# Dr. Számadó Róza:
# Önkormányzatok IT biztonságának kérdései

## Összefoglaló

Óbudai Egyetem Biztonságtudományi Doktori Iskolája a Belügyminisztárium közreműködésével 2018. novemberében felmérte az önkormányzatok információbiztonsági helyzetét. A felmérés eredményei alapján jól látszik, hogy a hazai önkormányzti kör – egybehangzóan a nemzetközi felmérések eredményeivel – nincs felkészülve az információbiztonság és kiberbiztonság által támasztott kihívásokra. Ez igaz minden területre. 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.

A vizsgálat eredményei azt mutatják, hogy az önkormányzatok információbiztonsági tudatossága nagyon alacsony, ami a kiberbiztonsági trendeket, irányokat és ez a technológiai fejlődést figyelembe véve hatalmas kockázatot hordoz. A technológia gyors fejlődése folyamatosan növeli a kitettséget, lehetetlenné vált a teljes biztonság megteremtése, ezért a megelőzésre és az ellenálló képesség növelésére kell koncentrálni, amelynek kritikus eleme az ember. Kiemelt figyelmet kell szentelni a tisztviselők, ezen belül is a vezetők felkészítésének, tudatosításának és motiválásának a támogató eszköztár széleskörű felhasználásával.

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 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 önkormányzatok esetében több kockázatot is azonosíthatunk: jelentős részük kiszervezi szolgáltatásai egy részét, többségüknél nincs jelszókezelési szabályzat, amit tovább súlyosbít a munkatársak alacsony információbiztonság-tudatossági szintje, illetve a mobil eszközök és külső eszközök használatára vonatkozó szabályozás hiánya.

## A kutatás indokoltsága

A mai modern, technológiaorientált társadalmunkban elkerülhetetlen, hogy kapcsolatba kerüljünk a kibertérrel. Az emberek mindennapi tevékenységük, munkájuk során szinte folyamatosan valamilyen információtechnológiai eszközt használnak. Manapság teljesen természetes, hogy internetet, számítógépet, okos telefonokat használunk és ezen túlmenően a információtechnológia már beférkőzhet akár lakásunkba is (Amazon Alexa, Google Home, okos otthonok). A folyamatos és dinamikus fejlődés immáron elkerülhetetlen és szembesülnünk kell ennek minden pozitív és negatív hatásával.

Az IKT[1] 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.

A szakértői elemzések mind azt jelzik, hogy az önkormányzatok információellátása, online jelenléte nagyfokú veszélynek van kitéve, ezek sérthetetlenségének biztosítása egyre nagyobb kihívást jelent.

Az önkormányzati kiberbiztonság kialakításakor számolni kell az alábbi tényezőkkel: az önkormányzatok önálló döntési hatáskörrel rendelkeznek a helyi közügyekben és a helyi szolgáltatások ellátásában, ami azért praktikus, mert nekik sokkal nagyobb a rálátásuk a saját életkörülményeikre és viszonyaikra. Ezen felül nem szabad figyelmen kívül hagyni, hogy a települések között rendkívül nagyok a különbségek nem csak lakosságszámban, hanem forrásokban és lehetőségekben is. Ebből következik, hogy az ország egyes területei között kiegyensúlyozatlan a fejlődés, ami köszönhető a magyar aprófalvas településszerkezetnek és az ebből fakadó különböző lokális gazdasági háttérnek.[1] Ennek megfelelően a kibervédelmi/információbiztonsági stratégiák kialakításakor tekintettel kell lenni az önkormányzatok (települések) jellemzőire, sajátosságaira is. Ahogy az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényt sem lehet minden település és önkormányzat tekintetében egységesen meg-

[1] 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.

valósítani, így a kiberbiztonsági előírásokat és stratégiákat is „hivatalra szabottan" kell megvalósulniuk.[2]

Az önkormányzatoknak az információs társadalomban kettős (jóformán egymásnak ellentmondó) nyomásnak kell megfelelniük. Egyrészt – az állampolgárok bizalmának fenntartása, illetve a jogszabályokban foglaltaknak való megfelelés érdekében – a helyi hatóságoknak fokozott figyelmet kell fordítani a közérdekű adatok nyilvánossá tételére, másrészt a velük megosztott információk biztonságban tartására. Ez a kettősség legegyszerűbben úgy magyarázható, hogy az államnak és hivatalainak kötelessége, hogy saját működéséről nyilvánosságra hozzon minden információt, ezzel fenntartva az átláthatóságot. Ezzel szemben a magánszemélyek (lakosok) adatai személyes adatnak minősülnek *(„személyes adatnak minősül valamely magánszeméllyel (érintettel [2]) kapcsolatba hozható adat – így különösen az érintett gazdasági jellemzőire vonatkozó információ – valamint az adatból levonható, az érintettre vonatkozó következtetés"*[3] és mint olyan, pontosan az ellentéte a hivatali adatoknak, hiszen fokozott védelem alatt állnak. Ezért is különösen fontos megértenünk, hogy az önkormányzatok elleni kibertámadások mekkora veszélyeket és kockázatokat rejthetnek magukban.

A fentiek fényében jogosan merülnek fel a kérdések, hogy: Milyen feladatokat ró az Információbiztonsági törvény az önkormányzatokra? Hogyan látják el a feladataikat? Van-e az önkormányzatnak kibervédelmi protokollja? Hogy működnek az önkormányzatok védelmi mechanizmusai? Stb.

Ezekre és ehhez hasonló kérdésekre keresi a választ az Óbudai Egyetem a Biztonságtudományi Doktori Iskola hallgatói, tanárai és kutatói az *„önkormányzati rendszerek biztonságosabbá tétele érdekében"* kezdeményezett kutatásban, melynek keretében kérdőíves[2] megoldással vizsgálták, kutatták a hálózatok, az azokon dolgozó személyzet biztonságát és biztonságtudatosságát, illetve az online jelenlétet.

Ennek a kutatásnak a jelentősége, hogy segíthet felszínre hozni azokat a problémákat, sérülékeny pontokat és a biztonságtudatos munkavégzéssel kapcsolatos gondokat, amelyekkel az önkormányzatoknak szembe kell néznie a hálózatok védelme, a személyi állomány oktatása, képzése és felkészítése területén.

[2] A kérdőív a tanulmány 1. melléklete.

## Vizsgálati keretek

### Információbiztonságról, kiberbiztonságról röviden

Jelen korunk információs kihívásokkal van tele, és nem kérdéses, hogy visszavonhatatlanul a digitalizáció korába léptünk. Az emberek, a szervezetek 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.

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.

A cél az információbiztonság megfelelő szintjének elérése, ahol az érintettek tisztában vannak a veszélyekkel és a biztonság érdekében megismerik, alkalmazzák és követik a biztonság érdekében szükséges szabályokat, eljárásrendeket.

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.

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.

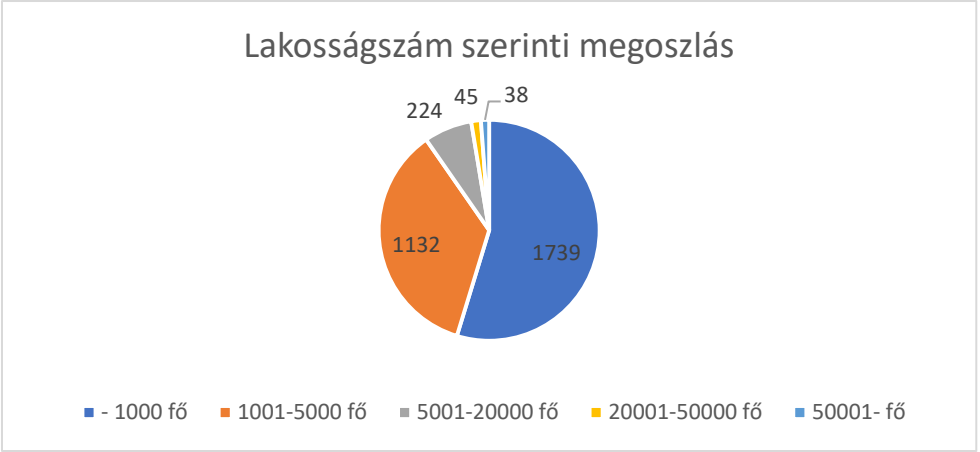
Az Európai Bizottság három cselekvési területet határozott meg a kiberbiztosnság érdekében: reziliencia erősítése és kiberbiztonsági kapacitások növelése, hatékony bűnügyi válaszadás, fokozott nemzetközi koordináció és együttműködés. Az ENISA a 2017-es jelentésében tételesen felsorolta a kiberfenyegetési 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.

## A vizsgált magyar önkormányzati szektor adatai, jellemzői

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.




1. 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.

Az önkormányzat feladatellátást a polgármesteri hivatalok végzik. 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

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 hivatal (települési, megyei önkormányzati hivatal, főpolgármesteri hivatal) működtetésével, illetve több önkormányzat által létrehozott közös önkormányzati hivatal útján gondoskodik a hivatali teendők ellátásáról.


2. ábra

*Az önkormányzati hivatalok típus szerinti megoszlása (2016)*

*Forrás:* a BM 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 képviselő-testület(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.

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. A 2017 – 2018-as vizsgálatok szeint – ebben az időben – mind az NVSZ, mind a BM saját kutatása szerint ennek a követelménynek az önkormányzatok nem felelnek meg. A vizsgálati megállapítások szerint 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.

## Online kérdőíves felmérés

Az önkormányzati rendszer szereplői az elmúlt években a változások nyomása alatt vannak. Ennek egy eleme a kiberbiztonsági kérdések és azok kezelése az helyi kormányzati térben. Ahhoz, hogy az előzőekben feltett kérdésekre válaszolni tudjunk szükséges felméri az önkormányzati vezetők és munkatársak kiberbiztonsággal kapcsolatos attitűdjeit, felkészültségét és gyakorlatát. Az érintettek nagy számára tekintettel a vizsgálat módszeréül az online kérdőív került kiválasztásra. A vizsgálat nem terjedt ki a kormányzati szerepvállalásra.

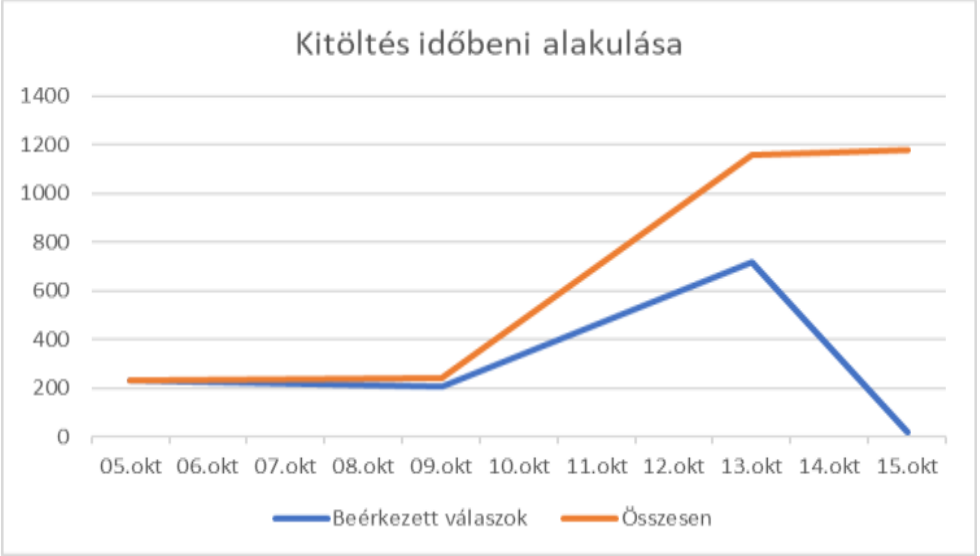
## A kérdőív felépítése

A kérdőív négy fő részből áll össze: egy adminisztratív és három tartalmi blokkra különült el. Az első blokk a kitöltőkre vonatkozó alap adatokat tartalmazza, míg a másik három az önkormányzatok kiberbiztonsági kérdéseivel foglalkozik: ki látja el az IT biztonsági feladatokat az önkormányzatnál; a megadott védekezési módok, eszközök alkalmazása és felkészültség; működési tapasztalatok. A szakmai blokkok összeállítása során az volt a cél, hogy átfogó képet kapjunk az önkormányzatok feladatellátásól a területen, a védekezési gyakorlatáról, felkészültségéről és működési gyakorlatáról a beérkezett válaszokon keresztül. A kitöltés anonimitás miatt a válaszadó települések gazdasági helyzet szerinti vizsgálatra nem került sor.

## A kérdőív felvételének tapasztalatai

A kutatáshoz tartozó első körös adatfelvétel (kérdőív) 2018. szeptember 26-án kezdődött és a Belügyminisztérium EBR42 rendszeren és az önkormányzati levelezőrendszeren keresztül lett kiküldve a polgármestereknek. A kitöltési határideje október 9. volt. Eddig az időpontig – egy emlékeztető kiküldésével – 440 önkormányzattól érkezett válasz. A 3178 önkormányzathoz viszonyítottan ez nagyon alacsony kitöltési arany volt ezért október 10.-én a BM Önkormányzati Koordinációs Irodája az ismételt email-es megkeresést indított az önkormányzati vezetőknek és velük együtt a jegyzőknek is. Ezen második körben – amelynek határideje október 13. napja volt – a kitöltők száma 736 volt, vagyis közel a kétszerese az első körös megkeresésnek, annak ellenére, hogy a kitöltésre jóformán fele annyi idő (munkanap) állt rendelkezésre.

A kitöltés üteme alapján előzetesen feltételezhető, hogy a hivatali oldal inkább érdekelt a kérdésben, mivel a jegyzők bekapcsolása a felhívásba jelentősen megnövelte a kitöltési arányt.




3. ábra
*A kitöltés időbeni alakulása*

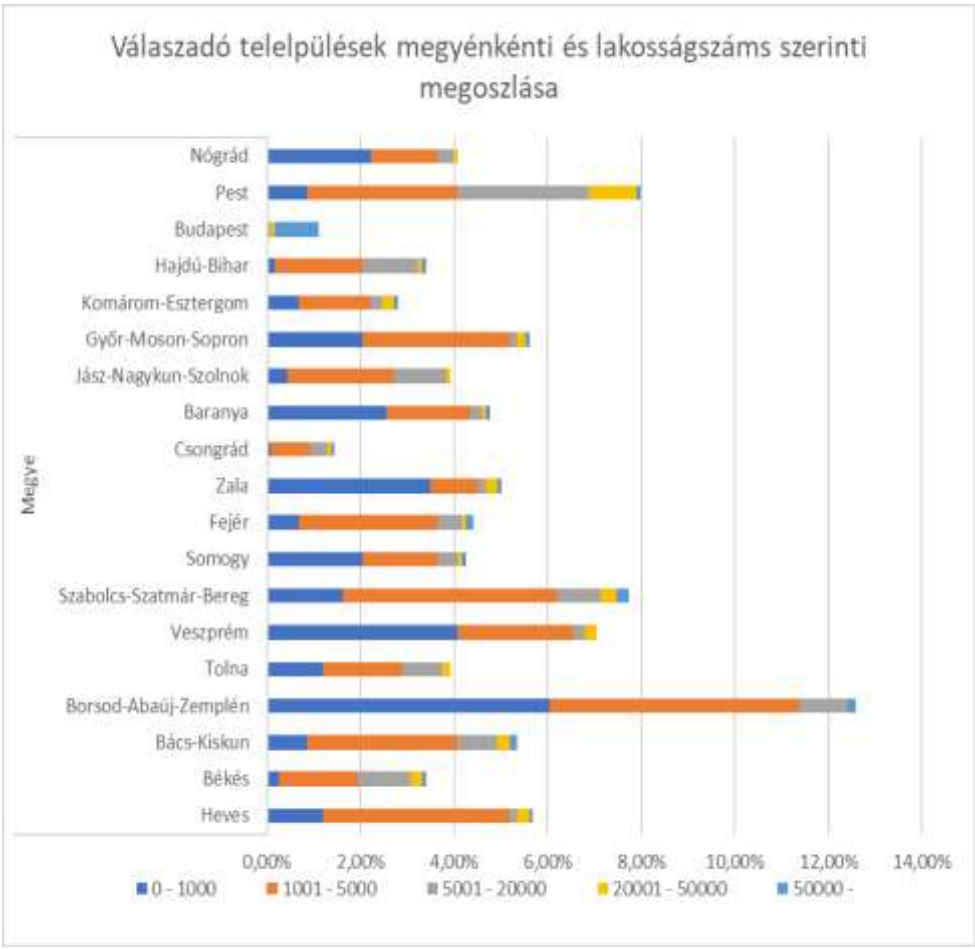
*Forrás:* saját szerkesztés.

A kérdőív október 15-én került lezárásra és összesen 1177 önkormányzat töltötte ki és küldte meg válaszait, ami a teljes településszámra vetítve 37 %.

## Kitöltők összetételének vizsgálata

Az alapadatok körében a települések földrajzi elhelyezkedésére, a lakosságszámára, a település jogállására és a hivatal típusára kérdeztünk rá. Kértük még megadni a kitöltő beosztását.

A válaszadó települések lakosságszám szerinti és földrajzi megoszlását jól szemlélteti a 4. ábra.




4. ábra

*Válaszadó települések földrajzi és lakosságszám szerinti megoszlása*

*Forrás:* saját szerkesztés.

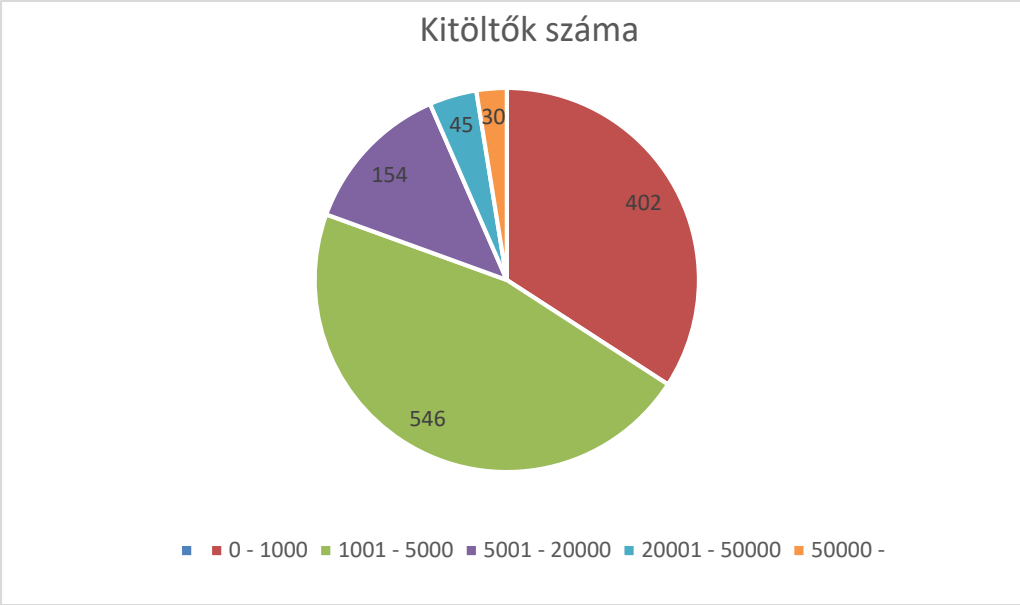
A diagramból jól látható, hogy darabszámra a legnagyobb válaszadási hajlandóság BAZ megyében volt, míg a legalacsonyabb Csongrád megyében.

Ha válaszadó települések számát az adott megye (és főváros) teljes településszámához viszonyítjuk, akkor egészen más képet kapunk. Az 1. táblázat számai azt mutatják meg, hogy az adott megye települései közül hányan tartották fontos a feltett kérdés. Ebből a szempontból vizsgálva azt mondhatjuk, hogy a kitöltési hajlandóság Jász-Nagykun-Szolnok megye települései részéről volt (59%). Érdekes adat, hogy ez a megközelítés is igen alacsony aktivitást sugall Csongrád megye esetében a 28%-os arányával.

**1. táblázat Megyénkénti kitöltési hajlandóság**

| Megye | Összes település | Válaszadók száma | Válaszadó települések aránya |
|---|---|---|---|
| Bács-Kiskun | 119 | 63 | 53% |
| Baranya | 301 | 56 | 19% |
| Békés | 75 | 40 | 53% |
| Borsod-Abaúj-Zemplén | 358 | 148 | 41% |
| Csongrád | 60 | 17 | 28% |
| Fejér | 108 | 52 | 48% |
| Főváros, fővárosi kerület | 24 | 13 | 54% |
| Győr-Moson-Sopron | 183 | 66 | 36% |
| Hajdú-Bihar | 82 | 40 | 49% |
| Heves | 121 | 67 | 55% |
| Jász-Nagykun-Szolnok | 78 | 46 | 59% |
| Komárom-Esztergom | 76 | 33 | 43% |
| Nógrád | 131 | 48 | 37% |
| Pest | 187 | 102 | 55% |
| Somogy | 246 | 50 | 20% |
| Szabolcs-Szatmár-Bereg | 229 | 91 | 40% |
| Tolna | 109 | 46 | 42% |
| Vas | 216 | 57 | 26% |
| Veszprém | 217 | 83 | 38% |
| Zala | 258 | 59 | 23% |
| Total | 3178 | 1177 | |

A kérdőívekből megállapítható, hogy a kitöltők 46,4%-a 1001-5000 közötti lakosságszámú települések, 34,2% a 0-1000 lakosság számú kistelepülések és 12,9% 5001-20.000 lakosságszám közötti települések és az 50.000 vagy annál nagyobb lakosú települések a kitöltők 7%-át teszik ki.




5. ábra

*Kitöltők száma települések lakosságszáma szerint*

*Forrás:* saját szerkesztés.

Első ránézésre úgy tűnhet, hogy a kistelepülések sokkal nagyobb hajlandóságot mutattak a kitöltésre, de ez esetben nem vennénk figyelembe a teljes sokaságon belüli arányokat.

Ennek figyelembe vételével megállapíthatjuk, hogy minél nagyobb lakosságszámú a település, arányaiban annál nagyobb kitöltési hajlandóságot mutatott. Ezt jól szemlélteti a 4. ábra.

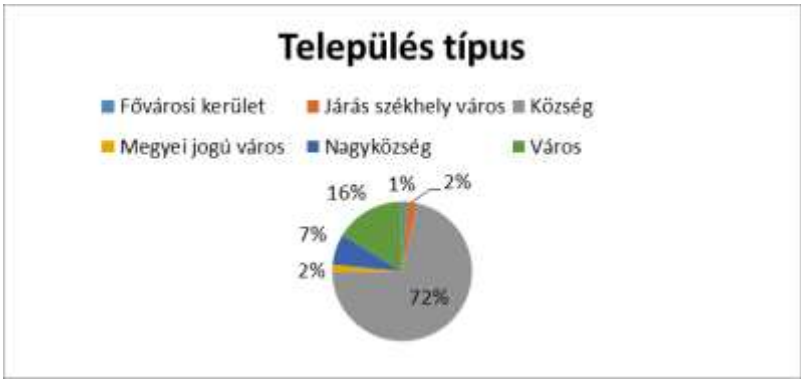

6. ábra

*Válaszadó települések földrajzi és lakosságszám szerinti megoszlása*

*Forrás:* saját szerkesztés.

Az ábrából láthatjuk, hogy míg az 1000 fő alatti településeknek kevesebb, mint negyede, az 1001 – 5000 fő közötti lakosságszámú településeknek már közel a fele tartotta fontosnak a felmérés kitöltését. Az 5000 fő feletti lakosságszámmal rendelkező települések esetében a kategóriába tartozó települések többsége rászánta az időt az adatszolgáltatásra.

A magyar településszerkezet alapvetően aprófalvas. A 4. diagrammból és az 5.-ből is láthatjuk, hogy a településszerkezeti arányok tükröződnek a válaszadó települések lakosságszám szerinti megoszlásában is.




7. ábra

*Válaszadó települések megoszlása település típus szerint*

*Forrás:* 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. Hivataltípus szempontjából elmondható, hogy a százalékok egyáltalán nem mutatnak szignifikáns különbséget. Az önálló hivatalok 29,7%-a, a közös hivatali székhelyek 32,5 %-a, míg a közös hivatali tagok 37,8%-a töltötte ki.


8. ábra

*Válaszadó települések megoszlása hivataltípus szerint*

*Forrás:* saját szerkesztés.

Érdekessé, és az előzőekkel egybecsengővé akkor válik az adat, ha a teljes sokaság arányaiban vizsgáljuk ezeket a számokat.

Az 8. ábrán láthatjuk, hogy a válaszok 38%-a közös hivatal tag önkormányzatától érkezett, azonban ezeknek a településeknek az aránya a teljes sokaságon belül közel 60%. A válaszok 30%-a közös hivatal székhelyéből érkezett, ami a teljes sokaságon belüli arány majd 7%-kal meghaladja és a 20%-os válaszadás az önálló önkormányzati hivatalokból szintén több, mint 3%-kal magasabb az önálló hivatalok teljes sokaságon belüli arányánál.

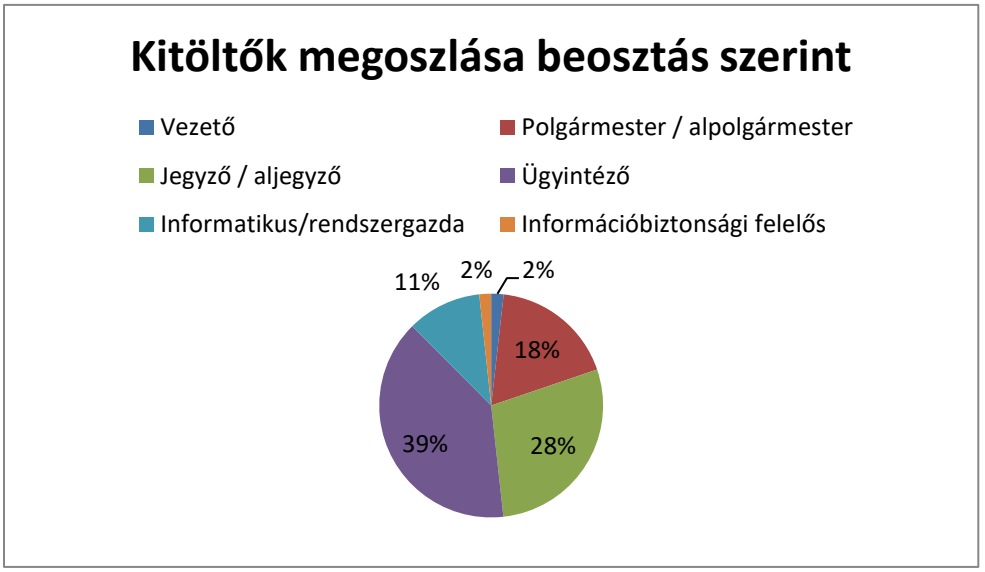
Ezek az adatok ismételten megerősítik azt az eddigi megállapítást, hogy a települések mérete jelentős összefüggést mutat azzal, hogy mennyire kerül középpontba az információbiztonság kérdése az önkormányzati működésben.

**2. táblázat Hivatal típus szerinti megoszlás a lakosságszám kategóriákon belül**

| település méret | hivatal típusa | | |
|---|---|---|---|
| | Közös hivatal tag | Közös hivatal székhely | Önálló |
| 0 - 1000 | 29,06% | 5,01% | 0,08% |
| 1001 - 5000 | 8,67% | 22,77% | 14,95% |
| 5001 - 20000 | 0,00% | 3,23% | 9,69% |
| 20001 - 50000 | 0,00% | 1,36% | 2,63% |
| 50000 - | 0,08% | 0,17% | 2,29% |

Kiegészítő információval szolgál a 2. táblázat. Az előzőekben láttuk, hogy minél nagyobb egy település, annál nagyobb volt a válaszadási hajlandóság. Ezt most kiegészíthetjük a fentiek alapján azzal, hogy a válaszadási hajlandóságot tovább növeli, ha székhely vagy önálló hivatallal rendelkezik a település.

A kitöltők beosztását tekintve legnagyobb részben a hivatalban dolgozó ügyintéző (39%) töltötte ki, ezt követően 28 %-ban jegyzők és aljegyzők, majd 18%-ban polgármesterek, illetve alpolgármesterek.




9. ábra

*Kitöltők megoszlása beosztás szerint*

*Forrás:* saját szerkesztés.

Figyelemre méltó adat, hogy az informatikus/rendszergazda, és IT biztonsági felelős kitöltőt a teljes válaszadói körnek csak 13%-a.

Az ügyintéző (39%), a jegyző/aljegyző (28%) jelentős száma megerősíti azt a feltételezést, hogy inkább hivatali szempontból tartják kiemelten fontosnak az információbiztonság kérdésit.

**3. táblázat Kitöltők megoszlása településkategóriánként.**

| Település méret | Kitöltő beosztása | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | adatvédelmi tisztviselő | egyéb | Információbiztonsági felelős | Informatikai Vezető | Informatikus | Informatikus/ rendszergazda | Jegyző / aljegyző | Polgármester/ alpolgármester | Ügyintéző | Vezető |
| 0 - 1000 | 0,00% | 0,08% | 0,00 % | 0,00% | 0,00 % | 0,68% | 6,88% | 9,26% | 17,08 % | 0,17 % |
| 1001 - 5000 | 0,00% | 0,00% | 0,85 % | 0,00% | 0,08 % | 2,12% | 16,74% | 7,90% | 17,93 % | 0,76 % |
| 5001 - 20000 | 0,00% | 0,00% | 0,08 % | 0,08% | 0,00 % | 4,67% | 3,65% | 0,00% | 3,31% | 0,42 % |
| 20001 - 50000 | 0,08% | 0,00% | 0,25 % | 0,00% | 0,00 % | 2,04% | 1,02% | 0,00% | 0,42% | 0,00 % |
| 50000 - | 0,00% | 0,00% | 0,51 % | 0,00% | 0,00 % | 1,19% | 0,08% | 0,00% | 0,34% | 0,42 % |

A harmadik tábla nem szolgál új információval, inkább csak annyi kiegészítő információt mutat, hogy – a kérdőív tanúsága szerint – az 5000 fő alatti lakosságszámú települések esetében vesz részt közvetlenül a polgármester az operatív ügyekben.

## A kérdőív feldolgozásának módszere

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 által a kérdésekre adott véleményét, az információbiztonsággal kapcsolatos tudatosságát hivatott felmérni.

Az első szakmai blokk az önkormányzatok információbiztonsági feladat ellátásának gyakorlatának felmérését célozta.

Arra kerestük a választ, hogy

- az Infotv. által előírt feladatokat, hogyan milyen erőforrással látják el,
- az információbiztonság érdekében milyen tevékenységeket végeznek és ezeket milyen gyakoriséggal,
- van-e és ha igen mi a véleményük a védekezés módjairól.

A második szakmai blokk az önkormányzatok védekezéséről, felkészültségéről, kiberbiztonsági kompetenciájáról alkotott vélemények feltárását tűzte ki célul.

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

## A kérdőív feldolgozásának eredményei

Az elemzésben szereplő kérdések válaszait – tekintettel az előzőekben már kifejtettekre, elsősorban - hivatal típusonként (közös hivatal székhelye, közös hivatal tagja, önálló hivatal) vizsgáltuk. A válaszok megoszlása többségében a „nem tudom" válaszok nélkül került ábrázolásra.

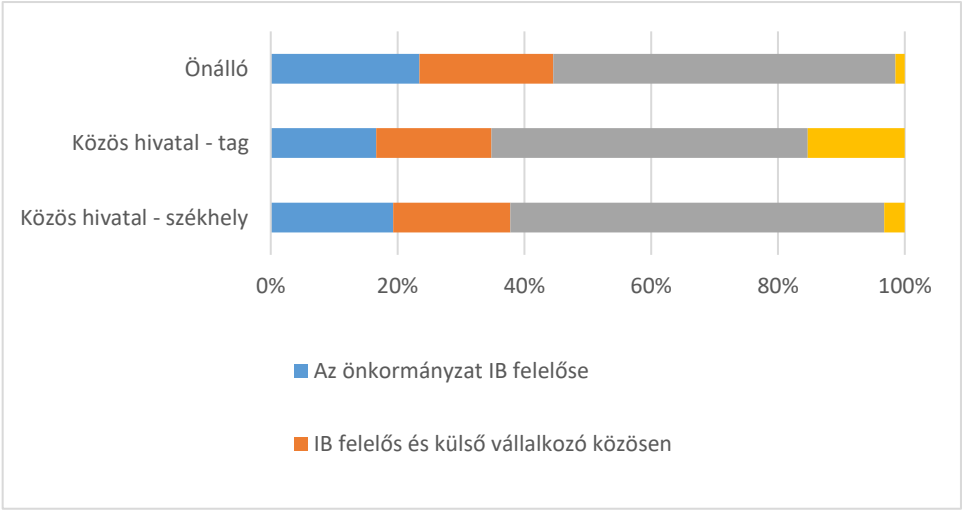
### Az Infotv. által előírt feladatok ellátása

Az első három, információbiztonsági feladatokra vonatkozó kérdésre adott válaszok hivatal típusonként hasonló mintázatot mutatnak (10.1 - 10.3. ábra). Minden hivatal típus esetén a leggyakoribb, hogy külső vállalkozás végzi a szóban forgó feladatokat. A közös hivatali tagoknál fordult elő leggyakrabban, hogy nincs ilyen feladatuk, vagy szabályzatuk.

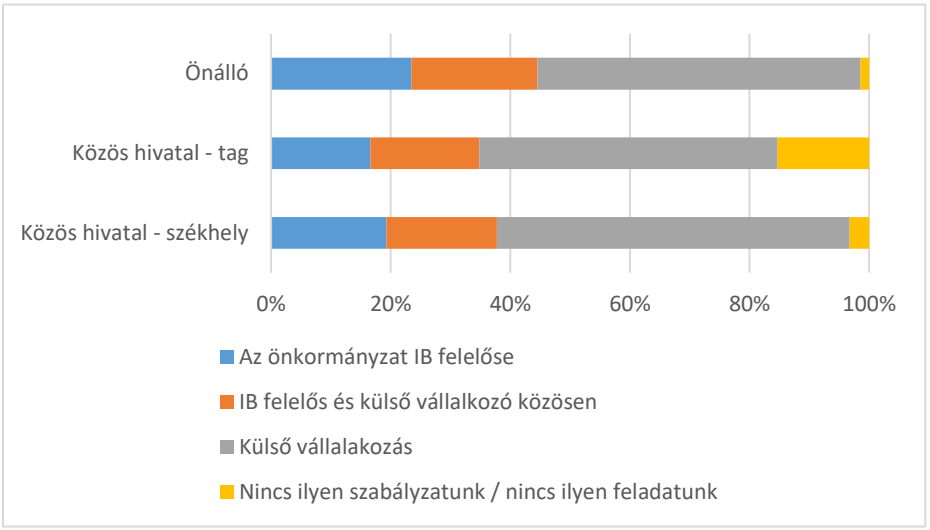
Az egyes felhasználók felelősségi köreinek megállapítására, kijelölésére vonatkozó kérdés válaszai alapján elmondható, hogy az önálló önkormányzatoknál legnagyobb a vezető általi kijelölés aránya, és közös önkormányzati tagoknál leggyakoribb, hogy nincs ilyen kijelölés (10.4. ábra).

Az incidenskezelés, adatszolgáltatás végzésére vonatkozó kérdés válaszai alapján elmondható, hogy a közös önkormányzati tagoknál legkevésbé jellemző, hogy önkormányzati IB felelős és leginkább jellemző, hogy vezető végzi e feladatokat (10.5. ábra).

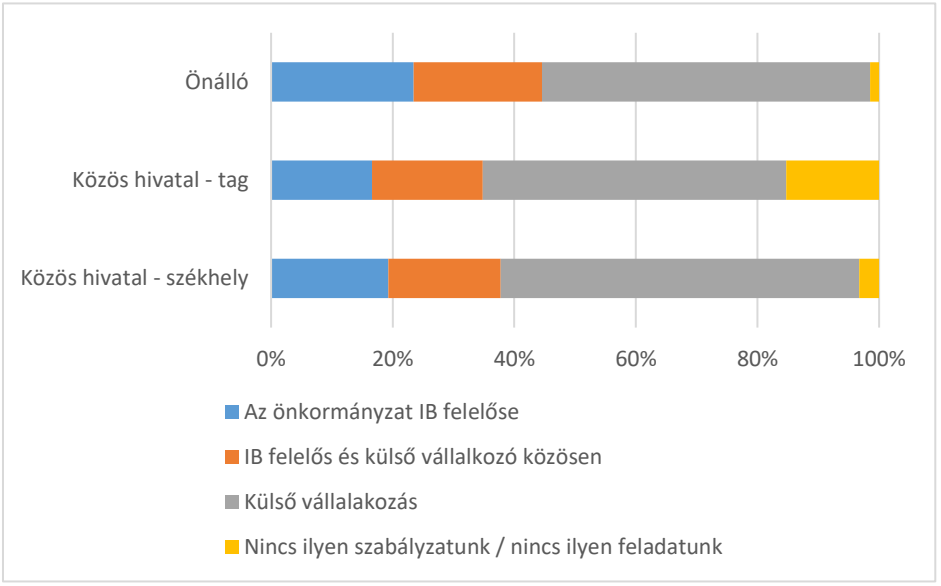
10.1 Az önkormányzatnál ki végzi az információbiztonsági feladatokat? Az információbiztonsági szabályzat készítése



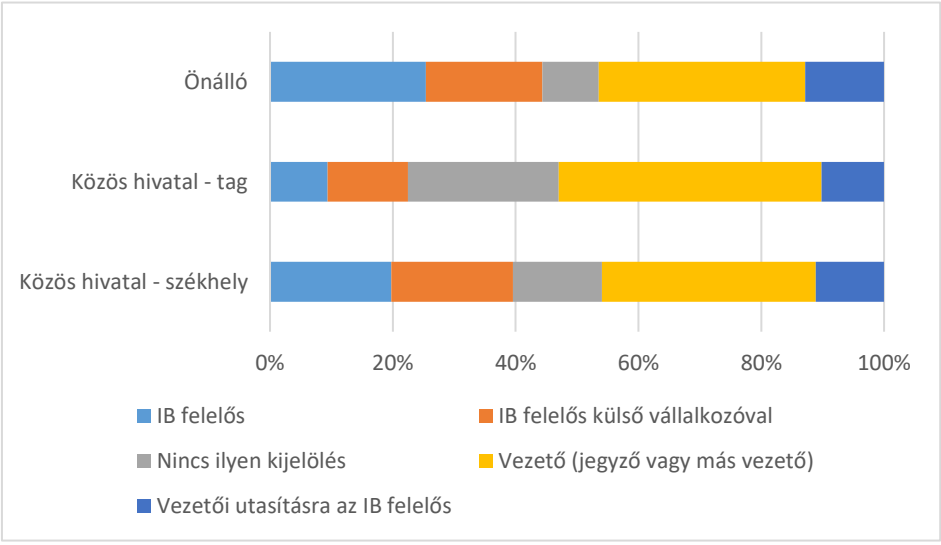
10.2 Az önkormányzatnál ki végzi az információbiztonsági feladatokat? Az önkormányzat IT rendszereinek osztályba sorolása



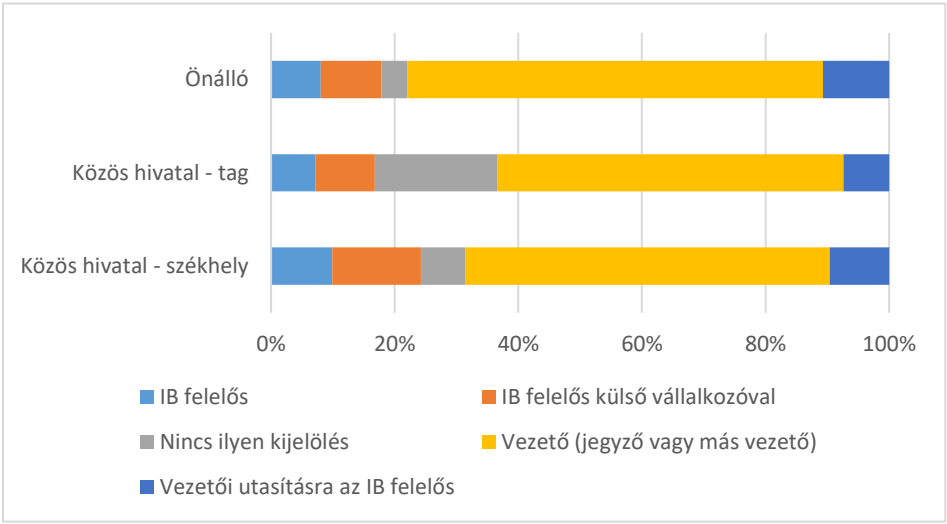

10.3 Az önkormányzatnál ki végzi az információbiztonsági feladatokat? Az önkormányzat IT rendszereinek kockázatelemzése



10.4 Az önkormányzatnál ki végzi az információbiztonsági feladatokat?
**Az egyes felhasználók felelősségi köreinek megállapítása,** kijelölése




10.5 Az önkormányzatnál ki végzi az információbiztonsági feladatokat?
Incidenskezelés, adatszolgáltatás az önkormányzatnál

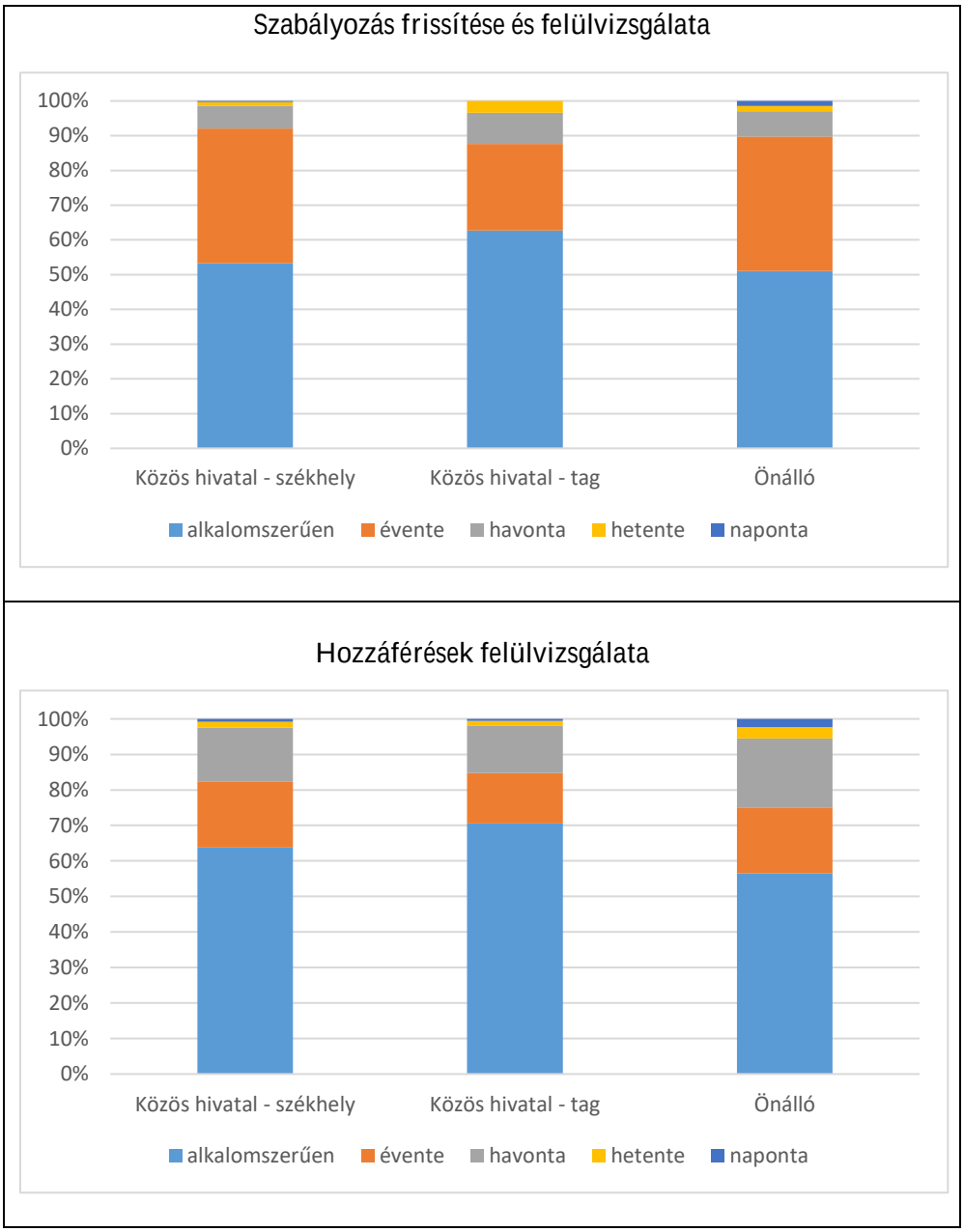


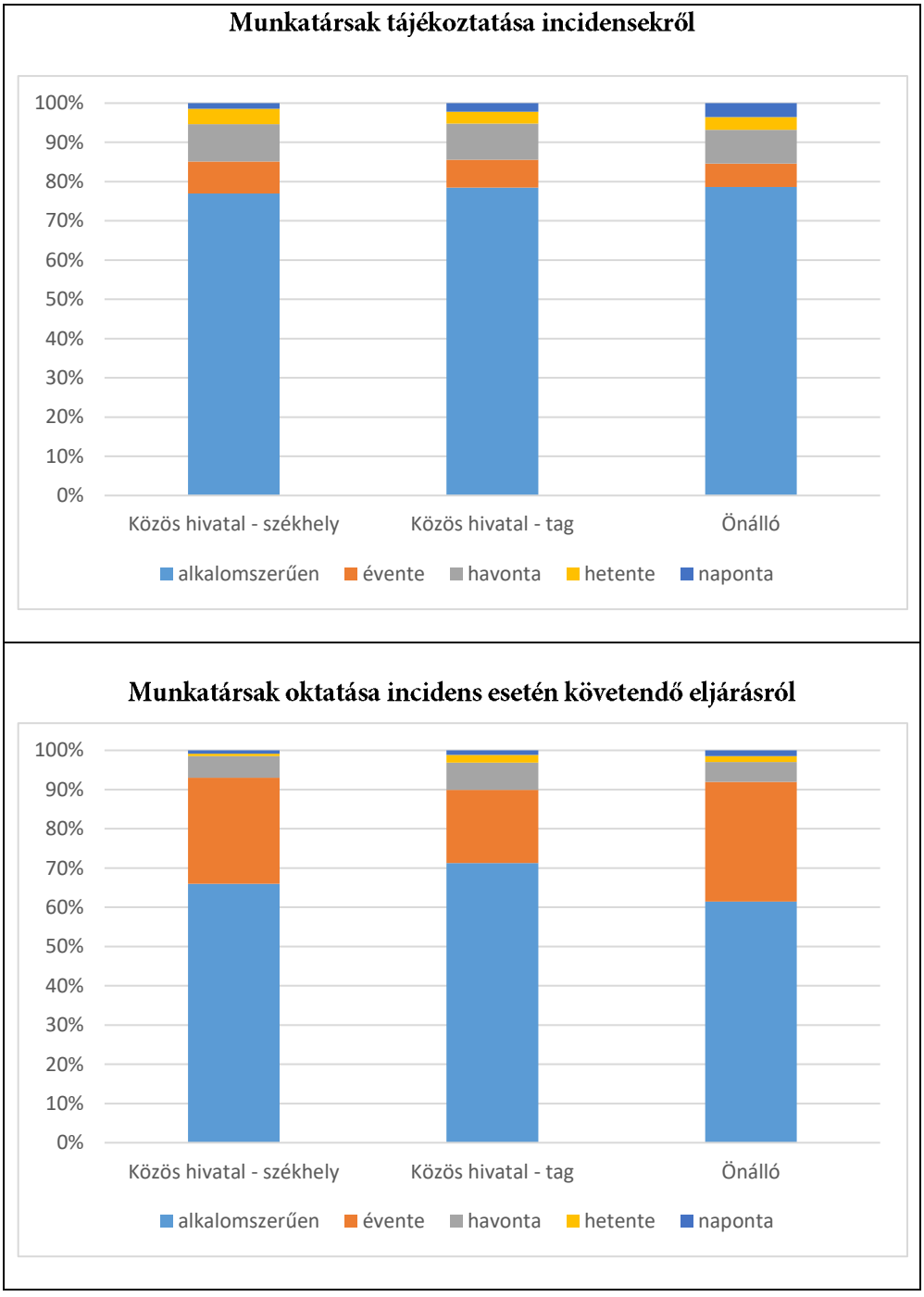

10. ábra

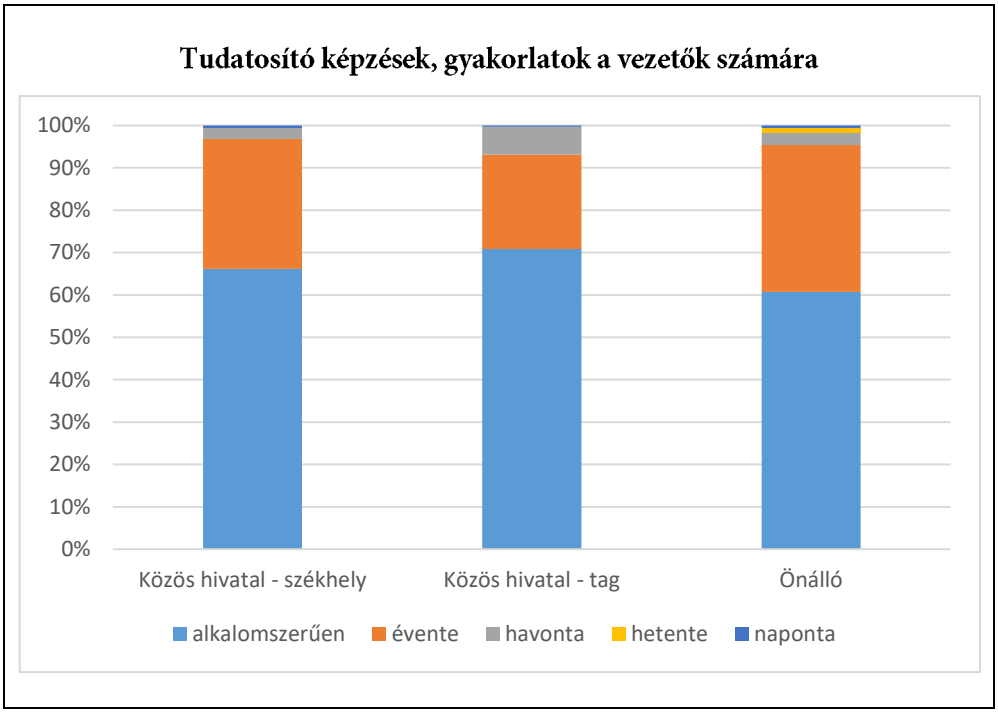
*Az önkormányzatnál ki végzi az információbiztonsági feladatokat?*

*Forrás:* saját szerkesztés.

**Mennyire van figyelem, fókusz az It biztonsági feladatokon?**
A „Milyen gyakran végzik az alábbi tevékenységeket?" kérdésekre adott válaszok hivatal típusonként nem mutattak számottevő eltérést (11. ábra).




Munkatársak tájékoztatása incidensekről
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Közös hivatal - székhely
Közös hivatal - tag
Önálló
alkalomszerűen
évente
havonta
hetente
naponta
Munkatársak oktatása incidens esetén követendő eljárásról
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Közös hivatal - székhely
Közös hivatal - tag
Önálló
alkalomszerűen
évente
havonta
hetente
naponta




11. ábra

*Milyen gyakran végzik ezeket a tevékenységeket?*

*Forrás:* saját szerkesztés.

Megyénként is megvizsgálva ezeket a kérdéseket (szintén a „nem tudom" válaszok nélkül), kisebb eltérések mutatkoztak a válaszokban:

Azon válaszadók aránya, akik hivatalában a szabályozás frissítését és felülvizsgálatát alkalomszerűen végzik, legnagyobb Fejér, Győr-Moson-Sopron és Tolna megyében. Olyan válaszadók, akik hivatalában naponta végzik e tevékenységeket mindössze 5 megyében fordultak elő: Borsod-Abaúj-Zemplén, Csongrád, Komárom-Esztergom, Pest és Szabolcs-Szatmár-Bereg (12. 1. ábra).

Azon válaszadók aránya, akik hivatalában a hozzáférések felülvizsgálatát csupán alkalomszerűen végzik, legnagyobb Budapesten, Győr-Moson-Sopron és Veszprém megyében. Azon válaszadók aránya, akiknél viszont naponta végzik e tevékenységet, a legnagyobb Csongrád és Nógrád megyében (12. 2. ábra).

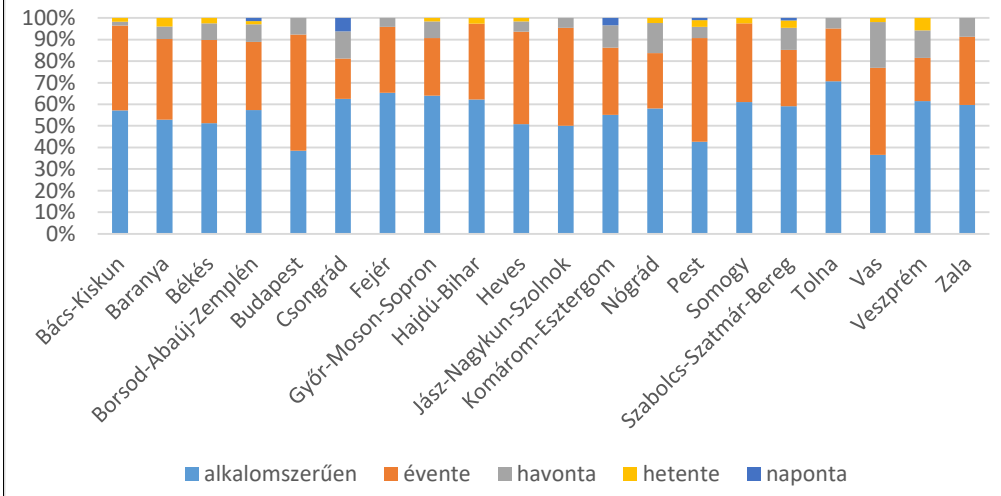
Azon válaszadók aránya, akik hivatalában alkalomszerűen tájékoztatják a munkatársakat incidensekről legnagyobb Budapesten, valamint Pest, Somogy, Bács-Kiskun és Borsod-Abaúj-Zemplén megyében (12. 3. ábra).

Azon válaszadók aránya, akik hivatalában alkalomszerűen végzik a munkatársak oktatását incidens esetén követendő eljárásról legnagyobb Borsod-Abaúj-

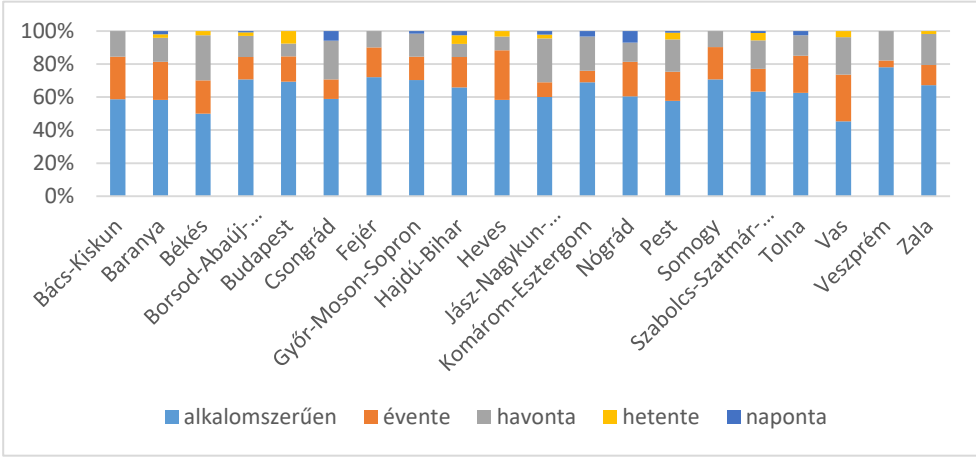
Zemplén, Csongrád, Jász-Nagykun-Szolnok, Szabolcs-Szatmár-Bereg és Tolna megyében (12. 4. ábra).

Azon válaszadók aránya, akik hivatalában alkalomszerűen tartanak tudatosító képzéseket, gyakorlatokat a vezetők számára legnagyobb Csongrád, Jász-Nagykun-Szolnok és Veszprém megyében (12. 5. ábra).

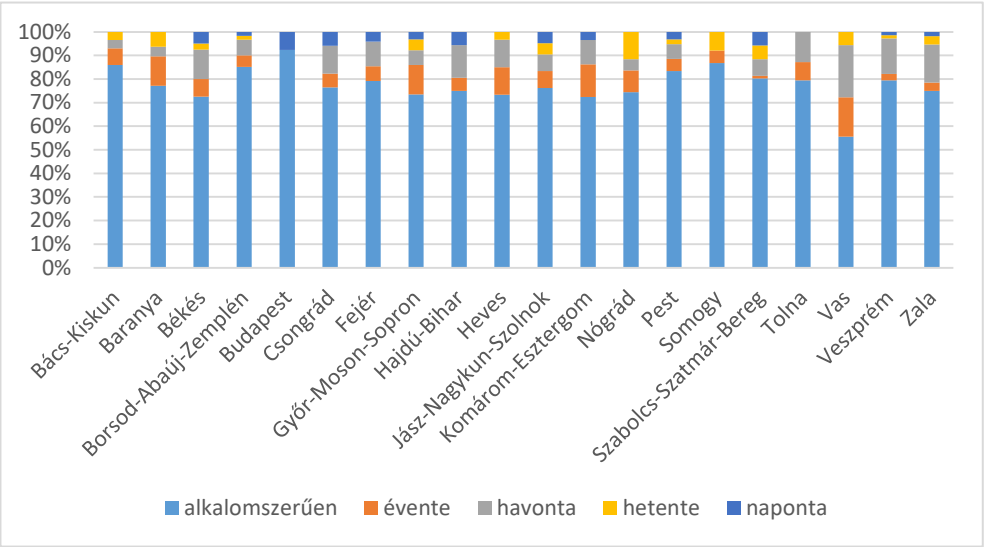
12.1 Szabályozás frissítése és felülvizsgálata



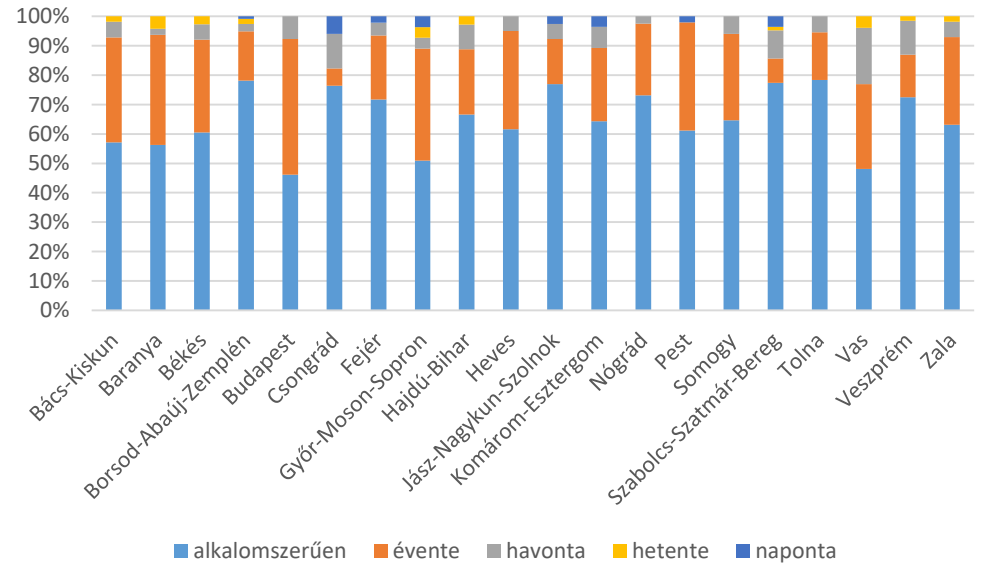

12.2 Hozzáférések felülvizsgálata

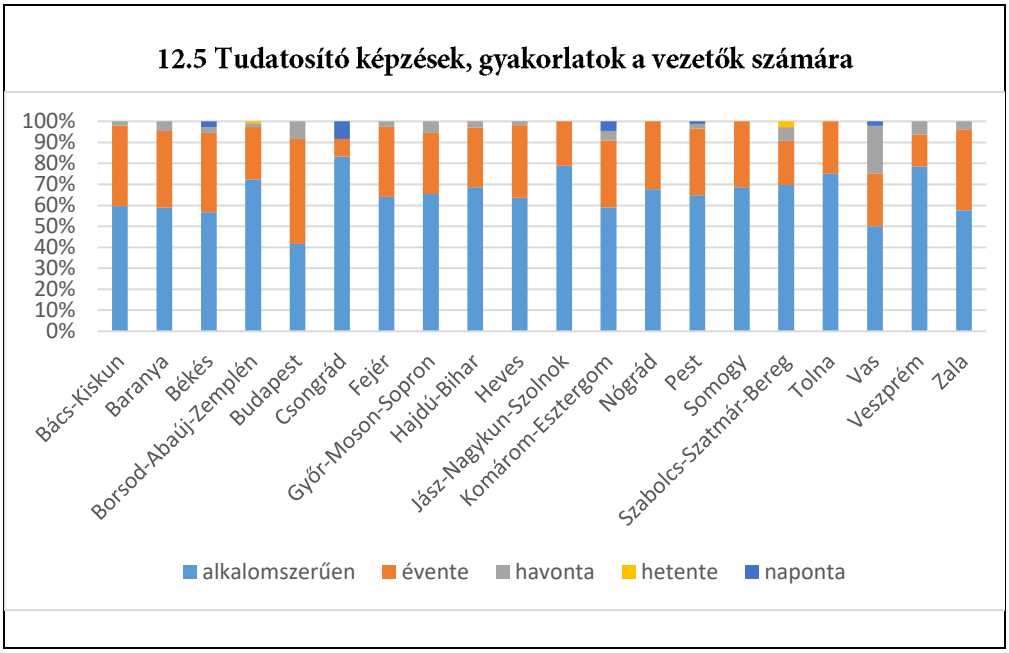


### 12.3 Munkatársak tájékoztatása incidensekről




### 12.4 Munkatársak oktatása incidens esetén követendő eljárásról






12. ábra

*Milyen gyakran végzik ezeket a tevékenységeket?*

*Forrás:* saját szerkesztés.

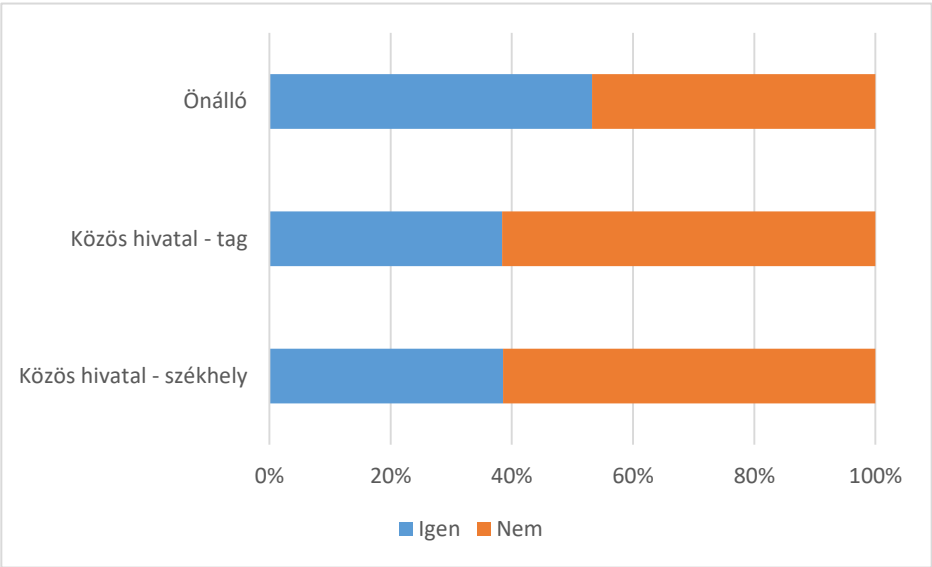
## Védekezés módjai

A kérdőív kérdései körbejárják az önkormányzatok védekezési gyakorlatát.

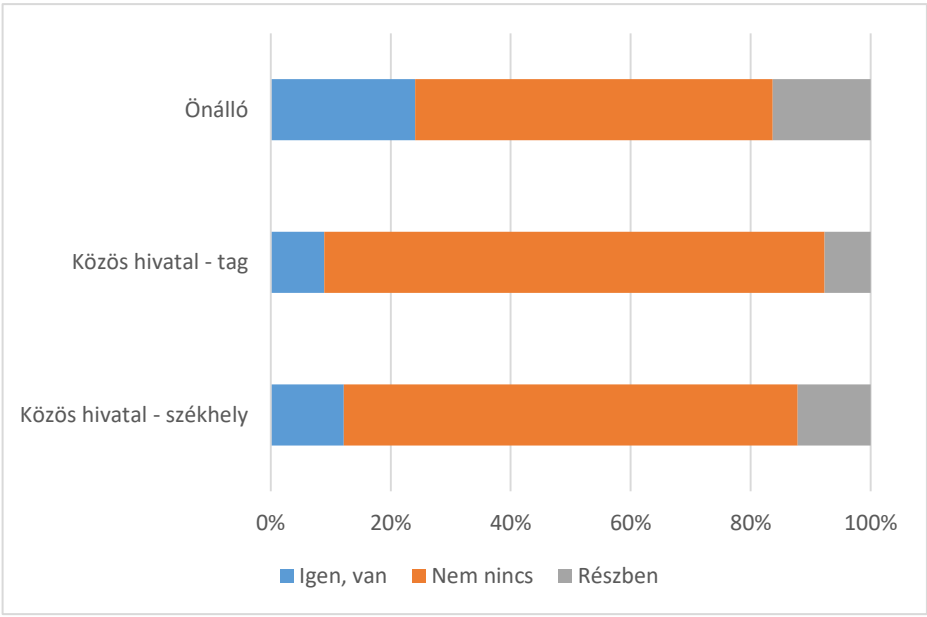
Az önálló önkormányzatok válaszadói körében valamivel nagyobb a levelezőrendszerhez kapcsolódó titkosítással rendelkezők aránya, az Üzletmenet folytonosság tervvel rendelkezők aránya, valamint a jelszókezelési és módosítási protokollal rendelkezők aránya, mint a közös önkormányzatok válaszadó körében (13.1 - 13.3. ábra).

A külső eszközök, alkalmazások használatának szabályozása a válaszok alapján hasonló az egyes hivatal típusok körében: Mindhárom hivatal típusnál leggyakoribb, hogy engedéllyel használhatók a külső adathordozók, tabletek, notebookok stb. és közösségi alkalmazások és legritkább, hogy tilos a használatuk (13.4 - 13.5. ábra).

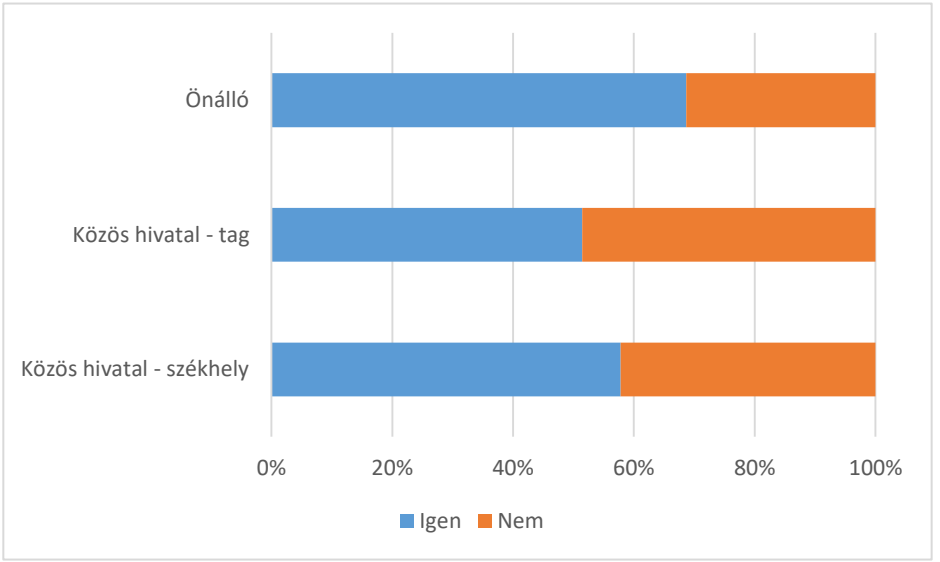
13.1 Működik-e titkosítás a levelezőrendszerhez kapcsolódóan?



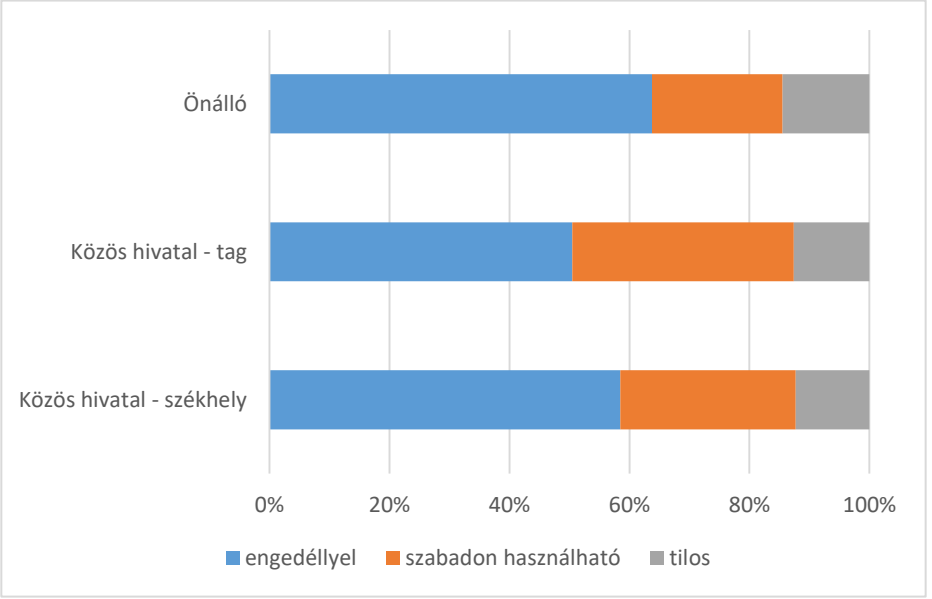

13.2 Rendelkeznek-e "Üzletmenet folytonosság terv" - vel" (BPC)?

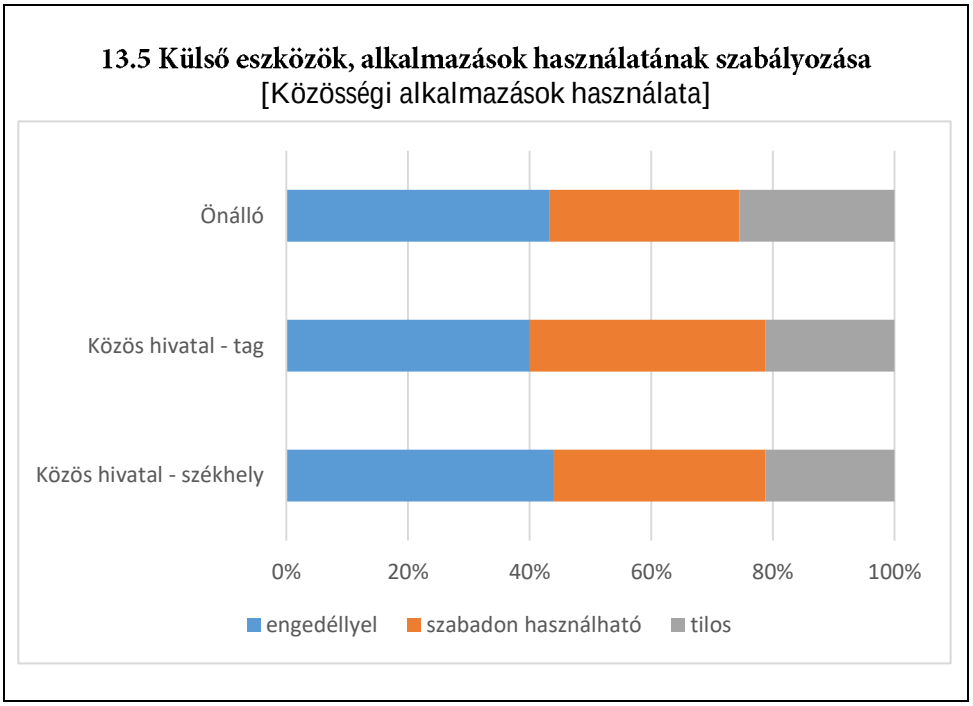


**13.3 Működik-e jelszókezelési és módosítási protokoll az önkormányzatnál?**




**13.4 Külső eszközök, alkalmazások használatának szabályozása [Külső eszközök használata (adathordozók, tablet, notebook stb.)]**






13. ábra
*Védekezés*

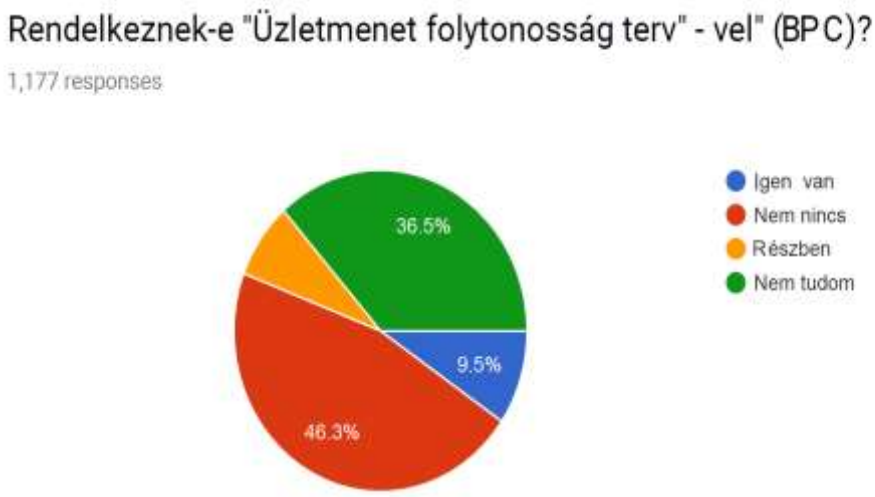
*Forrás:* saját szerkesztés.

A kérdőív kitér arra a kérdésre, hogy működik-e az önkormányzatnál jelszókezelési és módosítási protokoll és ha igen, melyek ezek, illetve ki készítette őket.

Arra a kérdésre, hogy melyek ezek a protokollok, amiket használnak, a kitöltők 13%-a válaszolt (158 db). 15% használ valamilyen tűzfalat vagy vírusirtót a jelszókezeléshez. 15% használja a folyamatos jelszómódosítás, illetve bonyolult karakterek használatának gyakorlatát, IB szabályokban rögzített eljárásokat.

Azt a kérdést, hogy ki készítette el a jelszókezelési és módosítási protokollt összesen 205-en válaszolták meg. Ennek elenyésző, 13%-a mondta azt, hogy az informatikus vagy rendszergazda munkatárs. 34% válaszolta azt, hogy külsőssel végeztetik el ezeket a munkákat (ebbe beletartoznak a külső vállalkozók, magánvállalkozók, megbízott cégek, Közinformatika Kft.).

## Üzletmenetfolytonossági terv megléte




14. ábra
*Üzletmenetfolytonossági terv*

*Forrás:* saját szerkesztés.

A fenti 14. ábrából látszódik, hogy a kitöltők 46,3%-nak nincsen üzletmenet folytonossági terve, míg 36,5% nem is tud róla, hogy van e vagy nincs. Ennek e tervnek azért van jelentősége, mert azt a célt szolgálja, hogy az üzleti tevékenységek akkor is folytatódhassanak, ha valamilyen informatikai (vagy egyéb) zavar keletkezik a működési feltételekben. Ennek ellenére a válaszadók szokatlanul nagy aránya nincs tisztában a terv meglétével, vagy egyáltalán nincs is nekik. Az ezzel kapcsolatos tudásátadás és az eredmény javítása mindenképpen javasolt a későbbiekben.

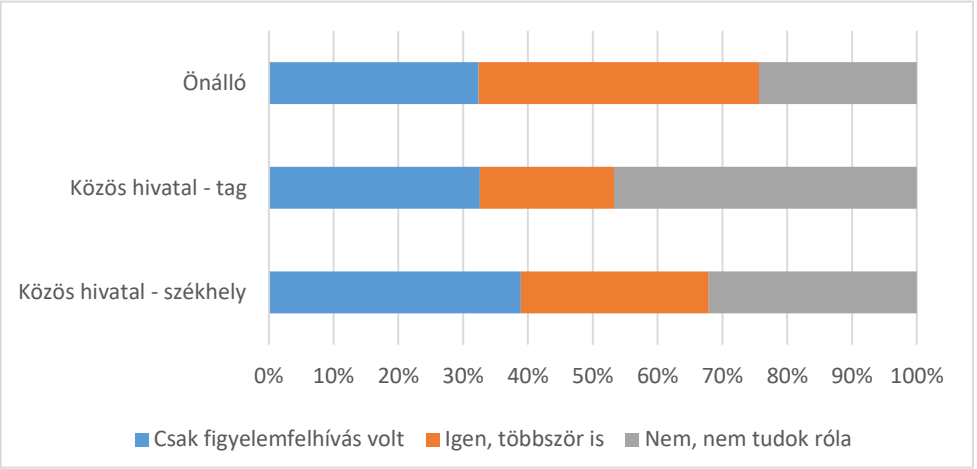
## Munkatársak tudatosítása, képzése

| **4. táblázat Szervezetének dolgozói vettek részt biztonságtudatosító oktatáson? (n:1177)** | | | |
|---|---|---|---|
| Hivatal típusa | Nem, nem tudok róla | Igen, többször is | Csak figyelemfelhívás volt |
| Közös hivatal tag | 18% | 8% | 12% |

| | | | |
|---|---|---|---|
| Közös hivatal szkhely | 10% | 9% | 13% |
| Önálló | 7% | 13% | 10% |
| Összesen | 35% | 30% | 35% |

A 4. táblázatból azt láthatjuk, hogy a válaszadó önkormányzati körnek csak 30%-ának esetében volt biztonságtudatosító oktatás, 35%-kuknál csak figyelemfelhívás volt és a dolgozók oktatására nem került sor, illetve a válaszadók 35%-ának nincs tudomása róla.

Ha a hivataltípus szerint vizsgáljuk meg a válaszok megoszlását, akkor a biztonságtudatosító oktatáson való észvételre vonatkozó kérdés válaszaiból az látható (15. ábra), hogy a közös hivatalok tagjainak körében legalacsonyabb az „igen, többször is" válaszok aránya és legmagasabb a „nem, nem tudok róla" válaszok aránya és az önálló hivatalok esetében a legmagasabb az „igen, többször is" válasz aránya.

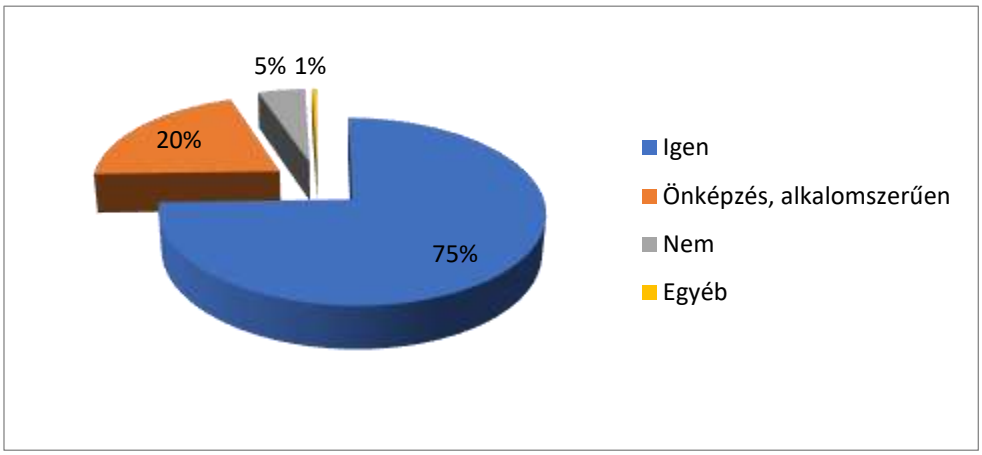



15. ábra

*Biztonságtudatosító képzésen való részvétel*

*Forrás:* saját szerkesztés.

Ezzel együtt a válaszadók igen jelentős hányada tartja fontosnak a dolgozók rendszeres képzését.




16. ábra

*Szükségesnek tartja a dolgozók rendszeres biztonságtudatosító képzését, oktatását?*

*Forrás:* saját szerkesztés.

Ez azt jelezheti számunkra, hogy a válaszadók látják a terület fontosságát, azonban rendelkezésre álló eszközök nem támogatják ennek megvalósítását kellőképpen. Az egyéb válaszok is ezt támasztják alá, ahol az idő, a finanszírozás és a megfelelő képzési struktúra és kínálat hiányát említik.

## A válaszadó települések tapasztalatai, véleménye

Az alábbiakban alaposabban megvizsgáljuk a kérdőív azon kérdéseit, melyre a válaszadónak lehetősége volt saját szavas választ adni. Ezek elsősorban a válaszadók véleményére, tapasztalataira fókuszáltak.

Arra a kérdésre, hogy *Ön szerint az önkormányzat információbiztonsága érdekében mi a legfontosabb feladat?* nem volt kötelező a válaszadás és a válaszadóknak mintegy a negyede ( 23%) töltötte ki (1177-ből 265 válaszadó).

A válaszok között kiemelkedő aránnyal fordult elő az a vélekedés, hogy a legfontosabb feladat a szabályok, illetve a törvények megismerése és betartása. Ezt vagy ezzel összefüggő választ a jelen kérdést kitöltők 27%-a adta. A második helyen a biztonságot emelték ki (értve ezt a rendszerre, eszközök és szoftverek biztonságosabbá tételére), illetve az adatok védelmét, amely magában foglalja mind a személyes, mind az önkormányzati adatok óvását is.

A másik nyitott kérdésben arra voltunk kíváncsiak, hogy történt e valaha kibertámadás az önkormányzat informatikai eszközei ellen, és ha igen, akkor mi történt és hogyan kezelték azt *(Van-e ismeretük informatikai eszközözeik elleni támadásokról, volt-e már ilyen incidensük?, Ha igen, akkor mi történt? Hogyan kezelték?).*

Az első kérdésre az összes kitöltő 15%-a adott igenlő választ (beleértve azokat is, akiknél akár többször is megtörtént) és 85% adta azt a választ, hogy nem történt incidens vagy nem tud róla.

Az igennel válaszolók 30%-a írta meg, hogy milyen konkrét incidens történt az esetükben, illetve hogyan kezelték azt. A válaszadók 18%-át valamilyen vírus (levelező rendszeren keresztül, honlapon) támadta meg. 8% esetében az informatikus végzettségű kolléga, vagy külső szakember oldotta mega a problémát. A válaszok egy része sajnos nem volt értelmezhető, mert nem releváns válaszok érkeztek.

Az önkormányzatnál alkalmazott IB módszerek/gyakorlat/tapasztalat rubrikát összesen 172 település válaszadója töltötte ki. 20%-uk gondolja úgy, hogy a náluk alkalmazott módszerek, gyakorlatok beválnak, folyamatos működésben vannak, vagy most építik ki őket. 11% gondolja, hogy ezek a gyakorlatok vagy nem kivitelezhetőek, vagy nincs rá megfelelő anyagi forrás és „gyerekcipőben járnak". 5%-a a válaszadóknak az IB szabályzat, illetve módszerek szerint jár el. A kitöltők 14%-ának gyakorlatát képezik a tűzfalak, vírusirtók üzemeltetése, a jelszó védelem, havi riportok készítése, rendszeres ellenőrzés és a kollégák oktatása.

Ugyanezen kérdésközhöz tartozik az is: *Ha következett be incidens akkor az Ön véleménye szerint ennek mi volt a fő oka?* A válaszadók 58%- vallja azt, hogy a munkatársak felkészületlensége, protokoll hiány vagy külső vírus volt az ok.

Érte már támadás az önkormányzat honlapját vagy más közösségi alkalmazását? kérdésre 66-an válaszoltak úgy, hogy nem, vagy nem tudnak róla és mindössze 5 önkormányzat állította, hogy igen, egyszer vagy többször is. Ezek közül egy esetben egy külső cég, egyben pedig rendszergazda segítségével sikerült elhárítani a problémát.

## Az online felmérés eredményeinek összefoglalása

A kérdőív – ahogyan az már az előzőekben jelzésre került – három fő területet vizsgált az önkormányzat működésében:

- ki látja el az információbiztonsághoz kapcsolódó feladatokat?
- figyelem, módszerek, eszközök és felkészültség terén hogyan kezeli a kérdést az önkormányzat a témát?
- milyen működési tapasztalatai vannak?

Az elemzés során az egyes kérdésekre érkezett válaszokat hivatal típus szerint kerültek vizsgálatra, néhány esetben a földrajzi elhelyezkedés is.

## Az önkormányzatok Infotv. által előírt feladatok ellátása

Az információbiztonsági feladatokat – függetlenül a hivataltípustól – a válaszadó önkormányzatok több, mint 50 %-a szervezi ki külső vállalkozás részére. Nem volt jelentős eltérés a hivataltípus szerint sem a szabályzat készítésében, sem az önkormányzati informatikai rendszerek osztályba sorolása és a kockázatelemzés készítése kérdés esetében sem.

A felhasználók felelősségi köreinek meghatározása, kijelölése kérdésre adott válaszból látható, hogy az önálló hivatallal rendelkezők esetében leginkább a vezetői kijelölés a jellemző – a válaszadók közel két harmadánál – és a közös hivatali tagok esetében a legkevésbé, de ez esetben is közel ötven százalék a vezetői kijelölés.

Az incidens kezelés és adatszolgáltatásra érkezett válasz alapján elmondható, hogy mindhárom hivataltípus esetében jelentős a vezetői figyelem, a legmagasabb a közös hivatali tag önkormányzatok esetében, 40% feletti.

## Figyelem, fókusz a területen

A „Milyen gyakran végzik az alábbi tevékenységeket?" kérdés kapcsán az alábbi eredmények születtek:

A szabályzatok, hozzáférések felülvizsgálata hivataltípusonként hasonló eredményeket mutattak. Jellemzően alkalomszerűen vagy évente foglalkoznak ezzel a kérdéssel.

A munkatársak tájékoztatása, oktatása incidensekről és azok kezeléséről a válaszok tanúsága szerint alkalomszerű. Az incidenskezelés esetén követendő eljárások oktatásánál is inkább csak felmerülés esetén alkalomszerűen történik.

Külön figyelmet érdemel, hogy a vezetők részére sincs rendszeres tudatosító képzés, ami jelentős magyarázattal szolgál a terület elhanyagoltságára. Minden szervezettípus esetében kiemelt jelentősége van a vezetői elkötelezettségnek, azonban a közszféra, így az önkormányzatok esetében ez hatványozottan igaz. Minden hivatal típus esetében a válaszadók több mint 60%-a (közös hivatal tag válaszadók esetében 70%) mondta azt, hogy a vezetők részére tudatosító képzések és gyakorlatok csak alkalomszerűen vannak. Az évi gyakoriság legnagyobb arányban (30%) az önálló hivatallal rendelkező önkormányzatok esetében jelezték. A földrajzi elhelyezkedések szerinti elemzés esetében is csak kisebb eltérés volt azonosítható.

## Védekezés módjai

A kérdések számossága nem tette lehetővé a védekezés módjainak teljes feltérképezését, inkább csak a felkészültségről, az attitűdről kívánt egy képet szerezni.

A kérdésekre érkezett válaszok alapján a védekezés terén a kép nem rózsás. A levelezőrendszerekhez kapcsolódó titkosítás a legmagasabb az önálló hivatalok esetében, de a beérkezett válaszok alapján itt is alig haladja meg az 50%-ot, míg a másik két hivataltípus esetében nem éri el a 40%-ot. A jelszókezelési és módosítási protokoll már lényegesen jobb képet mutat, de még ezen a területen is jelentős azon önkormányzatok száma – a válaszadók között – ahol nincs ilyen sem (13.3. ábra). Az „Üzletmenet folytonossági terv" (BPC) esetében pedig valószínűsíthető, hogy az önkormányzatok jelentős része nem ismeri ezt az eszközt és nem is használja. A terv jelentősége abban áll, hogy biztosítsa a folyamatos működés lehetőségét, akkor is ha valamilyen zavar keletkezik a működési feltételekben. A válaszadóknak csak 9,5%-a állította határozottan, hogy rendelkezik ilyen tervvel (14. ábra) és 82,8%-ka a

válaszadóknak azt jelezte, hogy nincs vagy nem tudja. A külső alkalmazások és eszközök használatában a válaszok elemzése alapján nem látnak a válaszadó önkormányzatoknál jelentős fenyegetést.

A munkatársak tudatosító képzése, rendszeres oktatása – finoman fogalmazva is – nincs a beérkezett válaszok elemzése alapján fókuszban. A kérdőívet kitöltő önkormányzatok 35%-ánál sem figyelemfelhívó tájékoztatásra, sem oktatásra nem került sor a válaszadó tudomása szerint. A válaszadóknak csak 30% mondta azt, hogy sor került (többször is) oktatásra és a legmagasabb arány az önálló hivatalok esetében. Érdekes kontrasztot kínál, hogy miközben nagyon alacsony a munkatársak képzése a válaszadó önkormányzatoknál, ezzel szemben 75% fontosnak tartja a rendszeres képzését a munkatársaknak és 20% pedig alkalomszerűen javasolja a képzést (15. ábra).

## Működési tapasztalatok

A működési tapasztalatok kapcsán többségében voltak a szabadszavas válaszokat engedő kérdések, illetve az igen – nem válaszlehetőségekhez kapcsolódó szabadszavas kiegészítő kérdések.

A válaszadók közel 30%-a szerint fontos, hogy a hivatalban megfelelő legyen a szabályozás, ismerjék az előírásokat a munkatársak és tartsák be azokat. Hasonló gyakoriságú volt azon válaszok aránya, ahol a megfelelő hardver és szoftver fontosságát emelték ki.

A történt-e valamilyen incidens már az önkormányzatnál, ott a válaszadók 15%-a válaszolt igennel. Az igennel válaszolók számára opcionális volt, hogy válaszoljanak a „Konkrét incidens" és „Hogyan kezelték" kérdésekre és sajnos ezen kitöltőknek csak 30%-a válaszolt ezekre a kérdésre. Elsősorban vírustámadásokról számoltak be a levelezőrendszer, honlap ellen. A kezelés módjánál a kezelőt jelölték meg – informatikus, külsős szakember –. A bekövetkezett incidensekkel kapcsolatban a válaszadók többsége szerint is kiemelt szerepe van a humán erőforrás felkészültségének vagy felkészületlenségének.

Azon önkormányzatok esetében, akik komolyan foglalkoznak az információbiztonság kérdésével ott folyamatos fejlesztésekről számoltak be.

## Javaslatok

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 [4]. Ez tükröződik a Bizottság és a NIS irányelv javaslataiban is. 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 képzés, oktatás, tudatosítás kiemelt prioritás.

- 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. Szükséges annak vizsgálata, hogy a hazai képzési paletta biztosít-e olyan képzéseket, amelyeket a gyakorlatiasság, a tudatosítás érdekében sokszínű módszerek és az önkormányzati hivatalok felkészítéséhez alkalmazkodni képesek. Ki kell dolgozni és rendszeresen felülvizsgálni egyszerű, könnyen érthető és autodidakta módon feldolgozható képzési anyagokat.
- 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.

## Felhasznált irodalom

[1] Számadó Róza- Önkormányzatok kiberbiztonságának és online képességének vizsgálata, figyelemmel az emberi tényező fejlesztésének kérdéseire, Doktori Disszertáció, 2018. ÓE BDI, http://bdi.uni-obuda.hu/sites/default/files/Doktori_(PhD)_ertekezes_-_Szamado_Roza.pdf

[2] ÖFFK II., Kutatás III., Kutatási Ajánlás, 3.1.2 Jogszabály-felülvizsgálattal összefüggő ajánlások az Info Tv. közzétételi kötelezettségének újragondolásával kapcsolatban

[3] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, forrás: https://net.jogtar.hu/jogszabaly?docid=A1100112.TV

[4] 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.)

## Melléklet - Kérdőív

Önkormányzatok IT biztonságának kérdései

Az Óbudai Egyetem a Biztonságtudományi Doktori Iskola hallgatóinak, tanárainak és kutatóinak bevonásával a önkormányzati rendszerek biztonságosabbá tétele érdekében kutatást kezdeményezett, melynek keretében kérdőíves megoldással vizsgálni, kutatni szeretnék a hálózatok, az azokon dolgozó személyzet biztonságát és biztonságtudatosságát, az online jelenlétet. Kérem, hogy a téma fontosságára való tekintettel segítse, hogy értékelhető eredmény szülessen és a kérdőív kitöltéséről - 2018. október 9-ig - szíveskedjen gondoskodni. A kérdőív kitöltése maximum 10 percet vesz igénybe. Segítségét előre is köszönjük!

*Alapadatok*

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 tag

**Kitöltő beosztása**

polgármester/alpolgármester
jegyző/aljegyző
Információbiztonsági felelős
ügyintéző
egyéb:

*Jelölje a megfelelő választ. Az Információbiztonsági felelős további jelölése "IB felelős.*

Az önkormányzatnál ki végzi az információbiztonsági feladatokat?

| Külső vállalkozás | Az önkormányzat IB felelőse | az önkormányzat részmunkaidős munkatársa | IB felelős és külső vállalkozó közösen | Nincs ilyen szabályzatunk/nincs ilyen feladatunk | Nem tudom |
|---|---|---|---|---|---|

Információbiz-
tonsági szabályzat
készítése

Az önkormányzat
IT rendszereinek
osztályba sorolása

Az önkormányzat
IT rendszereinek
kockázatelemzése

Az önkormányzatnál ki végzi az alábbi feladatokat?

| | IB felelős | Vezető (jegyző vagy más vezető) | Vezetői utasításra az IB felelős | IB felelős külső vállalkozóval | Nincs ilyen kijelölés | Nem tudom |
|---|---|---|---|---|---|---|
| Az egyes felhasználók felelősségi köreinek megállapítása, kijelölése | | | | | | |
| Incidenskezelés, adatszolgáltatás az önkormányzatnál | | | | | | |

Milyen gyakran végzi az alábbi tevékenységket?
Kérjük x-el jelezze a megfelelő választ:

| | *naponta* | *hetente* | *havonta* | *évente* | *alkalom-szerűen* | nem tudom |
|---|---|---|---|---|---|---|
| Szabályozás frissítése és felülvizsgálata | | | | | | |
| hozzáférések felülvizsgálata | | | | | | |
| munkatársak tájékoztatása incidensekről | | | | | | |
| munkatársak oktatása incidens esetén követendő eljárásról | | | | | | |
| tudatosító képzések, gyakorlatok a munkatársak számára | | | | | | |
| tudatosító képzések, gyakorlatok a vezetők számára | | | | | | |
| továbbképzések, gyakorlatok az információbiztonsági felelős számára | | | | | | |

Milyen gyakran végzi az alábbi tevékenységket?
*Kérjük x-el jelezze a megfelelő választ:*

| | *naponta* | *hetente* | *havonta* | *évente* | *alkalom-szerűen* | nem tudom |
|---|---|---|---|---|---|---|
| információs eszközök/alkalmazások vizsgálata | | | | | | |
| a hardverek és szoftverek felülvizsgálata | | | | | | |
| biztonsági felülvizsgálat | | | | | | |
| teljes körű biztonsági mentés | | | | | | |
| az adatok biztonsági mentése | | | | | | |
| szoftverfrissítések letöltése | | | | | | |
| kémprogramkereső és -eltávolító programok frissítése | | | | | | |

Ön szerint az önkormányzat információbiztonsága érdekében mi a legfontosabb feladat?
Rövid szöveges válasz.

Védekezés

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

1=igen, vannak
2= nem, nincsenek
3= részben
4= nem tudom

Ha igen, akkor
melyek ezek? (szöveges válasz)

Rendelkeznek-e "Üzletmenet folytonossági Terv"-vel (BCP)

1=igen, van
2= nem, nincs
3= részben
4= nem tudom

Ha igen, akkor ki készítette? (szöveges válasz)

**Működik-e titkosítás a levelező rendszerhez kapcsolódóan?**

1 = igen
2 = nem
3= nem tudom

**Működik**-e jelszókezelési és módosítási protokoll az önkormányzatnál?

1 = igen
2 = nem
3 = nem tudom

**Külső eszközök, alkalmazások használata**

| | tilos | engedéllyel | szabadon használ-ható |
|---|---|---|---|
| Külső eszközök használata (adathordozók, tablet, notebook stb.) | | | |
| Közösségi alkalmazások használata | | | |

Szervezetének dolgozói vettek-e részt biztonságtudatosító oktatáson?

1=igen, többször is
2= nem, nem tudok róla
3= Csak figyelemfelhívás volt

**Működési tapasztalatok**

Van-e ismeretük informatikai eszközözeik elleni támadásokról, volt-e már ilyen incidensük?

igen, egyszer
igen, többször is
nem, nem tudok róla
nem tudok róla

Ha igen, akkor hogyan kezelték? (szöveges válasz)

Érte már támadás az önkormányzat honlapját vagy más közösségi alkalmazását?

igen, egyszer
igen, többször is
nem, nem tudok róla
nem tudok róla

Ha igen, akkor mi történt, hogyan kezelték? (szöveges válasz)

**Ha következett be incidens akkor az Ön véleménye szerint ennek mi volt a fő** oka?

Technikai felkészültség hiánya
IB folyamatok kidolgozatlansága, hiányos működése
Protokollok hiánya
Munkatársak felkészületlensége
Munkatársak figyelmetlensége
Szabályzatok be nem tartása

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

Tilos
Engedéllyel
Szabadon használható

Szükségesnek tartja-e a dolgozók rendszeres biztonságtudatosító képzését, oktatását?

1=igen

2= nem

3= csak önképzési formában

Ha igen, akkor ezt milyen gyakorisággal javasolja? (szöveges válasz)

Az önkormányzatnál alkalmazott IB módszerek / gyakorlat / tapasztalat:

Szöveges kifejtés

Az Ön tapasztalata szerint mi lehet eredményes az információbiztonság területén? Mit javasol?

Szöveges kifejtés

## Táblázatjegyzék



## Ábrajegyzék