

## **A Kormány**

### **.../2015. (... ...) Korm. rendelete**

#### **a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól**

A Kormány

az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 24. § (1) bekezdés *e), j) és k)* pontjában,

a 6. § (3) bekezdése 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. Értelmező rendelkezések**

##### **1. § E rendelet alkalmazásában**

1. *adminisztrátori jogosultsággal rendelkező informatikai biztonsági vizsgálat*: olyan biztonsági vizsgálati eljárás, amelynek során a vizsgálatot végző személy rendszergazdai jogosultsággal rendelkezik, és az eljárás célja, hogy megfelelőségi listák alapján a teljes informatikai rendszer állapota ellenőrzésre kerüljön;
2. *automatizált informatikai biztonsági vizsgálat*: olyan biztonsági vizsgálati eljárás, amelynek során a szervezet informatikai rendszerének a sérülékenységei célszoftverek segítségével kerülnek feltérképezésre;
3. *átlagostól jelentősen eltérő elektronikus információs rendszer*: a biztonsági vizsgálattal érintett szervezet (a továbbiakban: érintett szervezet) elektronikus információs rendszere az átlagostól jelentősen eltér, ha:
  - a) a rendszer
    - aa) a külső internetes tartományban több mint 20 IP címen elérhető eszközzel,
    - ab) több mint 10 webes szolgáltatással,
    - ac) a belső hálózat tekintetében több mint 50 szerverrel,
    - ad) több mint 500 munkaállomással,
    - ae) több mint 5 vezeték nélküli hálózattal, vagy
    - af) több mint 500 fős felhasználói létszámmal rendelkezik, vagy
  - b) az érintett szervezet több mint három telephelyen rendelkezik a vizsgálattal érintett elektronikus információs rendszerrel;
4. *belső informatikai biztonsági vizsgálat*: olyan biztonsági vizsgálati eljárás, amelynek során a szervezet informatikai rendszerének sérülékenységvizsgálata a belső hálózati végpontról közvetlenül történik;
5. *biztonsági esemény-kezelési megbízott*: az elektronikus információs rendszert üzemeltető szerv vezetője által a biztonsági események kivizsgálására megbízott személy;

Az előterjesztést a Kormány nem tárgyalta meg, ezért az nem tekinthető a Kormány álláspontjának

## **TERVEZET**

6. *célszoftverek*: a biztonsági vizsgálati eljárás során a sérülékenységvizsgálat egyes fázisainak végrehajtására kifejlesztett szoftverek;
7. *eseménykezelő központ*: az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 19. § (2) – (4) bekezdés alapján biztonsági események kezelésére hatáskörrel rendelkező szerv;
8. *kézi informatikai biztonsági vizsgálat*: olyan biztonsági vizsgálati eljárás, amelynek során a szervezet informatikai rendszerének sérülékenységei a vizsgálatot végző személy által egyedileg, manuálisan összeállított lekérdezések alkalmazásával kerülnek feltérképezésre;
9. *külső informatikai biztonsági vizsgálat*: az informatikai rendszer internet felőli, külső sérülékenységvizsgálata, amelynek során az interneten fellelhető, nyilvános adatbázisokban való szabad keresésre, célzott információgyűjtésre, valamint az elérhető számítógépek szolgáltatásainak, sebezhetőségének feltérképezésére kerül sor;
10. *regisztrált felhasználói jogosultság nélküli informatikai biztonsági vizsgálat*: olyan biztonsági vizsgálati eljárás, amelynek során a vizsgálatot végző személy semmilyen előzetes információval nem rendelkezik a szervezet informatikai rendszeréről, és nincs felhasználói jogosultsága a rendszerhez;
11. *regisztrált felhasználói jogosultsággal rendelkező informatikai biztonsági vizsgálat*: olyan biztonsági vizsgálati eljárás, amelynek során a vizsgálatot végző személy a számára külön létrehozott felhasználói jogosultsággal végzi a vizsgálatot;
12. *titkosítási eljárás*: olyan eljárás, amely az adat megismerhetőségét azáltal korlátozza, hogy az adat egy algoritmus segítségével átalakításra kerül olyan jelsorozattá, ami olvashatatlan azon személy számára, aki nem rendelkezik a visszaalakításhoz szükséges egyedi jelsorozattal álló kulccsal;
13. *titkosítási kulcs*: titkosítási eljárás során alkalmazott olyan jelsorozat, amelynek ismeretében a titkosított állomány megismerhető;
14. *webes vizsgálat*: olyan biztonsági vizsgálati eljárás, amely során automatizált és kézi vizsgálatok útján kerülnek feltárára a webes alkalmazások sérülékenységei;
15. *vezeték nélküli hálózat informatikai biztonsági vizsgálat*: olyan biztonsági vizsgálati eljárás, amelynek során a vezeték nélküli hozzáférési és kapcsolódási pontok keresése, feltérképezése, titkosítási eljárások elemzése, titkosítási kulcsok visszafejthetőségének ellenőrzése célszoftverek és kézi vizsgálat útján történik.

## **2. A kormányzati eseménykezelő központ feladat- és hatásköre**

2. § A Kormány az Ibtv. 19. §-a szerinti kormányzati eseménykezelő központként (a továbbiakban: Központ) a Nemzetbiztonsági Szakszolgálatot jelöli ki.
3. § (1) A Központ a biztonsági események és fenyegetések kezelésével támogatja az állami és önkormányzati szerveket, amelynek céljából együttműködik
  - a) az állami és önkormányzati szervek elektronikus információs rendszerei biztonságának felügyeletét ellátó hatósággal, a zárt célú, a polgári hírszerző

Az előterjesztést a Kormány nem tárgyalta meg, ezért az nem tekinthető a Kormány álláspontjának

## **TERVEZET**

tevékenységhez kapcsolódó, a honvédelmi célú, valamint a létfontosságú létesítmények, rendszerek elektronikus információs rendszerei biztonsági felügyeletét ellátó hatóságokkal (a továbbiakban együtt: hatóság),

- b) az Ibtv. 19. § (2)-(4) bekezdésekben megjelölt eseménykezelő szervekkel (a továbbiakban: eseménykezelő központ),
- c) a rendvédelmi szervekkel és a Katonai Nemzetbiztonsági Szolgálattal,
- d) a Nemzeti Média- és Hírközlési Hatósággal és az általa működtetett Országos Informatikai és Hírközlési Főügyelettel,
- e) az elektronikus hírközlési szolgáltatókkal, kormányzati célú hírközlési szolgáltatóval,
- f) az elektronikus kereskedelmi szolgáltatókkal és közvetítő szolgáltatókkal,
- g) a magyar és nemzetközi hálózatbiztonsági és információbiztonsági szervezetekkel, valamint
- h) iparági szereplőkkel (a továbbiakban együtt: együttműködő szervek).

(2) A Központ a biztonsági eseményre vagy fenyegetésre utaló tevékenységeket kivizsgálhatja és szükség esetén riasztást ad ki a kormányzati célú hírközlési szolgáltató, a felhasználók, az eseménykezelő központ és a hatóság felé.

#### **4. § A Központ a biztonságiesemény-kezelési feladatkörében felelős:**

- a) a biztonsági események bejelentésének napi 24 órában történő fogadásáért és nyilvántartásáért,
- b) a tudomására jutott biztonsági eseményekről az érintettek haladéktalan értesítéséért,
- c) a bejelentett vagy egyéb módon tudomására jutott biztonsági események felszámolásának elősegítéséért, koordinálásáért,
- d) a biztonsági eseményekről személyes adatokat nem tartalmazó nyilvántartás vezetéséért, amely tartalmazza a biztonsági esemény kapcsán megtett intézkedéseket és azok eredményét,
- e) az érintett szerv számára a biztonsági események kezelése során szakmai támogatás nyújtásáért.

**5. § (1)** A Központ a biztonsági események megelőzése céljából ellátja az állami és önkormányzati szervek elektronikus információs rendszereit érintő fenyegetésekkel összefüggő tájékoztatási és tudatosítási feladatokat.

(2) A Központ az (1) bekezdéssel összefüggő felelőssége körében, az elektronikus információs rendszereket veszélyeztető sérülékenységekkel és fenyegető kockázatokkal összefüggésben felelős:

- a) a magyar és nemzetközi hálózatbiztonsági és információbiztonsági szervezetektől, vagy más szervektől bejövő tájékoztatások, riasztások fogadásáért,
- b) az elektronikus információs rendszerek biztonságáért felelős személyek tájékoztatásáért,
- c) az eseménykezelő központ tájékoztatásáért,
- d) a sérülékenységekről és fenyegetésekről, valamint a javasolt biztonsági intézkedésekről a honlapján rendszeres tájékoztatás nyújtásáért.

(3) A Központ

Az előterjesztést a Kormány nem tárgyalta meg, ezért az nem tekinthető a Kormány álláspontjának

**TERVEZET**

- a) elemzéseket, jelentéseket készít a magyar és nemzetközi információbiztonsági irányokról,
- b) a hatáskörébe tartozó szerveknél bekövetkezett biztonsági eseményekről negyedévente jelentést tesz a Nemzeti Kiberbiztonsági Koordinációs Tanács részére,
- c) évente jelentést készít a tevékenységéről az irányító miniszter részére.

(4) A Központ az (1) bekezdéssel összefüggő tájékoztató és tudatosító tevékenységgel összefüggésben:

- a) a kiberbiztonsági tudatosság növelése érdekében tájékoztatási célú, szemléletformáló kampányokat szervezhet, hírleveleket bocsáthat ki,
- b) nem kötelező érvényű állásfoglalásokat, ajánlásokat adhat ki,
- c) a biztonsági események kezelésére irányuló tájékoztatót tarthat,
- d) kormányzati információtechnológiai, hálózatbiztonsági, és biztonságiesemény-kezelési együttműködési fórumot működtethet,
- e) részt vesz az infokommunikációs biztonságra vonatkozó stratégiák és szabályozások előkészítésében.

### **3. Az eseménykezelő központ feladat-és hatásköre**

**6.** § (1) A Kormány a honvédelmi célú elektronikus információs rendszereket érintő biztonsági események és fenyegetések kezelésére a honvédelemért felelős miniszter irányítása alatt álló Honvédelmi Célú Elektronikus Információs Rendszerek Eseménykezelő Központját jelöli ki, melynek feladatait a Katonai Nemzetbiztonsági Szolgálat a szakmai irányítása és koordinálása alatt álló, szakfeladat szerint elkülönülő - a honvédelemért felelős miniszter irányítása alatt álló központi hivatalnál, szervnél, szervezetnél működő - eseménykezelő központokkal együtt látja el..

(2) A Kormány a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszereit érintő biztonsági események és fenyegetések kezelésére a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat szervezeti keretén belül működő eseménykezelő központot (a továbbiakban: IntCERT) jelöli ki.

(3) A Kormány a kijelölt létfontosságú létesítmény, rendszer elektronikus információs rendszereit érintő biztonsági események és fenyegetések kezelésére a Belügyminisztérium Országos Katasztrófavédelmi Főigazgatóságot jelöli ki. A Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja elnevezéssel működő eseménykezelő központ – az állami és önkormányzati elektronikus információs rendszerek, a zárt célú, a honvédelmi célú, valamint a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat által üzemeltetett létfontosságú rendszerek és létesítmények kivételével – ellátja a nemzeti létfontosságú rendszerek és létesítmények védelmével kapcsolatos hálózatbiztonsági tevékenységet.

(4) Az (1)-(3) bekezdés szerinti eseménykezelő központ a hatáskörébe tartozó elektronikus információs rendszerek tekintetében,

- a) eseménykezelési felelősségi körében ellátja a Központ 4. §,

Az előterjesztést a Kormány nem tárgyalta meg, ezért az nem tekinthető a Kormány álláspontjának

**TERVEZET**

*b)* tájékoztatási körében ellátja a Központ 5. § (2) bekezdés *b)* pontja, továbbá a 5. § (3) bekezdés *c)* pontja,

*c)* tudatosítási körében ellátja a Központ 5. § (4) bekezdés *a)*-*c)* pontja

szerinti feladatait.

**7. § (1)** Az eseménykezelő központ a hatáskörébe tartozó elektronikus információs rendszerek tekintetében

*a)* nyilvántartást vezet a hatáskörébe tartozó és együttműködő szervekkel való kapcsolattartáshoz szükséges elérhetőségekről,

*b)* az észlelt, valamint a tudomására jutott biztonsági eseményekről haladéktalanul tájékoztatja a Központot.

(2) Az eseménykezelő központ a működésének megkezdéséről - működésének tervezett megkezdését megelőzően legalább öt nappal - a Központot tájékoztatja, a kapcsolattartáshoz szükséges adatokat, valamint a kapcsolattartási adatok változását haladéktalanul bejelenti a Központnak.

#### **4. A biztonsági események kezelésének, műszaki vizsgálatának szabályai**

**8. § (1)** Az állami és önkormányzati szervek elektronikus információs rendszereit érintő biztonsági események kivizsgálásában kizárólag

*a)* az elektronikus információs rendszer biztonságáért felelős személy,

*b)* biztonságiesemény-kezelési megbízott, továbbá

*c)* a hatáskörrel rendelkező eseménykezelő központ vehet részt.

(2) A nemzetbiztonsági védelem alá eső szerv vezetője – a 6. § (1)-(3) bekezdésben meghatározott szervek kivételével –

*a)* az elektronikus információs rendszer biztonságáért felelős személy esetében a feladatra történő kinevezése,

*b)* a biztonságiesemény-kezelési megbízott esetében a feladatra történő megbízása tervezett hatályba lépését megelőző 30 nappal véleményezés céljából – az érintett személy hozzájárulásával – megküldi a Központ részére a kinevezésben, illetve a megbízásban szereplő személy adatait.

(3) A Központ a feladatra történő kinevezés, illetve a megbízás hatályba lépésének időpontjáig köteles a véleményét a véleménykérő szerv vezetője részére megküldeni.

(4) A biztonságiesemény-kezelési megbízottat az Ibtv-ben meghatározott elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személynek kell tekinteni.

**9. § (1)** Az állami és önkormányzati szervek kötelesek a Központ részére az elektronikus információs rendszereiken bekövetkezett biztonsági eseményeket haladéktalanul bejelenteni.

(2) A biztonsági eseménnyel érintett szervezet a Központ kérésére köteles a biztonsági események kezeléséhez szükséges műszaki, technikai adatokat, információkat összegyűjteni és elektronikus formában átadni vagy egyéb módon hozzáférhetővé tenni.

(3) Ha a szerv bármely okból nem képes a (2) bekezdés szerinti adatok összegyűjtésére, a Központ begyűjtheti az adatokat. Az érintett szervezet gondoskodik arról, hogy a Központ az adatokhoz hozzáférjen.

(4) A Központ az érintett szervvel együttműködve kidolgozza a biztonsági esemény felszámolásához szükséges intézkedéseket, amelyeket az érintett szerv végrehajt.

(5) A Központ a biztonsági eseményről technológiai naplót vezet, amely tartalmazza a biztonsági esemény kivizsgálásának támogatása során tett intézkedéseket, és azok eredményét is.

**10. § (1)** A Központ a hatáskörébe tartozó szervektől és az eseménykezelő központtól kért és kötelezően átadott információk és adatok alapján, az állami és önkormányzati rendszereket érintő, biztonsági eseményre vagy fenyegetésre utaló jeleket elemezi, kiértékeli, és folyamatos ügyeleti rendszerén keresztül értesíti az elektronikus információs rendszer üzemeltetőjét a biztonsági esemény bekövetkeztének veszélyéről vagy fennállásáról, valamint a javasolt intézkedésekről.

(2) A Központ a kormányzati célú hálózathoz, valamint a központosított informatikai és hírközlési szolgáltatótól átvett műszaki adatok és információk folyamatos figyelésével értékelést végezhet, valamint keresheti a hálózatok, illetve szolgáltatások működését érintő biztonsági eseményre vagy fenyegetésre utaló jeleket.

(3) A kormányzati célú hírközlési szolgáltató, valamint a központosított informatikai és hírközlési szolgáltató a Központ által történő biztonságiesemény-kezelés során köteles

- a) a biztonsági eseményben érintettek (támadó/támadott) beazonosításához szükséges műszaki, technikai adatok Központ részére történő átadására,
- b) az ismert fenyegetések elleni védelmi intézkedések, műszaki, technikai megoldások alkalmazására,
- c) a Központ kérésére adatokat szolgáltatni a hálózati forgalomba való beavatkozásra utaló jelek elemzése, kiértékelése céljából,
- d) a Központ által meghatározott feladatokban együttműködni.

**11. § (1)** A biztonsági eseményekkel összefüggő adatok műszaki vizsgálatának célja, hogy a bekövetkezett biztonsági események kivizsgálása révén

- a) feltárja a biztonsági esemény bekövetkeztének okait, körülményeit, az okozott kár mértékét,
- b) behatárolja a biztonsági esemény által érintett elektronikus információs rendszerek, rendszerelemek körét,
- c) javaslatot tegyen a biztonsági esemény által okozott kár elhárítására, és
- d) a bekövetkezett biztonsági eseményből levonható tanulságokról tájékoztassa a biztonsági eseménnyel érintett más szerveket és a hatóságot annak érdekében, hogy a jövőben a biztonsági esemény bekövetkezése megelőzhető legyen.

(2) Az érintett szerv köteles a vizsgálat lefolytatásához szükséges adatokat, dokumentumokat, eszközöket és egyéb információkat Központ rendelkezésére bocsátani.

## **5. Sérülékenységvizsgálat**

**12. §** (1) A nemzetbiztonsági védelem alá eső szervek elektronikus információs rendszerei, az Ibtv. 2. § (1) bekezdése szerinti állami és önkormányzati szervek európai létfontosságú rendszerelemmé vagy nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemeinek elektronikus információs rendszerei, valamint a zárt célú elektronikus információs rendszerek sérülékenységvizsgálatát – a (2) és (3) bekezdés kivételével - a Központ végzi.

(2) A polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszerei sérülékenységvizsgálatát a 6. § (2) bekezdése szerinti eseménykezelő központ végzi.

(3) A honvédelmi célú elektronikus információs rendszerek sérülékenységvizsgálatát a 6. § (1) bekezdése szerinti eseménykezelő központ végzi.

(4) Gazdasági társaság abban az esetben végezhet sérülékenységvizsgálatot, ha:

- a) a gazdasági társaság nevében és alkalmazásában eljárva a sérülékenységvizsgálatban részt vevő személy az Ibtv-ben meghatározott feltételeken túl rendelkezik a sérülékenységvizsgálat lefolytatásához szükséges ismeretek meglétét igazoló végzettséggel, és ezen a szakterületen legalább 2 év szakmai tapasztalattal,
- b) a gazdasági társaság bejegyzésre került a sérülékenységvizsgálat lefolytatására jogosult gazdasági társaságok nyilvántartásába.

(5) A sérülékenységvizsgálat lefolytatására jogosult gazdasági társaságokról az Alkotmányvédelmi Hivatal – személyes adatot nem tartalmazó – nyilvántartást vezet. A nyilvántartás tartalmazza a gazdasági társaság adatait, a sérülékenységvizsgálatban részt vevő személyek számát és a sérülékenységvizsgálat lefolytatásához szükséges ismereteket igazoló végzettség megnevezését és megszerzési idejét.

(6) Az (5) bekezdés szerinti adatok tekintetében az Alkotmányvédelmi Hivatal egyéni, írásbeli kérelem alapján, annak beérkezésétől számított 15 napon belül nyújt tájékoztatást.

(7) A nyilvántartásba való felvételt a gazdasági társaság kezdeményezi az Alkotmányvédelmi Hivatal felé, a (4) bekezdés a)-c) pontjaiban meghatározott feltételek meglétét igazoló okiratok benyújtásával. A nyilvántartásba való felvételre vonatkozóan a Központ véleményezési joggal rendelkezik.

(8) A sérülékenységvizsgálat lefolytatására jogosult gazdasági társaság az alkalmassági feltételeket érintő változásokról, valamint a sérülékenységvizsgálatban részt vevő személyeket érintő változásokról a változást követő 8 napon belül értesíti az Alkotmányvédelmi Hivatalt. Az Alkotmányvédelmi Hivatal jogosult az alkalmassági feltételek meglétét, valamint a nyilvántartásban szereplő adatok valódiságát ellenőrizni. Az értesítési kötelezettség

elmulasztása esetén, valamint az alkalmassági feltételek meglétének hiánya esetén az Alkotmányvédelmi Hivatal jogosult a gazdasági társaságot a nyilvántartásából törölni.

**13. § (1)** A sérülékenységvizsgálat célja az esetleges biztonsági események bekövetkeztét megelőzően a szervezet elektronikus információs rendszere, rendszerelemei gyenge pontjainak feltárása, valamint a feltárt hibák elhárítására vonatkozó részletes megoldási javaslatok kidolgozása az elektronikus információs rendszerek, rendszerelemek védelmének és biztonságának megerősítése érdekében.

(2) A sérülékenységvizsgálat tárgya az adatok, információk kezelésére használt elektronikus információs rendszereknek, rendszerelemeinek, eszközöknek, eljárásoknak, és kapcsolódó folyamatoknak, valamint az ezeket kezelő személyek általános informatikai felkészültségének, és a szervezetnél használt informatikai és információbiztonsági előírások, szabályok betartásának vizsgálata.

**14. § (1)** A sérülékenységvizsgálat során a sérülékenységvizsgálati eljárását megalapozó dokumentációban meghatározottak szerint az alábbi vizsgálatok (a továbbiakban együtt: vizsgálat) elvégzésére kerül sor:

- a) külső vizsgálat,
- b) webes vizsgálat,
- c) belső vizsgálat,
- d) vezeték nélküli hálózat vizsgálat.

(2) A vizsgálat az (1) bekezdés a)–d) pontjában meghatározott irányultságok tekintetében három típusú jogosultsági fázist tartalmazhat:

- a) regisztrált felhasználói jogosultság nélküli vizsgálat,
- b) regisztrált felhasználói jogosultsággal rendelkező vizsgálat és
- c) adminisztrátori jogosultsággal rendelkező vizsgálat.

(3) A sérülékenységvizsgálat határideje a hatóság határozatának keltétől, illetve az előzetesen egyeztetett kezdési időponttól számítva az (1) bekezdésben meghatározott vizsgálatok szerint:

- a) külső vizsgálat esetén harminc nap,
- b) webes vizsgálat esetén hetvenöt nap,
- c) belső vizsgálat esetén kilencven nap,
- d) vezeték nélküli hálózat vizsgálat esetén harminc nap,

**15. § (1)** A Központ által lefolytatott sérülékenységvizsgálatot a hatóság rendeli el, vagy az Ibtv. hatálya alá tartozó szerv kezdeményezi egyéni kérelem alapján.

(2) A vizsgálat előkészítése során a vizsgálatot végző szerv sérülékenységvizsgálati dokumentációt készít. A sérülékenységvizsgálati dokumentációban rögzíti a vizsgálati feladatokat, célokat, a technikai és személyi feltételeket, a módszertant, az egyeztetések, a vizsgálat várható befejezésének dátumát.

(3) Ha a sérülékenységvizsgálatot a hatóság rendeli el, akkor a sérülékenységvizsgálati dokumentációban a határozatban rögzített vizsgálati feladatokat kell feltüntetni. A sérülékenységvizsgálat egyedi kezdeményezése esetén a vizsgálati feladatokra a kezdeményező szerv javaslatot tehet, amelyről a vizsgálatot végző szerv dönt.



Az előterjesztést a Kormány nem tárgyalta meg, ezért az nem tekinthető a Kormány álláspontjának

## **TERVEZET**

(4) A sérülékenységvizsgálati dokumentációt a vizsgálatot végző szerv megküldi az érintett szervezet részére. Az érintett szervezet a sérülékenységvizsgálati dokumentáció tartalmára a kézhezvételtől számított öt munkanapon belül észrevételt tehet. Az észrevétel nem érintheti a hatóság által elrendelt vizsgálatokat. Az észrevételekről a vizsgálatot végző szerv dönt.

**16. §** (1) A vizsgálatot végző szerv a vizsgálat során kellő gondossággal eljárva, törekedni köteles a vizsgált rendszer által nyújtott szolgáltatások szükségesnél nem nagyobb mértékű korlátozására. A vizsgálatot végző szerv köteles a korlátozás várható mértékéről és időtartalmáról az ellenőrzött szervezetet előzetesen tájékoztatni.

(2) Hatósági határozat alapján elrendelt sérülékenységvizsgálat esetén a kötelezett szerv köteles a vizsgálat lefolytatásához szükséges adatokat, dokumentumokat, eszközöket és egyéb információkat a Központ rendelkezésére bocsátani, valamint tűrni a vizsgálatból fakadó, a vizsgált rendszeren bekövetkezett szolgáltatáscsökkenést.

(3) Egyedi kezdeményezés esetén az érintett szerv a 15. § (4) bekezdés szerinti észrevételezés során kizárhatja azon vizsgálatokat, amelyek jelentős szolgáltatáscsökkenést eredményeznek.

(4) A Központ a vizsgálatra irányadó határidőt annak letelte előtt egy alkalommal legfeljebb harminc nappal meghosszabbíthatja, és erről az érintett szervezetet és a hatóságot értesíti.

(5) Amennyiben az érintett szervezet elektronikus információs rendszere, rendszereleme az átlagostól jelentősen eltér, és emiatt egyedi eljárás szükséges, az vizsgálati határidő további harminc nappal meghosszabbítható.

**17. §** (1) A sérülékenységvizsgálat lezárásakor a Központ állásfoglalást készít, és azt öt munkanapon belül megküldi az érintett szervezet és a hatóság részére.

(2) Az (1) bekezdés szerinti állásfoglalás tartalmazza:

- a) a vizsgálati eredmények leírását, és
- b) a rövid-, közép- és hosszú távú intézkedésekre vonatkozó intézkedési javaslatokat.

## **6. Záró rendelkezések**

**18. §** Ez a rendelet 2015. július 1-jén lép hatályba.

**19. §** (1) E rendelet 12. §-a a belső piaci szolgáltatásokról szóló 2006. december 12-i 2006/123/EK európai parlamenti és tanácsi irányelvnek való megfelelést szolgálja.

(2) E rendelet tervezetének a belső piaci szolgáltatásokról szóló 2006. december 12-i 2006/123/EK európai parlamenti és tanácsi irányelv 15. cikk (7) bekezdése szerinti előzetes bejelentése megtörtént.

**20. §** A kormányzati célú hálózatokról szóló 346/2010. (XII. 28.) Korm. rendelet 6. §-a a következő (8) bekezdéssel egészül ki:

„(8) A kormányzati célú hírközlési szolgáltató jogszabályban foglaltak szerint köteles együttműködni a kormányzati eseménykezelő központtal a biztonsági eseménykezelési és sérülékenységvizsgálati feladatok végrehajtása érdekében.”

Az előterjesztést a Kormány nem tárgyalta meg, ezért az nem tekinthető a Kormány álláspontjának

**TERVEZET**

**21. §** Hatályát veszti az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjainak, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről szóló 233/2013. (VI. 30.) Korm. rendelet.

### **Indoklás**

Az Ibtv. és végrehajtási rendeleteinek hatályba lépésével megalakult a Kormányzati Eseménykezelő Központ (Központ), valamint az BM Országos Katasztrófavédelmi Főigazgatóság szervezetén belül a Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja (LRLIBEK). Bár az elektronikus információs rendszerek kormányzati eseménykezelő központjának, ágazati eseménykezelő központjának, valamint a létfontosságú rendszerek és létesítmények eseménykezelő központja feladat- és hatásköréről szóló 233/2013. (VI. 30.) Korm. rendelet (a továbbiakban: R1) számos szerv részére lehetővé tette ágazati eseménykezelő központ létrehozását, azonban ezek – elsősorban költségvetési okokból – nem jöttek létre. Jelenleg adottak a feltételek a honvédelmi célú rendszerek eseménykezelését támogató eseménykezelő központ létrehozására a Honvédelmi Minisztérium szervezetén belül, továbbá a hírszerzési célú rendszerek eseménykezelő központjának létrehozására az Információs Hivatal szervezetén belül.

Figyelemmel arra, hogy az elektronikus információbiztonság közvetve vagy közvetlenül az e-közigazgatásért felelős miniszter felelősségi körébe került, továbbá hogy indokolt a hatósági és a végrehajtási jellegű kiberbiztonsági tevékenységek szétválasztása és az eseménykezelési tevékenység hatékonyabbá tétele, szükségessé vált az R1 helyett új rendelet megalkotása, mely szabályozza az eseménykezelő központok tevékenységét, az eseménykezelés eljárásrendjét, valamint a sérülékenységvizsgálat eljárási szabályait.

A tervezet a korábbinál átláthatóbb, kategorizált módon tartalmazza a Központ feladatait. Kiemelendő, hogy a jogszabályváltozás széleskörű együttműködési lehetőséget rögzít, nem kizárólag más eseménykezelő központok és a hatóság, hanem rendvédelmi, nemzetbiztonsági szervek, hírközlési szolgáltatók, elektronikus kereskedelmi szolgáltatók, hazai és nemzetközi hálózatbiztonsági és információbiztonsági szervezetek és iparági szereplők – így az összes, elektronikus információbiztonság szempontjából jelentős szereplő – felé. A széleskörű együttműködési lehetőség biztosítja a Központ számára a kibertér biztonságával összefüggő minél több információ begyűjtését, elemzését és a pontos, gyors tájékoztatást.

A tervezet meghatározza Honvédelmi Minisztérium, az Információs Hivatal és a BM Országos Katasztrófavédelmi Főigazgatóság szervezetén belül kialakításra kerülő, illetve került eseménykezelő központok feladatait, a Központtal való együttműködés rendjét. A korábbi szabályzással szemben nem hagyja nyitva további eseménykezelő központok esetleges, állami szervek egyedi döntésén alapuló létrehozását.

A tervezet meghatározza továbbá a biztonsági eseménykezelés eljárásrendjét, külön hangsúlyt fektetve a biztonsági eseményeknek az eseménykezelő központok részére történő kötelező, haladéktalan bejelentésére, továbbá a biztonsági események felderítéséhez szükséges információk átadására, valamint annak biztosítására, hogy minden szervezetnél kompetens, képzett személyek lássák el az eseménykezelés és az eseménykezelő központtal való

Az előterjesztést a Kormány nem tárgyalta meg, ezért az nem tekinthető a Kormány álláspontjának

## **TERVEZET**

együttműködés feladatát. Az eseménykezelés eljárásrendjének egységesítése jelentős mértékben hozzájárulhat ahhoz, hogy az állami és önkormányzati szervek elektronikus információs rendszereit érintő biztonsági események mielőbbi azonosítása, elemzése, felszámolása, és újbóli előfordulás megelőzése szélesebb körben, gyorsabban és hatékonyabban megtörténhessen.

A tervezet rögzíti a sérülékenységvizsgálat eljárásrendjét és a sérülékenységvizsgálat elvégzésére jogosult gazdasági társaságokkal szemben támasztott követelményeket, külön kiemelve azon jelentősebb – nemzetbiztonsági védelem alá eső, létfontosságú rendszerelemmé nyilvánított, illetve zárt célú – rendszereket, melyek tekintetében kizárólag a Központ rendelkezik hatáskörrel. A sérülékenységvizsgálat eljárásrendje hasonló a korábbi szakhatósági eljárásrendhez. Az eljárásrend megkülönbözteti a hatóság által elrendelt sérülékenységvizsgálatot (ekkor a sérülékenységvizsgálatot a határozatnak megfelelően kell lefolytatni), valamint az érintett szerv önkéntes kezdeményezésére lefolytatott sérülékenységvizsgálatot, ahol a jogszabály jelentős szabadságot biztosít a vizsgálatot kezdeményező és azt lefolytató szervezet közötti megállapodás tartalmára nézve, egyúttal a vizsgálattal érintett rendszerek szolgáltatásfolytonosságának biztosítására vonatkozó garanciális elemeket is megfogalmaz. Az eljárásrend és a vizsgálati feltételek rögzítése lehetővé teszi, hogy a vizsgálatok – hatósági vagy szakhatósági eljáráson kívül is – egységes rend szerint és magas szakmai színvonalon kerüljenek elvégzésre.