INFORMÁCIÓBIZTONSÁG ÉS ADATVÉDELEM A GYAKORLATBAN – EGY ORSZÁGOS FELMÉRÉS ÉS JEGYZŐI INTERJÚK TAPASZTALATAI

Balatoni Péter[1] – Varga János[2]


Az önkormányzati hivataloknak az elmúlt két évben több nagy kihívással kellett megküzdeni, témánk szempontjából a legfontosabbak az alábbiak voltak:

- csatlakozás az önkormányzati ASP rendszerhez, a régi, lokális rendszerek felszámolása (migrálás, archiválás);
- az elektronikus ügyintézés bevezetése;
- az Európai Parlament és a Tanács EU 2016/679 rendelete (általános adatvédelmi rendelet) követelményeinek teljesítése;
- a fentieknek megfelelő új információbiztonsági követelmények bevezetése.

Az ASP-rendszerhez történő csatlakozás nem csak egy számítógépes program cseréjét jelentette számukra, hanem egy teljesen új ügyviteli, technikai környezetre történő áttérést, ami természetesen a hivatal belső szabályzatainak felülvizsgálatát, a munkafolyamatok szervezésének a módosítását, fejlesztését is megkövetelte. Ebben az információbiztonságnak kiemelt szerepe volt és van.

- Az ASP-csatlakozásnak kiemelt feltétele a rendszert működtető Magyar Államkincstár által meghatározott biztonsági intézkedések helyi szabályzatokba történő beépítése és következetes végrehajtása.[3]
- Az elektronikus ügyintézést veszélyeztető biztonsági incidensek a hivatalok teljes működését akadályozhatják, az ügyintézői elektronikus rendszerek védelme tehát a hivatalok működőképességének alapfeltétele lett.
- Az adatvédelem központi feladata a biztonságos adatkezeléshez, illetve adatfeldolgozáshoz szükséges műszaki és szervezési intézkedések meghatározása és végrehajtása.[4]
- Az ügyvitel szinte teljes körű elektronizálása következtében a hivatali munka szabályozásában mindenütt megjelennek az informatikai feltételek és követelmények (iratkezelés, munkavédelem, vagyonvédelem, gazdálkodás, közzétételi tevékenység stb.).

Az információbiztonság e központi szerepét szem előtt tartva az Okos Önkormányzat Akadémia szakértői munkacsoportja 2017-ben és 2018-ban felmérést végzett annak megállapítására, hogy az önkormányzati hivatalok hogyan felelnek meg az állami és önkormányzati szervek elektronikus információbiztonságáról szóló a 2013. évi L. törvény (a továbbiakban: Ibtv.) rendelkezéseinek. A felmérést a portálunkon kitölthető, rövid, a legfontosabb kérdésekre fókuszáló kérdőívvel végeztük, melyet 2018 évben 16 nyugat-dunántúli önkormányzati hivatal jegyzőjével különböző időpontokban lefolytatott interjúsorozat egészített ki.

A kérdőív a két jelzett évben nem volt teljesen azonos, 2018-ban azt az adatvédelemre vonatkozó kérdésekkel egészítettük ki, egyúttal néhány kevésbé aktuális kérdés elhagyásra került. A kérdések az alábbiak voltak:

Kérdőív az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, valamint a 2016/679 általános adatvédelmi EU rendelet (GDPR) végrehajtásának helyzetéről

1. *Van-e a hivatalban jelenleg az informatikai biztonságért felelős személy?*
   Igen, kinevezett belső munkatárs.
   Igen, megbízott külső személy, vagy vállalkozó.

[1] Mérnök informatikus, rendszerszervező. Az OKOS Önkormányzat Akadémia és a Dokumentumtár.hu Országos Dokumentumküldő és Adatgyűjtő Rendszer alapító tagja. 8 évig volt az Egyesület az Információs Társadalomért elnöke. Több mint 20 éve dolgozik országos hatáskörű szervek, önkormányzati hivatalok, jogszabályból eredő informatikai feladatainak támogatásában.

[2] Mérnök-közgazdász, rendszerszervező. Több évtizedes tapasztalattal rendelkezik önkormányzati informatikai rendszerek fejlesztésében, bevezetésében és üzemeltetésében. Az Okos Önkormányzat Akadémia szakértői konzorcium egyik alapítója, ennek keretében végez tanácsadói munkát az információbiztonság és az adatvédelem aktuális önkormányzati feladatainak megoldásában.

[3] Magyar Államkincstár: *Tájékoztatás az önkormányzati ASP rendszerekhez csatlakozáshoz megvalósítandó informatikai biztonsági követelményekről*, Verziószám: 2.0 Kiadás dátuma: 2018. 06. 18.

[4] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) 2. szakasz: Adatbiztonság.

Jelenleg, átmenetileg nincs informatikai biztonsági felelős, keressük a megoldást.
Nincs, és korábban sem volt informatikai biztonsági felelősünk.

2. *Meghatározták-e a hivatal mint szervezet előírt biztonsági szintjét?*
Igen, és az előírt biztonsági szintet már elértük.
Igen, de még nem értük el az előírt szintet.
Nem, még nem határoztuk meg.
3. *Elvégezték-e a hivatal által használt informatikai rendszerek osztályba sorolását?*
Igen, és eleget tettünk a törvény által előírt felülvizsgálati kötelezettségeinknek.
Igen, de már több mint 3 éve nem vizsgáltuk felül őket.
Nem, még nem végeztük el az informatikai rendszerek osztályba sorolását.
4. *Rendelkezik-e a hivatal hatályos informatikai biztonsági szabályzattal?*
Igen, és az alapján végezzük a feladatainkat.
Igen, de a mindennapi munkában nem tudjuk kellően hasznosítani.
Nem, nem készült még ilyen szabályzat.
5. *Az informatikai biztonsági ismereteket oktatják-e évente az érintett munkatársaknak?*
Igen, minden évben van ilyen oktatás.
Nem minden évben, de volt már ilyen oktatás.
Nem volt még ilyen jellegű oktatás.
6. *A nemzeti elektronikus információbiztonsági hatóság tartott-e már ellenőrzést a hivatalukban?*
Igen.
Nem.
7. *Megnyugtatónak érzi-e a hivatal informatikai biztonsági helyzetét?*
Igen, a kockázatokat ismerjük, a szükséges intézkedéseket megtettük.
Részben: vannak még nem kezelt kockázatok, de ismerjük őket, és elfogadott cselekvési terv alapján dolgozunk a megoldásukon.
Nem, mert nem ismerjük elég alaposan a biztonsági helyzetünket, és az informatikai biztonság érdekében szükséges teendőinket.
8. *Igényelne-e segítséget az informatikai biztonság kezeléséhez?*
Távoktatást a törvény által meghatározott feladatokról.
Segédleteket a törvény által meghatározott feladatok ellátásához.
Konferenciát az informatikai biztonságot érintő aktuális feladatokról (pl. ASP csatlakozással, elektronikus ügyintézéssel összefüggésben)
Tájékoztatást az informatikai biztonsági felelős feladatainak szolgáltatás formájában történő ellátásáról.
9. *Jelenleg van-e a hivatalnak a gdpr-nek megfelelő adatvédelmi tisztviselője?*
Igen, külső személy.
Igen, hivatali dolgozó.
Nincs.
10. *Az adatvédelmi kötelezettségek közül mely(ek) megoldásához igényelne támogatást?*
Szabályzat készítéséhez.
Adatvédelmi nyilvántartásokhoz.
Adatvédelmi tájékoztató összeállításához.
Folyamatos szakmai támogatáshoz, oktatáshoz.
Nem igénylek támogatást.
11. *Amennyiben szüksége van támogatásra, milyen formában venné azt igénybe?*
Belső adatvédelmi tisztviselő folyamatos szakmai támogatása (költségkímélő megoldás).
Külső adatvédelmi tisztviselő megbízása (költségesebb megoldás).

Az információbiztonság és az adatvédelem helyzete a kérdőívek alapján

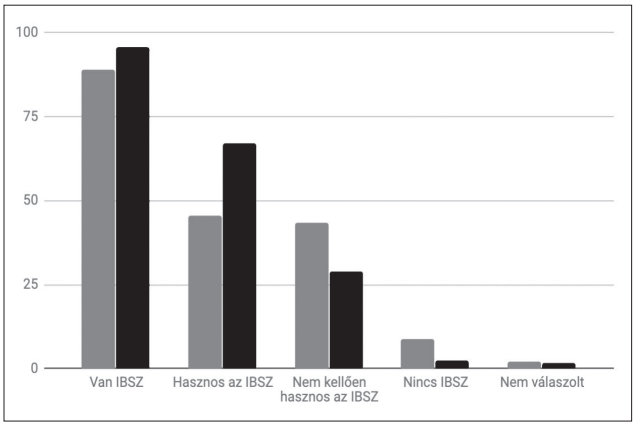
A felmérések az OKOS Önkormányzat Akadémia céljait a válaszadók száma tekintetében teljesítették, hiszen a 2017-es évben a jegyzők 10%-a, a 2018-as évben pedig a jegyzők több mint 13%-a válaszolt.

A felmérés nem tekinthető reprezentatívnak, mivel a kitöltésnél nem volt cél többek között a különböző típusú hivatalok egyenlő arányú szerepeltetése, viszont a válaszok jelentős mennyisége miatt mégis átfogó képet kapunk az információbiztonsággal és az adatvédelemmel kapcsolatos felkészültség fokáról.

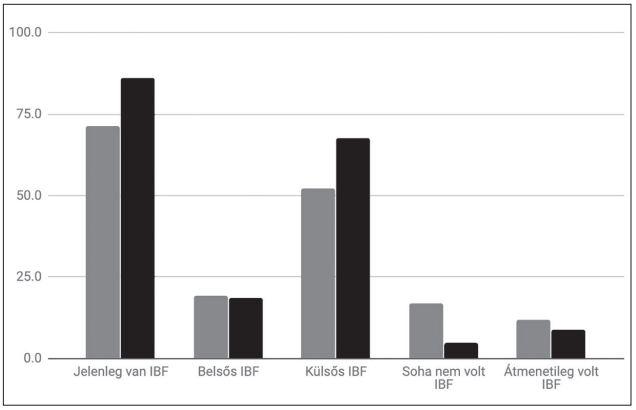
A felmérés információbiztonsággal kapcsolatos kérdéseit 2017-ben és 2018-ban is feltettük, így azokkal kapcsolatban növekvő tendencia rajzolódik ki, mind a felelősök, mind a szabályzatok aránya tekintetében.

A megbízott információbiztonsági felelősökkel rendelkező hivatalok aránya 71%-ról 86%-ra nőtt 2018-ra, így gyakorlatilag majdnem minden hivatalban van információbiztonsági felelős.

Hasonlóan mindkét vizsgált évben, az információbiztonsági felelősök 19%-a belső munkatárs, a külső megbízottak aránya viszont jelentősen megnövekedett 52%-ról közel 68%-ra.



1. ábra
Az információbiztonsági felelőssel kapcsolatos kérdésekre adott válaszok a válaszadók százalékában első oszlopban a 2017-es, a másodikban a 2018-as adatokkal



2. ábra
Az informatikai biztonsági szabályzattal kapcsolatos kérdésekre adott válaszok a válaszadók százalékában első oszlopban a 2017-es a másodikban a 2018-as adatokkal

A fenti arányok vélhetően az ASP források biztosításának hatására emelkedtek.

Jelentősen növekedett az informatikai biztonsági szabályzatok száma is, míg 2017-ben a hivatalok 89%-a rendelkezett szabályzattal, addig 2018-ban ez az arány közel 96%-ra nőtt. A szabályzatok napi használatát nem garantálja a szabályzatokkal lefedett hivatalok magas aránya. 2018-ban a megkérdezett jegyzők 67%-a ítélte hasznosnak a szabályzatot, közel 29%-uk nem ítélte kellően hasznosnak. A fentiek szerint a hivatalok közel harmadában nagy valószínűséggel nem használják a szabályzatot.

Az információbiztonsági feladatok egyik visszatérő eleme az oktatás. Az információbiztonsági tárgyú oktatások száma 49%-ról közel 74%-ra emelkedett, viszont 2018-ban annak ellenére, hogy a hivatalok jelentős része rendelkezik információbiztonsági felelőssel, 25%-uknál nem volt oktatás. Az oktatás hiánya mellett érdekes adat, hogy közel 38%-uknál volt minden évben oktatás, a többi válaszadónál az oktatás egyszeri alkalmat jelentett.

A Nemzeti Elektronikus Információbiztonsági Hatóság ellenőrzései mindkét vizsgált évben közel azonos arányban a hivatalok 6%-át érintették.

Az adatvédelmi feladatok támogatásának vizsgálata 2018-ban került be a felmérésbe. A válaszadók közel 51%-ának van adatvédelmi tisztviselője, ebből közel azonos arányban, azaz 26%-ban belső munkatárs, 24%-ban pedig külsős szakértő látja el a feladatokat.

Az információbiztonság és az adatvédelem jegyzői interjúk tükrében

Az interjúkhoz használt kérdéssor a kérdőívekhez képest lényegesen terjedelmesebb és részletesebb volt, és felölelte az önkormányzati hivatal információbiztonsági tevékenységének teljes körét, az Ibtv. végrehajtása érdekében bevezetett adminisztratív, logikai és fizikai védelmi intézkedéseket. A kb. egy órányi időtartamú interjúkat jellemzően községi közös önkormányzati hivatalokban, illetve kisebb polgármesteri hivatalokban végeztük 2018 első félévében. Valamennyi érintett hivatal csatlakozott már ebben az időben az önkormányzati ASP-rendszerhez, és régi, lokális rendszereiket folyamatosan kivezetve a napi feladataik ellátásához már a központilag biztosított modulokat és szolgáltatásokat használták. Az interjúk összegzése során csaknem azonos informatikai helyzetet és biztonsági problémákat sikerült azonosítanunk, melyek a kritikus pontokon megegyeztek a kérdőíves felmérés eredményeivel is.

Az érintett körben az információbiztonsági feladatok formálisan minden esetben teljesítettek voltak, vagy – tekintettel a folyamatban lévő, az ASP bevezetéséhez kapcsolódó pályázatokra – már ismert határidőre teljesültek. A *„formális teljesítés”* alatt azt értjük, hogy ugyan van szabályzat, vannak szabályozott eljárások, de a mindennapi munkában még nem tudatosultak az ezekben megfogalmazott követelmények. Ennek egyik fő okát abban látták a megkérdezett jegyzők, hogy az informatikai biztonsági szabályzatokat kezdetben – jobb híján – a helyi önkormányzati sajátosságokat korlátozottan figyelembe vevő, indokolatlanul terjedelmes sablonok alapján készítették, ezért a leírtak értelmezése, végrehajtása a hivatal munkatársai számára nem volt egyszerű feladat. A kötelező biztonsági intézkedések végrehajtását a kisebb hivatalokban nehezítette az is, hogy a rendszergazda szolgáltatás a rendelkezésre álló forrásokból csak korlátozottan beszerezhető, gyakran kizárólag a számítástechnikai eszközök eseti javítására korlátozódik, így számos nélkülözhetetlen feladat (helyi jogosultságok kezelése, szoftverek biztonsági frissítése stb.) elvégzése késedelmet szenved, vagy meg sem történik. A felmérés idején a helyi számítógépeken a felhasználói fiókok általában rendszergazda jogosultságúak voltak, ami a kártékony (pl. az e-mail csatolmányokban érkező) szoftverek akaratlan telepítésének állandó veszélyét hordozza magában. Erről a veszélyről azonban a felhasználók általában nem is tudtak, mivel az előírt éves biztonságtudatosságot fejlesztő oktatást jellemzően nem tartották meg.

Fentiek ellenére a biztonsági helyzet kifejezetten jónak értékelhető, az érintett körben a megelőző öt évben mindössze egy olyan biztonsági incidens történt, amit a hatóságnak be kellett jelenteni. Ez az incidens egyébként egy külső szolgáltatónál bekövetkezett szolgáltatás kiesés és súlyos adatvesztés volt, mellyel kapcsolatban legfeljebb a szolgáltatási szerződést illetően lehetett a hivatallal szemben kifogást emelni. A hivatalok többsége rendelkezik valamilyen vírusvédelmi szoftverrel vagy megoldással, a felhasználóknak pedig a munka mellett idejük sincs az esetlegesen veszélyt jelentő internetes aktivitásra.

Az ASP-csatlakozás során a pályázati lehetőségeknek köszönhetően megújult a hivatalok gépparkja, infrastruktúrája. A központi szolgáltatás nagyrészt mentesíti a hivatalokat a helyi mentésektől, az adatvesztés lehetősége minimális. Az ASP bevezetésével új szintre emelkedett a hivatalok elektronikus információs rendszereinek biztonsága, egyúttal jelen-

tős tehertől szabadultak meg a hivatalok a helyi, biztonsági szempontból is elavult rendszerek megszüntetésével. Ezzel együtt elérkezett az idő az informatikai biztonsági szabályzatok és a biztonságszervezés hivatali gyakorlatának a felülvizsgálatára, melynek során az alábbi követelmények szem előtt tartását javasoljuk:

- Az informatikai biztonsági szabályzatot olyan szakszerű, de közérthető megfogalmazásban kell elkészíteni, hogy azt a jegyző és a szabályzattal érintettek megértsék.
- A szabályzat csak az adott hivatalban ténylegesen végrehajtandó, konkrét intézkedéseket tartalmazza.
- A szabályzathoz célszerű elkészíteni egy közérthető, lényegre törő kivonatot, *„házirendet"* a számítógépet használó ügyintézők részére, amely konkrétan tartalmazza a tiltott tevékenységeket, illetve a számítógép használata során betartandó fő szabályokat.
- Az informatikai biztonsági házirendet minden évben kötelező oktatni és az ismeretét számon kell kérni – ennek célszerű formája az on-line rövid videóelőadásokra épülő, esetleg játékos formában megoldott ismeretátadás és tesztkitöltés. Az éves oktatás kötelező jellegét a szabályzatban is rögzíteni kell.
- Az érintett vezetők és kulcsszereplők (jegyző, aljegyző, rendszergazda) részére az elektronikus információs rendszerek biztonságáért felelős személy évente tartson továbbképzést.

Hogyan felelhetnek meg a kis hivatalok az információbiztonsági és adatvédelmi kihívásoknak?

A fenti követelmények megvalósítása, bevezetése és folyamatos fenntartása komplex feladat.

A kis hivatalok nehezen oldják meg az információbiztonsággal és az adatvédelemmel kapcsolatos feladataikat is, de sokszor problémát jelentenek, vagy irreálisan sok energiát emésztenek fel olyan feladatok, mint a korábbi regisztrációval a központi rendszerhez csatlakozott önkormányzatok kapcsolása az ASP-rendszerhez, vagy az elektronikus ügyintézés kérdései.

Az információbiztonsági és adatvédelmi feladatok megoldására az alábbi lehetőségek állnak a hivatalok rendelkezésére:

- Belső munkatársak részvételével és szakértelmével, hivatali időben oldják meg a feladatokat. Ez a megoldás városi hivatalok esetében valódi megoldási lehetőség, a kis hivatalok esetében elvi lehetőség marad, hiszen sok helyen nincs erőforrás ezen feladatok hivatalon belüli megoldására.
- Külső szakértők bevonásával a feladatok teljes körű megoldása és folyamatos követése költségigényes, így a nagy ráfordítás miatt elvi lehetőség marad ez is a kis hivatalok tekintetében.

Hogy lehet mégis megoldani a jogszabályi kötelezettségeket?

Három szempontot kell figyelembe venni, melyekkel a feladatok megoldása olcsóbbá és mégis magas színvonalon tarthatóvá válik:

- Priorozálás
  Az információbiztonsággal és az adatvédelemmel kapcsolatos jogszabályokat nemcsak kis önkormányzati hivatalok, hanem országos hatáskörű szervek működésének szabályozására alkották. Sok olyan feladat került szabályozásra, ami kis önkormányzatoknál nem releváns. Ezeket a feladatokat nem kell elvégezni, nem kell szabályozni, nem kell oktatni.
- Szabványosítás
  Minden önkormányzati hivatal néhány kategóriába besorolható az információbiztonsággal és az adatvédelemmel kapcsolatos felkészültségi szintje tekintetében. A különböző kategóriák szerinti hivatalok feladatai nagyon hasonlóak, így nem kell külön, eltérő szabályozást bevezetni minden hivatalnak, lehet olyan megoldást és jó gyakorlatokat igénybe venni, amelyek máshol már jól beváltak. A feladatellátás hasonlósága miatt a közösségen belül felmerült problémát célszerűen közre lehet adni, hogy máshol ne okozzon gondot, így a feladatellátás és a problémák megoldása is hatékonyabb lehet.
- Automatizálás
  Ha hasonló feladatokat végzünk, akkor automatizálással, például online oktatással és az oktatással kapcsolatos értesítések és ellenőrzések automatikus kiküldésével nagy mennyiségű emberi munka szabadul fel.

Az automatizálás, a szabványosítás és a jó gyakorlatok közreadása is jellemzően közösségi szinten nyújt előnyöket, közösségi szinten értelmezhetők.

A jegyzők közösségének erejét kihasználva az OKOS Önkormányzat Akadémia szakértői konzorciuma célja, hogy egyszerű eszközökkel, közérthetően, kis önkormányzati hivatalok számára nyújtson támogatást, ezért 2019 márciusától egy minden jegyző számára ingyen elérhető regisztrációhoz kötött online tudásanyagot adunk közre videók formájában az okosonkormanyzat.hu oldalon, amelyen keresztül a jegyzők

- tájékozódhatnak az információbiztonság és az adatvédelem kérdéseiről,
- választ kaphatnak aktuális, a közösségen belül felmerült feladatok gyors megoldására,
- tájékozódhatnak például a hatósági vizsgálatok menetéről és az elkerülésük módjáról.

A kis önkormányzati hivatalok jegyzői előtt álló komplex feladatok megoldásához és a feladatmegoldás hatékonyságának növeléséhez csak a jegyzők közösségén keresztül vezet út. Küldetésünk az, hogy ezt az utat a jegyzők számára elérhetővé tegyük és a célok elérését megkönnyítsük.