MAGYARORSZÁG KORMÁNYA

Közli: Magyar Közlöny

A K O R M Á N Y

----

rendelete

Magyarország kiberbiztonságáról szóló törvény végrehajtásáról

A Kormány
a Magyarország kiberbiztonságáról szóló 2024. évi … törvény 81. § (1) bekezdés b)-i) pontjában, 81. § (2) bekezdés 2-6., 8-11, 15-18. és 21-25. pontjában kapott felhatalmazás alapján,
a 121. § tekintetében a villamos energiáról szóló 2007. évi LXXXVI. törvény 170. § (1) bekezdés 7. pontjában kapott felhatalmazás alapján,
a 122. § tekintetében a minősített adat védelméről szóló 2009. évi CLV. törvény 37. § c) pontjában kapott felhatalmazás alapján,
a 123. § és a 124. § tekintetében a légiközlekedésről szóló 1995. évi XCVII. törvény 73. § (1) bekezdés v) pontjában kapott felhatalmazás alapján,
a 125. § tekintetében a villamos energiáról szóló 2007. évi LXXXVI. törvény 170. § (1) bekezdés 24. pontjában kapott felhatalmazás alapján,
a 126. §, 131. §, 135. § és 136. § tekintetében a jogalkotásról szóló 2010. évi CXXX. törvény 31. § (1) bekezdés b) pontjában kapott felhatalmazás alapján,
a 127. § tekintetében az államháztartásról szóló 2011. évi CXCV. törvény 109. § (1) bekezdés 15. pont d) alpontjában kapott felhatalmazás alapján,
a 128. § tekintetében a hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény 290. § (1) bekezdés c) pontjában, az egyes fizetési szolgáltatókról szóló 2013. évi CCXXXV. törvény 88. § a) pontjában, a biztosítási tevékenységről szóló 2014. évi LXXXVIII. törvény 437. § c) pontjában és a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló 2007. évi CXXXVIII. törvény 180. § (1) bekezdés a) pontjában kapott felhatalmazás alapján,
a 129. § tekintetében a nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény 110. § (1) bekezdés 3. pontjában kapott felhatalmazás alapján,
a 130. § tekintetében Magyarország kiberbiztonságáról szóló törvény 81. § (2) bekezdés 7. pontjában kapott felhatalmazás alapján,
a 132. § tekintetében az egységes elektronikuskártya-kibocsátási keretrendszerről szóló 2014. évi LXXXIII. törvény 21. § (1) bekezdés b) pontjában kapott felhatalmazás alapján,
a 133. § tekintetében az Alaptörvény 15. cikk (3) bekezdésében meghatározott eredeti jogalkotói hatáskörében,
a 134. § tekintetében a Magyarország biztonsági érdekét sértő külföldi befektetések ellenőrzéséről szóló 2018. évi LVII. törvény 12. § b) pontjában kapott felhatalmazás alapján,
a 137. § tekintetében az Alaptörvény 15. cikk (3) bekezdésében meghatározott eredeti jogalkotói hatáskörében,
a 138. §, 139. § és a 140. § tekintetében a Magyarország kiberbiztonságáról szóló törvény 81. § (2) bekezdés 19. pontjában kapott felhatalmazás alapján,
a 141. § tekintetében a médiaszolgáltatásokról és a tömegkommunikációról szóló 2010. évi CLXXXV. törvény 206. § (3c) bekezdés a) és b) pontjában kapott felhatalmazás alapján,
a 142. § tekintetében az Alaptörvény 15. cikk (2) bekezdésében meghatározott eredeti jogalkotói hatáskörében,

a 143. § tekintetében a honvédelemről és a Magyar Honvédségről szóló 2021. évi CXL. törvény 110. § (1) bekezdés 17. pontjában kapott felhatalmazás alapján,
a 144. § tekintetében a Magyarország kiberbiztonságáról szóló törvény 81. § (2) bekezdés 10. pontjában kapott felhatalmazás alapján,
a 145. § és a 146. § tekintetében a Magyarország kiberbiztonságáról szóló törvény 81. § (2) bekezdés 19. pontjában kapott felhatalmazás alapján,
a 147–150. § tekintetében a Magyarország kiberbiztonságáról szóló törvény 81. § (2) bekezdés 13. pontjában kapott felhatalmazás alapján,
a 151. § tekintetében a földgázellátásról szóló 2008. évi XL. törvény 132. § 50. pontjában kapott felhatalmazás alapján,
a 152. § tekintetében a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény 113. § (1) bekezdés 13. pontjában kapott felhatalmazás alapján,
a 153. § tekintetében a digitális államról és a digitális szolgáltatások nyújtásának egyes szabályairól szóló 2023. évi CIII. törvény 113. § (1) bekezdés 11–13. pontjában kapott felhatalmazás alapján,
az Alaptörvény 15. cikk (1) bekezdésében meghatározott feladatkörében eljárva a következőket rendeli el:

I. Fejezet

Általános rendelkezések

1. Hatály

1. §

(1) E rendeletnek a szervezetek kötelezettségeire és a kiberbiztonság hatósági felügyeletére vonatkozó rendelkezéseit – a (2) bekezdésben foglalt kivétellel – a Magyarország kiberbiztonságáról szóló 2024. évi … törvény (a továbbiakban: Kiberbiztonsági tv.) 1. § (1) bekezdés a)-c) pontja szerinti szervezetekre kell alkalmazni.
(2) E rendeletnek az elektronikus információs rendszer biztonságáért felelős személyre vonatkozó rendelkezéseit az alábbi szervezetekre kell alkalmazni:

a) a Kiberbiztonsági tv. 1. § (1) bekezdés a)–c) pontja szerinti szervezetekre,

b) a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti azon szervezetekre, amelyek a kritikus szervezetek ellenálló képességéről szóló 2024. évi … törvény (a továbbiakban: Kszetv.) alapján kritikus szervezetként vannak kijelölve, vagy a Kszetv. alapján kritikus infrastruktúraként kijelölt infrastruktúrát üzemeltetnek (a továbbiakban együtt: kritikus szervezet) kijelölt, , valamint

c) a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti azon szervezetekre, amelyek a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény (a továbbiakban: Vbö.) alapján az ország védelme és biztonsága szempontjából jelentős szervezetként kerültek kijelölésre vagy a Vbö. alapján az ország védelme és biztonsága szempontjából jelentős infrastruktúraként kijelölt infrastruktúrát üzemeltetnek (a továbbiakban együtt: az ország védelme és biztonsága szempontjából jelentős szervezet).

(3) E rendeletnek a kiberbiztonsági gyakorlatokra, valamint a kiberbiztonsági bírságokra vonatkozó rendelkezéseit a Kiberbiztonsági tv. 1. § (1) bekezdése szerinti szervezetekre kell alkalmazni.
(4) E rendelet kiberbiztonsági tanúsításra vonatkozó rendelkezéseit az információs és kommunikációs technológiai (a továbbiakban: IKT) termékek, IKT-szolgáltatások vagy IKT-folyamatok (a továbbiakban együtt: IKT-termék) tanúsításával kapcsolatos tevékenység vonatkozásában kell alkalmazni.
(5) E rendelet sérülékenységvizsgálatra vonatkozó rendelkezései

a) a Kiberbiztonsági tv. 1. § (1) bekezdés a)-c) pontja szerinti szervezetek elektronikus információs rendszereit, valamint

b) a megállapodásban foglalt eltérésekkel a Kiberbiztonsági tv. 61. §-a szerinti megállapodásban meghatározott elektronikus információs rendszereket

érintő sérülékenységvizsgálatokra alkalmazandóak.

(6) E rendelet kiberbiztonsági incidenskezelésre, valamint a kiberbiztonsági válsághelyzet kezelésére vonatkozó rendelkezéseit

a) a Kiberbiztonsági tv. 1. § (1) bekezdése szerinti szervezetek, valamint

b) az e rendeletben meghatározott eltérésekkel az (EU) 2022/2554 európai parlamenti és tanácsi rendelet hatálya alá tartozó szervezetek

elektronikus információs rendszereit érintő kiberbiztonsági incidensek kezelésére kell alkalmazni.

(7) E rendelet sebezhetőségek kezelésére vonatkozó rendelkezései

a) a Kiberbiztonsági tv. 1. § (1) bekezdése szerinti szervezetek elektronikus információs rendszerei kapcsán felfedezett sérülékenységek, valamint

b) az IKT-termék kapcsán felfedezett sebezhetőségek

kezelésére, bejelentésére alkalmazandóak.

2. Értelmező rendelkezések

2. §

E rendelet alkalmazásában

1. *adminisztrátori jogosultsággal rendelkező vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek során a vizsgálatot végző személy rendszergazdai jogosultsággal rendelkezik, és az eljárás célja, hogy megfelelőségi listák alapján az érintett elektronikus információs rendszer valamennyi elemének az állapota teljeskörűen ellenőrzésre kerüljön;
2. *alkalmazásvizsgálat*: olyan sérülékenységvizsgálati módszer, amelynek során az alkalmazások – ideértve az asztali, a mobil- és a webalkalmazásokat is – sérülékenységei automatizált és kézi vizsgálati módszerek felhasználásával kerülnek feltérképezésre;
3. *automatizált sérülékenységfelderítés és -elemzés:* olyan sérülékenységvizsgálati módszer, amelynek a során a szervezet elektronikus információs rendszerének a sérülékenységei kizárólag célszoftverek segítségével kerülnek feltérképezésre és dokumentálásra;
4. *CSIRT*: az (EU) 2022/2555 európai parlamenti és tanácsi irányelv szerinti **s**zámítógép-biztonsági eseményekre reagáló csoport;
5. *CSIRT-hálózat*: az Európai Unió tagállamai által kijelölt CSIRT-eknek az (EU) 2022/2555 európai parlamenti és tanácsi irányelv szerint létrehozott hálózata**;**
6. *egyedüli kapcsolattartó pont*: az (EU) 2022/2555 európai parlamenti és tanácsi irányelv alapján az Európai Unió tagállamai által kijelölt összekötő feladatokat ellátó szerv;
7. *európai sebezhetőség-adatbázis:* az IKT-termékben található nyilvánosan ismert sérülékenységeknek – az (EU) 2022/2555 európai parlamenti és tanácsi irányelv rendelkezései alapján – az Európai Uniós Kiberbiztonsági Ügynökség (a továbbiakban: ENISA) által felállított és működtetett nyilvántartása, amely tartalmazza
   a) a sebezhetőséget leíró információkat,
   b) az érintett IKT-terméket, valamint a sebezhetőség súlyosságát azon körülmények szempontjából, amelyek között a sebezhetőség kihasználható,
   c) a kapcsolódó javítások elérhetőségét, valamint elérhető javítás hiányában az illetékes hatóságok vagy a CSIRT-ek által a sérülékeny IKT-termékek felhasználói számára a közzétett sebezhetőségből fakadó kockázatok mérséklésének módjáról kiadott útmutatást;

8. *figyelemfelhívás:* a Központ által a magyar kiberteret általánosan veszélyeztető, különös figyelmet érdemlő fenyegetettségekről, új támadási módszerekről, eseményekről kiadott tájékoztatás;
9. *figyelmeztetés:* a Központ által valamely fenyegetés esetén kiadott figyelemfelhívás, olyan esetekben, amikor nincs folyamatban lévő kiberbiztonsági incidens vagy a kiberbiztonsági incidens nem volt kritikus;
10. *incidenskezelési terv:* az incidensek kezelésére irányuló tervdokumentum, amely a hiányosságok megszüntetésével párhuzamosan tartalmazza az incidensek megelőzése, észlelése, elemzése és elszigetelése vagy az incidensre való reagálás és az incidenst követően a működés helyreállítása érdekében végrehajtandó feladatokat, a feladatok teljesítésének mérföldköveit, a kapcsolódó végrehajtási határidőket, a végrehajtásért felelős személy megjelölését és az ehhez szükséges erőforrásokat;
11. *intézkedési terv*: a szervezet rendelkezésében lévő elektronikus információs rendszer vonatkozásában megállapított biztonsági osztály kapcsán meghatározott védelmi intézkedések teljesítése, a hiányosságok felszámolása érdekében végrehajtandó feladatokat, a feladatok teljesítésének mérföldköveit, a kapcsolódó végrehajtási határidőket, a végrehajtásért felelős személy megjelölését és az ehhez szükséges erőforrásokat tartalmazó tervdokumentum;
12. *kézi vizsgálat:* olyan sérülékenységvizsgálati módszer, amelynek során a szervezet elektronikus információs rendszerének sérülékenységei a vizsgálatot végző személy által egyedileg, kézi úton összeállított lekérdezések alkalmazásával kerülnek feltérképezésre;
13. *kiberbiztonsági gyakorlat*: az információbiztonsági szabályzatban megjelölt szervezeti és eszközrendszer megfelelőségének és működőképességének vizsgálata céljából végrehajtott komplex feladat;
14. *kiber-fizikai rendszerek biztonsági vizsgálata*: olyan sérülékenységvizsgálati módszer, amelynek során a kiber-fizikai rendszerek sérülékenységei a vizsgálatot végző személy által, elsősorban passzív technikák és eljárások alkalmazásával, az elektronikus információs rendszer funkcionális működésének negatívan történő befolyásolása nélkül, illetve folyamatos rendszerfelügyeleti támogatás mellett aktív eszközökkel kerülnek feltérképezésre;
15. *Központ:* a nemzeti kiberbiztonsági incidenskezelő központ;
16. *közvetítő szolgáltató:* az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló törvény szerinti fogalom;
17. *külső informatikai biztonsági vizsgálat:* olyan sérülékenységvizsgálati módszer, amelynek során az elektronikus információs rendszer internet irányából elérhető elemei vonatkozásában az interneten fellelhető, nyilvános adatbázisokban való szabad keresésre, célzott információgyűjtésre, valamint az elektronikus információs rendszer elérhető szolgáltatásainak, sérülékenységeinek feltérképezésére kerül sor;
18. *pszichológiai manipulációs vizsgálat:* olyan sérülékenységvizsgálati módszer, amelynek során az emberek befolyásolására alapozva lehetőség nyílik bizalmas információk megszerzésére vagy kártékony program terjedésére és működésére;
19. *regisztrált felhasználói jogosultsággal rendelkező vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek során a vizsgálatot végző személy a számára külön létrehozott felhasználói jogosultsággal végzi a vizsgálatot;
20. *regisztrált felhasználói jogosultság nélküli vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek során a vizsgálatot végző személy semmilyen előzetes információval nem rendelkezik a vizsgált elektronikus információs rendszerről, és nincs felhasználói jogosultsága a rendszerhez;
21. *riasztás*: folyamatban lévő incidens vagy incidenssorozat megszakítása érdekében széles körben alkalmazott rendszerekben azonnali intézkedést igénylő figyelemfelhívás;
22. *sérülékenység kockázati besorolása*: a sérülékenységvizsgálatot végző által alkalmazott módszertan szerint meghatározott kockázatelemzési eredmény;

23. *szándékolt incidens*: olyan incidens, amelyet szándékos jogellenes vagy rosszhiszemű cselekmény idéz elő;

24. *szolgáltatói nyilvántartás:* az ENISA által az (EU) 2022/2555 európai parlamenti és tanácsi irányelv alapján vezetett, a DNS-szolgáltatók, a legfelső szintű doménnév-nyilvántartók, a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek, a felhőszolgáltatók, az adatközpont-szolgáltatók, a tartalomszolgáltató hálózati szolgáltatók, az irányított szolgáltatók és az irányított biztonsági szolgáltatók, valamint az online piacterek, az online keresőprogramok és a közösségimédia-szolgáltatási platformok nyilvántartása;

25. *vezeték nélküli hálózat informatikai biztonsági vizsgálat:* olyan sérülékenységvizsgálati módszer, amelynek során a vezeték nélküli hozzáférési és kapcsolódási pontok keresése, feltérképezése, titkosítási eljárások elemzése, titkosítási kulcsok visszafejthetőségének ellenőrzése célszoftverek és kézi vizsgálat útján történik.

II. Fejezet

A szervezetek kötelezettségei

3. Adatosztályozás

3. §

(1) A Kiberbiztonsági tv. 9. §-a szerint adatosztályozásra köteles szervezet az adatok osztályozását az 1. mellékletben meghatározott szempontok alapján végzi el.

(2) A szervezet vezetőjének a tervezett külföldi adatkezelésre vagy nem privát felhőhasználatra irányuló döntését megelőzően

a) a Kiberbiztonsági tv. 1. § (1) bekezdés a) pontja szerinti szervezet költség-haszon elemzést és kilépési tervet,

b) a Kiberbiztonsági tv. 1. § (1) bekezdés b) és c) pontja szerinti szervezet legalább kilépési tervet készít.

(3) A költség-haszon elemzés keretében a szervezet vizsgálja és kimutatja az aktuálisan alkalmazott technológiához képest a nem privát felhőszolgáltatás igénybevételével járó előnyöket és hátrányokat, a kilépési terv keretében megtervezi a felhőszolgáltatás alkalmazásáról a helyi környezetre vagy privát felhő használatára történő visszaállás lépéseit, annak következményeit és költségvonzatát.

(4) A Kiberbiztonsági tv. 1. § (1) bekezdés a) pontja szerinti szervezet vezetője abban az esetben dönt a külföldi adatkezelés vagy a nem privát felhőszolgáltatás igénybevétele mellett, amennyiben a költség-haszon elemzés és a kilépési terv eredményei alapján a külföldi adatkezelés vagy a nem privát felhőszolgáltatás igénybevétele a szervezet számára megalapozottan előnyökkel jár.

(5) A szervezet az adatosztályozás eredményét a biztonsági osztályba sorolás eredményének bejelentése keretében jelenti be a 16. § (1) bekezdése szerinti nemzeti kiberbiztonsági hatóság (a továbbiakban: nemzeti kiberbiztonsági hatóság) részére.

4. Védelmi intézkedésekre vonatkozó rendelkezések

4. §

(1) A védelmi intézkedések meghatározása és megfelelőségének mérlegelése során – amennyiben rendelkezésre áll – a szervezet figyelembe veszi az Európai Bizottság és az ENISA által, a kritikus ellátási láncok vonatkozásában elvégzett összehangolt biztonsági kockázatértékelések eredményeit.

(2) Ha a szervezet vagy a kiberbiztonsági audit során az auditor az adott elektronikus információs rendszerre vonatkozó biztonsági osztályhoz kapcsolódó védelmi intézkedések értékelése során

hiányosságot állapít meg, akkor a szervezet – a vizsgálat vagy az audit eredményének kézhezvételét követő 90 napon belül – intézkedési tervet készít a hiányosság megszüntetésére, amelyet jóváhagyásra benyújt a nemzeti kiberbiztonsági hatóság részére.

5. Biztonsági osztályba sorolás felülvizsgálata

5. §

(1) A szervezet soron kívül felülvizsgálja a biztonsági osztályba sorolást, ha az elektronikus információs rendszer kockázati környezetében vagy az adatosztályozásban változás következik be.
(2) A biztonsági osztályba sorolás felülvizsgálatának eredményét a szervezet 15 napon belül megküldi a nemzeti kiberbiztonsági hatóság részére.

6. Az információbiztonsági szabályzat felülvizsgálata

6. §

A szervezet az információbiztonsági szabályzatot soron kívül felülvizsgálja és módosítja

a) olyan változás esetén, amely érinti az elektronikus információs rendszer biztonságát, bizalmasságát, rendelkezésre állását, sértetlenségét vagy a szervezet által nyújtott szolgáltatást,
b) az újonnan felmerülő kockázat kezelése érdekében, ha a bekövetkezett kiberbiztonsági incidenssel vagy incidensközeli helyzettel összefüggő kockázatot a kockázatelemzés során nem vizsgálták,
c) az ellenőrzés, a kiberbiztonsági audit vagy a kiberbiztonsági gyakorlat alkalmával feltárt hiányosságok alapján, a nemzeti kiberbiztonsági hatóság által előírtak szerint.

7. §

A Kiberbiztonsági tv. 8. § (7) bekezdése szerinti kiberbiztonsági információmegosztási megállapodások keretében az információmegosztás során a szervezetek az információk érzékeny jellegét tiszteletben tartva járnak el.

7. A nemzeti kiberbiztonsági hatósággal való együttműködés

8. §

(1) A szervezet a nemzeti kiberbiztonsági hatóság – honvédelmi célú elektronikus információs rendszer vonatkozásában a honvédelmi kiberbiztonsági hatóság – által meghatározott és közzétett formátumban, elektronikus úton tesz eleget bejelentési és adatszolgáltatási kötelezettségének, ezzel egyidejűleg megküldi a bejelentett adatokat igazoló dokumentumokat.
(2) A Kiberbiztonsági tv. 8. § (4) bekezdés f) pontja szerinti bejelentés keretében a szervezet megküldi a nemzeti kiberbiztonsági hatóságnak

a) az elektronikus információs rendszer biztonsági osztályba sorolásának eredményét,
b) a biztonsági osztály alapján meghatározott védelmi intézkedéseket, beleértve a helyettesítő védelmi intézkedéseket,
c) a b) pont szerinti védelmi intézkedések megfelelőségének értékelését, valamint
d) a b) pont szerinti védelmi intézkedések aktuális státuszát.

9. §

(1) A szervezet jogutódlással történő megszűnése esetén a jogutód a változást követő 15 napon belül köteles nyilvántartásba vétel céljából bejelenteni a jogutódlást a nemzeti kiberbiztonsági hatóság részére.
(2) A szervezet a jogutódlás nélkül történő megszűnését – legkésőbb a megszűnés időpontjáig – köteles bejelenteni a nemzeti kiberbiztonsági hatóság részére.
(3) Ha a nemzeti kiberbiztonsági hatóság tudomást szerez a szervezet jogutódlás nélkül történő megszűnéséről, hivatalból intézkedik annak nyilvántartásban történő rögzítéséről.

8. Kiberbiztonsági gyakorlatok

10. §

(1) A Kiberbiztonsági tv. 1. § (1) bekezdése szerinti
a) alapvető szervezet kétévente,
b) szervezet a Központ kötelezése alapján vagy
c) szervezet a nemzeti kiberbiztonsági hatóság kötelezése alapján
önállóan, vagy a Központ irányításával kiberbiztonsági gyakorlatot folytat le.
(2) A szervezet a kiberbiztonsági gyakorlat lefolytatásába bevonja az elektronikus információs rendszer üzemeltetésében, a kapcsolódó szolgáltatások nyújtásában részt vevő közreműködőit.
(3) A szervezet által önállóan szervezett gyakorlatot a szervezet maga folytatja le vagy e célból közreműködőt vehet igénybe. Az önállóan szervezett gyakorlat lefolytatása vonatkozásában a Központ módszertant határoz meg, amelyet a honlapján közzétesz.
(4) A szervezet az önállóan lefolytatott gyakorlatról – a Központ honlapján közzétett módszertan alapján – készített értékelő beszámolót a gyakorlat lefolytatását követő 30 napon belül megküldi a Központ részére. A beszámoló tartalmazza legalább a gyakorlat forgatókönyvét, résztvevőit, a lezajlott eseményeket, a gyakorlat eredményességének értékelését.
(5) A gyakorlat megfelelőségét a Központ értékeli. Ha a gyakorlat során vagy az önállóan lefolytatott gyakorlatról beküldött beszámoló alapján a Központ hiányosságokat állapít meg, a jelzése alapján a nemzeti kiberbiztonsági hatóság felszólítja – a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti szervezet kivételével – a szervezet vezetőjét a nem megfelelő védelmi intézkedések módosítására, és a gyakorlat megismétlésére kötelezheti.
(6) Az (1) bekezdés b) és c) pontja szerinti kötelezés esetén a kiberbiztonsági gyakorlaton való részvétel kötelező.

9. Az elektronikus információs rendszer biztonságáért felelős személy

11. §

(1) Az elektronikus információs rendszer biztonságáért felelős személy feladatát a szervezet igényeihez igazodva és annak rendelkezése szerint látja el.
(2) A szervezet vezetője az elektronikus információs rendszer biztonságáért felelős személy kijelölését vagy megbízását
a) megelőzően meggyőződik a meghatározott jogszabályi követelményeknek való megfelelőségéről,
b) követően nyilvántartásba vétel érdekében bejelenti a nemzeti kiberbiztonsági hatóság részére, egyidejűleg megküldi a bejelentett adatokat igazoló dokumentumokat.
(3) Az elektronikus információs rendszer biztonságáért felelős személyre vonatkozó bejelentés magában foglalja a vonatkozó munka-, megbízási szerződés vagy más megállapodás másolatának hatóság számára történő megküldését olyan módon, hogy abból csak a hatóság számára releváns, a feladat- és hatásköre ellátáshoz szükséges információ legyen megismerhető. A megállapodáshoz

csatolni kell az adott személy végzettségét, képzettségét igazoló okirat, vagy a szakterületi gyakorlatot igazoló okirat, vagy nyilatkozat másolatát.
(4) Az elektronikus információs rendszer biztonságáért felelős személyre vonatkozó megállapodásnak legalább a következőket kell tartalmaznia:
a) a szerződő felek azonosítására alkalmas adatokat,
b) az elektronikus információs rendszer biztonságáért felelős személy feladatait ellátó természetes személy azonosítására alkalmas adatokat,
c) a megbízás tárgyát,
d) a felek jogait és kötelezettségeit a hatályos jogszabályokban foglaltaknak megfelelően.
(5) Az elektronikus információs rendszer biztonságáért felelős személy büntetlen előéletét a szervezet vezetője – a nemzeti kiberbiztonsági hatóság, honvédelmi célú elektronikus információs rendszer vonatkozásában a honvédelmi kiberbiztonsági hatóság által meghatározott módon – igazolja.
(6) A szervezet vezetője az elektronikus információs rendszer biztonságáért felelős személyt kötelezheti, hogy a szervezettel fennálló jogviszonya alatt a büntetlen előélet követelményének való megfelelést igazolja.

12. §

(1) Az elektronikus információs rendszer biztonságáért felelős személy az e feladatkörében a nemzeti kiberbiztonsági hatóság előtti eljárásra a nemzeti kiberbiztonsági hatóság általi nyilvántartásba vételét követően válik jogosulttá, és képviseleti joga megszűnésének bejelentéséig vagy a nemzeti kiberbiztonsági hatóság általi hivatalból való törléséig képviseletre jogosult személynek kell tekinteni.
(2) Az elektronikus információs rendszer biztonságáért felelős személy
a) gondoskodik a szervezet elektronikus információs rendszereinek biztonságával összefüggő tevékenységek jogszabályokkal való összhangjának megteremtéséről és fenntartásáról,
b) gondoskodik a kockázatkezelési keretrendszer szerinti tevékenységek tervezéséről, szervezéséről, koordinálásáról, elvégzéséről és ellenőrzéséről,
c) előkészíti és a szervezet vezetőjének jóváhagyását követően megküldi a nemzeti kiberbiztonsági hatóság részére a szervezet információbiztonsági szabályzatát,
d) előkészíti a szervezet elektronikus információs rendszereinek biztonsági osztályba sorolását,
e) előkészíti és a szervezet vezetőjének egyetértésével kezdeményezi a nemzeti kiberbiztonsági hatóságnál a szervezet elektronikus információs rendszereivel kapcsolatos engedélyezési eljárásokat,
f) megtartja vagy megszervezi a továbbképzésre kötelezett személyek részére jogszabályban előírt továbbképzéseket,
g) véleményezi az elektronikus információs rendszerek biztonsága szempontjából a szervezet elektronikus információbiztonságot érintő szabályzatait és szerződéseit,
h) folyamatos és tervezett ellenőrzéseket végez annak vizsgálatára, hogy a szervezet elektronikus információbiztonságra vonatkozó belső normáiban lévő előírások hogyan valósulnak meg, ennek megállapításait írásban rögzíti a szervezet vezetője számára,
i) felülvizsgálja, hogy a szervezet elektronikus információbiztonságot érintő belső szabályzatai összhangban vannak-e a hatályos jogszabályokkal és a szervezet belső szabályozóival,
j) az ellenőrzések és az esetleges incidensek tapasztalatai felhasználásával – a fejlesztendő területekre vonatkozó javaslatokat tartalmazó – biztonsági helyzetértékelést készít a szervezet vezetője számára,
k) legalább évente megvizsgálja a 4. § (2) bekezdése szerinti intézkedési tervet és beszámolót készít a szervezet vezetője számára az előrehaladásról, amiben kiemeli az esetleges lemaradásokat és a rövid távon szükséges intézkedéseket,
l) kapcsolatot tart a nemzeti kiberbiztonsági hatósággal és a kiberbiztonsági incidenskezelő központtal,

m) a szervezet bármely elektronikus információs rendszerét érintő incidensről tájékoztatja e rendeletben meghatározott szervet,

n) együttműködik a Kszetv. szerinti kritikus szervezet ellenálló képességéért felelős vezetővel, valamint a Vbö. szerinti ellenálló képességért felelős vezetővel.

(3) Ha az elektronikus információs rendszer biztonságáért felelős személy feladatait a szervezeten kívüli személy végzi, feladatait alapvető szervezeteknél legalább kéthavonta egy napon, fontos szervezeteknél legalább háromhavonta egy napon – dokumentált módon – az érintett szervezetnél való fizikai jelenlét mellett köteles ellátni.

10. Elektronikus információs rendszer fejlesztése, továbbfejlesztése esetén követendő eljárásrend

13. §

(1) A szervezet az elektronikus információs rendszer fejlesztésére, továbbfejlesztésére (a továbbiakban együtt: fejlesztés) irányuló szerződésekben köteles meghatározni a fejlesztő részére a sérülékenységvizsgálat során feltárásra kerülő sérülékenységek javítására vonatkozó feltételeket.

(2) A szervezet az elektronikus információs rendszer fejlesztése esetén a tervezési életciklusban elvégzett adatosztályozás és osztályba sorolás eredményét és indokolását a nemzeti kiberbiztonsági hatóság – honvédelmi célú elektronikus információs rendszer vonatkozásában a honvédelmi kiberbiztonsági hatóság – által a honlapján közzétett nyomtatványon és mellékleteivel együtt nyújtja be a nemzeti kiberbiztonsági hatóság részére.

(3) A nemzeti kiberbiztonsági hatóság az adatosztályozást és a biztonsági osztályba sorolást felülbírálhatja, és indokolt esetben magasabb vagy alacsonyabb szintű besorolást is megállapíthat.

(4) A szervezet vezetője biztosítja, hogy a biztonsági osztályhoz kapcsolódó védelmi követelmények a fejlesztés során megvalósuljanak.

(5) A szervezet a fejlesztés során felülvizsgálja

a) az adatosztályozást, amennyiben az elektronikus információs rendszerben kezelendő adatok körében, valamint

b) a biztonsági osztályba sorolást, amennyiben az elektronikus információs rendszer kockázati környezetében

változás következik be.

(6) A szervezet a felülvizsgálat eredményeként kapott besorolást a nemzeti kiberbiztonsági hatóságnak jóváhagyásra benyújtja. A biztonsági osztályba sorolás vizsgálata során a nemzeti kiberbiztonsági hatóság a 30. § szerint jár el.

14. §

(1) Az elektronikus információs rendszer használatbavétele, illetve meglévő elektronikus információs rendszer továbbhasználata kapcsán a szervezet vezetője által hozott döntésnek a nemzeti kiberbiztonsági hatóság általi jóváhagyását a szervezet a nemzeti kiberbiztonsági hatóság – honvédelmi célú elektronikus információs rendszer vonatkozásában a honvédelmi kiberbiztonsági hatóság – honlapján közzétett nyomtatványon kérelmezi.

(2) A kérelemnek tartalmaznia kell a biztonsági osztályba sorolás eredményeként kapott, elvárt védelmi intézkedések megvalósításáról készült valamennyi dokumentációt.

(3) A nemzeti kiberbiztonsági hatóság a jóváhagyását adja, ha meggyőződött róla, hogy az érintett elektronikus információs rendszer valamennyi elvárt kiberbiztonsági kritériumot teljesíti és ezzel egyidőben nyilvántartásba veszi az elektronikus információs rendszert. Ellenkező esetben a hatóság hiánypótlásra, a hiányosságok javítására, pótlására szólít fel és megtilthatja az elektronikus információs rendszer használatba vételét, továbbhasználatát.

11. A központi rendszerek és a központi szolgáltatások esetén irányadó rendelkezések

15. §

(1) A felhasználó szervezet, ha a rendelkezésében lévő elektronikus információs rendszerhez kapcsolódóan központi szolgáltatást vesz igénybe, megküldi a központi szolgáltatónak az elektronikus információs rendszer

a) nevét,

b) biztonsági osztályát,

c) rövid funkcióleírását, valamint

d) a kijelölt kapcsolattartó személyek – ideértve az adatgazda, az üzemeltetési felelős és az elektronikus információs rendszer biztonságáért felelős személy – alábbi adatait:

da) neve,

db) beosztása,

dc) kapcsolattartásra alkalmas elektronikus levelezési címe, telefonszáma.

(2) A központi rendszer felett rendelkezési jogot gyakorló szervezet vagy a központi szolgáltató a központi rendszerként, támogató rendszerként vagy központi szolgáltatásként való minősülés megállapítása érdekében előzetesen egyeztet a nemzeti kiberbiztonsági hatósággal. A nemzeti kiberbiztonsági hatóság az egyeztetésbe bevonhatja a felhasználó szervezeteket.

(3) A szolgáltatást nyújtó szolgáltatáskatalógusában rögzíti a központi szolgáltatás megnevezését, valamint, hogy

a) az általa nyújtott szolgáltatás központi szolgáltatásnak, központi rendszernek, támogató rendszernek vagy egyéb szolgáltatásnak minősül,

b) a központi szolgáltatás vagy támogató rendszer milyen biztonsági osztály követelményeinek megfelelő szolgáltatásokat tud nyújtani,

c) a központi szolgáltatást megvalósító elektronikus információs rendszerek milyen biztonsági osztály követelményeinek felelnek meg.

(4) Több szolgáltató által együttesen nyújtott központi szolgáltatás vonatkozásában a szolgáltatók megállapodásban rögzítik az általuk nyújtott szolgáltatásrészek tekintetében a felelősségi határokat, valamint az adott szolgáltatásrész által biztosított védelmi intézkedéseket.

III. Fejezet

A kiberbiztonság hatósági felügyelete

12. A nemzeti kiberbiztonsági hatóságra vonatkozó általános rendelkezések

16. §

(1) A Kormány

a) a Kiberbiztonsági tv. 23. § (1) bekezdés a) pontja szerinti nemzeti kiberbiztonsági hatóságként, valamint

b) az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (a továbbiakban: Ekertv.) 15/B. §-a szerinti hatóságként

a Nemzetbiztonsági Szakszolgálatot jelöli ki.

(2) A Kormány a Kiberbiztonsági tv. 23. § (2) bekezdése szerinti honvédelmi kiberbiztonsági hatóságként a honvédelemért felelős minisztert jelöli ki.

(3) A honvédelmi kiberbiztonsági hatóság tevékenységére – a 18. § e) pontjában, a 25. §-ban, a 39. § (2) és (3) bekezdésében foglaltak kivételével – a nemzeti kiberbiztonsági hatóságra vonatkozó rendelkezéseket kell alkalmazni.

17. §

(1) A nemzeti kiberbiztonsági hatóság jogosult

a) a biztonsági osztályba sorolást, a védelmi intézkedéseket és az ehhez kapcsolódó eljárási szabályok teljesülését ellenőrizni,

b) a minimálisan elvárt védelmi intézkedéseket meghatározni,

c) a szervezet által meghatározott biztonsági osztályhoz tartozó védelmi intézkedéseken túl további biztonsági követelményeket meghatározni,

d) a szervezet által elfogadott kiberbiztonsági kockázatkezelési intézkedések – többek között a dokumentált kiberbiztonsági szabályzatok – értékeléséhez, valamint az információk bejelentésére vonatkozó kötelezettség betartásának értékeléséhez szükséges tájékoztatást kérni,

e) a védelmi intézkedések és az ehhez kapcsolódó eljárási szabályok teljesülését ellenőrizni,

f) rendszeres, eseti és célzott biztonsági ellenőrzéseket végezni, ideértve a helyszíni ellenőrzéseket, a távoli felügyeleti intézkedéseket és a véletlenszerű ellenőrzéseket is,

g) a felügyeleti feladatai ellátásához szükséges adatokhoz, dokumentumokhoz és információkhoz hozzáférni és ezeket bekérni, illetve a megküldött dokumentumok felülvizsgálatát elrendelni,

h) eljárása során – a honvédelmi elektronikus információs rendszerek kivételével – független értékelőt igénybe venni, és az általa végzett ellenőrzés eredményét, továbbá a szervezet által megbízott független értékelő jelentésében vagy a kiberbiztonsági auditjelentésben foglaltakat figyelembe venni,

i) az elektronikus információs rendszerekre és eszközökre, a szervezetekre nemzetközi egyezmények vagy nemzetközi szabványok alapján, illetve az ezeken alapuló hazai követelmények vagy ajánlások alapján kiadott biztonsági tanúsítványokat figyelembe venni,

j) európai uniós jogi aktus által meghatározott kiberbiztonsági követelményeknek való megfelelést részben vagy egészben az informatikáért felelős miniszter rendeletében meghatározott védelmi követelményeknek való megfelelésnek tekinteni,

k) az ellenőrzés során feltárt hiányosságok felszámolásához szükséges intézkedéseket elrendelni, ezek teljesülését ellenőrizni,

l) a felügyeleti jogkörébe tartozó szervezetek vonatkozásában szabvány alkalmazására, európai vagy hazai kiberbiztonsági tanúsítási rendszerek által tanúsított IKT-termék használatára, illetve minősített bizalmi szolgáltatás igénybevételére iránymutatásokat kiadni,

m) az elektronikus információs rendszerek használatba vételének, meglévő elektronikus információs rendszer továbbhasználatának jóváhagyása során helyszíni ellenőrzést tartani és sérülékenységvizsgálatot elrendelni,

n) a Központ megkeresése alapján a szervezet elektronikus információs rendszere kapcsán bejelentett sérülékenység felszámolásához szükséges intézkedéseket elrendelni, ezek teljesülését ellenőrizni, illetve egyedi mérlegelés alapján sérülékenységvizsgálatot elrendelni.

(2) A nemzeti kiberbiztonsági hatóság jogszabályban meghatározott feladatainak ellátása érdekében jogosult

a) a szervezettől,

b) a szervezet felett hatósági, felügyeleti vagy ellenőrzési jogkört gyakorló szervezettől,

c) közhiteles nyilvántartásokból és

d) az adatkezelést végző szervtől

térítésmentesen adatot igényelni vagy átvenni.

(3) A nemzeti kiberbiztonsági hatóság a (2) bekezdés alapján személyes adatot nem igényelhet vagy vehet át, illetve kizárólag a jogszabályban meghatározott feladatainak ellátása érdekében elengedhetetlenül szükséges adatot igényelhet vagy vehet át.

18. §

A nemzeti kiberbiztonsági hatóság feladatai ellátása során együttműködik az elektronikus információbiztonság területén

a) a kiberbiztonsági incidenskezelő központokkal,
b) a kiberbiztonsági tanúsító hatósággal,
c) a Kszetv. szerinti kijelölő hatósággal és szakhatósággal,
d) a Vbö. szerinti kijelölő hatósággal és szakhatósággal,
e) az (EU) 2022/2554 európai parlamenti és tanácsi rendelet szerinti hatósággal,
f) a rendvédelmi szervekkel,
g) a nemzetbiztonsági szolgálatokkal,
h) a Nemzeti Adatvédelmi és Információszabadság Hatósággal,
i) az Európai Unió tagállamainak vagy harmadik országok kiberbiztonsági felügyeleti hatóságaival,
j) más tagállamok illetékes hatóságaival, valamint
k) a katonai kibertér műveleti erőkkel.

19. §

Ha a szervezet jelentős kiberbiztonsági incidensről értesíti a nemzeti kiberbiztonsági hatóságot, a nemzeti kiberbiztonsági hatóság a kézhezvételt követően továbbítja az értesítést a Központnak.

20. §

(1) A nemzeti kiberbiztonsági hatóság és a Kszetv. szerinti kijelölő hatóság együttműködése keretében

a) szükség szerint információt cserél a kritikus szervezetek kijelöléséről, a kritikus szervezetként kijelölt alapvető szervezeteket érintő nem kiberbiztonsági kockázatokról, fenyegetésekről és eseményekről, az említett kockázatokra, fenyegetésekre és eseményekre való reagálásként hozott intézkedésekről, valamint nem kiberbiztonsági jellegű kockázatok, fenyegetések és események, ideértve a kritikus szervezetek által végrehajtott kiberbiztonsági és fizikai intézkedéseket, valamint az ilyen szervezetek tekintetében végzett felügyeleti tevékenységek eredményeiről,
b) a nemzeti kiberbiztonsági hatóság tájékoztatja a Kszetv. szerinti hatóságot, amikor a Kszetv. szerint kijelölt kritikus szervezettel szemben hatósági felügyeleti intézkedést tesz az (EU) 2022/2555 európai parlamenti és tanácsi irányelvnek való megfelelés biztosítása érdekében,
c) a Kszetv. szerinti hatóság megkereséssel élhet a nemzeti kiberbiztonsági hatóság felé hatósági jogköreinek gyakorlása, intézkedés megtétele érdekében a Kszetv. szerint kijelölt kritikus szervezet esetében az (EU) 2022/2555 európai parlamenti és tanácsi irányelvnek való megfelelés biztosítása érdekében.

(2) A nemzeti kiberbiztonsági hatóság és a Vbö. szerinti kijelölő hatóság együttműködése keretében az (1) bekezdés szerint jár el az ország védelme és biztonsága szempontjából jelentős szervezetek vonatkozásában.

(3) A nemzeti kiberbiztonsági hatóság az (EU) 2022/2554 európai parlamenti és tanácsi rendelet szerinti hatósággal történő együttműködés keretében tájékoztatja az (EU) 2022/2554 európai parlamenti és tanácsi rendelet 32. cikk (1) bekezdése szerint létrehozott felvigyázási fórumot, amikor hatósági felügyeleti intézkedést tesz annak érdekében, hogy a Kiberbiztonsági tv. hatálya alá tartozó,

az (EU) 2022/2554 európai parlamenti és tanácsi rendelet 31. cikke szerint kritikus harmadik fél IKT-szolgáltatónak kijelölt alapvető szervezetek megfeleljenek az (EU) 2022/2555 európai parlamenti és tanácsi irányelvnek.
(4) A honvédelmi kiberbiztonsági hatóság és a Vbö. szerinti honvédelmi ágazati kijelölő hatóság együttműködése keretében az (1) bekezdés szerint jár el.

21. §

(1) Ha egy szervezet egynél több európai uniós tagállamban nyújt szolgáltatásokat, vagy egy vagy több európai uniós tagállamban nyújt szolgáltatásokat, és hálózati és információs rendszerei egy vagy több másik uniós tagállamban találhatóak, a nemzeti kiberbiztonsági hatóság szükség szerint együttműködik a másik tagállam illetékes hatóságával. Az együttműködés keretében a nemzeti kiberbiztonsági hatóság

a) az általa alkalmazott felügyeleti intézkedésekről – az egyedüli kapcsolattartó ponton keresztül – tájékoztathatja az érintett európai uniós tagállam illetékes hatóságát,

b) felkérheti a másik európai uniós tagállam illetékes hatóságát felügyeleti intézkedések megtételére,

c) egy másik európai uniós tagállam illetékes hatóságától származó indokolt kérelem kézhezvételét követően – a saját erőforrásaihoz mérten arányos módon – kölcsönös segítséget nyújt a megkereső hatóság számára annak érdekében, hogy a felügyeleti intézkedéseket hatékonyan, eredményesen és következetesen lehessen végrehajtani.

(2) A nemzeti kiberbiztonsági hatóság nem utasíthatja el a megkeresést, kivéve, ha megállapítja, hogy nem rendelkezik hatáskörrel a kért segítség nyújtására, a kért segítség nem arányos a nemzeti kiberbiztonsági hatóság felügyeleti feladataival, vagy a megkeresés olyan információra vonatkozik, vagy olyan tevékenységeket foglal magában, amelyek közlése vagy végrehajtása ellentétes lenne Magyarország nemzetbiztonságának, közbiztonságának vagy védelmének alapvető érdekeivel. A megkeresés elutasítása előtt a nemzeti kiberbiztonsági hatóság konzultálhat más illetékes hatósággal, valamint az Európai Bizottsággal és az ENISA-val.
(3) A nemzeti kiberbiztonsági hatóság – közös megegyezés alapján – közös felügyeleti intézkedéseket hajthat végre más európai uniós tagállamok illetékes hatóságaival.

13. A nemzeti kiberbiztonsági hatóság hatósági eljárása

22. §

(1) A nemzeti kiberbiztonsági hatóság eljárásaiban

a) a kérelem kormányablaknál való előterjesztése kizárt,

b) kétszeri hiánypótlásra való felszólításnak van helye a (2) bekezdésben foglalt kivétellel.

(2) A nemzeti kiberbiztonsági hatóság mellőzi az ismételt hiánypótlást, amennyiben a hiánypótlásra ugyanazon szervezet vonatkozásában ugyanazon hiányosságra figyelemmel kerülne sor.
(3) A nemzeti kiberbiztonsági hatóság az eljárását lezáró döntésének meghozatala előtt a szervezettel egyeztetést folytathat le.

23. §

(1) A nemzeti kiberbiztonsági hatóság kiberbiztonsági incidens esetén hatósági eljárást indít abban az esetben, ha

a) a kiberbiztonsági incidenst – a Központ jelzése alapján – a szervezet önállóan vagy a Kiberbiztonsági tv. 70. § (3) bekezdés b) pontja szerinti gazdálkodó szervezet igénybevételével nem tudta megoldani,

b) a kiberbiztonsági incidens mérete, az incidens által okozott kár értéke ezt indokolja,
c) a Központ kezdeményezése esetén.
(2) A honvédelmi kiberbiztonsági hatóság a tudomására jutott kiberbiztonsági incidens kivizsgálása érdekében hatósági eljárást indít.

24. §

A nemzeti kiberbiztonsági hatóság az alapvető vagy fontos szervezetek nyilvántartásából történő törlésről
a) hivatalból vagy
b) az érintett szervezet kérelmére
dönthet.

25. §

(1) Az elektronikus információs rendszer biztonságáért felelős személy feladatainak ellátására alkalmas személyek nyilvántartásába való felvételét kérheti – a hatóság honlapján közzétett formanyomtatványon – a nemzeti kiberbiztonsági hatóságtól az érintett, amennyiben megfelel a Kiberbiztonsági tv.-ben és az e rendeletben foglalt feltételeknek.
(2) Az (1) bekezdés szerinti kérelem tartalmazza az elektronikus információs rendszer biztonságáért felelős természetes személy
a) azonosításához szükséges természetes személyazonosító adatokat,
b) elektronikus levelezési címét,
c) az informatikáért felelős miniszter rendeletében előírt végzettség, szakképzettség, akkreditált nemzetközi képzettség vagy az informatikáért felelős miniszter rendeletében meghatározott szakterületen szerzett szakmai tapasztalat igazolására szolgáló adatokat és dokumentumokat.
(3) Ha az elektronikus információs rendszer biztonságáért felelős természetes személy a Kiberbiztonsági tv.-ben és az e rendeletben meghatározott feltételeket nem teljesíti, a nemzeti kiberbiztonsági hatóság a nyilvántartásba vételre irányuló kérelmet elutasítja. A kérelmező a hatósági döntés véglegessé válását követő 90 napon belül új nyilvántartásba vételi kérelmet nem nyújthat be.
(4) A nyilvántartásba vételt követően a nemzeti kiberbiztonsági hatóság a honlapján közzéteszi az elektronikus információs rendszer biztonságáért felelős természetes személy nevét és elektronikus levelezési címét.
(5) A nyilvántartásba vett elektronikus információs rendszer biztonságáért felelős természetes személynek folyamatosan meg kell felelnie a Kiberbiztonsági tv. 11. § (3) és (8) bekezdésében, valamint az e rendeletben meghatározott feltételeknek.
(6) Az elektronikus információs rendszer biztonságáért felelős természetes személy a bejelentett adatokban bekövetkező változást annak bekövetkezésétől számított 15 napon belül bejelenti a nyilvántartásba vétel érdekében a nemzeti kiberbiztonsági hatóság részére.
(7) A nemzeti kiberbiztonsági hatóság törli a nyilvántartásból az elektronikus információs rendszer biztonságáért felelős természetes személyt
a) kérésére, vagy
b) a Kiberbiztonsági tv. 11. § (3) bekezdésében meghatározott feltételeknek való meg nem felelés esetén.
(8) A nemzeti kiberbiztonsági hatóság törölheti a nyilvántartásból az elektronikus információs rendszer biztonságáért felelős természetes személyt, ha
a) a Kiberbiztonsági tv. 11. § (8) bekezdése szerinti képzési, továbbképzési kötelezettségét nem teljesíti,
b) a 12. § (3) bekezdése szerinti kötelezettséget nem teljesíti, vagy

c) a Kiberbiztonsági tv.-ben és az e rendeletben meghatározott feladatainak ellátására való alkalmatlanságát állapítja meg.

14. Az alapvető, illetve fontos szervezetként történő azonosítás eljárásrendje

26. §

(1) A nemzeti kiberbiztonsági hatóság megvizsgálja az alapvető vagy fontos szervezetként történő azonosítás lehetőségét, amennyiben

a) a Kszetv. alapján a szervezet nem került kritikus szervezetként kijelölésre, és a Kiberbiztonsági tv.-ben meghatározott azonosítási szempontoknak való megfelelés valószínűsíthető,

b) a Vbö. alapján a szervezet nem került az ország védelme és biztonsága szempontjából jelentős szervezetként kijelölésre, és a Kiberbiztonsági tv.-ben meghatározott azonosítási szempontoknak való megfelelés valószínűsíthető,

c) a szervezet vagy létesítmény nemzetbiztonsági védelem alá tartozik, vagy

d) a nemzeti kiberbiztonsági hatóság, a sérülékenységvizsgálat, az incidensvizsgálat vagy a Központ adatai alapján az azonosítás szükségessége felmerült.

(2) Ha a Kszetv. alapján kritikus szervezetként, valamint a Vbö. alapján az ország védelme és biztonsága szempontjából jelentős szervezetként való kijelölésre irányuló eljárás alapján a szervezet nem került kritikus szervezetként, illetve az ország védelme és biztonsága szempontjából jelentős szervezetként kijelölésre, vagy a kijelölés visszavonásra kerül, a Kszetv., valamint a Vbö. szerinti kijelölő hatóság e döntésről tájékoztatja a nemzeti kiberbiztonsági hatóságot.

(3) Ha az azonosítás feltételei fennállnak, a nemzeti kiberbiztonsági hatóság eljárást indít, amelyben közli az érintett szervezettel azokat az adatokat, amelyek szerint megfelel az alapvető vagy fontos szervezetként történő azonosítás kritériumainak.

(4) Ha a szervezet az eljárást megindító végzés tartalmával egyetért, erről 20 napon belül tájékoztatja a nemzeti kiberbiztonsági hatóságot.

(5) Ha a szervezet az eljárást megindító végzés tartalmával nem ért egyet, 20 napon belül köteles a részletes indokolással ellátott véleményét a nemzeti kiberbiztonsági hatóság részére megküldeni. A részletes indokolással ellátott vélemény tartalmazza a szervezet

a) által nyújtott szolgáltatás részletes leírását,

b) a szolgáltatás nyújtásában közreműködő elektronikus információs rendszerei felsorolását, azok szerepét, súlyát a szolgáltatás nyújtásában,

c) más szolgáltatások nyújtásában történő közreműködését, valamint

d) a Kiberbiztonsági tv.-ben az alapvető vagy fontos szervezetként való azonosíthatóság vonatkozásában meghatározott szempontok megállapíthatósága szempontjából releváns adatokat.

(6) A nemzeti kiberbiztonsági hatóság az érintett szervezet által megküldött információkat a Kiberbiztonsági tv. 1. § (6) bekezdésében foglalt szempontok szerint mérlegelve a hatósági eljárást lezáró érdemi döntésében rendelkezik az alapvető vagy fontos szervezetként történő azonosításról vagy annak mellőzéséről.

27. §

(1) A nemzeti kiberbiztonsági hatóság

a) legalább három évente,

b) az alapvető vagy fontos szervezet kérelmére a megszűnésekor vagy

c) az alapvető vagy fontos szervezet által bejelentett változásra tekintettel

felülvizsgálja az azonosításra okot adó körülményeket.

(2) A felülvizsgálat eredményétől függően fenntartja vagy visszavonja az azonosításra vonatkozó döntését.

28. §

Az azonosított alapvető vagy fontos szervezet soron kívül bejelenti a nemzeti kiberbiztonsági hatóság részére, ha a működési körülményeiben olyan változás áll be, amely befolyásolja vagy befolyásolhatja az alapvető vagy fontos státuszát.

15. Adatosztályozás vizsgálata

29. §

(1) A nemzeti kiberbiztonsági hatóság az adatosztályozás eredményét – a nem privát felhőszolgáltatás igénybevétele, illetve a külföldi adatkezelés jogszerűségének megállapítása érdekében – a biztonsági osztályba sorolás megalapozottságának vizsgálatára irányuló eljárás keretében értékeli.
(2) Ha a vizsgálat eredménye alapján nem egyértelmű az adatosztályozás szerinti besorolás, a nemzeti kiberbiztonsági hatóság eljárása keretében tisztázza, hogy a szervezet milyen és mekkora mennyiségű adatot kezel vagy tervez kezelni az elektronikus információs rendszerben.
(3) Ha a nemzeti kiberbiztonsági hatóság nem ért egyet az adatosztályozás eredményével, kötelezheti a szervezetet az adatosztályozás felülvizsgálatára, ismételt elvégzésére.
(4) Ha a vizsgálat eredménye alapján az elektronikus információs rendszerben kezelt vagy kezelni tervezett adatok köre alapján azok külföldi kezelése vagy azok vonatkozásában nem privát felhőszolgáltatás igénybevétele az 1. mellékletben foglaltak szerint nem lehetséges, a nemzeti kiberbiztonsági hatóság nem hagyja jóvá az elektronikus információs rendszer használatát.

16. Biztonsági osztályba sorolás vizsgálata

30. §

(1) Az elektronikus információs rendszerek biztonsági osztályba sorolásának vizsgálata a nemzeti kiberbiztonsági hatóságnak megküldött információk alapján, jogszabályban meghatározott szempontok szerint történik.
(2) Ha az elektronikus információs rendszerre vonatkozó, bejelentett biztonsági osztályba sorolást – ideértve az adott elektronikus információs rendszerre vonatkozó biztonsági osztály meghatározásánál feltárt hiányosság megszüntetésére irányuló intézkedési tervet – a nemzeti kiberbiztonsági hatóság jóváhagyja, az erre irányuló döntés a biztonsági osztályba sorolás későbbi önálló, illetve az érintett szervezet vagy szervezeti egység ellenőrzése során történő felülvizsgálatát nem zárja ki.
(3) A nemzeti kiberbiztonsági hatóság a szervezet által megállapított biztonsági osztályt felülbírálhatja és indokolással magasabb biztonsági osztályba sorolást is megállapíthat.
(4) Ha a nemzeti kiberbiztonsági hatóság az eljárása során az elektronikus információs rendszerre vonatkozó, a szervezet vezetője által megállapított és bejelentett biztonsági osztályba sorolásnál magasabb biztonsági osztályt állapít meg, a következő biztonsági osztályhoz tartozó követelmények elérésére irányadó határidő alkalmazása tekintetében a nemzeti kiberbiztonsági hatóság döntésének megfelelő osztályt kell alapul venni.
(5) Ha a nemzeti kiberbiztonsági hatóság az elektronikus információs rendszerre vonatkozó, bejelentett biztonsági osztályba sorolásnál alacsonyabb osztály alkalmazásának lehetőségét látja, arra javaslatot tesz a szervezetnek.

17. A nemzeti kiberbiztonsági hatóság éves ellenőrzési terve

31. §

(1) Az éves ellenőrzési tervet a nemzeti kiberbiztonsági hatóság előzetes kockázatértékelést követően a tárgyévet megelőző év november 30-áig állítja össze, amelynek összeállításához bevonhatja a Kszetv. szerinti kijelölő hatóságot és a Vbö. szerinti kijelölő hatóságot.
(2) A nemzeti kiberbiztonsági hatóság az éves ellenőrzési terv végrehajtását a tárgyévet követő év március 1-jéig értékeli.
(3) A nemzeti kiberbiztonsági hatóság az éves ellenőrzési tervet a végrehajtás során felülvizsgálja, és szükség szerint módosítja.
(4) A nemzeti kiberbiztonsági hatóság az ellenőrzési tervben foglaltaktól eltérhet, ha olyan azonnali ellenőrzéseket vagy eljárásokat kell lefolytatnia, amelyek a magyar kiberteret, a nemzeti elektronikus adatvagyont, az állam és az állampolgárok számára kiemelten fontos elektronikus információs rendszereket fenyegető súlyos biztonsági események elhárítását szolgálják.
(5) A honvédelmi kiberbiztonsági hatóság az éves ellenőrzési terve összeállításához adatot kér a Vbö. szerinti honvédelmi ágazati kijelölő hatóságtól. A honvédelmi kiberbiztonsági hatóság éves ellenőrzési tervét, valamint a (3) bekezdés szerinti módosítást a honvédelemért felelős miniszter jóváhagyja.

18. A hatósági ellenőrzés általános szabályai

32. §

(1) A nemzeti kiberbiztonsági hatóság ellenőrzést
a) az éves ellenőrzési terv alapján, vagy
b) soron kívül
végez.
(2) A nemzeti kiberbiztonsági hatóság soron kívüli ellenőrzést végezhet, ha azt jelentős kiberbiztonsági incidens bekövetkezése, ennek veszélye, vagy a jogszabályi követelményeknek a szervezet általi megsértése indokolja vagy olyan tény, körülmény jut a tudomására, amely azt indokolttá teszi.

33. §

(1) A nemzeti kiberbiztonsági hatóság az ellenőrzés elrendeléséről az érintett szervezet vezetőjét elektronikus úton az ellenőrzés megkezdése előtt legalább tíz nappal értesíti. Az értesítésnek tartalmaznia kell az ellenőrzés célját, tárgyát, az elrendelésre okot adó körülményeket, az elrendelést megalapozó jogszabályhelyek megjelölését, az ellenőrzés várható időtartamát és az ellenőrzés módját.
(2) Az (1) bekezdés szerinti értesítés mellőzhető, ha
a) súlyos fenyegetettség áll fenn,
b) jelentős kiberbiztonsági incidens történt,
c) az a) vagy b) pont szerinti körülmény bekövetkezése valószínűsíthető, vagy
d) az érintett szervezet a rendelkezésre álló adatok alapján az ellenőrzés eredményes lefolytatását feltehetően meghiúsítaná.
(3) A nemzeti kiberbiztonsági hatóság az ellenőrzést ellátó munkatársa részére megbízólevelet állít ki.

34. §

(1) A nemzeti kiberbiztonsági hatóság az eljárása során, feladatai ellátása érdekében – az intézkedéssel érintett szervezet működésének és ügyvitelének lehető legkisebb mértékű zavarása mellett – az ellenőrzés keretében jogosult önállóan vagy más hatósággal együtt
a) az érintett szervezet információtechnológiai tevékenységével összefüggő helyiségeibe belépni,

b) az érintett szervezet számára adatkezelést biztosító, adatfeldolgozást végző vagy információtechnológiai szempontból érintett helyszínein ellenőrzést tartani,
c) az ellenőrzés során bármely, az elektronikus információbiztonsággal kapcsolatos okiratot, dokumentumot, szerződést, aktív vagy passzív eszközt, információs rendszert, biztonsági intézkedést megismerni, ellenőrizni, az elektronikus információbiztonsággal kapcsolatos okiratokról, dokumentumokról, szerződésekről másolatot készíteni, valamint
d) információtechnológiai műszaki vizsgálatokat végezni, az információtechnológiai rendszerhez egyedileg biztosított belépési jogosultsággal.

(2) A nemzeti kiberbiztonsági hatóság az elektronikus információs rendszerek, és az azokban kezelt adatok biztonsága érdekében jogosult ellenőrizni minden olyan, az elektronikus információs rendszer védelmére vonatkozó intézkedést, amellyel az érintett elektronikus információs rendszert veszélyeztető fenyegetések kezelhetőek.

(3) Az ellenőrzés nem eredményezheti a titkos információgyűjtő munkára, a leplezett eszköz alkalmazására és az abban együttműködő személyekre, továbbá a titkos információgyűjtés és leplezett eszköz alkalmazásának eszközeire és módszereire vonatkozó adat megismerését.

35. §

(1) Az ellenőrzéssel érintett szervezet vezetője, munkatársa, alkalmazottja, illetve szerződéses jogviszony alapján az elektronikus információbiztonság tekintetében érintett egyéb közreműködő és az elektronikus információs rendszer biztonságáért felelős személy köteles a nemzeti kiberbiztonsági hatósággal együttműködni.

(2) Az elektronikus információs rendszer biztonságáért felelős személy köteles az ellenőrzésen részt venni.

(3) A szervezet köteles a nemzeti kiberbiztonsági hatóság által benyújtani kért dokumentumokat rendezett, átlátható formában átadni.

36. §

Az ellenőrzésről a nemzeti kiberbiztonsági hatóság jegyzőkönyvet készít, amelyet az ellenőrzés lezárását követő 15 napon belül írásban észrevételezésre megküld a szervezetnek. A szervezet azzal kapcsolatban 15 napon belül írásban tehet – a hatóságot nem kötelező – észrevételeket. Az észrevételek tisztázása érdekében a nemzeti kiberbiztonsági hatóság egyeztetést kezdeményezhet a szervezettel.

19. Jogkövetkezmények

37. §

(1) A nemzeti kiberbiztonsági hatóság az információbiztonsági követelmények teljesülése érdekében – megfelelő határidő kitűzése mellett – felszólítja a szervezet vezetőjét az elektronikus információbiztonságot veszélyeztető hiányosság, mulasztás, a biztonsági követelmény megsértése megszüntetésére, jogszabályban meghatározott kötelezettség teljesítésére, valamint az elvárt intézkedés megtételére.

(2) A nemzeti kiberbiztonsági hatóság azonnali intézkedések megtételére kötelezi az érintett szervezetet, ha az elektronikus információbiztonságot veszélyeztető hiányosság, mulasztás, a megsértett biztonsági követelmény súlyos kiberbiztonsági incidens bekövetkeztével fenyeget. Ezzel összefüggésben fegyelmi felelősség megállapítására tehet javaslatot a munkáltatói jogkör gyakorlója felé.

(3) A nemzeti kiberbiztonsági hatóság az incidenskezelő központ értesítése esetén megfelelő határidő tűzése mellett felszólítja a szervezetet vagy a közvetítő szolgáltatót a jogszabálysértő tevékenység,

vagy a jogsértő állapot megszüntetésére, ennek keretében bejelentési, adatszolgáltatási, együttműködési kötelezettségének teljesítésére.
(4) A hatósági döntés megtámadására nyitva álló keresetindítási határidő lejártáig, illetve közigazgatási per indítása esetén a bíróság jogerős határozatáig a vitatott jogszabálysértésekkel érintett adatok nem törölhetőek, illetve nem semmisíthetőek meg.

38. §

(1) A nemzeti kiberbiztonsági hatóság a jogkövetkezmények alkalmazása során az alábbi szempontokat veszi figyelembe:
a) az elektronikus információbiztonságot veszélyeztető hiányosság, mulasztás, a megsértett védelmi követelmény súlyát,
b) a jogsértés időtartamát,
c) történt-e jelentős kiberbiztonsági incidens vagy nagyszabású kiberbiztonsági incidens, vagy fennállt-e ilyen esemény bekövetkeztének veszélye,
d) az incidens hatását, vagy lehetséges hatását az érintett szervezetre, vagy más szervezetekre,
e) az okozott bármely vagyoni vagy nem vagyoni kárt, beleértve bármely pénzügyi vagy gazdasági veszteséget, az egyéb szolgáltatásokra gyakorolt hatásokat és az érintett felhasználók számát,
f) az esemény egyedi, vagy ismételt jellegét,
g) az érintett szervezet által korábban elkövetett releváns jogsértéseket,
h) a jogsértés elkövetőjének bármely szándékosságát vagy gondatlanságát,
i) az érintett szervezet magatartását, a szervezet által a vagyoni vagy nem vagyoni kár megelőzésére vagy mérséklésére tett bármely intézkedést,
j) a jóváhagyott magatartási kódexek vagy jóváhagyott tanúsítási mechanizmusok betartásra kerültek-e,
k) a felelősnek tartott természetes vagy jogi személyek illetékes hatóságokkal való együttműködésének szintjét, valamint
l) az alkalmazni tervezett jogkövetkezmény hatékonyságát, arányosságát és visszatartó erejét.
(2) Súlyos jogsértésnek minősülnek:
a) az ismételt jogsértések;
b) a jelentős események bejelentésének vagy orvoslásának elmaradása;
c) a hiányosságok orvoslásának elmaradása az illetékes hatóságok kötelező erejű utasításait követően;
d) a jogsértés megállapítását követően az illetékes hatóság által elrendelt ellenőrzések vagy ellenőrzési tevékenységek akadályozása;
e) a hamis vagy súlyosan pontatlan információk közlése.

39. §

(1) A Kiberbiztonsági tv. 1. § (1) bekezdés b) pontja hatálya alá tartozó, és egyidejűleg a Kiberbiztonsági tv. 2. és 3. melléklete szerinti szervezetnek minősülő szervezet esetében a Kiberbiztonsági tv. 7. §-a, 8. § (5) bekezdése és 16. §-a szerinti rendelkezések nemteljesítése vagy nem határidőben történő teljesítése esetén az SZTFH megkeresheti a nemzeti kiberbiztonsági hatóságot a felügyeleti intézkedések megtétele érdekében.
(2) A nemzeti kiberbiztonsági hatóság tájékoztatja
a) a Kszetv. szerinti kijelölő hatóságot vagy
b) a Vbö. szerinti kijelölő hatóságot,
ha a felügyeleti jogkörükbe tartozó szervezetet érintő intézkedések megtételére, illetve jogkövetkezmények alkalmazására kerül sor.

(3) A nemzeti kiberbiztonsági hatóság indokolatlan késedelem nélkül tájékoztatja a Nemzeti Adatvédelmi és Információszabadság Hatóságot, amennyiben a feladatellátása során a szervezet általi olyan jogsértésről szerez tudomást, amely személyes adatok sérelmével járt, illetve járhat a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) szóló, 2016. április 27-i (EU) 2016/679 európai parlamenti és tanácsi rendelet [a továbbiakban: (EU) 2016/679 európai parlamenti és tanácsi rendelet] 4. cikk 12. pontjában meghatározottak szerint és az adatvédelmi incidenst a szervezet nem jelentette be a Nemzeti Adatvédelmi és Információszabadság Hatóságnak.
(4) Ha az (EU) 2016/679 európai parlamenti és tanácsi rendelet alapján illetékes felügyeleti hatóság más uniós tagállamban található, a nemzeti kiberbiztonsági hatóság tájékoztatja a Nemzeti Adatvédelmi és Információszabadság Hatóságot a személyes adatok (3) bekezdésben említett potenciális sérelméről.
(5) Ha a Nemzeti Adatvédelmi és Információszabadság Hatóság a jogsértésért bírságot szab ki, az ugyanazon magatartásból eredő jogsértésért a nemzeti kiberbiztonsági hatóság nem szab ki bírságot, azonban indokolt esetben más jogkövetkezményt alkalmazhat.

20. Az információbiztonsági felügyelő

40. §

(1) A szervezethez kirendelésre kerülő információbiztonsági felügyelőt a nemzeti kiberbiztonsági hatóság pártatlan, objektív eljárás keretében választja ki.
(2) Az információbiztonsági felügyelő – ha a kirendelés indokai ezt lehetővé teszik – egyidejűleg több érintett szervezethez is kirendelhető.
(3) Határozott időtartamú kirendelés esetén a kirendelés meghosszabbítására a kirendelés idejének lejárta előtt, legfeljebb egy alkalommal kerülhet sor, a folyamatban lévő intézkedések lezárásáig. A kirendelés időtartamának meghatározásakor figyelemmel kell lenni az érintett szervezet kötelezettségszegésének súlyára és a fenyegetés elhárításához szükséges védelmi intézkedésekre.
(4) A kirendelésről szóló határozat tartalmazza a kirendelés célját, tárgyát, az információbiztonsági felügyelő személyazonosításához szükséges adatokat, a kirendelésre okot adó körülményeket, a jogszabályi hivatkozást, a kirendelés időtartamát, a tevékenység ellátásának módjára és rendszerességére vonatkozó adatokat, az információbiztonsági felügyelő díjának mértékét.
(5) Az információbiztonsági felügyelő a nemzeti kiberbiztonsági hatóság és az érintett szervezet bevonásával a nemzeti kiberbiztonsági hatóság által meghatározott határidőn belül intézkedési tervet készít a nemzeti kiberbiztonsági hatóság által megjelölt hiányosságok felszámolása érdekében. Az információbiztonsági felügyelő a hatóság által jóváhagyott intézkedési terv alapján jár el.
(6) Információbiztonsági felügyelőnek nem rendelhető ki az a személy, aki

a) az érintett szervezettel munkavégzésre irányuló jogviszonyban áll,
b) a kirendelést megelőző három évben az érintett szervezettel munkavégzésre irányuló jogviszonyban állt,
c) a kirendeléskor, vagy a kirendelést megelőző három évben az érintett szervezetnél rendszeres és tartós megbízási vagy vállalkozási jogviszonyban áll vagy állt,
d) az érintett szervezet vezetőjének, gazdasági vezetőjének vagy alkalmazottjának hozzátartozója e minőségének fennállása alatt, és annak megszűnésétől számított három évig,
e) az érintett szervezet képviselője, e minőségének fennállása alatt és annak megszűnésétől számított három évig, valamint
f) az, akitől az adott helyzet tárgyilagos megítélése üzleti érdekeltségből vagy egyéb okból nem elvárható (elfogultság).

41. §

(1) Az információbiztonsági felügyelő jogosult a jogszabályokban foglalt biztonsági követelmények és az ehhez kapcsolódó eljárási szabályok betartásával, teljesítésével összefüggésben

a) az érintett szervezet vezetőitől és bármely dolgozójától írásbeli és szóbeli tájékoztatást, adatszolgáltatást kérni,

b) az érintett szervezet információtechnológiával kapcsolatos valamennyi dokumentumába, okiratába betekinteni, arról másolatot, kivonatot készíttetni,

c) az érintett szervezet valamennyi információtechnológiával kapcsolatos helyiségébe belépni,

d) azonnali intézkedést javasolni az érintett szervezet vezetőjének a közvetlen fenyegetés elhárításához (működés korlátozása, leállítása),

e) intézkedést javasolni a jogszabályszerű működés kialakításához vagy helyreállításához, ennek keretében az érintett szabályzatok felülvizsgálatát kezdeményezni,

f) előzetesen véleményezni a működéssel kapcsolatos elektronikus információbiztonságot is érintő intézkedéseket, valamint

g) kifogással élni az érintett szervezet által megtett vagy elmulasztott intézkedései, döntései tekintetében.

(2) Az információbiztonsági felügyelő pénzügyi kötelezettségvállalásra nem jogosult.

(3) Az információbiztonsági felügyelő köteles

a) az érintett szervezetnél megbízólevelét bemutatni,

b) figyelemmel kísérni megbízatásának időpontjától kezdve az érintett szervezetnél a jogszabályokban foglalt biztonsági követelmények és eljárások megvalósulását, a jogszabályokban előírt feladatok ellátását,

c) feltárni azokat az okokat, amelyek a kötelezettség nem teljesítéséhez vagy a fenyegetés kialakulásához vezettek,

d) a c) pontban foglaltak és az érintett szervezet működésének ismert feltételei alapján a szükséges intézkedések végrehajtására irányuló intézkedési tervet készíteni,

e) azonnali intézkedéseket kezdeményezni úgy, hogy azok bevezetése nem lehetetleníti el az alaptevékenység ellátását, valamint azokról haladéktalanul értesíteni a nemzeti kiberbiztonsági hatóságot,

f) betartani a titoktartási kötelezettségre vonatkozó szabályokat,

g) a hatóságnak – a szervezettel való előzetes konzultációt követően – az intézkedési tervben megjelölt gyakorisággal beszámolni, a beszámolóban számot adni a megtett intézkedésekről, a biztonsági követelmények teljesüléséről, az elektronikus információbiztonság fejlődéséhez szükséges további intézkedésekről, valamint

h) a megbízatásának megszűnésekor összefoglaló beszámolót készíteni a működéséről, ideértve a megtett intézkedéseket és azok eredményét, és a javasolt további intézkedéseket, amelynek jóváhagyásáról a nemzeti kiberbiztonsági hatóság dönt.

(4) A szervezet vezetője, az elektronikus információs rendszer biztonságáért felelős személy, valamint a szervezet munkatársai kötelesek az információbiztonsági felügyelővel együttműködni, részére a szükséges információkat megadni, dokumentumokat átadni.

(5) A nemzeti kiberbiztonsági hatóság az információbiztonsági felügyelő alkalmazásának indokoltságát felülvizsgálhatja.

(6) Az információbiztonsági felügyelő kirendelésének megszűnésére a megbízólevélben meghatározott időtartam letelte előtt akkor kerülhet sor, ha

a) a kirendelés oka elhárult és az információbiztonsági felügyelő összefoglaló beszámolóját a nemzeti kiberbiztonsági hatóság jóváhagyta, vagy

b) az információbiztonsági felügyelőt a nemzeti kiberbiztonsági hatóság visszahívja.

(7) Az információbiztonsági felügyelőt a nemzeti kiberbiztonsági hatóság visszahívja, ha

a) megállapítja, hogy az érintett szervezetnél az információbiztonsági felügyelőnek felróhatóan nem érvényesülnek a biztonsági követelmények, vagy
b) kizárásra okot adó körülmény merült fel, vagy a kirendeléskor fennálló, kizárásra okot adó körülmény a nemzeti kiberbiztonsági hatóság tudomására jut.

(8) A (7) bekezdésben meghatározott esetben a nemzeti kiberbiztonsági hatóság jogosult új információbiztonsági felügyelőt kirendelni.

(9) Az információbiztonsági felügyelő kirendelésének megszűnéséről a nemzeti kiberbiztonsági hatóság írásban haladéktalanul tájékoztatja az érintett szervezet vezetőjét.

(10) Az információbiztonsági felügyelő tevékenységének ellátásáért – a mindenkori minimálbér hétszerese szerinti havi díjazást alapul véve – a kirendelésben meghatározott időtartammal arányos mértékű díjazásra, valamint igazolt költségeinek megtérítésére jogosult.

(11) Az információbiztonsági felügyelő díját és igazolt költségeit az érintett szervezet viseli.

21. Kiberbiztonsági bírság

42. §

(1) A Kiberbiztonsági tv. 30. § (2) bekezdése alapján
a) a nemzeti kiberbiztonsági hatóság a Kiberbiztonsági tv. 1. § (1) bekezdés a)-c) pontja szerinti szervezettel szemben a 2. mellékletben,
b) a Szabályozott Tevékenységek Felügyeleti Hatósága (a továbbiakban: SZTFH) a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti szervezettel szemben a 3. mellékletben

meghatározott mértékű kiberbiztonsági bírságot szabhat ki.

(2) Az (1) bekezdés alapján kiszabható bírság legmagasabb összege:
a) ha a szervezet alapvető szervezetnek minősül 10 millió eurónak megfelelő forintösszeg vagy, ha ez magasabb a szervezet előző pénzügyi évi globális éves forgalma teljes összege 2%-ának megfelelő összeg,
b) ha a szervezet fontos szervezetnek minősül 7 millió eurónak megfelelő forintösszeg vagy, ha ez magasabb a szervezet előző pénzügyi évi globális éves forgalma teljes összege 1,4%-ának megfelelő összeg.

(3) Az (1) és (2) bekezdés alapján kiszabható legmagasabb bírság forintösszegének meghatározásánál a bírság kiszabásáról szóló határozat meghozatala napján a Magyar Nemzeti Bank által közzétett euró-árfolyamot kell alapul venni.

(4) Ha a szervezet vezetője a jogszabályban előírt kötelezettségének nem tesz eleget, a nemzeti kiberbiztonsági hatóság 15 millió forintig terjedő bírsággal sújthatja, illetve ismételt jogsértés esetén sújtja.

43. §

Az Ekertv. 15/B. § (4) bekezdése alapján a közvetítő szolgáltatóval szemben a kiberbiztonsági incidensek kezelésével és kivizsgálásával kapcsolatosan az e rendeletben meghatározott feladatainak nem teljesítése esetén a nemzeti kiberbiztonsági hatóság 15 millió forintig terjedő kiberbiztonsági bírságot szabhat ki.

44. §

(1) A bírságot a kiberbiztonsági hatóság határozatának véglegessé válását követő 8 napon belül kell befizetni a kiberbiztonsági hatóság határozatban megjelölt, Magyar Államkincstárnál vezetett számlájára.

(2) A befizetés során az átutalás közlemény rovatában fel kell tüntetni a „kiberbiztonsági bírság” szöveget és a bírságot megállapító határozat számát.
(3) Több jogszabálysértés együttes fennállása esetén a bírság kiszabható legnagyobb mértéke az egyes jogszabálysértésekért kiszabható bírságok legnagyobb mértékének összege.
(4) A bírság megfizetése nem mentesít a büntetőjogi, valamint a polgári jogi felelősség, valamint a bírság kiszabására okot adó körülmény megszüntetésének kötelezettsége alól.
(5) A bírság ugyanazon tényállás mellett – az azonnal megszüntethető jogszabálysértések kivételével – a bírságot kiszabó végleges határozat közlését követő két hónap elteltével szabható ki ismételten.

IV. Fejezet

Kiberbiztonsági tanúsítás

22. A kiberbiztonsági tanúsító hatósági tevékenységre vonatkozó egyes rendelkezések

45. §

A Kormány a hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsító hatósági feladatok tekintetében a Kiberbiztonsági tv. 45. § (1) bekezdés b) pontja szerinti tanúsító hatóságként a honvédelemért felelős minisztert jelöli ki.

46. §

(1) A kiberbiztonsági tanúsító hatóság feladatait a Kiberbiztonsági tv. 45. § (1) bekezdés a) pontja alapján ellátó SZTFH, valamint a hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsító hatósági feladatok tekintetében a Kiberbiztonsági tv. 45. § (1) bekezdés b) pontja szerint kijelölt hatóság (a továbbiakban együtt: tanúsító hatóság) a Kiberbiztonsági tv. 49. § (2) bekezdése alapján az európai uniós jogi aktusok és a magyar jogszabályok megsértése (a továbbiakban: szabálytalanság) miatt a 4. mellékletben meghatározott mértékű bírságot szab ki.
(2) A kiszabott bírságot a tanúsító hatóság határozatának véglegessé válását követő 8 napon belül kell megfizetni a tanúsító hatóság határozatban megjelölt, Magyar Államkincstárnál vezetett számlájára.
(3) Több szabálytalanság együttes fennállása esetén a bírság kiszabható legnagyobb mértéke az egyes szabálytalanságokért kiszabható bírságok legnagyobb mértékének összege.
(4) A tanúsító hatóság a bírságot ugyanazon tényállás mellett a Kiberbiztonsági tv. 49. § (1) bekezdése alapján meghatározott határidő eredménytelen elteltét követően ismételten kiszabhatja.

47. §

Az IKT-termék biztonságát érintő sebezhetőségről vagy rendellenességről szóló tájékoztatást a tanúsító hatóság továbbítja a Központ részére.

V. Fejezet

Sérülékenységvizsgálat

23. A sérülékenységvizsgálatra vonatkozó általános rendelkezések

48. §

(1) A Kormány a Kiberbiztonsági tv. 57. § (1) bekezdés a) pontja szerinti állami szervként a Nemzetbiztonsági Szakszolgálatot jelöli ki (a továbbiakban: sérülékenységvizsgálat végzésére jogosult állami szerv).
(2) A honvédelmi célú elektronikus információs rendszerek vonatkozásában a sérülékenységvizsgálat lefolytatására a Katonai Nemzetbiztonsági Szolgálat jogosult.
(3) A Katonai Nemzetbiztonsági Szolgálat sérülékenységvizsgálati tevékenységére a sérülékenységvizsgálat végzésére jogosult állami szervre vonatkozó rendelkezéseket kell alkalmazni.
(4) A Kiberbiztonsági tv. 57. § (1) bekezdés c) pontja szerinti gazdálkodó szervezet által végzett sérülékenységvizsgálat során az e fejezetben foglaltak alkalmazandók.

49. §

(1) A sérülékenységvizsgálat célja a szervezet elektronikus információs rendszere, rendszerelemei gyenge pontjainak feltárása, valamint a feltárt sérülékenységek elhárítására vonatkozó megoldási javaslatok kidolgozása az elektronikus információs rendszerek, rendszerelemek védelmének és biztonságának megerősítése érdekében.
(2) A sérülékenységvizsgálat tárgya az adatok, információk kezelésére használt elektronikus információs rendszerek, rendszerelemek, eszközök, eljárások és kapcsolódó folyamatok vizsgálata, valamint az ezeket kezelő személyek és a szervezet általános informatikai felkészültségének vizsgálata.

24. Vizsgálati módszerek

50. §

(1) Teljeskörű sérülékenységvizsgálat során a sérülékenységvizsgálati eljárást megalapozó alapdokumentumban meghatározottak szerint az alábbi vizsgálatok elvégzésére kerül sor:
a) külső informatikai biztonsági vizsgálat,
b) belső informatikai biztonsági vizsgálat,
c) alkalmazásvizsgálat,
d) vezeték nélküli hálózat informatikai biztonsági vizsgálata, vagy
e) kiber-fizikai rendszerek biztonsági vizsgálata.
(2) A sérülékenységvizsgálat az (1) bekezdésben 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.

51. §

(1) Teljeskörűnek nem minősülő sérülékenységvizsgálati módszerek:
a) automatizált sérülékenységfelderítés és -elemzés,
b) pszichológiai manipulációs vizsgálat,
c) behatolásvizsgálat,
d) kriptográfiai megfelelőségvizsgálat és
e) forráskódvizsgálat.
(2) Az (1) bekezdés szerinti sérülékenységvizsgálati módszerek a teljeskörű sérülékenységvizsgálat részét képezhetik, alkalmazásuk azonban nem váltja ki a teljeskörű sérülékenységvizsgálatot.

52. §

(1) A sérülékenységvizsgálat végzésére jogosult állami szerv által elvégzett sérülékenységvizsgálat határideje a sérülékenységvizsgálati alapdokumentumban vagy a nemzeti kiberbiztonsági hatóság határozatában meghatározott időponttól számítva legfeljebb 90 nap.
(2) Ha a szervezet elektronikus információs rendszere, rendszereleme az átlagostól jelentősen eltér, és emiatt egyedi sérülékenységvizsgálati eljárás szükséges, a sérülékenységvizsgálati határidő legfeljebb 120 nap lehet.
(3) A sérülékenységvizsgálat végzésére jogosult állami szerv a sérülékenységvizsgálatra irányadó határidőt, annak letelte előtt egy alkalommal legfeljebb 30 nappal meghosszabbíthatja, és erről értesíti a szervezetet, valamint a nemzeti kiberbiztonsági hatóságot.
(4) A szervezet elektronikus információs rendszere az átlagostól jelentősen eltér, ha
a) az elektronikus információs rendszer
aa) a külső internetes tartományban több mint 10 IP címmel,
ab) több mint 10 webszolgáltatással, vagy
ac) a belső hálózat tekintetében több mint 50 szerverrel, vagy
ad) több mint 500 munkaállomással, vagy
ae) több mint 5 vezeték nélküli hálózattal vagy
af) több mint 500 fős felhasználói létszámmal
rendelkezik,
b) a szervezet több, mint három telephelyen rendelkezik a vizsgálattal érintett elektronikus információs rendszerrel, vagy
c) a szervezet a sérülékenységvizsgálatot indító alapdokumentumban erre vonatkozóan nyilatkozik és ezzel a sérülékenységvizsgálat végzésére jogosult állami szerv egyetért.

25. A sérülékenységvizsgálat lefolytatása

53. §

(1) A sérülékenységvizsgálat előkészítése során a sérülékenységvizsgálat végzésére jogosult állami szerv, valamint a Kiberbiztonsági tv. 57. § (1) bekezdés c) pontja szerinti, sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezet (a továbbiakban együtt: sérülékenységvizsgálatot végző szerv) sérülékenységvizsgálati alapdokumentumot készít.
(2) A sérülékenységvizsgálati alapdokumentumban rögzíteni kell legalább
1. a sérülékenységvizsgálatot végző szervezet megnevezését,
2. gazdálkodó szervezet esetében a sérülékenységvizsgálatot végző személy nevét,
3. az érintett elektronikus információs rendszer felett rendelkezési joggal rendelkező szervezetet,
4. az érintett elektronikus információs rendszer megnevezését, továbbá az érintett rendszerelemeket és alkalmazásokat,
5. az elektronikus információs rendszer adatkezelőjét,
6. a vizsgálat tárgyát,
7. a vizsgálati feladatokat, célokat,
8. a sérülékenységvizsgálati módszert,
9. a sérülékenységvizsgálat jogosultsági fázisát,
10. a sérülékenységvizsgálati és kockázatértékelési módszertant,
11. a sérülékenységvizsgálat lefolytatásához szükséges feltételeket és azok biztosításának módját,
12. a sérülékenységvizsgálat időtartamát, végrehajtásának ütemtervét,
13. a sérülékenységvizsgálat szüneteltetésére, megszüntetésére okot adó körülményeket, valamint
14. a szervezet vezetőjének vagy az általa meghatalmazott, döntési jogosultsággal rendelkező személy aláírását.

(3) Ha a sérülékenységvizsgálatot a nemzeti kiberbiztonsági hatóság rendeli el, a sérülékenységvizsgálati alapdokumentumban a hatósági döntésben rögzített vizsgálati feladatokat is rögzíteni kell, valamint nem kell feltüntetni a (2) bekezdés 14. pontjában foglaltakat.
(4) Ha a sérülékenységvizsgálatot a sérülékenységvizsgálat végzésére jogosult állami szerv indítja, nem kell feltüntetni a (2) bekezdés 14. pontjában foglaltakat.

54. §

(1) A sérülékenységvizsgálat szervezet általi kezdeményezése esetén a vizsgálati feladatokra a szervezet javaslatot tehet, amelyről a sérülékenységvizsgálatot végző szerv dönt.
(2) A sérülékenységvizsgálati alapdokumentumot a sérülékenységvizsgálatot végző szerv – legalább a sérülékenységvizsgálat megkezdését megelőzően 8 nappal – megküldi az érintett szervezet részére. Az érintett szervezet a sérülékenységvizsgálati alapdokumentum tartalmára a kézhezvételtől számított 5 napon belül észrevételt tehet. Az észrevétel nem érintheti a nemzeti kiberbiztonsági hatóság által elrendelt vizsgálatokat. Az észrevételekről a sérülékenységvizsgálatot végző szerv dönt.

55. §

(1) Ha a sérülékenységvizsgálati alapdokumentum aláírását követően a sérülékenységvizsgálati alapdokumentumban rögzítettekben változás következik be, a sérülékenységvizsgálatot végző szerv – a változás jelentőségének, súlyának figyelembevételével – az érintett elektronikus információs rendszer felett rendelkezési joggal rendelkező szervezettel folytatott egyeztetés alapján
a) kezdeményezheti a sérülékenységvizsgálati alapdokumentum módosítását,
b) módosíthatja a sérülékenységvizsgálat záró dátumát,
c) szüneteltetheti a sérülékenységvizsgálat végrehajtását,
d) megszüntetheti a sérülékenységvizsgálatot vagy
e) állásfoglalás kiadásával lezárhatja a sérülékenységvizsgálatot.
(2) A sérülékenységvizsgálati alapdokumentum aláírását követően a sérülékenységvizsgálati módszerben vagy módszertanban történő módosítási igény esetén a sérülékenységvizsgálatot végző szerv megszünteti vagy az aláírt sérülékenységvizsgálati alapdokumentumban foglaltak szerint lezárja a sérülékenységvizsgálatot.
(3) Ha a sérülékenységvizsgálati alapdokumentumban, valamint az e rendeletben foglalt feltételek hiánytalanul nem állnak rendelkezésre, a sérülékenységvizsgálat nem hajtható végre vagy a végrehajtását fel kell függeszteni.

56. §

(1) A sérülékenységvizsgálatot végző szerv a sérülékenységvizsgálat során kellő gondossággal eljárva köteles a vizsgált elektronikus információs rendszer által nyújtott szolgáltatásoknak a feltétlenül szükségesnél nem nagyobb mértékű korlátozására, a sérülékenységvizsgálatnak a szolgáltatás szempontjából nem kritikus időszakban történő elvégzésére. A sérülékenységvizsgálatot végző szerv köteles a korlátozás várható mértékéről és időtartalmáról az érintett szervezetet előzetesen tájékoztatni.
(2) A sérülékenységvizsgálatot végző szerv tájékoztatja a sérülékenységvizsgálattal érintett szervezetet az általa a vizsgálathoz használt IP címről vagy más egyedi technikai azonosítóról, amelyet a szervezet a vizsgálat időtartama alatt nem tilthat ki a szolgáltatás eléréséből, illetve gondoskodnia kell a szolgáltatásnak a sérülékenységvizsgálatot végző szerv általi eléréséről.
(3) A sérülékenységvizsgálatot végző szerv a polgári hírszerző tevékenységet végző nemzetbiztonsági szolgálat elektronikus információs rendszerei vonatkozásában lehetőség szerint gondoskodik arról, hogy az azokon tárolt adatok megismerése nélkül hajtsa végre a sérülékenységvizsgálatot.

57. §

A gazdálkodó szervezet által végzendő sérülékenységvizsgálat megkezdését a szervezet bejelenti a sérülékenységvizsgálat végzésére jogosult állami szerv részére.

58. §

(1) A szervezet köteles – a sérülékenységvizsgálati alapdokumentumban vagy a sérülékenységvizsgálat végzésére jogosult állami szerv általi elrendelés esetén az elrendelésben foglaltak szerint – a sérülékenységvizsgálat lefolytatásához szükséges adatokat, dokumentumokat, eszközöket és egyéb információkat a sérülékenységvizsgálatot végző szerv rendelkezésére bocsátani, valamint tűrni a sérülékenységvizsgálatból fakadó, a vizsgált elektronikus információs rendszeren bekövetkezett szolgáltatáscsökkenést, illetve -kiesést.
(2) Regisztrált felhasználói jogosultság nélküli vizsgálat esetén az érintett szervezet
a) megküldi a sérülékenységvizsgálatot végző szerv részére a vizsgálandó elektronikus információs rendszer, illetve szolgáltatás hozzáférési pontjaihoz tartozó adatokat, biztosítja – korlátozott hozzáférésű rendszer esetében is – a hozzáférési pontok fizikai és logikai elérésének lehetőségét,
b) biztosítja a sérülékenységvizsgálatot végző szerv számára a vizsgálandó elektronikus információs rendszer, illetve szolgáltatás monitorozását.
(3) Regisztrált felhasználói jogosultsággal rendelkező vizsgálat esetén az (1) bekezdésben meghatározottakon túl az érintett szervezet a sérülékenységvizsgálatot végző szerv részére megküldi
a) a felhasználói jogosultság mátrixot, valamint
b) a felhasználói dokumentációt.
(4) Adminisztrátori jogosultsággal rendelkező vizsgálat esetén a szervezet megküldi a sérülékenységvizsgálatot végző szerv részére a (2) és (3) bekezdésben foglaltakon túl a rendszertervet is.
(5) A szervezet a sérülékenységvizsgálati alapdokumentum elkészítését megelőzően legalább 8 nappal a sérülékenységvizsgálatot végző szerv részére jelzi azon időszakokat, amelyek a szervezet által nyújtott szolgáltatások vagy működése szempontjából nem megfelelőek a sérülékenységvizsgálat elvégzésére. A megjelölt időszakok nem tartoznak bele a sérülékenységvizsgálat e rendeletben meghatározott időtartamába.
(6) A sérülékenységvizsgálat alatt a szolgáltatások elérhetőségében bekövetkező változás esetén a bejelentést haladéktalanul, legkésőbb 3 napon belül meg kell tenni.
(7) Ha a szervezet nem vagy hibásan adja meg a sérülékenységvizsgálat elvégzéséhez szükséges adatokat, a sérülékenységvizsgálat végzésére jogosult állami szerv nem végzi el vizsgálatot vagy – a sérülékenységvizsgálat végzésére jogosult állami szerv vagy a nemzeti kiberbiztonsági hatóság által elrendelt sérülékenységvizsgálat esetén – kezdeményezi a nemzeti kiberbiztonsági hatóságnál a szervezet kötelezését az együttműködésre és az adatszolgáltatásra.
(8) A honvédelmi célú elektronikus információs rendszerek esetén a (2)–(6) bekezdésben meghatározott adatokat a honvédelmi kiberbiztonsági incidenskezelő központnak kell bejelenteni.

59. §

(1) A szervezet köteles a sérülékenységvizsgálattal érintett elektronikus információs rendszer működésében érintett valamennyi szervezetet írásban tájékoztatni a tervezett sérülékenységvizsgálatról, valamint a tájékoztatásban foglaltakban bekövetkezett változásokról.
(2) A tájékoztatásnak tartalmaznia kell
a) a sérülékenységvizsgálat végzésének tényét,
b) az érintett elektronikus információs rendszert,
c) amennyiben ismert, a sérülékenységvizsgálat tervezett kezdetét, időtartamát,

d) annak tényét, hogy az érintett elektronikus információs rendszer által nyújtott szolgáltatásban szolgáltatáskiesés, -csökkenés várható,
e) az elektronikus információs rendszer adatkezelője vonatkozásában az érintett elektronikus információs rendszerben tárolt vagy kezelt adatok megismerhetőségéhez és a sérülékenységvizsgálat elvégzéséhez való hozzájárulásra irányuló kérést, illetve
f) az elektronikus információs rendszer üzemeltetésében érintett szervezet vonatkozásában a sérülékenységvizsgálat elvégzésének tudomásul vételére irányuló kérést.

(3) A sérülékenységvizsgálattal érintett elektronikus információs rendszer
a) adatkezelője a sérülékenységvizsgálathoz való hozzájárulásról,
b) üzemeltetésében érintett szervezet a tájékoztatás tudomásul vételéről
írásban nyilatkozik.

(4) A nemzeti kiberbiztonsági hatóság kérésére a szervezet bemutatja a tájékoztatást, valamint a hozzájárulásról vagy a tudomásul vételről szóló nyilatkozatot.

60. §

(1) A sérülékenységvizsgálattal érintett elektronikus információs rendszer üzemeltetésében érintett szervezet a sérülékenységvizsgálatot nem akadályozhatja és köteles a sérülékenységvizsgálat lefolytatásához szükséges megfelelő hozzáféréseket biztosítani.

(2) Ha a sérülékenységvizsgálattal érintett elektronikus információs rendszer működésében érintett szervezet a sérülékenységvizsgálat elvégzését akadályozza, a sérülékenységvizsgálattal érintett elektronikus információs rendszer felett rendelkezési jogot gyakorló szervezet értesíti a nemzeti kiberbiztonsági hatóságot – honvédelmi célú elektronikus információs rendszer vonatkozásában a honvédelmi kiberbiztonsági hatóságot –, amely indokolt esetben kötelezheti az akadályozó szervezetet a sérülékenységvizsgálat tudomásul vételére és az akadályozó körülmény megszüntetésére. Hatáskör hiányában a nemzeti kiberbiztonsági hatóság kezdeményezheti az arra jogosult hatóság intézkedését a kötelezés érdekében.

61. §

A sérülékenységvizsgálat nemzetközileg elfogadott sérülékenységvizsgálati és kockázatértékelési módszertanok mentén folytatható. A sérülékenységvizsgálat során kizárólag olyan kockázatértékelési módszertan alkalmazható, amely figyelembe veszi legalább a sérülékenység hatásának mértékét, valamint a kihasználásának komplexitását.

62. §

(1) A sérülékenységvizsgálat lezárásakor a sérülékenységvizsgálatot végző szerv az általa készített állásfoglalást 8 napon belül – amennyiben az érintett szervezet elektronikus információs rendszere az átlagostól jelentősen eltér, úgy 21 napon belül – megküldi az érintett szervezet és a nemzeti kiberbiztonsági hatóság – honvédelmi célú elektronikus információs rendszer vonatkozásában a honvédelmi kiberbiztonsági hatóság – részére.

(2) Az állásfoglalásban fel kell tüntetni legalább az alábbiakat:
1. a sérülékenységvizsgálatot végző szerv megnevezését,
2. az érintett elektronikus információs rendszer felett rendelkezési joggal rendelkező szervezet megnevezését,
3. az érintett elektronikus információs rendszer megnevezését, továbbá az érintett rendszerelemeket és alkalmazásokat,
4. a sérülékenységvizsgálat időpontját, időtartamát,
5. a sérülékenységvizsgálat tárgyát,

6. a vizsgálati feladatokat, célokat,
7. az alkalmazott sérülékenységvizsgálati módszert,
8. a felhasznált sérülékenységvizsgálati és kockázatértékelési módszertant,
9. a vizsgálati eredmények leírását,
10. amennyiben az alkalmazott sérülékenységvizsgálati módszertan esetében értelmezhető, valamennyi vizsgált kockázatot, függetlenül attól, hogy adott rendszer a sérülékenységet tartalmazza-e vagy nem,
11. a sérülékenység megnevezését,
12. a sérülékenység leírását,
13. a sérülékenység kockázati besorolását,
14. a hatás besorolását és leírását,
15. a sérülékenység kihasználása komplexitásának besorolását és leírását,
16. lehetőség szerint a sérülékenység feltárásának részletes leírását,
17. a sérülékenység javítására tett javaslatot,
18. a rövid, közép- és hosszú távú intézkedésekre vonatkozó intézkedési javaslatokat,
19. utóvizsgálat lefolytatásának szükségességére irányuló javaslatot,
20. gazdálkodó szervezet esetében a sérülékenységvizsgálatot végző személy nevét, valamint
21. a sérülékenységvizsgálatot végző szerv aláírását.

(3) Az állásfoglalás tervezetét a sérülékenységvizsgálatot végző szerv megküldi a szervezet részére véleményezésre, amelyre egy ízben, 8 napon belül, a szervezet vezetője észrevételt tehet. Ebben javaslatot tehet a kockázat felülvizsgálatára és legfeljebb egy szintet módosíthat a kockázati besoroláson. A vélemény elfogadásáról a sérülékenységvizsgálatot végző szerv dönt.

(4) A kiberbiztonsági auditjelentésben foglaltakat a nemzeti kiberbiztonsági hatóság abban az esetben fogadja el a (2) bekezdés szerinti sérülékenységvizsgálati állásfoglalással azonos értékűnek, ha az tartalmazza (2) bekezdésben meghatározott szempontokat és információkat.

(5) A honvédelmi célú elektronikus információs rendszerek vonatkozásában lefolytatott sérülékenységvizsgálat állásfoglalás tervezetét az érintett szervezet a szakmai irányítását ellátó szervvel vagy a tulajdonosi joggyakorlóval is megosztja.

63. §

(1) Ha a sérülékenységvizsgálat során alkalmazott módszertan szerint kritikus vagy magas besorolásúnak minősülő sérülékenység kerül feltárásra, a szervezet köteles intézkedni a feltárt sérülékenységek kijavítása, kezelése vagy kockázatcsökkentő intézkedések megtétele érdekében

a) új elektronikus információs rendszer esetében a rendszer használatba vételéig,
b) egyéb esetben az állásfoglalás kézhezvételét követően haladéktalanul, de legkésőbb 30 napon belül.

(2) Az (1) bekezdés b) pontja esetében a szervezet – a sérülékenységvizsgálatot végző szervezettel, valamint a nemzeti kiberbiztonsági hatósággal való egyeztetést követően – mérlegeli az elektronikus információs rendszer használata felfüggesztésének szükségességét.

(3) A sérülékenységvizsgálat során alkalmazott módszertan szerint alacsony besorolásúnak minősülő sérülékenységek indokolási kötelezettség nélkül felvállalhatók.

(4) Az érintett szervezet az állásfoglalás kézhezvételét követő 30 napon belül sérülékenységkezelési tervet készít és megküldi a nemzeti kiberbiztonsági hatóság részére, amely továbbítja a sérülékenységvizsgálat végzésére jogosult állami szerv részére.

(5) A sérülékenységkezelési terv tartalmazza a sérülékenységvizsgálat során feltárt sérülékenységet, a sérülékenységkezelési intézkedéseket és feladatokat, a feladatok teljesítésének mérföldköveit, a kapcsolódó végrehajtási határidőket, a javítás technikai részleteit és azok rendszerre gyakorolt hatását, valamint az ehhez szükséges erőforrásokat.

26. Az utóvizsgálat

64. §

(1) Ha a sérülékenységvizsgálatot végző szerv az állásfoglalásban javaslatot tesz utóvizsgálat lefolytatására, a sérülékenységek megszüntetésére vonatkozó sérülékenységkezelési tervre irányuló döntésében a nemzeti kiberbiztonsági hatóság nyilatkozik, kötelezi-e utóvizsgálat elvégzésére a szervezetet.
(2) Ha az állásfoglalás kritikus vagy magas besorolású sérülékenységet állapít meg, utóvizsgálat lefolytatása kötelező.
(3) Kötelezően elvégzendő utóvizsgálat esetén a szervezet a nemzeti kiberbiztonsági hatóság által jóváhagyott sérülékenységkezelési tervben szereplő, utolsóként teljesítendő határidő leteltét követően kezdeményezi az utóvizsgálatot.
(4) A szervezet az utóvizsgálatot saját maga is kezdeményezheti, ez esetben a kezdeményezéssel egyidejűleg – amennyiben erre még a kezdeményezést megelőzően nem került sor – megküldi sérülékenységkezelési tervet a nemzeti kiberbiztonsági hatóság részére.
(5) Utóvizsgálat lefolytatására a sérülékenységkezelési terv kiberbiztonsági hatóság általi jóváhagyását követően vagy indokolt esetben a nemzeti kiberbiztonsági hatóság engedélyét követően kerülhet sor.
(6) Az utóvizsgálatról az utóvizsgálatot végző szerv utóvizsgálati állásfoglalást készít, amelyről tájékoztatja az érintett szervezetet és a nemzeti kiberbiztonsági hatóságot.
(7) Az utóvizsgálatra a sérülékenységvizsgálatra vonatkozó általános rendelkezések az irányadók.
(8) A honvédelmi célú elektronikus információs rendszerek vonatkozásában lefolytatott utóvizsgálati állásfoglalást az érintett szervezet a szakmai irányítását ellátó szervvel vagy a tulajdonosi joggyakorlóval is megosztja.

VI. Fejezet

A kiberbiztonsági incidensekkel kapcsolatos rendelkezések

27. A kiberbiztonsági incidenskezelő központok

65. §

(1) A Kormány a Kiberbiztonsági tv. 63. § (1) bekezdése szerinti nemzeti kiberbiztonsági incidenskezelő központként a Nemzetbiztonsági Szakszolgálatot jelöli ki.
(2) A Kormány a Kiberbiztonsági tv. 63. § (2) bekezdése szerinti honvédelmi kiberbiztonsági incidenskezelő központként a Katonai Nemzetbiztonsági Szolgálatot jelöli ki. A Katonai Nemzetbiztonsági Szolgálat a kiberbiztonsági incidensek és fenyegetések kezelését a szakmai irányítása és koordinálása alatt álló, szakfeladat szerint elkülönülő – a honvédelemért felelős miniszter irányítása, vezetése alatt álló szervnél, szervezetnél működő – incidenskezelő központokkal együtt látja el.

66. §

(1) Ágazaton belüli kiberbiztonsági incidenskezelő központként működhet az a szervezet, amely a Központ vagy más független szervezet vizsgálata és a Központ jóváhagyása alapján megfelel a Központ által meghatározott nemzetközi vagy európai uniós szabványokon alapuló feltételeknek.
(2) A vizsgálat alapján az ágazaton belüli kiberbiztonsági incidenskezelő központ, valamint a Központ együttműködési megállapodást köt, amelyben rögzítésre kerülnek az ágazaton belüli kiberbiztonsági incidenskezelő központ incidenskezelést érintő képességei, valamint a két szervezet közötti feladatelhatárolás és együttműködés szabályai.

(3) Az ágazaton belüli kiberbiztonsági incidenskezelő központot a Központtal kötött együttműködési megállapodásban meghatározott feladatai ellátása során – jogszabály vagy az együttműködési megállapodás eltérő rendelkezése hiányában – az adott feladat vonatkozásában a Központot megillető jogosultságok illetik meg.

67. §

(1) A Központ ellátja a következő feladatokat:

1. a kiberteret érintő fenyegetésekkel és a kiberbiztonsági incidensek megelőzésével kapcsolatos feladatkörében:

a) folyamatos adatgyűjtés mellett végzi a magyar kibertér rendszeres biztonsági helyzetértékelését, továbbá egységes módszertan szerint dinamikus kockázat- és eseményelemzést készít,

b) nyomon követi és elemzi a kiberfenyegetéseket, sérülékenységeket, kockázatokat és kiberbiztonsági incidenseket,

c) fogadja a kiberfenyegetettségekre és a kiberbiztonsági incidensekre vonatkozó hazai és nemzetközi bejelentéseket, feldolgozza a saját és a rendelkezésre álló egyéb forrásokból érkező fenyegetettségre és kiberbiztonsági incidensekre vonatkozó adatokat és értesíti az ügyfélkörébe tartozó érintetteket vagy értesíti és átadja az adatokat a hatáskörrel rendelkező incidenskezelő központnak,

d) folyamatosan működteti a kiberbiztonsággal kapcsolatos szolgáltatásait,

e) végzi a kormányrendelet szerinti korai figyelmeztető rendszer működtetését,

f) végzi az elosztott kormányzati csapdarendszer működtetését,

g) azonnali figyelmeztetéseket tesz közzé a kritikus hálózatbiztonsági fenyegetettségekről, gondoskodik ezek magyar nyelvű megjelenítéséről,

h) információkat cserélhetnek az alapvető és fontos szervezetekkel, valamint azok ágazati vagy ágazatközi csoportjaival;

2. a kiberbiztonsági incidenskezeléshez kapcsolódó feladatkörében:

a) fogadja, kezeli és koordinálja az elektronikus információs rendszereket érintő kiberbiztonsági incidensekre, fenyegetésekre, kiberbiztonsági incidens közeli helyzetekre vonatkozó bejelentéseket, tájékoztatásokat, riasztásokat,

b) fogadja és kezeli a magyar kiberteret érintő nemzetközi bejelentéseket,

c) végzi a kiberbiztonsági incidensek nemzeti szintű nyomon követését,

d) figyelemfelhívást, riasztást ad, figyelmeztetést ad ki, információt nyújt az érdekeltek számára kockázatokkal és a kiberbiztonsági incidensekkel kapcsolatosan,

e) figyelmeztetést adhat ki a felhasználók, a kiberbiztonsági incidenskezelő központok, a hatóságok, az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, az egyedüli kapcsolattartó pont felé,

f) kapcsolatot tart a szervezetekkel, szolgáltatókkal a bejelentett kiberbiztonsági incidensek kezelése érdekében, valamint megteszi és koordinálja az azok kezeléséhez szükséges intézkedéseket,

g) haladéktalanul értesíti a tudomására jutott kiberbiztonsági incidensekről az érintetteket, valamint az illetékes hatóságot,

h) segítséget nyújt az érintett szervezetek számára a kiberbiztonsági incidensek kezelése során,

i) nyilvántartja a hozzá beérkezett bejelentéseket, a megtett intézkedéseket és azok eredményét,

j) kivizsgálja, illetve támogatja a kiberbiztonsági incidensek, fenyegetések, kiberbiztonsági incidens közeli helyzetek kivizsgálását,

k) meghatározza a kiberbiztonsági incidensek és kockázatok kezelésére vonatkozó eljárásokat, valamint a kiberbiztonsági incidensek, kockázatok és információk osztályozására szolgáló eljárásokat és szabályokat,

l) jóváhagyja az ágazaton belüli incidenskezelő központ működését és működési rendjét,
m) biztosítja a folyamatos rendelkezésre állást;

3. kiberbiztonsági válsághelyzetek kezelését érintő feladatkörében:
a) ellátja – ha jogszabály eltérően nem rendelkezik – a kiberbiztonsági válsághelyzetek kezelése során az elektronikus információs rendszerek kiberbiztonságával és helyreállításával kapcsolatos feladatok koordinációját,
b) a 106. §-ban meghatározottak szerint képviseli Magyarországot az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatában (a továbbiakban: EU-CyCLONe) szervezetben,
c) részt vesz Magyarország Kiberválságkezelési Tervének kidolgozásában,
d) részt vesz az EU politikai szintű integrált válságelhárítási mechanizmus (a továbbiakban: IPCR) rendszerben;
e) a kiberbiztonsági válsághelyzet hatékony kezelése érdekében folyamatos kapcsolatot tart a nemzeti eseménykezelő központtal;

4. a sérülékenységeket, sebezhetőségeket érintő feladatkörében:
a) fogadja és koordinálja az elektronikus információs rendszereket érintő sérülékenységekkel, IKT-terméket érintő sebezhetőségekkel kapcsolatos bejelentéseket, tájékoztatásokat, korai előrejelzéseket, riasztásokat és tájékoztatást nyújt az érdekeltek számára,
b) honlapján közzéteszi a nemzetközileg publikált sérülékenységeket,
c) ellátja az európai uniós jogi aktusban meghatározott koordinátor CSIRT-feladatokat,
d) tájékoztatja az érdekelteket a sérülékenységekkel kapcsolatos információkról,
e) nyilvántartja a bejelentett sérülékenységeket, azokról szükség szerint tájékoztatja az ENISA-t,
f) részt vesz az (EU) 2019/881 európai parlamenti és tanácsi rendelet szerinti sebezhetőséggel kapcsolatos feladatok végrehajtásában;

5. tájékoztatási, tudatosító tevékenysége keretében:
a) elemzéseket, jelentéseket készít a hazai és nemzetközi információbiztonsági irányokról,
b) évente jelentést készít a tevékenységéről az informatikáért felelős miniszter, valamint kivonatolt formában a nyilvánosság részére,
c) a biztonságtudatos felhasználói magatartás elősegítése céljából oktatási anyagokat dolgoz ki és tréningeket tart, továbbá mind a hatáskörébe tartozó szervezetek, mind az állampolgárok részére felvilágosító, szemléletformáló kampányokat szervez,
d) részt vesz hazai és nemzetközi információbiztonsági és kibervédelmi gyakorlatokon, valamint ilyen gyakorlatokat tervezhet, szervezhet, és kötelezheti a szervezetet a gyakorlaton való részvételre,
e) az elektronikus információs rendszereket veszélyeztető sérülékenységekkel és fenyegető kockázatokkal összefüggésben tájékoztatja az elektronikus információs rendszerek biztonságáért felelős személyeket, az illetékes hatóságokat és a kiberbiztonsági incidenskezelő központokat,
f) rendszeres tájékoztatást nyújt a honlapján a sérülékenységekről és fenyegetésekről, valamint a javasolt biztonsági intézkedésekről,
g) részt vesz az információbiztonság tudatosításáért felelős intézmények tudatosítási programjában, szakértői-oktatói tevékenységet végezhet;

6. az európai uniós és nemzetközi együttműködés keretében:
a) fogadja és kezeli a magyar kiberteret érintő nemzetközi bejelentéseket,
b) képviseli Magyarországot a nemzetközi incidenskezelési együttműködésben,
c) részt vesz a CSIRT-hálózat tevékenységében,
d) kapacitásaiknak és hatásköreiknek megfelelően segítséget nyújt az (EU) 2022/2555 európai parlamenti és tanácsi irányelv 11. cikk (3) bekezdés f) pontja szerinti kölcsönös segítségnyújtás keretében a CSIRT-hálózat többi tagjának azok kérésére,

e) együttműködik harmadik országok nemzeti, számítógép-biztonsági eseményekre reagáló csoportjaival vagy azokkal egyenértékű harmadik országbeli szervekkel,
f) kapacitásainak és hatáskörének megfelelően részt vesz a CSIRT-hálózat többi tagja részére nyújtandó kölcsönös segítségnyújtásban, azok kérése esetén,
g) csereprogramot működtet más uniós tagállamok CSIRT-tisztviselőinek bevonásával,
h) részt vesz az (EU) 2022/2555 európai parlamenti és tanácsi irányelv 19. cikke szerinti szakértői értékelésben, és szakértői értékelést kezdeményezhet,
i) együttműködhet harmadik országok nemzeti, számítógép-biztonsági eseményekre reagáló csoportjaival vagy azokkal egyenértékű harmadik országbeli szervekkel,
j) csatlakozhat a kibervédelemmel kapcsolatos európai uniós és nemzetközi együttműködésekhez, együttműködési megállapodásokat köthet;

7. további feladatkörében:
a) indokolt esetben vagy a szervezet kérésére – a szervezet szolgáltatásainak működését nem sértő módon – elvégzi a szervezet elektronikus információs rendszereinek proaktív, behatolásmentes átvizsgálását biztonsági rések vagy nem biztonságosan konfigurált elektronikus információs rendszerek felderítése céljából,
b) meghatározza a kiberbiztonsági incidensek és kockázatok kezelésére vonatkozó eljárásokat, valamint a kiberbiztonsági incidensek, kockázatok és információk osztályozására szolgáló eljárásokat és szabályokat; ennek során együttműködik az érintett szervezetekkel,
c) kormányzati információtechnológiai és kiberbiztonsági incidenskezelési együttműködési fórumot működtethet,
d) részt vesz az kiberbiztonságra vonatkozó stratégiák és szabályozások előkészítésében,
e) előírhatja közös vagy szabványosított gyakorlatok, osztályozási rendszerek és rendszertanok elfogadását és alkalmazását, kötelező és nem kötelező érvényű állásfoglalásokat, ajánlásokat adhat ki a kiberbiztonsági incidensek megelőzésére és kezelésre vonatkozó eljárások, a kiberbiztonsági válsághelyzet kezelése, valamint a sérülékenységeknek összehangolt közzététele tekintetében.

(2) A Központ a kiberbiztonsági incidensek és fenyegetések kezelése céljából együttműködik
a) a kiberbiztonsági hatóságokkal,
b) a honvédelmi kiberbiztonsági incidenskezelő központtal,
c) az ágazaton belüli kiberbiztonsági incidenskezelő központokkal,
d) az alapvető és fontos szervezetekkel, valamint azok ágazati vagy ágazatközi csoportjaival,
e) a kiberbiztonsági incidensek kezelése tekintetében érintett szervezetekkel,
f) a rendvédelmi szervekkel,
g) a nemzetbiztonsági szolgálatokkal,
h) a Nemzeti Média- és Hírközlési Hatósággal és az általa működtetett Országos Informatikai és Hírközlési Főügyelettel,
i) az elektronikus hírközlési szolgáltatókkal, a központosított informatikai és elektronikus hírközlési szolgáltatókkal,
j) a Kszetv. szerinti kritikus szervezetekkel, hatóságokkal, továbbá a Vbö. szerinti, az ország védelme és biztonsága szempontjából jelentős szervezetekkel, hatóságokkal,
k) a Nemzeti Adatvédelmi és Információszabadság Hatósággal, valamint
l) a katonai kibertér műveleti erőkkel.

(3) A Központ erőforrásai függvényében kockázatalapú megközelítés alapján rangsorolhatja a feladatai végrehajtását.

68. §

(1) A honvédelmi kiberbiztonsági incidenskezelő központ a hatáskörébe tartozó elektronikus információs rendszerek tekintetében – a 67. § (1) bekezdés 1. pont f) alpontja, 67. § (1) bekezdés 2.

pont l) alpontja, 67. § (1) bekezdés 3. pont a) alpontja, 67. § (1) bekezdés 4. pont b), c) és f) alpontja, 67. § (1) bekezdés 5. pont f) alpontja és 67. § (1) bekezdés 6. pont a)–i) alpontja kivételével – ellátja a 67. § szerinti feladatokat.
(2) A honvédelmi kiberbiztonsági incidenskezelő központ a 67. § (1) bekezdés 5. pont b) alpontja szerinti jelentést a honvédelemért felelős miniszternek küldi meg.
(3) A honvédelmi kiberbiztonsági incidenskezelő központ a hatáskörébe tartozó elektronikus információs rendszerek tekintetében nyilvántartást vezet a hatáskörébe tartozó szervekkel való kapcsolattartáshoz szükséges elérhetőségekről.
(4) A honvédelmi kiberbiztonsági incidenskezelő központ a Központ kérésére átadja a Kiberbiztonsági tv. 66. § (5) bekezdése szerint továbbított fenyegetések, kiberbiztonsági incidensközeli helyzetek és kiberbiztonsági incidensek kezelésével és kivizsgálásával kapcsolatos adatokat.
(5) A honvédelmi kiberbiztonsági incidenskezelő központ tevékenységére – az (1) bekezdésben, a 81. §-ban és a 89. §-ban foglaltak kivételével – a Központra vonatkozó rendelkezéseket kell alkalmazni.

69. §

A Központnak meg kell felelnie a következő követelményeknek:
a) honlapján közzé kell tennie a Központhoz való bejelentésre alkalmas elérhetőségeket, és biztosítania kell a folyamatos elérhetőséget,
b) hivatali helyiségeit és a támogató információs rendszereit biztonságos helyszínen kell elhelyezni,
c) megfelelő rendszerrel kell rendelkeznie a bejelentések kezelésére és továbbítására,
d) biztosítania kell tevékenysége bizalmas jellegét és megbízhatóságát,
e) a feladatellátása megfelelő végrehajtásához elegendő és szakképzett humánerőforrással kell rendelkeznie,
f) redundáns rendszerekkel és tartalék munkaterülettel kell rendelkeznie a szolgáltatásai folyamatosságának biztosítása érdekében,
g) együttműködési kapcsolatokat alakít ki a magánszektor érintett szereplőivel.

28. Fenyegetettség-elemzés és prevenciós tevékenység

70. §

(1) A Központ a hatáskörébe tartozó elektronikus információs rendszert működtető szervektől és a kiberbiztonsági incidenskezelő központoktól kért és kötelezően átadott információk és adatok alapján, az elektronikus információs rendszereket érintő, kiberbiztonsági incidensre vagy fenyegetésre utaló jeleket elemezi, értékeli. A kiberbiztonsági incidens bekövetkezésének veszélyéről vagy fennállásáról, valamint a javasolt intézkedésekről értesíti az elektronikus információs rendszer felett rendelkezési jogot gyakorló szervezetnek az elektronikus információs rendszer biztonságáért felelős személyét.
(2) A Központ a központosított informatikai és elektronikus hírközlési szolgáltatótól átvett műszaki adatok és információk folyamatos figyelésével értékelést végezhet, valamint keresheti a hálózatok, illetve szolgáltatások működését érintő kiberbiztonsági incidensre vagy fenyegetésre utaló jeleket.
(3) A Központ a kiberbiztonsági incidensre vagy fenyegetésre utaló tevékenységeket kivizsgálja, és figyelmeztetést adhat ki a szervezetek, a felhasználók, a kiberbiztonsági incidenskezelő központok, az illetékes hatóságok, valamint az egyedüli kapcsolattartó pont, valamint az érintett szervek felé.

71. §

(1) A Központ által működtetett, fenyegetettségi információkat megosztó rendszer keretében az információgyűjtés kizárólag a szervezet elektronikus rendszereinek nyílt internet irányából elérhető portok és szolgáltatások típusára, és alapvető metaadataira vonatkozhat.
(2) Kiberbiztonsági tv. 65. § (6) bekezdése szerinti tevékenységre internetes címenként kizárólag napi egy alkalommal kerülhet sor. A keletkezett adatokat a Központ öt évig őrzi meg.

72. §

(1) A prevenciós célú eszközök alkalmazása és ezirányú szolgáltatások nyújtása (a továbbiakban: prevenciós eszközök) során a Központ kellő gondossággal eljárva köteles az érintett elektronikus információs rendszer által nyújtott szolgáltatásoknak a feltétlenül szükségesnél nem nagyobb mértékű korlátozására, és a prevenciós eszközöknek a szolgáltatás szempontjából nem kritikus időszakban történő alkalmazására.
(2) Az érintett szervezet köteles a prevenciós eszközök alkalmazásához szükséges adatokat, dokumentumokat, eszközöket és egyéb információkat a Központ rendelkezésére bocsátani, valamint tűrni a prevenciós eszközök alkalmazásából fakadó, az érintett elektronikus információs rendszeren bekövetkezett szolgáltatáscsökkenést, illetve -kiesést.

29. Sebezhetőségek kezelése

73. §

(1) Ha valamely európai kiberbiztonsági tanúsítási rendszert kiadó európai uniós jogi aktus tartalmaz az IKT- termék vonatkozásában észlelt kiberbiztonsági sebezhetőségek bejelentésének és kezelésének módjára vonatkozó szabályokat, úgy az abban foglaltak szerint kell eljárni.
(2) A sebezhetőséget bejelentő személy (a továbbiakban: bejelentő) vagy a felfedezett sebezhetőséggel érintett IKT-termék gyártója vagy szolgáltatója (a továbbiakban együtt: gyártó) az (1) bekezdés szerinti esetben is köteles tájékoztatni a Központot a felfedezett sebezhetőségről és az érintett IKT-termékről, valamint a Központ által kért információkról.

74. §

(1) Európai kiberbiztonsági tanúsítási rendszer hiányában az IKT-termék vonatkozásában a gyártó által a sebezhetőségekre vonatkozó információk harmadik felektől történő fogadására, kezelésére, a bejelentett sebezhetőség kijavítására és összehangolt közzétételére bevezetett eljárásrend az irányadó.
(2) A bejelentő vagy a felfedezett sebezhetőséggel érintett IKT-termékek gyártója az (1) bekezdés szerinti esetben is köteles tájékoztatni a Központot a felfedezett sebezhetőségről és az érintett IKT-termékről, valamint a Központ által kért információkról.

75. §

(1) A honvédelmi célú elektronikus információs rendszer kivételével az elektronikus információs rendszer felett rendelkezési joggal bíró szervezet, valamint az IKT-termék gyártója, lehetőséget biztosíthat arra, hogy – az általa meghatározott eljárásrend betartásával – bárki felkutathassa az elektronikus információs rendszereinek, rendszerelemeinek sérülékenységére, illetve IKT-terméke sebezhetőségére vonatkozó információkat.
(2) Az a szervezet vagy gyártó, amely élni kíván az (1) bekezdésben foglalt lehetőséggel, kidolgozza és a honlapján közzéteszi az általa meghatározott elektronikus információs rendszerei, rendszerelem, IKT-termék sebezhetőségeinek felkutatására, a bejelentésének fogadására, a bejelentő és a szervezet

egyeztetésére, a feltárt sebezhetőségek kijavítására, megosztására irányuló eljárásrendet és erről tájékoztatja a Központot.
(3) A szervezet vagy a gyártó – döntésétől függően – a bejelentő részére anyagi ellenszolgáltatást nyújthat.
(4) A szervezet által kidolgozásra kerülő eljárásrendben meg kell határozni legalább az alábbiakat:
a) mely elektronikus információs rendszerek, rendszerelemek, IKT-termék tartoznak a sebezhetőség-feltárási lehetőséggel érintett körbe, illetve milyen technikák használata engedélyezett vagy tiltott,
b) a szervezet mely kommunikációs csatornán várja a sebezhetőségre vonatkozó bejelentéseket,
c) a szervezet elfogadja-e az anonim bejelentéseket,
d) a bejelentések fogadásáért felelős szervezeti egység, vagy személy elérhetősége,
e) a bejelentővel történő egyeztetés folyamata, valamint a hibajavítás folyamatáról, aktuális helyzetéről való tájékoztatás módja,
f) a bejelentések eredményeként elvégzendő hibajavítások végrehajtására irányuló eljárásrend,
g) azon időkeret, amelyen belül a sebezhetőség javítását elvégzi.
(5) A sebezhetőség felkutatására vállalkozó személy a szervezet honlapján közzétett feltételek elfogadásával, illetve a szervezet és a személy közötti megállapodás alapján járhat el.
(6) Az (5) bekezdés szerinti megállapodásban a felek legalább az alábbi elemeket rögzítik:
a) a szervezet által biztosított felületet, amelyen a sebezhetőség felkutatására vállalkozó személy a sebezhetőségek felkutatását végezheti,
b) a bejelentés megtételének módját,
c) a bejelentő által átadandó információkat,
d) a bejelentő kéri-e névtelenségének megőrzését,
e) amennyiben a szervezet anyagi ellenszolgáltatást ad a bejelentésért, annak mértékét, feltételeit,
f) a szervezet rendelkezésére álló időtartamot a bejelentett sebezhetőség kivizsgálására, valamint kijavítására,
g) amennyiben a szervezet a kivizsgálást, illetve hibajavítást a megállapodásban foglalt határidőn belül elmulasztja, a bejelentő által a Központ értesítésének lehetőségét,
h) annak tényét, hogy a sérülékenységre vonatozó információkról más, érintett szervezet részére történő tájékoztatás nyújtására a Központ jogosult.
(7) Az (1) bekezdést alkalmazó szervezet, amennyiben az elektronikus információs rendszerét, rendszerelemét, IKT-termékét érintően sebezhetőséget jelentenek be, köteles
a) a bejelentett sebezhetőséget a megállapodásban foglalt, illetve a honlapján közzétett határidőn belül, ennek hiányában a lehető legrövidebb időn belül, de legfeljebb 30 napon belül megvizsgálni és a sebezhetőség megszüntetésére vonatkozó intézkedési tervet készíteni,
b) a bejelentő részére visszajelzést küldeni, a feltárt sebezhetőség vonatkozásában a bejelentővel egyeztetni,
c) a feltárt sebezhetőség kijavítására a megállapodásban foglalt határidőn belül, ennek hiányában a lehető legrövidebb időn belül, de a sebezhetőség súlyosságától függően a bejelentéstől számított legfeljebb 90 napon belül intézkedni,
d) a bejelentőt az intézkedések megtételéről értesíteni,
e) a sebezhetőség megszüntetésére vonatkozó intézkedési tervről, valamint a megtett intézkedésekről a Központot tájékoztatni,
(8) Ha az érintett szervezet a bejelentést követően – a megállapodásban vagy az általa kiadott eljárásrendben, illetve ezek hiányában 30 napon belül – nem tesz intézkedést a sebezhetőség kijavítása érdekében, a bejelentő jogosult értesíteni a Központot.
(9) Ha a bejelentő által felfedezett sebezhetőség más szervezet elektronikus információs rendszerét, rendszerelemét, IKT-termékét is érinti, úgy a szervezet bejelentése alapján a Központ a sebezhetőségről az érintett szervezetet tájékoztatja.
(10) A bejelentő köteles

a) a sebezhetőség feltárása érdekében kötött megállapodásban, illetve a jogszabályban meghatározottak szerint eljárni,
b) a feltárt hiányosságról, sérülékenységről az érintett szervezetet a szervezet által meghatározott csatornán keresztül a megállapodásban foglalt határidőn belül, erre irányuló megállapodás hiányában haladéktalanul értesíteni, részére a sebezhetőség azonosításához, a hibajavításhoz szükséges információkat, esetleges megoldási javaslatait megadni,

(11) A Központ
a) a bejelentett sebezhetőséget értékeli,
b) azonosítja az esetlegesen érintett további szervezeteket,
c) intézkedik az érintettekkel történő kapcsolatfelvétel érdekében,
d) a bejelentési, tájékoztatási, illetve együttműködési kötelezettségnek eleget nem tevő szervezetről tájékoztathatja az illetékes kiberbiztonsági hatóságot.

76. §

(1) Ha a 73–75. §-ban foglalt feltételek nem állnak fenn, a természetes vagy jogi személy által valamely elektronikus információs rendszer, IKT-termék vonatkozásában feltárt sebezhetőséget a Központ részére jelenti be. A bejelentést a Központ honlapján meghatározott módon kell megtenni.
(2) A Központ ajánlást adhat ki a sebezhetőségek jogszerű felderítési kereteinek, feltételeinek meghatározása érdekében.
(3) A bejelentő az (1) bekezdés szerinti bejelentés során
a) kérheti névtelenségének megőrzését,
b) köteles elérhetőségét megadni, amennyiben nem kéri névtelenségének megőrzését,
c) köteles megőrizni a bejelentés bizalmasságát,
d) köteles a rendelkezésére álló információkat, esetleges megoldási javaslatait a Központ rendelkezésére bocsátani,
e) köteles a sebezhetőségre vonatkozó információkat titokban tartani, arról kizárólag a Központot és az érintett szervezetet értesítheti,
f) a sebezhetőségről szóló értesítést és a kapcsolódó információknak az érintett szervezet részére történő átadását nem teheti ellenszolgáltatás nyújtásától függővé,
g) kizárólag a sebezhetőség bizonyításához szükséges intézkedések megtételére jogosult,
h) köteles tartózkodni az alábbi káros magatartásoktól:
ha) kártékony kód telepítése,
hb) adatok másolása, törlése, megváltoztatása,
hc) a rendszerben történő módosítások,
hd) ismételt bejelentkezések a rendszerbe,
he) a sebezhetőség és az azzal kapcsolatban megszerzett tudás harmadik féllel történő megosztása,
hf) egyéb módszerekkel történő mélyebb behatolás, illetve behatolási kísérlet.

(4) A bejelentés alapján a Központ
a) intézkedik az érintett szervezetek azonosítása és a velük való kapcsolatfelvétel érdekében,
b) segítséget nyújt a sérülékenységet bejelentőnek,
c) közvetítőként jár el a bejelentő, az elektronikus információs rendszer felett rendelkezési joggal bíró szervezet vagy az IKT-termék gyártója és egyéb érdekeltek között a sebezhetőség közzétételére vonatkozó egyeztetések lefolytatása és a sérülékenységek kezelése érdekében,
d) koordinálja a sebezhetőség közzétételének összehangolását,
e) gondoskodik a bejelentett sebezhetőséggel kapcsolatos intézkedések nyomon követéséről, és
f) kapcsolatot tart az ENISA-val a bejelentéseknek az európai sebezhetőség-adatbázisba történő bejelentése, illetve az adatbázisból történő lekérdezés érdekében.

(5) A Központ jelzése alapján a gyártó vagy az elektronikus információs rendszer felett rendelkezési joggal bíró szervezet 10 napon belül nyilatkozik, hogy a bejelentésben foglaltakat sebezhetőségnek tekinti-e, továbbá nyilatkozik a javítás vonatkozásában. A gyártó köteles a sebezhetőséget 30 napon belül kijavítani vagy javíthatatlan sebezhetőség esetén helyettesítő védelmi intézkedést bevezetni. A nyilatkozattételi vagy az intézkedési határidő eredménytelen elteltét követően a Központ intézkedhet a sebezhetőség publikálása iránt.
(6) Ha a bejelentő kihasznált sebezhetőséget jelent be a Központ részére, a Központ szükség szerint intézkedik
a) a sebezhetőség kapcsán riasztás kiadására,
b) az érintett IKT-termék gyártójával való kapcsolatfelvétel érdekében,
c) az érintett IKT-termék gyártójával folytatott egyeztetés alapján az ENISA értesítésére a sebezhetőségnek az európai sebezhetőség-adatbázisba történő felvétele érdekében.
(7) Ha a bejelentett sebezhetőség több európai uniós tagállamban is jelentős hatást gyakorolhat a szervezetekre, a Központ együttműködik az érintett európai uniós tagállamok koordinátorként kijelölt CSIRT-jeivel a CSIRT-hálózaton belül.
(8) A nyilvánosan ismert sebezhetőség az európai sebezhetőség-adatbázisba történő önkéntes bejelentését a gyártó a Központon keresztül teszi meg annak érdekében, hogy lehetővé tegye az IKT-terméket használók számára a megfelelő mérséklési intézkedések megtételét.

30. A kiberbiztonsági incidensek bejelentése

77. §

(1) A Kiberbiztonsági tv. 66. §-a szerinti bejelentés keretében a szervezet benyújt a Központ részére:
1. indokolatlan késedelem nélkül és minden esetben a kiberbiztonsági incidensről való tudomásszerzéstől számított 24 órán belül egy első bejelentést, amelyben fel kell tüntetni
  a) az érintett elektronikus információs rendszer megjelölését,
  b) a kiberbiztonsági incidens rövid leírását, ennek keretében annak jelzését, hogy az incidens üzemeltetési kiberbiztonsági incidensnek minősül-e,
  c) a kiberbiztonsági incidens státuszát,
  d) a kiberbiztonsági incidens időtartamát,
  e) ha becsülhető, a szolgáltatás helyreállításának várható időpontját,
  f) a kiberbiztonsági incidens által érintett adatok fajtáját, jellegét,
  g) a kiberbiztonsági incidens által érintett felhasználók számát,
  h) a szolgáltatás működésében támadt zavar mértékét,
  i) a kiberbiztonsági incidens kezelésére az üzemeltető által kijelölt kapcsolattartó személy és szervezet elérhetőségeit,
  j) közvetítő szolgáltató vagy központi szolgáltató igénybevétele esetén a közvetítő szolgáltató vagy központi szolgáltató megnevezését, elérhetőségét,
  k) a kiberbiztonsági incidens szándékolt incidensnek minősül-e,
  l) a kiberbiztonsági incidens által érintett terület földrajzi kiterjedését,
  m) lehet-e a kiberbiztonsági incidensnek határokon átnyúló hatása,
  n) minden olyan információt, amely lehetővé teszi Központ számára, hogy meghatározza az esemény határokon átnyúló hatásait;
2. amint rendelkezésre állnak, a fertőzöttségi mutatókat;
3. indokolatlan késedelem nélkül és minden esetben a kiberbiztonsági incidensről való tudomásszerzéstől számított 72 órán belül egy eseménybejelentést, amely adott esetben aktualizálja az 1. pontban említett információkat, és tartalmazza az incidens első értékelését, beleértve annak súlyosságát és hatását;
4. a Központ kérésére közbenső helyzetjelentést;

5. zárójelentést, legkésőbb a 3. pont szerinti eseménybejelentés benyújtását követő egy hónapon belül, amely tartalmazza a következőket:
   a) a kiberbiztonsági incidens részletes leírása, beleértve annak súlyosságát és hatását,
   b) a kiberbiztonsági incidenst valószínűleg kiváltó fenyegetés vagy kiváltó ok típusa,
   c) alkalmazott és folyamatban lévő mérséklési intézkedések,
   d) adott esetben a kiberbiztonsági incidens határokon átnyúló hatása;
6. ha a zárójelentés benyújtásának időpontjában még folyamatban van a kiberbiztonsági incidens, az addig elért eredményekről szóló jelentést;
7. a 6. pont szerinti esetben a kiberbiztonsági incidens kezelését követő egy hónapon belül egy zárójelentést.

(2) Kiberfenyegetés, kiberbiztonsági incidensközeli helyzet és üzemeltetési kiberbiztonsági incidens bejelentése során az (1) bekezdés rendelkezései alkalmazandók, amennyiben azok az adott esemény kapcsán értelmezhetők.

(3) A szervezetnek nem kell bejelentenie azt a kiberbiztonsági incidensközeli helyzetet és üzemeltetési kiberbiztonsági incidenst, amely az incidenskezelési folyamatba kerülés során, automatizmus által kezelésre, elhárításra került és nem járt a szolgáltatás degradációjával. Az ismétlődő kiberbiztonsági incidensközeli helyzetet és üzemeltetési kiberbiztonsági incidenst a szervezet ez esetben is bejelenti.

(4) Az (1) bekezdés 3. pontjától eltérően a bizalmi szolgáltató indokolatlan késedelem nélkül és minden esetben az incidensről való tudomásszerzést követő 24 órán belül értesíti a Központot a bizalmi szolgáltatásai nyújtására hatást gyakorló kiberbiztonsági incidensekről.

78. §

(1) A kiberfenyegetés, a kiberbiztonsági incidensközeli helyzet és a kiberbiztonsági incidens bejelentése a Központ – honvédelmi célú elektronikus információs rendszer vonatkozásában a honvédelmi kiberbiztonsági incidenskezelő központ – által meghatározott módon, elektronikus úton – amennyiben elérhető, a Központ által meghatározott elektronikus felületen – történik. Ha a szervezet elektronikus információs rendszere oly mértékben sérül, hogy az elektronikus úton történő bejelentés nem lehetséges, a bejelentés bármely más módon is megtehető.

(2) Jelentős vagy nagykiterjedésű kiberbiztonsági incidens esetén a szervezet a bejelentést a Központ felé haladéktalanul rövid úton, telefonon is megteszi.

(3) A kiberbiztonsági hatóság a hozzá érkezett bejelentést átteszi a Központhoz.

31. Kiberbiztonsági incidensek kezelése és vizsgálata

79. §

(1) A Központ a bejelentésre haladéktalanul és – ha lehetséges – az első bejelentés kézhezvételétől számított 24 órán belül választ ad. Ennek keretében visszajelzést küld az incidensről a bejelentő szervezetnek, valamint – a szervezet kérésére – útmutatást vagy operatív tanácsokat nyújt a lehetséges mérséklési intézkedések végrehajtásáról.

(2) A Központ technikai támogatást nyújt, ha az érintett szervezet ezt kéri.

80. §

(1) A szervezetek indokolatlan késedelem nélkül és térítésmentesen értesítik a szolgáltatásaikat igénybe vevőket azon kiberbiztonsági incidensekről, amelyek valószínűleg hátrányosan érintik a szolgáltatásnyújtásukat és a szolgáltatásaikat igénybe vevők részéről intézkedés megtétele szükséges.

(2) A szervezet indokolatlan késedelem nélkül – vagy amint az információ rendelkezésre áll – tájékoztatja a jelentős kiberfenyegetés által potenciálisan érintett szolgáltatásait igénybe vevőit azon

intézkedésekről, illetve fenyegetést orvosló lehetőségekről, amelyeket a szolgáltatások igénybe vevői a fenyegetésre válaszul maguk megtehetnek, illetve amelyekkel élhetnek.
(3) Ha a kiberbiztonsági incidens megelőzéséhez vagy egy folyamatban lévő kiberbiztonsági incidens kezeléséhez lakossági figyelemfelkeltés szükséges, vagy ha a kiberbiztonsági incidens nyilvánosságra hozatala egyébként közérdek, a Központ – az érintett szervezettel szükség szerint folytatott konzultációt követően – tájékoztatja az illetékes kiberbiztonsági hatóságot a nyilvánosság tájékoztathatósága érdekében.

81. §

(1) A Központ vizsgálja a kiberbiztonsági incidensek határon átnyúló hatását.
(2) Ha a jelentős kiberbiztonsági incidens két vagy több tagállamot érint, a Központ haladéktalanul tájékoztatja a jelentős eseményről a többi érintett európai uniós tagállamot és az ENISA-t.
(3) A Központ vagy az illetékes kiberbiztonsági hatóság kérésére az egyedüli kapcsolattartó pont a 77. § (1) bekezdése alapján kapott bejelentést továbbítja a kiberbiztonsági incidenssel érintett európai uniós tagállam egyedüli kapcsolattartó pontjának.
(4) A tájékoztatás során a Központ, valamint az egyedüli kapcsolattartó pont az érintett szervezet biztonsági és üzleti érdekeinek védelmére, valamint a benyújtott információk bizalmasságára figyelemmel jár el.
(5) A Központ feladatellátása során az Európai Unió tagállamai és harmadik országok nemzeti, számítógép-biztonsági eseményekre reagáló csoportjaival való kapcsolattartás, információcsere során a megfelelő információmegosztási protokollok – többek között a jelzőlámpa-protokoll (TLP) – használatával folytat információcserét, az adatvédelmi jogszabályokkal összhangban.

82. §

(1) A kiberbiztonsági incidensekkel összefüggő adatok műszaki vizsgálatának célja, hogy
a) feltárja a kiberbiztonsági incidens bekövetkeztének okait, körülményeit, az okozott kár mértékét,
b) behatárolja a kiberbiztonsági incidens által érintett elektronikus információs rendszerek, rendszerelemek körét,
c) javaslatot tegyen a kiberbiztonsági incidens által okozott kár elhárítására, és
d) a bekövetkezett incidensből levonható tanulságokról tájékoztassa a kiberbiztonsági incidenssel érintett más szerveket és az illetékes kiberbiztonsági hatóságot annak érdekében, hogy a jövőben az incidens bekövetkezése megelőzhető legyen.
(2) A kiberbiztonsági incidens vizsgálatáról készült jelentésben a vizsgálatot végző rögzíti az (1) bekezdés szerinti szempontokat és javaslatokat. A vizsgálatot végző a jelentést a vizsgálatok befejezését követően haladéktalanul megküldi az érintett szervezet, a Központ és az illetékes hatóság részére.

83. §

(1) A kiberbiztonsági incidens kezelése és kivizsgálása során az incidenssel érintett szervezet köteles együttműködni Központtal, amely együttműködés kiterjed
a) a bejelentéssel kapcsolatos információk átadására,
b) az incidensben érintettek, valamint az incidensért felelős beazonosításához szükséges műszaki, technikai adatok átadására,
c) a vizsgálat lefolytatásához szükséges adatok, dokumentumok, eszközök és egyéb információk, valamint az ezeket tartalmazó hiteles bitazonos másolatok rendelkezésre bocsátására,
d) az incidensben érintett infrastruktúrával kapcsolatos, speciális, ágazati sajátosságok megosztására,

e) a Központ szakembereinek tájékoztatására az incidens következményei elhárítása érdekében tett intézkedésekről, illetve az incidens vizsgálata során, az infrastruktúrával kapcsolatos beállításokról,
f) hozzáférés biztosítására a Központ szakemberei számára a kiberbiztonsági incidensben érintett infrastruktúrához, valamint
g) a Központ által végzett kockázatelemzés alapján szükségesnek ítélt korai figyelmeztető- vagy csapdarendszerek, szenzorok telepítésére.

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

(3) Ha a kiberbiztonsági incidenssel érintett szervezet bármely okból nem képes a (2) bekezdés szerinti adatok összegyűjtésére, a Központ képviselője helyszíni tanácsadás keretein belül, az érintett szervezet szakértőinek bevonásával javaslatot tesz a szükséges adatok összegyűjtésének és biztosításának módjára vagy a Központ begyűjtheti az adatokat. Az incidenssel érintett szervezet gondoskodik arról, hogy a Központ az adatokhoz hozzáférjen.

(4) Az érintett szolgáltatók a kiberbiztonsági incidensben érintett előfizetőkkel kapcsolatban a Központ kérésére kötelesek térítésmentesen – szükség szerint – tiltásokat bevezetni, felhasználói, előfizetői hozzáféréseket korlátozni, felfüggeszteni vagy megszüntetni.

84. §

(1) A kiberbiztonsági incidenssel érintett szervezet – a Központ támogatásával – kidolgozza és haladéktalanul végrehajtja a kiberbiztonsági incidens felszámolásához szükséges intézkedéseket.

(2) A szervezet a feltárt hiányosságok megszüntetésére vonatkozó incidenskezelési tervről a vizsgálatok lezárását követően tájékoztatja az érintett hatóságot.

(3) A kiberbiztonsági incidenssel érintett szervezet az incidens felszámolását követően felülvizsgálja az elektronikus információs rendszerei kockázatelemzésének, kockázatkezelésének teljeskörűségét, és végrehajtja a szükséges módosításokat.

85. §

A központi rendszer felett rendelkezési jogot gyakorló szervezet, valamint a központi szolgáltató az incidenskezelés során köteles
a) a kiberbiztonsági incidensben érintett szervezet, valamint az incidensért felelős beazonosításához szükséges műszaki, technikai adatok Központ részére történő átadására,
b) az ismert fenyegetések elleni védelmi intézkedések, műszaki, technikai megoldások alkalmazására,
c) a Központ kérésére a 83. § (1) bekezdése szerinti adatokat szolgáltatni a hálózati forgalomba való beavatkozásra utaló jelek elemzése, kiértékelése céljából, valamint
d) a Központ által meghatározott, kiberbiztonsági incidensekkel kapcsolatos feladatokban együttműködni.

86. §

(1) A kiberbiztonsági incidensek kezelése során a Központ szükség szerint megismerheti a közvetítő szolgáltatók különböző szolgáltatás- vagy üzletmenet folytonosságot biztosító szabályzóit, eljárásrendjeit, ideértve az üzletfolytonossági tervét, a katasztrófa helyreállítási tervét.

(2) A kiberbiztonsági incidens által érintett közvetítő szolgáltató a Központtal való együttműködés keretein belül a konkrét incidens kezelése érdekében a Központ kérésére az incidensben érintettek, a támadó és a támadott beazonosításához szükséges adatokat szolgáltat az incidenskezelő központ

részére, valamint az incidensben érintett előfizetőkkel kapcsolatban szükség szerint tiltásokat vezet be, felhasználói, illetve előfizetői hozzáféréseket korlátoz, függeszt fel, vagy szüntet meg.
(3) Veszélyesnek vagy károsnak ítélt szolgáltatás biztosítása esetén a Központ kötelezheti a közvetítő szolgáltatót adott szolgáltatás tiltására.

87. §

(1) A bejelentési, tájékoztatási, illetve együttműködési kötelezettségnek eleget nem tevő szervezetet, szolgáltatót a Központ jelenti a felügyeletét ellátó kiberbiztonsági hatóságnak.
(2) A Központ a kiberbiztonsági incidens kezelése, vizsgálata során tudomására jutott információk alapján kezdeményezheti a nemzeti kiberbiztonsági hatóságnál a kiberbiztonsági incidenssel érintett elektronikus információs rendszer sérülékenységvizsgálatának lefolytatására irányuló kötelezést.

88. §

A Központ a kiberbiztonsági incidensről zárt kezelésű technológiai naplót vezet, amely tartalmazza az incidens kivizsgálásának támogatása során tett intézkedéseket és azok eredményét is.

89. §

E fejezet rendelkezései az önkéntes bejelentések esetén is alkalmazandók.

32. Az (EU) 2022/2554 európai parlamenti és tanácsi rendelet hatálya alá tartozó szervezetek kiberbiztonsági incidenseinek kezelésére irányadó rendelkezések

90. §

(1) Az (EU) 2022/2554 európai parlamenti és tanácsi rendelet hatálya alá tartozó szervezetek kiberbiztonsági incidenseinek kezelése során – a 67. § (1) bekezdés 2. pont k) alpontja, valamint a 67. § (1) bekezdés 7. pont b) alpontja kivételével – a 65–67. §, a 73–76. §, a 78. §, a 79. §, a 81. §, a 83. § (1) bekezdés a)–f) pontja, a 83. § (2) és (3) bekezdése, a 84. § (1) bekezdése, valamint a 86–89. § szerinti rendelkezések alkalmazandók.
(2) Ahol e rendelet kiberbiztonsági hatóságot említi, ott az (EU) 2022/2554 európai parlamenti és tanácsi rendelet hatálya alá tartozó szervezetek vonatkozásában az (EU) 2022/2554 európai parlamenti és tanácsi rendelet szerinti hatóságot kell érteni.
(3) A kiberbiztonsági gyakorlaton való részvétel Központ általi elrendelése esetén a kiberbiztonsági gyakorlaton való részvétel kötelező. Az (EU) 2022/2554 európai parlamenti és tanácsi rendelet hatálya alá tartozó szervezetek kiberbiztonsági gyakorlat által érintett körét, valamint a kiberbiztonsági gyakorlat tervezett időpontját a Központ az (EU) 2022/2554 európai parlamenti és tanácsi rendelet szerinti hatósággal való előzetes egyeztetés alapján állapítja meg.

VII. Fejezet

A kiberbiztonsággal kapcsolatos feladatok koordinációjának szervezetrendszere

33. A kiberbiztonságért felelős biztos

91. §

(1) A kiberbiztonságért felelős biztos helyettest bízhat meg. A helyettes a megbízatása keretei között jár el.
(2) A kiberbiztonságért felelős biztost be kell vonni a kiberbiztonsággal kapcsolatos jogszabályok megalkotásába és felülvizsgálatába.
(3) A kiberbiztonságért felelős biztos a Nemzeti Kiberbiztonsági Munkacsoport döntése alapján kezdeményezheti az informatikáért felelős miniszternél a kiberbiztonsággal kapcsolatos jogszabályok felülvizsgálatát.

34. A Nemzeti Kiberbiztonsági Munkacsoport

92. §

(1) A Nemzeti Kiberbiztonsági Munkacsoport elnökét – akadályoztatása esetén – a 91. § (1) bekezdése szerint megbízott személy helyettesíti.
(2) A Nemzeti Kiberbiztonsági Munkacsoport tagjai:
a) miniszterek,
b) a Nemzetbiztonsági Szakszolgálat főigazgatója,
c) az SZTFH elnöke,
d) a Magyar Nemzeti Bank elnöke,
e) a védelmi és biztonsági igazgatás központi szervének vezetője és
f) a miniszterelnök nemzetbiztonsági főtanácsadója
által delegált, 1-1 vezető beosztású személy.
(3) A (2) bekezdés a) pontja szerint a miniszterek a Nemzeti Kiberbiztonsági Munkacsoportba önállóan, egymástól függetlenül delegálnak tagokat.
(4) A (2) bekezdésben meghatározottakon túl a Nemzeti Kiberbiztonsági Munkacsoport tagjai a kiberbiztonságért felelős biztos által felkért személyek.
(5) A Nemzeti Kiberbiztonsági Munkacsoport tagjainak visszahívásáról a Nemzeti Kiberbiztonsági Munkacsoport elnökének javaslatára a tagot delegáló személy dönt.
(6) A Nemzeti Kiberbiztonsági Munkacsoport elnöke a Nemzeti Kiberbiztonsági Munkacsoport munkájáról legalább félévente beszámol az informatikáért felelős miniszternek.

35. Operatív Törzs

93. §

(1) Az Operatív Törzs vezetőjeként, elnökeként eljáró kiberbiztonságért felelős biztost – akadályoztatása esetén – a 91. § (1) bekezdése alapján megbízott személy helyettesíti.
(2) Az Operatív Törzs tagjai:
a) a 92. § (2) bekezdése szerinti szervek vagy szervezetek által delegált operatív feladatokat ellátó vezető beosztású személy,
b) a hivatásos katasztrófavédelmi szerv központi szerve által delegált vezető beosztású személy,
c) a kiberbiztonsági válsághelyzet kezelésében érintett szerv vagy szervezet által delegált vezető beosztású személy,
d) a kiberbiztonságért felelős biztos által felkért személyek.

36. Kiberbiztonsági Fórum

94. §

A Nemzeti Kiberbiztonsági Munkacsoport által felkért egyetemi, kutatói, szakmai, gazdasági és más nem kormányzati szereplőkből álló Kiberbiztonsági Fórum (a továbbiakban: Fórum) vezetését a Nemzeti Kiberbiztonsági Munkacsoport elnöke, a Fórum munkájának szakmai koordinálását a kiberbiztonságért felelős biztos által kijelölt személy látja el.

37. Kiberbiztonsági Almunkacsoportok

95. §

(1) A Nemzeti Kiberbiztonsági Munkacsoport koordinációs tevékenységét, valamint döntéseinek végrehajtását a Nemzeti Kibertér Munkacsoport és a Nemzetközi és Európai Uniós Kibertér Munkacsoport (a továbbiakban együtt: Kiberbiztonsági Almunkacsoportok) segíti.
(2) A Nemzeti Kibertér Munkacsoport vezetését a Nemzetbiztonsági Szakszolgálat vezetője által kijelölt, a Nemzetbiztonsági Szakszolgálat személyi állományába tartozó személy látja el.
(3) A Nemzetközi és Európai Uniós Kibertér Munkacsoport vezetését – az informatikáért felelős miniszterrel egyeztetve – a külpolitikáért felelős miniszter által kijelölt kibertér koordinátor látja el.
(4) A Kiberbiztonsági Almunkacsoportok tagjai a Kiberbiztonsági Almunkacsoportok vezetői által felkért állami szervek vagy szervezetek által delegált személyek és nem kormányzati szakértők, valamint a kiberbiztonságért felelős biztos. A Nemzeti Kiberbiztonsági Munkacsoport javaslatot tehet a Kiberbiztonsági Almunkacsoportok vezetői részére a Kiberbiztonsági Almunkacsoportok tagjainak a felkérésével összefüggésben.
(5) A Nemzeti Kibertér Munkacsoport javaslatára a Nemzeti Kiberbiztonsági Munkacsoport jogi kötelező erővel nem rendelkező ajánlásokat adhat ki a kibertámadások kezelése és az elektronikus információbiztonság területén alkalmazandó legjobb gyakorlatokról.
(6) A Nemzeti Kibertér Munkacsoport szükség szerint közreműködik a kiberbiztonsági válsághelyzetek ágazati és kormányzati kezeléséhez szükséges szakmai háttérfeladatok végrehajtásában, a kiberbiztonsági események kiberbiztonsági válsághelyzetté történő minősítéssel kapcsolatos és a Magyarország által képviselendő vonatkozó álláspontokkal összefüggő szakmai javaslatok és mandátumok kialakításában.
(7) A Nemzeti Kibertér Munkacsoport feladata a nemzeti kiberbiztonság erősítése valamennyi ágazatban.
(8) A Nemzetközi és Európai Uniós Kibertér Munkacsoport feladata az állami szervek közötti, a nemzetközi szervezetekben, az Európai Unióban, valamint a két- és többoldalú együttműködésekben zajló kiberbiztonsági munkával kapcsolatos rendszeres információcsere elősegítése és egyeztetés a Magyarország által képviselendő vonatkozó álláspontjának kialakítását illetően.
(9) A Nemzeti Kiberbiztonsági Munkacsoport kérésére a Kiberbiztonsági Almunkacsoportok keretében tematikus munkacsoportok is létrehozhatók.

38. Titkárság

96. §

A Nemzeti Kiberbiztonsági Munkacsoport, a Fórum és a Kiberbiztonsági Almunkacsoportok működtetésével kapcsolatos adminisztratív teendőket a kiberbiztonságért felelős biztos irányításával, az informatikáért felelős miniszter által biztosított titkárság (a továbbiakban: Titkárság) látja el. A Titkárság ellátja a kiberbiztonságért felelős biztos szakértői támogatását is.

39. A kormányzati koordinációs szervek feladatai

97. §

(1) A Nemzeti Kiberbiztonsági Munkacsoport feladata a Magyarország Nemzeti Kiberbiztonsági Stratégiájában meghatározott cselekvési területeken a kormányzati tevékenység koordinációjának elősegítése és a végrehajtás figyelemmel kísérése, a kiberbiztonsággal kapcsolatos jogszabályok véleményezése.
(2) A Nemzeti Kiberbiztonsági Munkacsoport a Fórum javaslatainak és véleményének figyelembevételével, az (1) bekezdésben meghatározott cselekvési területekhez társított kormányzati intézkedéseket tartalmazó akciótervet (a továbbiakban: Nemzeti Kiberbiztonsági Akcióterv) a Kiberbiztonsági Almunkacsoportok és a kiberbiztonságért felelős biztos irányításával készíti el, melynek elfogadásáról a Kormány dönt. A Nemzeti Kiberbiztonsági Akciótervet a Nemzeti Kiberbiztonsági Munkacsoportnak évente felülvizsgálja.
(3) A Nemzeti Kiberbiztonsági Akcióterv éves felülvizsgálatának koordinációját – a Kiberbiztonsági Almunkacsoportok bevonásával – a Titkárság látja el.

98. §

(1) A Nemzeti Kiberbiztonsági Munkacsoport a feladatai ellátásához igazodva szükség szerint, de legalább háromhavonta tart ülést, melyet a kiberbiztonságért felelős biztos hív össze.
(2) A Nemzeti Kiberbiztonsági Munkacsoport üléseit a Nemzeti Kiberbiztonsági Munkacsoport elnöke vagy helyettese vezeti. Az ülésekről emlékeztetőt a Titkárság készít.

99. §

(1) Az Operatív Törzs a feladatai ellátásához igazodva szükség szerint, de legalább háromhavonta tart ülést, melyet a kiberbiztonságért felelős biztos hív össze.
(2) Az Operatív Törzs feladatai:
a) a kiberbiztonsági válsághelyzetet eredményező kiberbiztonsági incidensek megelőzésével, elhárításával, megakadályozásával, következményeinek enyhítésével, valamint az ezekre való felkészüléssel kapcsolatos feladatok végrehajtása,
b) a kiberbiztonsági incidensekre vonatkozó információk cseréje, összegzése, értékelése,
c) javaslattétel a kiberbiztonsági válsághelyzetek megelőzése, kezelésére való felkészülés érdekében kiberbiztonsági képzésre, gyakorlatokra,
d) a tudomására jutott kiberbiztonsági incidensek nyomon követése, beleértve a fenyegetések és kockázatok folyamatos elemzését,
e) a bekövetkezett jelentős vagy nagyszabású kiberbiztonsági incidens kiberbiztonsági válsághelyzetté történő minősítésére javaslattétel,
f) kiberbiztonsági válsághelyzetben a felderítő, műveleti intézkedések összehangolása és a szükségesnek ítélt hatósági intézkedések kezdeményezése,
g) kiberbiztonsági válsághelyzet esetén az érintett szervek, szervezetek bevonásával a helyreállás időigényének, valamint a kiesett szolgáltatások pótolhatóságának vizsgálata,
h) a Nemzeti Kiberbiztonsági Munkacsoport szükség szerinti tájékoztatása a közös helyzetismeretről, a megtett intézkedésekről.
(3) Az Operatív Törzs tagjainak és az egyéb érintett szerveknek az Operatív Törzs részére történő tájékoztatási kötelezettsége nem érinti azok jogszabályban, más közjogi szervezetszabályozó eszközben előírt tájékoztató tevékenységét és egyéb kötelezettségeit.
(4) Az Operatív Törzs működési rendjét maga alakítja ki, az ülésére az állandó tagok napirend felvételét kezdeményezhetik. A napirendre vonatkozó javaslatot az elnökhöz írásban, indokolással ellátva kell benyújtani.
(5) Az Operatív Törzs tevékenységéről legalább félévente beszámol a Nemzeti Kiberbiztonsági Munkacsoport részére.

100. §

(1) A Fórum a feladatai ellátásához igazodva szükség szerint, de legalább háromhavonta tart ülést. Üléseit a Nemzeti Kiberbiztonsági Munkacsoport elnöke vagy az általa kijelölt tag hívja össze.
(2) A Fórum üléseit a Nemzeti Kiberbiztonsági Munkacsoport elnöke vagy az általa kijelölt tag vezeti. Az ülésekről emlékeztetőt a Tikárság készít.

101. §

(1) A Kiberbiztonsági Almunkacsoportok a feladataik ellátásához igazodva szükség szerint, de legalább háromhavonta tartanak ülést. Az üléseket a Kiberbiztonsági Almunkacsoportok vezetői hívják össze.
(2) A Kiberbiztonsági Almunkacsoportok üléseiről emlékeztetőt a Titkárság készít.

102. §

A Nemzeti Kiberbiztonsági Munkacsoport, a Fórum és a Kiberbiztonsági Almunkacsoportok működésére vonatkozó eljárási szabályokat a tagok által készített és a Nemzeti Kiberbiztonsági Munkacsoport elnöke által jóváhagyott ügyrend tartalmazza.

103. §

A Nemzeti Kiberbiztonsági Munkacsoport, a Fórum, a Kiberbiztonsági Almunkacsoportok és az Operatív Törzs tagjai, valamint a munkájukban közreműködő állami vezető, kormánytisztviselő, közalkalmazott, adó- és vámhatósági szolgálati jogviszonyban foglalkoztatott, hivatásos szolgálati jogviszonyban, rendvédelmi igazgatási alkalmazotti jogviszonyban, nemzetbiztonsági szolgálati jogviszonyban, nemzetbiztonsági alkalmazotti jogviszonyban foglalkoztatott, hivatásos katonai szolgálati viszonyban, honvédelmi alkalmazotti jogviszonyban, kizárólagos állami tulajdonban álló gazdasági társaság vezető tisztségviselője vagy munkavállalója díjazásban nem részesül.

104. §

A Nemzeti Kiberbiztonsági Munkacsoporttal kapcsolatos kommunikációs feladatokat a kiberbiztonságért felelős biztos vagy helyettese látja el és felügyeli.

VIII. Fejezet

A nemzeti koordinációs központ

105. §

A Kormány a Kiberbiztonsági tv. 75. §-a szerinti nemzeti koordinációs központként a Nemzetbiztonsági Szakszolgálatot jelöli ki.

IX. Fejezet

A kiberbiztonsági válsághelyzetek kezelése

40. A kiberbiztonsági válsághelyzetek kezelésének szervezetrendszere

106. §

(1) A kiberbiztonsági válsághelyzet kezelésével kapcsolatos feladatokat az érintett személyek, szervek és szervezetek a Kiberbiztonsági tv.-ben és az e rendeletben meghatározottak figyelembevételével, a rájuk vonatkozó jogszabályi rendelkezések és közjogi szervezetszabályozó eszközben előírtak alapján hajtják végre.
(2) A kiberbiztonsági válsághelyzet feltételeinek a fennállását az Operatív Törzs folyamatosan figyelemmel kíséri, és ha a kiberbiztonsági válsághelyzet elrendelésének a feltételei már nem állnak fenn, kezdeményezi az informatikáért felelős miniszternél, hogy tegyen javaslatot a Kormánynak a kiberbiztonsági válsághelyzetet elrendelő kormányrendelet hatályon kívül helyezésére.
(3) A kiberbiztonsági válsághelyzet kezelésével kapcsolatos igazgatási és koordinációs feladatokat a Vbö. 52. § c) pontjában meghatározott nemzeti eseménykezelő központ (a továbbiakban: nemzeti eseménykezelő központ) biztosítja, az érintett kiberbiztonsági incidenskezelő központ aktív támogatásával.
(4) A kiberbiztonsági válsághelyzet kezelésével kapcsolatban megtett ágazati intézkedésekről a védelmi és biztonsági igazgatás központi szervét, valamint az informatikáért felelős miniszter előterjesztése útján a Védelmi Tanácsot haladéktalanul tájékoztatni kell.
(5) A kiberbiztonsági válsághelyzet kezelésével kapcsolatos nemzetközi együttműködéssel összefüggő feladatokat, az IPCR felületen történő tagállami információcsere koordinációját a védelmi és biztonsági igazgatás központi szerve végzi.
(6) A kiberbiztonsági válsághelyzet kezelésével kapcsolatos szakmai feladatokat Magyarország képviseletében az EU-CyCLONe-ban

a) vezető tisztviselői, ügyvezetői szinten a védelmi és biztonsági igazgatás központi szerve,
b) szakértői szinten
  ba) a Nemzetbiztonsági Szakszolgálat,
  bb) az informatikáért felelős miniszter által vezetett minisztérium és felkérés alapján a honvédelemért felelős miniszter által vezetett minisztérium

látja el.

41. A kiberbiztonsági tervezés és felkészülés rendje

107. §

(1) Magyarország nemzeti kiberválságkezelési tervét (a továbbiakban: nemzeti kiberválságkezelési terv) a kiberbiztonságért felelős biztos koordinációjával a Központ – a Nemzeti Kiberbiztonsági Munkacsoport javaslatai alapján – készíti el.
(2) A nemzeti kiberválságkezelési tervet az Ország Összehangolt Védelmi Tervében foglaltakra figyelemmel, azzal összhangban kell elkészíteni.
(3) A nemzeti kiberválságkezelési terv legalább az alábbiakat határozza meg:

a) a nemzeti felkészültségi intézkedések és tevékenységek célkitűzései,
b) a kiberbiztonsági válsághelyzetek kezelésével foglalkozó hatóságok feladatai és felelősségei,
c) a kiberbiztonsági válsághelyzetek kezelésére szolgáló eljárások, beleértve azok integrálását az általános nemzeti válságkezelési keretbe és az információcserére szolgáló csatornákba,
d) nemzeti felkészültségi intézkedések, beleértve a gyakorlatokat és a képzési tevékenységeket,
e) az érintett állami és magán érdekelt felek, valamint az érintett infrastruktúra azonosítása,
f) nemzeti eljárások és megállapodások az érintett nemzeti hatóságok és szervek között.

(4) A nemzeti kiberválságkezelési terv elfogadását követő három hónapon belül be kell nyújtani az Európai Bizottság és az EU-CyCLONe részére a (3) bekezdésben foglalt releváns információkat, amelyben nem szerepeltethetők a nemzetbiztonsági szempontból érzékeny információk, valamint

amelyek közlése ellentétes lenne Magyarország nemzetbiztonsági, honvédelmi, közbiztonsági vagy alapvető érdekeivel vagy azokat sértené.
(5) A (4) bekezdés szerinti információkat a védelmi és biztonsági igazgatás központi szerve küldi meg az Európai Bizottság és az EU-CyCLONe részére a Védelmi Tanács véleményének kikérését követően.

108. §

(1) A Kiberbiztonsági tv. 74. § (10) bekezdése szerinti kiberbiztonsági tervet a szakmai standardok és kormányzati iránymutatások alapján kell elkészíteni, amelynek folyamatos nyomonkövetéséről, valamint a kapcsolódó intézkedések felülvizsgálatáról a készítő szervezet vezetője gondoskodik.
(2) A kiberbiztonsági terv a szervezet Védelmi és Biztonsági Intézkedési Tervének része, amely a védelmi és biztonsági szervezet működésére jellemző speciális intézkedéseket tartalmazza.

109. §

(1) Az Operatív Törzs a kiberbiztonsági válsághelyzetekre történő felkészülés érdekében
a) ágazati vagy központi kiberbiztonsági válságkezelési gyakorlat, valamint
b) a kiberbiztonság és kibertudatosság erősítése érdekében oktatás és képzés
megszervezését kezdeményezheti.
(2) Az (1) bekezdés a) pontja szerinti gyakorlatot az Operatív Törzs
a) a nemzeti kiberbiztonsági hatósággal, a védelmi és biztonsági igazgatás központi szervével és a hivatásos katasztrófavédelmi szerv központi szervével, valamint az érintett ágazatot képviselő szervezettel együttműködve, indokolt esetben a Katonai Nemzetbiztonsági Szolgálat, valamint a Magyar Honvédség bevonásával szervezi,
b) a kritikus infrastruktúrákat üzemeltető, valamint az ország védelme és biztonsága szempontjából jelentős szervezetek szükség szerinti bevonásával bonyolítja le, valamint
c) központi gyakorlattá történő minősítés esetén a védelmi és biztonsági igazgatás központi szervének irányításával bonyolítja le.
(3) Az (1) bekezdés a) pontja szerinti gyakorlat, illetve az (1) bekezdés b) pontja szerinti oktatás, képzés által érintett szervezet köteles a gyakorlaton, illetve az oktatáson és a képzésen részt venni, valamint a szükséges feltételeket biztosítani.

110. §

A kiberbiztonsági válsághelyzetekre történő felkészülés, valamint a kiberbiztonsági válsághelyzetek kezelése érdekében – a jogszabályban meghatározott kiberbiztonsági feladatokra figyelemmel – az elektronikus hírközlési szolgáltató, a közvetítő szolgáltató, a központi rendszer felett rendelkezési jogot gyakorló szervezet, valamint a központi szolgáltató együttműködik a nemzeti eseménykezelő központtal, a Központtal és az Operatív Törzzsel.

42. Nagy kiterjedésű incidens bejelentése, az Európai Bizottság és a tagállamok tájékoztatása

111. §

(1) Az Európai Bizottságot, valamint az EU-CyCLONE vezető tisztviselői szintjét a nagyszabású kiberbiztonsági incidensekről a 106. § (6) bekezdés a) pontja szerint kijelölt személy tájékoztatja.
(2) Az érintett uniós tagállamok EU-CyCLONE-on keresztüli tájékoztatásának tartalmáról az Operatív Törzs javaslata alapján a kiberbiztonsági válsághelyzet kezelése érdekében a Kormány által kijelölt személy vagy szervezet vezetője dönt.

X. Fejezet

Együttműködés és jelentéstétel

43. Nemzeti együttműködés

112. §

(1) A nemzeti kiberbiztonsági hatóság, az SZTFH, a honvédelmi kiberbiztonsági hatóság, az (EU) 2022/2554 európai parlamenti és tanácsi rendelet szerinti hatóság, az egyedüli kapcsolattartó pont, a Központ, a honvédelmi kiberbiztonsági incidenskezelő központ, valamint az ágazaton belüli kiberbiztonsági incidenskezelő központ együttműködik a jogszabályban meghatározott kötelezettségek végrehajtása érdekében.

(2) Az (1) bekezdésben említett szervezetek együttműködnek és együttműködési megállapodást köthetnek

a) a bűnüldöző hatóságokkal,

b) a Nemzeti Adatvédelmi és Információszabadság Hatósággal,

c) a polgári légi közlekedés védelmének közös szabályairól és a 2320/2002/EK rendelet hatályon kívül helyezéséről szóló, 2008. március 11-i 300/2008/EK európai parlamenti és tanácsi rendelet szerinti hatósággal,

d) a polgári légi közlekedés területén alkalmazandó közös szabályokról és az Európai Unió Repülésbiztonsági Ügynökségének létrehozásáról és a 2111/2005/EK, az 1008/2008/EK, a 996/2010/EU, a 376/2014/EU európai parlamenti és tanácsi rendelet és a 2014/30/EU és a 2014/53/EU európai parlamenti és tanácsi irányelv módosításáról, valamint az 552/2004/EK és a 216/2008/EK európai parlamenti és tanácsi rendelet és a 3922/91/EGK tanácsi rendelet hatályon kívül helyezéséről szóló, 2018. július 4-i (EU) 2018/1139 európai parlamenti és tanácsi rendelet szerinti hatósággal,

e) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről szóló, 2014. július 23-i 910/2014/EU európai parlamenti és tanácsi rendelet (a továbbiakban: 910/2014/EU európai parlamenti és tanácsi rendelet) szerinti felügyeleti szervvel,

f) az Európai Elektronikus Hírközlési Kódex létrehozásáról szóló, 2018. december 11-i (EU) 2018/1972 európai parlamenti és tanácsi irányelv [a továbbiakban: (EU) 2018/1972 európai parlamenti és tanácsi irányelv] szerinti nemzeti szabályozó hatósággal,

g) a Kszetv. szerinti kijelölő hatósággal,

h) a Vbö. szerinti kijelölő hatósággal, valamint

i) az egyéb ágazatspecifikus uniós jogi aktusok szerinti illetékes hatósággal.

(3) Az (1) bekezdés szerinti szervezetek és a 910/2014/EU európai parlamenti és tanácsi rendelet, az (EU) 2022/2554 európai parlamenti és tanácsi rendelet, valamint az (EU) 2018/1972 európai parlamenti és tanácsi irányelv szerinti hatóság rendszeresen információkat cserélnek, többek között a kiberbiztonsági incidensekkel és kiberfenyegetésekkel kapcsolatban.

(4) A nemzeti kiberbiztonsági hatóság, valamint a Központ az (EU) 2022/2554 európai parlamenti és tanácsi rendelet szerinti hatóság nyilvántartásából megismerheti az alábbi adatokat:

a) a szervezet azonosításához szükséges adatokat,

b) a szervezet elérhetőségeit, ideértve elektronikus elérhetőségeket, valamint a szervezet által használt nyilvános IP címeket vagy IP-tartományokat, valamint a szervezet székhelyét, telephelyét, fióktelepét,

c) a szervezet alapvető vagy fontos szervezetnek minősülését,

d) nem Magyarországon bejegyzett szervezet Magyarország területén működő képviselőjének nevét vagy cégnevét, levelezési címét, telefonszámát és elektronikus levelezési címét,

e) az elektronikus információs rendszer biztonságáért felelős személy feladatait ellátó személy nevét, közvetlen elérhetőséget biztosító telefonszámát, elektronikus elérhetőségét, valamint

f) a szervezet elektronikus információs rendszereinek megnevezését.

113. §

(1) Az SZTFH tájékoztatja az egyedüli kapcsolattartó pontot

a) kétévente március 15-ig a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti szervezetek vonatkozásában az (EU) 2022/2555 európai parlamenti és tanácsi irányelv I. vagy II. mellékletében említett ágazatok és alágazatok szerinti bontásban az alapvető és fontos szervezetek számáról;

b) a DNS-szolgáltatók, a legfelső szintű doménnév-nyilvántartók, a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek, a felhőszolgáltatók, az adatközpont-szolgáltatók, a tartalomszolgáltató hálózati szolgáltatók, az irányított szolgáltatók és az irányított biztonsági szolgáltatók, valamint az online piacterek, az online keresőprogramok és a közösségimédia-szolgáltatási platformok vonatkozásában a következő alábbi adatokról:

ba) a szervezet neve,

bb) az (EU) 2022/2555 európai parlamenti és tanácsi irányelv I. vagy II. mellékletében említett érintett ágazat, alágazat és szervezettípus,

bc) a szervezet székhelye, telephelye, fióktelepe, vagy nem az Európai Unióban letelepedett szervezet esetében kijelölt képviselőjének a címe,

bd) a szervezet és kijelölt képviselőjének elérhetőségei, beleértve e-mail-címét és telefonszámát is,

be) azok az európai uniós tagállamok, amelyekben a szervezet szolgáltatásokat nyújt;

c) a b) pont szerinti adatok változásáról a változás bejelentését követő 30 napon belül.

(2) Az (EU) 2022/2554 európai parlamenti és tanácsi rendelet szerinti hatóság tájékoztatja az egyedüli kapcsolattartó pontot kétévente március 15-ig az alábbi ágazatok szerinti szervezetek számáról:

a) banki szolgáltatások ágazat esetében a hitelintézetekre és befektetési vállalkozásokra vonatkozó prudenciális követelményekről és a 648/2012/EU rendelet módosításáról szóló, 2013. június 26-i 575/2013/EU európai parlamenti és tanácsi rendelet 4. cikk 1. pontjában meghatározott hitelintézetek,

b) pénzügyi piaci infrastruktúrák ágazat esetében

ba) a pénzügyi eszközök piacairól, valamint a 2002/92/EK irányelv és a 2011/61/EU irányelv módosításáról szóló, 2014. május 15-i 2014/65/EU európai parlamenti és tanácsi irányelv 4. cikk (1) bekezdés 24. pontjában meghatározott kereskedési helyszínek működtetői, valamint

bb) a tőzsdén kívüli származtatott ügyletekről, a központi szerződő felekről és a kereskedési adattárakról szóló, 2012. július 4-i 648/2012/EU európai parlamenti és tanácsi rendelet 2. cikk 1. pontjában meghatározott központi szerződő felek.

(3) A nemzeti kiberbiztonsági hatóság tájékoztatja az egyedüli kapcsolattartó pontot:

a) kétévente március 31-ig

aa) a Kiberbiztonsági tv. 1. § (1) bekezdés a)-c) pontja szerinti szervezetek vonatkozásában az (EU) 2022/2555 európai parlamenti és tanácsi irányelv I. vagy II. mellékletében említett ágazatok és alágazatok szerinti bontásban az alapvető és fontos szervezetek számáról, valamint

ab) az azonosított alapvető és fontos szervezetek számáról, az (EU) 2022/2555 európai parlamenti és tanácsi irányelv I. vagy II. mellékletében említett ágazatuk, alágazatuk, az általuk nyújtott szolgáltatás típusa szerinti bontásban, valamint az azonosításuk alapjául szolgáló rendelkezésről,

b) az Európai Bizottság kérése esetén az ab) pontban említett alapvető és fontos szervezetek nevéről, amennyiben az nemzetbiztonsági, honvédelmi vagy egyéb biztonsági érdeket nem sért.

(4) A Központ háromhavonta tájékoztatja az egyedüli kapcsolattartó pontot a bejelentett kiberbiztonsági incidensekről, kiberfenyegetésekről és majdnem bekövetkezett eseményekről a bejelentésekre vonatkozó statisztikai kimutatás megküldése útján.

44. Az egyedüli kapcsolattartó pont

114. §

(1) Az egyedüli kapcsolattartó pont összekötő feladatokat lát el
a) az Európai Bizottság felé,
b) az ENISA felé,
c) a többi európai uniós tagállam egyedüli kapcsolattartó pontjával,
d) az (EU) 2022/2555 európai parlamenti és tanácsi irányelv együttműködési csoportjával (a továbbiakban: NIS Együttműködési Csoport), valamint a NIS együttműködési csoportjával, valamint
e) a magyar kiberbiztonsági szervekkel.
(2) Az egyedüli kapcsolattartó pont a 113. § szerinti adatszolgáltatások alapján megküldi
a) az Európai Bizottságnak és a NIS Együttműködési Csoportnak: kétévente az (EU) 2022/2555 európai parlamenti és tanácsi irányelv I. vagy II. mellékletében említett egyes ágazatok és alágazatok tekintetében az alapvető és fontos szervezetek számát;
b) az Európai Bizottságnak kétévente az azonosított alapvető és fontos szervezetek számát, az (EU) 2022/2555 európai parlamenti és tanácsi irányelv I. vagy II. mellékletében említett ágazatukról és alágazatukról, az általuk nyújtott szolgáltatás típusáról, valamint az azonosításuk alapjául szolgáló rendelkezésről szóló releváns információkat;
c) az Európai Bizottságnak kérésére a b) pontban említett alapvető és fontos szervezetek nevét, amennyiben az nemzetbiztonsági, honvédelmi vagy egyéb biztonsági érdeket nem sért;
d) az ENISA-nak a 113. § (1) bekezdés b) pontja szerinti információkat a szolgáltatói nyilvántartáshoz.
(3) Az egyedüli kapcsolattartó pont – a Központ 113. § (4) bekezdése szerinti adatszolgáltatása alapján – háromhavonta összefoglaló jelentést nyújt be az ENISA-nak a bejelentett jelentős incidensekről, incidensekről, kiberfenyegetésekről és incidens közeli helyzetekről.

115. §

(1) Az adatszolgáltatási és tájékoztatási kötelezettség teljesítése során érzékeny információ csak akkor osztható meg az Európai Bizottsággal és más európai uniós szervekkel, ha az információcsere az (EU) 2022/2555 európai parlamenti és tanácsi irányelv alkalmazásához szükséges. A megosztott információnak az információcsere célja szempontjából lényeges és arányos mértékre kell korlátozódnia.
(2) Az információcsere során meg kell őrizni a rendelkezésre bocsátott információk bizalmas jellegét, és óvni kell az érintett szervezetek biztonsági és üzleti érdekeit.
(3) Az adatszolgáltatás és tájékoztatás keretében nem szolgáltatható olyan adat vagy információ, amely ellentétes lenne Magyarország nemzetbiztonsági, honvédelmi vagy alapvető biztonsági érdekeivel vagy azt sértené.

45. Európai szakértői értékelés

116. §

(1) A nemzeti kiberbiztonsági hatóság és a Központ – a Nemzeti Kiberbiztonsági Munkacsoport egyetértésével – kezdeményezhet és önkéntes alapon részt vehet az (EU) 2022/2555 európai parlamenti és tanácsi irányelv szerinti szakértői értékelésekben (a továbbiakban: európai szakértői értékelés). Az európai szakértői értékelés a következők legalább egyikéből áll:

a) az (EU) 2022/2555 európai parlamenti és tanácsi irányelv 21. és 23. cikkében említett kiberbiztonsági kockázatkezelési intézkedések és jelentéstételi kötelezettségek végrehajtásának szintje;

b) a képességek szintje, ideértve a rendelkezésre álló pénzügyi, technikai és humán erőforrásokat, valamint az illetékes hatóságok feladatai ellátásának hatékonyságát;

c) a CSIRT-ek műveleti képességei;

d) az (EU) 2022/2555 európai parlamenti és tanácsi irányelv 37. cikkében említett kölcsönös segítségnyújtás végrehajtási szintje;

e) az (EU) 2022/2555 európai parlamenti és tanácsi irányelv szerinti 29. cikkében említett kiberbiztonsági információmegosztási megállapodások végrehajtási szintje;

f) határokon vagy ágazatokon átnyúló jellegű konkrét kérdések.

(2) Az európai szakértői értékelést – a NIS Együttműködési Csoport által kidolgozott módszertan alapján – kiberbiztonsági szakértők végzik.

(3) A nemzeti kiberbiztonsági hatóság és a Központ az európai szakértői értékelés

a) kezdeményezése során konkrét kérdéseket határozhat meg az európai szakértői értékelés céljából,

b) megkezdése előtt értesíti a részt vevő tagállamokat az európai szakértői értékelés hatóköréről, beleértve a konkrét kérdéseket is,

c) megkezdése előtt – a NIS Együttműködési Csoport által közzétett módszertan alapján – önértékelést végezhet az értékelt szempontokról, és ezt az önértékelést átadhatja a kijelölt kiberbiztonsági szakértőknek,

d) során az értékelésben részt vevő szakértőt érintő összeférhetetlenség kockázatát az európai szakértői értékelés megkezdése előtt, illetve a tudomásszerzést követően haladéktalanul jelezi az érintett tagállamnak, a NIS Együttműködési Csoportnak, az Európai Bizottságnak és az ENISA-nak,

e) megkezdését megelőzően, illetve a tudomásszerzést követően – megfelelő indoklással ellátva – kifogást emelhet a szakértőt kijelölő tagállamnál a szakértő kijelölésével szemben,

f) eredményeként készített jelentés-tervezet vonatkozásában észrevételt tehet,

g) tárgyában készített jelentést vagy annak kivonatát honlapján közzéteheti.

117. §

(1) A más európai uniós tagállam által kezdeményezett európai szakértői értékelés esetén a Magyarország részéről delegálandó kiberbiztonsági szakértő kiválasztása során a NIS Együttműködési Csoport által kidolgozott módszertanban meghatározott szempontok figyelembevételével kell eljárni.

(2) Az európai értékelésben résztvevő szakértő

a) a NIS Együttműködési Csoport által kidolgozott magatartási kódexben meghatározottak szerint jár el,

b) az európai szakértői értékelés során kapott információkat kizárólag az értékelés végrehajtása érdekében használhatja fel,

c) az európai szakértői értékelés során kapott érzékeny vagy bizalmas információt nem közölheti harmadik személlyel,

d) köteles jelezni a személyével szemben fennálló összeférhetetlenséget okozó körülményeket a kijelölést megelőzően, illetve a körülmény felmerülését vagy tudomására jutását követően haladéktalanul,

e) az értékelést végző szakértőkkel közösen jelentést készít az európai szakértői értékelés eredményeiről és következtetéseiről.

XI. Fejezet

Záró rendelkezések

46. Hatályba léptető rendelkezések

118. §

(1) Ez a rendelet – a (2) bekezdésben foglalt kivétellel – 2025. január 1-jén lép hatályba.
(2) A 42.-44. §, a 46. §, a 47. §, a 144. §, a 2. melléklet, a 3. melléklet és a 4. melléklet az e rendelet kihirdetését követő 16. napon lép hatályba.

47. Átmeneti rendelkezések

119. §

(1) A központi szolgáltató a 15. § (3) bekezdésében foglalt kötelezettséget a 2025. év folyamán akként teljesíti, hogy a központi szolgáltatással kapcsolatos, 15. § (3) bekezdésében foglalt információkat a szolgáltatáskatalógus helyett a felhasználó szervezet számára elérhetővé teszi.
(2) Az SZTFH a 113. § (1) bekezdése szerinti adatszolgáltatást első alkalommal 2025. március 31-ig teljesíti az egyedüli kapcsolattartó pont felé.
(3) Az (EU) 2022/2554 európai parlamenti és tanácsi rendelet szerinti hatóság a 113. § (2) bekezdése szerinti adatszolgáltatást első alkalommal 2025. március 31-ig teljesíti az egyedüli kapcsolattartó pont felé.
(4) A nemzeti kiberbiztonsági hatóság a 113. § (3) bekezdés a) pontja szerinti adatszolgáltatást első alkalommal 2025. március 31-ig teljesíti az egyedüli kapcsolattartó pont felé.
(5) A Központ a 113. § (4) bekezdése szerinti adatszolgáltatást első alkalommal 2025. március 31-ig teljesíti az egyedüli kapcsolattartó pont felé.
(6) Az egyedüli kapcsolattartó pont
a) a 114. § (2) bekezdés a) és b) pontja szerinti adatszolgáltatást első alkalommal 2025. április 17-ig,
b) a 114. § (2) bekezdés d) pontja szerinti adatszolgáltatást 2025. április 17-ig,
c) a 114. § (3) bekezdése szerinti adatszolgáltatást első alkalommal 2025. április 17-ig
teljesíti.
(7) Az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet [a továbbiakban: 187/2015. (VII. 13.) Korm. rendelet] rendelkezései alapján folyamatban lévő hatósági ügyeket a nemzeti kiberbiztonsági hatóság a 187/2015. (VII. 13.) Korm. rendelet szerint zárja le.

48. Az Európai Unió jogának való megfelelés

120. §

(1) Ez a rendelet
a) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU)

2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) szóló, 2022. december 14-i (EU) 2022/2555 európai parlamenti és tanácsi irányelvnek, valamint

b) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről szóló 2022. december 14-i (EU) 2022/2557 európai parlamenti és tanácsi irányelvnek

való megfelelést szolgálja.

(2) Ez a rendelet

a) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) szóló, 2019. április 17-i (EU) 2019/881 európai parlamenti és tanácsi rendeletnek,

b) az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontnak és a nemzeti koordinációs központok hálózatának a létrehozásáról szóló, 2021. május 20-i (EU) 2021/887 európai parlamenti és tanácsi rendeletnek, valamint

c) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról szóló, 2022. december 14-i (EU) 2022/2554 európai parlamenti és tanácsi rendeletnek, valamint

d) a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, valamint a 168/2013/EU és az (EU) 2019/1020 rendelet, és az (EU) 2020/1828 irányelv módosításáról (a kiberrezilienciáról szóló rendelet) szóló, 2024. október 23-i (EU) 2024/2847 európai parlamenti és tanácsi rendeletnek

a végrehajtásához szükséges rendelkezéseket állapít meg.

49. Módosító rendelkezések

121. §

A villamos energiáról szóló 2007. évi LXXXVI. törvény egyes rendelkezéseinek végrehajtásáról szóló 273/2007. (X. 19.) Korm. rendelet 90. § (5) bekezdésében az „a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről” szövegrész helyébe a „Magyarország kiberbiztonságáról” szöveg lép.

122. §

A minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010. (V. 6.) Korm. rendelet 34/A. § (2) bekezdésében az „az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 19. § (1)–(3) bekezdése szerinti eseménykezelő” szövegrész helyébe a „Magyarország kiberbiztonságáról szóló törvény szerinti kiberbiztonsági incidenskezelő” szöveg lép.

123. §

A polgári légiközlekedés védelmének szabályairól és a Légiközlekedés Védelmi Bizottság jogköréről, feladatairól és működésének rendjéről szóló 169/2010. (V. 11.) Korm. rendelet a következő 47. §-sal egészül ki:

„47. §

Ez a rendelet az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az

(EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) szóló, 2022. december 14-i (EU) 2022/2555 európai parlamenti és tanácsi irányelvnek való megfelelést szolgálja.”

124. §

A polgári légiközlekedés védelmének szabályairól és a Légiközlekedés Védelmi Bizottság jogköréről, feladatairól és működésének rendjéről szóló 169/2010. (V. 11.) Korm. rendelet

a) 40/A. § (10) bekezdésében az „Az eseménykezelési” szövegrész helyébe az „A kiberbiztonsági incidenskezelési” szöveg és az „az eseménykezelést” szövegrész helyébe az „a kiberbiztonsági incidenskezelést” szöveg,

b) 1. melléklet 8.11.3. pontjában az „az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 13. § (8)” szövegrész helyébe az „a Magyarország kiberbiztonságáról szóló 2024. évi … törvény 11. § (3)” szöveg

lép.

125. §

A megújuló energiaforrásból és a nagy hatásfokú kapcsolt energiatermelésből nyert villamos energia származásának igazolásáról szóló 309/2013. (VIII. 16.) Korm. rendelet 2. § (2) bekezdésében az „az állami és önkormányzati szervek elektronikus információbiztonságáról” szövegrész helyébe az „a Magyarország kiberbiztonságáról” szöveg lép.

126. §

Hatályát veszti 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.

127. §

A támogatásból megvalósuló fejlesztések központi monitoringjáról és nyilvántartásáról szóló 60/2014. (III. 6.) Korm. rendelet

a) 2. § 1. pontjában az „az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L.” szövegrész helyébe a „Magyarország kiberbiztonságáról szóló” szöveg és az „Ibtv.” szövegrész helyébe a „Kiberbiztonsági tv.” szöveg,

b) 9/A. § (3) bekezdésében az „Ibtv.” szövegrész helyébe az „a Kiberbiztonsági tv.” szöveg

lép.

128. §

A pénzügyi intézmények, a biztosítók és a viszontbiztosítók, továbbá a befektetési vállalkozások és az árutőzsdei szolgáltatók informatikai rendszerének védelméről szóló 42/2015. (III. 12.) Korm. rendelet 5/A. § (12) bekezdésében az „az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet 22. § (5) bekezdése” szövegrész helyébe az „a Magyarország kiberbiztonságáról szóló 2024. évi ... törvény 57. § (1) bekezdés c) pontja” szöveg lép.

129. §

A nemzeti felsőoktatásról szóló 2011. évi CCIV. törvény egyes rendelkezéseinek végrehajtásáról szóló 87/2015. (IV. 9.) Korm. rendelet 2. melléklet 4. pont l) alpontjában az „az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről” szövegrész helyébe az „a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről” szöveg és a „3.” szövegrész helyébe a „jelentős” szöveg lép.

130. §

A központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) Korm. rendelet

a) 1. § b) pontjában az „az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.)” szövegrész helyébe az „a Magyarország kiberbiztonságáról szóló 2024. évi … törvény (a továbbiakban: Kiberbiztonsági tv.)” szöveg,

b) 2. § nyitó szövegrészében az „Az Ibtv. 11. § (2) és (3) bekezdése” szövegrész helyébe az „A Kiberbiztonsági tv. 6. § (6) bekezdése és 19. §-a” szöveg,

c) 2. § a) pont ab) alpontjában az „az Ibtv. 11. § (3) bekezdése” szövegrész helyébe az „a Kiberbiztonsági tv. 19. §-a” szöveg,

d) 2. § g) pont ga) alpontjában az „az Ibtv. 19. § (1)–(3) bekezdése” szövegrész helyébe az „a Kiberbiztonsági tv. 63. §-a” szöveg és az „eseménykezelő” szövegrész helyébe a „kiberbiztonsági incidenskezelő” szöveg,

e) 2. § g) pont gb) alpontjában a „biztonsági események” szövegrész helyébe a „kiberbiztonsági incidens” szöveg, az „az Ibtv. 19. § (1)–(3) bekezdése” szövegrész helyébe az „a Kiberbiztonsági tv. 63. §-a” szöveg és az „eseménykezelő” szövegrész helyébe a „kiberbiztonsági incidenskezelő” szöveg,

f) 2. § g) pont gc) alpontjában az „az Ibtv. 19. § (1)–(3) bekezdése szerinti eseménykezelő központok által végzett informatikai biztonsági eseménykezelésben a biztonsági eseményről szóló” szövegrész helyébe az „a Kiberbiztonsági tv. 62. §-a szerinti kiberbiztonsági incidenskezelő központok által végzett kiberbiztonsági incidenskezelésben” szöveg és az „az Ibtv. 19. § (1)–(3) bekezdése szerinti eseménykezelő” szövegrész helyébe az „a Kiberbiztonsági tv. 62. §-a szerinti kiberbiztonsági incidenskezelő” szöveg,

g) 3. § a) pontjában az „az Ibtv. 14. §” szövegrész helyébe az „a Kiberbiztonsági tv. 23. §” szöveg,

h) 3. § b) pontjában az „az Ibtv. 19. § (1)–(3) bekezdése” szövegrész helyébe az „a Kiberbiztonsági tv. 63. §-a” szöveg,

i) 3. § c) pontjában az „az Ibtv.” szövegrész helyébe az „a Kiberbiztonsági tv.” szöveg,

j) 4. § (1) bekezdésében az „az Ibtv. 19. §” szövegrész helyébe az „a Kiberbiztonsági tv. 62. §” szöveg, az „eseménykezelő” szövegrész helyébe a „kiberbiztonsági incidenskezelő” szöveg és az „eseménykezelési” szövegrészek helyébe az „incidenskezelési” szöveg

lép.

131. §

Hatályát veszti a 187/2015. (VII. 13.) Korm. rendelet.

132. §

Az egységes elektronikuskártya-kibocsátási keretrendszerről szóló 2014. évi LXXXIII. törvény végrehajtásáról szóló 304/2017. (X. 27.) Korm. rendelet 15. § (4) bekezdés c) pontjában az „az állami

és önkormányzati szervek elektronikus információbiztonságáról” szövegrész helyébe az „a Magyarország kiberbiztonságáról” szöveg lép.

133. §

A Kormányzati Adatközpont működéséről szóló 467/2017. (XII. 28.) Korm. rendelet 6. § (1) bekezdés d) pontjában az „az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L.” szövegrész helyébe az „a Magyarország kiberbiztonságáról szóló” szöveg és a „besorolási szinthez” szövegrész helyébe a „biztonsági osztályhoz” szöveg lép.

134. §

A Magyarország biztonsági érdekét sértő külföldi befektetések ellenőrzéséről szóló 2018. évi LVII. törvény végrehajtásáról szóló 246/2018. (XII. 17.) Korm. rendelet 1. melléklet 9. alcíme az alábbiak szerint módosul:

„9. Magyarország kiberbiztonságáról szóló 2024. évi … törvény 1. § (1) bekezdés a)–c) pontja szerinti szervezet, a Kszetv. alapján kritikus szervezetként kijelölt szervezet, valamint a Vbö. alapján az ország védelme és biztonsága szempontjából jelentős szervezetként kijelölt szervezet elektronikus információs rendszere vonatkozásában bejelentési kötelezettség alá tartozó tevékenységek

1. A Magyarország kiberbiztonságáról szóló 2024. évi … törvény (a továbbiakban: Kiberbiztonsági tv.) 1. § (1) bekezdés a)–c) pontja szerinti szervezet, a Kszetv. alapján kritikus szervezetként kijelölt szervezet, valamint a Vbö. alapján az ország védelme és biztonsága szempontjából jelentős szervezetként kijelölt szervezet elektronikus információs rendszere vonatkozásában a Kiberbiztonsági tv. 6. § (5) bekezdés d) pontja szerinti tevékenység végzése vagy az abban való közreműködés.
2. A Magyarország kiberbiztonságáról szóló 2024. évi … törvény (a továbbiakban: Kiberbiztonsági tv.) 1. § (1) bekezdés a)–c) pontja szerinti szervezet, a Kszetv. alapján kritikus szervezetként kijelölt szervezet, valamint a Vbö. alapján az ország védelme és biztonsága szempontjából jelentős szervezetként kijelölt szervezet elektronikus információs rendszere vonatkozásában a Kiberbiztonsági tv. szerinti sérülékenységvizsgálat elvégzése.”

135. §

Hatályát veszti az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről szóló 270/2018. (XII. 20.) Korm. rendelet.

136. §

Hatályát veszti az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól szóló 271/2018. (XII. 20.) Korm. rendelet.

137. §

Az egységes Állami Alkalmazás-fejlesztési Környezetről és az Állami Alkalmazás-katalógusról, valamint az egyes kapcsolódó kormányrendeletek módosításáról szóló 314/2018. (XII. 27.) Korm. rendelet

a) 9. § (4) bekezdés h) pontjában az „az állami és önkormányzati szervek elektronikus információbiztonságáról” szövegrész helyébe az „a Magyarország kiberbiztonságáról” szöveg,

b) 19. § (2) bekezdésében az „az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 5. és 6. §-ában” szövegrész helyébe az „a Magyarország kiberbiztonságáról szóló 2024. évi … törvényben (a továbbiakban: Kiberbiztonsági tv.)” szöveg,

c) 19. § (3) bekezdésében az „az Ibtv. 5. és 6. §-ában” szövegrész helyébe az „a Kiberbiztonsági tv.-ben” szöveg,

d) 19. § (4) bekezdésében az „az Ibtv.” szövegrész helyébe az „a Kiberbiztonsági tv.” szöveg,

e) 19. § (5) bekezdésében az „az Ibtv. 5. és 6. §-ában” szövegrész helyébe az „a Kiberbiztonsági tv.-ben” szöveg

lép.

138. §

Az elektronikus információbiztonsági korai figyelmeztető rendszerről szóló 214/2020. (V. 18.) Korm. rendelet 11. §-a helyébe a következő rendelkezés lép:

„11. §

Ez a rendelet az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) szóló, 2022. december 14-i (EU) 2022/2555 európai parlamenti és tanácsi irányelvnek való megfelelést szolgálja.”

139. §

Az elektronikus információbiztonsági korai figyelmeztető rendszerről szóló 214/2020. (V. 18.) Korm. rendelet 3. § (1) bekezdés a) pontja helyébe az alábbi rendelkezés lép:

(A korai figyelmeztető szolgáltatás igénybevételére jogosultak:)

„*a)* a Kiberbiztonsági tv. 1. § (1) bekezdés a)-c) pontjában meghatározott szervek – ide nem értve a a Kiberbiztonsági tv. szerinti honvédelmi kiberbiztonsági incidenskezelő központ által támogatott szerveket –,”

140. §

Az elektronikus információbiztonsági korai figyelmeztető rendszerről szóló 214/2020. (V. 18.) Korm. rendelet

a) 1. § f) pontjában az „az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 11. § (1) bekezdés c) pontja” szövegrész helyébe az „a Magyarország kiberbiztonságáról szóló 2024. évi ... törvény (a továbbiakban: Kiberbiztonsági tv.) 6. § (3) bekezdés 2. pontja” szöveg,

b) 1. § g) pontjában a „biztonsági eseményekre” szövegrész helyébe a „kiberbiztonsági incidensekre” szöveg,

c) 5. § (1) bekezdés c) pontjában a „biztonsági esemény” szövegrész helyébe a „kiberbiztonsági incidens” szöveg, az „az Ibtv. 19. § (1) bekezdése szerinti eseménykezelő” szövegrész helyébe

az „a Kiberbiztonsági tv. szerinti nemzeti kiberbiztonsági incidenskezelő” szöveg és az „az Ibtv. 19. § (2) bekezdése szerinti eseménykezelő” szövegrész helyébe az „a Kiberbiztonsági tv. szerinti honvédelmi kiberbiztonsági incidenskezelő” szöveg,

d) 6. § (2) bekezdés nyitó szövegrészében az „az Ibtv. 11. § (1) bekezdés c)” szövegrész helyébe az „a Kiberbiztonsági tv. 6. § (3) bekezdés 2.” szöveg,

e) 7. § (2) bekezdésében a „Biztonsági esemény” szövegrész helyébe a „Kiberbiztonsági incidens” szöveg és az „az Ibtv.-ben” szövegrész helyébe az „a Kiberbiztonsági tv.-ben” szöveg,

f) 9. § c) pontjában az „az Ibtv. 19. § (1) bekezdése szerinti eseménykezelő” szövegrész helyébe az „a Kiberbiztonsági tv. szerinti nemzeti kiberbiztonsági incidenskezelő” szöveg

lép.

141. §

Az adatok végleges hozzáférhetetlenné tételét lehetővé tevő alkalmazás biztosításával kapcsolatos eljárási szabályok meghatározásáról szóló 726/2020. (XII. 31.) Korm. rendelet

a) 11. § (2) bekezdés h) pontjában az „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 szóló 271/2018. (XII. 20.) Korm. rendelet 22. § (5) bekezdése” szövegrész helyébe a „Magyarország kiberbiztonságáról szóló 2024. évi ... törvény 57. § (2) bekezdés d) pontja” szöveg,

b) 11. § (3) bekezdés r) pontjában a „biztonsági eseményeket” szövegrész helyébe a „kiberbiztonsági incidenseket” szöveg

lép.

142. §

A Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet 191. §-ában a „nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 8. § (8) bekezdésében” szövegrész helyébe a „Magyarország kiberbiztonságáról szóló 2024. évi … törvény 69. § (1) bekezdésében” szöveg lép.

143. §

A honvédelemről és a Magyar Honvédségről szóló törvény egyes rendelkezéseinek végrehajtásáról szóló 614/2022. (XII. 29.) Korm. rendelet 44. §-ában az „az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény 19. § (1) bekezdésében meghatározott eseménykezelő” szövegrész helyébe az „a Magyarország kiberbiztonságáról szóló törvény szerinti honvédelmi kiberbiztonsági incidenskezelő” szöveg lép.

144. §

Hatályát veszti a kiberbiztonsági bírságok mértékéről, a bírság kiszabásának és befizetésének részletes eljárási szabályairól szóló 305/2023. (VII. 11.) Korm. rendelet.

145. §

A honvédelmi célú elektronikus információs rendszerek korai figyelmeztető rendszeréről szóló 578/2023. (XII. 19.) Korm. rendelet 2. § 14. pontja helyébe a következő rendelkezés lép:
(E rendelet alkalmazásában)

„*14. szakfeladat szerint elkülönülő* incidenskezelő *központ:* Magyarország kiberbiztonságáról szóló törvény végrehajtásáról szóló kormányrendelet szerinti szakfeladat szerint elkülönülő incidenskezelő központ,”

146. §

A honvédelmi célú elektronikus információs rendszerek korai figyelmeztető rendszeréről szóló 578/2023. (XII. 19.) Korm. rendelet

a) 2. § 7. pontjában a „biztonsági esemény” szövegrész helyébe a „kiberbiztonsági incidens” szöveg,

b) 4. § (3) bekezdésében az „eseménykezelő” szövegrész helyébe az „incidenskezelő” szöveg,

c) 4. § (4) bekezdésében az „eseménykezelő” szövegrészek helyébe az „incidenskezelő” szöveg,

d) 12. § (1) bekezdés a) pontjában az „eseménykezelő” szövegrész helyébe az „incidenskezelő” szöveg,

e) 12. § (3) bekezdésében az „eseménykezelő” szövegrészek helyébe az „incidenskezelő” szöveg,

f) 12. § (4) bekezdésében az „eseménykezelő” szövegrész helyébe az „incidenskezelő” szöveg

lép.

147. §

A hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsításról szóló 608/2023. (XII. 22.) Korm. rendelet 1. § 1. pontja helyébe a következő rendelkezés lép:

(E rendelet alkalmazásában)

„*1.* kiberbiztonsági incidenskezelő központ: a Magyarország kiberbiztonságáról szóló 2024. évi ... törvény (a továbbiakban: Kiberbiztonsági tv.) szerinti honvédelmi kiberbiztonsági incidenskezelő központ,”

148. §

A hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsításról szóló 608/2023. (XII. 22.) Korm. rendelet 3. §-a helyébe a következő rendelkezés lép:

„3. §

A Kiberbiztonsági tv. alapján a hadipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsító hatósági feladatok tekintetében a Kormány által kijelölt hatóság (a továbbiakban: tanúsító hatóság) tanúsításfelügyeleti tevékenységet európai vagy nemzeti kiberbiztonsági tanúsítási rendszer hatálya alá tartozó hadiipari IKT-termék, hadiipari IKT-szolgáltatás vagy hadiipari IKT-folyamat vonatkozásában végez. A tanúsító hatóság hatásköre a Magyarországon letelepedett gyártó, illetve megfelelőségértékelő szervezet tevékenységére terjed ki.”

149. §

A hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsításról szóló 608/2023. (XII. 22.) Korm. rendelet

a) 8. § (1) bekezdésében a „Kibertan.tv. 12. §-a” szövegrész helyébe a „Kiberbiztonsági tv. 44. § (1) bekezdése” szöveg,

b) 11. § (2) bekezdésében a „Kibertan.tv. 5. §” szövegrész helyébe a „Kiberbiztonsági tv. 46. §” szöveg,

c) 12. § (1) bekezdésében a „Kibertan.tv. 13. §” szövegrész helyébe a „Kiberbiztonsági tv. 47. §” szöveg,
d) 12. § (3) bekezdés d) pontjában az „az Ibtv.” szövegrész helyébe az „a Kiberbiztonsági tv.” szöveg,
e) 18. § (1) bekezdés nyitó szövegrészében a „Kibertan.tv. 14. §” szövegrész helyébe a „Kiberbiztonsági tv. 48. §” szöveg,
f) 22. § (5) bekezdésében a „Kibertan.tv. 5. §” szövegrész helyébe a „Kiberbiztonsági tv. 46. §” szöveg,
g) 23. § (2) bekezdésében a „Kibertan.tv. 5. §” szövegrész helyébe a „Kiberbiztonsági tv. 46. §” szöveg,
h) 26. § (4) bekezdésében a „Kibertan.tv. 5. §” szövegrész helyébe a „Kiberbiztonsági tv. 46. §” szöveg,
i) 36. §-ában az „az eseménykezelő” szövegrész helyébe az „a kiberbiztonsági incidenskezelő” szöveg

lép.

150. §

Hatályát veszti a hadiipari kutatással, fejlesztéssel, gyártással és kereskedelemmel összefüggő kiberbiztonsági tanúsításról szóló 608/2023. (XII. 22.) Korm. rendelet 2. §-a.

151. §

A megújuló gázok származásának igazolásáról szóló 215/2024. (VII. 29.) Korm. rendelet 2. § (2) bekezdésében az „az állami és önkormányzati szervek elektronikus információbiztonságáról” szövegrész helyébe az „a Magyarország kiberbiztonságáról” szöveg lép.

152. §

A digitális állampolgárság egyes szabályairól szóló 321/2024. (XI. 6.) Korm. rendelet 60. § (3) bekezdés e) pontjában az „az állami és önkormányzati szervek elektronikus információbiztonságáról” szövegrész helyébe a „Magyarország kiberbiztonságáról” szöveg és a „biztonsági esemény” szövegrész helyébe a „kiberbiztonsági incidens” szöveg lép.

153. §

A digitális szolgáltatások, a digitális állampolgárság szolgáltatások és támogató szolgáltatások részletes műszaki követelményeiről szóló 322/2024. (XI. 6.) Korm. rendelet
a) 144. § (3) bekezdés a) pontjában az „a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről” szövegrész helyébe a „Magyarország kiberbiztonságáról” szöveg,
b) 144. § (7) bekezdésében a „kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről” szövegrész helyébe a „Magyarország kiberbiztonságáról” szöveg

lép.

1. melléklet a .../2024. (...) Korm. rendelethez

Az adatosztályozás végrehajtásához irányadó szempontok

1. Alapvető cél

Az adatok osztályozásának célja, hogy az elektronikus információs rendszerben kezelt adatok bizalmasság, sértetlenség és rendelkezésre állás szempontjából értékelésre kerüljenek és azok biztonsági súlyának megfelelően kerüljön kialakításra a kockázatarányos védelem. Az adatosztályozás emellett hozzájárul az elektronikus információs rendszerben kezelt adatok külföldön vagy felhőben történő kezelésének egyértelmű meghatározásához.

2. Az adatok bizalmasság szerinti besorolása

2.1. B1 szintű adatok

Ezen adatok bizalmasságának sérülése vagy elvesztése nem, vagy csak elhanyagolható mértékű anyagi vagy reputációs veszteséget okozhat a szervezetnek

2.2. B2 szintű adatok

Ezen adatok bizalmasságának sérülése vagy elvesztése csak kis mértékben okozhat anyagi vagy reputációs veszteséget a szervezetnek

2.3. B3 szintű adatok

Ezen adatok bizalmasságának sérülése vagy elvesztése jelentős anyagi vagy reputációs veszteséget okozhat a szervezetnek.

2.4. B4 szintű adatok

Ezen adatok bizalmasságának sérülése vagy elvesztése kritikus mértékű anyagi vagy reputációs veszteséget okozhat a szervezetnek.

3. Az adatok sértetlenség és rendelkezésre állás szerinti értékelése

3.1. SR1: az adatok **SÉRTETLENSÉGE VAGY RENDELKEZÉSRE ÁLLÁSA NEM KRITIKUS**

Az elektronikus információs rendszeren tárolt és kezelt adatok sértetlenségének vagy rendelkezésre állásának sérülése vagy elvesztése a szervezetnek vagy más személynek nem, vagy csak elhanyagolható mértékben okozhat anyagi vagy reputációs veszteséget.

3.2. SR2: az adatok **SÉRTETLENSÉGE VAGY RENDELKEZÉSRE ÁLLÁSA KRITIKUS**

Az elektronikus információs rendszeren tárolt és kezelt adatok sértetlenségének vagy rendelkezésre állásának sérülése vagy elvesztése a szervezetnek vagy más személynek jelentős, vagy kritikus mértékű anyagi vagy reputációs veszteséget okozhat.

4.Az adatosztályozás eredménye

4.1. Titkosítás

A B2 szintű adatok esetén: **ha technológiai szempontból lehetséges,** gondoskodni kell a titkosításról, amennyiben külföldi adatkezelés vagy nem privát felhőszolgáltatás igénybevétele valósul meg.

A **B3-4** szintű adatok esetén: **minden esetben** gondoskodni kell a titkosításról, amennyiben külföldi adatkezelés vagy nem privát felhőszolgáltatás igénybevétele valósul meg.

4.2. Az adatkezelés helyszíne

4.2.1. SR2 besorolású adatok esetén: Ha jogszabály másként nem rendelkezik, az adatok kezelésére földrajzi korlátozással kerülhet sor. Az adatok csak EGT-tagállam területén tárolhatók. Külföldi adattárolás esetén egyidejűleg gondoskodni kell az adatnak Magyarország területén való rendelkezésre állásáról is.
4.2.2. A 4.2.1. alpontban foglaltakon túl az adatkezelés lehetséges helyszínének meghatározásához összeadandó az adat B és SR kategóriájának megnevezésében szereplő számértéke. Ha jogszabály másként nem rendelkezik, a kapott eredmény alapján az adatok az alábbi F1-F4 kategóriákba sorolhatók, melyekre a következő előírások alkalmazandók:
4.2.2.1. F1: ha a B és SR összesített értéke: 2
Az F1 besorolású adatok
- földrajzi korlátozás nélkül,
- nem privát felhőszolgáltatás igénybevétele esetén: korlátozás nélkül
kezelhetők és tárolhatók.
4.2.2.2. F2: ha a B és SR összesített értéke: 3
Az F2 besorolású adatok
- SR1 besorolású adatok esetén földrajzi korlátozás nélkül, SR2 besorolású adatok esetén kizárólag EGT tagállam területén,
- nem privát felhőszolgáltatás igénybevétele esetén:
- EGT tagállam területén kívül kizárólag harmadik fél által tanúsított nem privát felhőben, vagy
- EGT tagállam területén belül akár nem tanúsított nem privát felhőben is
kezelhetők és tárolhatók.
4.2.2.3. F3: ha a B és SR összesített értéke: 4
Az F3 besorolású adatok
- kizárólag EGT tagállam területén belül
- nem privát felhőszolgáltatás igénybevétele esetén:
- harmadik fél által tanúsított nem privát felhőben, vagy
- nem tanúsított nem privát felhőszolgáltatás igénybevétele esetén kizárólag Magyarország területén kezelhetők és tárolhatók.
4.2.2.4. F4: ha a B és SR összesített értéke: 5 vagy 6
Az F4 besorolású adatok
- kizárólag Magyarország területén,
- nem privát felhőszolgáltatás igénybevétele esetén:
- harmadik fél által tanúsított privát felhőben vagy
- kormányzati felhőben kezelhetők.

	A	B	C
1	**B1**	F1	F2
2	**B2**	F2	F3
3	**B3**	F3	F4
4	**B4**	F4	F4

2. melléklet a .../2024. (...) Korm. rendelethez

A Kiberbiztonsági tv. 1. § (1) bekezdés a)-c) pontja szerinti szervezettel szemben kiszabható kiberbiztonsági bírság mértéke

	A	B	C
1	**A jogszabálysértés megnevezése**	**A bírság legkisebb mértéke (forint)**	**A bírság legnagyobb mértéke (forint)**
2	az elektronikus információs rendszer biztonságáért felelős személy hatósági nyilvántartásba vételére irányuló kérelem benyújtásának elmulasztása	200.000	2.000.000
3	információbiztonsági szabályzat hatósági nyilvántartásba vételére irányuló kérelem benyújtásának elmulasztása	200.000	2.000.000
4	biztonsági osztályba sorolási kötelezettség elmulasztása	200.000	4.000.000
5	az elektronikus információs rendszer biztonságáért felelős személy adatainak módosítására irányuló kérelem benyújtásának elmulasztása	200.000	2.000.000
6	alapvető kiberhigiéniai gyakorlatok és kiberbiztonsági képzések szervezése vagy az ezeken való részvétel igazolásának elmulasztása	400.000	4.000.000
7	eseménykezelő központtal való együttműködési kötelezettség elmulasztása	500.000	50.000.000
8	a nemzeti kiberbiztonsági hatóság vagy a sérülékenységvizsgálat végzésére jogosult állami szerv által elrendelt sérülékenységvizsgálati, illetve esemény kivizsgálási kötelezettség elmulasztása	500.000	50.000.000
9	a nemzeti kiberbiztonsági hatóság által jóváhagyott sérülékenységkezelési terv szervezet általi végrehajtásának elmulasztása	200.000	10.000.000
10	arányos biztonsági intézkedések bevezetésének és alkalmazásának elmulasztása	200.000	10.000.000

11	a kiberbiztonsági incidens bejelentésének elmulasztása	500.000	5.000.000
12	a szervezet által nyújtott szolgáltatás igénybe vevői, illetve az egyéb érintettek részére elrendelt tájékoztatási kötelezettség elmulasztása	2.000.000	20.000.000
13	zárójelentés elkészítésnek elmulasztása, illetve nem megfelelő módon történő teljesítése	500.000	5.000.000
14	a nemzeti kiberbiztonsági hatóság végleges, végrehajtható határozatában foglalt kötelezésének nem teljesítése	1.000.000	50.000.000
15	az információbiztonsági felügyelővel való együttműködés elmulasztása	1.000.000	40.000.000
16	közvetítő szolgáltató együttműködési kötelezettségének megszegése	1.000.000	40.000.000
17	a Kiberbiztonsági tv. 1. § (1) bekezdés b) pontja hatálya alá tartozó, és egyidejűleg a Kiberbiztonsági tv. 2. és 3. melléklet szerinti szervezetnek minősülő szervezet esetében a Kiberbiztonsági tv. 8. § (5) bekezdése szerinti nyilvántartásba vétel érdekében történő adatszolgáltatás nem teljesítése	a Kiberbiztonsági tv. 1. § (1) bekezdés b) pontja hatálya alá tartozó, és egyidejűleg a Kiberbiztonsági tv. 2. és 3. melléklet szerinti szervezetnek minősülő szervezet előző üzleti évi nettó árbevételének – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének –, vagy előző évi költségvetési bevételi előirányzatának 0,5%-a, de legalább 1 000 000 forint	a Kiberbiztonsági tv. 1. § (1) bekezdés b) pontja hatálya alá tartozó, és egyidejűleg a Kiberbiztonsági tv. 2. és 3. melléklet szerinti szervezetnek minősülő szervezet előző üzleti évi nettó árbevételének – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének –, vagy előző évi költségvetési bevételi előirányzatának legfeljebb 2%-a, de legfeljebb 150 000 000 forint
18	a Kiberbiztonsági tv. 1. § (1) bekezdés b) pontja hatálya alá tartozó, és egyidejűleg a Kiberbiztonsági tv. 2. és 3. melléklet szerinti szervezetnek minősülő szervezet esetében a Kiberbiztonsági tv. 8. § (5) bekezdése szerinti nyilvántartásba vétel érdekében történő	50 000 forint	a Kiberbiztonsági tv. 1. § (1) bekezdés b) pontja hatálya alá tartozó, és egyidejűleg a Kiberbiztonsági tv. 2. és 3. melléklet szerinti szervezetnek minősülő szervezet előző üzleti évi nettó árbevételének

	adatszolgáltatás határidőn túl történő teljesítése		– árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének – vagy előző évi költségvetési bevételi előirányzatának legfeljebb 0,1%-a, de legfeljebb 15 000 000 forint
19	a Kiberbiztonsági tv. 1. § (1) bekezdés b) pontja hatálya alá tartozó, és egyidejűleg a Kiberbiztonsági tv. 2. és 3. melléklet szerinti szervezetnek minősülő szervezet esetében a Kiberbiztonsági tv. 7. § (1) bekezdése szerinti felügyeleti díjfizetés elmulasztása	500 000 forint	a kiberbiztonsági éves felügyeleti díj maximum tízszerese
20	a Kiberbiztonsági tv. 1. § (1) bekezdés b) pontja hatálya alá tartozó, és egyidejűleg a Kiberbiztonsági tv. 2. és 3. melléklet szerinti szervezetnek minősülő szervezet esetében a Kiberbiztonsági tv. 8. § (3) bekezdése szerinti adatváltozás megküldésének elmulasztása	50 000 forint	1 000 000 forint
22	a Kiberbiztonsági tv. 1. § (1) bekezdés b) pontja hatálya alá tartozó, és egyidejűleg a Kiberbiztonsági tv. 2. és 3. melléklet szerinti szervezetnek minősülő szervezet esetében a Kiberbiztonsági tv. 16. § (1) bekezdése szerinti kiberbiztonsági audit határidőn belüli lefolytatásának elmulasztása	1 000 000 forint	50 000 000 forint

3. melléklet a .../2024. (...) Korm. rendelethez

A Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti szervezettel szemben kiszabható kiberbiztonsági bírság mértéke

	A	B	C
1	A szabálytalanság megnevezése	A bírság legkisebb mértéke	A bírság legnagyobb mértéke
2	A Kiberbiztonsági tv. 8. § (5) bekezdése szerinti nyilvántartásba vétel érdekében történő adatszolgáltatás nem teljesítése	a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti szervezet előző üzleti évi nettó árbevételének - árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének -, vagy előző évi költségvetési bevételi előirányzatának 0,5%-a, de legalább 1 000 000 forint	a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti szervezet előző üzleti évi nettó árbevételének – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének –, vagy előző évi költségvetési bevételi előirányzatának legfeljebb 2%-a, de legfeljebb 150 000 000 forint
3	A Kiberbiztonsági tv. 8. § (5) bekezdése szerinti nyilvántartásba vétel érdekében történő adatszolgáltatás határidőn túl történő teljesítése	50 000 forint	a a Kiberbiztonsági tv. 1. § (1) bekezdés d) és e) pontja szerinti szervezet előző üzleti évi nettó árbevételének – árbevétel hiányában a tárgyévi árbevétel egész évre vetített időarányos részének – vagy előző évi költségvetési bevételi előirányzatának legfeljebb 0,1%-a, de legfeljebb 15 000 000 forint
4	A Kiberbiztonsági tv. 7. § (1) bekezdése szerinti felügyeleti díjfizetés elmulasztása	500 000 forint	a kiberbiztonsági éves felügyeleti díj maximum tízszerese
5	A Kiberbiztonsági tv. 8. § (3) bekezdése szerinti adatváltozás megküldésének elmulasztása	50 000 forint	1 000 000 forint
6	A Kiberbiztonsági tv. 6. § (2) bekezdése szerinti kötelezettség nem teljesítése	1 000 000 forint	42. § (2) bekezdése szerinti összeg
7	A Kiberbiztonsági tv. 16. § (1) bekezdése szerinti kiberbiztonsági audit határidőn belüli lefolytatásának elmulasztása	1 000 000 forint	50 000 000 forint

4. melléklet a .../2024. (...) Korm. rendelethez

A tanúsító hatóság által kiszabható bírság mértéke

	A	B	C
1	A szabálytalanság megnevezése	A bírság legkisebb mértéke forintban meghatározva	A bírság legnagyobb mértéke forintban meghatározva
2	Megfelelőségi önértékelés esetén az uniós megfelelőségi nyilatkozatnak az (EU) 2019/881 európai parlamenti és tanácsi rendelet 53. cikk (3) bekezdésében előírt megküldési kötelezettség nemteljesítése a tanúsító hatóság és az Európai Uniós Kiberbiztonsági Ügynökség részére	50 000	100 000
3	Megfelelőségi önértékelés esetén a Kiberbiztonsági tv. 43. § (3) bekezdésében előírt dokumentumok megküldésére vonatkozó kötelezettség nemteljesítése a tanúsító hatóság részére	50 000	100 000
4	A Kiberbiztonsági tv. 44. § (1) bekezdésében foglalt feltételeknek nem megfelelő szervezet általi megfelelőségértékelési tevékenység végzése	1 000 000	50 000 000
5	Megfelelőségi jelölés Kiberbiztonsági tv. 42. § (2) bekezdése szerinti jogosulatlan használata	300 000	50 000 000
6	A Kiberbiztonsági tv. 48. § (5) bekezdése szerinti adatszolgáltatás elmulasztása	50 000	5 000 000
7	A Kiberbiztonsági tv. 41. § (3) bekezdésében meghatározott, a sebezhetőség vagy rendellenesség bejelentésére irányuló kötelezettség teljesítésének elmulasztása	300 000	5 000 000
8	Az A:2-A:7 mezőben nem szereplő, a tanúsító hatóság által feltárt, a Kiberbiztonsági tv. 49. § (1) bekezdése szerinti hiányosságok alapján a szükséges módosítások végrehajtásának, intézkedések megtételének elmulasztása	200 000	10 000 000