Számadó Róza
doktorandusz
Óbudai Egyetem Biztonságtudományi Doktori Iskola

Önkormányzatok megfelelési képessége a kiberbiztonsági kihívásoknak – védekezőképesség

A tanulmány fókuszában a helyi önkormányzatok kiberbiztonsági képességének a vizsgálata áll az emberi tényező jelenőségének fokozott figyelembevételével.

A kérdések, amelyekre választ kerestem: Felkészültek-e az önkormányzatok a kibertérből érkező kihívásokra? Milyen fenyegetettséggel nézhetnek szembe? Tudatában vannak-e a fenyegetettség hatásainak? Rendelkeznek-e a szükséges eszközökkel, felkészült emberi erőforrással?

Elméleti kutatásaim, a nemzetközi és hazai tapasztalatok 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. Feltételezésem 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.

A felkészültség, az információbiztonsági kultúra kialakítása kiemelt figyelmet kapott az elmúlt húsz évben, különös tekintettel arra, hogy a különböző incidensek legnagyobb része a csekély felkészültség és információbiztonsági tudatosság hiányából következett be. Az emberi tényező fejlesztése véleményem szerint 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.

Jelen tanulmány keretei nem teszik lehetővé, hogy a teljes vizsgálat bemutatásra kerüljön, így – a felmérés adatainak bemutatását követően – az önkormányzatok kiberbiztonsági helyzetének feltárását célzó online felmérésnek a fő eredményei kerülnek bemutatásra.

Online kérdőíves felmérés

A kérdőív aktualitása

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. Ahhoz, hogy megállapításokat lehessen tenni és javaslatokat megfogalmazni, elengedhetetlennek tartottam felméri az elméleti és a szabályozási keretek felhasználásával az önkormányzati vezetők és munkatársak: az önkormányzatok kiberbiztonsággal kapcsolatos attitűdjeit, felkészültségét és gyakorlatát.

A kérdőív háttere

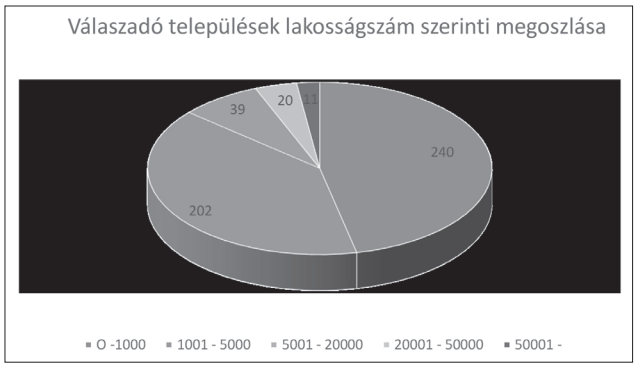
Az önkormányzatok kiberbiztonsági kérdéseinek vizsgálatához 2018. január elején – a tesztelést követően – a teljes önkormányzati kör részére elektronikus úton került kiküldésre a kérdőív (1. melléklet), amire 2018. február 13-ig 512 válasz érkezett. A kitöltés önkéntes és anonim volt. A kérdőív kérdéseinek leírása az 1. 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.

Beérkezett válaszok megoszlása

A beérkezett válaszok érékelése során vizsgáltam, hogy mi a jellemző az egyes kérdésekre adott válaszokra a települések lakosságszáma és a település hivatal típusa szerint:

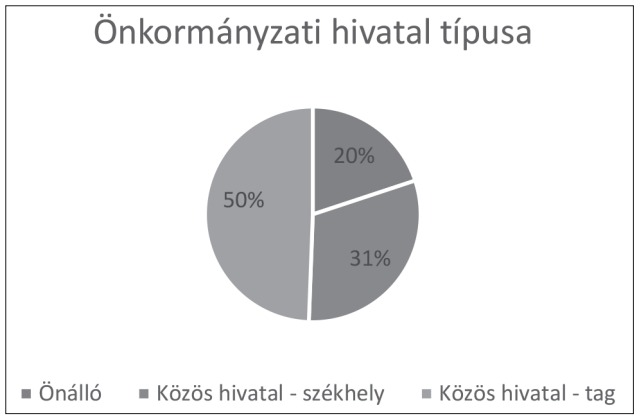
A magyar településszerkezet alapvetően aprófalvas és a diagrammból láthatjuk is, hogy a településszerkezeti arányok tükröződnek a válaszadó települések lakosságszám szerinti megoszlásában is.

1. ábra
Válaszadó települések megoszlása lakosságszám szerint



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

2. ábra
Válaszadó települések megoszlása önkormányzati hivatalok típusa szerint



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

Az önkormányzatok operatív munkaszervezete a polgármesteri hivatal. 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 13. 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.

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.

A kérdőív feldolgozásának módszerei és eredményei

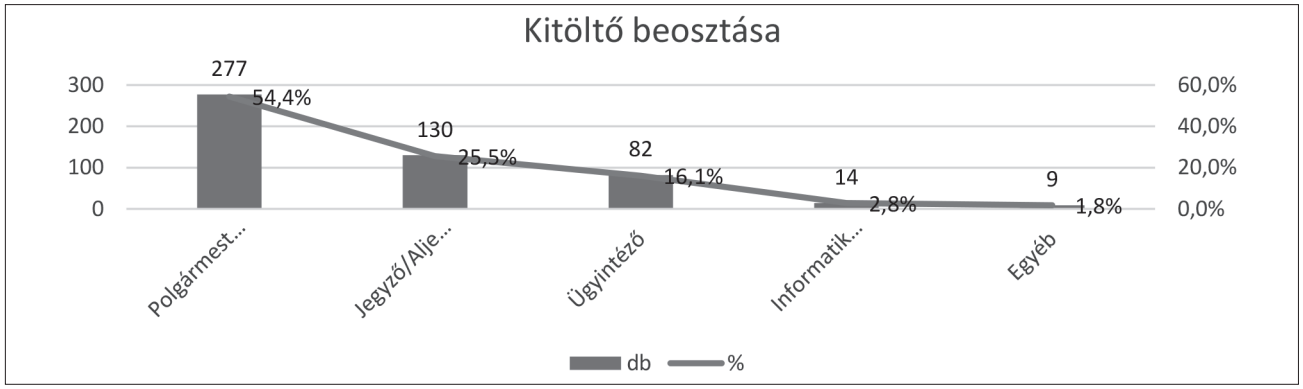
A kérdőívre adott válaszok értékelése kérdések jellegétől függően leíró statisztikai, matematikai statisztikai módszerekkel és a szöveges válaszok esetében egyszerű összegzéssel készült.

A három szakmai blokk az önkormányzati válaszadók által a kérdésekre adott véleményét, az információbiztonsággal kapcsolatos tudatosságát hivatott felmérni.

Az első szakmai blokk a kibertérrel, kiberbiztonsággal kapcsolatos vélemények összegyűjtését célozta. Ebből a blokkból a tanulmány szempontjából releváns,hogy a felkészülés során milyen beavatkozásokat preferálnak.

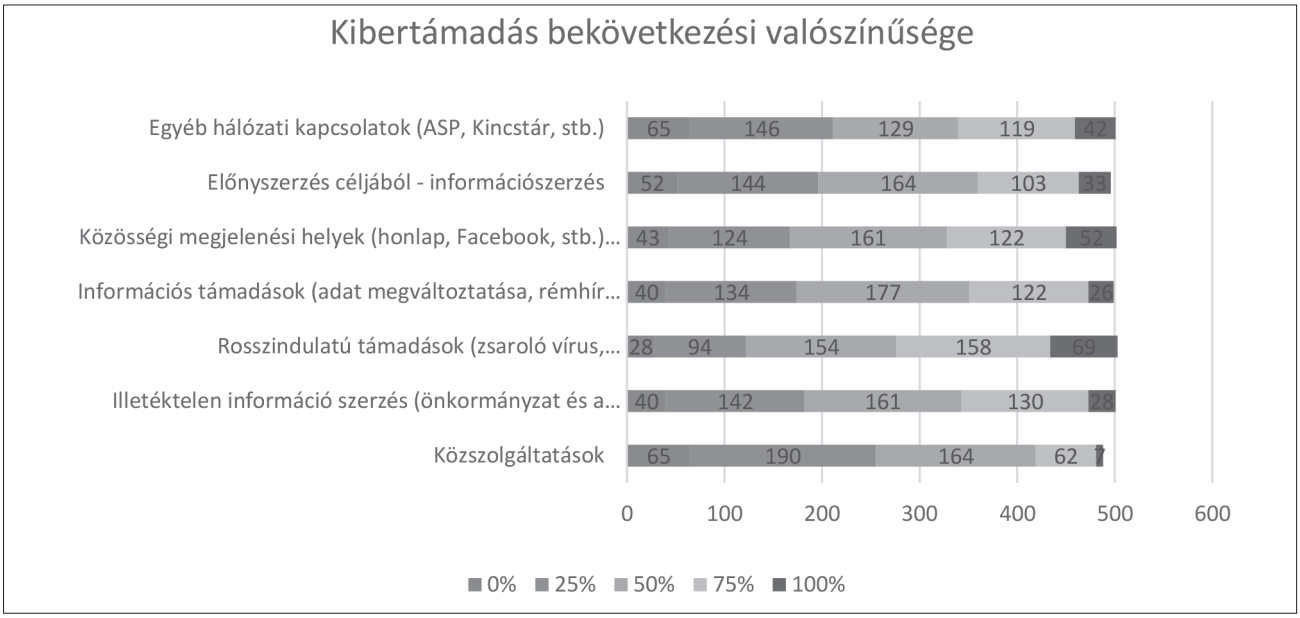
A második szakmai blokk az önkormányzatok felkészültségéről, kiberbiztonsági kompetenciájáról alkotott vélemények feltárását tűzte ki célul. Ennek keretében arról kértem a válaszadókat nyilatkozni, hogy véleményük szerint a különböző kiberbiztonsági helyzetekben mi jellemző az önkormányzatra, illetve e rész második kérdésében a meglévő információbiztonsági (védekező/reagáló) képességét, felkészültségét kértem minősíteni a szervezetnek. jelen tanulmányban a helyzetelemzésnek ezen része kerül részletesen bemutatásra.

3. ábra
Válaszadók megoszlása a szervezetben betöltött pozíciójuk szerint



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

4. ábra
Adott területen egy kibertámadás bekövetkezési valószínűsége (összefoglalás)



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

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:
– felkészültség, képesség;
– kiberfenyegetettség megítélése;
– sebezhetőség;
– védekező/reagáló képesség;
– szabályozás rendelkezésre állása.

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

Az egyes komponenseket a szakmai kérdésblokkonon belül tárgyaltam.

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, rendsze-

rek biztonsága, közbiztonság) sebezhetőségével kapcsolatosan 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, alig van, vagy 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 3.-hoz. itt 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 menynyire 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%.

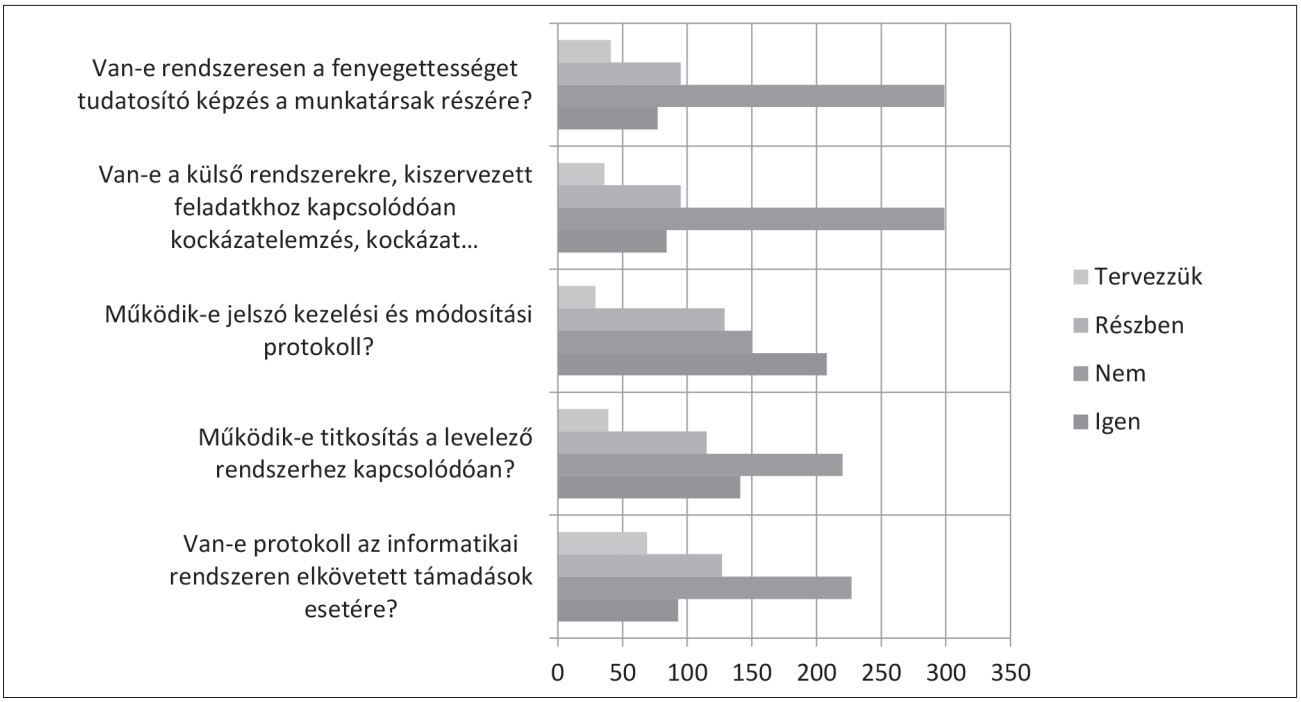
A válaszadók szerint kibertámadás esetére van helyreállítási terve az önálló hivatalok több mint 40%-nak, és nincs vagy alig a taghivatalok több mint 40%-nak.

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 kiberbiztonsági védekező és reagáló képesség főkomponensbe a kötelezettségeket és lehetőségeket összefoglaló kérdések közül a 3.-7. kérdéseket és az informatikai rendszerek

5. ábra
Adott területek védekező/reagáló képessége (összefoglalás)



elleni támadás és a működési tapasztalatok köréből a támadások esetére kialakított protokollokat, védelmi mechnizmusok kérdések eredményeit sorolta a főkomponens analízis.

A kötelezettsége, lehetőségek kérdésblokkon belül az került felmérésre, hogy milyen védekező, reagáló képességgel rendelkeznek az önkormányzatok egy esetlegesen bekövetkező vagy bekövetkezett támadás esetén. A legjobb eredményt – ami önmagában sem mutat túl rózsás képet – a jelszó kezelése és módosítása protokoll megléte kérdésre érkezett.

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.

Ezzel együtt a meglévő eredmények azt mutatják, hogy az önkormányzatok védekező és reagáló képessége nagyon alacsony. A válaszadó önkormányzatok mintegy negyedénél van protokoll csak kialakítva egy esetleges kibertámadás esetére, a levelezőrendszer az önálló hivatalok esetében mintegy 37%-ánál és többi önkormányzatnál pedig csak negyedénél titkosított, jelszókezelési és módosítási eljárásrend is kevesebb mint a válaszadók 50%-a esetében van. 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 is kevés pozitív válasz érkezett a munkatársak tudatosító képzésére. A hivatalok 18,8%(önálló hivatalokkal rendelkező önkormányzatok) és 12,7% (közös hivatalhoz tartozó önkormányzat) válaszadói nyilatkozták és a közös hivatal székhely önkormányzatai esetében is csak a válaszadók 15,6%-a nyilatkozta, hogy van náluk ilyen felkészítés. A működés során bekövetkezett támadás esetére pedig csak a válaszadók 10%-ának van eljárásrendje.

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 tapaszaltak. 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 a 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 és 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 hivatalok 46,5%-ban szabadon használhatóak, és 50% esetében pedig engedélyhez kötöttek. A közösségi felületekkel kapcsolatosan – nem volt kötelező kitölteni – csak 218 válasz érkezett, és jelentősen keverednek ezek is a magánhasználat során szerzett tapasztalatokkal. Ezek használata kevés helyen tiltott.

A felmérések eredményei azt mutatják, hogy az önkormányzatok jelentős része nem felkészült egy esetlegesen bekövetkező kibertámadásra. De nem csak nem felkészült, de nem is fektet jelentős hangsúlyt a resiliencia, az ellenálló képesség növelésére. Ez nem meglepő annak tükrében, hogy a kiberfenyegetettséggel kapcsolatos tudatosság, a fenyegetettség mértékének megítélése igen alacsony. Az eredmények alapján az önkormányzati rendszerek sérülékenyek és kiemelkedően sebezhetőek. Nem mutat biztatóbb képet a védekező és reagálóképességet vizsgáló kérdésekre adott válaszok elemzése sem. A főkomponens elemzés azonban arra is rámutatott, hogy mind a sebezhetőség, mint a védekező/reagáló képesség esetében szükséges további vizsgálatok lefolytatása, mert a vizsgált változókkal nem mutatkozott szignifikáns összefüggés.

Összegzés

Melléklet

Online felmérés kérdései

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	–1000
	1001–5000
	2001–5000
	5001–20 000
	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 valószínűségét?
- 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, kockázat menedzsment 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