

A Kormány

..../2015. (VI....) Korm. rendelete

a központosított informatikai és elektronikus hírközlési szolgáltató feladatköréről, továbbá a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről szóló 484/2013. (XII. 17.) Korm. rendelet módosításáról

A Kormány

az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 24. § (1) bekezdés g) pontjában kapott felhatalmazás alapján, valamint a 6. § tekintetében az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 24. § (1) bekezdés f) pontjában kapott felhatalmazás alapján, az Alaptörvény 15. cikk (1) bekezdésében meghatározott feladatkörében eljárva a következőket rendeli el:

1. Értelmező rendelkezések

1. §

E rendelet alkalmazásában szolgáltató: a központosított informatikai és elektronikus hírközlési szolgáltató (a továbbiakban: központi szolgáltató) részére jogszabályban meghatározott, az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) hatálya alá tartozó elektronikus információs rendszerek felhasználói számára a központi szolgáltató által kötelezően biztosítandó központosított informatikai és elektronikus hírközlési szolgáltatások.

2. A központi szolgáltató feladatai

2. §

Az Ibtv. 2.§ (2) bekezdés a) és b) pontja, valamint 11. § (2) és (3) bekezdése alapján a központi szolgáltató

a) kialakítja az informatikai biztonsági irányítási rendszerét, aminek keretében

- aa) kidolgozza a vonatkozó szabályzatokat a rendszer működési követelményeinek megfelelően;
- ab) megismerteti az a) pont szerinti szabályzatokat a központi szolgáltató szolgáltatását igénybevevő szervezettel;
- ac) rendszeresen felülvizsgálja az a) pont szerinti szabályzatokat;
- ad) kidolgozza az a) pont szerinti szabályzatok módosításait;
- ae) ellenőrzi az a) pont szerinti szabályzatok megfelelő alkalmazását.

b) azonosítja és nyilvántartja:

ba) a szolgáltatásokat;

TERVEZET

- bb)* a szolgáltatások felhasználóit, az üzemeltető felhasználókat, valamint a szolgáltatás biztosításához igénybevett támogatókat és fejlesztőket, továbbá a hozzáférési jogosultságaikat;
- bc)* a szolgáltatások biztosításához szükséges vagyonelemek (hardver és szoftver elemek);
- bd)* a szolgáltatásokhoz kapcsolódó távoli hozzáféréseket;
- be)* a központi szolgáltató által a szolgáltatások biztosításához igénybevett külső szolgáltatásokat;
- bf)* a szolgáltatások *ca)* pontban meghatározott kritikusságát.

c) folyamatos kockázatelemzés keretében:

- ca)* meghatározza a szolgáltatások és az azokat biztosító vagyonelemek, valamint az igénybe vett külső szolgáltatások kritikusságát és fenyegetettségének mértékét;
- cb)* elvégzi a szolgáltatások kockázatértékelését;
- cc)* az egyes kockázati értékek alapján meghatározza a szolgáltatások biztosításához szükséges és a kockázatokkal arányos védelmi intézkedéseket;
- cd)* kidolgozza az alkalmazott védelmi intézkedések hatékonyságának mérési módszereit;
- ce)* folyamatos felülvizsgálat keretében meggyőződik az alkalmazott védelmi intézkedések megfelelőségéről és szükség esetén új védelmi intézkedéseket vezet be.

d) az azonosítási és hozzáférés-kezelési tevékenysége körében:

- da)* biztosítja a szolgáltatások igénybevételét az általa azonosított és nyilvántartott felhasználók, informatikai eszközök és kapcsolódó szolgáltatások számára;
- db)* az *a)* pont szerinti felhasználói kör részére biztosítja a szolgáltatásokhoz való hozzáférési jogosultságot;
- dc)* biztosítja a *b)* pontban meghatározott jogosultságok szükség szerinti kiosztását, módosítását és visszavonását.

e) folyamatosan ellenőrzi szolgáltatásainak biztonsági állapotát, amelynek keretében:

- ea)* biztosítja a szolgáltatások nyújtásában használt vagyonelemek által létrehozott üzemi és biztonsági információk folyamatos gyűjtését;
- eb)* biztosítja az *a)* pontban meghatározott információk biztonsági szempontú elemzését;
- ec)* azonosítja a biztonsági eseményeket és összegyűjti az azokkal kapcsolatos információkat.

f) folyamatosan biztosítja a szolgáltatások nyújtásában használt vagyonelemek biztonsági állapotának megfelelőségét, aminek keretében:

- fa)* intézkedik az azonosított biztonsági események kockázatainak elhárításáról;
- fb)* az *e)* pont *eb)* alpontja szerinti elemzések alapján biztonságnövelő megelőző intézkedéseket vezet be;
- fc)* értesíti a felhasználókat az azonosított biztonsági eseményekről és az azok elhárítása érdekében megtett intézkedésekről.

g) az elektronikus információs rendszereket veszélyeztető biztonsági események, kockázatok kezelése során:

- ga)* tájékoztatja a Nemzeti Elektronikus Információbiztonsági Hatóságot, a Kormányzati Eseménykezelő Központot, a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat, valamint a honvédelmi célú és az európai vagy nemzeti létfontosságú létesítménnyé, rendszerre törvény alapján kijelölt rendszerek eseménykezelő központjait, továbbá az érintett felhasználókat az azonosított biztonsági eseményekről és fenyegetettségekről;

TERVEZET

- gb) biztosítja a biztonsági események azonosításához szükséges, bizonyíték értékű információkat;
- gc) fogadja és kivizsgálja a Nemzeti Elektronikus Információbiztonsági Hatóságtól, a Kormányzati Eseménykezelő Központtól, a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat, valamint a honvédelmi célú és az európai vagy nemzeti létfontosságú létesítménnyé, rendszerre törvény alapján kijelölt rendszerek eseménykezelő központjaitól, továbbá az érintett felhasználóktól érkező informatikai biztonsági bejelentéseket;
- gd) közreműködik a bejelentett informatikai biztonsági események elhárításában.

3. A központi szolgáltató együttműködési kötelezettsége

3. §

A központi szolgáltató együttműködik a Nemzeti Elektronikus Információbiztonsági Hatósággal, a Kormányzati Eseménykezelő Központtal, a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat, valamint a honvédelmi célú és az európai vagy nemzeti létfontosságú létesítménnyé, rendszerre törvény alapján kijelölt rendszerek eseménykezelő központjaival.

4. §

A központi szolgáltató a szolgáltatás nyújtása során az Ibtv. 11. § (3) bekezdésében foglaltak szerint együttműködik

- a) az Ibtv. hatálya alá tartozó szervezetekkel, valamint
- b) az a) pont szerinti szervezetek által, az Ibtv. 11. § (1) bekezdés c) pontja alapján kinevezett vagy megbízott elektronikus információs rendszer biztonságáért felelős személlyel.

4. Záró rendelkezések

5. §

Ez a rendelet 2015. július 1-jén lép hatályba.

5. A Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről szóló 484/2013. (XII. 17.) Korm. rendelet módosítása

6. §

(1) A Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről szóló 484/2013. (XII. 17.) Korm. rendelet (a továbbiakban: Korm. rendelet) 1. § (1) bekezdése helyébe a következő rendelkezés lép:

„(1) A Nemzeti Kiberbiztonsági Koordinációs Tanács (a továbbiakban: Tanács) feladatait a kiemelt fontosságú ügyekben a Kormány ülései előtt állásfoglalásra jogosult Nemzetbiztonsági Kabinet látja el. A Tanács elnöke az e-közigazgatásért felelős miniszter.”

(2) A Korm. rendelet 3. §-a helyébe a következő rendelkezés lép:

„(1) A Tanács koordinációs tevékenységét, valamint döntéseinek végrehajtását a Nemzetbiztonsági Kabinet munkáját támogató Nemzetbiztonsági Munkacsoport (a továbbiakban: Munkacsoport) segíti.

(2) A Tanács felkérésére további munkacsoport is létrehozható.

(3) A Munkacsoport javaslatára a Tanács jogi kötelező erővel nem rendelkező ajánlásokat adhat ki a kibertámadások kezelése és az elektronikus információbiztonság területén alkalmazandó legjobb gyakorlatokról.”

(3) A Korm. rendelet 4. §-a helyébe a következő rendelkezés lép:

„4. § A Tanács és a Munkacsoport működtetésével kapcsolatos adminisztratív teendőket az e-közigazgatásért felelős miniszter által vezetett minisztériumban működő titkárság (a továbbiakban: Titkárság) látja el. ”

(4) A Korm. rendelet 5. § (2) bekezdése helyébe a következő rendelkezés lép:

„(2) A Tanács az (1) bekezdésben meghatározott cselekvési területekhez társított kormányzati intézkedéseket tartalmazó akciótervet (a továbbiakban: Nemzeti Kiberbiztonsági Akcióterv) a Munkacsoport irányításával készíti el, amelynek elfogadásáról a Kormány dönt. A Nemzeti Kiberbiztonsági Akciótervet a Tanácsnak évente felül kell vizsgálnia.”

(5) A Korm. rendelet 8. §-a helyébe a következő rendelkezés lép:

„(1) A Munkacsoport feladatai ellátásához igazodva szükség szerint, de legalább félévente tart ülést, amelyet a Munkacsoport (2) bekezdésben meghatározott vezetője hív össze.

(2) A Munkacsoport ülését az e-közigazgatásért felelős miniszter vezeti. Az ülésekről emlékeztetőt a Titkárság készít.”

(6) A Korm. rendelet

a) 5. § (3) bekezdésében a „Kiberbiztonsági Munkacsoportok” szövegrész helyébe a „Munkacsoport”;

b) 9. §-ában a „Tanács, a Fórum és a Kiberbiztonsági Munkacsoportok” szövegrész helyébe a „Tanács és a Munkacsoport”

c) 10. §-ában a „Tanács, a Fórum, és a Kiberbiztonsági Munkacsoportok” szövegrész helyébe a „Tanács és a Munkacsoport”

szöveg lép.

(7) Hatályát veszti a Korm. rendelet

a) 1. § (2)-(5) bekezdése;

b) 2. §-a; valamint

c) 7. §-a.

Indoklás

I.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 24. § (1) bekezdés g) pontjában (T/4857. sz. törvényjavaslat révén) kapott felhatalmazás alapján a Kormánynak kormányrendeletben szükséges meghatározni a központosított informatikai és elektronikus hírközlési szolgáltató (NISZ Zrt.) feladatait az elektronikus információs rendszerekben kezelt állami és önkormányzati adatvagyon védelme érdekében.

A központosított informatikai és elektronikus hírközlési szolgáltató NISZ Zrt. informatikai szolgáltatások nyújtásával biztosítja az informatikai és hírközlési infrastruktúrát az állami és önkormányzati adatvagyon kezeléséhez az állami és önkormányzati szervek jelentős részének. E szolgáltatásokat, mint központosított informatikai és elektronikus hírközlési szolgáltatásokat a 309/2011. (XII. 23.) Korm. rendelet határozza meg.

A szolgáltatásokat igénybevevő állami és önkormányzati szervek a 2013. évi L. törvény szerint besorolják az elektronikus információs rendszereiket biztonsági osztályokba, és meghatározzák a szükséges védelmi intézkedéseket, azonban az intézkedések egy jelentős része a hatáskörükön túlmutat, mivel a szolgáltatásokat biztosító infrastruktúrát a központosított informatikai és elektronikus hírközlési szolgáltató biztosítja, azaz a védelmi intézkedéseket is a szolgáltató kell, hogy életbe léptesse.

Annak érdekében, hogy egyértelműen meghatározásra kerüljön a 2013. évi L. törvény szerinti feladatok végrehajtásának felelőse, a Kormánynak rendeletben kell meghatároznia a központosított informatikai és elektronikus hírközlési szolgáltató informatikai biztonsági feladatait.

A tervezet 1. §-a ezért meghatározza a központosított informatikai és elektronikus hírközlési szolgáltató azon szolgáltatásait, amelyekre a jogszabály vonatkozik.

A tervezet 2. §-a ugyanakkor részletesen meghatározza azokat a feladatokat, amelyeket a központosított informatikai és elektronikus hírközlési szolgáltatónak végre kell hajtania a szolgáltatásai biztosítása során, a 2013. évi L. törvény értelmében, az állami és önkormányzati adatvagyon védelmének érdekében.

A tervezet 3-4. §-a meghatározza a szolgáltató együttműködési kötelezettségeit a 2013. évi L. törvényben meghatározott szervezetekkel, felhasználói körrel, valamint az egyes szervezeteknél kinevezett vagy megbízott, az elektronikus információs rendszer biztonságáért felelős munkatársaival.

II.

A tervezet módosítja a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről szóló 484/2013. (XII. 17.) Korm. rendeletet is.

A jogszabály-módosítás a Nemzeti Kiberbiztonsági Koordinációs Tanács vezetését a Belügyminisztériumhoz telepíti. A munkavégzés hatékonyságának növelése érdekében indokolt, hogy a Nemzeti Kiberbiztonsági Koordinációs Tanács, illetve a kiberbiztonsági munkacsoportok feladatainak ellátása a Nemzetbiztonsági Kabinet, illetve Nemzetbiztonsági Munkacsoport keretében történjen.