Jelen előterjesztés csak tervezet, amelynek közigazgatási egyeztetése folyamatban van. A minisztériumok közötti egyeztetés során az előterjesztés koncepcionális kérdései is jelentősen módosulhatnak, ezért az előterjesztés jelen formájában nem tekinthető a Kormány álláspontjának.

A dokumentum célja a társadalmi egyeztetés elindítása és a jogalkotási folyamat átláthatóvá tétele, amelynek alapján, illetve eredményeként a mellékelt tervezet valamennyi tartalmi és formai eleme módosulhat!

A tervezet előterjesztője Közigazgatási és Igazságügyi Minisztérium.

TERVEZET!

2012. évi … törvény
az elektronikus információbiztonságról

A nemzet érdekében kiemelten fontos – napjaink információs társadalmát érő fenyegetések miatt – a nemzeti vagyon részét képező nemzeti elektronikus adat- és információs vagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága.
A modern állam és annak polgárai, a gazdasági és a civil szervezetek számára e rendszerek és rendszerelemek nélkülözhetetlenek, a társadalom működése szempontjából alapvetőek, a működésükbe történő beavatkozással zavarhatóak és megbéníthatóak. Az elektronikus információs rendszerek és rendszerelemek nem csak a fizikai veszélyeknek vannak kitéve, hanem más, az úgynevezett kibertérből érkező fenyegetéseknek is.
A törvény célja az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmasságának, sértetlenségének és rendelkezésre állásának, valamint ezek rendszerelemei sértetlenségének és rendelkezésre állásának zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme.
Mindezekre figyelemmel az Országgyűlés a következő törvényt alkotja:

I. Fejezet
Általános rendelkezések

1. A törvény hatálya

1. §

(1) E törvény hatálya kiterjed
a) a központi államigazgatási szervek – kivéve a Kormány és a kormánybizottságok – adatait kezelő szervezetek,
b) a Köztársasági Elnöki Hivatal adatait kezelő szervezetek,
c) az Országgyűlés Hivatala adatait kezelő szervezetek,
d) az Alkotmánybíróság Hivatala adatait kezelő szervezetek,
e) a bíróságok adatait kezelő szervezetek,
f) az ügyészségek adatait kezelő szervezetek,
g) az Alapvető Jogok Biztosának Hivatala adatait kezelő szervezetek,
h) az Állami Számvevőszék adatait kezelő szervezetek,
i) a Magyar Nemzeti Bank adatait kezelő szervezetek,
j) a fővárosi és megyei kormányhivatalok adatait kezelő szervezetek,
k) a helyi önkormányzatok képviselő-testületének hivatalai, a hatósági igazgatási társulások adatait kezelő szervezetek,
l) a Magyar Honvédség adatait kezelő szervezetek,
m) a külképviseletek adatait kezelő szervezetek,
n) a külön jogszabályban meghatározott, a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói,
o) az európai létfontosságú rendszerelemmé és a nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelem üzemeltetője
elektronikus információs rendszereinek védelmére.

(2) A minősített adatokat kezelő elektronikus információs rendszereket érintően

a) e törvény rendelkezéseit a minősített adat védelmére vonatkozó jogszabályokban meghatározott eltérésekkel kell alkalmazni,
b) a 14-18. §-ban meghatározott feladatok ellátásáról a minősített adatok védelmének szakmai felügyeletéért felelős miniszter saját hatáskörében gondoskodik.

(3) A rendvédelmi szervek, a Katonai Nemzetbiztonsági Szolgálat és a Magyar Honvédség, valamint a külpolitikáért felelős miniszter diplomáciai információs célokra használt zárt célú elektronikus információs rendszerei, valamint a Honvédelmi Tanács és a kormány speciális működését biztosító infokommunikációs támogató rendszerei esetében a 14-18. §-ban meghatározott feladatok ellátásáról a Magyar Honvédség és a Katonai Nemzetbiztonsági Szolgálat esetében a honvédelemért felelős miniszter, a rendvédelmi szervek esetében a rendvédelemért felelős miniszter, a diplomáciai információs célokra használt rendszer esetén a külpolitikáért felelős miniszter gondoskodik.

2. §

Az elektronikus információs rendszerekre és eszközökre nemzetközi egyezmények vagy nemzetközi szabványok alapján kiadott biztonsági tanúsítványokat a Nemzeti Elektronikus Információvédelmi Hatóság az eljárása során figyelembe veszi.

3. §

(1) Törvény eltérő rendelkezése hiányában az 1. § (1) bekezdés n) pontjában megjelölt elektronikus információs rendszerek – a (2) bekezdésében meghatározott kivétellel – az Európai Unió országai területén üzemeltethetőek.

(2) Az 1. § (1) bekezdés a)-k) pontjában megjelölt szervezetek adatai és a nemzeti adatvagyon részét képező adatok Magyarország területén üzemeltetett elektronikus információs rendszerekben kezelhetőek.

(3) A (2) bekezdésben megjelölt elektronikus információs rendszerek a Nemzeti Elektronikus Információvédelmi Hatóság engedélyével az Európai Unió országai területén belül is üzemeltethetőek.

(4) A törvény hatálya alá tartozó elektronikus információs rendszert működtető, nem Magyarországon bejegyzett vállalkozásnak Magyarország területén működő képviselőt kell kijelölnie, aki az e törvényben foglaltak végrehajtásáért, mint a szervezet vezetője felel.

2. Értelmező rendelkezések

4. §

E törvény alkalmazásában

1. adat: tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas;

2. adatkezelés: az alkalmazott eljárástól függetlenül az adatokon végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala,

összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adatok további felhasználásának megakadályozása;

3. adminisztratív védelem: a védelem érdekében hozott szervezési, szabályozási, ellenőrzési intézkedések, továbbá a védelemre vonatkozó oktatás;

4. auditálás: előírások teljesítésére vonatkozó megfelelőségi vizsgálat, ellenőrzés;

5. bizalmasság: az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról;

6. biztonsági esemény: az elektronikus információs rendszerben kedvezőtlen változást előidéző esemény, más néven incidens;

7. biztonsági esemény kezelés: az elektronikus információs rendszerben bekövetkezett biztonsági esemény, incidens dokumentálása, következményeinek felszámolása, a bekövetkezés okainak és felelőseinek megállapítása, és a hasonló biztonsági események, incidensek jövőbeni előfordulásának megakadályozása érdekében végzett tervszerű tevékenység, más néven incidenskezelés;

8. biztonsági osztályba sorolás: az adatnak az adatkezelés során a kezelés módjára, körülményeire, a védelem eszközeire vonatkozó, a védelem erősségét meghatározó osztályozása;

9. biztonsági stratégia: a biztonságpolitikában kitűzött célok megvalósításának útja, módszere, amely az éves beszerzési és beruházási tervek kiindulási alapja;

10. biztonságpolitika: a biztonsági célok, alapelvek és a szervezet vezetői elkötelezettségének bemutatása a biztonság irányítására és támogatására;

11. elektronikus információs rendszer*:* adatok, információk kezelésére használt eszközök (környezeti infrastruktúra, hardver, hálózat és adathordozók), eljárások (szabályozás, szoftver és kapcsolódó folyamatok), valamint az ezeket kezelő személyek együttese;

12. elektronikus információs rendszer biztonsága: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint a rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos;

13. életciklus: az elektronikus információs rendszer tervezését, fejlesztését, üzemeltetését és megszüntetését magába foglaló időtartam;

14. észlelés: a biztonsági esemény bekövetkezésének felismerése;

15. fejlesztő: személy, csoport vagy szervezet, aki (amely) egy adott elektronikus információs rendszer vagy e rendszer elemeinek tervezését, fejlesztését, kivitelezését vagy a már meglévő rendszer vagy rendszerelemek módosítását végzi;

16. felhasználó: személy, csoport vagy szervezet, aki (amely) egy adott elektronikus információs rendszert igénybe vesz;

17. fenyegetés: olyan művelet vagy esemény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát;

18. fizikai védelem: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető-rendszer, a megfigyelő rendszer, a tápáramellátás, a túlfeszültség- és a villámvédelem, valamint a tűzvédelem;

19. folytonos védelem: az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósuló védelem;

20. információ: bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti;

21. kibertér: az elektronikus információs rendszerek olyan átfogó tartománya, amely tartalmazza az egymással összefüggő információs hálózatok infrastruktúráit, beleértve az internetet, a távközlési hálózatokat, a számítógépes rendszereket, ideértve a beágyazott processzorokat és vezérlőket is;

22. kibervédelem: a kibertérből jelentkező fenyegetések elleni védelem, ideértve a saját kibertér képességek megőrzését;

23. kockázat: a fenyegetettség mértéke, amely a kárnagyság és a relatív gyakoriság (bekövetkezési valószínűség) szorzata;

24. kockázatelemzés: az elektronikus információs rendszer értékének, sérülékenységeinek (gyenge pontjainak), fenyegetéseinek, a várható károknak és ezek bekövetkezési gyakoriságának felmérése útján megállapított kockázatok csökkentésére irányuló intézkedésrendszer kidolgozása;

25. korai figyelmeztetés: valamely fenyegetés várható bekövetkezésének jelzése a fenyegetés bekövetkezése előtt annyi idővel, hogy hatékony védelmi intézkedéseket lehessen hozni;

26. létfontosságú információs rendszerelem*:* a létfontosságú rendszerelemek azon elektronikus információs létesítményei, eszközei vagy szolgáltatásai, amelyek működésképtelenné válása, vagy megsemmisülése a létfontosságú rendszerelemeket, vagy azok részeit elérhetetlenné tenné, vagy működőképességüket jelentősen csökkentené;

27. logikai védelem: az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem;

28. megelőzés: a fenyegetés bekövetkezésének elkerülése;

29. reagálás: a bekövetkezett biztonsági esemény terjedésének megakadályozására vagy késleltetésére, a további károk mérséklésére tett intézkedések;

30. rendelkezésre állás: annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek;

31. sértetlenség: az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az elvárt forrásból származik (hitelesség) és a származás megtörténtének bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek tulajdonsága, amely arra vonatkozik, hogy a rendszerelem rendeltetésének megfelelően használható;

32. sérülékenység: az elektronikus információs rendszer olyan része vagy tulajdonsága, amelyen keresztül valamely fenyegetettség megvalósulhat;

33. sérülékenység vizsgálat: az elektronikus információs rendszerek gyenge pontjainak (biztonsági rések) feltárása és az ezeken keresztül fenyegető biztonsági események megelőzésére irányuló intézkedések kidolgozása;

34. szervezet: az 1. §-ban meghatározott szervek és ezen szervek részére adatkezelést végző természetes személy, jogi személyek, valamint jogi személyiséggel nem rendelkező gazdasági társaságok;

35. teljes körű védelem: az elektronikus információs rendszer valamennyi elemére kiterjedő védelem;

36. üzemeltető: az a természetes, jogi személy vagy jogi személyiség nélküli szervezet, aki vagy amely az elektronikus információs rendszer vagy annak részei működtetését végzi és a működésért felelős;

37. védelmi feladatok: megelőzés és korai figyelmeztetés, észlelés, reagálás, eseménykezelés;

38. zárt célú elektronikus információs rendszer: törvényben vagy kormányrendeletben meghatározott elkülönült elektronikus információs, informatikai vagy hírközlési rendszer, hálózat;

39. zárt védelem: az összes számításba vehető fenyegetettséget figyelembe vevő védelem.

II. Fejezet
Elektronikus információbiztonsági követelmények

3. Alapvető elektronikus információbiztonsági követelmények

5. §

Az e törvény hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában meg kell valósítani

a) az elektronikus információs rendszerben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása, valamint

b) az elektronikus információs rendszer és elemeinek sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.

6. §

Az elektronikus információs rendszernek az 5. §-ban meghatározott feltételeknek megfelelő védelme körében a szervezetnek külön jogszabályban előírt logikai, fizikai és adminisztratív védelmi intézkedéseket kell meghatároznia, amelyek támogatják:
a) a megelőzést és a korai figyelmeztetést,
b) az észlelést,
c) a reagálást,
d) az eseménykezelést.

4. Az elektronikus információs rendszerek biztonsági osztályba sorolása

7. §

(1) Annak érdekében, hogy az e törvény hatálya alá tartozó elektronikus információs rendszerek, valamint az azokban kezelt adatok védelme a kockázatokkal arányosan biztosítható legyen, az elektronikus információs rendszereket be kell sorolni egy-egy biztonsági osztályba a bizalmasság, a sértetlenség és a rendelkezésre állás szempontjából (a továbbiakban: biztonsági osztályba sorolás).

(2) A biztonsági osztályba sorolás alkalmával – az érintett elektronikus információs rendszer vagy az általa kezelt adat bizalmasságának, sértetlenségének vagy rendelkezésre állásának sérülése szempontjából – 1-től 5-ig számozott fokozatot kell alkalmazni, a számozás emelkedésével párhuzamosan szigorodó védelmi előírásokkal együtt.

(3) A biztonsági osztályba sorolást a szervezet vezetője hagyja jóvá, és gondoskodik annak a jogszabályoknak és kockázatoknak való megfelelőségéről, a felhasznált adatok teljességéről és időszerűségéről. A biztonsági osztályba sorolást a szervezet informatikai biztonsági szabályzatában kell rögzíteni.

(4) A szervezetnek az elektronikus információs rendszer bizalmasság, sértetlenség és rendelkezésre állás szerinti biztonsági osztálya alapján az 5. és 6. §-ban előírt védelmi intézkedéseket kell megvalósítania az adott elektronikus információs rendszerre vonatkozóan.

(5) A szervezet az e törvényben meghatározott feltételeknek megfelelő, az adott szervezetre irányadó besorolási szintnél magasabb szintű, kivételes esetben alacsonyabb szintű biztonsági osztályba sorolást is megállapíthat.

8. §

(1) A biztonsági osztályba sorolást három évenként felül kell vizsgálni.

(2) Az elektronikus információs rendszer biztonságát érintő változás esetén a biztonsági osztályba sorolást soron kívül meg kell ismételni.

(3) A 7. § (2) bekezdésében foglaltakkal összhangban előírt, az elektronikus információs rendszerre vonatkozó biztonsági osztály eléréséhez a szervezetnek lehetősége van a biztonsági intézkedések fokozatos kivitelezésére. Ennek keretében a magasabb biztonsági osztályhoz rendelt biztonsági intézkedések kivitelezésére két év áll rendelkezésére.

(4) A szervezet a külön jogszabályban meghatározott szempontok alapján megvizsgálja elektronikus információs rendszereit, és annak alapján meghatározza, hogy a vizsgálat elvégzésekor melyik biztonsági osztálynak felel meg.

(5) Ha a vizsgálat alapján meghatározott biztonsági osztály alacsonyabb, mint az adott szervezetre a 7. § (2) bekezdésében előírt biztonsági osztály, akkor a szervezetnek a vizsgálatot követő 90 napon belül cselekvési tervet kell készítenie a számára előírt biztonsági osztály elérésére.

5. Az elektronikus információs rendszert kezelő szervezetek biztonsági szintje

9. §

(1) A kockázatokkal arányos, költséghatékony védelem kialakítása érdekében az elektronikus információs rendszert kezelő szervezeteket az elektronikus információs rendszerek védelmére való felkészültsége alapján biztonsági szintekbe kell sorolni az 1. mellékletben meghatározott szempontok szerint.

(2) A szervezet biztonsági szintje a szervezet elektronikus információs rendszereinek legmagasabb biztonsági osztályával azonos besorolású, de legalább
a) az 1. § (1) bekezdés b) - d), g) és k) pontjába tartó szervezetek esetén 2.,
b) az 1. § (1) bekezdés a), e), f), h)-j) pontjába tartó szervezetek esetén 3.,
c) az 1. § (1) bekezdés l) és m) pontjába tartó szervezetek esetén 4.,
d) az 1. § (1) bekezdés n) és o) pontjába tartó szervezetek esetén 5.
szintű.

(3) A szervezet az e törvényben meghatározott feltételeknek megfelelő, az adott szervezetre irányadó besorolási szintnél magasabb szintű besorolást is megállapíthat.

(4) A Nemzeti Elektronikus Információvédelmi Hatóság a szervezet – kivéve az 1. § (2) és (3) bekezdésében meghatározott elektronikus információs rendszerek esetében – által megállapított biztonsági szintet felülbírálhatja és magasabb, kivételes esetben alacsonyabb szintű besorolást is megállapíthat.

10. §

(1) A szervezet az 1. mellékletben meghatározott szempontok alapján megvizsgálja elektronikus információs rendszereit, és annak alapján meghatározza, hogy a vizsgálat elvégzésekor melyik biztonsági szintnek felel meg.

(2) Ha a vizsgálat alapján meghatározott biztonsági szint alacsonyabb, mint az adott szervezetre a 9. § (2) bekezdésében előírt biztonsági szint, akkor a szervezetnek a vizsgálatot

követő 90 napon belül cselekvési tervet kell készítenie a számára előírt biztonsági szint elérésére.

(3) Ha a biztonsági szint a vizsgálat alapján az 1. szintet nem éri el, akkor azt az (1) bekezdésben meghatározott szempontok szerint lefolytatott vizsgálatot követő egy éven belül meg kell valósítani.

(4) A 9. § (2) bekezdésében előírt biztonsági szint teljesítése során a szervezetnek lehetősége van az előírt biztonsági szint fokozatos elérésére. Ennek keretében a magasabb biztonsági szint elérésére – minden egyes szintet érintően, a következő magasabb szintre lépéshez – két év áll rendelkezésére.

(5) A biztonsági szint meghatározását a 9. § (2) bekezdésében előírt biztonsági szint elérését követően három évenként dokumentált módon felül kell vizsgálni.

(6) Az elektronikus információs rendszer biztonságát érintő változás esetén a biztonsági szintbe sorolást soron kívül meg kell ismételni.

(7) Az elektronikus információs rendszer biztonsági szintbe sorolását a szervezet vezetője hagyja jóvá, és gondoskodik annak a jogszabályoknak és kockázatoknak való megfelelőségéről, a felhasznált adatok teljességéről és időszerűségéről. A biztonsági szintbe sorolást a szervezet informatikai biztonsági szabályzatában kell rögzíteni.

6. A szervezeteknek az elektronikus információs rendszereik védelmét biztosító kötelezettségei

11. §

(1) Az 1. § (1) bekezdésében meghatározott szervezet vezetője köteles gondoskodni az elektronikus információs rendszerek védelméről a következők szerint:
a) biztosítja az elektronikus információs rendszereire irányadó biztonsági osztály tekintetében a külön jogszabályban meghatározott követelményeket,
b) biztosítja a szervezetre irányadó biztonsági szint tekintetében a külön jogszabályban meghatározott követelményeket,
c) az elektronikus információs rendszer biztonsági osztálya és biztonsági szintje követelményrendszerének megfelelően az elektronikus információs rendszer biztonságáért felelős személyt nevez ki, vagy bíz meg,
d) kiadja a szervezet elektronikus információs rendszereire vonatkozó biztonságpolitikáját,
e) kiadja a szervezet elektronikus információs rendszerei védelmének felelőseire, feladataira és az ehhez szükséges hatáskörökre, illetve a felhasználókra vonatkozó informatikai biztonsági szabályzatot,
f) meghatározza a szervezet elektronikus információs rendszereinek biztonsági stratégiáját,
g) gondoskodik az e törvény hatálya alá tartozó elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról,
h) rendszeresen végrehajtott biztonsági kockázatelemzések, ellenőrzések, auditok lefolytatása révén meggyőződik arról, hogy a szervezet e törvény hatálya alá tartozó elektronikus információs rendszereinek biztonsága megfelel-e a jogszabályoknak és a kockázatoknak,
i) gondoskodik az elektronikus információs rendszer eseményeinek nyomon követhetőségéről,

j) biztonsági esemény bekövetkezésekor minden rendelkezésére álló erőforrás felhasználásával gondoskodik a biztonsági eseményre történő gyors és hatékony reagálásról, és az ezt követő eseménykezelésről,
k) ha az e törvény hatálya alá tartozó elektronikus információs rendszer létrehozásában, üzemeltetésében, adatkezelésében, auditálásában, karbantartásában vagy javításában közreműködőt vesz igénybe, gondoskodik arról, hogy az e törvényben foglaltak szerződéses kötelemként teljesüljenek,
l) a fokozott veszéllyel járó tevékenység szabályai szerint felelős azért, hogy az érintetteket a biztonsági követelményekről és a lehetséges fenyegetésekről haladéktalanul tájékoztassa,
m) megteszi az e törvény hatálya alá tartozó az elektronikus információs rendszer védelme érdekében felmerülő egyéb szükséges intézkedéseket.

(2) Az (1) bekezdésben meghatározott feladatokért a szervezet vezetője akkor is felelős, ha az e törvény hatálya alá tartozó elektronikus információs rendszer létrehozásában, üzemeltetésében, adatkezelésében, auditálásában, karbantartásában vagy javításában közreműködőt – ide nem értve azon elektronikus információs rendszereket, amelyek tekintetében jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltatót, illetve központi adatkezelőt és adatfeldolgozó szolgáltatót – vesz igénybe.

(3) A jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató, illetve központi adatkezelő és adatfeldolgozó szolgáltató igénybe vétele esetén az (1) és (2) bekezdésben írt feltételek teljesítését a jogszabály által kijelölt központosított informatikai és elektronikus hírközlési szolgáltató, illetve központi adatkezelő és adatfeldolgozó szolgáltató felett felügyeletet gyakorló miniszter biztosíttatja az érintett szolgáltatóval.

12. §

A szervezet vezetője köteles együttműködni a Nemzeti Elektronikus Információvédelmi Hatósággal. Ennek során:
a) a 11. § (1) bekezdés c) pontjában írt, az elektronikus információs rendszer biztonságáért felelős személyről tájékoztatást nyújt,
b) a szervezet informatikai biztonsági szabályzatát tájékoztatás céljából megküldi
a Nemzeti Elektronikus Információvédelmi Hatóságnak.

13. §

(1) Az elektronikus információs rendszer biztonságáért felelős személy feladata ellátása során a szervezet vezetőjének közvetlenül adhat tájékoztatást, jelentést.

(2) Az elektronikus információs rendszer biztonságáért felelős személy felel a szervezetnél előforduló valamennyi, az elektronikus információs rendszerek védelméhez kapcsolódó feladat ellátásáért. Ennek körében:
a) gondoskodik a szervezet által üzemeltetett, illetve a szervezet adatait feldolgozó elektronikus információs rendszerek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
b) elvégzi az a) pont szerinti tevékenységek tervezését, szervezését, irányítását, koordinálását és ellenőrzését,

c) előkészíti és kiadmányozásra felterjeszti a szervezet elektronikus információs rendszereire vonatkozó informatikai biztonsági szabályzatot,
d) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet e tárgykört érintő szabályzatait és szerződéseit,
e) kapcsolatot tart a Nemzeti Elektronikus Információvédelmi Hatósággal.

(3) Az elektronikus információs rendszer biztonságáért felelős személy a törvény hatálya alá tartozó bármely elektronikus információs rendszerét érintő biztonsági eseményről haladéktalanul értesíti a külön jogszabályban kijelölt szervet.

(4) Amennyiben a szervezet elektronikus információs rendszereinek mérete vagy biztonsági igényei indokolják, a szervezeten belül információbiztonsági szervezeti egység hozható létre, melyet az elektronikus információs rendszer biztonságáért felelős személy vezet.

(5) Az elektronikus információs rendszer biztonságáért felelős személy feladatköre a szervezet valamennyi elektronikus információs rendszerének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, adatkezelésében, auditálásában, vizsgálatában, kockázatelemzésében, karbantartásában vagy javításában közreműködők e törvény hatálya alá tartozó elektronikus információs rendszereit érintő, biztonsággal összefüggő tevékenységére kiterjed.

(6) Ha a szervezet elektronikus információs rendszerének, illetve annak védelmének a tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, adatkezelésében, auditálásában, vizsgálatában, kockázatelemzésében, karbantartásában vagy javításában közreműködőt vesz igénybe, az elektronikus információs rendszer biztonságáért felelős személy e törvény szerinti feladatai és felelőssége más személyre nem átruházható.

(7) Az elektronikus információs rendszer biztonságáért felelős személy jogosult a szervezet elektronikus információs rendszere tervezésében, fejlesztésében, létrehozásában, üzemeltetésében, adatkezelésében, auditálásában, vizsgálatában, kockázatelemzésében, karbantartásában vagy javításában közreműködőktől a biztonsági követelmények teljesülésével kapcsolatban tájékoztatást kérni. Ennek keretében a követelményeknek való megfelelőség alátámasztásához szükséges bekérni a közreműködői tevékenységgel kapcsolatos adatot, illetve az elektronikus információs rendszerek biztonsága tárgyában keletkezett valamennyi dokumentumot.

(8) A törvény hatálya alá tartozó szervezeteknél csak olyan személy végezheti az elektronikus információs rendszer biztonságáért felelős személy feladatait, aki büntetlen előéletű, rendelkezik a feladatellátáshoz szükséges felsőfokú végzettséggel és szakképzettséggel.

(9) Az elektronikus információs rendszer biztonságáért felelős személy és az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában közreműködök miniszteri rendeletben meghatározott rendszeres szakmai képzésen, továbbképzésen vesznek részt.

III. Fejezet
Az elektronikus információs rendszerek biztonsági felügyelete

7. A Nemzeti Elektronikus Információvédelmi Hatóság

14. §

(1) Az e törvény hatálya alá tartozó elektronikus információs rendszerek biztonságának felügyeletét az informatikáért felelős miniszter látja el a minisztérium szervezeti keretében önálló feladattal és hatósági jogkörrel rendelkező Nemzeti Elektronikus Információvédelmi Hatóság (a továbbiakban: Hatóság) útján.

(2) A Hatóság feladata:
a) az osztályba sorolás és a biztonsági szint megállapításának ellenőrzése és az ellenőrzés eredménye alapján döntés meghozatala,
b) az elektronikus információs rendszerek osztályba sorolására és a szervezetek biztonsági szintjeire vonatkozó, jogszabályban meghatározott követelmények teljesülésének ellenőrzése,
c) jogszabály eltérő rendelkezése hiányában a szervezetek elektronikus információs rendszer biztonságáért felelős személyének véleményezése,
d) együttműködés az elektronikus ügyintézési felügyelettel a szabályozott elektronikus ügyintézési szolgáltatás szolgáltatókra vonatkozó biztonsági követelmények teljesülésének ellenőrzésében,
e) a hozzá érkező biztonsági eseményekkel kapcsolatos bejelentések kivizsgálása,
f) kapcsolattartás az elektronikus információbiztonság területén a nemzetbiztonsági szolgálatokkal,
g) javaslattétel a kritikus infrastruktúra védelmi feladatok kormányzati koordinációjáért felelős miniszternek a nemzeti létfontosságú rendszerelem kijelölésére,
h) éves és egyedi jelentések készítése a Kormány részére az elektronikus információs rendszerek biztonságával, a létfontosságú információs rendszerelemek védelmével, és a kibervédelem helyzetével kapcsolatban.

(3) A Hatóság a (2) bekezdés a), b) és e) pontjában meghatározott feladatának ellátása során a minősített adat védelmének szakmai felügyeletéért felelős miniszter szakhatóságként jár el.

(4) A (2) bekezdés a) és b) pontjában foglalt feladatok ellátása körében az informatikáért felelős miniszter az e-közigazgatásért felelős miniszternek, valamint a minősített adatok védelmének szakmai felügyeletéért felelős miniszter egyetértésével éves ellenőrzési tervet (a továbbiakban: éves ellenőrzési terv) készít.

15. §

(1) A Hatóság nyilvántartja és kezeli
a) a szervezet nevét, székhelyét, levelezési címét, cégjegyzékszámát, statisztikai számjelét és adóazonosító számát, képviselőjének nevét, telefon- és telefaxszámát, e-mail címét,
b) a szervezet elektronikus információs rendszereinek megnevezését, a rendszerek biztonsági osztályának és a szervezet biztonsági szintjének besorolását,
c) a szervezet az elektronikus információs rendszer biztonságáért felelős személy természetes személyazonosító adatait, telefon- és telefaxszámát, e-mail címét, szakirányú végzettségét, a végzettséget igazoló okirat sorszámát,
d) a szervezet informatikai biztonsági szabályzatát,
e) a biztonsági eseményekkel kapcsolatos bejelentéseket.

(2) Az (1) bekezdésben meghatározott adatok kezelésének célja az elektronikus információs rendszerek védelmével kapcsolatos kötelezettségek teljesítése és hatósági ellenőrzésének biztosítása.

(3) A Hatóság az (1) bekezdés a)-c) pontja szerinti adatokat a szervezet bejelentése alapján hivatalból veszi nyilvántartásba.

(4) A Hatóság a nyilvántartásból adatot az eljárás lefolytatásának biztosítása céljából a közigazgatási eljárásban résztvevő hatóságok részére továbbíthat.

(5) Az (1) bekezdésben meghatározott nyilvántartásban szereplő adatokat azok megváltozását követő öt év elteltével törölni kell.

16. §

(1) A Hatóság az elektronikus információs rendszerek, és az azokban kezelt adatok biztonsága érdekében jogosult megtenni, elrendelni, ellenőrizni minden olyan az elektronikus információs rendszer védelmére vonatkozó intézkedést, amellyel az érintett elektronikus információs rendszert veszélyeztető fenyegetések elháríthatók. Ennek érdekében jogosult:
a) az érintett szervezeteknél e törvényben és a végrehajtására kiadott jogszabályokban foglalt biztonsági követelményeket és az ehhez kapcsolódó eljárási szabályok teljesülését ellenőrizni,
b) a követelményeknek való megfelelőség alátámasztásához szükséges dokumentumokat bekérni, illetve a 13. § b) pontja alapján megküldött dokumentációt felülvizsgálni,
c) a biztonsági osztályba sorolást, a biztonsági szint megállapítását, vagy a védelmi intézkedéseket ellenőrizni, az ott feltárt hiányosságok felszámolásához szükséges intézkedéseket elrendelni, ezek teljesülését ellenőrizni, nem teljesülés esetén bírságot kiszabni vagy információbiztonsági gondnokot kirendelni,
d) a központi és az európai uniós forrásból megvalósuló fejlesztési projektek tervezési szakaszában kötelező jelleggel ellenőrizni az információbiztonsági követelmények megtartását,
e) részt venni a hazai információbiztonsági, létfontosságú információs rendszerelem védelmi, kibervédelmi, valamint felkérésre a fenti tárgykörben tartott nemzetközi gyakorlatokon,
f) egyetértési jogot gyakorolni a kormányzati eseménykezelő központnak az ágazatok közötti, a biztonsági események esetén követendő szabályokról és felelősségi körökről szóló tervezetével kapcsolatban.

(2) Ha a törvény hatálya alá tartozó szervezet az e törvényben és végrehajtási rendeleteiben foglaltaknak felszólítás ellenére nem tesz eleget, a Hatóság az eset összes körülményeinek mérlegelésével bírságot szabhat ki, amely további nem teljesülés esetén megismételhető. Közigazgatási szervek esetében a bírság kiszabása helyett információbiztonsági gondnok kirendelését kell alkalmazni.

(3) A Hatóságnak a (2) bekezdésben meghatározott hatáskörében hozott döntésével szemben az érintett a kézbesítéstől számított 15 napon belül keresettel fordulhat a Fővárosi Törvényszékhez. A bíróság eljárására a polgári perrendtartás közigazgatási perekre vonatkozó rendelkezéseit kell alkalmazni.

8. Információbiztonsági gondnok

17. §

(1) Közigazgatási szerv tekintetében a Hatóság a 16. § (2) bekezdése szerinti esetben az érintett szervezetekhez információbiztonsági gondnokot rendelhet ki.

(2) Az információbiztonsági gondnok a fenyegetés elhárításához szükséges védelmi intézkedések eredményes megtétele érdekében a Kormány rendeletében meghatározott intézkedéseket, eljárásokat javasolhat, a szervezet intézkedései tekintetében kifogással élhet.

(3) Az információbiztonsági gondnok határozott időtartamra szóló megbízásáról és a megbízás visszavonásáról az informatikáért felelős miniszter gondoskodik. Az információbiztonsági gondnok tevékenységének szakmai irányítását az informatikáért felelős miniszter végzi.

(4) Az információbiztonsági gondnok felett a (3) bekezdésben foglaltakon felüli munkáltatói jogokat a Hatóság vezetője gyakorolja.

(5) Az információbiztonsági gondnok közszolgálati tisztviselői jogviszonyára a minisztériumban főosztályvezető-helyettesi munkakörben alkalmazott kormánytisztviselőre vonatkozó szabályokat kell alkalmazni.

9. A Nemzeti Biztonsági Felügyelet feladatai az elektronikus információs rendszerek biztonsága vonatkozásában

18. §

E törvény teljesülése érdekében a Nemzeti Biztonsági Felügyelet
a) éves ellenőrzési terv alapján, és e törvény 15. § (2) bekezdés a), b) és e) pontjában foglaltakra tekintettel szakhatóságként, továbbá egyedi esetekben a Hatóság felkérésére sérülékenység vizsgálatot végez, valamint biztonsági események adatainak műszaki vizsgálatát végzi,
b) a törvény hatálya alá tartozó szervezetek elektronikus információs rendszerében a szervezet felkérésére sérülékenység vizsgálatot végez, valamint biztonsági események adatainak műszaki vizsgálatát végzi,
c) a feltárt hiányosságokról, a sérülékenységek megszüntetésére vonatkozó intézkedési tervről a vizsgálat lezárását követően haladéktalanul tájékoztatja a vizsgált szervezet az elektronikus információs rendszer biztonságáért felelős személyt,
d) hazai információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokat szervez,
e) a nemzetközi információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokon felkérésre képviseli Magyarországot, koordinálja, irányítja a magyarországi felek részvételét,
f) véleményezési jogot gyakorol a kormányzati eseménykezelő központnak az ágazatok közti, a biztonsági események esetén követendő szabályokról és felelősségi körökről szóló tervezetével kapcsolatban,
g) az a)-c) pontban foglalt feladatok végrehajtásáról a Hatóság részére tájékoztatást ad.

10. A kormányzati eseménykezelő központ[1]

19. §

(1) A Kormány e törvényben foglalt eseménykezelési feladatok ellátása érdekében

[1]Kormányzati Számítástechnikai Sürgősségi Reagáló Egység [Computer Emergency Response Team (CERT)]

kormányzati eseménykezelő központot működtet a katasztrófák elleni védekezésért felelős miniszter irányítása alatt.

(2) Az 1. § (3) bekezdésében meghatározott szervezetek az eseménykezelési feladatok ellátása érdekében ágazati eseménykezelő központot hozhatnak létre.

(3) Az autonóm államigazgatási szervek és az önálló szabályozó szervek vezetői által az eseménykezelési feladatok ellátása érdekében létrehozott ágazati eseménykezelő központ a biztonsági eseményekhez kapcsolódó adatait köteles haladéktalanul a kormányzati eseménykezelő központ részére továbbítani.

(4) A kormányzati eseménykezelő központ akkreditált nemzeti eseménykezelő központként részt vesz az eseménykezelő központok nemzetközi együttműködésében.

(5) Az ágazati eseménykezelő központok a fenntartó döntése alapján részt vehetnek az eseménykezelő központok nemzetközi együttműködésében, és e célból akkreditálhatóak.

(6) Az egyes ágazati eseménykezelő központok a kormányzati eseménykezelő központtal, mint nemzeti eseménykezelési koordinátorral együttműködnek.

20. §

(1) A kormányzati eseménykezelő központ ellátja a következő feladatokat:
a) az ágazati eseménykezelő központok szakmai támogatása,
b) a nemzetközi eseménykezelési együttműködésekben Magyarország képviselete és az ágazati eseménykezelő központok tájékoztatása a nemzetközi szervezetektől tudomására jutott információbiztonságot érintő eseményekről, fenyegetettségekről,
c) az e törvény által érintett szervezetekkel való kapcsolattartás a bejelentett incidensek fogadására, valamint az azok kezeléséhez szükséges operatív intézkedések megtétele és koordinálása,
d) napi rendszerességű hálózatbiztonsági helyzetértékelések elvégzése,
e) folyamatos 24 órás ügyelet működtetése,
f) a biztonsági események kivizsgálása során az érintett szervezeteknél elvégzi a biztonsági események adatainak műszaki vizsgálatát,
g) a szervezeteknél előforduló incidensek adatainak gyűjtése, ezekről negyedévente jelentés készítése a tanácsadó testület részére,
h) elemzések, jelentések készítése a tanácsadó testület részére a hazai és nemzetközi információbiztonsági irányokról,
i) azonnali figyelmeztetések közzététele a kritikus hálózatbiztonsági eseményekről, ezek magyar nyelvű megjelenítése,
j) a sérülékenységek közzététele a honlapján.

(2) Az ágazati eseménykezelő központok – az (1) bekezdés a) és b) pontban meghatározottak kivételével – az általuk támogatott ágazatok tekintetében ellátják a kormányzati eseménykezelő központ feladatait.

21. §

Az elektronikus információs rendszerek biztonságát érintő kérdések felmérése, a kibervédelem helyzetének figyelemmel kísérése és az ehhez kapcsolódó feladatok

irányvonalainak meghatározása érdekében tanácsadó testület működik.

11. Adatvédelmi rendelkezések

22. §

A Hatóság, a Nemzeti Biztonsági Felügyelet, a kormányzati eseménykezelő központ és ágazati eseménykezelő központ munkatársai az e törvényben meghatározott, az elektronikus információs rendszerek védelmével összefüggő feladataik ellátása során megismert minősített adatokat, személyes adatokat, üzleti titkot, banktitkot, biztosítási titkot, értékpapír titkot, pénztár titkot, orvosi titkot kizárólag a feladat ellátásának időtartama alatt jogosultak kezelni.

IV. Fejezet
Oktatás-képzés, kutatás-fejlesztés

23. §

A Nemzeti Közszolgálati Egyetem a képzési tevékenységének ellátásával összefüggésben
a) a 11. § (1) bekezdés f) pontjában, a 13. § (8) bekezdésében meghatározott képzés érdekében kidolgozza és a közigazgatás-fejlesztésért felelős miniszter elé terjeszti a vezetők, az elektronikus információs rendszer biztonságáért felelős személyek képzési, továbbképzési követelményeit, oktatási programját,
b) kidolgozza és a közigazgatás-fejlesztésért felelős miniszter elé terjeszti a 13. § (8) bekezdésében meghatározott képzettségi követelményeket,
c) gondoskodik a vezetők, az elektronikus információs rendszer biztonságáért felelős személyek, és az általuk irányított szervezeti egységek munkatársai képzéséről és éves továbbképzéséről,
d) közreműködik az információbiztonsági, kibervédelmi, létfontosságú információs rendszer védelmi gyakorlatokon,
e) részt vesz a információvédelmi stratégiák és elemzések elkészítésében.

V. Fejezet
Záró rendelkezések

12. Felhatalmazó rendelkezések

24. §

(1) Felhatalmazást kap a Kormány, hogy rendeletben meghatározza
a) a Hatóság feladatát, a hatósági ellenőrzés lefolytatásának részletes szabályait,
b) a 17. § alapján kijelölésre kerülő információbiztonsági gondnok feladatkörét és eljárásának rendjét,
c) a 15. § (3) bekezdése szerinti szakhatóság feladat- és hatáskörét,
d) a 19. § (1) bekezdése szerinti kormányzati eseménykezelő központ és az ágazati eseménykezelő központok feladat- és hatáskörét, és
e) a 21. § szerinti tanácsadó testületet, annak feladat- és hatáskörét.

(2) Felhatalmazást kap

a) az informatikáért felelős miniszter, hogy az e-közigazgatásért felelős miniszterrel és a minősített adatkezelésért felelős miniszterrel egyetértésben meghatározza a 6. és 7. §-okban előírt technológiai biztonsági követelményeket, továbbá a biztonsági osztályba sorolás követelményeit,
b) a közigazgatás-fejlesztésért felelős miniszter, hogy az e törvényben meghatározott vezetői, az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmát,
c) az informatikáért felelős miniszter, hogy a törvény hatálya alá tartozó szervezetek hatósági nyilvántartásba vételének rendjét,
d) az informatikáért felelős miniszter, hogy a minősített adatok védelmének szakmai felügyeletéért felelős miniszterrel és az adópolitikáért felelős miniszterrel egyetértésben a Hatóság, a Nemzeti Biztonsági Felügyelet azon eljárásait, amelyekért igazgatási szolgáltatási díjat kell fizetni, a fizetendő igazgatási szolgáltatási díj mértékét, az igazgatási szolgáltatási díj beszedésével, kezelésével, nyilvántartásával, visszatérítésével, felhasználásával kapcsolatos szabályokat, valamint a mentességek körét

rendeletben határozza meg.

13. Hatálybalépés

25. §

Ez a törvény 2013. március 1-jén lép hatályba.

14. Átmeneti rendelkezések

26. §

(1) A szervezetnek a már működő elektronikus információs rendszere a 7. § szerinti biztonsági osztályba sorolását első alkalommal a törvény hatálybalépését követő egy éven belül el kell végeznie.

(2) A szervezetnek a 10. § szerinti biztonsági szintbe sorolást első alkalommal a törvény hatálybalépését követő egy éven belül el kell végeznie.

(3) A szervezetnek az e törvény 15. § (5) bekezdésének a), c) és d) pontjaiban foglalt adatokat e törvény hatálybalépésétől számított 60 napon belül nyilvántartásba vétel céljából be kell jelentenie a Hatóságnak.

15. Módosító rendelkezések

27. §

(1) A minősített adat védelméről szóló 2009. évi CLV. törvény 10. § (4) bekezdése helyébe a következő rendelkezés lép:

„(4) Minden olyan szervnél, ahol minősített adatot kezelnek, meg kell teremteni a minősített adat védelméhez szükséges, az adat minősítési szintjének megfelelő

a) az e törvényben és a végrehajtására kiadott rendeletekben meghatározott személyi, fizikai és adminisztratív, valamint
b) az e törvényben és az elektronikus információbiztonságról szóló törvény és végrehajtására kiadott jogszabályokban meghatározott elektronikus

biztonsági feltételeket. Ha a szerv a minősített adatot elektronikus rendszeren kezeli, mind az elektronikus rendszerét, mind pedig magát a szervet automatikusan az elektronikus információbiztonságról szóló törvényben meghatározott legmagasabb biztonsági osztályba és biztonsági szintbe kell besorolni.”

(2) A minősített adat védelméről szóló 2009. évi CLV. törvény 20. § (2) bekezdése a következő v) ponttal egészül ki:

(A Nemzeti Biztonsági Felügyelet)
„v) elvégzi az elektronikus információbiztonságról szóló jogszabályokban számára meghatározott feladatokat.”

28. §

Hatályát veszti a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény 4. §-a.

Melléklet a … törvényhez

A szervezetek biztonsági szintjének meghatározása

a szervezet biztonsági szintje 1. akkor, amikor az kezdeti, ad hoc jellegű, azaz:
a) a szervezet felismerte az elektronikus információs rendszerei biztonsága szükségességét,
b) az elektronikus információs rendszerek biztonsága szükségességének tudatossága elsősorban az egyéneken múlik,
c) az elektronikus információs rendszerek biztonságával megkésve, az eseményekre reagálva foglalkoznak,
d) az elektronikus információs rendszerek biztonságát nem mérik,
e) az észlelt biztonsági szabálysértésekre a felelős keresés a válasz, mert a felelősségi körök nincsenek tisztázva,
f) az elektronikus információs rendszerek biztonsági szabályainak megsértésére adott reakció nem mutatható ki előre.

a szervezet biztonsági szintje 2. akkor, amikor az ismételhető, de ösztönös jellegű, azaz:
a) az elektronikus információs rendszerek biztonságával kapcsolatos felelősségeket és feladatokat egy, az elektronikus információs rendszer biztonságáért felelős személyhez rendelték hozzá, bár irányítási hatásköre korlátozott,
b) az elektronikus információs rendszerek biztonsága szükségességének tudatossága elaprózott és korlátozott,
c) annak ellenére, hogy az elektronikus információs rendszerek előállítanak biztonságra vonatkozó információkat, azokat nem elemzik,
d) előfordul, hogy a külső felek által nyújtott elektronikus információs szolgáltatások nem foglalkoznak a szervezet konkrét biztonsági igényeivel,
e) az elektronikus információs rendszerek biztonsági szabályzatai kidolgozása folyamatban van, de a vonatkozó szaktudások és eszközök nem megfelelőek,
f) az elektronikus információs rendszerek biztonságára vonatkozó jelentések nem teljesek, lehetnek félrevezetők, illetve nem tárgyszerűek,
g) van információbiztonsági képzés, de a részvétel elsősorban az egyének kezdeményezésén múlik,
h) az elektronikus információs rendszerek biztonságára úgy tekintenek, mint elsősorban az informatika felelősségére és területére, és a szakmai vagy üzleti területek úgy érzik, hogy az elektronikus információs rendszerek biztonsága nem az ő szakterületük.

a szervezet biztonsági szintje 3. akkor, amikor az szabályozható folyamat, azaz:
a) az elektronikus információs rendszerek biztonsági eljárásait meghatározták, és azokat összehangolták a biztonságpolitikával,
b) a biztonságtudatosságot megteremtették, és azt a vezetés támogatja,
c) az elektronikus információs rendszerek biztonságával kapcsolatos felelősségeket meghatározták, és azokat ismerik, de betartatásuk nem következetes,
d) a kockázatelemzés eredményeképpen létezik biztonsági terv és léteznek biztonsági megoldások,
e) a biztonsági jelentések nem szakmai (üzleti) megközelítésűek,
f) ad hoc jellegű biztonsági tesztelést végeznek (például behatolás tesztelést),
g) a biztonsági képzés az informatika és az üzleti területek rendelkezésére áll, de az ütemezése és a megtartása nem formalizált.

a szervezet biztonsági szintje 4. akkor, amikor az irányított és mérhető, azaz:
a) az elektronikus információs rendszerek biztonságával kapcsolatos felelősségi köröket egyértelműen meghatározták, menedzselik és betartatják,
b) a biztonsági kockázat- és hatáselemzés végrehajtása következetes,
c) a biztonságpolitika és az informatikai biztonsági szabályzat részeként konkrét biztonsági alapszinteket határoznak meg,
d) a biztonság tudatosítását elősegítő módszerek alkalmazása kötelező,
e) a felhasználói azonosítás, hitelesítés és jogosultság engedélyezés szabványosított,
f) törekszenek arra, hogy a biztonsági auditálásért és irányításért felelős munkatársak elektronikus információs rendszerek biztonságához kapcsolódó szakmai képesítést szerezzenek meg,
g) a biztonság tesztelését szabványos és formális folyamatok felhasználásával végzik, amelyek eredményeképpen a biztonsági szintek javulnak,
h) az elektronikus információs rendszerek biztonsági folyamatait koordinálják a szervezet általános biztonsági funkcióival,
i) az elektronikus információs rendszerek biztonságára vonatkozó jelentések az üzleti célkitűzésekhez kapcsolódnak,
j) az információbiztonsági képzést mind a szakmai (üzleti), mind az informatikai részlegeknél megtartják,
k) az információbiztonsági képzést a szakmai (üzleti) igények és a meghatározott biztonsági kockázati profilok alapján tervezik meg és menedzselik,
l) a biztonságirányítási célokat és metrikákat meghatározták, de még nem mérik.

a szervezet biztonsági szintje 5. akkor, amikor az optimalizált, azaz:
a) az elektronikus információs rendszerek biztonsága a szakmai (üzleti) és az informatikai vezetés közös felelőssége, és integrálva van a szervezeti biztonság szakmai (üzleti) célkitűzéseivel,
b) az elektronikus információs rendszerek biztonsági követelményeit egyértelműen meghatározták, optimalizálták és beépítették egy jóváhagyott biztonsági tervbe,
c) a felhasználók és az ügyfelek egyre inkább felelősek a biztonsági követelmények meghatározásáért, és a biztonsági funkció közreműködik már az alkalmazási rendszerek tervezési szakaszában,
d) a biztonsági rendkívüli eseményekkel haladéktalanul, automatizált eszközökkel támogatott, formalizált, rendkívüli helyzetkezelési eljárások segítségével foglalkoznak,
e) rendszeresen biztonsági felméréseket végeznek a biztonsági terv megvalósítása eredményességének értékelése céljából,
f) a fenyegetésekre és sebezhetőségekre vonatkozó információkat módszeresen, szisztematikusan begyűjtik és elemzik,
g) a kockázatok enyhítésére irányuló megfelelő kontrollokról haladéktalanul tájékoztatást nyújtanak és megvalósítják,
h) a folyamatos folyamatjavítás érdekében felhasználják a biztonsági tesztelést, a biztonsági rendkívüli események a probléma gyökerét feltáró elemzését és a kockázatok felismerését aktívan kezdeményezik,
i) a biztonsági folyamatokat és technológiákat a szervezetben integrálták,
j) a biztonságirányításra vonatkozó metrikákat mérik, begyűjtik és tájékoztatást adnak az eredményekről,
k) a vezetés ezen mutatókat felhasználja a biztonsági terv folyamatos javítási folyamat keretében történő kiegészítésére.

ÁLTALÁNOS INDOKOLÁS

A modern állam, és annak minden szervezete és polgára kiszolgáltatottá vált a számítógépekből, kommunikációs eszközökből és automata rendszerekből álló bonyolult, többszörösen összetett információs infrastruktúrának. Az elektronikus információs rendszerek nélkülözhetetlenné váltak a társadalom egésze számára, mert az állam működése, a különböző szolgáltatások megvalósítása és igénybevétele elképzelhetetlen ezen rendszerek nélkül. Már önmagukban ezeknek az információs rendszereknek a kiesése is katasztrófahelyzetet idézhet elő. Információs rendszereink és hálózataink – azok közül is elsősorban azok, amelyek működése elengedhetetlen a társadalom és a gazdaság zavartalan működéséhez – egyre gyakrabban szembesülnek az igen sokféle forrásból származó biztonsági fenyegetéssel. A szándékos károkozások olyan formái, mint a különböző hackercsoportok számítógépvírusokkal történő vagy az információs rendszer leállására vezető ún. szolgáltatás megtagadást eredményező támadásai egyre gyakoribbá, általánosabbá válnak, ugyanakkor ezek egyre vakmerőbbek és egyre bonyolultabbak is. Folyamatosan növekvő fenyegetést jelent sérülékeny információs rendszereinkre a hadviselés egy új formája, amelyet kiberműveleteknek (angolul: cyber operations) neveznek, de még inkább a békeidőkben is állandóan fenyegető terrorizmus számítógépes változata, a kiberterrorizmus. A különböző információs infrastruktúrák, eszközök, és szolgáltatások bármelyikének megsemmisülése vagy sérülése a társadalom széles rétegeit érintheti. A modern gazdasági berendezkedés mellett a társadalom nincs felkészülve arra, hogy a kiesett infrastruktúrák, eszközök vagy szolgáltatások nélkül működjön, így ezeket – egyértelműen – védeni kell.

A törvénytervezet az állam kiberbiztonságot érintő szerepét és feladatait meghatározó Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozat figyelembevételével készült.

Bizonyos közigazgatási informatikai rendszerek biztonságát korábban az elektronikus közszolgáltatás biztonságáról szóló 223/2009. (X. 14.) Korm. rendelet szabályozta, amely 2012. áprilisában hatályon kívül helyezésre került, így jelenleg nincsen olyan jogszabály, amely egységes biztonsági követelményeket szabna az elektronikus információk védelmével kapcsolatban.

A minősített adatok és az ezeket kezelő elektronikus információs rendszerek védelme a minősített adatok védelméről szóló 2009. évi CLV. törvényben és a végrehajtására kiadott rendeletekben szabályozásra került.

A nemzet szempontjából fontos, a minősített adatok körébe nem tartozó, de a kezelt adatok jellegére és a nyilvántartások alapján végzett állami feladatok fontosságára tekintettel kiemelt jelentőségű állami nyilvántartások védelmének biztosítását a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény szolgálja.

Jelen törvény hatálya kiterjed a létfontosságú infrastruktúrákra is, melynek alapvető rendelkezéseit – a Kormány 2012. szeptembert 12-ei ülésén megvitatott és elfogadott – a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvényjavaslat tartalmazza.

A törvényjavaslat tudatosan használja az információbiztonság, információs rendszer kifejezések előtt az „elektronikus” jelzőt. Az információbiztonság ugyanis a szóban, rajzban,

írásban, a kommunikációs, informatikai és más elektronikus rendszerekben, vagy bármilyen más módon kezelt adatok védelmére vonatkozik. Ezzel szemben az elektronikus információs rendszerek biztonsága csak az elektronikus információs rendszerekben szereplő adatok, és az azokat kezelő rendszer védelmét jelenti. A törvényjavaslat pedig az elektronikus információs rendszerekben tárolt, kezelt információk védelmét célozza az azokat kezelő szervezetek biztonságának növelésén keresztül.

Az elektronikus információs rendszerek védelme egy igen széles körű információvédelem része, amely önállóan is működtethető. A NATO *Security within the North Atlantic Treaty Organisation* direktívája szerinti elektronikus információvédelmen (INFOSEC) kívül az információvédelem többi részét (személyi védelem, dokumentumvédelem, fizikai védelem) is magába foglalja, de csak az elektronikus információs rendszer vonatkozásában.

Az elektronikus információs rendszerek értelmezése az informatikai, a kommunikációs, és az egyéb elektronikus rendszerek konvergenciájára épül. Az információs társadalomhoz és a médiához kötődő iparágak konvergenciáról az Európai Bizottság *i2010: európai információs társadalom a növekedésért és a foglalkoztatásért című* (COM(2003) 784) közleménye az európai audiovizuális politika szabályozásának jövőjére vonatkozóan megállapítja, hogy „Az információs társadalom és a média területén működő szolgáltatások, hálózatok és eszközök digitális konvergenciája végre mindennapjaink valóságává válik …”. Ezt is figyelembe véve az elektronikus információs rendszerekhez tartozik:

1. a számítástechnikai rendszerek és hálózatok, ide értve az internet szolgáltatást is;
2. a vezetékes, a mobil, a rádiós és műholdas távközlés;
3. a vezetékes, a rádiófrekvenciás és műholdas műsorszórás;
4. a rádiós vagy műholdas navigáció;
5. az automatizálási, vezérlési és ellenőrzési rendszerek (SCADA[2], távmérő, távérzékelő és telemetriai rendszerek, stb.);
6. a fentiek felderítéséhez, lehallgatásához vagy zavarásához használható rendszerek.

A törvényjavaslat egy preventív szabályozási környezetnek az alapjait kívánja megteremteni, amely ténylegesen a megelőzést helyezi előtérbe és ezen keresztül a biztonsági problémák kialakulásának mérséklését és az előforduló incidensek számának csökkentését célozza.

RÉSZLETES INDOKOLÁS

Az 1. §-hoz

A törvényjavaslat 1. §-a a szabályozás személyi és tárgyi hatályát határozza meg.
A személyi hatály az alkotmányos rend fenntartása szempontjából kiemelt fontosságú közszolgálati szervek adatait kezelő szervezetek és a nemzeti adatvagyont kezelő szervezetek mellett az európai és nemzeti létfontosságú információs rendszerek, rendszerelemek közé tartozó szervezetekre terjed ki. Az érintett szervek felsorolásának alapját a központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvény, a bíróságok szervezetéről és igazgatásáról szóló 2011. évi CLXI. törvény, az ügyészségről szóló 2011. évi CLXIII. törvény és a fővárosi és megyei kormányhivatalokról, valamint a fővárosi és megyei kormányhivatalok kialakításával és a területi integrációval összefüggő törvénymódosításokról szóló 2010. évi CXXVI. törvény képezi.

[2] Supervisory Control and Data Acquisition (System) – vezérlő és adatgyűjtő rendszer

A tárgyi hatály a kiemelt fontosságú közszolgálati szervek adatait és a nemzeti adatvagyont kezelő szervezetek, valamint az európai és nemzeti létfontosságú információs infrastruktúrák elektronikus információs rendszereinek védelmére vonatkozik.

Ez a személyi és tárgyi hatály kellően széles körű ahhoz, hogy Magyarország kibervédelme szempontjából minden, az állam működése szempontjából lényeges elektronikus információs rendszer védelmére kitérjen.

A törvényjavaslat az egységes szabályozási környezet kialakítása érdekében rendelkezik a más törvényekkel való összhangról. Ennek értelmében a minősített adatok vonatkozásában e törvény rendelkezéseit a minősített adat védelméről szóló 2009. évi CLV. törvényben foglalt eltérésekkel kell alkalmazni.

A törvényjavaslat kifejezetten elkülöníti a Magyar Honvédség, a rendvédelmi szervek és a Katonai Nemzetbiztonsági Szolgálat, valamint a külpolitikáért felelős miniszter diplomáciai információs célokra használt – külön jogszabályban meghatározott – zárt célú elektronikus információs rendszereit. Ezeknek az esetében is kötelező a megfelelő biztonság kialakítása és fenntartása, de a rendszerek fokozott védelme érdekében a hatósági és eseménykezelési feladatok az irányítást ellátó miniszter felelősségi körén belül maradnak, így nem nő azok köre, akik ezen érzékeny rendszereket, azok védelmi megoldásait megismerhetik, vagy akár annak védelmét felülbírálhatnák.

A 2. §-hoz

A nemzeti adatvagyont kezelő szervezetek, illetve a létfontosságú rendszerelemként számításba vehető szervezetek egy része komoly munkával és jelentős költségekkel auditáltatta szervezetét az informatikai biztonságirányítási rendszerről szóló nemzetközi ISO/IEC 27001 szabvány szerint, illetve a nemzetközi egyezménnyel elfogadott Common Criteria szerint minősített informatikai eszközöket használ. Ezek a minősítések megfelelő védelmet biztosítanak, így – és a jogbiztonság megőrzését is szem előtt tartva – ezen tanúsítványokat a hatóság az eljárása során figyelembe veszi.

A 3. §-hoz

A törvényjavaslat arra való tekintettel, hogy napjainkban fontos kérdés az adatok külső szolgáltatónál történő tárolása, illetve az elektronikus információs rendszerek kiszervezése általánosan elfogadott gyakorlattá vált (ezzel a nemzeti adatvagyon törvény is foglalkozik már), korlátozza az adatvagyon Magyarország területén kívüli kezelését. Ez a tilalom nem terjedhet ki azonban a Magyar Honvédségre és a külképviseletekre, mert ezek feladatukból adódóan külföldön is kell, hogy dolgozhassanak adataikkal, elektronikus információs rendszereikkel. A létfontosságú információs infrastruktúrákhoz olyan intézmények tartozhatnak (pénzintézetek, távközlési szolgáltatók, stb.), amelyek esetében a csak Magyarország területén belül engedélyezett adatkezelés súlyos költségkihatásokkal járhat. Itt az adatok Európai Unión belüli kezelésének kényszere elégséges korlátozás, mert az uniós és az uniós országok nemzeti szabályozása megfelelő védelmet és ellenőrizhetőséget biztosít.

Mivel a nemzeti adatvagyon eleme része lehet a létfontosságú információs infrastruktúráknak, de kötelezően nem az, ezért a törvényjavaslat szerinti szigorító kivétel a csak hazai kezelésre.

Az adatok külső szolgáltatónál történő tárolása, illetve az elektronikus információs rendszerek kiszervezése miatt került a törvényjavaslatba az a kényszer, hogy amennyiben nem Magyarországon bejegyzett cég végzi az adatok kezelését, akkor legyen elérhető

kapcsolattartó személy, illetve ez a személy legyen felkérhető, utasítható a törvény végrehajtásával kapcsolatban, és akár a felelősségre vonásra is sor kerülhessen.

A 4. §-hoz

A 4. § a törvényjavaslat értelmező rendelkezéseit tartalmazza.
Az értelmező rendelkezések az elfogadott és általánosan alkalmazott hazai szakkifejezésekre épülnek. Ezek jelentős része a Kormány 3296/1991. (VII.5.) határozata alapján 1991.november 27-én létrehozott Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága 12. számú ajánlásaként 1996. április 2-án elfogadott Informatikai Rendszerek Biztonsági Követelményei című dokumentumban rögzítésre került. Az itt leírt fogalmak és definíciók az Informatikai Biztonság Kézikönyve (Verlag Dashöfer, Budapest, 2000-2005), illetve a Közigazgatási Informatikai Bizottság 25. és 28. számú ajánlásaiban is megjelentek, a nemzetközi szakirodalmat, szabványokat figyelembe véve újra feldolgozva korábbi definíciókat. Az információ- és kommunikációtechnológiák konvergenciája miatt magyarul az informatikai és kommunikációs technológia, néha az informatikai és kommunikációs rendszerek kifejezéseket, gyakran az angol information and communication technology kifejezés rövidítését az ICT-t vagy ennek rossz magyarsággal való átírását az IKT-t használják. Emellett az informatikai, infokommunikációs technológia, vagy az infokommunikációs rendszerek kifejezéseket is alkalmazzák. Az eltérő fogalomhasználat egységesítése érdekében a törvényjavaslat az elektronikus információs rendszerek kifejezést használja.

Az 5-6. §-hoz

A törvényjavaslat egyik legfontosabb eleme az alapvető elektronikus információbiztonsági követelmények meghatározása. Az ebben a körben használt fogalmakat az informatika szakma már régóta használja ugyan, de azok törvényi szinten, általános követelményként történő megfogalmazása olyan előrelépést jelent az elektronikus információs rendszerek biztonsága területén, ami önmagában mérföldköve lehetne az elmúlt időszak ezirányú szabályozási törekvéseinek.

A törvényjavaslat az elektronikus információs rendszerek biztonságának általános követelményeit az elektronikus információs rendszerek biztonságának definíciójából levezetve, úgy határozza meg, hogy a védelem minden lehetséges módja (logikai, fizikai és adminisztratív védelem) a tervezéstől a megvalósításig felhasználásra kerüljön. A védelem olyan legyen, hogy lehetőleg kerülje el a fenyegetések bekövetkezését, de ha ez nem lehetséges, akkor erről annak bekövetkezése előtt az érintettek szerezzenek tudomást. Az elektronikus információs rendszerek esetében különösen fontos a biztonsági események bekövetkeztének azonnali, vagy gyors észlelése, hogy arra mielőbb reagálhasson a szervezet vezetése. A biztonsági esemény bekövetkezése után kiemelt szerepet kap a gyakran incidenskezelésnek is nevezett eseménykezelés. Ennek során a bekövetkezett biztonsági esemény dokumentálása, a bekövetkezett károk következményeinek a felszámolása, a biztonsági eseményt kiváltó okok kivizsgálása és felelősségek megállapítása és a szükséges felelősségre vonás után a szabályozás javításával, a védelmi intézkedések kiegészítésével vagy megerősítésével és az érintettek oktatásával, tudatosság képzésével gondoskodni kell arról, hogy az adott biztonsági események bekövetkezésének esélye kisebb legyen és az ezáltal okozott kár is csökkenjen.

A törvényjavaslat elfogadja azt a nézetet, hogy a védelem tevékenység, illetve tevékenységek

sorozata, amely arra irányul, hogy megteremtse, fejlessze, vagy szinten tartsa azt az állapot, amit biztonságnak nevezünk. A biztonság a védett rendszer olyan állapota, amelyben annak védelme az összes számításba vehető fenyegetettséget figyelembe veszi, a rendszer valamennyi elemére kiterjed, az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósul és annak költségei hosszútávon arányosak a fenyegetések által okozható károkkal.

A biztonság nagyon sok részletet jelent, ugyanakkor egy és oszthatatlan. Ezt az egy és oszthatatlan biztonságot a védelmi tevékenységek (folyamatok) részterületein keresztül lehet megvalósítani. Az információbiztonság alapvető feladatai a megelőzés és a korai figyelmeztetés, az észlelés, a reagálás és a biztonsági események kezelése. A korai figyelmeztetés előírásként történő meghatározása nem figyelmeztető rendszer kiépítésére, hanem a szervezet aktív cselekvési képességére vonatkozik, az észlelés folyamatának azon része, amely más szervezettől érkező figyelmeztetések azonosítására és feldolgozására utal.

A biztonság tervezése, kialakítása során e feladatok mindegyikére kellő hangsúlyt kell fektetni ahhoz, hogy a védelem elérje célját.

A 7-8. §-hoz

A védelemnek költséghatékonynak kell lennie, azaz csak a lehetséges veszteségek és károk nagyságrendjével arányosan indokolt a védelemre költeni. Ennek érdekében meg kell állapítani, hogy az adott elektronikus információs rendszer, illetve az abban kezelt adatok a bizalmasságának, a sértetlenségének vagy a rendelkezésre állásának elvesztése külön-külön milyen nagyságrendű károkat okoz. A nagyságrend megállapítása elégséges, mert egyrészt a pontos értéket nehéz, hosszadalmas és költséges meghatározni, másrészt a nagyságrend ismerete már elég ahhoz, hogy a védelemre történő ráfordítások értéke meghatározható legyen. Mivel az osztályba sorolást külön el kell végezni a bizalmassági, sértetlenségi és rendelkezésre állási szempontok szerint is, így minden egyes elektronikus információs rendszerre számos kombinációban állíthatók be a műszaki védelmi intézkedések. Ez biztosítja a kockázatarányos és költséghatékony műszaki védelmet. A biztonsági osztályozás részletszabályainak meghatározására a törvény végrehajtási rendeletében kerül sor.

Ilyen biztonsági osztályozás és a hozzátartozó követelmények már megtalálhatók az *Informatikai Biztonsági Irányítási Követelmények* című Közigazgatási Informatikai Bizottsági ajánlásban (KIB 25. sz. ajánlás 1-2. kötet), valamint hasonló követelménylistát tartalmaz a KIB 28. ajánlás is. A törvényjavaslat ezen technológiai követelményeknek miniszteri rendeletben történő megjelenítését szorgalmazza.

A szervezet vezetőjének a felelőssége, hogy az elektronikus információs rendszerek osztályba sorolását elvégezzék. Mivel a kockázatok folyamatosan változnak, ezért az osztályba sorolást rendszeresen frissíteni kell. Ez az elvárás biztosítja azt, hogy a biztonság ne egy statikus, egyszer kialakított állapot legyen, hanem a szervezetnek folyamatosan figyelemmel kelljen kísérnie a rá vonatkozó kockázatokat, azaz legyen egy kockázatkezelési folyamata. A mérvadó információbiztonsági szabványok és ajánlások kivétel nélkül ezt a lépést tekintik a legalapvetőbb elvárásnak a biztonság megteremtéséhez.

A szervezetek biztonsági osztályának és biztonsági szintjének meghatározása a fokozatosság elvére épül. Az adott osztály és szint elérése a szervezet feladat- és hatáskörének függvénye, amelyek biztosítják, hogy a szervezet a feladatellátásával, a közigazgatási

szervezetrendszerben elfoglalt helyével, piaci szerepével, valamint elektronikus információs rendszereinek jelentőségével, állapotával arányosan kerüljön kialakításra.

A 9-10. §-hoz

A megelőzés alapját képező, kockázatokkal arányos, költséghatékony védelem kialakításának egyik nemzetközileg elfogadott eszköze az információbiztonsági irányítási rendszer kialakítása a szervezetnél. Ez biztosítja, hogy az alapvető biztonsági követelmények meghatározása egy magas absztrakciós szinten is megtörténjen. Az Information Systems Audit and Control Association (ISACA) elismert nemzetközi szakmai szövetség *Control Objectives for Information and Related Technologies (COBIT)* című keretrendszere 4.1 verziója szerinti „érettségi modell" jól alkalmazható az információbiztonsági irányítási rendszer bevezetettségi szintjének meghatározásához. Ezt az érettségi modellt kissé átalakítva kerültek kialakításra a „szervezetek biztonsági szintjei". A szervezeti biztonság megteremtése azért is fontos, mert bevezetésének költsége elenyésző (elsősorban szabályozási feladatokat határoz meg), mégis jelentősen növeli az információbiztonság szintjét.

Eszerint minden érintett szervezetnek kötelessége rendszerszinten kezelnie az információbiztonságot.

A törvényjavaslat egyik fontos követelménye az, hogy a szervezetnek azt a biztonsági szintet kell elérnie az információbiztonsági irányítási rendszerében, amely megegyezik az általa kezelt elektronikus információs rendszerek közül a legmagasabb biztonsági osztállyal. Azaz, ha pl. nemzeti adatvagyon-elemet kezelő rendszere van a szervezetnek, a legmagasabb érettségi szintet kell elérnie, vagy ha pl. egy központi államigazgatási szerv olyan elektronikus információs rendszert kezel, melyben az információk bizalmassági besorolása 2., sértetlenségi besorolása 3., rendelkezésre állási besorolása pedig 1., akkor a szervezeti biztonsági szintjét 3. szintre kell hoznia. Ha ennél a szervezetnél minden érték 2., a szervezeti biztonsági szintje akkor is 3., hiszen a törvényjavaslat 9. § (2) bekezdés b) pontja eszerint rendelkezik.

A 7-9. és a 10-11. §-ok együttes alkalmazása költséghatékony megoldás, mert nem a szervezet egészénél egységesen, azonos biztonsági osztályba sorolva kell az elektronikus információs rendszerek védelmét megvalósítani, hanem ez rendszerenként eltérő lehet. A szervezet biztonsági szintjének elérése viszont garantálja, hogy az információbiztonsági irányítási rendszer a legmagasabb kockázatok által elvárt legyen.

A szervezeti biztonsági szintet ugyan az általa kezelt elektronikus információs rendszer besorolása határozza meg, de ennek a biztonsági szintnek az elérése jól tervezhető módon, kellő időráfordítással valósítandó meg. A szervezet vezetője kezdetben besorolja a szervezetet az aktuális érettségi szintre, majd kétévente köteles egy szintet lépni a skálán mindaddig, amíg eléri az elvárt szintet. Pl. egy olyan központi államigazgatási szervnél, ahol nincsen jelen az információbiztonsági szabályozás, akár 4 év is rendelkezésre áll a követelmények teljesítéséhez.

A 11-12. §-hoz

A törvényjavaslat ezen szakaszai az érintett szervezetek vezetőinek legfontosabb, a szervezet besorolási szintjétől és az elektronikus információs rendszer besorolási osztályától független feladatait és felelősségeit határozzák meg. Ezek a feladatok elsősorban adminisztratív

feladatok, amelyek arra vonatkoznak, hogy a szükséges szinten és a szükséges mélységben legyen szabályozva az elektronikus információs rendszerek biztonsága, és annak nevesített felelőse legyen a szervezetnél.

A szervezet vezetőjének felelősségét nem csökkenti, ha az elektronikus információs rendszer kiszervezésre kerül, függetlenül attól, hogy a közreműködőkkel kötött szerződésben köteles a törvényi rendelkezések kötelező alkalmazását előírni.

Az előírások között a folyamatos oktatás, képzés kötelezettségének rögzítése egy, a technikai fejlődés következtében gyorsan változó területnek való megfelelés miatt szükséges.

A szervezet vezetője köteles együttműködni a Nemzeti Elektronikus Információvédelmi Hatósággal, így lehetőség nyílik arra, hogy a védelmi tevékenységben szükséges kapcsolattartás és információcsere megvalósulhasson. Ezen információcsere egyik legfontosabb esete a törvényjavaslatban külön nevesítésre került: a szervezet vezetője köteles a bekövetkezett biztonsági eseményeket a Nemzeti Elektronikus Információvédelmi Hatóság, a Nemzeti Biztonsági Felügyelet és az incidenskezelési feladatokat ellátó kormányzati eseménykezelő központ tudomására hozni. Ez is hozzájárul az országos szintű kibervédelmi rendszer kialakításához; mely összhangban van az Európai Unió tervezett kibervédelmi intézkedéseivel.

A 13. §-hoz

A törvényjavaslat előírja, hogy a szervezeteknek legyen olyan munkatársa az elektronikus információs rendszer biztonságáért felelős személyében, aki képes az elektronikus információs rendszerek védelmének feladatait összefogni, koordinálni. Hatásköre mindenre ki kell, hogy terjedjen az elektronikus információs rendszerek védelme kapcsán, ugyanakkor felelőssége oszthatatlan. Az információs rendszer biztonságáért felelős személy alapfeladatainak meghatározására a szervezet besorolási szintjétől és az elektronikus információs rendszer besorolási osztályától függetlenül, általánosságban került sor.

A törvényjavaslat nagy hangsúlyt helyez a felhasználói tudatosság növelésére, melynek révén elérhető, hogy maguk az érintettek is körültekintően védjék adataik biztonságát, megértve a kérdés jelentőségét. Ennek érdekében a törvény hatálya alá tartozó szervezetek munkatársainak, kiemelten az elektronikus információs rendszer biztonságáért felelős személyeknek a törvény kötelező képzésen való részvételt ír elő.

A 14-16. §-hoz

A törvényjavaslat szerint létrejön az informatikáért felelős miniszter irányítása alatt, a minisztérium szervezeti keretében önálló feladattal és hatósági jogkörrel rendelkező Nemzeti Elektronikus Információvédelmi Hatóság (a továbbiakban: Hatóság), amely az információbiztonsággal kapcsolatos nyilvántartásokat vezeti, illetve ellenőrzi a törvény betartását.

Létrehozásának indoka, hogy kell egy olyan hatóság, amely képes ellenőrizni az e törvényben foglalt és az ahhoz kapcsolódó követelmény megvalósulását. Ennek keretében jogosult szankcionálni azokban az esetekben, amikor a szervezetnél az elektronikus információs rendszert veszélyeztető informatikai állapot alakul ki. Nem közigazgatási szervek esetében bírságolási joga van.

A 17 §-hoz

A Hatóság közigazgatási szervek esetében információbiztonsági gondnokot nevezhet ki. Az információbiztonsági gondnok jogosult a szervezet által meghozott védelmi intézkedéseket véleményezni, adott esetben az intézkedéssel szemben kifogással élhet. A fenyegetés elhárítása érdekében intézkedéseket, eljárásokat javasolhat. Ezzel a jogkörrel a törvényjavaslatban foglaltak megvalósítása jelentősen hatékonyabban történhet meg.

A 18. §-hoz

A Nemzeti Biztonsági Felügyelet (a továbbiakban: NBF) feladatai komplex rendszerbe foglalhatóak:

- egyrészről a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény szerinti szakhatóságként igazgatási szolgáltatási díj ellenében közreműködik az osztályba sorolás és a biztonsági szint meghatározására, a Hatósághoz érkező bejelentések kivizsgálására vonatkozó, a Hatóság által lefolytatott eljárásban, valamint a Hatóság éves ellenőrzési terv alapján végzett ellenőrző tevékenységében,
- másrészről a szervezet felkérésére az ellenőrzési tervtől függetlenül is végezhet sérülékenységvizsgálatot, feltárva ez által a biztonsági esemény bekövetkezését megelőzően az esetleges sérülékenységeket, hiányosságokat, költséghatékonnyá téve ez által a megelőzést,
- harmadrészről hazai információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokat szervez, valamint a nemzetközi információbiztonsági, létfontosságú információs infrastruktúra védelmi, kibervédelmi gyakorlatokon felkérésre képviseli Magyarországot, koordinálja, irányítja a magyarországi felek részvételét.

A Hatóság és az NBF közötti feladatmegosztás leképezi a kormányzaton belüli feladat meghatározást, melynek értelmében az informatikai terület ellenőrzése az informatikáért felelős miniszter feladat- és hatáskörébe, míg a szélesebb értelemben vett információbiztonság az e-közigazgatásért és a minősített adatok védelmének szakmai felügyeletéért felelős miniszter feladatkörébe tartozik.

A 19-20. §-hoz

A törvényjavaslat az incidenskezelés, a károk mérséklése érdekében megfogalmazza azokat az incidenskezelési funkciókat, melyek értelmében hálózatbiztonsági helyzetértékeléseket, folyamatos 24 órás ügyeletet kell működtetni.

A törvényjavaslat szerinti kormányzati eseménykezelő központ és annak feladatai korábban is léteztek, az időközben hatályon kívül helyezett, az elektronikus közszolgáltatás biztonságáról szóló 223/2009. (X. 14.) Korm. rendeletben. Ágazati eseménykezelő központból (CERT) több is létrehozható – a zárt célú hálózatok esetében ez egyébként is indokolt –, figyelemmel kell lenni azonban arra, hogy a nemzetközi CERT közösség elsősorban bizalmi elven működik, ezért indokolt, hogy Magyarországot egy nemzetközileg elismert CERT, a kormányzati eseménykezelő központ képviselje. A kormányzati eseménykezelő központ az ágazati eseménykezelő központok operatív tevékenységét koordinálja, így részt vesz az információk megosztásában. A kormányzati eseménykezelő központ támogatja a CERT-eket a nemzetközileg elfogadott működési rend kialakításában.

A 21. §-hoz

A törvényjavaslat értelmében tanácsadó testület jön létre és működik
- az elektronikus információs rendszerek biztonságát érintő kérdések felmérése,
- a kibervédelem helyzetének figyelemmel kísérése és
- az ehhez kapcsolódó feladatok irányvonalainak meghatározása érdekében.

A testület jellegéből adódóan sok szempontból képes áttekinteni az elektronikus információs rendszerek biztonságával, a létfontosságú információs infrastruktúrák védelmével, és a kibervédelemmel kapcsolatos feladatokat, javaslataiban képes megjeleníteni az abban résztvevők szakmai álláspontját.
Működése ez által hozzájárul az elektronikus információs rendszerek gyors fejlődéséhez, a fenyegetések változásához igazodó követelmények kialakításához.

A 22. §-hoz

Az elektronikus információs rendszerek összetettsége és működésének sajátossága miatt a gyakorlatban gyakran nem valósul meg a törvényes adatkezelés elvének betartása. A törvényjavaslat külön kiemeli a biztonságos és törvényes adatkezelés követelményeinek kölcsönös figyelembevételét.

A 23. §-hoz

A törvényjavaslat alapvető célja az az elektronikus információs rendszer biztonságáért felelős személy kötelező információbiztonsági képzésének előírása. A hazai felsőoktatási környezetben az információbiztonság területén jelenleg ilyen kötelező jellegű, intézményesített vezetőképzés nincs. A mérnök, a programozó és a gazdasági informatikus alapszakokon és mesterszakokon különböző műszaki jellegű oktatások vannak, amelyek között a Budapesti Műszaki Egyetemen és az Óbudai Egyetemen informatikai biztonsági szakirányú képzést is tartanak. A Nemzeti Közszolgálati Egyetemen a nemzetbiztonsági képzés keretén belül oktatnak informatikai védelmet. Akkreditált felnőttképzés e téren a Nemzetközi Technológiai Közhasznú Kft. (Puskás Alapítvány) informatikai biztonsági felelős képzése, amely alapvetően az időközben hatályon kívül helyezett, az elektronikus közszolgáltatás biztonságáról szóló 223/2009. (X. 14.) Korm. rendelet követelményeihez igazodik. A törvényjavaslatban előírt követelményeknek megfelelő képzés és a vezetőképzés erősítése érdekében mindezekre figyelemmel szükséges egy új átfogó képzési struktúra kialakítása.

Az információbiztonsági tudatosság növelése érdekében a Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Kara javaslatot tesz a képzési követelményekre, és részt vesz a törvény hatálya alá tartozó személyek kötelező oktatásában. Ez biztosítja, hogy az érintettek magas színvonalú képzésben részesüljenek.

A Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Kara az elektronikus információs rendszerek biztonsága, a létfontosságú információs infrastruktúrák védelme, a kibervédelem tekintetében a jövőben nemzeti és esetleges nemzetközi kutatóhelyként is részt vehet a szakterület kutatásában, fejlesztésében. E feladatokban való részvétellel az egyetemi oktatók-kutatók folyamatos gyakorlati ismereteket szereznek, illetve azokat karbantartják. Az oktatói-kutatói kapacitást a szükséges szakmai kidolgozó munkában költséghatékonyabban lehet felhasználni, mint külső cégeket igénybe venni erre a feladatra.

A törvényjavaslat az oktatás, fejlesztés és a gyakorlat kombinációjával egy magas szintű oktatási, kutatás-fejlesztési centrumot hoz létre az elektronikus információs rendszerek biztonságának területén.

A nemzetközi oktatási környezetben már számos akkreditált képzés elfogadott. Ezek közül a legelismertebbek közé tartozik:

- Az Information Systems Audit and Control Association (ISACA) nemzetközi szervezet Certified Information Security Manager (CISM) képzése, amelyet az USA Védelmi Minisztériuma is szakirányú képzésként ismer el és vezetői szintű ismereteket nyújt. A képzést Magyarországon felsőfokú oktatási intézményekben – külön megállapodás alapján –, az ISACA magyarországi szervezetének felügyeletével, hazai informatikai szakemberek külföldi tananyag és követelmények alapján tartják. A képzés eredményes elvégzését ANSI-ISO szabvány szerint akkreditált oklevél igazolja.
- Az International Information Systems Security Certification Consortium, Inc. Certified Information Systems Security Professional (CISSP) képzése az informatikai rendszerek technikai kérdéseinek biztonsági vonatkozásairól szól. A képzést Magyarországon a Budapesti Műszaki Egyetemen hazai informatikai szakemberek külföldi tananyag és követelmények alapján tartják. A képzés eredményes elvégzését ANSI-ISO szabvány szerint akkreditált oklevél igazolja.

Mindkét (CISM, CISSP) végzettség megszerzéséhez gyakorlati tapasztalatokat is igazolni kell, a képzések időtartama eltérő, a minősítések megtartásához éves szinten meghatározott kreditpontot kell elérni.

Nemzetközileg ismert és elfogadott még az EC-Council Certified Ethical Hacker és Certified Penetration Tester képzés, amely Magyarországon a Net Académia Oktatóközpontnál végezhető el.

A képzések üzleti alapon, a hazai viszonylatokhoz képest nagyon drágán működnek, ezért célszerű a költséghatékonyabb és a nemzetközi oktatási környezettel összhangban álló – adott esetben a későbbiekben mesterképzés útján elismertethető – hazai képzést előnyben részesíteni, ami egyúttal a kutatási kapacitás fejlesztését is lehetővé teszi.

A 24. §-hoz

A törvényjavaslat végrehajtásához a tervezetben megfogalmazott végrehajtási rendeletek kiadása szükséges.

A közigazgatási informatikai feladatok kormányzati koordinációjáról szóló 1026/2007. (IV. 11.) Korm. határozat 3. pontja alapján létrehozott Közigazgatási Informatikai Bizottság által 2008. júniusában kiadott, az információbiztonsági követelményekhez kapcsolódóan a meglévő és a terület részletes szabályozását szolgáló 25. ajánlásnak a Magyar Informatikai Biztonsági Irányítási Keretrendszer és Magyar Informatikai Biztonsági Értékelési és Tanúsítási Séma részeit és a 28. ajánlás IT biztonsági követelményrendszer – biztonsági szintek követelményeit rendeli felhasználni. Ezek az ajánlások a szakterület legfontosabb szabványaira, az ISO/IEC 27000-es sorozatra és a Common Criteriára épülnek, de nem teljesen azonosak azokkal. Ezeket a szabványokat már sok helyen használják hazánkban is, általánosan elfogadottak az Európai Unióban és a NATO-ban is. Miniszteri rendeletben történő kiadásukkal elérjük, hogy a hazai követelmények igazodjanak a nemzetközi szabványokhoz, de ennek ellenére Magyarország kormányzata saját hatáskörében képes azt szigorítani, vagy enyhíteni, igazítani a nemzeti igényekhez. A törvényjavaslatban foglalt követelményekhez kapcsolódóan a meglévő és a terület részletes szabályozását szolgáló

Közigazgatási Informatikai Bizottság 25. és 28. számú ajánlásait célszerű már a törvény elfogadásával egy időben egységes követelményrendszerként kiadni. Ez egyértelművé teszi a részletes szabályozás szakmai tartalmát, és biztos alapot teremt a későbbi szabályozáshoz. A Közigazgatási Informatikai Bizottság 28. ajánlása Európai Uniós forrásból finanszírozott, így megtérülési szempontból is indokolt a további felhasználása.

A 25. §-hoz

A törvényjavaslat hatályba léptető rendelkezést tartalmaz.

A 26. §-hoz

A törvényjavaslat alapján a törvény rendelkezései 2013. március 1–jén lépnek hatályba. Az átmeneti rendelkezések megfelelő türelmi időt határoznak meg annak érdekében, hogy a törvényjavaslat hatálya alá tartozó alanyok felkészülhessenek a törvényjavaslatban megfogalmazott követelmények betartására és betartatására.

A 27-28. §-hoz

A törvényjavaslat elfogadásával két törvény módosítása válik szükségessé:

- a minősített adatok védelméről szóló 2009. évi CLV. törvény kiegészítésével egyértelművé válik, hogy a minősített adatokat elektronikusan kezelő rendszerek tekintetében az elektronikus biztonság kialakítása során nem csak a minősített adatokra vonatkozó, hanem az e törvényben meghatározott követelményekre is figyelemmel kell lenni, ugyanakkor a besorolási kötelezettség automatizmusra épül: a minősített adatkezelő rendszerek külön vizsgálat nélkül sorolandóak be a legmagasabb védelmi szintet követelő osztályba,
- a nemzeti adatvagyonról szóló 2010. évi CLVII. törvény rendelkezéseinek hatályon kívül helyezését a differenciált, ezáltal költséghatékony információbiztonsági védelmi intézkedések iránti igény indokolja.