Számadó, R. – Nagy, I.:

Kiberbizonytalanság

Mit tehetnek az önkormányzatok kiberbiztonságuk növelése érdekében?

Az önkormányzatok helyzete és tennivalók – gyakorlati megoldások, praktikák.

PERSPECTIVES OF LOCAL GOVERNMENTS IN CENTRAL–EASTERN EUROPE GYAKORLAT ÉS INNOVÁCIÓK

NEMZETKÖZI KONFERENCIA

III. Szekció – Önkormányzatok a digitális térben

2019. MÁRCIUS 5.

A kutatás indokoltsága

- Növekvő fenyegetés a kibertérből.
- A közszféra és az önkormányzatok különösen kitett a kibertámadásoknak.
- Az incidensek közel 80 %-át emberi hiba okozza (tudatosság hiánya, tájékozatlanság, hanyagság, szabályok be nem tartása, szándékos károkozás).
- Képzéssel, tudatosítással jelentősen javítható a kiberbiztonság.

Kutatás célja:

Önkormányzatok kiberbiztonsági helyzetének megismerése

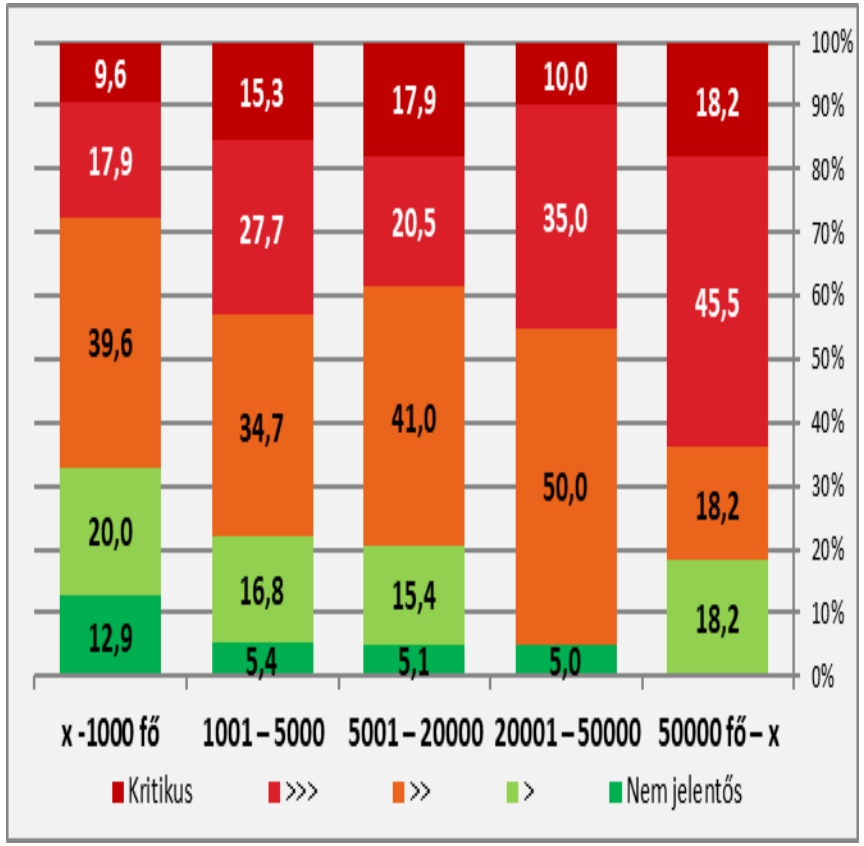
Online felmérés – fókuszcsoportos interjúk

- Megalapozó felmérés - 2018. január - február
- Teljes önkormányzati kör.
- 512 értékelhető válasz.
- Pontosítás fókuszcsoportos interjúkkal.

Vizsgált területek

1. Kiberfenyegetettség megítélése
2. Sebezhetőség
3. Felkészültség
4. Védekező képesség
5. Működési tapasztaltok

Kiberfenyegetettség megítélése

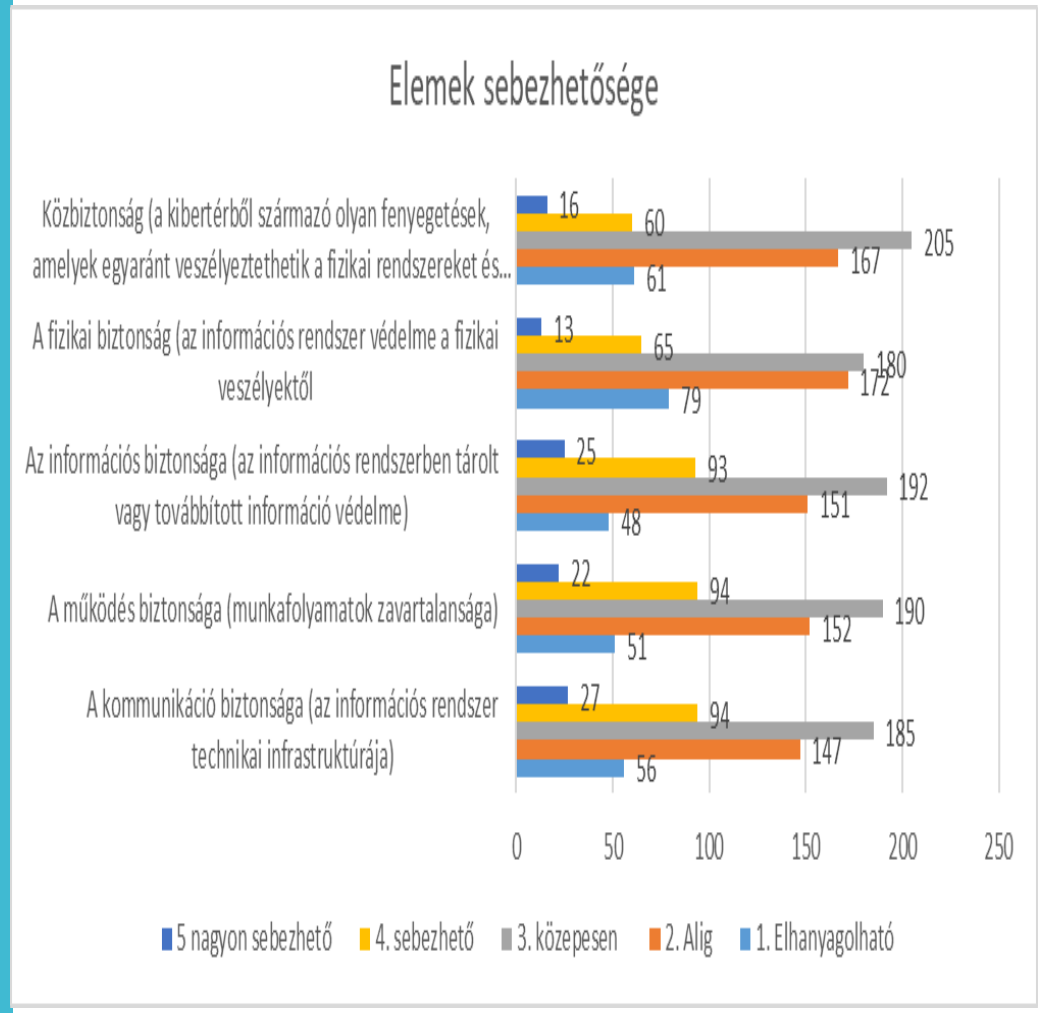


Ahhoz, hogy az önkormányzati szereplők megfelelő módon ítéljék meg a kiberfenyegetettség mértékét szükséges lenne:

- könnyen kezelhető, rövid, tömör és a laikus felhasználó számára is értelmezhető információs füzetekre, tájékoztató anyagokra;

- az önálló és a közös hivatalok székhely önkormányzatainál – ezek felhasználásával – legalább félévente egy – egy rövid (1- 2 órás) tájékoztatás/továbbképzés tartására (ezt tarthatná a rendszergazda, információbiztonsági felelős), fontos, hogy a vezetők is vegyenek részt ezeken az alkalmakon.

Sebezhetőségről alkotott vélemények



Sebezhetőség felismerésének segítése

- Információ a munkatársak részére a tudatosság növelésére:
  - a különböző szervezetek ellen elkövetett támadásokról, az incidensekről;
  - a támadás típusáról; hogyan valósult meg; mennyire volt sikeres a támadás – mennyire volt sikeres a védekezés, mi lehetett volna a megfelelő védekezés; honnan lehetett volna felismerni.
- Eszközök:
  - rendszeres tájékoztató csatorna pl. kormányzati hírlevél;
  - önkormányzati vezetők információval való ellátása.
- A vezetői elköteleződés elengedhetetlen. Kiemelten szükséges az önkormányzati vezetők képzése, tudatosítása, akár évente, az önkormányzati vezetők (különösen a jegyzői kör) kötelező képzése keretében.

Felkészültség

- 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.
- Az számítógépek és szoftverek állapotáról és a frissítésről már kevésbé volt pozitív a válaszadók véleménye. 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. A legelavultabb és nem frissített szoftverállományt a tag hivatalok válaszadói jelezték, 61,7%.
- A munkatársak felkészültségével és motivációjával kapcsolatban igen rossz eredmények születtek.
- A válaszadók szerint a munkatársak inkább nem felkészültek. Hivataltípustól függetlenül 28–33,1%-os arány lett az eredmény.

Felkészültség javítása

Segíthet, ha az önkormányzatok

- központi IT menedzsmentet valósítanak meg;
- kétszintű azonosítást vezetnek be;
- vezessék be a napi biztonsági mentést, ami két külön helyre menti le az adatokat titkosított kapcsolaton keresztül;
- dolgozzanak ki és alkalmazzanak védekező és reagáló képességet támogató eljárásrendeket.

Fontos, hogy az Internetre kapcsolt munkaállomások, szerverek és egyéb Internet alapú eszközök naprakészen legyenek tartva a vírusadatbázisok, Windows és Linux biztonsági frissítések aktualizálva legyenek.

Fontos:

- Jogosultság kezelés.
- Szabályok betartásának ellenőrzése.

Védekező – reagáló képesség

- 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 feladatok kiszervezéséhez kapcsolódó szabályozók 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.

Védekező képesség javítása

Alkalmazások védelme

- Könnyen leírható, de nehezen kitalálható jelszóval ellátni a védeni kívánt alkalmazásainkat (pl: E-mail, facebook, telefon, számítógép, tablet).
- A jelszavakat bizonyos időközönként (havonta, két havonta) változtassuk meg.
- Soha ne bízzuk másra a jelszavainkat!
- A hozzáféréseinkről vezessünk biztonságos helyen tartott nyilvántartást.
- Ne egy jelszót használjunk minden eszközünkhöz, hanem legyen több kombinációnk (legalább 6-7).
- Ha egy jelszót már megadtunk valamely alkalmazásunkhoz 3-4 hónap múlva ne újra ugyanazt a jelszót adjuk meg azért, mert arra emlékszünk.

Böngészők védelme

- Böngésző programoknál például Opera,Firefox ESR verziója megfelelően telepített reklám szűrőkkel.
- Egyszerű ellenőrző lista munkatársak részére
- Minta információbiztonsági ellenőrző lista az önkormányzati információbiztonság biztosításában résztvevő munkatársak részére[4] (mellékelteben részletesen).

Működési tapasztalatok

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 mobileszközök használatával kapcsolatos válaszok:

Csupán néhány %-ban jelezték, hogy tilos használni egyéb eszközöket;

a 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.

Használati praktikák

- Fontos, hogy az eszközök - ha lehetséges - ne állandóan „lógjanak” a neten csak akkor, amikor szükség van rá.
- Telefon esetében is csak azokat az alkalmazásokat használjuk, aminek a származásában biztosak vagyunk és akkor amikor szükség van rá. Ha befejeztük a munkát az adott alkalmazással akkor zárjuk be.
- A problémák is akkor lépnek fel amikor nem tartunk „rendet” a eszközeinken (pl.: nem zárjuk be a nem használt alkalmazást, jelszó nélkül lépünk be gépünkre vagy nem megbízható forrásból telepítünk alkalmazásokat pl:játékot).
- Ez főleg akkor veszélyes, amikor olyan személynek adjuk át az eszközeinket, akiben feltétel nélkül megbízunk (gyerekünk, jó ismerős) és az adott személy még a legnagyobb jóindulata ellenére is hibát követ el.

Összegzett megállapítások

- A teljes közszférára és az önkormányzati szektor nem a megfelelő helyen és szinten kezeli az információbiztonságot.
- Informatikai kérdésként kezelik, miközben a megfelelő működés érdekében az információbiztonságnak a szervezeti kultúra részének kellene lennie, vagyis tudatosság szükséges.
- A vezetők (polgármester, jegyző és képviselők) elkötelezettsége, tudatossága nélkül az önkormányzati hivatalokban nem biztosított a kérdés megfelelő szinten való kezelése.
- Szükséges a tudatosság növelése, a képzésfejlesztés. Ezt nemcsak az IT szakemberekre, hanem a munkavállalók teljes körére is ki kell terjeszteni a reziliecia növelése érdekében.
- Könnyen megvalósítható megoldások és iránymutatások betartatásával nagyrészt elkerülhetök lehetnek az informatikai incidensek.
- Az informatikai rendszer biztonságos üzemeltetéséhez elengedetlen a kollégák „házon belüli” továbbképzése.
- Megfelelő működéshez szükség van naprakész informatika szabályzatra, információ biztonsági szabályzatra, üzemeltetési dokumentációra és kijelölt személyekre, akik ezeket naprakészen tartják.