A 37/2016(11.24.) határozat melléklete

GKI digital
Kutató és Tanácsadó Kft.

Informatikai szabályzatok felülvizsgálata a Sajószentpéteri Polgármesteri Hivatal számára

2016. március

GKI digital
Kutató és Tanácsadó Kft.

A GKI csoport tagja

H-1092 Budapest Ráday utca 42-44. III. emelet

telefon: +36 1 318 1284 / 128
fax: +36 1 318 4023

Kapcsolat:

Madar Norbert | üzletágvezető
madar@gkidigital.hu
+36 30 541 0905

Timár Szabolcs | ügyvezető
timar@gkidigital.hu
+36 70 331 5843

1 Bevezetés

1.1 Előzmények

A 2013. évi L. törvény részletesen szabályozza az állami és önkormányzati szervek elektronikus információbiztonságát. A törvény részletes leírást tartalmaz az önkormányzatok számára kötelezően megvalósítandó tevékenységekről, szabályzatokról, valamint azok kötelező felülvizsgálatáról.

Az informatikai rendszerek folyamatos változásából kifolyólag az informatikai szabályzatokkal kapcsolatosan általános elvárás, hogy azokat évente egyszer felülvizsgálják, mind a vonatkozó törvényi szabályozásnak való megfelelés, mind annak a valóban használt megoldásokhoz való aktualitása miatt.

A fenti feladat elvégzése céljából a Sajószentpéteri Polgármesteri Hivatal a GKI Digital Kft.-t bízta meg a Hivatal informatikai szabályzatainak éves felülvizsgálatára.

A vizsgálat során az elvégzendő feladatok az alábbiak voltak:

- A Hivatal jelenlegi informatikai szabályzatainak felülvizsgálata, a törvényi megfeleléshez szükséges javítások elvégzése.
- A törvény hatályos változata értelmében feladatlista készítése, mely biztosítja a Hivatal számára a törvényi megfelelést.

1.2 A felülvizsgálat szempontjai

A hivatkozott törvényi előírásnak megfelelően az informatikai szabályzatok vizsgálata az alábbi területekre terjedt ki:

- jogszabályi megfelelés;
- a biztonsági besorolásnak való megfelelés;
- szabályozott területek köre;
- felelősségi körök meghatározása;
- szükséges informatikai jellegű stratégiák megléte.

Az informatikai szabályzatok felülvizsgálata során kizárólag a fenti szempontok vonatkozásában vizsgáltuk a Hivatal írott szabályzatait, az abban foglalt eljárásrendeknek – pl. megfelelő dokumentáció tényleges vezetése – gyakorlati alkalmazásának ellenőrzése nem képezte jelen vizsgálat tárgyát.

2 Elvárások az informatikai szabályzattal szemben

A polgármesteri hivatalok esetében az informatikai szabályzatokkal szembeni részletes elvárást a 2013. évi L. törvény alapján elkészített informatikai biztonsági besorolás szintje határozza meg. Éppen ezért a következőkben összefoglaljuk, hogy milyen biztonsági besorolása van a Sajószentpéteri Polgármesteri Hivatalnak és ez milyen elvárásokat támaszt az informatikai szabályzatokkal szemben.

2.1 A Hivatal informatikai biztonsági besorolása

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 7. § (1) bekezdése kimondja, hogy az elektronikus információs rendszereket biztonsági osztályba kellett sorolni. A hivatal jelenleg 14 olyan informatikai rendszert használ, melyek vonatkozásában az értékelést el kellett végezni. A hivatal elektronikus információs rendszerei az alábbi biztonsági osztályokba tartoznak.

Rendszer megnevezése	Rendszer biztonsági osztálya
EPER	3
KGR	2
E-kata	1
Bérleti díj	2
Lakbér	2
Wonkadó	3
KIR3	2
WINSZOC	3
Telephely engedély	2
Szabálysértés	2
Működési engedély	1
Szálláshely	1
Complex jogtár	1
ÉTDR	2

A hivatalra vonatkozóan a 2013. évi L. törvény és a vonatkozó végrehajtási rendeleteknek megfelelően az elvárt biztonsági szint: 3.

2.2 Elvárások az informatikai biztonsági besorolás alapján

Az informatikai szabályzatokkal szemben alapvető elvárás a különböző területekre vonatkozóan:

- megfelelő eljárásrendek leírása;
- felelősök, jogkörök meghatározása;
- szabályozott területek pontos meghatározása;
- dokumentálás módjának meghatározása.

Az informatikai szabályzatoknak a megfelelő biztonsági szint elérése szempontjából a hivatkozott törvény szabályozása értelmében három fő területen kell megfelelnie, illetve területenként elérni a szükséges szintet, tartalmat:

- adminisztratív elvárások,
- fizikai védelem szabályozása,
- logikai védelem szabályozása.

Az informatikai szabályzat felülvizsgálata során elsősorban a fentieknek való megfelelést vizsgáltuk. Emellett természetesen szem előtt kell tartani, hogy az informatikai rendszerek, hálózat felépítésének megváltozása során igényel-e a szabályzat módosítást, pontosítást, valamint a jelenlegi intézkedések megfelelnek-e az utolsó felülvizsgálat óta hatályba lépett jogszabályi előírásoknak.

3 Változások a jogszabályi környezetben

2015 márciusa, azaz az informatikai szabályzat utolsó felülvizsgálata óta az alábbi, a 2013. évi L. törvényt érintő módosítások léptek hatályba 2015.07.16-i dátummal:

- 187/2015. (VII. 13.) Korm. rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról
- 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól
- 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
- 42/2015. (VII. 15.) BM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének rendjéről

A fentiekkel párhuzamosan a következő jogszabályokat helyezték hatályon kívül:

- 233/2013. (VI. 30.) Korm. rendelet az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről
- 301/2013. (VII. 29.) Korm. rendelet a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról
- 77/2013. (XII. 19.) NFM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről

- 73/2013. (XII. 4.) NFM rendelet az elektronikus információbiztonságról szóló törvény hatálya alá tartozó egyes szervezetek hatósági nyilvántartásba vételének, a biztonsági események jelentésének és közzétételének rendjéről

A változások alapvetően a következő 3 területet érintették:

- szervezeti változások;
- hatósági adatszolgáltatás változása;
- biztonsági osztályba sorolás, biztonsági szintbe sorolás követelményeinek változása.

Az érintett jogszabályi változások hatásai az egyes területek vonatkozásában a következők.

3.1 Szervezeti változások

A 2014-es kormányzati átalakítás eredményeként már a korábbiakban a Belügyminisztériumhoz került a Nemzeti Biztonsági Felügyelet (korábbiakban: KIM), valamint a Nemzeti Elektronikus Információbiztonsági Hatóság (korábbiakban: NFM, továbbiakban: NEIH).

Az információbiztonsági törvény és annak végrehajtási rendeleteinek módosításával a Nemzeti Biztonsági Felügyelet sérülékenységvizsgálati szakhatósági feladatköre megszűnt, azt a Nemzetbiztonsági Szakszolgálat vette át.

A NEIH 2015. január 1-jétől a Belügyminisztérium főosztályaként tevékenykedett. Ezt a feladatkört mostantól szintén a Nemzetbiztonsági Szakszolgálat veszi át.

3.2 Hatósági adatszolgáltatás változása

A korábbiakban lehetősége volt a szervezetnek az Ibtv. 15. § (3) bekezdése szerinti adatokat ÁNYK űrlapon, elektronikusan aláírt elektronikus levélben, vagy postai úton is megküldeni a hatóság részére.

Az új szabályozás (42/2015. BM rendelet) szerint erre kizárólag elektronikus űrlap szolgáltatás igénybevételével a hatóság elektronikus adatbejelentési felületén kerülhet sor.

Fontos változás, hogy idáig az Ibtv. 15. § (1) bekezdése szerinti, az elektronikus információs rendszerek külön jogszabályban meghatározott technikai adatainak megküldésére vonatkozóan nem volt kötelezően meghatározott formai és tartalmi követelmény (a hatóság segédletet tett közzé a honlapján), mostantól ezeket az adatokat a hatóság által meghatározott formában kell megküldeni.

Az új szabály szerint elsőként a szervezet regisztrálja be az elektronikus információs rendszerek biztonságáért felelős személyt (továbbiakban: IBF), majd az IBF jelenti be a szervezetet.

A szervezet vezetőjének a feladata, hogy az így kapott regisztrációs űrlap hitelesített példányát biztonságos elektronikus kézbesítési szolgáltatás útján, vagy postai úton megküldje a hatóság számára.

Az új rendelet hatályba lépése előtt regisztrált szervezeteknek nem kell újra regisztrálniuk magukat.

3.3 Biztonsági osztályba sorolás, biztonsági szintbe sorolás követelményeinek változása

A legfontosabb változást a szervezetek biztonsági szintbe sorolásának a módja jelenti.

A törvény alapján valamennyi hatálya alá tartozó szervezetnek biztonsági szintbe kell sorolnia szervezetét és a megállapított biztonsági szinttől függően adminisztratív és fizikai védelmi intézkedéseket kell bevezetnie.

A korábbiakban az Ibtv. definiálta az egyes szervezetek minimális biztonsági szintjét, valamint azt, hogy legalább a legmagasabb biztonsági osztályba sorolt elektronikus információs rendszerével azonos biztonsági szinttel kellett, hogy megegyezzen.

A módosítást követően a fenti módszertant megszűntették, mostantól az elektronikus információs rendszerek felhasználásának a módja határozza meg egy szervezet biztonsági szintjét.

Változás továbbá, hogy az új szabály szerint nem csak a szervezetet, hanem a következő szervezeti egységeket is biztonsági szintbe kell sorolni. Az elektronikus információs rendszer

a) fejlesztését végző,
b) üzemeltetését végző,
c) üzemeltetéséért felelős vagy
d) információbiztonságáért felelős szervezeti egységek.

Ennek alapján **2-es a biztonsági szintje** a szervezetnek, amely **személyes adatokat kezel,** és a szervezet **jogszabály alapján kijelölt szolgáltatót** vesz igénybe.

> *Jogszabály alapján kijelölt szolgáltató lehet a központosított informatikai és elektronikus hírközlési szolgáltatásokról szóló 309/2011. (XII. 23.) Korm. rendelet alapján a Nemzeti Infokommunikációs Szolgáltató Zrt. (továbbiakban: NISZ) vagy az önkormányzati ASP központról és a közfeladatot ellátó szervek iratkezelésének általános követelményeiről szóló 335/2005. (XII. 29.) Korm. rendelet módosításáról szóló 62/2015. (III. 24.) Korm. rendelet alapján szintén a NISZ, illetve a Magyar Államkincstár.*

3-as a biztonsági szintje annak a szervezetnek, amely a szakfeladatait támogató elektronikus információs rendszert használ, **de nem üzemelteti azt.** A szervezet **kritikus adatot,** nem minősített, de közérdekű, vagy közérdekből nyilvános adatot kezel, központi üzemeltetésű, és több szervezetre érvényes biztonsági megoldásokkal védett elektronikus információs rendszerek vagy zárt célú elektronikus információs rendszer felhasználója, illetve feladatai támogatására más külső szolgáltatót vesz igénybe.

Az Ibtv. alapján kritikus adat: az Infotv. szerinti személyes adat, különleges adat vagy valamely jogszabállyal védett adat.

> *Az Info tv. szerint különleges adat:*
> *a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat,*
> *b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;*
> *Jogszabály által védett adat lehet az adótitok, az üzleti titok, az orvosi, ügyvédi, biztosítási, banktitok stb.*

4-es a szervezet biztonsági szintje, ha a szervezet vagy szervezeti egység a 3. szinthez rendelt jellemzőkön túl elektronikus információs rendszert vagy zárt célú elektronikus információs rendszert üzemeltet, vagy fejleszt.

> *Az Ibtv. alapján zártcélú elektronikus információs rendszer a nemzetbiztonsági, honvédelmi, rendészeti, diplomáciai információs feladatok ellátását biztosító, rendeltetése szerint elkülönült elektronikus információs rendszer, amely kizárólagosan a speciális igények kielégítését, az e célra létrehozott szervezet és technika működését szolgálja.*

5-ös biztonsági szintbe **kell sorolni azokat a szervezeteket, amelyek a 4. szinthez rendelt jellemzőkön túl** európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé **törvény alapján kijelölt rendszerelemek elektronikus információs rendszereinek üzemeltetője, fejlesztője, illetve az információbiztonsági ellenőrzések, tesztelések végrehajtására jogosult szervezet vagy szervezeti egység.**

4 Az informatikai szabályzat felülvizsgálata

A Hivatal által használt informatikai rendszerek biztonsági besorolását követően az elvárt biztonsági szintnek megfelelő szabályozáshoz szükséges kiegészítések a 2014.09.15-én elfogadott informatikai szabályzatban kerületek érvényesítésre.

A szabályzat által előírt rendszer-felülvizsgálat értelmében, 2016 márciusában a GKI Digital Kft. elvégezte az informatikai szabályzatok felülvizsgálatát annak ellenőrzése céljából, hogy az abban foglaltak ténylegesen igazodjanak a Hivatalnál található informatikai rendszerek működéséhez. A szabályzatok felülvizsgálata során a Hivatal részéről az informatikai biztonsági felelős támogatta munkánkat, rendelkezésünkre bocsátotta a szükséges dokumentumokat.

A felülvizsgálat eredményeképp összességében megállapítható, hogy **a Hivatal informatikai szabályzatai megfelelnek az elvárásoknak**, jelen formájában azok nem igényelnek kiegészítéseket.

A 2015.07.16-án életbe lépett jogszabályi változások alapján a Hivatal számára véleményünk szerint nem változott az információs biztonsági besorolás, mivel az általa használt rendszerek besorolása az új rendeletben foglaltak szellemében valósult meg, azaz figyelembe vette a Hivatal által kezelt adatok érzékenységét, valamint a használt információs rendszerek ismérveit.

A Hivatal számára az érintett jogszabály következtében felmerülő feladatok köre az alábbi területen jelenik meg:

Az egyes szervezeti egységeket is biztonsági szintbe kell sorolni. Ezek alapján be kell sorolni és be kell jelenteni az elektronikus információs rendszer

a) fejlesztését végző,
b) üzemeltetését végző,
c) üzemeltetéséért felelős vagy
d) információbiztonságáért felelős szervezeti egységek

biztonsági besorolását is.

Véleményünk szerint a kezelt adatok köre, valamint a használt elektronikus rendszerek köre alapján a fenti szervezeti egységek elvárt biztonsági szintje 2-es és 3-as között fog változni, attól függően, hogy mely szervezeti egység, mely elektronikus rendszerek üzemeltetésével kerül kapcsolatba.

4.1 Elvárt intézkedéseknek való megfelelés vizsgálata

A jogszabályok alapján a szervezetek számára az adott biztonsági szintnek megfelelő védelmi intézkedéseket kell megvalósítania, illetve azokat a szabályzataiban rögzítenie. Mivel a Hivatal biztonsági besorolása eddig is 3-as volt, ezért véleményünk szerint a jelenleg szabályozott védelmi intézkedések megfelelnek a jogszabályi elvárásoknak.

A következőkben részletesen bemutatjuk, hogy a szabályzatok ellenőrzése során milyen tartalmi szempontok meglétét, teljesülését ellenőriztük.

4.1.1 Adminisztratív védelmi intézkedések

Szervezeti szintű alapfeladatok

A Hivatal rendelkezik a szükséges szabályzatokkal és informatikai biztonsági stratégiával. A szabályzatok és stratégiák tartalmazzák az elvárt területeknek, a biztonsági besorolásnak megfelelő részletezettségű szabályozását. Az informatikai stratégia részletesen foglalkozik a felmerülő fejlesztési feladatokkal, azok megvalósíthatóságával, illetve kitér az informatikai biztonságot érintő területekre is.

Kockázatelemzés

Az informatikai szabályzat külön fejezetben foglalkozik a kockázatelemzéssel, a sérülékenység ellenőrzésével és a frissítések szabályozásával. A Hivatal informatikai rendszerei rendelkeznek az előírt informatikai biztonsági besorolással.

Tervezés

Az informatikai szabályzat részletesen foglalkozik a rendszerek felhasználóihoz kötődő folyamatok biztonsági szempontból való szabályozásával. Rendelkezik a jogosultságkezelés szabályozásáról és elvárt viselkedési formákat fogalmaz meg az internetes tevékenységek kapcsán. A szabályzat külön fejezetben foglalkozik az informatikai rendszerek biztonságának szabályozásával és a megfelelő működési környezet leírásával.

Biztonsági elemzés

A szabályzat részletesen foglalkozik az informatikai rendszerek biztonsági ellenőrzésével, meghatározza az ellenőrzési folyamatokat, felelősöket és jogköröket.

Emberi tényezőket figyelembe vevő – személy – biztonság

Az informatikai szabályzat részletesen foglalkozik a humán erőforráshoz kapcsolódó védelmi, biztonsági kérdések szabályozásával. Kitér az új, illetve a kilépő dolgozók kapcsán felmerülő szabályokra, valamint az érintett szervezettel szerződéses jogviszonyban álló (külső) szervezetre vonatkozó kérdésekre. Szabályozza a felhasználók jogköreit, azok nyilvántartási igényét.

Tudatosság és képzés

Az informatikai szabályzat rendelkezik a hivatali dolgozók informatika-biztonsági oktatásáról, és szabályozza az oktatásért felelős személyt.

4.1.2 Fizikai védelmi intézkedések

A Hivatal informatikai szabályzata részletesen foglalkozik az informatikai rendszerek, – köztük a szerverek tárolását biztosító terem – fizikai védelmével. A szabályzat előírja a szükséges fizikai intézkedéseket és a felülvizsgálati gyakoriságokat. Rendelkezik a vagyonvédelmi, tűzvédelmi előírásokkal és részletesen szabályozza a fizikai és környezeti biztonság területeit.

4.1.3 Logikai védelmi intézkedések

A törvényi szabályozásban meghatározott. a logikai védelmi intézkedések köré épülő szabályozások tekintetében a 3-as biztonsági besorolású informatikai rendszerrel rendelkező Hivatalok számára az alábbi területekre vonatkozóan kell megfelelő szabályozással és eljárásrendekkel rendelkeznie:

- Konfigurációkezelés
- Üzletmenet-(ügymenet-) folytonosság tervezése
- Karbantartás
- Adathordozók védelme
- Azonosítás és hitelesítés
- Hozzáférés ellenőrzése
- Rendszer- és információsértetlenség
- Naplózás és elszámoltathatóság
- Rendszer- és kommunikációvédelem
- Reagálás a biztonsági eseményekre

A jelenleg hatályos informatikai szabályzat a fenti területek mindegyikével külön fejezetben foglalkozik. Részletesen szabályozásra kerül a területek működési környezete, annak felelőse, az alkalmazandó eljárásrendek, valamint a felülvizsgálati időszakok. A szabályozás részletezettsége és kiterjedtsége megfelel a hivatkozott törvény által, a 3-as biztonsági besorolású hivatalokkal szemben támasztott követelményeknek.

5 Melléklet

5.1 A Hivatal informatikai hálózatának felépítése