

**Előterjesztés Dévaványa Város Önkormányzat Képviselő-testületének
2014. augusztus 15-i rendkívüli ülésére**

Tárgy: Az elektronikus információ biztonságából adódó feladatok

Tisztelt Képviselő-testület!

Az állami és önkormányzat szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényből fakadóan az elkövetkező időszakban több feladat hárul az önkormányzat képviselő-testületének hivatalára amelyről szeretnék tájékoztatást adni a Képviselő-testületnek.

A törvény megalkotásának célja a nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek biztonságának és védelmének biztosítása

A törvény rendelkezéseit alkalmazni kell az államigazgatás teljes szervezetrendszerére, a bíróságokra, ügyészségekre és többek között helyi önkormányzatok képviselő-testületeinek hivatalaira is. Ezen szervezeteknél biztosítani kell az elektronikus információs rendszerben kezelt adatok és információk bizalmasságát, sértetlenségét és rendelkezésre állását, valamint maguknak az információs rendszereknek a zárt és teljeskörű védelmét.

Annak érdekében, hogy ez a védelem biztosítható legyen a már működő elektronikus információs rendszereket biztonsági osztályba, magát a szervezetet pedig biztonsági szintbe kell besorolni.

Az információs rendszereket a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából 1-től 5-ig számozott fokozatba kell besorolni.

A számozás emelkedése párhuzamosan szigorodó védelmi előírásokkal jár együtt. A biztonsági osztályba sorolást – az auditot követően – a szervezet vezetője hagyja jóvá és felel annak a jogszabályoknak és kockázatoknak való megfeleléséért. A biztonsági osztályba sorolást a szervezet informatikai biztonsági szabályzatában kell rögzíteni. A biztonsági osztályba sorolást legalább háromévenként dokumentált módon felül kell vizsgálni. Ha a biztonsági osztály meghatározásánál a szervezet hiányosságot állapít meg 90 napon belül cselekvési tervet kell készíteni a hiányosság megszüntetésére.

Magának a szervezetnek a biztonsági szintje a szervezet elektronikus információs rendszereinek legmagasabb biztonsági osztályával azonos besorolású, de önkormányzati hivatali szervezet esetén legalább 2 szintű.

Ha az audit során meghatározott biztonsági szint alacsonyabb mint az adott szervezetre a jogszabályban előírt biztonsági szint, akkor a szervezetnek a vizsgálatot követő 90 napon belül cselekvési tervet kell készíteni a számára előírt biztonsági szint elérésére.

Ha a biztonsági szint a vizsgálat alapján az 1 szintet sem éri el, akkor az 1 szint eléréséhez szükséges intézkedéseket egy éven belül meg kell valósítani. (Meg kívánom jegyezni, hogy a környékünkön lévő városok közül Gyomaendrőd és Szarvas már elvégezte a biztonsági szint besorolására vonatkozó vizsgálatot, amely alapján egyik hivatali szervezet sem érte el az 1 szintet.)

Az 1 szint elérését követően a következő magasabb szintre lépéshez két év áll rendelkezésre. Azt feltételezve tehát, hogy a vizsgálat során a mi hivatali szervezetünk biztonsági szint besorolása sem éri el az 1 szintet, összesen három év áll rendelkezésre a 2 szint eléréséhez és az ehhez a szinthez tartozó fejlesztések megvalósításához.

A biztonsági szintet legalább három évenként dokumentált módon felül kell vizsgálni.

Az informatikai rendszerek biztonsági osztályba sorolása, illetve a szervezet biztonsági szintjének meghatározása és a cselekvési tervek kidolgozásán túl további feladatok is adódnak a törvényből.

Az egyik legfontosabb és leginkább költségigénnyel járó feladat a szervezetre irányadó biztonsági szintnek megfelelő, jogszabályban meghatározott követelmények teljesítése. (Az ide vonatkozó végrehajtási rendelet: a 77/2013. (XII.19.) NFM. rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológia biztonsági, valamint biztonságos információs eszközökre, termékekre vonatkozó, valamint a biztonsági osztályba és biztonsági szintbe sorolási követelményeiről.)

További feladatként jelentkezik az elektronikus információs rendszer biztonságáért felelős személy kinevezése vagy megbízása.

Ki kell adni a szervezet informatikai biztonságpolitikáját. Meg kell határozni és elfogadni a szervezet informatikai biztonsági stratégiáját.

Meg kell határozni és ki kell adni az informatikai biztonsági szabályzatot.

Gondoskodni kell dokumentált módon a szervezet munkatársainak információbiztonsági oktatásáról.

Rendszeresen végrehajtott kockázatelemzésekkel, ellenőrzésekkel, auditok lefolytatásával meg kell győződni arról, hogy a szervezet elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak.

A bekövetkezett biztonsági eseményekről és a tett intézkedésekről tájékoztatni kell a felügyeletet ellátó országos főhatóságot.

A törvényben és a végrehajtási rendeletekben meghatározott feladatok végrehajtását és az előírt követelmények teljesítését a Nemzeti Fejlesztési Minisztérium keretein belül országos főhatósággént működő Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) felügyeli.

A hivatali szervezet vezetője köteles együttműködni a hatósággal.

Ennek során nyilvántartásba vétel érdekében – be kell jelenteni a szervezet

- be kell jelenteni az informatikai biztonsági felelős személyt, adatait
- meg kell küldeni a hatóság részére az informatikai biztonsági osztályba sorolást, illetve szintbe sorolást is tartalmazó informatikai biztonsági szabályzatot
- hatósági ellenőrzés esetén együtt kell működni a hatósággal.

Külön végrehajtási jogszabály rögzíti, hogy az informatikai biztonsági felelős a jogszabályban előírt képzésen és éves továbbképzésen, az informatikai biztonsággal összefüggő feladatok ellátásában részt vevő személy és a szervezetfelelős vezetője a jogszabályban előírt éves továbbképzésen köteles részt venni.

A képzésekről a Nemzeti Közszolgálati Egyetem fog gondoskodni.

A Tisztelt Képviselő-testületnek a jogszabályi háttér rövid vázolásával azt kívántam bemutatni, hogy az információbiztonsággal kapcsolatban milyen feladatok hárulnak a hivatali szervezetre. A feladat végrehajtásába külsős szakértő cég bevonását javaslom. Erre vonatkozóan külön ajánlatkérés nélkül is több cég küldött már ajánlatot, de ezek nem pótolják

az egyedi ajánlatkérést, amely tartalmazni fogja a szervezet ide vonatkozó paramétereit és az elvégzendő feladatokat.

Amennyiben a Képviselő-testület is egyetért vele, javaslom, hogy ajánlattételre a következő cégeket kérjük fel:

1. ITSecure Kft. Budapest
2. ComPax Kft. Szeged
3. ALBACOMP RI Rendszerintegrációs Kft. Székesfehérvár
4. Blue Key Kft. Békéscsaba
5. Web Biztonság Informatika Kft. Békéscsaba

Kérem, hogy a Tisztelt Képviselő-testület fogadja el a tájékoztatást és hozzon döntést az ajánlatkérésről.

Dévaványa, 2014. augusztus 7.

Balogh Csilla
jegyző

Határozati javaslat:

___/2014. (VIII.15.) Dv. Kt. hat.

Dévaványa Város Önkormányzat Képviselő-testülete úgy dönt, hogy a Dévaványai Közös Önkormányzati Hivatal elektronikus rendszere biztonsági feladatainak teljeskörű ellátására és felelősségének viselésére – amely többek között tartalmazza a szervezet információs rendszereinek biztonsági osztályba és a szervezet biztonsági szintjére vonatkozó felmérést, valamint a szervezet információbiztonsági dokumentumainak előkészítését – helyi beszerzési eljárás keretében az alábbi ajánlattevőket kéri fel ajánlattételre:

1. ITSecure Kft. Budapest
2. ComPax Kft. Szeged
3. ALBACOMP RI Rendszerintegrációs Kft. Székesfehérvár
4. Blue Key Kft. Békéscsaba
5. Web Biztonság Informatika Kft. Békéscsaba

A képviselő-testület megbízza a jegyzőt a beszerzési eljárás lebonyolításával.

Felelős: Balogh Csilla jegyző
Fekete László műszaki irodavezető

Határidő: folyamatos