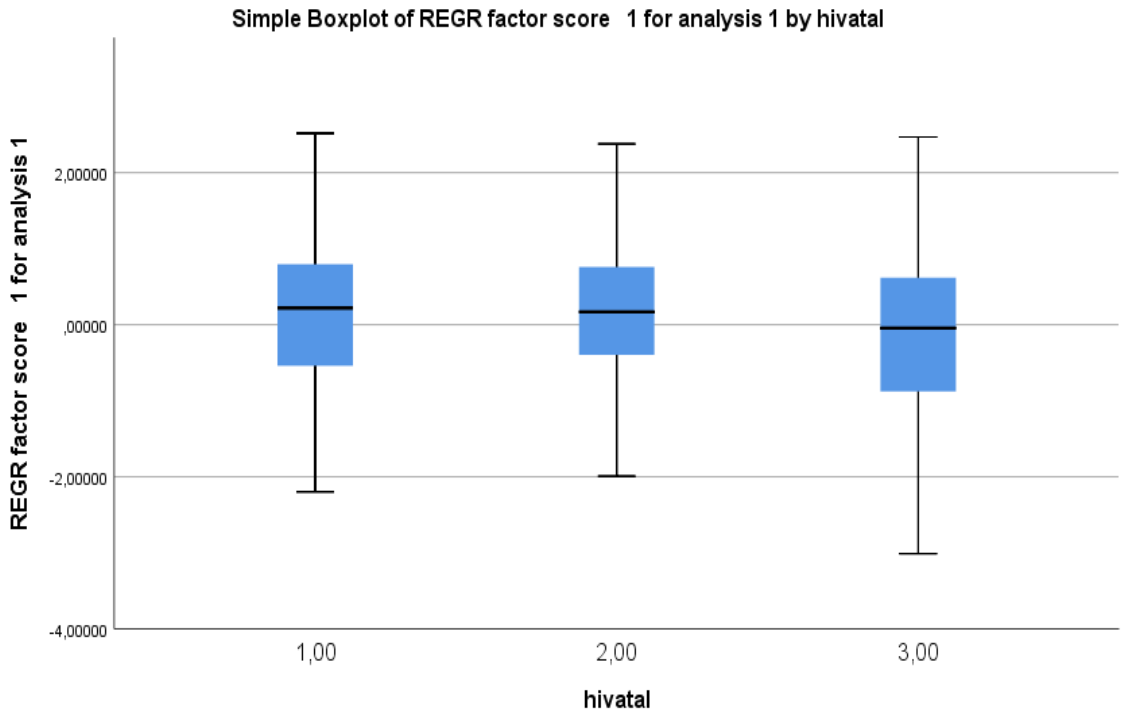


43. ábra

Felkészültség megítélése a különböző lakosságszám kategóriába tartozó települések esetében

Forrás: saját szerkesztés.

A 43. ábra jól szemlélteti, hogy lakosságszámot tekintve az 1-es csoport különbözik szignifikánsan az 5-östől. Azaz minél több lakos van egy településen, annál felkészültebbek a kibertámadásra. Ez nem jelent oksági összefüggést. Az feltételezhető, hogy a nagyobb települések erőforrásai számosabbak, azaz több lehetőségük van a szervezeti kompetenciáik fejlesztésére.



44. ábra

Felkészültség megítélése a különböző hivatali státuszú települések esetében

Forrás: saját szerkesztés.

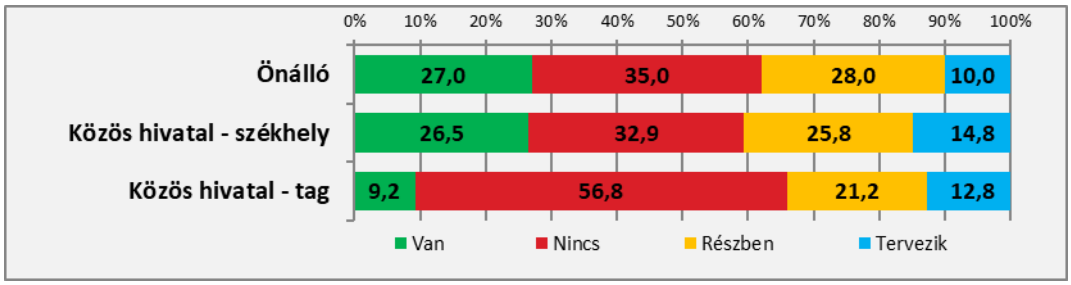
A hivatali státuszt tekintve a 3. csoportba tartozók különböznek szignifikánsan a többitől. A közös hivatalok tagjaira legkevésbé jellemző, hogy fel lennének készülve egy kibertámadásra. Ez megerősíti az előzőket, hiszen a kisebb lakosságszámú települések – jellemzően 1000 fő lakosságszám alattiak – a közös hivatalok tagjai és a nagyobb lakosságszámú települések tartoznak az önálló hivatalokat működtetők közé. Itt sem a hivatal státuszával, hanem a lakosságszám növekedésével vélelmezhető erőforrásnövekedéssel lehet oksági összefüggés.

4.2.5 Vizsgált terület (II.): felkészültség – képzettség – védekező/reagáló képesség Kötelezettségek – lehetőségek

1. kérdés

V**an-e protokoll az informatikai rendszeren elkövetett támadások esetére?**

Elég szomorú az az eredmény, hogy a válaszadók szerint az informatikai rendszeren elkövetett támadások esetére kevesebb, mint a negyedénél van kidolgozott protokoll. A kirendeltséghivatalok 9,2%-a, míg a székhely- és önálló hivatalok 26–27%-a rendelkezik ezzel.



45. ábra

Protokoll megléte kibertámadás esetére

Forrás: saját szerkesztés.

A leginkább jellemző státuszok: a nincs protokoll, vagy a részben meglévő eljárásrend kategóriái. Átlagosan a szervezetek 45%-a (a kirendeltségek 56,8%-a és a másik két hivatali csoport egyharmada) egyáltalán nem tud felmutatni protokollt, de további egynegyedük (24%) is csupán részben kidolgozott szakmai anyaggal rendelkezik (taghivatalok egyötöde és a másik két csoport 25,8–28%-a).

A hiányosságok pótlására átlagosan minden nyolcadik hivatalban betervezték a protokollok megalkotását, ezek közül is legnagyobb arányban a székhelyhivatalok (14,8%), a legkisebb hányadban pedig az önálló hivatalok (minden tizedik eset) szeretnék pótolni a mulasztásukat.

2. kérdés

Működik-e titkosítás a levelező rendszerhez kapcsolódóan?

A hivatali levelezőrendszerek használata átlagosan minden negyedik (27,5%) szervezetnél titkosított megfelelően. Az önálló hivatalok esetében ez az arány a szervezetek több, mint egyharmadára változik (36,6%), a másik két közigazgatási feladatellátási státusz esetén pedig a hivatalok átlagos mértéket produkálnak.

Sajnos a megfelelő szintű titkosításnál sokkal fajsúlyosabb annak hiánya. Teljes mértékben szabad és nem rejtett levelezés folyik a hivatalok 43%-ában, ezen belül is az önálló hivatalok egyharmadában (35,6%) és a kirendeltségként működő szervezetek kisebbik felében (46,6%).

16. táblázat

Az önkormányzatok levelezőrendszerének titkosítása

Forrás: saját szerkesztés.

Közigazgatási-feladatellátási státusz	Kötelezettségek – lehetőségek: a levelezőrendszer titkosítása									
	Van		Nincs		Részben		Tervezik		Σ	
	db	%	db	%	db	%	db	%	db	%
Önálló	37	*36,6*	36	*35,6*	22	*21,8*	6	*5,9*	*101*	*100,0*
Közös hivatal székhely	38	*24,5*	67	*43,2*	39	*25,2*	11	*7,1*	*155*	*100,0*
Közös hivatal tag	64	*25,7*	116	*46,6*	50	*20,1*	19	*7,6*	*249*	*100,0*
Összesen	*139*	*27,5*	*219*	*43,4*	*111*	*22,0*	*36*	*7,1*	*505*	*100,0*

Emellett minden feladatellátási státuszra jellemző, hogy az érintett hivatalok egynegyede, egyötöde csupán részben titkosított módszereket alkalmaz. A közös hivatalok esetében a központi szervezetnél ez az arány négyből egy egységre módosul (25,2%), míg a másik két hivatalcsoportnál marad a

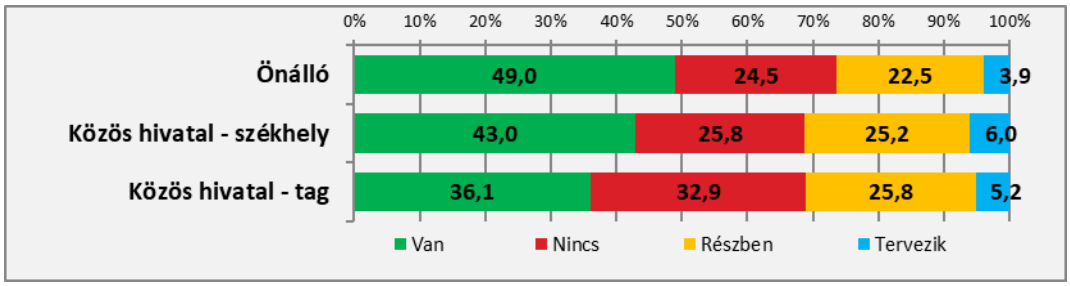
20,21%-os arány. Végül megemlítendő a hivatalok azon 7,1%-a is, amely tervezi, hogy titkosíttatja levelezőrendszerét.

3. kérdés

Működik-e jelszókezelési és -módosítási protokoll?

A különböző jelszavak kezelésére és módosítására a hivatalok kétharmadában (65,8%) részben vagy egészben áll rendelkezésre protokoll. A meglévő, komplett protokollok legnagyobb aránya az önállóan működő hivatalokhoz kapcsolható (a szervezetek fele: 49%), míg a legkisebb mértékben (az esetek egyharmada: 36,1%) a kirendeltséghivatalokra jellemző.

A nem komplex, csak részeiben kidolgozott eljárás minden hivataltípus egynegyedére jellemző (22,5–25,8%).



46. ábra

Protokoll megléte a jelszavak kezelésére és módosítására

Forrás: saját szerkesztés.

Ehhez hasonló az aránya a hiányzó protokollokat jelző hivataloknak is, annyi eltéréssel, hogy a legkisebb hivatalok esetében minden harmadik szervezet érintettsége felmerül (32,9%), míg a többi típusnál megmarad az egynegyedes arány. Végül protokollok létrehozását tervezik a jelszavak kezelésére és módosítására – átlagosan – minden huszadik hivatal esetében (5,1%).

4. kérdés

Van-e a külső rendszerekre kiszervezett feladatokhoz kapcsolódóan kockázatelemzés, kockázatmenedzsment-rendszer?

Olyan kockázatelemzés, kockázatmenedzsment, amely a külső rendszerekhez kapcsolódik, illetve a kiszervezett feladatok biztonságos elvégzését segítené, a vizsgált hivatalok jelentős részére nem jellemző. Átlagosan öt hivatalból három esetében ennek hiánya fedezhető fel (59%).

17. táblázat

Külső rendszerekre, kiszervezett feladatokra vonatkozó kockázatelemzés, kockázatmenedzsment megléte
Forrás: saját szerkesztés

Közigazgatási-feladatellátási státusz	Kötelezettségek – lehetőségek: kockázatelemzés									
	Van		Nincs		Részben		Tervezik		Σ	
	db	%	db	%	db	%	db	%	db	%
Önálló	23	*23,5*	51	*52,0*	22	*22,4*	2	*2,0*	*98*	*100,0*
Közös hivatal	34	*21,8*	76	*48,7*	34	*21,8*	12	*7,7*	*156*	*100,0*
Közös hivatal tag	26	*10,3*	172	*68,0*	36	*14,2*	19	*7,5*	*253*	*100,0*
Összesen	*83*	*16,4*	*299*	*59,0*	*92*	*18,1*	*33*	*6,5*	*507*	*100,0*

.

Ezen belül a székhelyhivatalok kisebbik felére (48,7%), valamint a kirendeltségek több, mint kétharmadára (68%) jellemző ez az állítás. Az önállóan működő hivataloknál is csaknem minden második eset említhető meg (52%).

Amennyiben nem létezőnek tekintjük a betervezett aktivitásokat is, akkor átlagosan 6,5%-kal emelkedni fog a hiányzó kategóriák arányszáma.

Átlagosan minden hatodik hivatal rendelkezik viszont a megfelelő kockázatelemzéssel és/vagy menedzsmenttel (16,4%). A kirendeltségek esetében ez az arány lecsökken 10%-ra, ami legalább a fele a másik két hivataltípusnál tapasztalt adatoknak, amelyek esetében minden negyedik, minden ötödik szervezet érintettségéről van szó (21,8% és 23,5%).

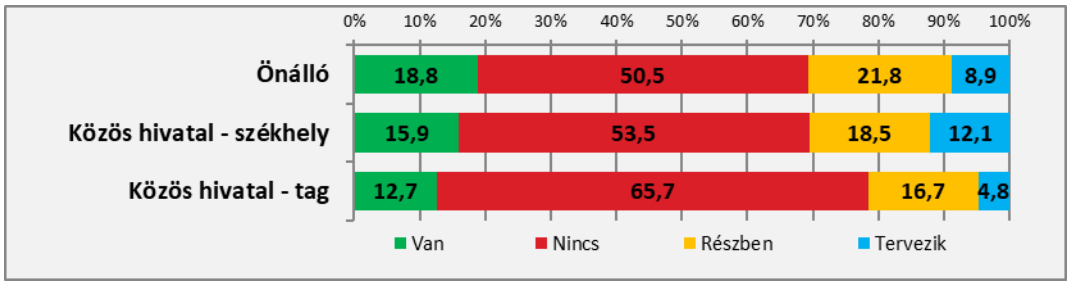
Végül, nem egészében, csak részeiben található meg a kockázatelemzés, illetve a kockázatmenedzsmentre kötelező feladatok szabályzata a hivatalok közel egyötödében (18,1%), ezen belül leginkább az önálló- és székhelyhivatalok esetében (21–22%), a legkevésbé van viszont a kirendeltséghivatalok csoportjában, ahol minden hetedik (14,2%) szervezet tart ennél az állapotnál a kifelé irányuló működési kapcsolatait illetően.

5. kérdés

Van-e rendszeresen fenyegetettséget tudatosító képzés a munkatársak részére?

A hivatalok átlagosan 60%-ában semmiféle olyan rendszeresen szervezett képzést nem jeleztek, amely témája a kiberfenyegetettség tudatosítása és az elhárítás személyes motiválása lenne. E megállapításon belül az önállóan működő és a székhelyként tevékenykedő hivatalok fele (50,5% és 53,5%), valamint a legkisebb mértékben a kirendeltséghivatalok kétharmada (65,7%) érintett a hiányolható képzések szempontjából.

Szervezett, irányított és rendszeres tematikus képzés csupán átlagosan minden hatodik-hetedik szervezet esetében figyelhető meg (14,9%). Legnagyobb arányban jellemző ez az önálló hivatalokra (ahol szinte minden ötödik szervezetre igaz: 18,8%), és legkevésbé a legkisebb hivatalokra (ahol minden nyolcadik szervezett jelezte ezt: 12,7%).



47. ábra

Rendszeres fenyegetettséget tudatosító képzés megléte a munkatársak részére

Forrás: saját szerkesztés.

A válaszoló szervezetek 16–22%-ában vannak ugyan próbálkozások, de a képzések vagy alkalmiak, vagy nem egészen tudatosak, így csak részben állnak rendelkezésre. Emellett tervezi minden tizenkettedik hivatal (7,9%), hogy beindítja a munkatársaknak a rendszeres képzést, de még jelenleg képzetlen a humánháttér e tekintetben.

A működési terület szakmai blokkot – a 3. kérdést – a főkomponens elemzés ehhez a komponenshez sorolta, így eredményeit itt mutatom be.

Van-e protokoll az informatikai rendszeren elkövetett támadások esetére, vannak-e védelmi mechanizmusok?

Az önkormányzati informatikai rendszereken elkövetett támadások esetében védelmi mechanizmusok, protokollok átlagosan csupán minden tizedik hivatal esetében adottak. Ezen belül az önállóan működő hivatalok egyötödének, a közös hivatalok esetében pedig a központi hivatalok egytizedének és a kirendeltségként működő szervezetek 6,5%-ának érintettsége körvonalazódik a válaszok alapján.

18. táblázat

Védelmi mechanizmusok, protokollok megléte a támadások esetére

Forrás: saját szerkesztés.

Közigazgatási-feladatellátási státusz	Informatikai védelmi mechanizmus, protokoll (támadások)							
	Van		Nincs		Részben		Σ	
	db	%	db	%	db	%	db	%
Önálló	20	20,0	41	41,0	39	39,0	100	100,0
Közös hivatal székhely	15	9,9	73	48,0	64	42,1	152	100,0
Közös hivatal tag	16	6,5	160	64,5	72	29,0	248	100,0
Összesen	51	10,2	274	54,8	175	35,0	500	100,0

Látható tehát, hogy nincsenek protokollok, védelmi mechanizmusok átlagosan a hivatalok több, mint a felében (54,8%). A legnagyobb mértékben ezek a taghivataloknál hiányoznak, ahol a szervezetek kétharmadában nincs protokoll és védelmi mechanizmus (64,5%), a legkevésbé jellemző pedig a székhelyhivatalokra a nevezett elemek hiánya, de a helyzet súlyosságát mutatja, hogy ebben a hivatali csoportban is minden második szervezet esetében pótolni szükséges a dokumentumokat.

Főkomponens elemzés – védekező/reagáló képesség

A sebezhetőséghez hasonlóan nincs szignifikáns kapcsolat a települési önkormányzatok esetében a lakosságszámmal, a hivatal típusával vagy a település jogállásával. Ez esetben vélelmezhető, hogy az elemzésbe bevont tényezőkön kívül még sok más egyéb tényező is befolyásolja: amelyek nem kerültek felmérésre. A későbbi vizsgálatok során vizsgálati terület lehet, hogy melyik elem vagy elemcsoport megléte vagy hiánya mutat szignifikáns összefüggést. Ennek feltárása segíthet optimalizálni a szervezeti erőfeszítéseket és növelheti a költséghatékonyságot.

Ettől függetlenül a meglévő eredmények azt mutatják, hogy az önkormányzatok védekező és reagáló képessége nagyon alacsony. A válaszadó önkormányzatok mintegy negyedénél van csak protokoll kialakítva egy esetleges kibertámadás esetére, a levelezőrendszer az önálló hivatalok esetében mintegy 37%-ánál, a többi önkormányzatnál pedig csak negyedénél titkosított, a jelszókezelési és módosítási eljárásrend is kevesebb, mint a válaszadók 50%-a esetében adott. A külső rendszerekre kiszervezett feladatokhoz kapcsolódóan kockázatelemzés, kockázatmenedzsment-rendszer működésére vonatkozóan a legmagasabb válaszadási arány az önálló hivatalok esetében érkezett, de ez is mindösszesen 23,5%, míg a közös hivatal tag önkormányzatai esetében ez 10,3%. Összességében kevés pozitív válasz érkezett a munkatársak tudatosító képzésére. Az önálló hivatalokkal rendelkező önkormányzatok esetében 18,8%, a közös hivatalhoz tartozó önkormányzatok esetében 12,7% és a közös hivatal székhely önkormányzatai esetében is csak a válaszadók 15,6 % nyilatkozta, hogy van náluk ilyen felkészítés. A működés során bekövetkezett támadás esetére pedig csak a válaszadók 10%-ának van eljárásrendje.

4.2.6. Vizsgált terület (III.): működési tapasztalatok

1. kérdés

Van-e ismeretük/információjuk informatikai eszközeik elleni támadásokról, volt-e már ilyen incidensük?

Az egyes, közigazgatási-feladatellátási státusz szerint besorolt hivatalok közül a legnagyobb arányban az önálló hivatalok esetében tapasztalható az, hogy voltak már támadások az informatikai eszközök ellen, illetve tudnak is ezekről az érintettek. A hivatalcsoportokon belül minden harmadik szervezet jelezte (31,7%) azt, hogy voltak már incidensek.

A közösen működtetett önkormányzati hivatalok esetében ennél vagy kevesebb támadás történt, vagy kevesebb ezzel kapcsolatban a meglévő ismeret, tájékoztatás. A székhelyként működő központi hivatalok egyötöde (20,6%) jelezte, hogy van tudomása támadásokról, míg a legkisebb hivataloknál ez az arány csupán 7,5%.

19 . táblázat

Megtörtént informatikai incidenssel kapcsolatos információ

Forrás: saját szerkesztés.

Közigazgatási-feladatellátási státusz	Információ informatikai támadásról					
	Van		Nincs		Σ	
	db	%	db	%	db	%
Önálló	32	*31,7*	69	*68,3*	*101*	*100,0*
Közös hivatal székhely	32	*20,6*	123	*79,4*	*155*	*100,0*
Közös hivatal tag	19	*7,5*	234	*92,5*	*253*	*100,0*
Összesen	*83*	*16,3*	*426*	*83,7*	*509*	*100,0*

A kirendeltségként működő szervezetek esetében valószínűsíthető, hogy esetükben nem arról van szó, hogy negyedannyi támadás érte volna a saját informatikai eszközeiket, mint az önálló hivatalokat, hanem inkább az lehet a háttérben, hogy a válaszoló személyek vagy nincsenek kellő mennyiségű, illetve minőségű információ és belső tájékoztatás birtokában a témával kapcsolatosan, vagy egyáltalán nem is vették észre az incidenseket.

2. kérdés

Ha történt incidens, mi történt? Hogyan kezelték?

Mindösszesen 83 esetben bekövetkezett támadásról, incidensről van tudomásunk. Közülük is 11 esetben nem kaptunk választ erre a kérdésre, a maradék 72 hivatali jelzés pedig szöveges információkat tartalmazott, és a válaszok a támadás fajtáját és/vagy az elvégzett feladatokat írták le.

Az *önálló hivatalok* esetében (27 válasz) a támadások megcélzott területei jellemzően a wifi-hálózatok, a levelezőrendszerek (vírusos levelek; a fiókok feltörése, a fiók feltörés után onnan spamek kiküldése), a weblap (feltörés, illetéktelen képek elhelyezése, a honlap lebénítása).

Az incidensek kezelése során általában az alábbi beavatkozásokat eszközölték: vírusirtás, fiókzárolás, biztonságosabb jelszavak beállítása, biztonsági mentésből visszaállítás, honlap működésének felfüggesztése, tűzfalak optimalizálása, portok tiltása, korlátozás fix IP-címekre, újraindítás, stb.).

A rendszerek természetesen több alkalommal is automatikusan kivédték a behatolásokat. Emellett kettő hivatal esetében nem tudták kezelni a problémákat. A támadások bekövetkezése után csupán egyetlen hivatal nevesítette azt, hogy náluk fejlesztés történt, így erősebb védekezési módszereket használnak azóta.

A *székhelyként működő hivatalok* (28 válasz) esetében érdekesség lehet, hogy egyetlen említés érkezett a levelezőrendszerek támadásával kapcsolatosan. Csupán a saját, vagy a települési weblapot érő incidenseket és a központi szervert ért támadásokat említettek meg.

Egyébként a támadások jellege és az okozott károk természete megegyezett a fentiekben felvázoltakkal, továbbá az elhárítás, a kármentés és a renoválás is hasonló módon zajlott.

A válaszok között egy alkalommal pedig arról szerezhettünk tudomást, hogy folyamatos képzéseik vannak (incidensre nem is került sor abban a hivatalban).

A *kirendeltségként* működő hivatalok válaszaiban (17 eset) a weblap nem jelenik meg, a támadások csaknem minden esetben a levelezőrendszerekhez köthetők. Ez érthető jelenség, hiszen a taghivatalok esetében fordul elő leggyakrabban, hogy nincs is saját, de akár települési weblap sem.

Elgondolkodtató viszont, hogy a 17 említett konkrét támadás közül három teljes sikerrel végződött, vagyis nem lehetett a számítógépeket megmenteni, azok az informatikai hulladékudvarokra kerültek, és új gépeket kellett helyettük beszerezni. Ilyen súlyos kimenetelű vagy lefolyású támadásokról nem olvashattunk az eddigi hivataltípusok esetében. Ez utalhat a munkatársak képzetlenségére és felkészítettlenségére, a képzések hiányára és a nem kellő tájékoztatásukra is, valamint a protokollok hiányára, az eszközök használatának nem megfelelő szabályozására is. Ezt a véleményt támasztják alá a három hivatal által megfogalmazott válaszok is.

Mind a három hivatal 1000 főnél kisebb lakosságszámú településen működik, és ebből két szervezet nem tartja veszélyesnek a kibertámadást, valamint annak következményeit sem. Emellett az egyes konkrét területeken a támadások valószínűségét általában 0–25% közé sorolták, viszont a hivatal sebezhetőségét felmérték, azt jellemzően közepesnek ítélték meg. A munkatársak felkészültsége véleményük szerint is alig jellemző. Továbbá információbiztonsági stratégia, adatkezelési szabályzat, protokoll nincs, a levelezőrendszerben titkosítást nem alkalmaznak és kockázatelemzéssel sem rendelkeznek. Fontos az is, hogy egyik hivatalban sincsenek fenyegetettséget tudatosító képzések, nincsenek védelmi mechanizmusok, viszont állításuk szerint az egyéb eszközöket a munkatársak csak engedéllyel használhatják.

Mint látható, a saját válaszok alapján gyakorlatilag biztonságtechnikai létminimumon tengődik a három hivatal. A rengeteg hiányosság eredménye egy idő után nem is vezethet máshová, mint egy valós kibertámadást követően a hulladékudvarra…

3. kérdés

A védekező/reagáló képesség főkomponenshez sorolta be a statisztikai elemzés és az alkalmazott struktúrának megfelelően részletesen ott szerepeltetem.

4. kérdés

Ha van protokoll vagy védelmi mechanizmus, akkor az milyen természetű?

A kérdésre mindösszesen 29 értékelhető válasz érkezett. A válaszokat kategorizálva az alábbi három csoport különíthető el.

Az *első csoportba* azok a válaszok tartoznak, amelyek a szabályozottságra, az előírások betartására helyezték leginkább a hangsúlyt. Ez esetben az informatikai Biztonsági Szabályzatot említették meg elsőként, de emellett egyéb belső rendelkezések is előírják a védekezéssel, a védelemmel kapcsolatos teendőket.

A *második csoportban a* védekezés technikai, technológiai jellege domborodik ki, ami fejlesztési elemeket is tartalmaz. Ide tartozik a vírusvédelem, a szoftverek és a tűzfalak fejlesztése, cseréje, emellett a biztonsági mentés, a külső merevlemezen történő adattárolás, a jelszavas egyéni védelmi rendszer kialakítása és az automatikus mechanizmusok mozgásterének kitágítása is.

A *harmadik csoport* a humánhátteret említette meg legfontosabb elemként. Olyan válaszok tartoznak ebbe a kategóriába, mint a szakember igénybevétele; az informatikus azonnali beavatkozása; a rendszergazda folyamatos készenléte és felügyelete, vagy az információbiztonsági felelős utasításai szerinti eljárásrend követése.

Fontos megjegyezni, hogy megemlítődött – igaz, hogy csupán egyetlen alkalommal – a kollégák folyamatos képzése az esetleges kibertámadások kezelésével kapcsolatban.

A legkisebb lakosságszámú településeken (1–1000 fő) elsősorban kirendeltséghivatalokkal találkozhatunk. Esetükben a kibertámadásokkal kapcsolatos védelmi mechanizmusok elsősorban a második csoport elemeire épülnek: vírusvédelem, tűzfal, biztonsági mentés és legfeljebb egyfajta szabályzat.

Ezeket a válaszokat minden esetben olyan hivatalok adták, amelyek az önkormányzat szempontjából egy kibertámadás lehetőségét nem tartották veszélyesnek, vagy legfeljebb közepes kockázatot láttak benne.

Ennek ellenpólusaként, az *önálló hivatalok* esetében a fent jelzett mindhárom, eltérő hangsúlyokat előtérbe helyező védelmimechanizmus-faktor egyaránt megjelenik a válaszokban, vagyis a kibertámadások elleni védekezés egy sokkal komplexebb, fejlettebb és modernebb formája körvonalazódik e hivatalok esetében, szemben a legkisebb települések önkormányzatainak esetével.

5. kérdés

Mi történik a régi informatikai eszközökkel?

Azon informatikai eszközök, amelyekre már nincs szüksége a hivataloknak, legtöbbször raktározásra, tárolásra kerülnek. Összesen 330 hivatal jelezte, hogy elsősorban ezt a módszert alkalmazzák. Ez a vizsgált szervezetek közel kétharmada (65,7%).

A kistelepülések taghivatalai a leggyakrabban – az esetek több, mint felében –, a központi hivatalok minden negyedik esetben és az önálló hivatalok közül minden hatodik alkalmazza a gépek átmeneti vagy végső tárolását.

A raktározás mellett a hivatalok előszeretettel értékesítik a lecserélendő számítógépeiket. Általában munkatársaknak kínálják fel megvételre a gépeket, de természetesen külső értékesítés is szóba jöhet.

A munkatársaknak történő eladásról 28 esetben van konkrét tudomásuk a válaszadóknak, ezek legnagyobb aránya a kistelepülések hivatalaihoz kapcsolódik, esetükben a régi gépek 40%-a valamelyik addigi felhasználónál köt ki. Emellett az ilyen tranzakciók fele a közös hivatalokra, egyötödük pedig az önállóan működő szervezetekre jellemző. Az elavult, lecserélendő számítógépek ajándékozás útján is kikerülnek a hivatalokból. A kistelepüléseken jellemző az ajándékozások csaknem fele (47,8%), az esetek jelentős részében a település más önkormányzati fenntartású intézményéhez vagy civil szervezetekhez kerülnek a számítógépek. A székhelyhivatalok az egyharmadát, míg az önálló szervezetek az ötödét valósítják meg az ajándékozásoknak.

A fentiek mellett *egyéb lehetőségek* is várnak a leselejtezett számítógépekre. Minden ötödik hivatali válasz ebbe a kategóriába tartozik (19,5%; 98 eset). A kategória jelentős része a gépek fizikai megsemmisítésének lehetőségeit mutatja be, összesen 36 hivatal jelzi a gépek elektronikai hulladékként történő leadását vagy elszállítását, bontását.

Emellett az egyéb kategóriába kerültek a nem tiszta, hanem kevert válaszok is. Ezek olyan hivatali gyakorlatokról számolnak be, amelyekben több módszer is általánosan alkalmazott – ilyen gyakorlat 59 szervezet esetében volt elkülöníthető. Végül ebbe a válaszcsoportba soroltuk azokat a hivatalokat is, amelyek esetében még soha nem történt meg, hogy megváltak voltak a gépeiktől. Esetükben nagyon idős számítógépekről van szó, amelyeket rendszeresen használnak a hivatali munkában. Lecserélésükre eddig nem volt lehetőség, és nincsen gyakorlatuk arra nézve, hogy milyen módszereket alkalmazhatnának, ha lecserélhetnék a jelen gépparkot. Összesen három hivatal jelezte ezt.

6. kérdés

Hogyan szabályozzák az egyéb eszközök (telefon, tablet, adathordozó) munkahelyi használatát?

A hivatalokban dolgozók egyéb eszközeinek használatára jellemző, hogy hasonló arányban vannak azon szervezetek, ahol mindenki szabadon használhatja eszközeit (46,5%), és ahol engedélyhez és/vagy szabályzathoz, utasításhoz kötött azok használata (utóbbi a hivatalok fele; 50%).

Nincs jelentős különbség a tekintetben, hogy az engedélyhez kötött, vagy éppen a szabad használattal érintett szervezetek milyen feladatellátási státuszban vannak.

Az esetek néhány százalékában – a fentiek mellett – előfordul az a helyzet is, mikor tilos a munkatársaknak egyéb eszközöket használniuk, és nem szabad a belső rendszerhez, hálózathoz kapcsolódniuk sem. Ez nem nagy számban, átlagosan a hivatalok 2,6%-ában fordul elő, és az eltérés itt sem jelentős az egyes hivatalcsoportok között. Megemlítendő, hogy e gyakorlat alkalmazása 13 hivatalt érint, amelyek közül három kivételével mind dunántúli, és több, mint a fele legfeljebb 5000 fős településhez kapcsolható, emellett a hivatalok fele kirendeltségként működik, 5 pedig székhelyhivatalként.

Az egyéb kategóriába olyan válaszok (5 eset) tartoznak, mint például: nincsenek írott szabályzatok, vagy telefonszabályzat van, de tablethasználat esetére nincs előírás, illetve szabad az egyéb eszközök használata, de kizárólag munkavégzéshez stb.

7. kérdés

Mik a közösségi média használatával kapcsolatos tapasztalataik? (honlap, Facebook, stb.)

Mindösszesen 218 értékelhető válasz állt rendelkezésre az elemzéshez. A hivatalok válaszaiban keverednek a munkahelyhez, a munkafolyamatokhoz kapcsolódó, továbbá a válaszoló személyek privát véleményei is, utóbbiak viszont az egyéni felhasználói tapasztalataikon alapultak.

A közösségi médiafelületekről általában csak azokat a válaszokat, véleményeket rögzítjük, amelyek nem igyekeznek megduplázni az egész elemzésben feltártakat, inkább színesítik, illetve más szemszögből is megvilágítják azokat. Emellett persze a tömegesen jelentkező válaszok kvázi törvényszerűségek, amiknek alapján általános jegyek felvázolására is kísérletet teszünk.

- A települési honlap megléte nagyban elősegíti a lakosság és az érdeklődők tájékozódását a településről, az önkormányzat és a hivatal munkájáról, a közösségi programokról.
- A honlap mint információhordozó jól betölti szerepét, jó tájékoztatási forma.

- Számos vélemény szól arról, hogy az önkormányzat kizárólag a honlapját használja, más közösségi portálokat nem.
- Általános megállapítás, hogy nagyon sok helyen szabadon használhatók, mindenki hozzáférhet munkaidőben is, vagy éppen ellenkezőleg, tiltott a használata vagy erősen szabályozott, engedélyköteles. Nagyszámú hivatalban csak indokolt esetben használnak közösségi médiát, más szervezeteknél viszont a munkatársak szívesen használják ezeket. Emellett vannak olyan önkormányzatok, ahol hivatali számítógépeken nem javasolt vagy tilos a közösségi lapok használata.
- Munkaidőben nem javasolt – sok településen – e webhelyek használata, vagy munkaidőben hivatali eszközön tiltott a magáncélú használatuk.
- Munkaidőben csak azok a személyek használhatják ezeket a portálokat, akiknek a munkafeladataik ellátását megköveteli (például szemlézés okán).
- A Facebook a hivatalok nagy csoportjánál kifejezetten letiltott.
- A hivatali honlapot és a facebookprofilt az arra jogosultak tudják csak kezelni.
- ASP-hez kapcsolódó, az ügyintézők munkáját segítő csoportok használata napi szinten mindenhol megengedett.
- Az információáramlás miatt fontos a Facebook.
- Az FB kialakult szellemisége nem teszi alkalmassá „hivatalos” kommunikációs célokra, mégis jelenleg a leghatékonyabb eszköz.
- Az idős korosztály a honlapot nem látogatja. A Facebookon hamarabb megtalálunk személyeket, például hagyatéki eljáráshoz kapcsolódóan, vagyis a munkánkat segíti.
- A Facebookon sok olyan komment, hozzászólás van, amely nincs kontrollálva. Sokszor indokolatlanul negatív vélemények is felkerülnek és gyorsan terjednek.
- A Facebook részben jó, de vannak butaságok is rajta, ezért én ritkán használom. Ügyfelek néha ezen keresnek meg problémáikkal. Ez esetenként segíti a kommunikációt.
- A Facebook lehet veszélyforrás is, a legtöbb támadás ezeken a felületeken kerül be a rendszerekbe. Minél többen használják, annál több felhasználónál tudnak kárt okozni.
- A Facebook hasznos, bár a sok információval van, aki nem tud mit kezdeni, és van, aki visszaél vele.

4.2.7. Önkormányzatok kiberbiztonsági kérdőívének fő megállapításai

A kérdőív elemzése leíró statisztikai és főkomponens módszerrel történt.

A főkomponens elemzésbe a kiberbiztonsággal kapcsolatosan az alábbi kérdéscsoportok kerültek bevonásra:

- Mennyire tartja veszélyesnek a bekövetkezés lehetőségét?
- Adott területen mennyire tartja valószínűnek a bekövetkezést?
- a felkészültséget jellemző kérdéseket és
- a kiberbiztonság biztosítását szolgáló területekre adott válaszokat.

Az elemzés öt fő komponenst kínált fel:

1. felkészültség, képesség;
2. kiberfenyegetettség megítélése;
3. sebezhetőség;
4. védekező/reagáló képesség;
5. szabályozás rendelkezésre állása.

Az egyes komponensek szignifikanciáját teszteltem két változóra: a települések lakosságszáma és a hivatalok típusa szerint.

Az egyes komponenseket az adott részen belül tárgyalom. Vizsgált területek:

- Kibertér – kiberbiztonság
- Felkészültség – képesség
- Működési tapasztaltok

Az egyes területek megállapításai:

I. Kibertér – kiberbiztonság

Az első blokk kérdési a válaszadók véleményét vizsgálta a kiberfenyegetettség veszélyességének, bekövetkezési valószínűségének és az egyes területek sebezhetősége kapcsán, továbbá, hogy mit gondolnak a védekezés módjáról.

Kiberfenyegetettség megítélése

A válaszadók közel 27%-a nem tartja veszélyesnek egy kibertámadás bekövetkezését. A válaszokat a települések lakosságszáma szerint csoportosítva azt láthatjuk, hogy minél nagyobb egy település, annál kevésbé becsüli alá egy kibertámadás bekövetkezésének valószínűségét. A válaszadók 5,5–12,7%-a kizártnak tartja, emellett 1,4–10,2% tartja biztosan bekövetkezőnek. Az itt vizsgált területek közül a legvalószínűbbnek a rosszindulatú támadásokat, míg a legkevésbé valószínűnek a közszolgáltatások elleni támadásokat tartják. Beszédes, hogy összességében hivatalok 70%-a a támadások bekövetkezésének lehetőségét 50% alá becsülte.

Az egyes részek elemzése változatos képet mutat. Összességében vizsgálva a második legnagyobb magyarázó erővel bíró komponens – a kiberfenyegetettség megítélése – eredménye szerint a lakosságszám hozott szignifikáns eredményt. E szerint az öt csoportba sorolt települések közül a legkisebb (1000 fő alatt) és a legnagyobb (50 001 főnél nagyobb) lakosságszámmal rendelkező települések tartják a kiberfenyegetettséget a legkevesebbre.

A szakirodalom, a nemzetközi tapasztalatok és a fókuszcsoportos interjún elhangzottak alapján a kistelepülések saját rendszerüket nem gondolják támadásra érdemesnek, míg a nagy települések esetében túlzott magabiztosságról lehet szó. Az önkormányzatok mint könnyen bevehető célpontok – figyelembe véve a kibertámadások megváltozott mintázatát – nemzeti szinten okozhatnak komoly nehézséget. Ez nem jelenti azt, hogy a másik 3 kategóriába tartozó települések válaszadói kiemeltnek tartanák a kiberfenyegetettséget, csupán annyit, hogy az előző két csoporthoz

képest gondolják valószínűbbnek. E területen a vezetői (polgármester, jegyző) tudatosság növelése elengedhetetlen a kockázat csökkentése érdekében.

Sebezhetőségről alkotott vélemények

A sebezhetőség vizsgálata során a válaszok tanúsága szerint nagy a bizonytalanság és az eltérés a sebezhetőség mértéke és az érintett területek kapcsán. A vizsgált elemek (kommunikáció, munkafolyamatok, információk biztonsága, rendszerek biztonsága, közbiztonság) sebezhetőségével kapcsolatosan (29. ábra) összességében a legkevésbé sebezhetőnek az információs rendszerekben tárolt adatokat találták (9,5%). Minden egyéb kategóriában 10% felett volt azon válaszadók aránya, akik elhanyagolhatónak, és 30% körül, akik alig sebezhetőnek ítélték az egyes elemeket. A válaszok átlaga alapján közel 40% gondolja közepesen sebezhetőnek a vizsgált elemeket. Sebezhetőnek 12–18,4% között vélelmezték az egyes elemeket, míg a legsebezhetőbbnek – minimális eltéréssel a többi elemtől és igen alacsony (5,5%) mértékben – az IKT rendszer technikai infrastruktúráját találták. Az eredmények nagyon széles spektrumon mozognak, de összességében nem árulkodnak a válaszadó hivatalnokok aggodalmáról az önkormányzat különböző folyamatainak, rendszerinek sebezhetősége miatt. A fókuszcsoporton tapasztaltak ennek jelentősen ellentmondanak, mert az ott elhangzott megállapítások szerint megfelelő szándék esetén az önkormányzati rendszereket védhetetlennek ítélték a jelenlegi technológiai rendszerek és a környezet mellett, illetve a hivatalok felkészültsége és a munkatársak tudatossága alapján.

A magyarázó erő szerinti harmadik főkomponens – sebezhetőség – elemzése nem mutatott szignifikáns összefüggést egyik változóval sem. Ez alapján vélelmezhető, hogy a vizsgálat vagy nem vizsgálta az összes sebezhetőséget befolyásoló elemet, vagy ez ezektől független.

II. Felkészültség/képesség

A második szakmai blokk azt vizsgálta, hogy milyen állítások jellemzik az önkormányzatok felkészültségét, képességét arra, hogy a kiberbiztonsági kérdéseket kezeljék, és milyen módszereket használnak, hogy a kötelezettségeiknek eleget tegyenek. Az e részben megfogalmazott állítások, kérdésekre adott válaszok adják az önkormányzatok kiberbiztonsági kérdéskörrel kapcsolatos véleményének legfontosabb részét. A főkomponens elemzés három komponenst adott ehhez a blokkhoz kapcsolódóan: a felkészültséget, képességet magyarázó komponenst, ami a legnagyobb magyarázóerővel rendelkezik, a negyediket a kiberbiztonságot elősegítő folyamatok meglétéhez és az ötödiket, a szabályozás rendelkezésre állásához kapcsolódót.

Felkészültség – képesség

Az önkormányzatokat jellemző állításokra adott válaszok az egyes területekről alkotott véleményt mutatják. A válaszadók 8 állítást 1–5-ig terjedő skálán értékeltek, ahol az 1-es a nem jellemzőt, míg az 5-ös a teljesen jellemzőt jelentette. Az állítások a rendszerek és hálózatok védettségéről, a rendszerhasználati szabályokról, a fejlesztésről, a munkatársak felkészültségéről és motiváltságáról, a hardver és szoftver elemek frissességéről, az online adatok biztonságáról és a helyreállítási terv meglétéről szóltak.

Az egyes kérdésekre adott válaszok részletesen elemzésre kerültek a hivatali státusz (önálló, közös hivatal székhely és közös hivatal tag) és a települések lakosságszáma szerinti csoportosításban. A rendszerek és hálózatok védettsége tekintetében optimista vélemények érkeztek a taghivatalok esetében is: közel 50%-osnak ítélték ezt, míg az önálló hivatalok esetében 69,8%-ról beszélhetünk. A rendszerhasználatot inkább szabályozottnak ítélték a válaszadók. A beérkezett válaszok alapján van és folyamatos az infrastrukturális fejlesztés az önkormányzatoknál, ami a vélemények szerint a hivatalok több, mint 50%-ában (47,5–57,9%) segíti a kiberbiztonság biztosítását. Ez egyben azt is jelenti, hogy a maradék hivatalok esetében csak részleteiben, vagy alig, esetleg nincs olyan fejlesztés, ami támogatná e cél elérését. Ez a legkevésbé az önálló hivatalokra (42,2%), és leginkább a közös hivatal tag önkormányzatokra (52,5%) jellemző. Az 5. a számítógépek és szoftverek állapotáról és a frissítésről szólt, szorosan kapcsolódva a harmadikhoz. Ez esetben viszont már kevésbé volt pozitív a válaszadók véleménye. A konkrét elemek esetén az előző eredményekhez nagyon hasonló válaszok érkeztek. Az önálló és székhely hivatalok esetében 54,1%, a tag hivatalok esetében 38,3% gondolja, hogy a gépeik és szoftvereik modernek és megfelelő módon frissítettek. Természetesen ennek a mérlegnek a másik oldalán azok vannak, amelyek esetében ez részleteiben, alig vagy egyáltalán nem így van. A legelavultabb és nem frissített szoftverállományt a tag hivatalok válaszadói jelezték (61,7%).

A munkatársak felkészültségével és motivációjával a 4. és a 6. kérdés foglalkozott. A válaszadók szerint a munkatársak inkább nem felkészültek. Hivataltípustól függetlenül 28–33,1%-os arány lett az eredmény. A felkészültség kapcsán nem várt eredmény, hogy az önálló hivatalok esetében ítélték a felkészült munkatársak arányát a legalacsonyabbnak (5,1%), és a legmagasabbra a taghivatalok esetében (9,1%). A 6. kérdés – *Kibertámadás során kire számíthatnak a hivatalok, és mennyire felkészültek a munkatársak?* – esetében is igen alacsony számokat adott a vizsgálat. A legmagasabb a székhely hivatalok (28,7%), míg a közel azonos (24,5–24,6%) eredmény született az önálló és tag hivatalok esetében. Jelentős eltérés a hivatalok között a munkatársak felkészültsége és motiváltságára vonatkozóan – a válaszok alapján – nem fedezhető fel.

Az adatok és online megjelenés biztonságával kapcsolatban jelentős eltérés mutatkozik az önálló, székhely és a tag hivatalok között. A tag hivatalok jelentős százaléka (26,7) esetében alig vagy nem biztosított, míg a székhely és önálló hivatalok esetében ez csak 15,3–16,7%.

A válaszadók szerint kibertámadás esetére van helyreállítási terve az önálló hivatalok több, mint 40%-nak, és nincs vagy alig a taghivatalok több, mint 40%-nak.

A főkomponens elemzés szignifikáns eredményt hozott mind a lakosságszám, mind a hivatal típusa szerint. A lakosságszám szerinti eredmény alapján, minél nagyobb lakosságszámú egy település, annál jobban felkészült, és rendelkezik a szükséges kompetenciákkal a kiberbiztonság biztosítása érdekében. A hivatali státusz szerinti eredmény nagyon hasonló, vagyis az önálló hivatalokra jellemző, hogy jobban fel vannak készülve egy kibertámadásra és annak kezelésére.

Védekező/reagáló képesség

A kiberbiztonságot támogató folyamatok megléte főkomponensbe a kötelezettségeket és lehetőségeket összefoglaló kérdések közül a 3. – 7. kérdésket és az informatikai rendszerek elleni támadás és a működési tapasztalatok köréből a támadások esetére kialakított protokollokat, védelmi mechanizmusok kérdések eredményeit sorolta az analízis.

A kötelezettségek, lehetőségek kérdésblokkon belül felmérésre került, hogy milyen védekező, reagáló képességgel rendelkeznek az önkormányzatok egy esetlegesen bekövetkező vagy bekövetkezett támadás esetén. A legjobb eredményt *a jelszó kezelése és módosítása protokoll megléte* kérdésre érkezett. Önálló hivatalok esetében 49%, közös hivatal székhelye esetében 43% és a tag önkormányzatok esetében 36,1% rendelkezik ilyen típusú protokollal. A kiszervezésekhez kapcsolódó feladatok megléte nem jellemző a válaszadók szerint. Az összes válaszadóból 59% jelezte ennek hiányát. A legalacsonyabb értékeket a tudatosító képzések és a bekövetkezett támadás esetén alkalmazandó eljárásrend hiányára adott válaszok mutatják. Az eredmények szerint az önkormányzatok védekező és reagáló képessége rendkívül alacsony.

A főkomponens elemzés – hasonlóan a sebezhetőséghez – nem hozott szignifikáns eredményt egyik változó esetében sem. Ez jelentheti azt, hogy sok egyéb tényező is meghatározza ezt a területet. További vizsgálat lenne szükséges, mivel ennek feltárása vélelmezhetően hatással lenne az erőforrások és erőfeszítések optimalizálására.

III. Működési tapasztalatok

A harmadik szakmai blokkja az online kérdőívnek a működési tapasztalatokra adott válaszokat célozta összegyűjteni.

Információbiztonsági incidenst a válaszadók közül 83 három esetben tapasztaltak. Ebből azonos számmal volt érintett (32 alkalom) önálló hivatal és közös hivatal székhely. A tag önkormányzatok közül mindösszesen 19 esetben jeleztek információbiztonsági eseményt. A visszajelzések alapján az önálló hivatalok esetében jellemzően a wifi-hálózatokat, levelező rendszereket támadták, ami mind jelentős lökést adott az érintett önkormányzatok számára a téma iránti fogékonyságnak. A székhelyként működő hivatalok inkább weblap és szerverek elleni támadásokat említettek. A tag önkormányzatoknál az incidensek a levelezőrendszerhez kötődtek. Ebből a körből három olyan esetről számoltak be a válaszadók, amikor a sikeres támadás teljesen tönkre tette a rendszert és az eszközöket.

A védekezési módra vonatkozóan három csoportba sorolhatók a válaszok. Az első csoport a szabályozottságot, a második a technológiát, a harmadik pedig az emberi tényező fejlesztését emelte ki.

A régi eszközök kapcsán vegyes a kép. A válaszadók véleménye szerint a leselejtezett gépekkel kapcsolatosan nem merül fel kockázat.

A mobileszközök használatával kapcsolatos válaszok alapján – a kiberfenyegetettséggel kapcsolatos alacsony megítéléshez hasonlóan – nincs veszélyérzete a válaszadó önkormányzatoknak. Csupán

néhány %-ban jelezték, hogy tilos használni egyéb eszközöket; ezek a hivatalok 46,5%-ban szabadon használhatóak, 50% esetében pedig engedélyhez kötöttek. A közösségi felületekkel kapcsolatosan – nem volt kötelező kitölteni – csak 218 válasz érkezett. Ezek is jelentősen keverednek a magánhasználat során szerzett tapasztalatokkal, használatuk kevés helyen tiltott.

4.3. Az önkormányzatok online megjelenési képessége – webability

Ahogy az előzőekben láthattuk az önkormányzatokra jelentős feladatot ró az Infotv. elvárása a közérdekű adatok közzétételével kapcsolatban. Ugyanakkor azt sem szabad elfelejteni, hogy milyen lehetőséget kínál a megfelelő online megjelenés. Egy jól használható, informatív, integrált online megjelenés növeli az állampolgári elégedettséget, csökkenti a hivatal leterheltségét és pozitívan hat a település fejlődésére. Az állampolgárok számára az önkormányzat képviseli – a legtöbb településen – az államot. Az okos eszközök, az internet tömeges használatának következtében megváltoztak az állampolgárok informálódási szokásai és igényei, amihez a kormányzat és az önkormányzatok nehezen alkalmazkodnak. Kétségtelen tény, hogy az önkormányzati hivatalok kapacitáshiánya, a területen lévő általános szakemberhiány miatt saját belső tudásukra kell támaszkodniuk, vagy külső szolgáltatót igénybe venniük – utóbbinak minden kockázatával.

A digitális állam, az e-közigazgatás sikerének záloga a digitális írástudás, azonban a közszférában van javítanivaló e tekintetben. A közszféra egyik innovációs lehetősége – amivel az angolszász és skandináv országok kiválóan élnek – a tudásmegosztás online módjaival való integrált kísérletezés. Felismerve az adatok és a fejlesztési folyamatok megnyitásából fakadó innovációs lehetőségeket, és az ezzel együtt járó költséghatékonysági és hosszú távú bizalmi hasznot, egyszerre működtetnek zárt és teljesen nyitott rendszereket is.

A fentiekből kifolyólag az egyik, talán a legfontosabb eleme lehetne a jövőbeni tudatos digitális transzformációt segítő politikának egy hazai önkormányzati tudásmegosztó hálózat létrehozása.

4.3.1. A vizsgálat háttere

A Belügyminisztérium 2017 májusától 2018. január végéig áttekintette a teljes önkormányzati webes megjelenést. A horizontális adatfelvétel az általános szempontokon túl több szempontból is vizsgálta az önkormányzatok online megjelenését.[17]

4.3.2. Az önkormányzatok online megjelenésének statisztikai elemzése

Faktoranalízis

Az önkormányzatok online megjelenését vizsgálva 12 változót vetettem alá faktoranalízisnek (7. melléklet), amit főkomponens módszerrel, a faktorok rotálását pedig varimax rotációval végeztem. Az adatelemzés az SPSS Statistics 20 szoftver segítségével történt.

Az elemzés előtt megvizsgáltam az adatokat a faktoranalízis alkalmazhatóságának szempontjából.

Az alkalmazhatóság feltételei

[17] Az adatok másodelemzésére kaptam engedélyt és lehetőséget.

Az anti-image korrelációs mátrix MSA (0,609 és 0,919 közötti) értékei alapján megállapítható, hogy a vizsgálatban szereplő egyes változókat a többi változó elenyésző hibanagysággal becsüli, így változó kizárására nem volt szükség.

A 12 változó *megfelelően* alkalmas a faktorelemzésre, amit a Bartlett-teszt (chi2 = 9180,9808, df = 66, sig. = 0,000), valamint a Kaiser–Meyer–Olkin-kritérium (KMO) is alátámasztott (KMO = 0,792).

A faktorok száma

A faktorok számának meghatározását két módszerrel is elvégeztem. Mind a Kaiser-kritérium (legalább 1 sajátértékkel rendelkező faktorok figyelembe vétele), mind a varianciahányad módszere (legalább 60%-os magyarázott összes variancia) 4 faktor alkalmazását indokolta. A 4 faktor az összes variancia 64,782%-át képes megmagyarázni.

A faktoranalízis eredményei és a faktorok értelmezése

A rotált komponensmátrix elemei alapján eredményként az 4. táblázatban látható változókból 4 faktor képezhető. Minél nagyobb a faktorsúly abszolút értéke, annál fontosabb szerepet játszik az adott változó a faktorban.

20. táblázat

Az önkormányzatok online megjelenésének rotált komponensmátrixa (faktormátrixa)

Forrás: a BM horizontális weblapértékelése (főkomponens módszer, varimax rotáció [KMO=0,792]) alapján saját szerkesztés.

	Faktor			
	1	2	3	4
A honlap menüpontjainak áttekinthetősége	0,869			
A honlap kezdőlapjának áttekinthetősége	0,864			
A tájékoztatás közérthetősége	0,612			
Az önkormányzat munkájáról, az ellátott feladatokról, eredményekről való megfelelő tájékoztatás megjelenítése		0,836		
Az önkormányzat által nyújtott szolgáltatásokkal kapcsolatos információk kereshetősége/megléte/közzététele		0,827		
A települési/önkormányzati stratégiákra vonatkozó dokumentumok közzététele		0,574		
A települési/önkormányzati programokra vonatkozó dokumentumok közzététele			0,772	
A honlap utolsó frissítésének dátuma			-0,687	
Információ, adatbázis elérhetősége az önkormányzat által fenntartott vagy működtetett intézményekről			0,579	
A weboldal a lakosság számára fontos és használható adatbázis-szolgáltatása			0,415	
A település Facebook oldalára vezető hivatkozás/link megléte				0,886
A Facebook honlapba való integráltsága				0,882

A kialakított négy faktor a következő:

F1: Felhasználóbarát kialakítás (user friendly)

F2: Informativitás

F3: Használhatóság (usability)

F4: Közösségi kapcsolódás

Faktorok

F1: Minél nagyobb e faktorérték, annál inkább felhasználóbarát az önkormányzat honlapja (minél kisebb, annál kevésbé felhasználóbarát) (pl: menüpontok áttekinthetősége, kezdőlap áttekinthetősége, tájékoztatás közérthetősége).

F2: Az egyes önkormányzatokra kiszámított faktorértékek között a magasabb érték a honlap nagyobb mértékű informativitását fejezi ki (pl. feladatokról, önkori munkájáról, eredményekről való tájékoztatás, önkormányzat által nyújtott szolgáltatásokkal kapcsolatos információk, nkormányzati stratégiák közzététele).

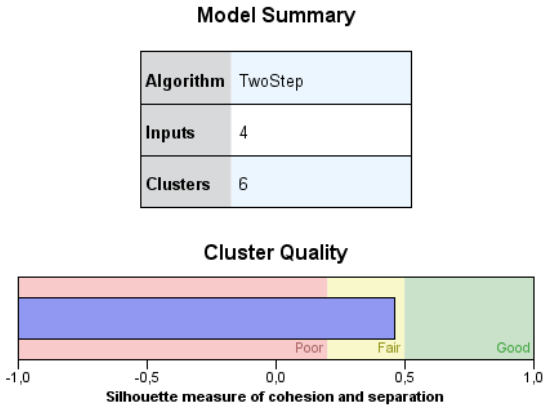
F3: Minél magasabb e faktor változó értéke, annál használhatóbb az önkormányzati honlap (pl. programok közzététele, frissítés, információs adatbázis elérhetősége az intézményekről, lakosság számára fontos adatbázis közzététele).

F4: Az önkormányzatokra kiszámított faktorértékek között a magasabb érték a magasabb szintű közösségi kapcsolódást jelez.

Klaszteranalízis

A következőkben elvégeztem a települések osztályozását az online megjelenést jellemző négy faktorváltozó szerint.

Az osztályozás klaszteranalízissel történt, aminek során a kétlépéses klaszterezés módszerét alkalmaztam Log-likelihood távolságmértékkel. A vágás Schwarz-féle Bayesi kritérium alapján történt. Hat klaszter született, így az osztályozás megfelelőnek minősíthető (50. ábra).

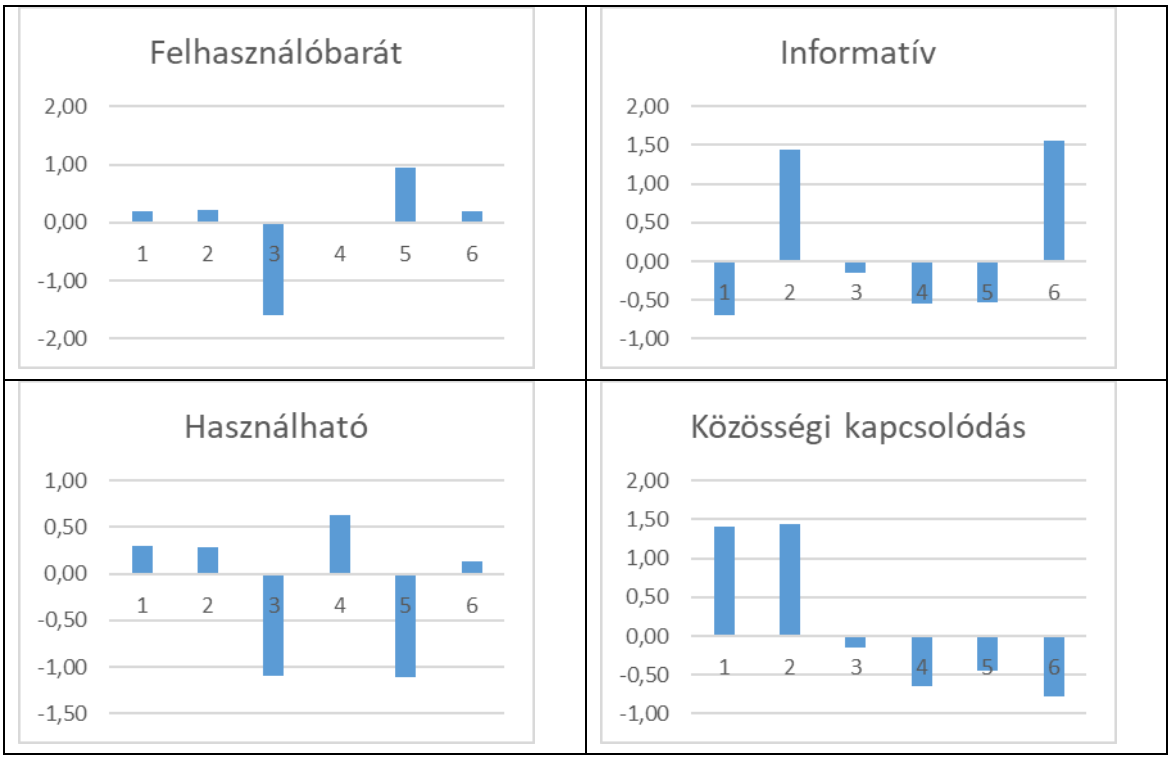


48. ábra

A klaszterezés minősítése

Forrás: saját szerkesztés.

Az 49. ábrán a négy osztályozó változó átlagait szemléltetem az egyes klaszterekben:

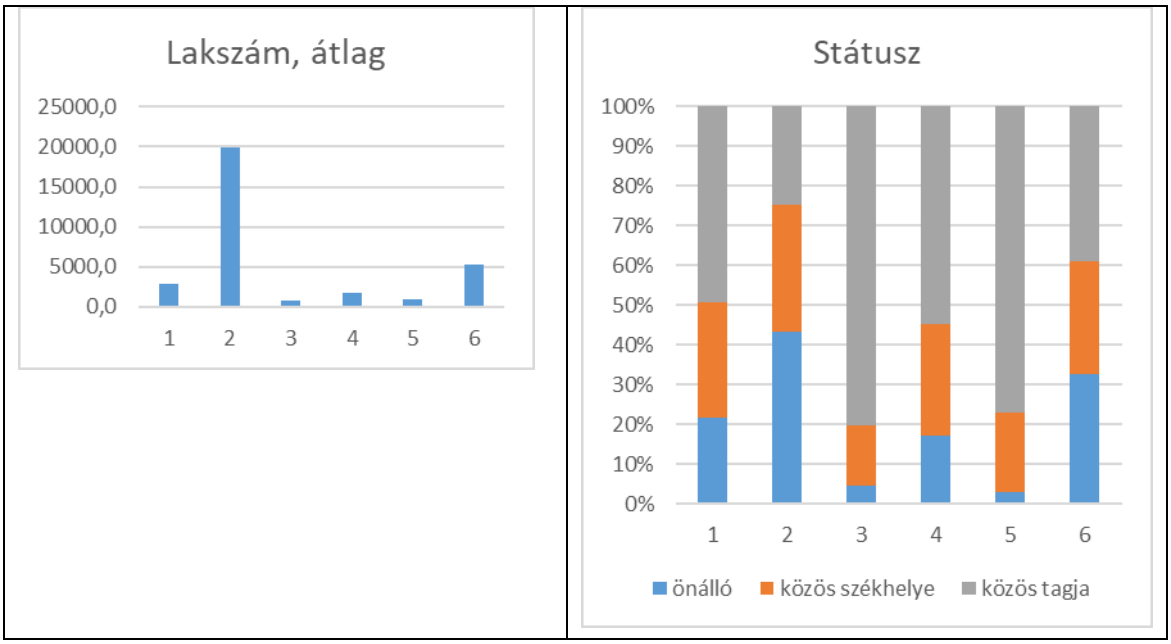


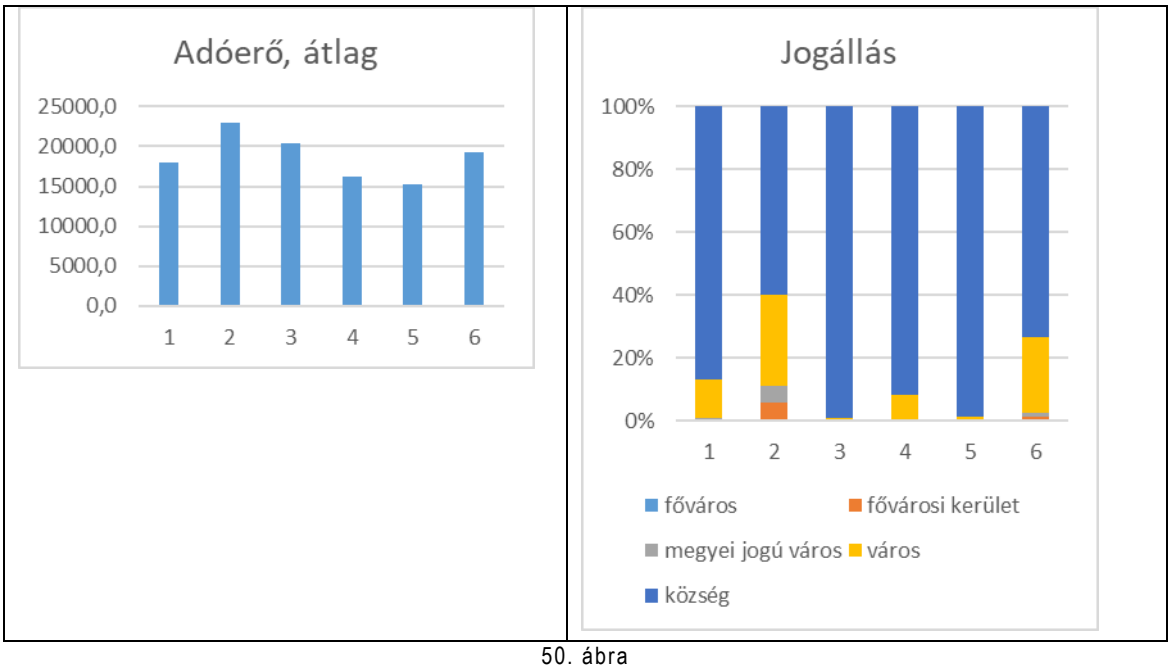
49. ábra

Az osztályozó változó átlagának alakulása az egyes klaszterekben

Forrás: saját szerkesztés.

A további ábrákon az egyes klaszterekbe tartozó települések jellemzése látható, további változók szerint.





50. ábra

Egyes klaszterek további jellemzése

Forrás: saját szerkesztés.

Az 49. és 50. ábrán a négy osztályozóváltozó és a további változók az alábbi jellemzést adják az egyes csoportokra a szervezetek online képessége (webability) szempontjából:

A klaszterek tagjait az osztályozó változók szerint – átlagosan – az alábbiak jellemzik:

- 1. klaszter

A csoportba tartozó települések online megjelenése felhasználóbarát – ha minimális mértékben is (átlaga 0,18) –, azonban a honlapjuk nem informatív, átlaga negatív tartományban van (-0,7). Használhatóság szempontjából pozitív a jellemzése (0,31), továbbá a közösségi kapcsolódás szempontjából kiemelkedően jó eredmény tapasztalható (1,41).

Ebbe a településcsoportba tartozó települések átlagos lakosságszáma közel 3000 fő, és átlagos adóerő-képesség szempontjából inkább az alsó harmadba tartoznak. A csoportba tartozó települések fele közös hivatal tagja, 30%-a közös hivatal székhelye és 20%-a önálló hivatalt tart fenn.

A fentiek alapján az ebbe a csoportba tartozó településeket alacsony adóerő-képesség mellett, a közösségi helyeken keresztüli kommunikáció jellemzi. Vélelmezhetően a weboldaluk fejlesztésére nem fordítanak nagy hangsúlyt, inkább a közösségi médián keresztül szólítják meg lakosaikat. Ennek lehet oka, hogy költséghatékonyabbnak tartják.

- 2. klaszter

A csoportba tartozó települések online megjelenése felhasználóbarát – szintén alacsony értékkel (átlaga 0,21) –, azonban a honlapjuk informativitása a második legmagasabb a klaszterek között (1,45). Használhatóság szempontjából pozitív, de a legalacsonyabb átlagos érték jellemzi (0,29), viszont a közösségi kapcsolódás szempontjából a legjobb eredményt mutathatja fel (1,44).

E településcsoportba tartozó települések átlagos lakosságszáma és adóerő-képessége a legmagasabb (közel 20 000 fő és átlagosan 23 000 Ft az adóerő-képesség). Ebbe a csoportba tartoznak a nagyvárárosok és a fővárosi kerületek. E települések negyede közös hivatal tagja, 30%-a közös hivatal székhelye, és 45%-a önálló hivatalt tart fenn.

A fentiek alapján az ebbe a csoportba tartozó településeket a magas adóerő-képesség mellett, a weboldal és a közösségi helyek hatékony kihasználása jellemzi. E hatékony felhasználás célja a nagylétszámú lakosság minél jobb, széleskörűbb tájékoztatása.

- 3. klaszter

A harmadik klaszterbe tartozó településeket negatív online képesség jellemzi. A csoportba tartozó települések online megjelenése kiugróan negatív a felhasználóbarát működés szempontjából (-1,6), és a honlapjuk sem informatív, átlaga – ha kis mértékben is – negatív tartományban van (-0,14). Átlagosan nem is minősülnek használhatónak a csoportba tartozó települések honlapjai; az átlaga a legnegatívabb e szempontból, és a közösségi kapcsolódásokat sem használják (-0,16).

E településcsoportba tartozó települések átlagos lakosságszáma 1000 fő alatti, bár adóerő-képesség szerint inkább a felső harmadba tartoznak. A csoportba tartozó települések 80%-a közös hivatal tagja, 15%-a közös hivatal székhelye, és 5%-a önálló hivatalt tart fenn.

A fentiek alapján az ebbe a csoportba tartozó települések a magas adóerő-képesség mellett sem fordítanak energiát az online képességük fejlesztésére, és a közösségi webhelyeket sem használják. Ennek oka az alacsony lakosságszám és az alacsony hivatali jelenlét lehet. A számok szerint az anyagi képesség nem elégséges az online képesség növekedéséhez.

- 4. klaszter

A negyedik klaszterbe tartozó településeket, bár kis mértékben, de szintén negatív felhasználóbarát online megjelenés jellemzi (-0,02). A honlapjuk nem informatív, átlaga – ha kis mértékben is – negatív tartományban van (-0,14). Használhatóság szempontjából viszont a legmagasabb érték jellemzi az ebbe a csoportba tartozó települések online megjelenését (0,63), ennek ellenére a közösségi kapcsolódás általagosan újra negatív értéket mutat (-0,65).

Ebbe a településcsoportba tartozó települések átlagos lakosságszáma kissé meghaladja az 1800 főt, és adóerő-képesség szempontjából az alsó harmadba tartoznak. A csoportba tartozó települések 55%-a közös hivatal tagja, 29%-a közös hivatal székhelye, és 16%-a önálló hivatalt tart fenn.

A fentiek alapján az ebbe a csoportba tartozó települések igyekeznek kihasználni a web adta költséghatékony lehetőségeket a lakosság tájékoztatásában, azonban az alacsony adóerő-képesség mellet nem fordítanak energiát az online megoldások felhasználóbarát és informatív jellegének növelésére. A közösségi kapcsolatok használata nem jellemzi ezt a csoportot.

- 5. klaszter

Az ötödik klaszterbe tartozó települések magas (a hat klaszter közül a legmagasabb) értéket mutatnak a felhasználóbarát megjelenés esetében, azonban az összes többi vizsgálati eredmény

negatív értéket vett fel. Nem informatív (-0,52), nem használható (-1,1) és a közösségi kapcsolódás átlaga szintén negatív értéket mutat (-0,45).

Ebbe a településcsoportba tartozó települések átlagos lakosságszáma 1000 fő alatti, adóerő-képesség szempontjából az alsó harmadba tartoznak. E csoportba tartozó települések 78%-a közös hivatal tagja, 19%-a közös hivatal székhelye, és 3%-a önálló hivatalt tart fenn.

A fentiek alapján az ebbe a csoportba tartozó települések igyekeznek kiszolgálni az állampolgárokat egy *user friendly* honlappal, azonban az alacsony adóerő-képesség mellett nem fordítanak energiát az online megoldások felhasználóbarát és informatív jellegének növelésére. A közösségi kapcsolatok használata nem jellemzi ezt a csoportot.

- 6. klaszter

A hatodik klaszterbe tartozó települések esetében a felhasználóbarát megjelenés értéke pozitív (0,2), továbbá az informativitást jellemző változó értéke a legmagasabb (1,56). Használhatóság jellemzi a csoport településeinek online megjelenését (1,14), azonban a közösségi kapcsolódás általgosan a legalacsonyabb értéket vette fel (-0,77).

Ebbe a településcsoportba tartozó települések átlagos lakosságszáma meghaladja az 5000 főt, adóerő-képesség szempontjából a középső alsó harmadba tartoznak. A csoportba tartozó települések között kiegyensúlyozottabban oszlanak meg a hivataltípusok. 40%-a közös hivatal tagja, 28%-a közös hivatal székhelye, és 32%-a önálló hivatalt tart fenn.

A fentiek alapján az ebbe a csoportba tartozó települések átlagosan jó és az informativitás szempontjából kiemelkedő online képességekkel rendelkeznek. A közösségi kapcsolatok használata viszont nem jellemzi ezt a csoportot.

4.3.3. Az önkormányzatok onlineképesség-vizsgálatának eredményei

A faktorváltozók mentén hat klaszter jött létre. Az elemzés alapján az alábbi eredmények kerültek megállapításra:

- 1000 fő feletti, de még alacsony lakosságszámmal rendelkező, inkább alacsony adóerő-képességű, relatíve kiegyensúlyozott hivatali aránnyal rendelkező települések a közösségi kapcsolódásokkal javítani tudják az online képességüket (1. klaszter);
- a nagyobb lakosságszámmal, önkormányzati hivatallal, inkább magas adóerő-képességgel rendelkező települések átlagosan jobb online képességgel rendelkeznek, és ők használják a közösségi kapcsolódásokat is (2. klaszter);
- az alacsony lakosságszámmal rendelkező, magas adóerő-képességű és hivatalhiányos települések esetében a közösségi kapcsolódás nem jellemző, továbbá az adóerő-képesség önmagában nem javítja az online képességet (3. klaszter);
- 1000 fő feletti, de még alacsony lakosságszámmal rendelkező, inkább alacsony adóerő-képességű, arányos hivatali aránnyal rendelkező települések fenn tudnak tartani használható online képességet (4. klaszter);
- 1000 fő alatti lakosságszámú, alacsony adóerő-képességű, hivatalhiányos települések inkább látszat online képességeket alakítanak ki (5. klaszter);

- 5000 fő feletti lakosságszámmal rendelkező, közepes adóerő-képességű, relatíve kiegyensúlyozott hivatali aránnyal rendelkező települések közösségi kapcsolódás nélkül ki tudnak alakítani informatív, elfogadhatóan felhasználóbarát és használható online képességet (6. klaszter).

4.4. Fókuszcsoportos interjú

Fókuszcsoportos interjúkat a kutatási fázis végén, a kapott eredmények értelmezése és a kérdéskörök tisztázása céljából tartottam.

4.4.1. A fókuszcsoportos interjúkészítés technikájának bemutatása

A fókuszcsoport egy kvalitatív kutatási módszer, amellyel emberek egy csoportjának véleményét, benyomásait, attitűdjeit vizsgálhatjuk. E kutatási formát általában a kutatás elején feltárás céljából, vagy a végén az eredmények ellenőrzési eszközeként használják, bár számos alkalommal a kutatás egyéb fázisaiban is előkerül mint olyan eszköz, ami az egyének lekérdezésén alapuló módszereket, a meglévő adatbázisok elemzése során kapott információkat és szempontokat kiegészíti. A fókuszcsoportos beszélgetésekben általában 6–10 fő vesz részt, a beszélgetést moderátor vezeti. A beszélgetés témája rendkívül változatos, használatos marketingkutatásoknál, illetve olyan helyzetekben, ahol nem kizárólag szakmai véleményt akarunk megismerni, hanem a résztvevők attitűdjére is kíváncsiak vagyunk.

A beszélgetés félig strukturált, vagyis a moderátor témavázlat alapján irányítja a beszélgetést, de nincsenek kötött kérdések, válaszok. Megkülönbözteti a fókuszcsoportot a csoportos interjútól az a tény, hogy a csoporttagok egymás közötti interakciója is meghatározó a fókuszcsoport eredményessége szempontjából. Épp ezért fókuszcsoportot célszerű különböző hátterű személyekből összeállítani, akik között valószínűleg a vizsgált témával kapcsolatban véleménykülönbség áll fenn.

Technika előnye a csoporttagok véleménycseréjéből származó többlet, tehát a résztvevők egymással történő interakciója. A résztvevők saját szavaikkal fejezhetik ki véleményüket, így spontán reakciókat figyelhetünk meg. A moderátor szintén felteheti spontánul felmerült kérdéseit, így irányíthatja a beszélgetést.

A fókuszcsoport hátránya, hogy nem számszerűsíthető, nem vonatkoztatható a népesség egészére.

4.4.2. A fókuszcsoport gyakorlatának feltételei, lefolytatása

A fókuszcsoporthoz 6–10 résztvevő jelenléte szükséges. Ennél kevesebb résztvevőnél nem valószínű, hogy kialakul a megfelelő interakció, ennél több résztvevőnél pedig fennáll a frakciózás, a kisebb csoportok kialakulásának veszélye. A kutatás során lezajlott fókuszcsoportos vizsgálat során a létszám biztosította a megfelelő feltételeket. A csoportot moderátor vezette, aki a lenti témavázlat alapján irányította a beszélgetést. Az elhangzottakat hangfelvevőre rögzítettük az esemény minél pontosabb leírása és a reakciók minél szélesebb skálájának elemzési lehetősége érdekében. A felvétel, a leírat elkészülte után tovább már nem használható a társadalomtudományi kutatásokban standardként használt adatvédelmi okokból kifolyólag.

A fókuszcsoportos vizsgálathoz a helyszínt a Települési Önkormányzatok Országos Szövetsége biztosította. A fókuszcsoportos interjú lefolytatására 2018. február 12-én került sor. Érdekképviseleti

oldalról két önkormányzati és egy fő informatikai szakemberként vett részt a fókuszcsoportos interjún. A kutatásban résztvevők közül további hat fő érkezett önkormányzatoktól, és egy résztvevő az ország kiberbiztonsági koordinátora volt. Így összesen tizenegy résztvevő volt a kutatás készítőjével (Számadó Róza) együtt. A csoportok vegyes összetétele biztosította az élénk beszélgetést, és a különböző meglátások, tapasztalatok megosztását és a vélemények ütköztetését.

4.4.3. A fókuszcsoportos vizsgálat során tervezett/feltett kérdések

A fókuszcsoport (tervezett) kérdései leginkább a résztvevők véleményére, tapasztalataira irányultak:

- Mennyire valós veszély egy kibertámadás az önkormányzati rendszerek ellen? Milyen területen okozhat ez nehézséget? Melyek a legsebezhetőbb területek?
- Mennyire felkészültek az önkormányzatok
    - az infrastrukturális elemek, hálózatok védelme kapcsán?
    - az információk, az adatok védelme területén?
    - a kockázatkezelés és a szabályozott működés kialakítása, és az érintett területen meglévő humán kapacitás, kompetenciák és tudatosság kapcsán?
- Milyen a részvevők javaslata?
- Mit gondol, az e-government, a rendszerek közötti átjárhatóság (interoperabilitás) és kiberbiztonsági kérdések hogyan egyeztethetők össze?

4.4.4. A fókuszcsoportos vizsgálat tanulságai

A fókuszcsoportos vizsgálat fontos, más kutatási módszerrel nem megszerezhető szempontokkal, információkkal és gyakorlatokkal szolgált a kutatás témája szempontjából, ezzel tovább mélyítve az ismereteket és megalapozva a javaslatokat. Az országos szintű szakértők és az érdekképviseleti oldalról érkezettek az általános elvárásokat és szempontokat említettek inkább. A helyi viszonyokban napi szinten gyakorlatot szerzők más szempontokból árnyalták ezt a képet. Valós önkritikával, tiszta képük van az önkormányzatok kiberbiztonsági helyzetéről, a tudatosság hiányáról, és értékes javaslatokat fogalmaztak meg a helyzet javítása érdekében.

A vizsgálat az alábbi főbb megállapításokkal szolgált.

- Mennyire látják valós veszélynek egy esetleges kibertámadást:

A megkérdezettek veszélyesnek tartanak egy esetleges kibertámadást, de nem tartják valószínűnek, hogy az önkormányzati rendszerek jelentősen ki lennének ennek téve. A tapasztalat azt mutatja, hogy az elmúlt 2–3 évben az önkormányzatok és kormányzati államigazgatási oldalak egy része (egészségügy, felsőoktatás), főként a gyengébb védelemmel ellátottak jelentős mennyiségben találkoztak a kibertérből érkező fenyegetéssel. Jellemzőek voltak a honlaprongálások, aminek nem annyira az adatszerzés, hanem inkább valamilyen propaganda volt a célja. Azok a korábbi incidensek, amelyek „beleturkáltak kicsit” a honlapba, nagyjából eltűntek. A másik nagy gondot a zsarolóvírusos támadások jelentették, és az ezek elleni védekezés jelenleg is nagy kihívás.

Arra keresünk válaszokat, hogy az önkormányzatok meg tudnak-e egyáltalán felelni, hogyan tudnak megfelelni ezeknek az elvárásoknak, esetleg lehet-e olyan szegmens, ami akár egy-egy javítással

helyzetállapot-javulást hozhatna. Arra a kérdésre, hogy van-e veszély vagy nincs, a válasz: igen, van, és ezt az önkormányzatok egyedül nem tudják kezelni. A résztvevők egyetértettek, hogy csak pénz és elszántság kérdése, hogy ma illetéktelenek hozzáférhessenek önkormányzati rendszerekhez, azonban véleményük szerint a kisebb települések, vagy ahol nagy stratégiai folyamatok nem zajlanak, kiesnek az esetleges támadók érdeklődési köréből.

- A megfelelés témakörében:

Az önkormányzati érintettségű résztvevők egyetértettek abban, hogy egy önkormányzat a számtalan különböző feladati között a kiberbiztonság sokadlagos kérdés. Akkor kap figyelmet, ha probléma merül fel. Természetesen a törvényi előírásoknak igyekeznek megfelelni, de ez nem feltétlenül jelenti, hogy az adott elvárásnak való megfeleléshez szükséges tevékenységek a mindennapokba beágyazódott módon megvalósulnak. A kisebb települések esetében általában a külsős cégek megírják a szabályzatokat, elvégzik a feladatot, azonban a kiberbiztonság érdekében rögzített szabályok nem kerülnek alkalmazásra a napi rutinszerű munkavégzés során. A kistelepülések esetében – a munkatársak számára – szinte meg sem fogalmazhatók azok a tényleges elvárások, amik ahhoz kellenek, hogy külső támadás vagy bármi ellen védekezni tudnánk. A résztvevő polgármesterek egybehangzó véleménye, hogy a települési önkormányzatokat általánosan kapacitáshiány jellemzi, a munkatársak túlterheltek és IT területen nem felkészültek, biztonsági tudatosságról meg csak igen ritkán beszélhetünk. További megállapítás, hogy az IT területen évtizedek óta beszélhetünk kompetenciahiányról, és az összes vonatkozó stratégiai elemzés megállapítja, hogy ez komoly problémát okoz. Szükséges lenne az önkormányzati rendszer szereplőinek motiválása. Rossz példaként említették az ASP-t. Véleményük szerint a megyei jogú városokra kitalált rendszert próbálják alkalmazni a kistelepüléseken, ahol a munkaerő nem tudja azt kezelni. Problémásnak látják, hogy a szabályozás nem szelektál szintenként vagy üzemméretenként. Ugyanakkor az is elhangzott, mintegy ellenpontként, hogy az ASP rendszerébe történő integrálása valamit javíthat a helyzeten, hiszen központi menedzsment működik. A résztvevők abban is egyetértettek, hogy az emberekből hiányzik a tudatosság, mindegy, hogy kis vagy nagy önkormányzatról beszélünk. A szabályzatokat a munkatársak aláírják, hogy elolvasták. Azonban – főleg, ha olyan szabályzat, ami megfelel az Ibtv.-nek – annak a nyelvezete olyan, hogy azt kevesen értik a hivatalban. Az egyik résztvevő saját véleménye szerint az ő hivatalukban is ilyen található. Feltételezése szerint jó, ha öt ember elolvasta a hivatalban, de kétszázan aláírták.

Önkormányzati informatikai vélemény, hogy annak idején az Ibtv. megjelenésekor az informatikusok örültek, hogy lesz szabályozás és könnyebb lesz a munka. Azóta viszont – véleménye szerint részben – nem kerültek kidolgozásra egyszerű végrehajtási szabályok, az egész ügy túlbonyolódott, jórészt papírgyártás lett, és a gyakorlati kérdésekre nem ad választ. Tapasztalata szerint sokszor előfordul, hogy a sok bába közt elvész a gyerek. Kijön egy jogszabály, törvény vagy rendelet az információ biztonsággal kapcsolatban, és van benne egy e betű, mint elektronikus, vagy i, mint informatika. A munkatársak IT területen tapasztalható ismerethiánya és így bizonytalansága miatt az irodai dolgozók ezt tovább adják az informatikusnak. Az informatikus a második jogszabályi hivatkozásnál, amire a jogszabály hivatkozik, közli, hogy ő nem jogász, ehhez nem ért. A végén akár

az egyszerű elvárások sem tudnak beépülni a mindennapokba a munkatársak által nehezen értelmezhető jogi vagy egyéb szaknyelvezet miatt.

Összességében a kérdezettek úgy látják, hogy bár igyekeznek megfelelni az Ibtv. elvárásinak ez még a megfelelő erőforrásokkal rendelkezőknek is inkább csak adminisztratív oldalról sikerül. Az erőforrásokkal kevésbé ellátott önkormányzatok a jelen körülmények között, ha nem kapnak segítséget – bár az információbiztonság fontosságát nem vitatják – szinte lehetetlen küldetésnek látják.

- Szakértelem, erőforrások rendelkezésre állása:

A résztvevők általános problémaként fogalmazták meg, hogy az önkormányzatok nem vagy nehezen találnak az informatikai feladatokra megfelelően képzett szakembert. Országosan szakemberhiány van ezen a területen, és az önkormányzatok nem tudnak versenyezni a forprofit szféra ajánlataival. Még nagyvárosi hivatalok is ezzel a nehézséggel néznek szembe.

A vidéki területeken még nehezebb hozzájutni a megfelelő szakértelemmel rendelkező szakemberhez. Járási, mikrotérségi szinteken, kistelepüléseken nincs informatikus, nincs információbiztonsági szakember, rendszergazda ezért az információbiztonsági feladatokat kiadják külső vállalkozásoknak. Különböző vállalkozások készítik a szabályzatokat, készítik az eljárásrendet. Az önkormányzat – jelentős részének – dolgozói inkább csak adminisztratív szinten felelnek meg az elvárásoknak, a felmerülő kérdéseket, problémákat ad hoc módon tudják kezelni, orvosolni.

A kistelepüléseken más szakterületre, például pénzügyi, igazgatási ügyintéző is nehéz szerezni és megtartani. Informatikai területen olcsóbb is a kiszervezés, hiszen az önkormányzatoknak nincs is keretük egy főállású informatikusra. Elmondásuk alapján a rendszergazdák, információbiztonsági szakemberek, a nagyvárosok hivatalait kivéve, általában részmunkaidőben vagy vállalkozási szerződés keretében látják el a feladatukat.

Ezen túl felmerül a szakemberek felkészültségbeli különbözősége is. Az egyes hivatalokban lokális, mini hálózatok működnek, és sok hivatal nyitna afelé, hogy valamilyen módon legyen kapcsolat a másik szerv hálózatával, viszont aggályosnak tartották a rendszergazdák különböző szintű felkészültségét. A bizonytalanságot növeli, hogy sok esetben nemcsak a folyamatban részt vevő dolgozók és vezetők, hanem a szakemberek sem biztos, hogy tényleg tudják kezelni az esetleges incidenseket, vírustámadásokat annak érdekében, hogy egységes védelmet, felügyeletet tudjanak biztosítani

Az önkormányzatok felkészültsége kapcsán biztos, hogy foglalkozni kell a méretgazdaságosság kérdésével is, ahol kettő-három fős személyzettel működő hivatalokról, meg négy-öt fővel működő több településes közös hivatalokról van szó. Az, hogy lokális, mini hálózatok működnek elkerülhetetlen, de a keletkezett információ és anyag strukturált tárolásának nincs jól bevált gyakorlata. A munkatársak csak a legszükségesebb mértékben rendelkeznek IT kompetenciákkal, online ismeretekkel.

Fontosnak tartották az idő kérdését is mint erőforrást. A központi rendszerek segítséget jelenthetnek az információbiztonság szempontjából is, azonban szükséges, hogy fel tudjanak készülni ezek

használatára. A hivatalok, az önkormányzatok elfogadják azokat a módszertani iránymutatásokat, amit kapnak, nem vitatják, azonban úgy vélik, hogy nincs elegendő idő a felkészülésre. A munkatársaknak nincs elég idejük, hogy fel tudjanak készülni, meg tudják tanulni, be tudják gyakorolni az új rendszerek kezelését, és úgy érzik, nem kapnak kellő mértékű és megfelelő segítséget. Az információbiztonság területén is kell idő az informatikai védelem szempontjából az informatikusoknak, hogy a változásokkal lépést tartsanak, a kollégáknak pedig, hogy ebbe be tudjanak kapcsolódni. Vagyis figyelemmel kell lenni az önkormányzatok méretbeli különbségeire is.

Az idő kérdését több szempontból is fontosnak találták a kérdezettek. Az egyik az informatikai gyors fejlődéséhez kapcsolódik, tehát a közszféra és az önkormányzatok jelentős lemaradással reagálnak, és próbálnak megoldásokat találni. A másik a rendelkezésre álló munkaidő arra, hogy az adott feladatot el tudják intézni mint munkavállalók, mint önkormányzatok.

Pozitív megállapításként fogalmazták meg az egységesítés kérdését a fent már jelzett korlátokkal. Az e-közigazgatás keretében az egységesítés, az ASP, a központi rendszerek sokat segíthetnek, jelentős előnyt jelenthetnek az önkormányzatoknak technikai szempontból. Továbbá hosszú távon létrejön a rendszerekhez való hozzáértés a humán erőforrás oldalán is.

Emellett az önkormányzati tapasztalat azt mutatja, hogy változnak az állampolgári elvárások és az internethasználati szokások. Az ügyfelek jelentős része már a közösségi alkalmazásokat preferálja. Jelentős kihívást jelent, hogy informatikai és információbiztonsági kérdésekben az önkormányzatok és az egyes közszolgák hogyan fogják utolérni magukat eszközhasználatban, tudásban, minőségben.

A változó környezetben az önkormányzati dolgozók folyamatosan kihívásokkal szembesülnek. A már említett ASP, de más központi rendszerek kezeléséhez által elvárt ismeretanyagot el kell sajátítaniuk és az elvárások csak nőnek. Úgy látják, hiányzik az az életpályamodell a köztisztviselők számára, ami segít áttekinteni, hogy milyen képzéssel mit érhet el, így az adott körülmények között nagyon nehéz motiválni őket. Különösen, hogy a kistelepülési hivatalokban dolgozók reggeltől estig az egyik feladatból esnek a másikba. Motiváció nélkül nehezen vehető rá plusz terhelésre a kolléga. Fontos megállapításként fogalmazódott meg, hogy a helyi politikai, szociális érdekek – érthető módon – felülírják az egyéb elvárásokat. Ha helyben felmerülő nehézségre kell választ adnia a képviselőtestületnek vagy a választások előtti népszerűségjavító intézkedésekre kell anyagi erőforrás, akkor azt kezeli prioritásként, és nem a munkatársak információbiztonsági képzését.

- Tudatosság

„Én egy kicsit úgy érzem magam a lehetőségekben, mintha száz évvel ezelőtt mindenkinek adunk egy autót, csak hogy senkit nem tanítottunk meg vezetni."[18]

A felhasználói kultúrából hiányzik a tudatosság, és nem jellemző a rendszerekre a strukturáltság. Egyetértés volt abban is, hogy nem méretfüggő, hogy a tudatosság hiányzik a munkatársakból és ezt szabályzatokkal nem lehet megoldani. Gyakorlatorientált támogatásra, képzésre és segédletekre van szükség.

[18] Forrás: egyik résztvevő.

Olyan megoldások kellenek, amelyek nem nehezítik a munkavégzést, nem növelik a munkavégzés idejét és nem támasztanak túl nagy elvárásokat a munkatársakkal szemben, mert ellenkező esetben ellenállást váltanak ki. A hivatali dolgozók részéről minden esetben várható ellenállás, mert először plusz teherként élik meg a változást, mivel nem segíti a munkájukat. Ezt mindenképpen kezelni szükséges, mert az emberi tényezőn el tud bukni a jól működő informatikai rendszer vagy a jó biztonsági eljárás. A felhasználó önmagában kockázat, hiszen lehet hanyagság, figyelmetlenség, nem is szükséges a szándékosság egy kiberbiztonsági incidenshez.

Az információbiztonsági kérdések érintettség, baj esetén kerülnek előtérbe. Azon hivatalok esetében, akik már elszenvedtek valamilyen kibertámadást, sokkal könnyebb az információbiztonság érdekében intézkedéseket bevezetni, a munkatársak sokkal motiváltabbak az elvárt intézkedések betartásában.

Az Ibtv. előírásait többen túlzó adminisztrációnak érzik, ami kevéssé növeli az önkormányzatok és munkatársaik motivációját, és kevés gyakorlati támogatást ad.

- Interjúalanyok javaslatai

A résztvevők komplex javaslatokat fogalmaztak meg az önkormányzati kiberbiztonság javítására, a probléma kezelésére. Általános egyetértés volt a fejlesztés, képzés szükségességének kérdésében, de – az időnyomás miatt – a szankciók bevezetését is fontosnak tartották a változások végrehajtásának érdekében.

A megfogalmazott javaslatok több dimenzióban merültek fel. Az egyik ilyen az állam és az önkormányzat közötti feladatelosztás, együttműködés és koordináció a kiberbiztonság érdekében. A másik az idősík. Milyen beavatkozások azok, amiktől rögtön várható eredmény, és mi az, amit pedig el kell kezdeni és – mintegy horizontális, állandó tevékenységet – folyamatos felülvizsgálat mellett majd hosszú távon fejti ki a hatásait.

A kérdezettek úgy látták, hogy két dologra kell fókuszálni, az illetéktelen hozzáférés megakadályozása, a másik pedig a helyreállíthatóság.

Arra a megállapításra jutottak, hogy az illetéktelen hozzáférést, egy nagy rendszerszintű – nem szabályzatokban kitalált –, hanem standardizált, sablonokat kínáló, megoldásokat nyújtó formában lehetne elképzelni, amit a központi kormányzat biztosít. Az önkormányzatok feladata a helyi közügyek intézése, a helyi közszolgáltatások biztosítása. A kiberbiztonság azonban nemzeti szint, így ezekre az esetekre önkormányzatok számára az államnak kell megoldást kínálnia. Szükség van az interoperabilitás minden szintjére, mivel a gyakorlatban a több ezer megvalósítási pont csak így fog igazán jól működni. Minimum ajánlásokat kell adni, és az Mötv. előírásainak megfelelően hozzárendelni a megvalósításhoz szükséges forrást. Ezen túl kiemelten fontos kialakítani – és folyamatos minőségbiztosítási és fejlesztési rendszerrel támogatva fenntartani – a felkészítési, a képzési és tudatosítási rendszert az önkormányzatok számára. Ehhez jó lenne, ha kialakításra kerülne valamilyen koordinációs, együttműködési rendszer: egy közös platform. Ez teret adhatna a szakemberek, vezetők eszmecseréjére, a szakemberek tapasztalatcseréjére, az információ és tudás cseréjére. A TÖOSZ képviselői részéről felmerült a tudatosság és a jó megoldások, jó gyakorlatok terjedésének gyorsítása érdekében egy kiberbiztonsági díj létrehozásának ötlete is, ami sikeresen

hozzájárulhatna a vezetői tudatosság javításához. A másik a működés biztonsága, a helyreállíthatóság, amit az önkormányzatoknak önmaguknak kell biztosítani a saját működési kereteik között. Ehhez viszont szükséges a munkatársak motivációja, tudatossága, valamint a vezetés elkötelezettsége és természetesen a tudatossága, a fenyegetettség felismerésének képessége.

A tudatosság kérdésköre kapcsán felmerült párhuzamként a környezettudatossággal való hasonlatosság. A környezettudatosság kialakulása sem volt gyors. Példaként került említésre, hogy Németországban is először ingyen szeméttárolókat adtak, s megkérték a lakosságot, hogy szelektíven gyűjtse a hulladékot, aztán büntették őket, majd megemelték a szemétdíjat, ha nem megfelelően gyűjtötték a hulladékot. Tehát valószínű, hogy a kibertudatosság esetében is ennek a fejlesztésnek és a szankcióknak is szerepet kell adni, de az emberek felkészítése nem maradhat el. Fel kell építeni az egész motivációs hátterét, hogy a hivatalnokok számára legyen értelme az elvárt tevékenységeknek, ami segítheti a tudatosságot.

Nagy segítséget jelentenének gyakorlati útmutatók, feldolgozott esettanulmányok, az önkormányzati jó gyakorlatok bemutatása. Ilyen lehetne egy gyakorlati felhasználói kézikönyv, egy-egy gyakorlati ajánlás és akár egyszerű napi csekklista, ami segíti a munkatársakat az információbiztonsággal kapcsolatos tevékenységük során, és persze a mindehhez szükséges idő biztosítása.

Elhangzott több megvalósult jó gyakorlat arról, hogy milyen módon biztosítható az önkormányzati rendszerek védettsége. Az egyik önkormányzati informatikus véleménye szerint rendszerszinten, komplexen kezelve kiváló eredményeket lehet elérni az önkormányzati rendszerek biztonsága érdekében, miközben ez nem igényel kiemelkedő tudásszintet, tudatosságot azonban igen. Javaslata szerint kettős védelmet kell megvalósítani. A belépők esetében vannak kitiltott IP-cím[19] tartományok, amikkel nem lehet belépni a weboldalra, ahonnan a tapasztalatok szerint már érkezett valamilyen támadás. A másik például – ami nem túl nagy befektetés –, ha bizonyos kapcsolatszám megemelkedik hat másodpercen belül, akkor a szerver automatikusan kikapcsolja azt a belépő felhasználót. Ez azon alapul, hogy egy ember másodpercenként 50 lekérést adjon az oldalnak. Ilyet biztos nem tud csinálni, tehát ezt már biztos nem gép csinálja. A kliens gépeken olyan reklámszűrők, víruskereső programok vannak telepítve, amik nem terhelik túl a gépeket, így a munkatársnak nem kell napi fél, egy percnél többet várakozni a belépésnél. Nagy ellenállást váltott ki a különböző közösségi alkalmazások és egyes levelezőrendszerek kitiltása, azonban, mivel a Facebookon keresztül érkezett a zsarolóvírus, a vezetői elköteleződés megvolt, így végrehajtották. Ebben a hivatalban központi informatikai menedzsment dolgozik. A belső hálózaton követhető minden kliensmozgás. Erre már rendelkezésre állnak megfelelő eszközök elérhető áron, ami naplózza az összes tevékenységet, így az információbiztonsági előírások be nem tartását is. Jellemző és szúrópróbaszerű lehetne a napi szintű mentés és biztonsági frissítés is. Nagyon fontos a rendszeres szakmai továbbképzés. A különböző eszközök és szakmai továbbképzések kapcsán is elhangzott, hogy az önkormányzati prioritás az egyéb helyi közügyeken van, és ha a polgármester vagy a jegyző

[19] Internetprotocol-cím: egy egyedi hálózati azonosító, amit az internetprotokoll segítségével kommunikáló számítógépek egymás azonosítására használnak. Minden, az internetre kapcsolt számítógépnek van IP-címe.

nem elkötelezett az információbiztonsági kérdések mellett, akkor a fejlesztésekre, védekezésre költhető költségvetési forrásokat a testület sokszor megnyirbálja.

Az önkormányzatok önerőből nem tudnak megfelelni a kiberbiztonsági kihívásoknak. Ez a terület nem is helyi, hanem – minimum – országos szintű kérdés, ami központi kezelést igényel. Ahhoz, hogy országosan – és az EU partnerségnek is megfelelve – egyenszilárdságú kiberbiztonságról beszélhessünk szükséges az állami szerepvállalás erősítése, az együttműködés, a koordináció javítása, amit az államtól várnak az önkormányzatok.

Szükség van információmegosztó platformok létrehozására, tudatosító képzésekre és egyszerű, autodidakta módon feldolgozható és könnyen, bárki számára elérhető e-learning módszerű képzésekre.

4.5. Az empirikus kutatás legfontosabb következtetései

4.5.1. Megállapítások

A nemzetközi tapasztalatok figyelembevételével és a hazai adatokat megvizsgálva, továbbá az empirikus kutatási eredményekre támaszkodva azt láthatjuk, hogy kiberbiztonsági szempontból a hazai önkormányzatok a jelenlegi körülmények között a hazai közszféra legnagyobb – a teljes lakosságra kiterjedő – és legkiszolgáltatottabb szektora. Maga a kérdéskör országos szintű, és az önkormányzatok nemzeti érdekből sem hagyhatók magukra, illetve nem is képesek önerőből megoldani a felmerülő nehézségeket, így szükséges a központi beavatkozás. Ahhoz, hogy országos szinten – és az EU partnerségnek is megfelelve – egyenszilárdságú kiberbiztonságról beszélhessünk, növelni kell az állami szerepvállalás mértékét, javítani az együttműködést és a koordinációt.

Az ENISA jelentésében [15] felsorolt tizenöt kiberfenyegetési módszer esetében arra hívják fel a figyelmet, hogy többségük az emberi tényezőhöz, a humánerőforrás képességeihez kapcsolódik. Az egyik ilyen aspektus a munkatársak tájékozatlansága: nem tudatosak az esetleges fenyegetettség kapcsán; nem kaptak megfelelő képzést, támogatást, iránymutatást, vagy hanyag módon nem tartják be a szabályokat, és ezzel okoznak információbiztonsági eseményeket. A másik aspektus, hogy a jelentésben felsoroltak közül, sok esetében javítani lehet a védekezési képességet az emberi erőforrás fejlesztésével, a tudatosság növelésével. A belső fenyegetés okozói minden esetben a munkatársak (vagy a szerződött partnerek) haszonszerzésből vagy hanyagságból, tudatlanságból.

A technológia gyors fejlődése még tovább növeli a veszélynek való kitettséget. Tulajdonképpen lehetetlenné vált a teljes biztonság megteremtése, ezért a megelőzésre és az ellenálló képesség növelésére kell koncentrálni. Ennek egyik kritikus eleme az ember.

A hazai önkormányzatok információbiztonsági gyakorlatának – az IT képességén belül –, online képességének vizsgálata és az önkormányzati és információbiztonsági szakemberek részvételével megtartott fókuszcsoportos interjú eredményei alapján az alábbi megállapítások tehetők:

- Az önkormányzatok jelentős része nem tesz eleget az Ibtv.-ben előírt jogszabályi kötelezettségeinek. Például a 3178 önkormányzatból – 2017 közepéig – 577 nyújtotta be az informatikai rendszerének osztályba sorolását, ami 20%. Ha nem vizsgálom a teljes önkormányzati kört, csak az önálló hivatalokat (545) és a közös hivatal székhely

önkormányzatait (738) – tekintettel a tagönkormányzatok erőforráshiányaira –, látható, hogy több, mint 4 évvel a törvény hatályba lépését követően is csak 40% teljesítette a törvény előírásait.

- A kiberbiztonsági szabályozás nemzetközi szinten is kiemelkedő módon került kialakításra, azonban a hangsúlyt a hatósági oldal jelenti. Az önkormányzati kör megállapítása szerint további adminisztratív terhet ró az önkormányzatokra, és nem ad megfelelő, a szektor sajátosságait figyelembe vevő támogatást. A nemzeti stratégiai célok elérése érdekében szükséges az állam részéről biztosítani a NIS irányelv [49] szerint előírt standardokat, a kibervédelmi eszközök elérhetőségét, az e-kormányzás terén alkalmazandó biztonsági előírások alkamazásának támogatását, a tudatosságnövelő beavatkozásokat.

  A hatósági oldalon túl nem kerültek kialakításra a nemzeti kiberbiztonságban érintett szervezetek, információbiztonsági szakértők és az önkormányzatok bevonásával a széleskörű tudás és információ megosztást támogató együttműködési és koordinációs hálózatok, munkacsoportok, amelyek oda-vissza, vertikálisan és horizontálisan is biztosítani tudnák az információcserét, a tapasztalatok és a tudás megosztását.
- Az önkormányzatok információbiztonsági gyakorlatának zavaraihoz jelentős mértékben hozzájárulnak a központi közigazgatás szereplői. Jellemzőek a hiányos feladatellátásból adódó nehézségek. Például a nem megfelelő felkészítés a rendszerhasználatra az ASP esetében, vagy a költségvetési források elmaradása a többletfeladatok finanszírozására.
- Általános megállapítás, hogy a magyar informatikai oktatás nem támogatja megfelelően a digitális kompetenciák fejlesztését, ezért teljes reformra szorul. Ennek azonban az a következménye, hogy e területen kiemelten lépett fel tudás- és szakemberhiány. Az önkormányzatoknál a közalkalmazotti bérezés sokszorosan alatta marad a versenyszféra béreinek, így az önkormányzatok e tekintetben szakember- és kapacitáshiánnyal küzdenek. Ennek következtében többségében – jellemzően a kisebb településeken – külső megbízással oldják meg az információbiztonsági feladatokat, ami nem biztosítja a folytonosságot és a felügyeletet. Az információbiztonságot nem lehet akcióként kezelni, hanem egy tudatosan felépített, állandóan fejlesztett folyamatként.
- Szintén általános következtetés, de az önkormányzati szektorra is igaz, hogy az önkormányzatok nem a megfelelő helyen és szinten kezelik az információbiztonságot. Informatikai kérdésként kezelik, miközben a megfelelő működés érdekében az információbiztonságnak a szervezeti kultúra részének kellene lennie, vagyis tudatosság szükséges. Ez nem működik a munkatársak motivációja és a vezetők elköteleződése nélkül. A kialakított központi képzések nem illeszkednek megfelelően az önkormányzaton belül az információbiztonság biztosítása érdekében kialakítandó szerepekhez. A vezetők (polgármester, jegyző és képviselők) elkötelezettsége, tudatossága nélkül az önkormányzati hivatalokban nem biztosított a kérdés megfelelő szinten való kezelése. A megvalósuló képzések nem gyakorlatorientáltak, nem dinamikusan megújulók, az oktatási módszerek nem illeszkedők. Az előző fordítottja is igaz, vagyis az IB szakembernek nemcsak a kibertámadásokkal, hanem a szervezeti működéssel is tisztában kell(ene) lennie, munkája komplex megközelítést igényel. Szükséges a tudatosság növelése, a képzésfejlesztés. Ezt

nemcsak az IT szakemberekre, hanem a munkavállalók teljes körére is ki kell terjeszteni a reziliecia növelése érdekében.

- A fentiekből következik, továbbá az önkormányzatok online képességének (webability) a vizsgálata is igazolta, hogy az önkormányzatok online képessége alacsony. Az önkormányzati webability a növekvő lakosságszámmal és/vagy hivatali ellátottsággal javul.
- Az online felmérés és a fókuszcsoportos interjú alapján az önkormányzatok vagy nem tartják fenyegetettnek, sebezhetőnek az önkormányzatok adatait és rendszereit, vagy nem gondolják, hogy célkeresztben lennének. A kiberbiztonsági kérdések kapcsán a tudatosság nagyon alacsony szintet mutat, ami a kiberbiztonsági trendeket, irányokat és technológiai fejlődést figyelembe véve (például: olyan támadások várhatók, amelyek célzottak, emberi beavatkozást már nem igényelnek) hatalmas kockázatot hordoz.
- A települési önkormányzatok közül csak a legnagyobbak rendelkeznek valamelyest védekezési képességgel és információbiztonsági kompetenciákkal. A kisebb települések jellemzően nincsenek felkészülve, és szélmalomharcnak gondolják, míg a nagyok túlzottan bíznak a saját képességeikben. Az 1001–50 000 fő lakosságszámú települések értelmezik leginkább helyén a kiberfenyegetettséget.

4.5.2. Következtetések, javaslatok

A) A kiberkoordináció kibővítése – önkormányzatok bevonása

A részletes javaslatot az 1. függelék tartalmazza.

- Szabályozási környezet, a 2013. évi L. törvény és a 484/2013. (XII. 17.) Korm. rendelet módosítása:
    - Nemzeti kibervédelmi tanács kibővítése.
    - Önkormányzati kiberbiztonsági munkacsoport létrehozása.
- A központi kormányzati szervezetek és az önkormányzatok közötti operatív koordinációs működés megvalósítása – operatív munkaszervezet létrehozása.

B) Önkormányzati információbiztonsági képzési rendszer átalakítása, bővítése.

A nemzetközi kutatások és elemzések alapján a vezető kockázati tényező továbbra is a humán erőforrás, míg a technológiai és a folyamatokból adódó kockázatok jóval kevésbé mérvadóak. A rendszer leggyengébb láncszeme az ember [10]. Ez tükröződik a Bizottság és a NIS irányelv javaslataiban is. A képzés, oktatás, tudatosítás kiemelt prioritás.

Mindezeken túl kiemelt figyelmet kell szentelni a vezetők felkészítésének, tudatosításának és motiválásának. Egy adott terület sikerességét minden szervezettípusban jelentősen befolyásolja a vezetői elköteleződés és a közigazgatásban ez a befolyás még meghatározóbb. Attól függően, hogy a polgármester vagy a jegyző mit gondol – vagy mit nem – a tennivalók tekintetében, meghatározza a teljes hivatal viszonyulását, motivációját az információbiztonság kérdésköréhez. A vezetők felkészítésének kiemelt szerepe van az kiberbiztonság elérésére tett kísérletek során.

Az online felmérés eredményei alapján az önkormányzatok védekező és reagáló képessége nagyon alacsony, a kiberfenyegetettség pedig egyre komolyabb veszélyt jelent, ami csak oktatással, képzéssel, rendszeres gyakorlati tanulással ellensúlyozható.

A hazai képzési palettát áttekintve sturkturált képzést és továbbképzést az NKE biztosít, azonban a gyakorlatiasság, a tudatosítás egyéb módszerei, az önkormányzati hivatalok felkészítése hiányos és hiányoznak az egyszerű, könnyen érthető és autodidakta módon feldolgozható képzési anyagok.

A fentiek és a fókuszcsoportos kutatásban megfogalmazódott önkormányzati elvárásoknak való megfelelés érdekében a rendszer átalakítására 2. függelékben teszek javaslatot.

A javaslat megvalósításához szükséges az érintett jogszabályok módosítása.

C) Önkormányzati információbiztonsági ellenőrző lista.

A listát a 3. függelék tartalmazza.

D) Önkormányzatok online képessége szerinti csoportosítása

A vizsgálat alapján elvégzett csoportosítást a 4. függelék tartalmazza.

ÖSSZEGZETT KÖVETKEZTETÉSEK

A kitűzött kutatási ambíciók teljesítése érdekében széleskörű kutatást végeztem. Az eredmények elemzését követően fogalmaztam meg téziseimet és ajánlásaimat.

A kutatómunka összegzése

A biztonságra törekvés az áthatja az életünket. A biztonságunk érdekében tett erőfeszítéseink színtere az elmúlt évtizedben jelentősen kibővült. Az IKT eszközök, az internet ma már a fejlett világ és az élet minden területét átszövik. Ez a változás robbanásszerűen történt, szinte észrevétlenül. A biztonságtudomány és ezen belül az információbiztonság mint tudományterület dinamikus fejlődésen megy keresztül. A közszféra szervezetei – és ezen belül az önkormányzatok még inkább – lassan reagálnak a technológiai és az állampolgári elvárásokra; a szervezeti működés és szervezeti kultúra pedig természetéből fakadóan reagál lassan. A központi és helyi kormányzatok információbiztonsági eseményeknek, incidenseknek való kitettsége jelentősen megnőtt az elmúlt évtizedekben.

Értekezésemben célul tűztem ki a téma tudományos igényű, komplex vizsgálatát, a gyakorlati alkalmazhatósági szempontok figyelembevételével. A kutatás fókuszában a szervezeti tudatosság működés, az emberi tényező, a humán erőforrás vizsgálata állt. Nem volt célja a technikai kérdések kérdések, a kiberfenyegetések típusainak, trendjeinek és kezelésének részletes kifejtése.

Az első fejezetben a biztonságtudomány fogalomkörének és vizsgálati területének bemutatását követően részletesen foglalkoztam az információbiztonság és kiberbiztonság fogalmi kereteivel és a jelenlegi helyzetével, továbbá a kormányzati szektor információs rendszereivel kapcsolatos kérdésekkel. Bemutattam az önkormányzati információbiztonsággal kapcsolatos elemzések eredményeit.

A második fejezetben áttekintettem az európai uniós és hazai szabályozási és szervezeti kereteket. A hazai kormányzati kiberkoordináció rendszerét és az önkormányzatok helyét a kiberkoordinációban. Az új NIS és GDPR irányelveket és azok elvárásainak megjelenését a szabályozás változásában.

A harmadik fejezet járja körbe az önkormányzatok kormányzati rendszerben betöltött helyét, mutatja be az önkormányzatok feladatait és az önkormányzati hivatalok típusait. Az értekezés szempontjából kiemelten fontos részként tárgyalom e helyütt az elektronikus információs rendszerekhez kapcsolódó képzések jelenlegi helyzetét. A fejezet jelentős pontja az önkormányzatok megfelelése (illetve nem megfelelése) az Ibtv. és az Infotv. elvárásainak. A harmadik fejezet foglalkozik a humánerőforrás-fejlesztés kérdésköreivel. Az emberi tényező fejlesztése, a tudatosítás, a képzés kapcsán meglévő és fejlesztendő tárgykörökkel.

A negyedik fejezet a dolgozat hangsúlyos része. Ez a fejezet tartalmazza a szakirodalomra, a nemzetközi és hazai tapasztalatokra alapozott empirikus kutatást. Az információbiztonság témakörében még nem került sor ilyen komplex felmérésre, ami alapján optimalizálni lehetne a beavatkozások irányait és a szükséges erőfeszítéseket. Ezt a hiányt igyekeztem pótolni az önkormányzati szektor esetében több összefüggő terület átfogó vizsgálatával. A kutatás keretében felmértem az önkormányzatok kiberbiztonsággal kapcsolatos véleményét, felkészültségét,

információbiztonsági képességeit és működési gyakorlatát. Erre online kérdőíves formában került sor, aminek eredményeit leíró és matematikai-statisztikai módszerekkel vizsgáltam. A fejezet gerincét az online felmérés eredményeinek elemzése és bemutatása teszi ki. A második vizsgálatra a Belügyminisztérium által készített, a teljes önkormányzati körre kiterjedő horizontális weblapértékelésre vonatkozó adatelemzése adott lehetőséget. Az információbiztonság, az e-közigazgatás megkívánja a digitális kompetenciák meglétét egyéni és szervezeti szinten. Az adatok faktor és klaszter analízist követő eredményeinek közlésére és az önkormányzatok tipizálására szintén a negyedik fejezetben került sor. Az empirikus kutatás és a fejezet harmadik része a fókuszcsoportos interjú eredményeit mutatja be. A fejezet végén összefoglalásra kerültek a megállapítások és következtetések.

Az elemzések eredményei alapján végeztem el a hipotézisek vizsgálatát, és alkottam meg téziseimet, az ajánlásokat és a kutatási eredményeimet.

Új tudományos eredmények

1. A szabályozási környezet, a kiberkoordináció, a szervezeti működés és a fókuszcsoportos interjú területein végzett kutatásaim alapján – a hipotézisemben felvetett feltételezéseimet igazolva – be**bizonyítottam, hogy a kormányzat és az önkormányzatok között a kapcsolat csak adminisztratív és hatósági szempontból kimunkált, továbbá nem alkalmazzák a kooperációból, koordinációból és együttműködésből származó előnyöket. Kidolgoztam és javaslatot tettem a kiberoordináció szabályozási és szervezeti működésének módosítására** (1. függelék).
2. **Bebizonyítottam, hogy az önkormányzatok gazdasági helyzete, a lakosságszám és a hivatali struktúrájuk az online képességük jelentősen befolyásoló tényezői.** Hipotéziseimet faktor- és klaszteranalízis elemzésekkel igazoltam, **kimutattam az online képesség** (webability) **feltételeinek szoros, a működést befolyásoló összefüggéseit**. Kutatási eredményeim alapján **kidolgoztam az önkormányzatok online képesség szerinti besorolását** (2. függelék). Kimutattam, hogy egyértelmű összefüggés mutatkozik a jobb online képesség és az önkormányzatok magasabb lakosságszáma, továbbá az önálló vagy székhely-önkormányzati hivatal megléte és az adóerő-képesség nagysága között, azzal a kitétellel, hogy önmagában az adóerő-képesség nem hat pozitívan az online képességre.
3. **A nemzetközi tapasztalatok feldolgozása és saját kutatásaim alapján igazoltam**, **hogy az önkormányzatok vezetői, munkatársai nincsenek tisztában az információbiztonsági kockázatokkal és tudatosságuk nagyon alacsony szintű, a fenyegetettség mértékét alul becsülik.** Az információbiztonság kérdéskörének megfelelő szintű kezelésében az önkormányzatok esetében különösen kritikus szerepe van a vezetőknek. Az IT kockázatokat nem, vagy csak részlegesen ismerik, a biztonságtudatosság az önkormányzati hivatalokban jellemzően alacsony szintű. Az alacsony tudás és tudatossági szint emelésére **továbbfejlesztettem a jelenlegi képzési elemeket is tartalmazó tudatosítási és képzési rendszert**, **amelyek bevezetésére javaslatot dolgoztam ki** az önkormányzatok információbiztonságban érintett vezetői, felelősei és résztvevői számára (3. függelék).

4. Empirikus kutatási módszerekkel **igazoltam, hogy az önkormányzatok nem rendelkeznek** az információs rendszerük használatához szükséges, a biztonságos működést támogató **protokollokkal,** egyszerűbb ellenőrzési listákkal, útmutatókkal a napi információbiztonsági feladatok ellátáshoz. Segítségül **egyszerű ellenőrzési listát dolgoztam ki**, amit használatra javaslok az önkormányzatok számára (4. függelék).
5. A fókuszcsoportos kutatás igazolta, hogy kapacitás, a szakember- és az erőforráshiány miatt az 5000 fő lakosságszám alatti települések többnyire külső vállalkozásokkal oldják meg az IT és IT biztonsági feladataikat, így sem a folytonosság, sem a naprakészség nem valósul meg.

Ajánlások

1. Az önkormányzatok számára az Infotv. teljesíthetősége, az állampolgárok bizalmának megerősítése, a település népességmegtartó képességének növelése és a versenyképesség javítása érdekében javaslom,
- hogy alkalmazásra kerüljenek települési online képesség javítását támogató integrált módszertanok (web és közösségi média alkalmazása települési környezetben);
- hogy erőforráshiányos környezetben mérjék fel az önkormányzatok a lakosaik online fogyasztási szokásait, és az igényeknek megfelelő irányba kezdjék meg a fejlesztéseket;
- hogy nemzetközi és hazai jó gyakorlatokat, esettanulmányokat tegyenek közzé a kiváló webability megvalósításáról;
- hogy online, interaktív képzési anyagokat biztosítsanak a munkatársaik számára.

2. Javaslom az önkormányzatokkal együttműködő központi kormányzati szereplők közös felkészítését a helyhatóságok vezetőivel, mivel a NEIH tapasztalatai szerint számos nehézséget okoz a kormányzati szereplők felkészületlensége.

3. Javaslom, hogy az önkormányzatok
- valósítsanak meg központi menedzsmentet;
- vezessenek be kétszintű azonosítást;
- vezessék be a napi biztonsági mentést;
- dolgozzanak ki és alkalmazzanak védekező és reagáló képességet támogató eljárásrendeket.

4. Javaslom a kiberbiztonsági kormányzati szervezeteknek, hogy az önkormányzatok részére
- készüljön rendszeresen (havonta, háromhavonta) rövid, köznapi nyelven online formában útmutató a kiberfenyegetettségi eseményekről;
- készüljön legalább évente rövid közérthető módszertani útmutató;
- készüljenek nem szakmai nyelvezettel, autodidakta módon feldolgozható e-learning módszerű kibervédekezési, kiberbiztonsági tudatosságot javító képzési anyagok.

IRODALOMJEGYZÉK

[1] BUKOVICS, I.: Létfontosságú infrastruktúrák; KDI előadás, 2016

[2] BEREK, L.: Biztonságtechnika, NKE, Budapest, 2014.

[3] MUNK, T. H.: Cyber-security in the European Region: Anticipatory Governance and Practices; The University of Warwick 2015.
https://www.research.manchester.ac.uk/portal/files/54570851/FULL_TEXT.PDF (letöltve: 2018. 01. 22.)

[4] BUKOVICS, I.: A kritikus infrastruktúrák rendszerkoncepciója - Egy kérdőív módszertani kritikája; In: HORVÁTH, A. /szerk./: Fejezetek a kritikus infrastruktúra védelemből Tanulmánykötet, Budapest, Magyar hadtudományi Társaság, 2013. pp.58–75.

[5] Országos Katasztrófavédelmi Főigazgatóság (OKF): A kritikus infrastruktúra.
http://www.katasztrofavedelem.hu/index2.php?pageid=lrl_index (letöltve: 2018. 03. 07.)

[6] RAJNAI Z. – FREGAN B.: Kritikus infrastruktúrák védelme (jogi szabályozás). In: BITAY E. /szerk./:XXI. Fiatal Műszakiak Tudományos Ülésszaka. Kolozsvár: Erdélyi Múzeum-Egyesület, 2016. pp. 349–352. http://hdl.handle.net/10598/29102 (letöltve: 2018. 03. 15)

[7] BONNYAI T.: A kritikusinfrastruktúra-védelem elemzése a lakosságfelkészítés tükrében (doktori értekezés tervezet) Budapest: NKE, 2014. DOI azonosító: 10.17625/NKE.2015.001

[8] ERDŐSI P. M. – CISA: ECDL / ICDL, IT biztonság; Budapest, Neumann János Számítógép-tudományi Társaság. 2013.

[9] HORVÁTH G. K.: Közérthetően (nem csak) az IT biztonságról; Budapest, KIFÜ 2013. http://www.kifu.gov.hu/kifu/sites/default/files/IT_brosura_v7.pdf (letöltve: 2018. 03. 05.)

[10] RAJNAI Z.: Információbiztonság tudatosság, In: BITAY E. /szerk./: XXI. Fiatal Műszakiak Tudományos Ülésszak Előadásai. Kolozsvár: Erdélyi Múzeum-Egyesület, 2017. pp.37–42. http://hdl.handle.net/10598/29758 (letöltve: 2018. 03. 15.)

[11] BELÁZ A. – BERZSENYI D.: Kiberbiztonsági Stratégia 2.0 – A kiberbiztonság stratégiai irányításának kérdései. Elemzések. Budapest, Stratégiai Védelmi Kutatóközpont 2017. http://netk.uni-nke.hu/uploads/media_items/svkk-elemzesek-2017-3-kiberbiztonsagi-strategia-2-0-belaz-a-berzsenyi-d.original.pdf (letöltve: 2017. 08. 23.)

[12] JUNCKER, Jean-Claude, az Európai Bizottság elnökének beszéde: Az Unió helyzete 2017. szeptember 13.; Strasbourg 2017. https://ec.europa.eu/commission/sites/beta-political/files/state-union-2017-brochure_hu.pdf (letöltve: 2018. 03. 15.)

[13] MUNCASTER, P.: Security Pros: People Are the Biggest Problem, Infosecurity Magazine, UK 2017. https://www.infosecurity-magazine.com/news/security-pros-people-are-the/ (letöltve:2018. 02. 20.)

[14] European Commission: Resilience, Deterrence and Defence: Building strong cybersecurity in Europe; https://ec.europa.eu/digital-single-market/en/news/resilience-deterrence-and-defence-building-strong-cybersecurity-europe (letöltve: 2018. 02. 21.)

[15] European Union Agency for Network and Information Security: ENISA Threat Landscape Report 2017. Top 15 Cyber-Threats and Trends; https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017 (letöltve: 2018. 02. 24.)

[16] Panda Security: 2017 Cybersecurity Trends; 2017. https://www.pandasecurity.com/mediacenter/pandalabs/annual-report-cybersecurity-predictions-2018/ (letöltve: 2018. 03. 18.)

[17] OLAJOS M.: Az IoT eszközök térnyerése az adatvédelem tükrében In: BOGÁRDI D. – KOCSIS G. /szerk./: Jog és innováció tanulmánykötet. Stádium Intézet Alapítvány Budapest, 2017. pp. 17–28. http://arsboni.hu/wp-content/uploads/2018/03/Arsboni-Tanulm%C3%A1nyk%C3%B6tet_20180305_uj_borit%C3%B3.pdf (letöltve: 2018. 03. 27.)

[18] EGGERS, W. D.: Government's cyber challenge. Protecting sensitive data for the public good; Deloitte Review 19. (2016) pp. 138–155. https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/risk/DR19-governments-cyber-challenge.pdf (letöltve: 2018. 02. 23.)

[19] LIPMAN P.: 4 Critical challenges to State and Local Government Cybersecurity Efforts (Industry Perspective); http://www.govtech.com/opinion/4-Critical-Challenges-to-State-and-Local-Government-Cybersecurity-Efforts.html (letöltve: 2018. 02. 22.)

[20] ROMERO L.: Eye-Opening Findings About Local Government Cyber Security; https://www.pivotpointsecurity.com/blog/local-government-cyber-security-issues/ (letöltve: 2018. 02. 22.)

[21] Socitm Insight Briefing: Push for local cyber security and resilience; Socitm Insight Briefing 83. (2015). http://www.socitm.net/insight (letöltve: 2018. 02. 21.)

[22] European Commission: Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity in Europe; http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017JC0450 (letöltve: 2018. 02. 22.)

[23] Európai Digitális Egységes Piaci Stratégia; http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM:3102_3 (letöltve: 2018. 03. 18.)

[24] Az európai digitális menetrend: http://www.europarl.europa.eu/atyourservice/hu/displayFtu.html?ftuId=FTU_2.4.3.html (letöltve: 2018. 03. 19.)

[25] Európai Digitális Egységes Piaci Stratégia; http://eu.kormany.hu/europai-digitalis-egyseges-piaci-strategia (letöltve: 2018. 03. 18.)

[26] Európai Bizottság tájékoztatója: Hogyan érinti az adatvédelmi reform a közösségi hálózatokat? 2016; file:///C:/Users/DrIsk/Downloads/PP-2016-00621-00-00-HU-TRA-00.pdf (letöltve: 2018. 01. 25.)

[27] BERZSENYI D.: Kiberbiztonsági analógiák és eltérések. A Közép-európai Kiberbiztonsági Platform részes országai által kiadott kiberbiztonsági stratégiák összehasonlító elemzése; Nemzet és Biztonság VII. 6. (2014) pp. 110–136. file:///C:/Users/DrIsk/Downloads/_cikkek_nb_2014_6_10_berzsenyi%20(2).pdf (letöltve: 2018. 02. 04.)

[28] MOLNÁR D.: Mérföldkövek a brit kiberbiztonság fejlődésében I. Az elméleti háttér megalapozása: a kiberbiztonsági stratégia; Hadmérnök XII. „KÖFOP" (2017) pp. 149–162.

[29] Digitális Jólét Program 2.0; Budapest 2017. http://www.kormany.hu/download/6/6d/21000/DJP20%20Strat%C3%A9giai%20Tanulm%C3%A1ny.pdf (letöltve: 2018. 03. 17.)

[30] RAJNAI Z. – FREGAN B.: Új alapokon a Magyarországi kibervédelmi stratégia. In: BITAY E. /szerk./: XXI. Fiatal Műszakiak Tudományos Ülésszak Előadásai. Kolozsvár: Erdélyi Múzeum-Egyesület, 2017. pp. 351–354. http://eda.eme.ro/bitstream/handle/10598/29842/XXII_FMTU_Rajnai.pdf?sequence=3 (letöltve: 2018. 02. 28.)

[31] ILLÉSSY M. – NEMESLAKI A. – SOM Z.: Elektronikus információbiztonság – tudatosság a magyar közigazgatásban; Információs Társadalom XIV. 1. (2014) pp. 52–73. http://real.mtak.hu/41849/1/i_tarsadalom_2014_1_illessy_nemeslaki_som.pdf (letöltve: 2018. 03. 17.)

[32] VERECZKEI Béla *Elektronikus információbiztonsági ellenőrzések tapasztalatai* című előadása az Önkormányzati Road Show keretében, 2017. október 04.

[33] KOVÁCS É.: Koordinációs mechanizmusok és fejlődésük az államigazgatásban (1990–2014). Phd-értekezés. Budapest, Budapesti Corvinus Egyetem Politikatudományi Doktori Iskola 2014. pp. 20–21. http://phd.lib.uni-corvinus.hu/788/1/Kovacs_Eva.pdf (letöltve: 2017. 12. 12.)

[34] RAJNAI Z.: Kibervédelem és kiberkoordináció. Vállalti aspektusok – vízió 2016. Budapest, 2016. njszt.hu/sites/default/files/rajnai.pptx (letöltve: 2018. 04. 08.)

[35] A Nemzeti Infokommunikációs Stratégia 2014–2020. Az infokommunikációs szektor fejlesztési stratégiája (2014–2020) v9.0; 2014. ttp://www.kormany.hu/download/a/f7/30000/NIS_v%C3%A9gleges.pdf (letöltve: 2018. 03. 10.)

[36] E-közigazgatási keretrendszer koncepció; Budapest, Belügyminisztérium 2015. http://www.kormany.hu/download/0/05/50000/E-k%C3%B6zigazgat%C3%A1si_keretrendszer_koncepci%C3%B3.pdf (letöltve: 2018. 02. 28.)

[37] MOLNÁR D.: Egységes Európai kibertér? Az Európai Unió kiberbiztonsági stratégiájának fejlődése; Hadmérnök XII. 1. (2017) pp. 255–267.

[38] KÓNYA L. – FARKAS ZS. – PUSZTAI A. – TÓZSA I. – SIMON B. – TÓTH F.: Önkormányzatok jogállása és döntési kompetenciája; Budapest, NKE 2014. p. 12.

[39] Önkormányzatiság Magyarországon; Kormányportál. http://2010-2014.kormany.hu/hu/mo/onkormanyzatisag-magyarorszagon (letöltve: 2017. 03. 10.)

[40] BEKÉNYI J. /szerk./: Szabályozási segédlet a helyi önkormányzati feladatok ellátásához; Budapest, Belügyminisztérium 2017.

[41] Érdemi nyilvánosság az önkormányzati döntéshozatalban. Útmutató helyi önkormányzatoknak; Budapest, NVSZ 2016. http://korrupciomegelozes.kormany.hu/download/6/42/a1000/%C3%9ATMUTAT%C3%93.pdf (letöltve: 2018. 03. 10.)

[42] Információszabadság állásfoglalások, jelentések; Budapest, NAIH. https://www.naih.hu/informacioszabadsag-allasfoglalasok,-jelentesek.html (letöltve: 2018. 03. 11.)

[43] BUDAI B. B. – HERMAN Sz.: Az Infotv. közzétételi kötelezettségének gyakorlata. Önkormányzati tanácsadó 3. Budapest, Menedzser praxis. 2018.

[44] NEWMAN D.: Top 6 Digital Transformation Trends In Government; 2017. https://www.forbes.com/sites/danielnewman/2017/06/29/top-6-digital-transformation-trends-in-government/#2e4e52dc7efc (letöltve: 2018. 01. 02.)

[45] ITBUSINESS: DJP 2.0: jött, látott, győzött; 2017. http://www.itbusiness.hu/Fooldal/rss_3/DJP_20_jott_latott_gyozott.html (letöltve: 2018. 03. 17.)

[46] Digitális Jólét Program: Magyarország Digitális Oktatási Stratégiája (DOS); 2016. http://www.kormany.hu/download/0/cc/d0000/MDO.pdf (letöltve: 2018. 03. 17.)

[47] (n. n.) Rosszul elköltött pénz; Biztosítási szemle 2017. http://www.biztositasiszemle.hu/cikk/elemzesek/NULL/rosszul_elkoltott_penz.6865.html (letöltve: 2018. 02. 03.)

[48] GAJDUSCHEK Gy.: Miben áll, és mérhető-e a kormányzati teljesítmény? Politikatudományi Szemle 2014. 23. évf. 3. szám pp. 97–118. http://www.poltudszemle.hu/szamok/2014_3szam/gajduschek.pdf (letöltés: 2017. 12. 21.)

[49] ENDRŐDI I.: Polgári védelmi ismeret. Budapest, Magyar Polgári Védelmi Szövetség 2015. www.mpvsz.hu/letoltes/document/download.php?id=125-polgari-vedelemi-ismeret2015.pdf (letöltve: 2018. 04. 05.)

[50] 234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról

[51] A Bizottság közleménye a Tanács és az Európai Parlament részére – A létfontosságú infrastruktúrák védelme a terrorizmus elleni küzdelemben

[52] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

[53] 2016. évi CXVI. törvény az egyes belügyi tárgyú törvények módosításáról

[54] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról;

[55] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

[56] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)

[57] 2012/2015. (XII. 29.) Korm. határozat az internetről és a digitális fejlesztésekről szóló nemzeti konzultáció (InternetKon) eredményei alapján a Kormány által végrehajtandó Digitális Jólét Programjáról

[58] 38/2012. (III. 12.) Kormányrendelet a kormányzati stratégiai irányításáról

[59] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[60] 26/2013. (X. 21.) KIM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról

[61] 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól

[62] 484/2013. (XII. 17.) Korm. rendelet a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről

[63] A TANÁCS 98/83/EK IRÁNYELVE (1998. november 3.) az emberi fogyasztásra szánt víz minőségéről

[64] 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól

[65] 2016. évi CL. törvény az általános közigazgatási rendtartásról

[66] 2013. évi CCXX. törvény az állami és önkormányzati nyilvántartások együttműködésének általános szabályairól

[67] Magyarország Alaptörvénye (2011. április 25.)

[68] 2011. évi CLXXXIX. törvény Magyarország helyi önkormányzatairól

[69] 273/2012. (IX. 28.) Korm. rendelet a közszolgálati tisztviselők továbbképzéséről

[70] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

[71] 2015. évi XCVI. törvény az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény és a közadatok újrahasznosításáról szóló 2012. évi LXIII. törvény módosításáról

[729] 61/2012. (XII. 11.) BM rendelet a települések katasztrófavédelmi besorolásáról, valamint a katasztrófák elleni védekezés egyes szabályairól szóló 62/2011. (XII. 29.) BM rendelet módosításáról

[73] 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;

[74] 2015. évi CXXX. törvény az e-kártya megvalósításához szükséges egyes törvények, valamint az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény módosításáról

[75] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról

[76] 234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról

[77] Önkormányzati rendeletek – Nemzeti Jogszabálytár.
http://njt.hu/njt.php?onkormanyzati_rendeletek (letöltve: 2018. 03. 21.)

[78] Magyar Államkincstár Általános Információk: http://www.allamkincstar.gov.hu/hu/koltsegvetesi-informaciok/torzskonyv_altalanos (letöltve: 2018. 03. 21.)

RÖVIDÍTÉSJEGYZÉK

Rövidítés	
IKT	Info-kommunikációs technológia
NEIH	Nemzeti Elektronikus Információbiztonsági Hatóság
BM	Belügyminisztérium
NKIV	Nemzeti kritikus infrastruktúrák védelme
ENISA	Európai Hálózat- és Információbiztonsági Ügynökség
IoT	Dolgok Internete
GDPR	General Data Protection Regulation
NIS	Network and Information Security
NIS-irányelv	Hálózatok és információs rendszerek biztonságáról szóló irányelv
PPP	public private partnership
CECSP	Central European Cyber Security Platform
Ibtv.	az állami és önkormányzati szervek elektronikus információbiztonságáról szóló a 2013. évi L. törvény
Infotv.	az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény
DJP	Digitális Jólét Program
SWOT	Strenghts, Weaknesses, Opportunities, Threats
IB	információbiztonság
BM OKF	Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság
NKE	Nemzeti Közszolgálati Egyetem
GovCERT	Kormányzati Eseménykezelő Központ
NKI	Nemzeti Kibervédelmi Intézet
BM OKF LRLIBEK	BM OKF Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ
HunCERT	MTA–SZTAKI által működtetett információbiztonsági eseménykezelő szervezet
NIIF	Nemzeti Információs Infrastruktúra Fejlesztési Program
NIIF CSIRT	Kormányzati Informatikai Fejlesztési Ügynökség által működtetett

	számítógépes biztonsági eseménykezelő szervezet
BM ÖKI	BM Önkormányzati Koordinációs Iroda
DOS	Digitális Oktatási Stratégia
CERT-UK	Computer emergency response team United Kingdom
EIB	elektronikus információbiztonság
ASP	Application Service Provider
OGP	Open Government Partnership
NAIH	Nemzeti Adatvédelmi és Információszabadság Hatóság
NVSZ	Nemzeti Védelmi Szolgálat

TÁBLÁZATJEGYZÉK

1. táblázat: A CECSP országok első kiberbiztonsági stratégiáinak összehasonlítása
2. táblázat: Ibtv. elvárásainak való önkormányzati megfelelés
3. táblázat: Az adatkezelési szabályzat megléte
4. táblázat: A főkomponens analízis eredményei.
5. táblázat: A GLM analízisek eredményei
6. táblázat: A kibertámadás bekövetkezésének veszélyessége
7. táblázat: Kibertámadás bekövetkezésének valószínűsége rosszindulatú támadás céljából lakosságszám-kategóriák szerint
8. táblázat: Kibertámadás bekövetkezésének valószínűsége az információs rendszer ellen
9. táblázat: Kibertámadás bekövetkezésének valószínűsége információszerzés, előnyszerzés céljából
10. táblázat: Az önkormányzat sebezhetőségének állapota a működés biztonságát tekintve lakosságszám-kategóriák szerint
11. táblázat: Az önkormányzat sebezhetőségének állapota az információbiztonság tekintetében lakosságszám-kategóriák szerint
12. táblázat: Az önkormányzat sebezhetőségének állapota a közbiztonság tekintetében lakosságszám-kategóriák szerint
13. táblázat: Kibertámadás esetén az önkormányzatra jellemző állítások a dolgozók tájékozottsága és felkészültsége tekintetében
14. táblázat: Az önkormányzatra jellemző állítások a kibertámadások elhárítására motivált és felkészült munkatársak tekintetében
15. táblázat: Kibertámadás esetén az önkormányzatra jellemző állítások a helyreállítási terv alkalmazhatósága tekintetében
16. táblázat: Az önkormányzatok levelezőrendszerének titkosítása

17. táblázat: Külső rendszerekre, kiszervezett feladatokra vonatkozó kockázatelemzés, kockázatmenedzsment megléte
18. táblázat: Védelmi mechanizmusok, protokollok megléte a támadások esetére
19. táblázat: Megtörtént informatikai incidenssel kapcsolatos információ
20. táblázat: Az önkormányzatok online megjelenésének rotált komponensmátrixa (faktormátrixa)

ÁBRAJEGYZÉK

1. ábra Információbiztonsági funkciók és szervezetek 42
2. ábra A kormányzati kiberkoordináció szervezetei 44
4. ábra Kormányzati szolgáltatási platform 49
5. ábra Települések számának megoszlása lakosságszám szerint (2016.01.01.) 55
6. ábra Az önkormányzati hivatalok típus szerinti megoszlása (2016) 56
7. ábra Információbiztonsági stratégia rendelkezésre állása (2018.02.13.) 59
8. ábra Informatikai rendszerek ellen elkövetett támadások esetén követendő protokollok kidolgozottsága 60
9. ábra Összefoglaló – Az egyes közzétételi egységek előfordulási aránya (%). 63
10. ábra Magyarország Digitális Oktatási Stratégiájának szerkezete 65
11. ábra Válaszadó települések megoszlása lakosságszám szerint 74
12. ábra Válaszadó települések megoszlása önkormányzati hivatalok típusa szerint 74
13. ábra Válaszadók megoszlása a szervezetben betöltött pozíciójuk szerint 75
14. ábra A kibertámadás bekövetkezésének veszélyessége 79
15. ábra A kibertámadás bekövetkezésének veszélyessége lakosságszám-kategóriák szerint 80
16. ábra Adott területen egy kibertámadás bekövetkezési valószínűsége (összefoglalás) 80
17. ábra Kibertámadás bekövetkezésének valószínűsége a közszolgáltatások esetében 81
18. ábra Közszolgáltatások elleni kibertámadás bekövetkezésének valószínűsége (összegezve) 81
19. ábra Kibertámadás bekövetkezésének valószínűsége illetéktelen információszerzés céljából 82
20. ábra Kibertámadás bekövetkezésének valószínűsége illetéktelen információszerzés céljából lakosságszám-kategóriák szerint 83
21. ábra Kibertámadás bekövetkezésének valószínűsége rosszindulatú támadás céljából 83
22. ábra Kibertámadás bekövetkezésének valószínűsége a hivatal online közösségi helye elleni támadás szerint 85
23. ábra Kibertámadás bekövetkezésének valószínűsége a hivatal online közösségi helye ellen lakosságszám-kategóriák szerint 85

24. ábra Kibertámadás bekövetkezésének valószínűsége információszerzés, előnyszerzés céljából lakosságszám-kategóriák szerint 86
25. ábra Kibertámadás bekövetkezésének valószínűsége egyéb hivatali hálózati kapcsolatok ellen . 87
26. ábra Kibertámadás bekövetkezésének valószínűsége egyéb hivatali hálózati kapcsolatok ellen a lakosságszám-kategóriák szerint 88
27. ábra Kiberfenyegetettség megítélése a különböző lakosságszám kategóriába tartozó települések esetében 88
28. ábra Elemek sebezhetősége (összefoglaló) 89
29. ábra Az önkormányzat sebezhetőségének állapota a kommunikáció biztonsága szerint 90
30. ábra Az önkormányzat sebezhetőségének állapota a kommunikáció biztonságát tekintve lakosságszám-kategóriák szerint 90
31. ábra Az önkormányzat sebezhetőségének állapota a működés biztonsága szerint 91
32. ábra Az önkormányzat sebezhetőségének állapota az információbiztonság tekintetében 92
33. ábra Az önkormányzat sebezhetőségének állapota a fizikai biztonság tekintetében 93
34. ábra Az önkormányzat sebezhetőségének állapota a fizikai biztonság tekintetében lakosságszám-kategóriák szerint 94
35. ábra Az önkormányzat sebezhetőségének állapota a közbiztonság tekintetében 94
36. ábra A válaszadók véleménye a kiberbiztonság érdekében szükséges teendőkkel/módszerekkel kapcsolatban 96
37. ábra A felkészülés módszerei 96
38. ábra Kibertámadás esetén az önkormányzatra jellemző állítások a rendszer és a hálózat védettsége tekintetében 98
39. ábra Kibertámadás esetén az önkormányzatra jellemző állítások a rendszerhasználat szabályozottsága tekintetében 98
40. ábra Kibertámadás esetén az önkormányzatra jellemző állítások a folyamatos infrastrukturális fejlesztés tekintetében 99
41. ábra Kibertámadás esetén az önkormányzatra jellemző állítások a számítógépek és szoftverek frissítése és modernizációja tekintetében 100
42. ábra Kibertámadás esetén az önkormányzatra jellemző állítások az adatok, online megjelenések megfelelő biztosítottsága tekintetében 102
43. ábra Felkészültség megítélése a különböző lakosságszám kategóriába tartozó települések esetében 103
44. ábra Felkészültség megítélése a különböző hivatali státuszú települések esetében 104

45. ábra Protokoll megléte kibertámadás esetére 105
46. ábra Protokoll megléte a jelszavak kezelésére és módosítására 106
47. ábra Rendszeres fenyegetettséget tudatosító képzés megléte a munkatársak részére 108
48. ábra A klaszterezés minősítése 122
49. ábra Az osztályozó változó átlagának alakulása az egyes klaszterekben 123
50. ábra Egyes klaszterek további jellemzése 124

MELLÉKLETEK

1. melléklet – Elektronikus információbiztonsági vezető szakirányú továbbképzési szak[20]

Az oklevélben szereplő szakképzettség megnevezése: Elektronikus információbiztonsági vezető.

A képzési idő 2 félév; a képzés óraszáma 300 óra.

A felvétel feltétele: A képzésben legalább alapképzésben (korábban főiskolai szintű képzésben) szerzett oklevéllel rendelkezők vehetnek részt. Azok, akik angol nyelvű alapfokú komplex nyelvvizsgával, vagy ezzel egyenértékű bizonyítvánnyal, oklevéllel rendelkeznek.

A képzés célja: A képzés fő célja az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott elektronikus információs rendszer biztonságáért felelős személyek feladatellátáshoz szükséges szakmai kompetenciák átadása és a biztonságtudatos szemléletmód kialakítása.

A képzés célcsoportja: A szakirányú végzettség birtokában az elektronikus információs rendszer biztonságáért felelős személyek a megfelelő információbiztonsági rendszer kialakítása és fenntartása mellett ismereteivel és hozzáállásával növeli a szervezet biztonságát, neveli a munkatársakat, így összességében csökkenti a szervezet biztonsági kitettségét a hagyományos és informatikai támadókkal szemben.

A képzés során elsajátítandó kompetenciák, tudáselemek, megszerezhető ismeretek: A képzés során az elektronikus információs rendszer biztonságáért felelős személyek munkájához szükséges kompetenciák, ismeretek szerezhetők meg: jogi, igazgatási, biztonsági, minőségi, vezetési alapok; kockázatkezelés; biztonsági rendszer irányítása; incidensek kezelése.

A képzés során megszerezhető személyes adottságok, készségek: Magabiztos szakmai tudás az elektronikus információs rendszer biztonságáért felelős személy munkájában, a kötelezett szervek bármelyikénél. Problémafelismerő- és megoldó készség, biztonságtudatos gondolkodásmód. Képesség a rendszerek átlátására és a szükséges intézkedések megfelelő kialakítására.

A képzés módszertana: A levelező rendszerű képzés elméleti és gyakorlati órák segítségével, valamint e-learning támogatásával járul hozzá az ismeretek elsajátításához, és az ismeretek gyakorlatban történő hasznosításához.

A szakképzettség megszerzéséhez összegyűjtendő kreditek száma: 60 kreditpont.

A képzés főbb tárgyai: Minőségügyi ismeretek; Biztonságtechnika; Biztonságpolitika; Jogi és közigazgatási ismeretek; Vezetéselmélet; Információbiztonsági szabványok; Irányítási rendszerek; Kockázatértékelés, kockázatmenedzsment; Kockázatmenedzsment gyakorlat; Információbiztonsági program; Biztonsági technológiák alkalmazása; Információbiztonsági stratégia és vezetés; Biztonság támogatása; Biztonságtudatossági gyakorlat; Rendszerek biztonsága; Hálózatok biztonsága; Biztonsági tesztelés gyakorlat; Incidens-menedzsment, BCP, DRP integráció; Incidens-menedzsment gyakorlat.

[20] Elektronikus információbiztonsági vezető szakirányú továbbképzési szak, NKE; https://vtkk.uni-nke.hu/szakiranyu-tovabbkepzesek/szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto (letöltve: 2018. 03. 17.)

2. melléklet – Elektronikus információs rendszerek vezetői és résztvevői továbbképzések

Program neve	Célcsoport	Tematika	E-learning	Képzési díj
Továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára	Az elektronikus információs rendszerek védelméért felelős vezetők	1. Az információbiztonság folyamata 2. Az informatikai biztonság jogi szabályozása	0 óra gyakorlat 0 óra elmélet 8 óra e-learning	0 Ft
Továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára	Az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek.	1. Adminisztratív védelem 2. Az információbiztonság folyamata 3. Az informatikai biztonság jogi szabályozása 4. Fizikai védelem 5. Logikai védelem	0 óra gyakorlat 0 óra elmélet 50 óra e-learning	0 Ft
Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára – Célzott kibertámadások	Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott, az elektronikus információs rendszerek védelméért felelős vezetők.	1. Újdonságok a magyar kibervédelmi szabályozásban 2. Új típusú támadások államok és szervezetek ellen 3. Állami feladatok a közszolgálatot érő célzott kibertámadások esetén	0 óra gyakorlat 0 óra elmélet 8 óra e-learning	0 Ft
Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető		A kibertér aktuális nemzetközi biztonságpolitikai kihívásai 1. A kiberteret érintő nemzetközi megállapodások 2016-ban 2. Információs műveletek a kibertérben 3. A terrorizmus támogatása informatikai eszközökkel, és az ez elleni fellépés módszerei 4. A hadviselés kiterjesztése a		

számára – Incidensmenedzsment		kibertérre Biztonsági eseménykezeléssel kapcsolatos elvárások a hazai és nemzetközi jogban 1. Eseménykezelés az Ibtv. tükrében 2. Eseménykezelési elvárások a GDPR szabályozásban 3. Eseménykezelés az NIS tükrében		
Éves továbbképzés az EIB rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára – Célzott kibertámadások	Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 13. § (11) bekezdésében meghatározott, az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek.	1. Az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személyek kötelezettségei a célzott támadások elhárításában a 2013. évi L. törvény (Ibtv.) és végrehajtási rendeletei szerint 2. Cyber kill chain – műszaki védelem a célzott támadások ellen 3. Információgyűjtés a célzott támadások kivitelezéséhez 4. Social engineering technikák 5. Kártékony kódok használata a célzott támadások végrehajtásában	0 óra gyakorlat 0 óra elmélet 25 óra e-learning	0 Ft
Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára – Incidensmenedzsment Név:		A kibertér aktuális nemzetközi biztonságpolitikai kihívásai 1. A kiberteret érintő nemzetközi megállapodások 2016-ban 2. Információs műveletek a kibertérben 3. A terrorizmus támogatása informatikai eszközökkel, és az ez elleni fellépés módszerei 4. A hadviselés kiterjesztése a kibertérre Biztonsági eseménykezeléssel kapcsolatos elvárások a hazai és nemzetközi jogban 1. Eseménykezelés az Ibtv. tükrében 2. Eseménykezelési elvárások a GDPR szabályozásban 3. Eseménykezelés az NIS tükrében 4. Megfelelőség biztosítása az üzemeltetés során 5. Megfelelőség biztosítása a fejlesztés során Az eseménykezelés műszaki eszköztára – üzemeltetői, fejlesztői feladatok 1. Az incidensmenedzsment műszaki eszköztára – áttekintés 2. Referenciaarchitektúrák kis, közepes és nagy szervezetek számára 3. Üzemeltetői tevékenységek	0 óra gyakorlat 0 óra elmélet 25 óra e-learning	0 Ft

		4. Fejlesztői tevékenységek az incidensmenedzsment támogatására Incidenskezelés felhasználói szemmel 1. A biztonsági incidensek bemutatása, felismerésük lehetőségei 2. Az incidensek jelentésének folyamata 3. Részvétel az incidenskezelésben		
Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára (okoseszközök)		A továbbképzési program 3 egymásra épülő modulból áll: 1. Bevezető az okoseszközök világába 2. Okoseszközökhöz kapcsolódó adatvédelmi kérdések 3. Az okoseszközökhöz kapcsolódó kiberbiztonsági kihívások.	0 óra gyakorlat 0 óra elmélet 25 óra e-learning	0 Ft

Forrás: NKE http://archiv.vtki.uni-nke.hu/tovabbkepzes/celcsoportok/kepzesek-az-elektronikus-informacios-rendszer-biztonsagaert-felelos-szemely-reszere (saját szerkesztés)

3. melléklet — Online kérdőív kérdései

Az *Önkormányzatok és kiberbiztonság* című, 2018 januárjában az önkormányzatok részére elektronikusan megküldött kérdőív kérdései.

1.	**Alapadatok – Válasszon a legördülő listából!**										
	Megye	1. Bács-Kiskun megye									
		2. Baranya megye									
		3. Békés megye									
		4. Borsod-Abaúj-Zemplén megye									
		5. Csongrád megye									
		6. Fejér megye									
		7. Győr-Moson-Sopron megye									
		8. Hajdú-Bihar megye									
		9. Heves megye									
		10. Jász-Nagykun-Szolnok megye									
		11. Komárom-Esztergom megye									
		12. Nógrád megye									
		13. Pest megye									
		14. Somogy megye									
		15. Szabolcs-Szatmár-Bereg megye									
		16. Tolna megye									
		17. Vas megye									
		18. Veszprém megye									
		19. Zala megye									
	Lakosságszám	–1 000									
		1 001–5 000									

		2 001–5 000									
		5 001–20 000									
		20 001–50 000									
		50 001–									
	Település típusa	község									
		nagyközség									
		város									
		járásszékhely város									
		megyei jogú város									
	Hivatal típusa	önálló									
		közös hivatal székhelye									
		közös hivatal									
	Kitöltő	polgármester									
		jegyző									
		ügyintéző									
		informatikus egyéb									
2.	**Kibertér – kiberbiztonság**										
	Ön az önkormányzat szempontjából mennyire tartja veszélyesnek egy esetlegesen bekövetkező kibertámadás lehetőségét?										
	Skála:	1. – 5.	1 = nem jelentős; 5 = kritikus								
	Mely területen és milyen valószínűnek a tartja kibertámadás bekövetkezési valószínüségét?										
		Közszolgáltatások Illetéktelen információszerzés (önkormányzat és a lakosok adatai) Rosszindulatú támadások (zsarolóvírus, rendszerbénítás) Információs támadások (adatmegváltoztatás, rémhírterjesztés, egyéb) Közösségi megjelenési helyek (honlap, Facebook, stb.) támadása Előnyszerzés céljából – információszerzés Egyéb hálózati kapcsolatok (ASP, Kincstár, stb.)										
		Valószínűség	0–100%	25 %-os lépésekkel							
	Mennyire tartja sebezhetőnek az önkormányzatnál az alábbi elemeket?										
		A kommunikáció biztonsága (az információs rendszer technikai infrastruktúrája)									
		A működés biztonsága (munkafolyamatok zavartalansága)									
		Az információ biztonsága (az információs rendszerben tárolt vagy továbbított információ védelme)									
		A fizikai biztonság (az információs rendszer védelme a fizikai veszélyektől)									
		Közbiztonság (a kibertérből származó olyan fenyegetések, amelyek egyaránt veszélyeztethetik a fizikai rendszereket és a kiberteret, pl.: kiterjedt szolgáltatás megtagadással járó támadás)									

	1–5.	1 = elhanyagolható; 5 = nagyon sebezhető										
	A felkészülés során Ön szerint a védekezés, az elrettentés vagy a fejlesztés a legfontosabb?											
		1 = védekezés										
		2 = fejlesztés										
		3 = elrettentés										
3	**Felkészültség/képesség**											
	Az egyes területeken az önkormányzatra mennyire jellemzőek az alábbi állítások:											
		Rendszereink és hálózatunk védett.										
		A rendszerhasználat szabályozott.										
		A folyamatos fejlesztés sokat tesz hozzá a védelemhez.										
		Munkatársaink tisztába vannak a fenyegetésekkel és felkészültek.										
		Gépeink és szoftvereink modernek és folyamatosan frissítjük őket.										
		Munkatársaink motiváltak és felkészültek, hogy elhárítsák az esetleges támadásokat.										
		Adataink, online megjelenéseink megfelelően biztosítottak.										
		Ha sérülés történik a helyreállítási terv segítségével gyorsan működőképes a rendszerünk.										
	Skála:	1: nem; 2: alig; 3: részleteiben; 4: többségében; 5: teljesen										
	Kötelezettségek/lehetőségek											
		Van-e az önkormányzatnak információbiztonsági stratégiája?										
		Van-e az önkormányzatnak adatkezeléssel foglalkozó szabályzata?										
		Van-e protokoll az informatikai rendszeren elkövetett támadások esetére?										
		Működik-e titkosítás a levelező rendszerhez kapcsolódóan?										
		Működik-e jelszókezelési és -módosítási protokoll?										
		Van-e a külső rendszerekre, kiszervezett feladatokhoz kapcsolódóan kockázatelemzés, kockázatmenedzsment rendszer?										
		Van-e rendszeres fenyegetettséget tudatosító képzés a munkatársak részére?										
	Válasz lehetőségek: 1: igen; 2: nem; 3: részben; 4: tervezzük											
4.	**Működési tapasztalatok**											
	Van-e ismeretük informatikai eszközeik elleni támadásokról, volt-e már ilyen incidensük?											
		1 = igen										
		2 = nem										
			ha igen, akkor hogyan kezelték, mi történt: (leírás)									
	Van-e protokoll az informatikai rendszeren elkövetett támadások esetére, vannak-e védelmi mechanizmusok?											

		1 = igen, vannak									
		2 = nem, nincsenek									
		3 = részben									
			Ha igen, akkor melyek ezek?		(szöveges válasz)						
	Mi történik a régi informatikai eszközökkel?										
		1 = eladásra kerül a munkatársaknak									
		2 = elajándékozzuk									
		3 = leselejtezés után raktárba kerül									
		4 = egyéb									
	Hogyan szabályozzák az egyéb eszközök (telefon, tablet, adathordozók) használatát?										
		1 = tilos									
		2 = engedéllyel használható									
		3 = mindenki szabadon használhatja									
		4 = egyéb									
	Közösségi média használatával kapcsolatos tapasztalataik (honlap, Facebook, stb.)										
		rövid szöveges válasz									

4. melléklet – Változók a főkomponens elemzésben

veszélyes	Ön az önkormányzat szempontjából mennyire tartja veszélyesnek egy esetlegesen bekövetkező kibertámadás lehetőségét?
kiber1	Mely területen és milyen valószínűnek a tartja kibertámadás bekövetkezési valószínűségét? [Közszolgáltatások]
kiber2	Mely területen és milyen valószínűnek a tartja kibertámadás bekövetkezési valószínűségét? [Illetéktelen információszerzés (önkormányzat és a lakosok adatai)]
kiber3	Mely területen és milyen valószínűnek a tartja kibertámadás bekövetkezési valószínűségét? [Rosszindulatú támadások (zsaroló vírus, rendszerbénítása)]
kiber4	Mely területen és milyen valószínűnek a tartja kibertámadás bekövetkezési valószínűségét? [Információs támadások (adat megváltoztatása, rémhírterjesztés, egyéb)]
kiber5	Mely területen és milyen valószínűnek a tartja kibertámadás bekövetkezési valószínűségét? [Közösségi megjelenési helyek (honlap, Facebook, stb.) támadása]
kiber6	Mely területen és milyen valószínűnek a tartja kibertámadás bekövetkezési valószínűségét? [Előnyszerzés céljából – információszerzés]
kiber7	Mely területen és milyen valószínűnek a tartja kibertámadás bekövetkezési valószínűségét? [Egyéb hálózati kapcsolatok (ASP, Kincstár, stb.)]

sebezheto1	Mennyire tartja sebezhetőnek az önkormányzatnál az alábbi elemeket? [A kommunikáció biztonsága (az információs rendszer technikai infrastruktúrája)]
sebezheto2	Mennyire tartja sebezhetőnek az önkormányzatnál az alábbi elemeket? [A működés biztonsága (munkafolyamatok zavartalansága)]
sebezheto3	Mennyire tartja sebezhetőnek az önkormányzatnál az alábbi elemeket? [Az információs biztonsága (az információs rendszerben tárolt vagy továbbított információ védelme)]
sebezheto4	Mennyire tartja sebezhetőnek az önkormányzatnál az alábbi elemeket? [A fizikai biztonság (az információs rendszer védelme a fizikai veszélyektől]
sebezheto5	Mennyire tartja sebezhetőnek az önkormányzatnál az alábbi elemeket? [Közbiztonság (a kibertérből származó olyan fenyegetések, amelyek egyaránt veszélyeztethetik a fizikai rendszereket és a kiberteret – pl.: kiterjedt szolgáltatás megtagadással járó támadás)]
jellemzo1	Az egyes területeken az önkormányzatra mennyire jellemzőek az alábbi állítások: Kibertámadás esetén [rendszereink és hálózatunk védett.]
jellemzo2	Az egyes területeken az önkormányzatra mennyire jellemzőek az alábbi állítások: Kibertámadás esetén [a rendszerhasználat szabályozott.]
jellemzo3	Az egyes területeken az önkormányzatra mennyire jellemzőek az alábbi állítások: Kibertámadás esetén [a folyamatos fejlesztés sokat tesz hozzá a védelemhez]
jellemzo4	Az egyes területeken az önkormányzatra mennyire jellemzőek az alábbi állítások: Kibertámadás esetén [munkatársaink tisztába vannak a fenyegetésekkel és felkészültek.]
jellemzo5	Az egyes területeken az önkormányzatra mennyire jellemzőek az alábbi állítások: Kibertámadás esetén [gépeink és szoftvereink modernek, és folyamatosan frissítjük őket.]
jellemzo6	Az egyes területeken az önkormányzatra mennyire jellemzőek az alábbi állítások: Kibertámadás esetén [munkatársaink motiváltak és felkészültek, hogy elhárítsák az esetleges támadásokat.]
jellemzo7	Az egyes területeken az önkormányzatra mennyire jellemzőek az alábbi állítások: Kibertámadás esetén [adataink, online megjelenéseink megfelelően biztosítottak.]
jellemzo8	Az egyes területeken az önkormányzatra mennyire jellemzőek az alábbi állítások: Kibertámadás esetén [ha sérülés történik a helyreállítási terv segítségével gyorsan működőképes a rendszerünk.]
kötelezettseg1	Kötelezettségek – lehetőségek [Van-e az önkormányzatnak információbiztonsági stratégiája?]

kötelezettseg2	Kötelezettségek – lehetőségek [Van-e az önkormányzatnak adatkezeléssel foglalkozó szabályzata?]
kötelezettseg3	Kötelezettségek – lehetőségek [Van-e protokoll az informatikai rendszeren elkövetett támadások esetére?]
kötelezettseg4	Kötelezettségek – lehetőségek [Működik-e titkosítás a levelező rendszerhez kapcsolódóan?]
kötelezettseg5	Kötelezettségek – lehetőségek [Működik-e jelszókezelési és módosítási protokoll?]
kötelezettseg6	Kötelezettségek – lehetőségek [Van-e a külső rendszerekre, kiszervezett feladatkhoz kapcsolódóan kockázatelemzés, kockázat menedzsment rendszer?]
kötelezettseg7	Kötelezettségek – lehetőségek [Van-e rendszeresen a fenyegetettséget tudatosító képzés a munkatársak részére?]
protokoll	Van-e protokoll az informatikai rendszeren elkövetett támadások esetére, vannak-e védelmi mechanizmusok?

Forrás: saját szerkesztés.

5. melléklet – Lakosságszám csoportok a főkomponens elemzéshez

Független változók	Csoportszám	Csoportosítás alapja	Elemszám (n)
lakosságszám (fő)	1	0–1000	240
	2	1001–5000	202
	3	5001–20 000	39
	4	20 001–50 000	20
	5	50 001–	11
hivatal	1	önálló	102
	2	közös hivatal székhelye	157
	3	közös hivatal tagja	253
település	1	község	409
	2	nagyközség	20
	3	város	62
	4	járásszékhely város	12
	5	nagyobb város (megyei jogú városok + 2 db. fővárosi kerület)	9

Forrás: saját szerkesztés.

6. melléklet – A faktoranalízis eredményei

KMO és Bartlett teszt

KMO and Bartlett's Test		
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,792
Bartlett's Test of Sphericity	Approx. Chi-Square	9180,981
	df	66
	Sig.	,000

Anti-image korrelációs mátrix

	Könnyen átlátható-e a honlap kezdőlapja	A honlap menü pontjai könnyen átláthatóak	A honlap utolsó frissítésének dátuma	Van-e hivatkozás/link a település FB oldalára?	Integrált-e a honlapba a FB?	lakosság számára fontos és használható adatbázissal	az ellátott feladatokról, eredményekről?	Közérthető-e a tájékoztatás?	programokra vonatkozó dokumentumok?	stratégiákra vonatkozó dokumentumok?	szolgáltatásokkal kapcsolatosan?	fenntartott vagy működtetett intézményekről?
Könnyen átlátható-e a honlap kezdőlapja	,748[a]	-0,614	0,004	0,011	-0,012	-0,063	-0,026	-0,169	-0,052	0,007	-0,035	0,021
A honlap menü pontjai könnyen átláthatóak	-0,614	,751[a]	0,076	-0,012	-0,028	-0,102	-0,006	-0,134	0,108	-0,067	-0,035	-0,089
A honlap utolsó frissítésének dátuma	0,004	0,076	,885[a]	0,063	0,041	0,092	-0,029	0,101	0,228	0,118	0,015	0,104
Van-e hivatkozás/link a település FB oldalára?	0,011	-0,012	0,063	,609[a]	-0,590	-0,022	-0,049	0,015	-0,013	0,041	-0,049	-0,004
Integrált-e a honlapba a FB?	-0,012	-0,028	0,041	-0,590	,617[a]	-0,014	-0,002	0,014	-0,085	-0,040	0,015	0,009
Rendelkezik-e a weboldal a lakosság számára fontos és használható adatbázissal	-0,063	-0,102	0,092	-0,022	-0,014	,919[a]	-0,082	-0,074	-0,087	-0,090	-0,116	-0,176
Található-e megfelelő tájékoztatás a honlapon az önkormányzat munkájáról, az ellátott feladatokról, eredményekről?	-0,026	-0,006	-0,029	-0,049	-0,002	-0,082	,755[a]	0,001	-0,017	-0,162	-0,455	0,011
Közérthető-e a tájékoztatás?	-0,169	-0,134	0,101	0,015	0,014	-0,074	0,001	,878[a]	-0,100	-0,014	0,069	-0,229

Találhatóak-e a honlapon települési/önkormányzati programokra vonatkozó dokumentumok?	-0,052	0,108	0,228		-0,013	-0,085	-0,087	-0,017	-0,100	,844[a]	-0,102	-0,023	-0,113
Találhatóak-e a honlapon települési/önkormányzati stratégiákra vonatkozó dokumentumok?	0,007	-0,067	0,118		0,041	-0,040	-0,090	-0,162	-0,014	-0,102	,894[a]	-0,148	-0,033
Talál-e információt az önkormányzat által nyújtott szolgáltatásokkal kapcsolatosan?	-0,035	-0,035	0,015		-0,049	0,015	-0,116	-0,455	0,069	-0,023	-0,148	,769[a]	-0,069
Van-e információ, adatbázis az önkormányzat által fenntartott vagy működtetett intézményekről?	0,021	-0,089	0,104		-0,004	0,009	-0,176	0,011	-0,229	-0,113	-0,033	-0,069	,879[a]

Megmagyarázott varianciahányad

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative (%)	Total	% of Variance	Cumulative (%)	Total	% of Variance	Cumulative (%)
1	3,839	31,988	31,988	3,839	31,988	31,988	2,232	18,600	18,600
2	1,532	12,766	44,755	1,532	12,766	44,755	1,964	16,366	34,966
3	1,336	11,131	55,886	1,336	11,131	55,886	1,947	16,225	51,191
4	1,068	8,896	64,782	1,068	8,896	64,782	1,631	13,591	64,782
5	0,734	6,116	70,898						
6	0,652	5,429	76,328						
7	0,619	5,158	81,486						
8	0,603	5,027	86,513						
9	0,535	4,458	90,970						
10	0,43	3,608	94,578						

	3								
11	0,380	3,164	97,742						
12	0,271	2,258	100,000						

Rotált komponensmártix

	Component			
	1	2	3	4
A honlap menü pontjai könnyen átláthatóak	0,869	0,175	0,097	0,085
Könnyen átlátható-e a honlap kezdőlapja	0,864	0,154	0,086	0,071
Közérthető-e a tájékoztatás?	0,612	-0,023	0,443	-0,025
Található-e megfelelő tájékoztatás a honlapon az önkormányzat munkájáról, az ellátott feladatokról, eredményekről?	0,091	0,836	0,029	0,082
Talál-e információt az önkormányzat által nyújtott szolgáltatásokkal kapcsolatosan?	0,122	0,827	0,083	0,075
Találhatóak-e a honlapon települési/önkormányzati stratégiákra vonatkozó dokumentumok?	0,110	0,574	0,359	0,012
Találhatóak-e a honlapon települési/önkormányzati programokra vonatkozó dokumentumok?	-0,032	0,121	0,772	0,124
A honlap utolsó frissítésének dátuma	-0,189	-0,096	-0,687	-0,151
Van-e információ, adatbázis az önkormányzat által fenntartott vagy működtetett intézményekről?	0,357	0,136	0,579	-0,022
Rendelkezik-e a weboldal a lakosság számára fontos és használható adatbázissal	0,388	0,376	0,415	0,061
Van-e hivatkozás/link a település FB oldalára?	0,048	0,093	0,083	0,886

Integrált-e a honlapba a FB?	0,063	0,055	0,126	0,882

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.[a]
a. Rotation converged in 5 iterations.

Forrás: saját szerkesztés.

7. melléklet – Közbiztonsági referens felkészítése

A katasztrófák elleni védekezés egyes szabályairól szóló 62/2011. (XII. 29.) BM rendelet meghatározza a polgári védelmi felkészítés követelményeit és a felkészítendő célcsoportokat.

A polgári védelmi szervezetek és az önkéntes mentőszervezetek katasztrófavédelmi felkészítésének célja a természeti, a civilizációs és egyéb eredetű katasztrófák, veszélyhelyzetek megelőzésére, elhárítására és a helyreállítás során jelentkező, – a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvényben meghatározott – feladatok végrehajtására való felkészülés, továbbá a károsító események bekövetkezése esetén a következmények lehető legkisebbre történő csökkentése.

Magyarország településeinek kockázatértékelésen alapuló katasztrófavédelmi osztályba sorolása megtörtént. A településeken megalakításra kerültek a települési polgári védelmi szervezetek, valamint elkészültek a települések katasztrófavédelmi osztályba sorolásának megfelelő települési veszélyelhárítási tervek.

A polgári védelmi szervezeteket és az önkéntes mentőszervezeteket úgy kell felkészíteni, hogy képesek legyenek az azonosított veszélyeztető hatások és a települések katasztrófavédelmi osztályba sorolása alapján kidolgozott veszélyelhárítási tervekben megfogalmazott események következményeinek a kezelésére.

A katasztrófavédelmi felkészítést a megyei (fővárosi) katasztrófavédelmi igazgatóság, a katasztrófavédelmi kirendeltségek és a hivatásos tűzoltóparancsnokságok állománya végzi. Az egyes gyakorlatok végrehajtása során bevonásra kerülhetnek a speciális szaktudással rendelkező állami és civil szervezetek, így különösen a karitatív szervezetek, a vízügyi igazgatóságok, a mentőszolgálatok, a polgárőrség, a Magyar Honvédség, a megyei (fővárosi) polgári védelmi szövetségek, valamint a megyei (fővárosi) tűzoltó szövetségek.

FELADATOK

Felkészítés előkészítése és végrehajtása során jelentkező feladatok:

A megalakítási terv és a technikai állománytábla pontosítása.	Felelős: kirendeltségvezető Határidő: felkészítés előtt 30 nappal
Érintettek értesítése a felkészítésről.	Felelős: kirendeltségvezető Határidő: felkészítés előtt 8 nappal
A felkészítéshez tartozó foglakozási jegy elkészítése.	Felelős: kirendeltségvezető Határidő: felkészítés előtt 10 nappal

Felkészítés helyének biztosítása.	Felelős: kirendeltségvezető Határidő: felkészítés előtt 8 nappal
Felkészítés során felhasznált anyag, felszerelés, ellátás biztosítása.	Felelős: kirendeltségvezető Határidő: felkészítés napján
Oktatási napló, munkavédelmi napló, jelenléti ív előkészítése, vezetése.	Felelős: a felkészítés vezetője Határidő: felkészítés előtt 5 nappal, illetve a felkészítés napján
Gyakorlat esetén az érintett lakosság tájékoztatása a gyakorlatról.	Felelős: kirendeltségvezető Határidő: felkészítés előtt 8 nappal
Gyakorlat esetén levezetési terv elkészítése és felterjesztése a katasztrófavédelmi igazgatóságra.	Felelős: kirendeltségvezető Határidő: felkészítés előtt 15 nappal

1. függelék a/2017. (…) BM OKF utasítás mellékletéhez

TEMATIKA

INFOKOMMUNIKÁCIÓS SZAKFELADATOT ELLÁTÓ ÁLLOMÁNY FELKÉSZÍTÉSÉRE

Téma	**óra**	**Szükséges eszközök**
Elmélet: riasztási-tájékoztatási feladatok, riasztási jelzések, riasztás, tájékoztatás módszerei, eszközei, a riasztó eszközök működtetése, függelmi viszonyok, irányítás, jelentés és az együttműködés rendje, a mozgósítás szabályai.	2	mozgósítási terv, laptop, projektor
Gyakorlat: riasztó eszközök működtetése, riasztási jelzések leadása.	1	riasztó eszközök

A felkészítést úgy kell végrehajtani, hogy a szakfeladatokat ellátók alkalmasak legyenek az alábbi feladatok végrehajtására:

- a lakosság helyi riasztása és tájékoztatása,
- a polgári védelmi szervezetek állományának riasztása,
- a riasztásra szolgáló technikai eszközök és berendezések működtetése,

- a hivatásos katasztrófavédelmi szervek, a polgári védelmi szervezetek, az irányító és együttműködő szervek, szervezetek közötti kommunikáció biztosítása,
- az informatikai és kommunikációs eszközök üzemeltetése, a vezetés infokommunikációs feltételeinek biztosítása,
- a katasztrófaelhárítási feladatok során igénybe vett kormányzati célú hálózatok üzemeltetőjével való kapcsolattartás.

Függelék

1. függelék - kiberkoordináció kibővítése – az önkormányzatok bevonása

- Szabályozási környezet felülvizsgálata (2013. évi L. törvény és 484/2013. (XII. 17.) Korm. rendelet)
    - Nemzeti Kiberbiztonsági Koordinációs Tanács tagjainak bővítése az önkormányzatokért felelős miniszterrel
    - Önkormányzati kiberbiztonsági munkacsoport létrehozása

- A központi kormányzati szervezetek és az önkormányzatok közötti operatív koordinációs működés megvalósítása – operatív munkaszervezet létrehozása.

Célja és feladata:

- szereplők közötti horizontális és vertikális információáramlás biztosítása;
- az aktuális helyzet feltérképezése, a felmerülő problémák, nehézségek összegyűjtése, becsatornázása a Tanács felé;
- az önkormányzatokat érintő szabályozás véleményezése, javaslattétel;
- közreműködés önkormányzati ellenőrző listák, útmutatók, módszertanok kidolgozásában és disszeminálásában;
- az önkormányzati tudatosság rendszeres felmérése és a tudatosító akciók, rendezvények, versenyek szervezése;
- együttműködés önkormányzati érdekképviseleti szervezetekkel az információbiztonság témakörében;
- önkormányzati jó gyakorlatok gyűjtése és terjesztése;
- önkormányzati információbiztonságban érintett szervezetek információmegosztási és partnertségi platformjának létrehozása és operatív munkaszervezeti feladatainak ellátása.

2. függelék – Javaslat önkormányzati képzési és tudatosítási rendszer átalakítására

	Felelős vezető	IB felelős[21]	IB résztvevők
Alap tanfolyamok (NKE)	Továbbképzés és éves továbbképzés (a tananyag éves felülvizsgálata szükséges)	Az Ibtv. elvárt minősítés vagy NKE EIB vezető képzés	Továbbképzés és éves továbbképzés (a tananyag éves felülvizsgálata szükséges)
Vezetői tanfolyamok BM OKF (polgárivédelmi felkészítések mintájára, kötelező részvétel)	Információbiztonsági és kibervédelmi felkészítés vezetők részére. (gyakorlatorientált, támaszkodva a nemzetközi és hazai tapasztalatokra). Minimum 4 óra, évi gyakoriséggal.	Információbiztonsági és kibervédelmi felkészítés IB felelősök részére (esettanulmányok feldolgozása, szimulációk lefolytatása). Minimum évi kétszeri gyakoriséggal, alkalmanként 4 óra.	
Munkatársi: IB felelős			Rendszeresen (3 havonta, 2 óra): A szak-, levelező és online rendszerek kezeléséhez, az információbiztonság érdekében. Esetileg: Új szabályozás, új rendszer vagy incidens esetén.
Felelős: OKF érintett szakmai és területi szervezetei Bevont: Kibervédelmi Koordináció (KK)	Megyei önkormányzati kibervédelmi gyakorlat. Évente. Rendelhető hozzá verseny, díjak, elismerés a hivatalok és munkatársak részére a motiváció növelése érekében.		

[21] IB felelőst több önkormányzat is alkalmazhat közösen.

	Felelős vezető	IB felelős[21]	IB résztvevők
szervezetei együttműködő kibervédelmi szervezetek és KK munkacsoportjai			
Információs, partnerségi platform KK – operatív önkormányzati kiberkoordinációs szervezet	Információ és tapasztalatcsere. Szabályozás trendek megismerése, megvitatása.	Események, incidensek, trendek, megoldások. Tudás, tapasztalat, jó gyakorlatok megosztása.	
KK – operatív önkormányzati kiberkoordinációs szervezet Önkormányzati szövetségek	Tudatosító programok: Önkormányzati elismerés a jó gyakorlatot megvalósító önkormányzatok számára.	Fejlesztő programok: Nemzetközi és hazai események, incidensek és megoldásaik megosztása.	Tudatosítás, támogatás: Egyszerű útmutatók, könnyen kezelhető kiadványok, e-learninges tananyagok. pl.: Tippek, trükkök a zsarolóvírusok felismerésére
KK és partnerszervezetek	Tudásmegosztó portál létrehozása és üzemeltetése.		

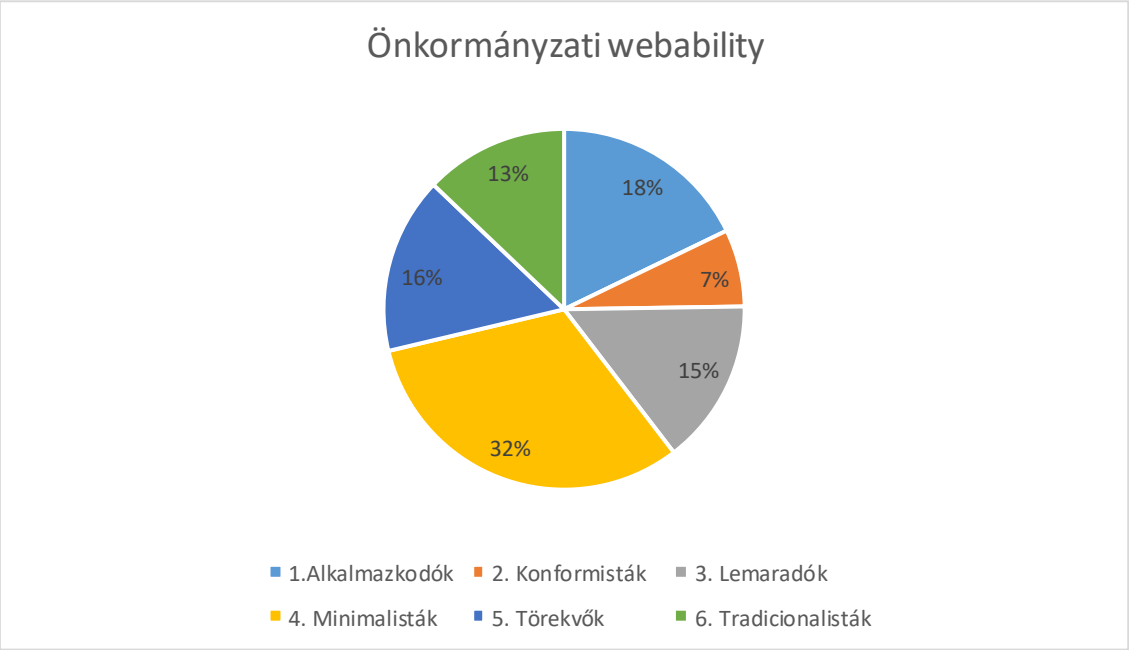
Forrás: saját szerkesztés.

3. függelék – Önkormányzatok online képessége szerinti csoportok

A kialakult csoportok online képessége vizsgálatra került az osztályozó változók mentén (felhasználóbarát, informativitás, használhatóság és közösségi kapcsolódás), illetve az egyes csoportok online megjelenését mi jellemzi lakosságszámuktól, adóerő-képességüktől, hivatali struktúrájuktól és jogállásuktól függően.

Az önkormányzatok online képessége szerint az alábbi klaszterek jöttek létre:

- 1. klaszter – Alkalmazkodó
- 2. klaszter – Konformista
- 3. klaszter – Lemaradó
- 4. klaszter – Minimalista
- 5. klaszter – Törekvő
- 6. klaszter – Tradicionalista



Önkormányzatok online képesség szerinti megoszlása

Forrás: saját szerkesztés.

A klaszterek tagjait az osztályozó változók szerint – átlagosan – az alábbiak jellemzik:

- **1. klaszter – Alkalmazkodó**

Ebbe a településcsoportba tartozó települések átlagos lakosságszáma közel 3000 fő és átlagos adóerő-képesség szempontjából inkább alsó harmadba tartoznak. A településeket alacsony adóerő-képesség mellett, a közösségi helyeken keresztüli kommunikáció jellemzi. Vélelmezhetően a weboldaluk fejlesztésére nem fordítanak nagy hangsúlyt, inkább a közösségi médián keresztül szólítják meg a lakosaikat. Ennek lehet oka, hogy költséghatékonyabbnak tartják vagy egy lelkes munkatárs. Ez a megoldás jól alkalmazkodik az ügyfélelvárások változásához is e településszerkezet esetében. A magyar önkormányzatok 18%-a tartozik ebbe a körbe.

- **2. klaszter – Konformista**

Ebbe a településcsoportba tartozó települések átlagos lakosságszáma és adóerő-képessége a legmagasabb (közel 20 000 fő és átlagosan 23 000 Ft az adóerő-képesség). Ez alapján ebbe a csoportba tartoznak a nagyvárosok és a fővárosi kerületek. A csoportba tartozó települések negyede közöshivatal tag, 30%-a közös hivatal székhelye és 45% önálló hivatalt tart fenn.

A fentiek alapján az ebbe a csoportba tartozó településeket magas adóerő-képesség mellett, a weboldal és a közösségi helyek hatékony kihasználása jellemzi annak érdekében, hogy a nagylétszámú lakosságot minél jobban, széleskörűbben, hatékonyabban tájékoztassák. Cél az ügyfélelvárásoknak való megfelelés.

- **3. klaszter – Lemaradók**

A harmadik klaszterbe tartozó településeket negatív online képesség jellemzi, vagy a webability átlagos hiánya. Ebbe a településcsoportba tartozó települések átlagos lakosságszáma 1000 fő alatti, bár adóerő-képessége szerint inkább a felső harmadba tartoznak. A csoportba tartozó települések

80%-a közöshivatal tag, 15%-a közös hivatal székhelye és 5%-a önálló hivatalt tart fenn. Jogállás szerint a városok száma ebben a csoportban elenyésző.

A fentiek alapján az ebbe a csoportba tartozó településeket magas adóerő-képesség mellett, nem fordítanak energiát az online képességük fejlesztésére és a közösségi webhelyeket sem használják. Ennek oka lehet az alacsony lakosságszám, a városi jogállású települések hiánya, vagy az, hogy online kommunikációjukat elsősorban a székhely online tájékoztatása fedi le.

A csoport érdekessége, hogy átlagosan magas adóerő-képesség jellemzi az idetartozó településeket, azonban a számok szerint nem motiváltak az érintettek az online képességük növelésében, tehát az anyagi képesség nem magyarázza a webability meglétét vagy annak hiányát.

- **4. klaszter – Minimalisták**

Ebbe a településcsoportba tartozó települések átlagos lakosságszáma kissé meghaladja az 1800 főt és adóerő-képesség szempontjából az alsó harmadba tartoznak. A csoportba tartozó települések 55%-a közöshivatal tag, 29%-a közös hivatal székhelye és 16%-a önálló hivatalt tart fenn. Jogállás szerint a csoport tagjainak kevesebb, mint 10%-a város.

Az elemzés azt mutatja, hogy az ebbe a csoportba tartozó településeket igyekeznek kihasználni a web adta költséghatékony lehetőségeket a tájékoztatatásban, azonban az alacsony adóerő-képesség mellet nem fordítanak az online megoldások felhasználóbarát és informatív jellegére. A közösségi kapcsolatok használata nem jellemzik ezt az önkormányzati csoportot.

- **5. klaszter – Törekvők**

Ebbe a településcsoportba tartozó települések átlagos lakosságszáma 1000 fő alatti, adóerő-képesség szempontjából az alsó harmadba tartoznak. A csoportba tartozó települések 78%-a közöshivatal tag, 19%-a közös hivatal székhelye és 3%-a önálló hivatalt tart fenn.

A fentiek alapján az ebbe a csoportba tartozó települések igyekeznek kiszolgálni az állampolgárokat egy user friendly honlappal, azonban az alacsony adóerő-képesség mellett nem fordítanak az online megoldások használhatóságára és informatív jellegére. A közösségi kapcsolatok használata nem jellemzik ezt a csoportot, amit az aprófalvas jelleg mellett a városi települések minimális jelenléte magyarázhat.

- **6. klaszter – Tradicionalisták**

Ebbe a településcsoportba tartozó települések átlagos lakosságszáma meghaladja az átlagos 5000 főt, adóerő-képesség szempontjából a középső alsó harmadba tartoznak. A csoportba tartozó települések között kiegyensúlyozottabban oszlanak meg a hivatal típusok. 40%-a közös hivatal tag, 28%-a közös hivatal székhelye és 32%-a önálló hivatalt tart fenn. Jogállás szerint a csoport negyede város.

A fentiek alapján az ebbe a csoportba tartozó településeket átlagosan jó, az informativitás szempontjából pedig kiemelkedő online képességekkel rendelkeznek. Az elemzés szerint törekszenek az online tér adta lehetőségek kihasználására, az állampolgári bizalom erősítésére, azonban a hagyományos web eszközökkel, a közösségi kapcsolatok használata nem jellemzik ezt a csoportot.

Az elemzés alapján látható, hogy a webability a magyar önkormányzatok jelentős részének nem tartozik az erősségei közé, azonban alakulása összefüggést mutat a lakosságszámmal, a hivatal típusával és a település státuszával. Érdekes éredmény, hogy a magasabb adóerő-képesség nincs közvetlen összefüggésben az online képesség változásával.

4. függelék – Információbiztonsági ellenőrző lista az önkormányzati információbiztonság biztosításában résztvevő munkatársak részére

Az ellenőrző lista egyszerű segítséget nyújt az érintettek számára abban, hogy milyen tevékenységeket, milyen gyakran szükséges elvégezni.

Naponta végzendő tevékenységek:

- vírusirtó programok frissítése;
- kémprogramkereső és -eltávolító programok frissítése;
- szoftverfrissítések letöltése;
- az adatok biztonsági mentése.

A napi frissítések automatizálása ahol lehetséges.

Figyelmeztetés, tájékoztatás és tanácsok a munkatársak felé az esetleges incidensekről, eseményekről és arról, hogy mire figyeljenek.

Hetente végzendő tevékenységek:

- teljes körű biztonsági mentés és tárolása történjen külön helységben.

Évente (minimum) végzendő tevékenységek:

- éves biztonsági felülvizsgálat;
- a hardverek és szoftverek éves felülvizsgálata;
- információs eszközök/alkalmazások vizsgálata;
- tudatosító képzések, gyakorlatok a munkatársak számára belépéskor és rendszeresen évente;
- munkatársak tájékoztatása a használható eszközökről és alkalmazásokról belépéskor és utána évente;
- az elfogadott szabályozás rendszeres frissítése és felülvizsgálata évente;
- hozzáférések rendszeres felülvizsgálata.

Alkalomszerűen/szükség szerint:

- új partnerekkel biztonsági elvárások közlése;
- incidens esetén házirend felülvizsgálata, monitoring rendszer felülvizsgálata.

Köszönetnyilvánítás

Számtalan mindenkinek tartozom köszönettel, akitől sok féle módon kaptam támogatást és segítséget. Nélkülük nem jutottam volna idáig, nem készítettem volna el az értekezésem.

Mindenek előtt köszönettel tartozom azoknak a barátaimnak és munkatársaimnak, akik biztattak, hogy induljak el ezen az úton. Köszönettel tartozom Farkasné Dr. Gasparics Emesének aki közvetlen felettesemként támogatta tudományos ambícióimat.

Tisztelettel tartozom - előző iskolámnak -, a Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskolájának, hogy a segítettek és támogattak a képzési folyamatomban, hogy gyakorlatias kompetenciáim kiegészüljenek elméleti, módszertani tudással. Hálás vagyok Tózsa Professzornak, hogy támogatásával átsegített a megterhelőnek, nehéznek megélt időszakokon, Bukovics Professzornak, hogy alapos módszertani megközelítését megkísérelte átadni nekem.

Hálával tartozom Berek Professzor úrnak, hogy nem sajnálta az idejét, hogy segítsen eligazodnom a biztonságtudomány területén és hogy ellásson tanácsokkal értekezésem teljessége érdekében.

Az értekezés empirikus kutatási tevékenységének lefolytatásához témavezetőm szakmai segítségén túl támogatást kaptam a munkahelyemtől, mivel lehetővé tették az önkormányzatok horizontális weblapértékelésének keretében felvett adatok használatát a dolgozatomhoz.

Folyamatosan pozitív visszajelzéseket és segítséget kaptam önkormányzati vezetőktől. Köszönettel tartozom a Települési Önkormányzatok Országos Szövetségének és személy szerint Dr. Gyergyák Ferenc főtitkár úrnak a fókuszcsoportos interjú megszervezésében nyújtott segítségéért.

Kiemelt köszönettel tartozom témavezetőmnek, Professzor Dr. Rajnai Zoltánnak, aki már évek óta segíti szakmai tanácsaival a munkámat. Témavezetőként a kutató munkám és a doktori értekezés készítése során mindig rendelkezésemre állt a felmerülő kérdések megvitatására, figyelemmel kísérte a kutatási tevékenységemet és ellátott tanácsaival, átsegített a nehézségeken. Nélküle ez a dolgozat nem készülhetett volna el.

Ezen az úton szinte mindenkitől csak biztatást, támogatást kaptam. Ezúton is köszönöm mindazoknak is a segítséget, akiket a számosság okán nem állt módomban név szerint felsorolni, de hálatelt szívvel gondolok rájuk. Végül köszönöm a biztatást és támogatás a családomnak!

A dolgozatom kutatásaihoz az Új Széchenyi Terv keretein belül az **EFOP-3.6.1-16-2016-00010** számú projekt biztosított forrást.

A kutatás az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósult meg, mely támogatáshoz ezúton szeretnék köszönetet mondani.

A tézispontokhoz kapcsolódó tudományos közlemények jegyzéke

1. Számadó Róza

Önkormányzatok helye a kormányzati kiberkoordinációban

JEGYZŐ ÉS KÖZIGAZGATÁS XX:(2) p.27. 29 p. (2018)

2. Számadó Róza

Önkormányzatok kiberbiztonsági helyzete a nemzetközi és hazai tapasztalatok tükrében

ÚJ MAGYAR KÖZIGAZGATÁS 11:(2) p. 1. 5 p. (2018)

3. Számadó Róza

Analysing online capabilities of local governments

ACTA TECHNICA CORVINIENSIS – BULLETIN OF ENGINEERING 2018:(3) p. 1. 12 p. (2018)

4. Számadó Róza

ÖNKORMÁNYZATOK MEGFELELÉSI KÉPESSÉGE A KIBERBIZTONSÁGI KIHÍVÁSOKNAK: Online felmérés eredményei

ÚJ MAGYAR KÖZIGAZGATÁS 2018:(3) pp. 1-12. (2018)

5. Számadó Róza

Impact of Leaders: The Impact of the Engagement of Local Government Leaders' on the Effectiveness of Participatory Planning as Found in the Local Community Academy Program1 (2014–2015)

ACADEMIC AND APPLIED RESEARCH IN MILITARY AND PUBLIC MANAGEMENT SCIENCE 16:(1) pp. 63-76. (2017)

További tudományos közlemények

6. Számadó Róza

Inkluzív önkormányzat építés

Az Önkormányzati szaktanácsadó szakirányú továbbképzési szak Inkluzív önkormányzat és fejlesztéspolitika I. c. tantárgyának egyetemi tankönyve

Budapest: Dialóg Campus Kiadó, 2018. 97 p. (ISBN:978-615-5889-06-6)

7. Számadó Róza (szerk.)

Inkluzív önkormányzat tervezés: Önkormányzati szaktanácsadó szakirányú továbbképzési szak Inkluzív önkormányzat és fejlesztéspolitika II. c. tantárgyának egyetemi tankönyve

Budapest: Dialóg Campus Kiadó, 2018. 126 p.

(ISBN:978-615-5889-04-2)

8. Belényesi Emese , Számadó Róza

Önkormányzatok tervezési gyakorlata – tervek és a valóság.

ÚJ MAGYAR KÖZIGAZGATÁS 3:(3) pp. 28-40. (2015)

9. Farkasné Gasparics Emese , Számadó Róza

A településmenedzsment átalakulása a működési keretek tükrében

POLGÁRI SZEMLE: GAZDASÁGI ÉS TÁRSADALMI FOLYÓIRAT 11:(1--3) pp. 1-15. (2015)

10. Holcreiter Marianna , Számadó Róza , Szilágyi Ildikó , Treszkán Hováth Viktória

Pályázatmenedzsment

Budapest: Nemzeti Közszolgálati Egyetem, 2015. 149 p.

(ISBN:978-615-5057-41-0)

11. Számadó Róza , Gáspár Mátyás , Göndör András , Belényesi Emese , Brecsok Anna , Jenei Ágnes , Dömötör Ildikó

Csóka Gabriella (szerk.)

Fejlesztő közösségek: A helyi közösségi akadémiák hálózata

Budapest: Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet, 2015. 62 p.

12. Számadó Róza

Inkluzív önkormányzat

Budapest: Nemzeti Közszolgálati Egyetem, 2015. 130 p.

(ISBN:ISBN 978 615 5057 35 9)

13. Számadó Róza (szerk.)

Módszertani kézikönyv: Szociális szövetkezetek az alakulástól a fenntartható működésig

Budapest: Országos Foglalkoztatási Közalapítvány (OFA), 2011.