271/2018. (XII. 20.) Korm. rendelet

az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének és műszaki vizsgálatának, továbbá a sérülékenységvizsgálat lefolytatásának szabályairól

A Kormány

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

az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 17. § (1a) bekezdés *b)* és *c)* pontjában kapott felhatalmazás alapján,

az Alaptörvény 15. cikk (1) bekezdésében meghatározott feladatkörében eljárva a következőket rendeli el:

1. Értelmező rendelkezések

1. § E rendelet alkalmazásában

1. *adminisztrátori jogosultsággal rendelkező informatikai biztonsági vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek a során a vizsgálatot végző személy rendszergazdai jogosultsággal rendelkezik, és az eljárás célja, hogy megfelelőségi listák alapján az érintett szervezet teljes informatikai rendszerének az állapota ellenőrzésre kerüljön;
2. *alapvető szolgáltatást nyújtó szolgáltató:* a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény (a továbbiakban: Lrtv.) alapján alapvető szolgáltatást nyújtóként azonosított szolgáltató;
3. *automatizált vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek a során az érintett szervezet informatikai rendszerének a sérülékenységei célszoftverek segítségével kerülnek feltérképezésre;
4. *bejelentés-köteles szolgáltatást nyújtó:* az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (a továbbiakban: Ekertv.) 2. § *j)* pontja szerinti szolgáltatást nyújtó szolgáltató;
5. *belső informatikai biztonsági vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek a során az érintett szervezet informatikai rendszerének sérülékenységvizsgálata a belső hálózati végpontról közvetlenül történik;
6. *biztonságiesemény-kezelési megbízott:* az érintett szervezet vezetője által a biztonsági események kivizsgálásával az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (a továbbiakban: Ibtv.) 11. § (6) bekezdése szerint megbízott személy;
7. *célszoftver:* a biztonsági vizsgálati eljárás során a sérülékenységvizsgálat egyes fázisainak végrehajtására kifejlesztett szoftver;

8. *CSIRT-ek hálózata:* a tagállami számítógép-biztonsági eseményekre reagáló szerveknek a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-i (EU) 2016/1148 európai parlamenti és tanácsi irányelv által létrehozott hálózata;

9. *érintett szervezet:* a biztonsági vizsgálattal vagy sérülékenységvizsgálattal érintett, elektronikus információs rendszert üzemeltető szervezet;

9a.[1] *felhasználói dokumentáció:* a vizsgálandó informatikai rendszer, illetve szolgáltatás rövid összefoglaló leírását, továbbá a funkcióinak részletezett használati leírását tartalmazó dokumentum;

9b.[2] *felhasználói jogosultság mátrix:* a vizsgálandó informatikai rendszer, illetve szolgáltatás felhasználóinak jogosultságait, a jogosultságok tekintetében alkalmazott szinteket és ezek közötti átjárhatóság feltételeit ismertető dokumentum;

9c.[3] *funkció-tesztelési terv:* a vizsgálandó informatikai rendszer, illetve szolgáltatás egyes funkcióinak részletes tesztelési folyamatát vagy egy végrehajtott tesztelés eredményeit rögzítő dokumentum;

10. *kézi informatikai biztonsági vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek a során az érintett szervezet informatikai rendszerének sérülékenységei a vizsgálatot végző személy által egyedileg, manuálisan összeállított lekérdezések alkalmazásával kerülnek feltérképezésre;

11. *közvetítő szolgáltató:* az Ekertv. 2. § *l)* pontja szerinti szolgáltató;

12. *külső informatikai biztonsági vizsgálat:* az informatikai rendszer internet felőli, külső sérülékenységvizsgálata, amelynek a során az interneten fellelhető, nyilvános adatbázisokban való szabad keresésre, célzott információgyűjtésre, valamint az elérhető számítógépek szolgáltatásainak, sebezhetőségének feltérképezésére kerül sor;

13. *regisztrált felhasználói jogosultság nélküli informatikai biztonsági vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek a során a vizsgálatot végző személy semmilyen előzetes információval nem rendelkezik az érintett szervezet informatikai rendszeréről, és nincs felhasználói jogosultsága a rendszerhez;

14. *regisztrált felhasználói jogosultsággal rendelkező informatikai biztonsági vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek a során a vizsgálatot végző személy a számára külön létrehozott felhasználói jogosultsággal végzi a vizsgálatot;

15. *pszichológiai manipuláció:* olyan tevékenységi forma, technikák és módszerek összessége, amely az emberek befolyásolására alapozva teszi lehetővé bizalmas információk megszerzését vagy kártékony program terjedését és működését;

15a.[4] *rendszerterv:* a rendszerismertető leírást, a fejlesztési, a megvalósítási és üzemeltetési dokumentációt, továbbá az érintett rendszer, illetve szolgáltatás bevezetésére, üzembe helyezésére vonatkozó terveket naprakészen tartalmazó dokumentum;

16. *titkosítási eljárás:* olyan eljárás, amely az adat megismerhetőségét azáltal korlátozza, hogy az adat egy algoritmus segítségével átalakításra kerül olyan jelsorozattá, ami olvashatatlan annak a számára, aki nem rendelkezik a visszaalakításhoz szükséges egyedi jelsorozatból álló kulccsal;

---

1 *Beiktatta: 375/2020. (VII. 30.) Korm. rendelet 105. § (1). Hatályos: 2020. VII. 31-től.*
2 *Beiktatta: 375/2020. (VII. 30.) Korm. rendelet 105. § (1). Hatályos: 2020. VII. 31-től.*
3 *Beiktatta: 375/2020. (VII. 30.) Korm. rendelet 105. § (1). Hatályos: 2020. VII. 31-től.*
4 *Beiktatta: 375/2020. (VII. 30.) Korm. rendelet 105. § (2). Hatályos: 2020. VII. 31-től.*

17. *titkosítási kulcs:* titkosítási eljárás során alkalmazott olyan jelsorozat, amelynek az ismeretében a titkosított állomány megismerhető;

18. *webes vizsgálat:* olyan biztonsági vizsgálati eljárás, amelynek a során automatizált és kézi vizsgálatok útján kerülnek feltárásra a webes alkalmazások sérülékenységei;

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

2. A Központ feladat- és hatásköre

2. § A Kormány az Ibtv. 19. § (1) bekezdése, valamint az Ekertv. 6/B. § (1) bekezdése alapján eseménykezelő központként (a továbbiakban: Központ) a Nemzetbiztonsági Szakszolgálatot jelöli ki.

3. § (1) A Központ kezeli

a)[1] az Ibtv. 2. §-ában - az Ibtv. 19. § (2) bekezdése szerinti kivétellel - meghatározott szervek nyílt,

b) a bejelentés-köteles szolgáltatók,

c) a honvédelmi létfontosságú rendszerelemek kivételével az európai vagy nemzeti létfontosságú rendszerelemmé kijelölt létfontosságú rendszerelemeket működtetők,

d) a központosított informatikai és elektronikus hírközlési szolgáltató elektronikus információs rendszereit érintő biztonsági eseményeket és fenyegetéseket.

(2) A Központ a biztonsági események és fenyegetések kezelése céljából együttműködik

a) az elektronikus információs rendszerek felügyeletére kijelölt hatóságokkal,

b)[2] az Ibtv. 19. § (2) bekezdése szerinti eseménykezelő központtal (a továbbiakban: eseménykezelő központ),

c) a rendvédelmi szervekkel,

d) a Nemzeti Média- és Hírközlési Hatósággal és az általa működtetett Országos Informatikai és Hírközlési Főügyelettel,

e) az elektronikus hírközlési szolgáltatókkal, a központosított informatikai és elektronikus hírközlési szolgáltatóval,

f) az Lrtv. szerinti üzemeltetőkkel, kijelölő és javaslattevő hatóságokkal, valamint

g) a Nemzeti Adatvédelmi és Információszabadság Hatósággal.

(3) A Központ a hatáskörébe tartozó elektronikus információs rendszerek tekintetében részt vesz a CSIRT-ek hálózatának tevékenységében.

(4) A Központ a biztonsági eseményre vagy fenyegetésre utaló tevékenységeket kivizsgálja, és szükség esetén figyelmeztetést ad ki a felhasználók, az eseménykezelő központok, a hatóságok, 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 szerinti egyedüli kapcsolattartó pont (a továbbiakban: egyedüli kapcsolattartó pont), valamint az (1) bekezdés szerinti szervek felé.

---

1 *Módosította: 375/2020. (VII. 30.) Korm. rendelet 114. § a).*
2 *Módosította: 375/2020. (VII. 30.) Korm. rendelet 114. § b).*

(5) A Központ tájékoztatja az egyedüli kapcsolattartó pontot a biztonsági események kezelésére vonatkozó, jogszabályban nem részletezett eljárásrendjéről.

(6) A Központ ellátja az alábbi feladatokat:

a) a biztonsági események nemzeti szintű nyomon követése;

b) a kockázatokkal és biztonsági eseményekkel kapcsolatos tájékoztatás, korai előrejelzés, riasztás, bejelentéstétel és információterjesztés az érdekeltek számára;

c) reagálás a biztonsági eseményekre;

d) dinamikus kockázat- és eseményelemzések, valamint a biztonsági eseményekkel kapcsolatos helyzetkép készítése;

e) sérülékenységvizsgálat lefolytatása.

(7) A Központ meghatározza a biztonsági események és kockázatok kezelésére vonatkozó eljárásokat, valamint a biztonsági események, kockázatok és információk osztályozására szolgáló eljárásokat és szabályokat. Ennek során a Központ együttműködik az (1) bekezdésben meghatározott szervezetekkel.

4. § A Központ a biztonságiesemény-kezelési feladatkörében felelős

a) a tudomására jutott biztonsági eseményekről az érintettek haladéktalan értesítéséért,

b) a biztonsági eseményekről nyilvántartás vezetéséért, amely tartalmazza a biztonsági esemény kapcsán megtett intézkedéseket és azok eredményét, valamint

c) a külön kormányrendelet szerinti korai figyelmeztető rendszer működtetéséért.

5. § (1) A Központ a biztonsági események megelőzése céljából a 3. § (1) bekezdése szerinti szervezetek elektronikus információs rendszereit érintő fenyegetésekkel összefüggő tájékoztatási és tudatosítási feladatokat a (2)-(4) bekezdésben meghatározottak szerint látja el.

(2) A Központ az elektronikus információs rendszereket veszélyeztető sérülékenységekkel és fenyegető kockázatokkal összefüggésben felelős

a) az elektronikus információs rendszerek biztonságáért felelős személyek tájékoztatásáért,

b) a hatóságok és az eseménykezelő központok tájékoztatásáért, valamint

c) a sérülékenységekről és fenyegetésekről, valamint a javasolt biztonsági intézkedésekről a honlapján rendszeres tájékoztatásnyújtásáért.

(3) A Központ

a) elemzéseket, jelentéseket készít a magyar és a nemzetközi információbiztonsági irányokról,

b) a hatáskörébe tartozó biztonsági eseményekről negyedévente jelentést tesz a Nemzeti Kiberbiztonsági Koordinációs Tanács részére, valamint

c) évente jelentést készít a tevékenységéről a polgári nemzetbiztonsági szolgálatokért felelős miniszter részére.

(4) A Központ

a) nem kötelező érvényű állásfoglalásokat, ajánlásokat adhat ki,

b) a biztonsági események kezelésére irányuló tájékoztatót tarthat, részt vehet az információbiztonság tudatosításáért felelős intézmények tudatosítási programjában, szakértői-oktatói tevékenységet végezhet,

c) kormányzati információtechnológiai és biztonságiesemény-kezelési együttműködési fórumot működtethet, valamint

d) részt vesz az infokommunikációs biztonságra vonatkozó stratégiák és szabályozások előkészítésében.

3. Az eseménykezelő központok feladat- és hatásköre

6. § (1) A Kormány az Ibtv. 19. § (2) bekezdése alapján a honvédelmi célú elektronikus információs rendszereket érintő biztonsági események és fenyegetések kezelésére a Katonai Nemzetbiztonsági Szolgálatot jelöli ki. A Katonai Nemzetbiztonsági Szolgálat a biztonsági események és fenyegetések kezelését a szakmai irányítása és koordinálása alatt álló, szakfeladat szerint elkülönülő - a honvédelemért felelős miniszter irányítása, vezetése alatt álló szervnél, szervezetnél működő - eseménykezelő központokkal együtt látja el.

(2)[1]

(3)[2] Az eseménykezelő központ a hatáskörébe tartozó elektronikus információs rendszerek tekintetében

a) biztonságiesemény-kezelési feladatkörében ellátja a Központ 4. § szerinti,

b) tájékoztatási feladatkörében ellátja a Központ 5. § (2) bekezdés *b)* pontja és 5. § (3) bekezdés *c)* pontja szerinti,

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

feladatait.

(4)[3] Az eseménykezelő központ az 5. § (3) bekezdés *c)* pontja szerinti jelentést a honvédelemért felelős miniszternek küldi meg.

7. §[4] (1) Az eseménykezelő központ a hatáskörébe tartozó elektronikus információs rendszerek tekintetében

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

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

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

(3) Az eseménykezelő központ eljárására a 3. § (7) bekezdését, a 14-18. §-t, a 20-21. §-t és a 23-29. §-t alkalmazni kell.

4. A biztonsági események bejelentése

8. § (1) Az Ibtv. 19. § (1) bekezdés *b)-c)* pontja szerinti szervezetek, valamint a közvetítő szolgáltató kötelesek a Központ részére az elektronikus információs rendszereikben bekövetkezett biztonsági eseményeket haladéktalanul bejelenteni.

(2) Az érintett szervezet a honvédelmi célú elektronikus információs rendszert érintő biztonsági eseményt és fenyegetést a honvédelmi miniszter belső rendelkezése szerint a 6. § (1) bekezdésben kijelölt eseménykezelő központnak jelenti be.

9. § (1) Az alapvető szolgáltatást nyújtó szolgáltatók indokolatlan késedelem nélkül bejelentik a Központnak az általuk nyújtott alapvető szolgáltatások folytonosságára jelentős hatást gyakorló biztonsági eseményeket.

---

1 *Hatályon kívül helyezte: 375/2020. (VII. 30.) Korm. rendelet 114. § második b). Hatálytalan: 2020. VII. 31-től.*
2 *Megállapította: 375/2020. (VII. 30.) Korm. rendelet 106. § (1). Hatályos: 2020. VII. 31-től.*
3 *Beiktatta: 375/2020. (VII. 30.) Korm. rendelet 106. § (2). Hatályos: 2020. VII. 31-től.*
4 *Megállapította: 375/2020. (VII. 30.) Korm. rendelet 107. §. Hatályos: 2020. VII. 31-től.*

(2) A biztonsági esemény hatása jelentőségének meghatározása érdekében az alapvető szolgáltatást nyújtó szolgáltató tájékoztatásának az alábbi adatokat is tartalmaznia kell:

a) az alapvető szolgáltatás zavara által érintett felhasználók száma,

b) a biztonsági esemény időtartama,

c) a biztonsági esemény által érintett terület földrajzi kiterjedése.

(3) Ha egy alapvető szolgáltatásokat nyújtó szolgáltató valamely, a kritikus társadalmi és gazdasági tevékenységek fenntartása szempontjából alapvetőnek tekintett szolgáltatás nyújtását egy harmadik fél bejelentés-köteles szolgáltatóra alapozza, az említett szolgáltatónak be kell jelentenie minden olyan esetet, amikor a bejelentés-köteles szolgáltatót érintő biztonsági esemény jelentős hatást gyakorol az alapvető szolgáltatások folytonosságára.

10. § A bejelentés-köteles szolgáltatást nyújtó - a 11. §-ban, valamint az információs társadalommal összefüggő szolgáltatások elektronikus információbiztonságának felügyeletéről és a biztonsági eseményekkel kapcsolatos eljárásrendről szóló kormányrendeletben meghatározottak szerint - haladéktalanul bejelenti a Központ részére az elektronikus információs rendszerein bekövetkezett azon biztonsági eseményeket, amelyek jelentős hatást gyakorolnak az általa az Európai Unión belül kínált bejelentés-köteles szolgáltatás nyújtására.

11. § (1) A biztonsági események bejelentése elsődlegesen elektronikus úton történik, ha azonban az elektronikus információs rendszer oly mértékben sérül, hogy az nem lehetséges, a bejelentés bármely más módon megvalósítható.

(2) A bejelentés tartalmazza legalább

a) a biztonsági esemény rövid leírását, státuszát,

b) a szolgáltatás működésében támadt zavar mértékét,

c) az esemény kezelésére az üzemeltető által kijelölt kapcsolattartó személy és szervezet elérhetőségeit,

d) a biztonsági esemény hatását meghatározó szempontokat, valamint

e) közvetítő szolgáltató igénybevétele esetén a közvetítő szolgáltató megnevezését, elérhetőségét.

12. § (1) A Központ - a 9. § (1) bekezdése és a 10. §-a szerinti bejelentések alapján - vizsgálja az alapvető szolgáltatást nyújtók, valamint a bejelentés-köteles szolgáltatást nyújtók szolgáltatásaira jelentős hatást gyakorló biztonsági események határon átnyúló hatását, és közvetlenül vagy az egyedüli kapcsolattartó pont útján indokolt esetben tájékoztatja a jelentős hatást gyakorló biztonsági eseményekről a többi érintett tagállamot.

(2) A Központnak az (1) bekezdés szerinti tájékoztatás során biztosítania kell a szolgáltatók biztonságát, gondoskodnia kell arról, hogy ne sérüljenek a kereskedelmi érdekei és a bejelentésben foglalt információk bizalmassága.

5. Önkéntes bejelentés

13. § (1) Azok az Lrtv. szerinti ágazati szereplők, akiket nem azonosítottak alapvető szolgáltatásokat nyújtó szolgáltatóként, önkéntes alapon bejelenthetik a Központnak az olyan biztonsági eseményeket, amelyek jelentős hatást gyakorolnak az általuk nyújtott szolgáltatások folytonosságára. Ez a rendelkezés nem alkalmazható azon rendszerelemek vonatkozásában, amelyek az Lrtv. alapján európai vagy nemzeti létfontosságúvá kerültek kijelölésre.

(2) A bejelentés-köteles szolgáltatók önkéntes alapon bejelenthetnek minden olyan eseményt, amelyek számukra addig ismeretlen jellemzőkkel bírtak, ideértve különösen a sérülékenységet kihasználó új módszereket, a kihasználásra vonatkozó adatokat, sebezhető pontokat vagy fenyegetéseket.

(3) A Központ az önkéntes bejelentésekkel szemben előnyben részesítheti a kötelezően vizsgálandó bejelentések feldolgozását. Az önkéntes bejelentéseket csak akkor kell feldolgozni, ha az nem jelent aránytalan vagy indokolatlan terhet a Központ számára.

(4) Az önkéntes bejelentés eredményeként a bejelentő szervezet számára nem írható elő olyan kötelezettség, amely ne vonatkozott volna rá a bejelentés megtétele nélkül is.

6. A biztonsági események kezelésének, műszaki vizsgálatának szabályai

14. § Az állami és önkormányzati szervek elektronikus információs rendszereit érintő biztonsági események kivizsgálásában első sorban

a) az elektronikus információs rendszer biztonságáért felelős személy,

b) biztonságiesemény-kezelési megbízott, valamint

c) a hatáskörrel rendelkező eseménykezelő központ vehet részt.

15. § (1)[1] A nemzetbiztonsági védelem alá eső szerv vezetője - a 6. § (1) bekezdésében meghatározott szervek kivételével -

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

b) a biztonságiesemény-kezelési megbízott esetében a feladatra történő megbízása

tervezett hatálybalépését megelőző harminc nappal véleményezés céljából - az érintett személy hozzájárulásával - megküldi a Központ részére a kinevezésben, illetve a megbízásban szereplő személy adatait.

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

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

16. § (1) A bejelentett biztonsági esemény kivizsgálása során a biztonsági eseménnyel érintett szervezet köteles együttműködni a Központtal, amely együttműködés kiterjed:

a) a bejelentéssel kapcsolatos információk átadására,

b) a biztonsági eseményben érintettek (támadó/támadott) beazonosításához szükséges műszaki, technikai adatok Központ részére történő átadására,

c) a Központ szakembereinek tájékoztatására a biztonsági esemény következményei elhárítása érdekében tett intézkedésekről, illetve a biztonsági esemény vizsgálata során, az infrastruktúrával kapcsolatos beállításokról,

d) hozzáférés biztosítására a Központ szakemberei számára az incidensben érintett infrastruktúrához, valamint

e) a Központ által végzett kockázatelemzés alapján szükségesnek ítélt korai figyelmeztető- vagy csapdarendszerek, szenzorok telepítésére.

(2) Az együttműködés keretein belül az alapvető szolgáltatást nyújtó szolgáltatók az incidensben érintett infrastruktúrával kapcsolatos, speciális, ágazati sajátosságokat megosztják a Központtal.

---

1 *Módosította: 375/2020. (VII. 30.) Korm. rendelet 114. § c).*

(3) A bejelentés-köteles szolgáltatók, valamint az Lrtv. 4. melléklet 26. sora szerinti alapvető szolgáltatást nyújtó szolgáltatók az együttműködés keretein belül az incidensben érintett előfizetőkkel kapcsolatban a Központ kérésére kötelesek szükség szerint tiltásokat bevezetni, illetve (felhasználói, előfizetői) hozzáféréseket korlátozni, felfüggeszteni vagy megszüntetni.

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

(2) Ha a biztonsági eseménnyel érintett szervezet - a (3) bekezdés kivételével - bármely okból nem képes az (1) bekezdés szerinti adatok összegyűjtésére, a Központ begyűjtheti az adatokat. A biztonsági eseménnyel érintett szervezet gondoskodik arról, hogy a Központ az adatokhoz hozzáférjen.

(2a)[1] Az Információs Hivatal az (1) és (2) bekezdés szerinti, a biztonsági események kezeléséhez szükséges műszaki, technikai adatokat, információkat úgy köteles átadni vagy egyéb módon hozzáférhetővé tenni, hogy az ne eredményezze az elektronikus információs rendszeren tárolt adatok Központ általi megismerését.

(3) Ha a biztonsági eseménnyel érintett bejelentés-köteles szolgáltatást nyújtó bármely okból nem képes az (1) bekezdés szerinti adatok összegyűjtésére, az eseménykezelő központ képviselője helyszíni tanácsadás keretein belül, az érintett szervezet szakértőinek bevonásával javaslatot tesz a szükséges adatok összegyűjtésének és biztosításának módjára. A biztonsági eseménnyel érintett bejelentés-köteles szolgáltatást nyújtó gondoskodik arról, hogy az eseménykezelő központ az adatokhoz hozzáférjen.

(4) A biztonsági eseményekkel érintett szerv - az (5) bekezdés kivételével - köteles a vizsgálat lefolytatásához szükséges adatokat, dokumentumokat, eszközöket és egyéb információkat a Központ rendelkezésére bocsátani.

(5) A biztonsági eseményekkel érintett bejelentés-köteles szolgáltató köteles a vizsgálat lefolytatásához szükséges adatokat, dokumentumokat, eszközöket és egyéb információkat tartalmazó, bitazonos másolatokat a Központ rendelkezésére bocsátani.

(6) A Központ - a (7) bekezdés kivételével - a biztonsági eseménnyel érintett szervezettel együttműködve kidolgozza a biztonsági esemény felszámolásához szükséges intézkedéseket, amelyeket a biztonsági eseménnyel érintett szervezet köteles végrehajtani.

(7) A biztonsági eseménnyel érintett bejelentés-köteles szolgáltatást nyújtó a biztonsági esemény felszámolásához szükséges intézkedéseket kidolgozza, és haladéktalanul végrehajtja. A Központ támogatja a biztonsági eseménnyel érintett bejelentés-köteles szolgáltatást nyújtót a biztonsági esemény felszámolásához szükséges intézkedések kidolgozásában.

(8) A biztonsági eseménnyel érintett bejelentés-köteles szolgáltatást nyújtó az esemény felszámolását követően felülvizsgálja az elektronikus információs rendszerei kockázatelemzésének, kockázatkezelésének teljeskörűségét, és végrehajtja a szükséges módosításokat.

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

---

1 *Beiktatta: 375/2020. (VII. 30.) Korm. rendelet 108. §. Hatályos: 2020. VII. 31-től.*

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

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

(3) A központosított informatikai és elektronikus hírközlési szolgáltató a Központ által történő biztonságiesemény-kezelés során köteles

a) a biztonsági eseményben érintettek, a támadó és a támadott beazonosításához szükséges műszaki, technikai adatok Központ részére történő átadására,

b) az ismert fenyegetések elleni védelmi intézkedések, műszaki, technikai megoldások alkalmazására,

c) a Központ kérésére a 17. § (1) bekezdése szerinti adatokat szolgáltatni a hálózati forgalomba való beavatkozásra utaló jelek elemzése, kiértékelése céljából, valamint

d) a Központ által meghatározott, biztonsági eseményekkel kapcsolatos feladatokban együttműködni.

19. § (1) A biztonsági események kivizsgálása során az eseménykezelő központ szükség szerint megismerheti a közvetítő szolgáltatók különböző szolgáltatás- vagy üzletmenet folytonosságot biztosító szabályzóit, eljárásrendjeit, ideértve különösen az üzletfolytonossági tervét, a katasztrófa helyreállítási tervét.

(2) A biztonsági esemény által érintett közvetítő szolgáltató az eseménykezelő központtal való együttműködés keretein belül a konkrét biztonsági esemény kezelése érdekében az eseménykezelő központ kérésére a biztonsági eseményben érintettek, a támadó és a támadott beazonosításához szükséges adatokat szolgáltat a 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 az eseménykezelő központ kötelezheti a közvetítő szolgáltatót adott szolgáltatás tiltására.

(4) A Központ értesíti az Ekertv. 6/B. § (3) bekezdése szerinti hatóságot, ha a közvetítő szolgáltató nem teljesíti együttműködési kötelezettségét.

20. § A biztonsági eseményekkel összefüggő adatok műszaki vizsgálatának célja, hogy a bekövetkezett biztonsági események kivizsgálása révén a Központ

a) feltárja a biztonsági esemény bekövetkeztének okait, körülményeit, az okozott kár mértékét,

b) behatárolja a biztonsági esemény által érintett elektronikus információs rendszerek, rendszerelemek körét,

c) javaslatot tegyen a biztonsági esemény által okozott kár elhárítására, és

d) a bekövetkezett biztonsági eseményből levonható tanulságokról tájékoztassa a biztonsági eseménnyel érintett más szerveket és a hatóságot annak érdekében, hogy a jövőben a biztonsági esemény bekövetkezése megelőzhető legyen.

21. § A bejelentési, tájékoztatási, illetve együttműködési kötelezettségnek eleget nem tevő szervezetet a Központ jelenti az adott elektronikus információs rendszer felügyeletét ellátó hatóságnak.

7. Sérülékenységvizsgálat

22. § (1) A nemzetbiztonsági védelem alá eső állami és önkormányzati szervek elektronikus információs rendszerei, az Ibtv. 2. § (1) bekezdése szerinti állami és önkormányzati szervek európai létfontosságú rendszerelemmé vagy nemzeti létfontosságú rendszerelemmé törvény alapján kijelölt rendszerelemeinek elektronikus információs rendszerei, valamint a zárt célú elektronikus információs rendszerek sérülékenységvizsgálatát - a (2) és (3) bekezdésben meghatározott kivétellel - a Központ végzi. A Központ jogosult továbbá az Ibtv. 18. § (3) bekezdése szerinti állami szervként a sérülékenységvizsgálat lefolytatására.

(2)[1]

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

(4) Az Ibtv. 18. § (3) bekezdés *b)* pontja szerinti gazdálkodó szervezet (a továbbiakban: gazdálkodó szervezet) abban az esetben végezhet sérülékenységvizsgálatot, ha

a) a gazdálkodó szervezet nevében és alkalmazásában eljárva a sérülékenységvizsgálatban részt vevő személy az Ibtv. 18. § (4) bekezdésében meghatározott feltételeken túl rendelkezik a sérülékenységvizsgálat lefolytatásához szükséges ismeretek meglétét igazoló végzettséggel, és ezen a szakterületen legalább 2 év szakmai tapasztalattal, valamint

b) a gazdálkodó szervezet bejegyzésre került a sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezetek nyilvántartásába.

(5) A sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezetekről az Alkotmányvédelmi Hivatal nyilvántartást vezet. A nyilvántartás tartalmazza a gazdálkodó szervezet adatait, a sérülékenységvizsgálatban részt vevő személyek számát és a sérülékenységvizsgálat lefolytatásához szükséges ismereteket igazoló végzettség megnevezését és megszerzésének az idejét.

(6) Az (5) bekezdés szerinti adatok tekintetében az Alkotmányvédelmi Hivatal egyedi, írásbeli kérelem alapján, annak beérkezésétől számított tizenöt napon belül nyújt tájékoztatást azon elektronikus információs rendszereket üzemeltető szervezet részére, amelyek az Ibtv. 18. § (2) bekezdése alapján jogosultak sérülékenységvizsgálatot kezdeményezni.

(7) A nyilvántartásba való felvételt a gazdálkodó szervezet kezdeményezi az Alkotmányvédelmi Hivatal felé, a (4) bekezdésben meghatározott feltételek meglétét igazoló okiratok benyújtásával. A (4) bekezdésben meghatározott feltételek szakmai megfelelősége tekintetében a Központ nyilatkozata irányadó.

---

1 *Hatályon kívül helyezte: 375/2020. (VII. 30.) Korm. rendelet 114. § d). Hatálytalan: 2020. VII. 31-től.*

(8) Az Alkotmányvédelmi Hivatal elutasítja a nyilvántartásba történő felvételi kérelmet, ha

a) a gazdálkodó szervezet nem rendelkezik az Ibtv. 18. § (3) bekezdés *b)* pontjában megkövetelt telephely biztonsági tanúsítvánnyal,

b) a Központ nyilatkozata alapján a sérülékenységvizsgálat lefolytatásához szükséges ismeretek meglétét igazoló végzettség, és ezen a szakterületen legalább 2 év szakmai tapasztalat nem áll fenn, vagy

c) a gazdálkodó szervezet által közölt adatok a valóságnak nem felelnek meg.

(9) A sérülékenységvizsgálat lefolytatására jogosult gazdálkodó szervezet az alkalmassági feltételeket érintő változásokról, valamint a sérülékenységvizsgálatban részt vevő személyeket érintő változásokról a változást követő nyolc napon belül értesíti az Alkotmányvédelmi Hivatalt.

(10) Az Alkotmányvédelmi Hivatal jogosult az alkalmassági feltételek meglétét, valamint a nyilvántartásban szereplő adatok valódiságát ellenőrizni. Az értesítési kötelezettség elmulasztása esetén, valamint az alkalmassági feltételek meglétének hiánya esetén az Alkotmányvédelmi Hivatal a gazdálkodó szervezetet a nyilvántartásából törli.

(11) Az (5) bekezdés szerint vezetett nyilvántartásba felvételre került gazdálkodó szervezetnek a felvételt követő minden második évben ismételten meg kell küldenie az Alkotmányvédelmi Hivatal részére a (4) és (7) bekezdés szerinti okiratokat. A megküldést a biztonsági vezető útján, az Alkotmányvédelmi Hivatal által a felvételről kiállított tanúsítványban feltüntetett hónapnak megfelelő hónap utolsó napjáig kell teljesíteni.

(12) Az Alkotmányvédelmi Hivatal a megküldött dokumentumok alapján ismételten ellenőrzi, hogy teljesülnek-e a (4) bekezdésben meghatározott feltételek.

(13) Ha a (11) bekezdésben meghatározott adatszolgáltatási kötelezettségének a gazdálkodó szervezet nem tesz eleget, akkor a gazdálkodó szervezetet az Alkotmányvédelmi Hivatal törli a nyilvántartásból.

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

(2) A sérülékenységvizsgálat tárgya az adatok, információk kezelésére használt elektronikus információs rendszerek, rendszerelemek, eszközök, eljárások és kapcsolódó folyamatok vizsgálata, valamint az ezeket kezelő személyek általános informatikai felkészültségének és az érintett szervezetnél használt informatikai és információbiztonsági előírások, szabályok betartásának vizsgálata.

(3)[1] Az Információs Hivatal biztosítja, hogy az elektronikus információs rendszerét érintő sérülékenységvizsgálat az azon tárolt adatok megismerése nélkül kerül végrehajtásra a Központ által.

24. § (1)[2] A sérülékenységvizsgálat során a sérülékenységvizsgálati eljárását megalapozó alapdokumentumban meghatározottak szerint az alábbi vizsgálatok elvégzésére kerül sor:

a) külső informatikai biztonsági vizsgálat,

b) webes vizsgálat,

c) automatizált vizsgálat,

---

1 *Beiktatta: 375/2020. (VII. 30.) Korm. rendelet 109. §. Hatályos: 2020. VII. 31-től.*
2 *Módosította: 375/2020. (VII. 30.) Korm. rendelet 113. § a).*

d) pszichológiai manipuláció,
e) belső informatikai biztonsági vizsgálat, illetve
f) vezeték nélküli hálózat informatikai biztonsági vizsgálata.

(2) A sérülékenységvizsgálat az (1) bekezdés *a)-c)*, *e)* és *f)* pontjában meghatározott irányultságok tekintetében három típusú jogosultsági fázist tartalmazhat:
a) regisztrált felhasználói jogosultság nélküli vizsgálat,
b) regisztrált felhasználói jogosultsággal rendelkező vizsgálat és
c) adminisztrátori jogosultsággal rendelkező vizsgálat.

(3) A sérülékenységvizsgálat határideje a hatóság határozatának keltétől, illetve az előzetesen egyeztetett kezdési időponttól számítva az (1) bekezdésben meghatározott vizsgálatok szerint:
a) külső informatikai biztonsági vizsgálat esetén harminc nap,
b) webes vizsgálat esetén hetvenöt nap,
c) pszichológiai manipuláció esetén kilencven nap,
d) belső informatikai biztonsági vizsgálat esetén kilencven nap,
e) vezeték nélküli hálózat informatikai biztonsági vizsgálat esetén harminc nap.

(4)[1] Regisztrált felhasználói jogosultság nélküli vizsgálat esetén az érintett szervezet
a) a Központ részére megküldi a vizsgálandó informatikai rendszer, illetve szolgáltatás hozzáférési pontjaihoz tartozó adatokat, biztosítja - korlátozott hozzáférésű rendszer esetében is - a hozzáférési pontok fizikai és logikai elérésének lehetőségét,
b) biztosítja a Központ számára a vizsgálandó informatikai rendszer, illetve szolgáltatás monitorozását,
c) biztosítja a funkció-tesztelési tervet, valamint
d) biztosítja a tesztelés eredményéről szóló dokumentációt.

(5)[2] Regisztrált felhasználói jogosultsággal rendelkező vizsgálat esetén a (4) bekezdésben meghatározottakon túl az érintett szervezet a Központ részére megküldi
a) a felhasználói jogosultság mátrixot, valamint
b) a felhasználói dokumentációt.

(6)[3] Adminisztrátori jogosultsággal rendelkező vizsgálat esetén az érintett szervezet a Központ részére megküldi a (4) és (5) bekezdésben foglaltakon túl a rendszertervet.

25. § (1)[4] A sérülékenységvizsgálat előkészítése során a sérülékenységvizsgálatot végző szerv sérülékenységvizsgálati alapdokumentumot készít. A sérülékenységvizsgálati alapdokumentumban rögzíti a vizsgálati feladatokat, célokat, a technikai és személyi feltételeket, a módszertant, az egyeztetések, a sérülékenységvizsgálat várható befejezésének dátumát.

(2)[5] Ha a sérülékenységvizsgálatot a hatóság rendeli el, akkor a sérülékenységvizsgálati alapdokumentumban a határozatban rögzített vizsgálati feladatokat kell feltüntetni. A sérülékenységvizsgálat egyedi kezdeményezése esetén a vizsgálati feladatokra a kezdeményező javaslatot tehet, amelyről a sérülékenységvizsgálatot végző szerv dönt.

---

1 *Beiktatta: 375/2020. (VII. 30.) Korm. rendelet 110. §. Hatályos: 2020. VII. 31-től.*
2 *Beiktatta: 375/2020. (VII. 30.) Korm. rendelet 110. §. Hatályos: 2020. VII. 31-től.*
3 *Beiktatta: 375/2020. (VII. 30.) Korm. rendelet 110. §. Hatályos: 2020. VII. 31-től.*
4 *Módosította: 375/2020. (VII. 30.) Korm. rendelet 113. § b).*
5 *Módosította: 375/2020. (VII. 30.) Korm. rendelet 113. § c).*

(3)[1] A sérülékenységvizsgálati alapdokumentumot a sérülékenységvizsgálatot végző szerv megküldi az érintett szervezet részére. Az érintett szervezet a sérülékenységvizsgálati alapdokumentum tartalmára a kézhezvételtől számított nyolc napon belül észrevételt tehet. Az észrevétel nem érintheti a hatóság által elrendelt vizsgálatokat. Az észrevételekről a sérülékenységvizsgálatot végző szerv dönt.

(4)[2] A sérülékenységvizsgálat nem hajtható végre, ha a sérülékenységvizsgálati alapdokumentumban, valamint az e rendeletben foglalt feltételek hiánytalanul nem állnak rendelkezésre.

(5)[3] A sérülékenységvizsgálat végrehajtását fel kell függeszteni, ha a sérülékenységvizsgálati alapdokumentumban, valamint az e rendeletben foglalt feltételek nem állnak rendelkezésre.

26. § (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) Hatósági határozat alapján elrendelt sérülékenységvizsgálat esetén az érintett szervezet köteles 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.

(3) Egyedi kezdeményezés esetén az érintett szervezet a 25. § (3) bekezdése szerinti észrevételezés során kizárhatja azokat a vizsgálatokat, amelyek jelentős szolgáltatáscsökkenést eredményeznek.

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

27. § (1) A Központ saját hatáskörében indított sérülékenységvizsgálat végrehajtása érdekében a 22. § (1) bekezdése szerinti szervezetek kötelesek bejelenteni a webes szolgáltatások, weboldalak és web-szerverek elérhetőségére vonatkozó egyedi technikai adatokat, azonosítókat a Központ részére.

(2)[4] A honvédelmi célú elektronikus információs rendszerek esetén az (1) bekezdésben meghatározott adatokat a 6. § (1) bekezdése szerinti eseménykezelő központnak kell bejelenteni.

(3) A webes szolgáltatások elérhetőségében bekövetkező változás esetén a bejelentést 3 napon belül meg kell tenni.

(4) A Központ tájékoztatja az érintett szervezetet az általa a vizsgálathoz használt IP címről vagy más egyedi technikai azonosítóról, amelyet az érintett szervezet nem tilthat ki a webes szolgáltatás eléréséből.

28. § (1) Az érintett szervezet elektronikus információs rendszere az átlagostól jelentősen eltér, ha *a)* az elektronikus információs rendszer

---

1 *Módosította: 375/2020. (VII. 30.) Korm. rendelet 113. § d).*
2 *Beiktatta: 375/2020. (VII. 30.) Korm. rendelet 111. §. Hatályos: 2020. VII. 31-től.*
3 *Beiktatta: 375/2020. (VII. 30.) Korm. rendelet 111. §. Hatályos: 2020. VII. 31-től.*
4 *Megállapította: 375/2020. (VII. 30.) Korm. rendelet 112. §. Hatályos: 2020. VII. 31-től.*

aa) a külső internetes tartományban több mint 20 IP címen elérhető eszközzel,

ab) több mint 10 webes szolgáltatással,

ac) a belső hálózat tekintetében több mint 50 szerverrel,

ad) több mint 500 munkaállomással,

ae) több mint 5 vezeték nélküli hálózattal vagy

af) több mint 500 fős felhasználói létszámmal rendelkezik, vagy

b) az érintett szervezet több, mint három telephelyen rendelkezik a vizsgálattal érintett elektronikus információs rendszerrel.

(2) Ha az érintett szervezet elektronikus információs rendszere, rendszereleme az átlagostól jelentősen eltér, és emiatt egyedi sérülékenységvizsgálati eljárás szükséges, a sérülékenységvizsgálati határidő a 24. § (3) bekezdésében meghatározottakon túl további harminc nappal meghosszabbítható.

29. § (1) A sérülékenységvizsgálat lezárásakor a sérülékenységvizsgálatot végző szerv állásfoglalást készít, és azt nyolc napon belül megküldi az érintett szervezet és a hatóság részére.

(2) Az (1) bekezdés szerinti állásfoglalás tartalmazza

a) a vizsgálati eredmények leírását és

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

(3)[1] A sérülékenységvizsgálatot végző szerv a 28. § (1) bekezdésében meghatározott bármely feltétel fennállása esetén az állásfoglalást 21 napon belül megküldi az érintett szervezet és a hatóság részére.

8. Záró rendelkezések

30. § Ez a rendelet 2019. január 1-én lép hatályba.

31. § (1) Ez a rendelet

a) a belső piaci szolgáltatásokról szóló, 2006. december 12-i 2006/123/EK európai parlamenti és tanácsi irányelvnek,

b) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló, 2016. július 6-i (EU) 2016/1148 európai parlamenti és tanácsi irányelvnek való megfelelést szolgálja.

(2) Ez a rendelet a hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése céljából a digitális szolgáltatók által figyelembe veendő elemek és a biztonsági események hatása jelentőségének megállapítására szolgáló paraméterek pontosabb meghatározása tekintetében az (EU) 2016/1148 európai parlamenti és tanácsi irányelv alkalmazására vonatkozó szabályok meghatározásáról szóló, 2018. január 30-i (EU) 2018/151 bizottsági végrehajtási rendelet végrehajtásához szükséges rendelkezéseket állapít meg.

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

33. §[2]

---

1 *Beiktatta: 375/2020. (VII. 30.) Korm. rendelet 112. §. Hatályos: 2020. VII. 31-től.*

2 *Hatályon kívül helyezve: 2010. évi CXXX. törvény 12. § alapján. Hatálytalan: 2019. I. 2-től.*

TARTALOMJEGYZÉK