A Kormány

…/2013. (……) Korm. rendelete

az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről

A Kormány
az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 24. § (1) bekezdés *e)* pontjában,
a 7-8. §, valamint a 10. § tekintetében a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény 14. § *i)* pontjában kapott felhatalmazás alapján, az Alaptörvény 15. cikk (1) bekezdésében meghatározott feladatkörében eljárva a következőket rendeli el:

1. A kormányzati eseménykezelő központ feladat- és hatásköre

1. §

A Kormány az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban Ibtv.) 19. §-a szerinti kormányzati eseménykezelő központként (a továbbiakban: Központ) a Nemzetbiztonsági Szakszolgálatot jelöli ki.

2. §

(1) A Központ az általa végzett tevékenységről, a lehetséges veszélyforrásokról és elhárításuk lehetőségeiről évente jelentést készít az irányítását ellátó miniszter részére.

(2) A Központ a Nemzeti Média- és Hírközlési Hatósággal (a továbbiakban: NMHH) és az általa működtetett Országos Informatikai és Hírközlési Főügyelettel (a továbbiakban: OIHF), a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatósággal, valamint az ágazati eseménykezelő központokkal együttműködésben védi az Ibtv.-ben meghatározott állami és önkormányzati szervek által használt rendszereket a globális kibertérből érkező támadások ellen.

(3) A Központ a (2) bekezdés szerinti feladatkörében technikai védelmi, megelőző, koordinációs, valamint szakmai támogató és tájékoztatási tevékenységet végez.

(4) A Központ az állami és önkormányzati rendszerek védelmével kapcsolatos hálózatbiztonsági tevékenysége ellátása keretében, mint biztonsági eseménykezelő központi szervezet felelős
a) a hálózatbiztonság fenntartásának és fokozásának elősegítéséért,
b) az információ-megosztó és eseménykezelési feladatok ellátása érdekében, a hálózatbiztonságot érintő eseménnyel összefüggésben az érintettek riasztásáért,
c) a megelőzés érdekében a szükséges technikai beavatkozások elvégzéséért, gyakorlatok szervezéséért.

(5) A Központ ellátja a Nemzeti Távközlési Gerinchálózat vonatkozásában a biztonsági eseménykezelés feladatait.

(6) A Központ képviseli Magyarországot a nemzetközi hálózatbiztonsági, valamint a létfontosságú információs infrastruktúrák védelmére szakosodott szervezetekben és együttműködési fórumokon, valamint támogatja az egyéb, jogszabályban meghatározott nemzetközi együttműködéseket.

3. §

(1) A Központ kormányzati számítógépes biztonsági eseménykezelő központként működik, 24 órás ügyeleti rendszerben.

(2) A Központ:

a) kezeli a magyar és nemzetközi hálózatbiztonsági és létfontosságú információs infrastruktúra védelmi szervezetektől, vagy más szervektől a bejövő riasztásokat,

b) ellátja az informatikai rendszereket és hírközlő hálózatokat érintő biztonsági események elhárításának koordinálását,

c) tájékoztatja a kapcsolódó hálózatokat és az ágazati eseménykezelő központokat a tudomására jutott sérülékenységekről,

d) a tudomására jutott sérülékenységekről, biztonsági esemény bekövetkeztének veszélyéről vagy fennállásáról, valamint a javasolt intézkedésekről nyilvántartást vezet,

e) a hatáskörébe tartozó hálózatok tekintetében folyamatos helyzetértékelést végez,

f) a sérülékenységről, fenyegetettségről, káros szoftverekről, biztonsági eseményekről rendszeresen jelentéseket készít, biztonsági eseménykezelési támogatást nyújt, koordinál a hazai és nemzetközi szervezetek felé a biztonsági eseményt kiváltó okok megszüntetése, illetve kezelése érdekében,

g) gyűjti a biztonsági események adatait,

h) műszaki szempontból elemzi a biztonsági események adatait.

(3) A Központ:

a) szakmai támogatást nyújt az ágazati eseménykezelő központok működéséhez,

b) írásbeli és szóbeli tájékoztatást, adatszolgáltatást kérhet az ágazati eseménykezelő központoktól,

c) naprakészen tartja az ágazati eseménykezelő központokkal való kapcsolattartáshoz szükséges elérhetőségeket,

d) az ágazati eseménykezelő központoktól átvett információk és adatok alapján, az állami és önkormányzati rendszereket érintő, internet-forgalomba való beavatkozásra utaló jeleket elemzi, kiértékeli, és folyamatos ügyeleti rendszerén keresztül értesíti az elektronikus információs rendszer üzemeltetőjét a biztonsági esemény bekövetkeztének veszélyéről vagy fennállásáról, valamint a javasolt intézkedésekről,

e) a kormányzati célú hálózatból, valamint a kormányzati célú hírközlési szolgáltatásokból vett műszaki adatok és információk folyamatos figyelésével értékelést végez, valamint keresi a hálózatok, illetve szolgáltatások működésébe való beavatkozásra utaló jeleket,

f) a gyanús tevékenységeket kivizsgálja és szükség esetén riasztást ad ki a kormányzati célú hírközlési szolgáltató, a felhasználók, az ágazati eseménykezelő központok és az Ibtv. 3. § (3) bekezdése szerinti hatóság (a továbbiakban: hatóság), valamint a Nemzeti Biztonsági Felügyelet felé,

g) elvégzi a biztonsági események adatainak lehetőség szerinti, távolról történő, online vizsgálatát a biztonsági események mielőbbi észlelése, okozójának, forrásának azonosítása és a szükséges intézkedések megtételének érdekében,

h) állásfoglalásokat, ajánlásokat adhat ki, annak érdekében, hogy a tevékenységével érintett szervek védelmi szintje folyamatosan magas szintű legyen.

(4) A Központ:

a) tájékoztatja a hatóságot a hatáskörébe tartozó szerveket érintő megállapításairól,

b) tájékoztatja a hatóságot az ágazatok közötti, a biztonsági események esetén követendő szabályokról és felelősségi körökről,

c) tájékoztatja a hatóságot a tudomására jutott információbiztonságot érintő eseményekről, fenyegetésekről, sérülékenységről,

d) haladéktalanul tájékoztatja a Nemzeti Kiberbiztonsági Koordinációs Tanácsot, amennyiben olyan eseményt észlel, amely Magyarország kiberbiztonsági helyzetére jelentős hatással van.

(5) A Központ

a) együttműködik az informatikai és hálózatbiztonsági védelemben érintett magyar nemzetbiztonsági szolgálatokkal és bűnüldöző szervekkel, iparági szereplőkkel,

b) részt vesz az infokommunikációs biztonságra vonatkozó stratégiák és ágazati szabályozások előkészítésében,

c) tájékoztatási célú, szemléletformáló kampányokat szervez, hírleveleket bocsát ki,

d) kormányzati információtechnológiai, hálózatbiztonsági, és biztonsági eseménykezelési együttműködési fórumot működtethet,

e) információs infrastruktúra-védelmi és kibervédelmi gyakorlatokat szervezhet, külföldi rendezvényeken ellátja Magyarország képviseletét,

f) a kormányzati információbiztonsági tudatossága növelése érdekében tájékoztató, felkészítő tevékenységet végezhet.

4. §

(1) A Központ, a tudomására jutott sérülékenységekről a hatóság, a Nemzeti Biztonsági Felügyelet, az Alkotmányvédelmi Hivatal, az általános rendőrségi feladatok ellátására létrehozott szerv, a Nemzeti Adó-és Vámhivatal kockázatértékelését követően értesíti a rendszer üzemeltetőjét. Terrorveszélyeztetett rendszerelem tekintetében a rendszer üzemeltetője csak a Terrorelhárítási Központ kockázatértékelését követően értesíthető.

(2) Ha az (1) bekezdés szerinti kockázatértékelés eredménye kritikus sérülékenységre utal, a rendszer üzemeltetőjének figyelmét haladéktalanul felhívja a sérülékenység elhárítására, megszüntetésére, javaslatot tesz az elhárítás, megszüntetés módjára.

(3) Ha a (2) bekezdésben rögzített felhívás ellenére az üzemeltető intézkedései a sérülékenységet nem küszöbölik ki, a Központ a hatóság intézkedését kezdeményezi.

(4) A Központ együttműködik az ágazati eseménykezelő központokkal, a hálózatbiztonsági feladatokat ellátó más szervezetekkel, valamint mindazokkal a szervezetekkel, amelyek informatikai rendszert és hírközlő hálózatot tartanak fenn vagy üzemeltetnek.

2. Az ágazati eseménykezelő központ feladat- és hatásköre

5. §

Az ágazati eseménykezelő központ:

a) az általa támogatott ágazat tekintetében ellátja a Központ 3. §-ban meghatározott feladatait a 3. §

aa) (2) bekezdés *a)*-*c)* és *f)* pontja,

ab) (3) bekezdés *a)*-*d)* pontja,

ac) (4) bekezdése,

ad) (5) bekezdés *d)*-*e)* pontja

kivételével,

b) napi rendszerességgel hálózatbiztonsági helyzetértékeléseket végez,

c) együttműködik az ágazathoz tartozó szervezetek informatikai biztonsági felelőseivel és a Központtal,

d) együttműködik a hatósággal és a Nemzeti Biztonsági Felügyelettel,

e) az észlelt, valamint a tudomására jutott, a feladatkörébe tartozó rendszereket érintő eseményekről haladéktalanul tájékoztatja a Központot,

f) a biztonsági eseményekről nyilvántartást vezet, amely tartalmazza az esemény kapcsán megtett intézkedéseket és azok eredményét.

6. §

(1) Az ágazati eseménykezelő központ a működésének megkezdéséről – működésének tervezett megkezdését megelőzően legalább öt nappal – a Központot tájékoztatja, a kapcsolattartáshoz szükséges adatokat megadja.

(2) Az ágazati eseménykezelő központ a kapcsolattartási adatok változását haladéktalanul bejelenti a Központnak.

3. A létfontosságú rendszerek és létesítmények eseménykezelő központjának feladat- és hatásköre

7. §

(1) A Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóság hálózatbiztonsági feladata körében, a honvédelmi szempontból létfontosságú rendszerek és létesítmények kivételével, nemzeti létfontosságú rendszerek és létesítmények védelmével kapcsolatos hálózatbiztonsági tevékenység ellátása érdekében eseménykezelő központot működtet Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (a továbbiakban: LRLIBEK) elnevezéssel.

(2) Az LRLIBEK az általa végzett tevékenységről, a lehetséges veszélyforrásokról és elhárításuk lehetőségeiről évente jelentést készít az irányítását ellátó, a katasztrófák elleni védekezésért felelős miniszter részére.

(3) Az LRLIBEK az NMHH-val és az OIHF-fel, valamint a Központtal együttműködésben védi a nemzeti létfontosságú rendszerek és létesítmények szolgáltatásait a globális kibertérből érkező támadások ellen.

8. §

(1) Az LRLIBEK feladatkörében:

a) technikai védelmi, megelőző, tájékoztatási és oktatási tevékenységet végez,

b) részt vesz az infokommunikációs biztonságra, valamint a létfontosságú elektronikus információs rendszerek és létesítmények védelmére vonatkozó stratégiák és ágazati szabályozások előkészítésében.

(2) Az LRLIBEK a nemzeti létfontosságú rendszerek és létesítmények védelmével kapcsolatos hálózatbiztonsági tevékenysége ellátása keretében, mint biztonsági eseménykezelő szervezet a kijelölt létfontosságú rendszerelemek vonatkozásában felelős

a) a hálózatbiztonság fenntartásának elősegítéséért, fokozásáért,

b) az információ-megosztó és eseménykezelési feladatok ellátása érdekében, a Központtól kapott tájékoztatás alapján, a létfontosságú rendszerelem hálózatbiztonságát érintő eseménnyel összefüggésben az érintett üzemeltető riasztásáért.

(3) Az LRLIBEK:

a) a magyar és nemzetközi hálózatbiztonsági szervezetektől a Központon keresztül kapott riasztások kezelésére – a nemzeti létfontosságú rendszerek és létesítmények érintettsége esetén – számítástechnikai sürgősségi reagáló egységként működik folyamatos rendelkezésre állással,

b) ellátja a nemzeti létfontosságú rendszerelemként azonosított informatikai rendszerek és hírközlő hálózatok felé irányuló, a globális kibertérből érkező beavatkozások elhárításának koordinálását,

c) továbbítja az OIHF és a Központ részére a nemzeti létfontosságú rendszerelemek felé az informatikai rendszerek és hírközlő hálózatok oldaláról érkezett, támadásra utaló információkat a támadó hazai és nemzetközi együttműködésben történő lokalizációja és megbénítása érdekében,

d) rendszeres tájékoztatást ad a nemzeti létfontosságú rendszerelemként azonosított informatikai rendszerek és hírközlő hálózatok felé a felismert és publikált sérülékenységekről,

e) az OIHF-től és a Központtól, vagy más hálózatbiztonsági szervezettől átvett információk és adatok alapján, a nemzeti létfontosságú rendszerelemet érintő, a globális kibertérből érkező beavatkozást, és az internet-forgalomba való beavatkozásra utaló jeleket kiértékeli, és folyamatos ügyeleti rendszerén keresztül értesíti a létfontosságú rendszerelem üzemeltetőjét, valamint az érintett hálózatbiztonsági és létfontosságú elektronikus információs rendszer és létesítmény üzemeltetőjét,

f) tájékoztatási célú, szemléletformáló kampányokat szervez, hírleveleket bocsát ki,

g) együttműködik az informatikai és hálózatbiztonsági, valamint a létfontosságú elektronikus információs rendszerek és létesítmények védelmében érintett magyar nemzetbiztonsági szolgálatokkal és bűnüldöző szervekkel, iparági szereplőkkel,

h) a megelőzés érdekében a szükséges technikai beavatkozásokat elvégzi,

i) a Belügyminisztérium és szervei érintett informatikai munkatársai részére képzéseket szervez, tart.

(4) Ha az LRLIBEK által elvégzett kockázatértékelés eredménye kritikus sérülékenységre utal, az üzemeltetőt határidő megadásával felszólítja a sérülékenység elhárítására, megszüntetésére, javaslatot tesz az elhárítás, megszüntetés módjára. Az LRLIBEK a tudomására jutott sérülékenységekről, eseményekről tájékoztatja a Központot.

(5) Az LRLIBEK együttműködik a létfontosságú elektronikus információs rendszert és létesítményt üzemeltető szervezetekkel, a hálózatbiztonsági feladatokat ellátó más szervezetekkel, valamint mindazokkal a szervezetekkel, amelyek informatikai rendszert és hírközlő hálózatot azonosítottak létfontosságú rendszerelemként.

(6) Az LRLIBEK – a Központtal együttműködésben – képviseli a létfontosságú rendszereket és létesítményeket üzemeltető szervezeteket a hálózatbiztonság védelmére szakosodott együttműködési fórumokon és szervezetekben.

4. Záró rendelkezések

9. §

Ez a rendelet 2013. július 1-jén lép hatályba.

10. §

Hatályát veszti a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról szóló 65/2013. (III. 8.) Korm. rendelet 14. §-a.