►B

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2555 IRÁNYELVE

(2022. december 14.)

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)

(EGT-vonatkozású szöveg)

(HL L 333., 2022.12.27., 80. o.)

Helyesbítette:

►C1 Helyesbítés, HL L 90206., 2023.12.22., 1. o. (2022/2555)

▼B

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2555 IRÁNYELVE

(2022. december 14.)

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)

(EGT-vonatkozású szöveg)

I. FEJEZET

II. ÁLTALÁNOS RENDELKEZÉSEK

1. cikk

Tárgy

(1) Ez az irányelv a belső piac működésének javítása érdekében intézkedéseket határoz meg az egységesen magas szintű kiberbiztonság Unión belüli elérése céljából.

(2) Ennek érdekében ezen irányelv a következőket állapítja meg:

a) a tagállamok számára azt előíró kötelezettségek, hogy nemzeti kiberbiztonsági stratégiákat fogadjanak el, valamint illetékes hatóságokat, kiberválságok kezelésével foglalkozó hatóságokat, kiberbiztonsággal foglalkozó egyedüli kapcsolattartó pontokat (a továbbiakban: egyedüli kapcsolattartó pontok) és számítógép-biztonsági eseményekre reagáló csoportokat (a továbbiakban: CSIRT-ek) jelöljenek ki vagy hozzanak létre;

b) kiberbiztonsági kockázatkezelési intézkedések és bejelentési kötelezettségek az I. vagy a II. mellékletben említett típusú szervezetek, valamint az (EU) 2022/2557 irányelv szerint kritikus szervezetként azonosított szervezetek számára;

c) szabályok és kötelezettségek a kiberbiztonsági információk megosztására vonatkozóan;

d) felügyeleti és végrehajtási kötelezettségek a tagállamok számára.

2. cikk

Hatály

(1) ►C1 Ezt az irányelvet az I. vagy II. mellékletben említett típusú olyan állami vagy magánszervezetekre kell alkalmazni, amelyek a 2003/361/EK ajánlás mellékletének 2. cikke szerint középvállalkozásoknak minősülnek vagy meghaladják az említett cikk (1) bekezdésében a középvállalkozásokra vonatkozóan előírt felső határértékeket, és amelyek az Unión belül nyújtják szolgáltatásaikat vagy végzik tevékenységeiket. ◄

▼B

Az említett ajánlás melléklete 3. cikkének (4) bekezdése ezen irányelv alkalmazásában nem alkalmazandó.

(2) Ez az irányelv – méretüktől függetlenül – az I. vagy II. mellékletben említett típusú szervezetekre is alkalmazandó, amennyiben:

a) a szolgáltatásokat a következők nyújtják:

i. nyilvános elektronikus hírközlő hálózatok szolgáltatói vagy nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatók;

ii. bizalmi szolgáltatók;

iii. legfelső szintű doménnév-nyilvántartók és doménnévrendszer-szolgáltatók;

b) a szervezet egy tagállamban az egyetlen szolgáltató egy olyan szolgáltatás tekintetében, amely elengedhetetlen a kritikus társadalmi vagy gazdasági tevékenységek fenntartásához;

c) a szervezet által nyújtott szolgáltatás zavara jelentős hatással lehet a közvédelemre, a közbiztonságra vagy a közegészségre;

d) a szervezet által nyújtott szolgáltatás zavara jelentős rendszerszintű kockázatot idézhet elő, különösen azokban az ágazatokban, ahol az említett zavarnak határokon átnyúló hatása lehet;

e) a szervezet kritikus, mivel nemzeti vagy regionális szinten különös fontossággal bír az adott ágazat vagy szolgáltatás típusa, vagy a tagállam más, kölcsönösen függő ágazatai szempontjából;

f) a szervezet:

i. valamely tagállam által annak nemzeti jogával összhangban meghatározott, központi kormányzathoz tartozó közigazgatási szerv; vagy

ii. valamely tagállam által annak nemzeti jogával összhangban meghatározott, regionális szintű közigazgatási szerv, amely kockázatalapú értékelés alapján olyan szolgáltatásokat nyújt, amelyek zavara jelentős hatást gyakorolhat kritikus fontosságú társadalmi vagy gazdasági tevékenységekre.

(3) Ez az irányelv – méretüktől függetlenül – az (EU) 2022/2557 irányelv szerint kritikus szervezetként azonosított szervezetekre is alkalmazandó.

▼B

(4) Ez az irányelv – méretüktől függetlenül – a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetekre is alkalmazandó.

(5) A tagállamok rendelkezhetnek úgy, hogy ez az irányelv alkalmazandó a következőkre:

a) helyi szintű közigazgatási szervek;

b) oktatási intézmények, különösen, ha kritikus fontosságú kutatási tevékenységeket végeznek.

(6) Ez az irányelv nem érinti a tagállamoknak a nemzetbiztonság védelmével kapcsolatos felelősségüket és az egyéb alapvető állami funkciók védelmére vonatkozó hatáskörüket, beleértve az állam területi integritásának biztosítását és a közrend fenntartását.

(7) Ez az irányelv nem alkalmazandó azokra a közigazgatási szervekre, amelyek a nemzetbiztonság, a közbiztonság, a védelem vagy a bűnüldözés – többek között a bűncselekmények megelőzése, kivizsgálása, felderítése és büntetőeljárás alá vonása – területén végzik tevékenységeiket.

(8) A tagállamok egyes olyan szervezeteket, amelyek a nemzetbiztonság, a közbiztonság, a védelem vagy a bűnüldözés – többek között a bűncselekmények megelőzése, kivizsgálása, felderítése és büntetőeljárás alá vonása – területén végzik tevékenységeiket vagy amelyek kizárólag az e cikk (7) bekezdésében említett közigazgatási szervek számára nyújtanak szolgáltatásokat, az említett tevékenységek vagy szolgáltatások tekintetében mentesíthetnek a 21. vagy 23. cikkben megállapított kötelezettségek alól. Ilyen esetekben a VII. fejezetben említett felügyeleti és végrehajtási intézkedések nem alkalmazandók az említett egyes tevékenységekre vagy szolgáltatásokra. Amennyiben a szervezetek kizárólag az e bekezdésben említett típusú tevékenységeket végeznek vagy ilyen típusú szolgáltatásokat nyújtanak, a tagállamok ezeket a szervezeteket is mentesíthetik a 3. és 27. cikkben megállapított kötelezettségek alól.

(9) A (7) és (8) bekezdés nem alkalmazandó, ha a szervezet bizalmi szolgáltatóként tevékenykedik.

(10) Ez az irányelv nem alkalmazandó azokra a szervezetekre, amelyeket a tagállamok mentesítettek az (EU) 2022/2554 rendelet hatálya alól az említett rendelet 2. cikkének (4) bekezdésével összhangban.

(11) Az ezen irányelvben meghatározott kötelezettségek nem foglalják magukban olyan információk szolgáltatását, amelyek közzététele ellentétes lenne a tagállamok nemzetbiztonságának, közbiztonságának vagy védelmének alapvető érdekeivel.

(12) Ezt az irányelvet az (EU) 2016/679 rendelet, a 2002/58/EK irányelv, a 2011/93/EU [1] és a 2013/40/EU [2] európai parlamenti és tanácsi irányelv, valamint az (EU) 2022/2557 irányelv sérelme nélkül kell alkalmazni.

---

[1] Az Európai Parlament és a Tanács 2011/93/EU irányelve (2011. december 13.) a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról (HL L 335., 2011.12.17., 1. o.).

[2] Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról (HL L 218., 2013.8.14., 8. o.).

▼B

(13) Az EUMSZ 346. cikkének sérelme nélkül az uniós vagy nemzeti szabályok értelmében bizalmas információkat – például az üzleti titoktartási szabályokat – csak akkor lehet megosztani a Bizottsággal és az ezen irányelv szerinti más érintett hatóságokkal, ha az említett információcsere ezen irányelv alkalmazásához szükséges. A megosztott információnak az információcsere célja szempontjából lényeges és arányos mértékre kell korlátozódnia. Az információcsere során meg kell őrizni a rendelkezésre bocsátott információk bizalmas jellegét, és óvni kell az érintett szervezetek biztonsági és kereskedelmi érdekeit.

(14) A szervezetek, az illetékes hatóságok, az egyedüli kapcsolattartó pontok és a CSIRT-ek az ezen irányelv céljaihoz szükséges mértékig és az (EU) 2016/679 rendelettel összhangban folytatnak személyesadatkezelést, és ezen adatkezelés során különösen az említett rendelet 6. cikkére támaszkodnak.

A személyes adatok ezen irányelv szerinti kezelését a nyilvános elektronikus hírközlő hálózatok szolgáltatói vagy a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatók az adatvédelemre és a magánélet védelmére vonatkozó uniós joggal, különösen a 2002/58/EK irányelvvel összhangban végzik.

3. cikk

Alapvető és fontos szervezetek

(1) Ezen irányelv alkalmazásában a következő szervezeteket kell alapvető szervezetnek tekinteni:

▼C1

a) az I. mellékletben említett típusú azon szervezetek, amelyek meghaladják a 2003/361/EK ajánlás mellékletének 2. cikke (1) bekezdésében a középvállalkozásokra vonatkozóan előírt felső határértékeket;

▼B

b) a minősített bizalmi szolgáltatók és a legfelső szintű doménnév-nyilvántartók, valamint a DNS-szolgáltatók, méretüktől függetlenül;

c) a nyilvános elektronikus hírközlő hálózatok szolgáltatói vagy a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatók, amelyek a 2003/361/EK ajánlás mellékletének 2. cikke szerint középvállalkozásoknak minősülnek;

d) a 2. cikk (2) bekezdése f) pontjának i. alpontjában említett közigazgatási szervek;

e) az I. vagy II. mellékletben említett típusú bármely egyéb szervezetek, amelyeket egy tagállam a 2. cikk (2) bekezdésének b)–e) pontja alapján alapvető szervezetekként azonosított;

f) az ezen irányelv 2. cikkének (3) bekezdésében említett, az (EU) 2022/2557 irányelv értelmében kritikus szervezetként azonosított szervezetek;

g) amennyiben a tagállam úgy rendelkezik, azon szervezetek, amelyeket az adott tagállam 2023. január 16. előtt az (EU) 2016/1148 irányelvvel vagy a nemzeti joggal összhangban alapvető szolgáltatásokat nyújtó szereplőként azonosított.

▼B

(2) Ezen irányelv alkalmazásában az I. vagy II. mellékletben említett típusú összes olyan szervezetet, amely az e cikk (1) bekezdése értelmében nem minősül alapvető szervezetnek, fontos szervezetnek kell tekinteni. Ebbe beletartoznak azok a szervezetek, amelyeket a tagállamok a 2. cikk (2) bekezdésének b)–e) pontja alapján fontos szervezetként azonosítottak.

(3) A tagállamok 2025. április 17-ig összeállítják az alapvető és fontos szervezetek, valamint a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek jegyzékét. A tagállamok az említett jegyzéket rendszeresen, de az említett időpontot követően legalább kétévente felülvizsgálják, és adott esetben frissítik.

(4) A (3) bekezdésben említett jegyzék összeállítása céljából a tagállamok előírják az említett bekezdésben említett szervezetek számára, hogy az illetékes hatóságoknak nyújtsák be legalább a következő információkat:

a) a szervezet neve;

b) a cím és naprakész elérhetőségek, beleértve az e-mail-címeket, IP-tartományokat és telefonszámokat;

c) adott esetben az I. vagy II. mellékletben említett megfelelő ágazat és alágazat; valamint

d) adott esetben azon tagállamok jegyzéke, ahol az ezen irányelv hatálya alá tartozó szolgáltatásokat nyújtják.

A (3) bekezdésben említett szervezetek haladéktalanul, és minden esetben a változás időpontjától számított két héten belül bejelentenek az e bekezdés első albekezdése alapján benyújtott adatokban bekövetkező bármely változást.

A Bizottság az Európai Uniós Kiberbiztonsági Ügynökség (a továbbiakban: ENISA) segítségével indokolatlan késedelem nélkül iránymutatásokat nyújt és sablonokat bocsát rendelkezésre ez e bekezdésben megállapított kötelezettségekre vonatkozóan.

A tagállamok nemzeti mechanizmusokat hozhatnak létre abból a célból, hogy a szervezetek bejegyeztessék magukat.

(5) 2025. április 17-ig és azt követően kétévente az illetékes hatóságok bejelentik:

a) a Bizottságnak és az együttműködési csoportnak az I. vagy a II. mellékletben említett egyes ágazatok és alágazatok tekintetében a (3) bekezdés szerint a jegyzékben felsorolt alapvető és fontos szervezetek számát; valamint

b) a Bizottságnak a 2. cikk (2) bekezdésének b)–e) pontja alapján azonosított alapvető és fontos szervezetek számáról, az I. vagy a II. mellékletben említett ágazatukról és alágazatukról, az általuk nyújtott szolgáltatás típusáról, valamint a 2. cikk (2) bekezdésének b)–e) pontjában megállapítottak közül az azonosításuk alapjául szolgáló rendelkezésről szóló releváns információkat.

▼B

(6) 2025. április 17-ig és a Bizottság kérésére a tagállamok bejelenthetik a Bizottságnak az (5) bekezdés b) pontjában említett alapvető és fontos szervezetek nevét.

4. cikk

Ágazatspecifikus uniós jogi aktusok

(1) Amennyiben az ágazatspecifikus uniós jogi aktusok előírják, hogy az alapvető vagy fontos szervezetek kiberbiztonsági kockázatkezelési intézkedéseket fogadjanak el, vagy bejelentsék a jelentős biztonsági eseményeket, és ha ezek a követelmények hatásukban legalább egyenértékűek az ezen irányelvben meghatározott kötelezettségekkel, akkor ezen irányelv vonatkozó rendelkezései – beleértve a VII. fejezetben meghatározott, a felügyeletre és a végrehajtásra vonatkozó rendelkezéseket – nem alkalmazandók az említett szervezetekre. Amennyiben az ágazatspecifikus uniós jogi aktusok hatálya nem terjed ki az ezen irányelv hatálya alá tartozó, adott ágazatban működő valamennyi szervezetre, ezen irányelv vonatkozó rendelkezései továbbra is alkalmazandók azokra a szervezetekre, amelyek nem tartoznak az említett ágazatspecifikus uniós jogi aktusok hatálya alá.

(2) Az e cikk (1) bekezdésében említett követelmények az ezen irányelvben megállapított kötelezettségekkel hatásukban egyenértékűnek tekintendők, ha:

a) a kiberbiztonsági kockázatkezelési intézkedések hatásukban legalább egyenértékűek a 21. cikk (1) és (2) bekezdésében megállapítottakkal; vagy

b) az ágazatspecifikus uniós jogi aktus előírja az eseménybejelentésekhez való azonnali – adott esetben automatikus és közvetlen – hozzáférést a CSIRT-ek, az illetékes hatóságok vagy az ezen irányelv szerinti egyedüli kapcsolattartó pontok számára, és ha a jelentős események bejelentésére vonatkozó követelmények hatásukban legalább egyenértékűek az ezen irányelv 23. cikkének (1)–(6) bekezdésében megállapítottakkal.

(3) A Bizottság 2023. július 17-ig iránymutatásokat ad ki, amelyekben pontosítja az (1) és (2) bekezdés alkalmazását. A Bizottság rendszeresen felülvizsgálja az említett iránymutatásokat. Az említett iránymutatások kidolgozása során a Bizottság figyelembe veszi az együttműködési csoport és az ENISA valamennyi észrevételét.

5. cikk

Minimális harmonizáció

Ez az irányelv nem akadályozza meg a tagállamokat abban, hogy magasabb szintű kiberbiztonságot biztosító rendelkezéseket fogadjanak el vagy tartsanak fenn, feltéve, ha e rendelkezések összhangban vannak a tagállamok uniós jogban megállapított kötelezettségeivel.

6. cikk

Fogalommeghatározások

Ezen irányelv alkalmazásában:

▼B

1. „hálózati és információs rendszer”:

   a) az (EU) 2018/1972 irányelv 2. cikkének 1. pontjában meghatározott elektronikus hírközlő hálózat;

   b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatikus kezelését végzi; vagy

   c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;

2. „hálózati és információs rendszerek biztonsága”: a hálózati és információs rendszerek azon képessége, hogy adott bizonyossággal ellenálljanak minden olyan eseménynek, amely veszélyeztetheti a rajtuk tárolt, továbbított vagy kezelt adatok vagy az említett hálózati és információs rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét vagy bizalmasságát;

3. „kiberbiztonság”: az (EU) 2019/881 rendelet 2. cikkének 1. pontjában meghatározott kiberbiztonság;

4. „nemzeti kiberbiztonsági stratégia”: valamely tagállam koherens kerete, amely meghatározza a kiberbiztonság területén követendő stratégiai célokat és prioritásokat és a megvalósításukhoz szükséges irányítási intézkedéseket az adott tagállamban;

5. „majdnem bekövetkezett (near miss) esemény”: olyan esemény, amely veszélyeztethette volna a hálózati és információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét vagy bizalmasságát, de amelynek bekövetkezését sikerült megakadályozni, vagy amely nem következett be;

6. „esemény”: olyan esemény, amely veszélyezteti a hálózati és információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét vagy bizalmasságát;

7. „nagyszabású kiberbiztonsági esemény”: olyan esemény, amely olyan mértékű zavart okoz, amely meghaladja valamely tagállamnak az arra való reagálása képességét, vagy amely legalább két tagállamra jelentős hatást gyakorol;

8. „eseménykezelés”: minden olyan tevékenység és eljárás, amelynek célja az esemény megelőzése, észlelése, elemzése és elszigetelése vagy az eseményre való reagálás és az eseményt követően a működés helyreállítása;

▼B

9. „kockázat”: egy esemény által okozott veszteség vagy zavar lehetősége, amelyet az említett veszteség vagy zavar nagyságrendje és az adott esemény bekövetkezési valószínűsége kombinációjaként kell kifejezni;

10. „kiberfenyegetés”: az (EU) 2019/881 rendelet 2. cikkének 8. pontjában meghatározott kiberfenyegetés;

11. „jelentős kiberfenyegetés”: olyan kiberfenyegetés, amelyről – technikai jellemzői alapján – feltételezhető, hogy jelentős vagyoni vagy nem vagyoni kárt okozva súlyos hatást gyakorolhat egy szervezet hálózati és információs rendszereire vagy a szervezet szolgáltatásainak felhasználóira;

12. „IKT-termék”: az (EU) 2019/881 rendelet 2. cikkének 12. pontjában meghatározott IKT-termék;

13. „IKT-szolgáltatás”: az (EU) 2019/881 rendelet 2. cikkének 13. pontjában meghatározott IKT-szolgáltatás;

14. „IKT-folyamat”: az (EU) 2019/881 rendelet 2. cikkének 14. pontjában meghatározott IKT-folyamat;

15. „sérülékenység”: valamely IKT-termék vagy IKT-szolgáltatás gyengesége, érzékenysége vagy hiányossága, amely egy kiberfenyegetés során kihasználható;

16. „szabvány”: az 1025/2012/EU európai parlamenti és tanácsi rendelet (3) 2. cikkének 1. pontjában meghatározott szabvány;

17. „műszaki előírás”: az 1025/2012/EU rendelet 2. cikkének 4. pontjában meghatározott műszaki előírás;

18. „internetes exchange pont” olyan hálózati létesítmény, amely elsősorban az internetes forgalomcsere megkönnyítése érdekében lehetővé teszi kettőnél több, egymástól független hálózat összekapcsolását (a továbbiakban: autonóm rendszerek), amely kizárólag autonóm rendszerek részére biztosít összekapcsolást, és amely nem kívánja meg, hogy a részt vevő bármely két autonóm rendszer között zajló internetes forgalom egy bármely harmadik autonóm rendszeren is áthaladjon, továbbá nem változtatja meg az említett forgalmat, és egyéb módon sem avatkozik be abba;

19. „doménnévrendszer” vagy „DNS”: hierarchikusan felépülő elnevezési rendszer, amely lehetővé teszi az internetes szolgáltatások és erőforrások azonosítását, lehetővé téve a végfelhasználók eszközei számára az internetes útvonal-meghatározási és összekapcsolási szolgáltatások igénybevételét e szolgáltatások és erőforrások elérése érdekében;

(3) Az Európai Parlament és a Tanács 1025/2012/EU rendelete (2012. október 25.) az európai szabványosításról, a 89/686/EGK és a 93/15/EGK tanácsi irányelv, a 94/9/EK, a 94/25/EK, a 95/16/EK, a 97/23/EK, a 98/34/EK, a 2004/22/EK, a 2007/23/EK, a 2009/23/EK és a 2009/105/EK európai parlamenti és tanácsi irányelv módosításáról, valamint a 87/95/EGK tanácsi határozat és az 1673/2006/EK európai parlamenti és tanácsi határozat hatályon kívül helyezéséről (HL L 316., 2012.11.14., 12. o.).

▼B

20. „DNS-szolgáltató”: olyan szervezet, amely a következőket nyújtja:

    a) nyilvánosan elérhető rekurzív doménnév-feloldási szolgáltatások az internetes végfelhasználók számára; vagy

    b) hiteles doménnév-feloldási szolgáltatások harmadik felek általi felhasználásra, a gyökérnévszerverek kivételével;

21. „legfelső szintű doménnév-nyilvántartó”: olyan szervezet, amelyre egy meghatározott legfelső szintű domént bíztak, és amely felelős egyrészt a legfelső szintű domén kezeléséért – ideértve a legfelső szintű domén alatti doménnevek nyilvántartásba vételét –, másrészt a legfelső szintű domén technikai üzemeltetéséért, amely magában foglalja a névszervereinek üzemeltetését, adatbázisainak karbantartását és a legfelső szintű domén zónafájlok elosztását a névszerverek között, függetlenül attól, hogy ezen üzemeltetési tevékenységek bármelyikét maga a szervezet végzi vagy azokat kiszervezi, kivéve azonban azon eseteket, amikor a legfelső szintű doménneveket a nyilvántartó kizárólag saját használatra veszi igénybe;

22. „doménnév-nyilvántartási szolgáltatásokat nyújtó szervezet”: regisztrátor vagy regisztrátorok nevében eljáró ügynök, például titkosított vagy meghatalmazott regisztrációs szolgáltató vagy viszonteladó;

23. „digitális szolgáltatás”: az (EU) 2015/1535 európai parlamenti és tanácsi irányelv [4] 1. cikke (1) bekezdésének b) pontjában meghatározott szolgáltatás;

24. „bizalmi szolgáltatás”: a 910/2014/EU rendelet 3. cikkének 16. pontjában meghatározott bizalmi szolgáltatás;

25. „bizalmi szolgáltató”: a 910/2014/EU rendelet 3. cikkének 19. pontjában meghatározott bizalmi szolgáltató;

26. „minősített bizalmi szolgáltatás”: a 910/2014/EU rendelet 3. cikkének 17. pontjában meghatározott minősített bizalmi szolgáltatás;

27. „minősített bizalmi szolgáltató”: a 910/2014/EU rendelet 3. cikkének 20. pontjában meghatározott minősített bizalmi szolgáltató;

28. „online piactér”: a 2005/29/EK európai parlamenti és tanácsi irányelv [5] 2. cikkének n) pontjában meghatározott online piactér;

29. „online keresőprogram”: az (EU) 2019/1150 európai parlamenti és tanácsi rendelet [6] 2. cikkének 5. pontjában meghatározott online keresőprogram;

---

(4) Az Európai Parlament és a Tanács (EU) 2015/1535 irányelve (2015. szeptember 9.) a műszaki szabályokkal és az információs társadalom szolgáltatásaira vonatkozó szabályokkal kapcsolatos információszolgáltatási eljárás megállapításáról (HL L 241., 2015.9.17., 1. o.).

(5) Az Európai Parlament és a Tanács 2005/29/EK irányelve (2005. május 11.) a belső piacon az üzleti vállalkozások fogyasztókkal szemben folytatott tisztességtelen kereskedelmi gyakorlatairól, valamint a 84/450/EGK tanácsi irányelv, a 97/7/EK, a 98/27/EK és a 2002/65/EK európai parlamenti és tanácsi irányelvek, valamint a 2006/2004/EK európai parlamenti és tanácsi rendelet módosításáról („Irányelv a tisztességtelen kereskedelmi gyakorlatokról”) (HL L 149., 2005.6.11., 22. o.).

(6) Az Európai Parlament és a Tanács (EU) 2019/1150 rendelete (2019. június 20.) az online közvetítő szolgáltatások üzleti felhasználói tekintetében alkalmazandó tisztességes és átlátható feltételek előmozdításáról (HL L 186., 2019.7.11., 57. o.).

▼B

30. „felhőszolgáltatás": olyan digitális szolgáltatás, amely igény szerinti adminisztrációt és kiterjedt távoli hozzáférést tesz lehetővé megosztható számítástechnikai erőforrások méretezhető és rugalmas készletéhez, beleértve azt is, amikor ezeket az erőforrásokat több helyszínen osztják el;

31. „adatközpont-szolgáltatás": olyan szolgáltatás, amelynek részét képezik olyan struktúrák vagy struktúracsoportok, amelyek az adattárolási, -kezelési és -továbbítási szolgáltatásokat nyújtó informatikai és hálózati berendezések központosított elhelyezésére, összekapcsolására és működtetésére szolgálnak az energia-elosztás és a környezetvédelmi ellenőrzés összes létesítményével és infrastruktúrájával együtt;

32. „tartalomszolgáltató hálózat": földrajzilag elosztott szerverek hálózata, amelynek célja a tartalomszolgáltatók és a szolgáltatásokat nyújtók nevében biztosítani, hogy a digitális tartalmak és szolgáltatások széleskörűen, akadálymentesen és gyorsan az internetfelhasználók rendelkezésére álljanak;

33. „közösségimédia-szolgáltatási platform": olyan platform, amely lehetővé teszi a végfelhasználók számára, hogy több eszközön keresztül kapcsolódjanak, tartalmakat osszanak meg és fedezzenek fel és kommunikáljanak egymással, különösen csevegések, bejegyzések, videók és ajánlások révén;

34. „képviselő": az Unióban letelepedett minden olyan természetes vagy jogi személy, akit vagy amelyet kifejezetten kijelöltek arra, hogy valamely, az Unióban nem letelepedett DNS-szolgáltató, legfelső szintű doménnév-nyilvántartó, doménnév-nyilvántartási szolgáltatásokat nyújtó szervezet, felhőszolgáltató, adatközpont-szolgáltató, tartalomszolgáltató hálózati szolgáltató, irányított szolgáltató, irányított biztonsági szolgáltató, vagy egy online piactér, online keresőprogram vagy közösségimédia-szolgáltatási platform szolgáltatója nevében eljárjon, és akihez vagy amelyhez az illetékes nemzeti hatóság vagy a CSIRT a szervezet ezen irányelv szerinti kötelezettségeit illetően az adott szervezet helyett fordulhat;

35. „közigazgatási szerv": olyan szerv, amelyet az adott tagállam a nemzeti joggal összhangban ilyenként elismer, kivéve az igazságszolgáltatást, a parlamenteket és a központi bankokat, és amely megfelel a következő kritériumoknak:

    a) az általános érdekű szükségletek kielégítése céljából jött létre, és nincs ipari vagy kereskedelmi jellege;

    b) jogi személyiséggel rendelkezik, vagy jogszabály alapján jogosult egy másik, jogi személyiséggel rendelkező szervezet nevében eljárni;

    c) finanszírozását többnyire az állam, regionális hatóságok vagy más, közjog által szabályozott szervek végzik, irányítása az említett hatóságok vagy szervek felügyelete alatt áll, vagy van olyan igazgatási, irányító vagy felügyelő testülete, amely tagjainak több mint felét az állam, a regionális hatóságok vagy más, közjog által szabályozott szervek nevezik ki;

    d) hatásköre van arra, hogy természetes vagy jogi személyekhez a személyek, áruk, szolgáltatások vagy tőke határokon átnyúló mozgásával kapcsolatos jogaikat érintő közigazgatási határozatokat vagy szabályozási döntéseket intézzen;

▼B

36. „nyilvános elektronikus hírközlő hálózat”: az (EU) 2018/1972 irányelv 2. cikkének 8. pontjában meghatározott nyilvános elektronikus hírközlő hálózat;

37. „elektronikus hírközlési szolgáltatás”: az (EU) 2018/1972 irányelv 2. cikkének 4. pontjában meghatározott elektronikus hírközlési szolgáltatás;

38. „szervezet”: olyan természetes vagy jogi személy, amelyet letelepedési helyének nemzeti joga alapján hoztak létre és elismertek, és amely a saját nevében eljárva jogokat gyakorolhat és kötelezettségei lehetnek;

39. „irányított szolgáltató”: olyan szervezet, amely IKT-termékek, -hálózatok, -infrastruktúra, -alkalmazások vagy bármely más hálózati és információs rendszer telepítésével, irányításával, üzemeltetésével vagy karbantartásával kapcsolatos szolgáltatásokat nyújt az ügyfelek helyiségeiben vagy távolról végzett segítségnyújtás vagy aktív adminisztráció révén;

40. „irányított biztonsági szolgáltató”: olyan irányított szolgáltató, amely a kiberbiztonsági kockázatok kezeléséhez kapcsolódó tevékenységeket végez, vagy segítséget nyújt ilyen tevékenységekhez;

41. „kutatóhely”: olyan szervezet, amelynek elsődleges célja alkalmazott kutatás vagy kísérleti fejlesztés folytatása az említett kutatás eredményeinek kereskedelmi célokra való hasznosítása céljából, de amely nem foglalja magában az oktatási intézményeket.

II. FEJEZET

ÖSSZEHANGOLT KIBERBIZTONSÁGI KERETEK

7. cikk

Nemzeti kiberbiztonsági stratégia

(1) A magas szintű kiberbiztonság elérése és fenntartása céljából minden tagállam nemzeti kiberbiztonsági stratégiát fogad el, amely előírja a stratégiai célokat, az e célok eléréséhez szükséges erőforrásokat, valamint a megfelelő szakpolitikai és szabályozási intézkedéseket. A nemzeti kiberbiztonsági stratégiának a következőket kell tartalmaznia:

a) a kiberbiztonságra vonatkozó tagállami stratégia céljai és prioritásai, különösen az I. és II. mellékletben említett ágazatokra vonatkozóan;

b) az e bekezdés a) pontjában említett célok és prioritások eléréséhez szükséges irányítási keretrendszer, ideértve a (2) bekezdésben említett szakpolitikákat;

c) a releváns érdekelt felek szerepét és felelősségi körét nemzeti szinten tisztázó irányítási keret, amely alapul szolgál az ezen irányelv szerinti illetékes hatóságok, egyedüli kapcsolattartó pontok és CSIRT-ek közötti nemzeti szintű együttműködéshez és koordinációhoz, valamint az említett szervek és az ágazatspecifikus uniós jogi aktusok szerinti illetékes hatóságok közötti koordinációhoz és együttműködéshez;

▼B

d) a releváns eszközök azonosítására szolgáló mechanizmus és a kockázatok értékelése az adott tagállamban;

e) az eseményekre való felkészültséget, az azokra való reagálási képességet és az eseményeket követően a működés helyreállítását biztosító intézkedések azonosítása, ideértve a köz- és magánszféra közötti együttműködést is;

f) a nemzeti kiberbiztonsági stratégia végrehajtásában részt vevő különféle hatóságok és érdekelt felek listája;

g) az ezen irányelv és az (EU) 2022/2557 irányelv szerinti illetékes hatóságok közötti, a kockázatokkal, a kiberfenyegetésekkel és az eseményekkel, továbbá a nem kiberbiztonsági jellegű kockázatokkal, fenyegetésekkel és eseményekkel kapcsolatos információk megosztását és adott esetben a felügyeleti feladatok ellátását célzó fokozott koordináció szakpolitikai kerete;

h) a kiberbiztonsággal kapcsolatos tudatosság általános szintjének a polgárok körében történő fokozását célzó terv, ideértve a szükséges intézkedéseket is.

(2) A nemzeti kiberbiztonsági stratégia részeként a tagállamok szakpolitikákat fogadnak el különösen:

a) a szervezetek által szolgáltatásaik nyújtásához használt IKT-termékek és IKT-szolgáltatások ellátási lánca kiberbiztonságának kezelésére;

b) az IKT-termékek és IKT-szolgáltatások kiberbiztonsággal kapcsolatos követelményeinek a közbeszerzésekbe történő felvételére és meghatározására vonatkozóan, többek között a kiberbiztonsági tanúsítás, a titkosítási követelmények és a nyílt forráskódú kiberbiztonsági termékek használata tekintetében;

c) a sérülékenységek kezelésére, amely magában foglalja a sérülékenységek 12. cikk (1) bekezdése szerinti összehangolt közzétételének előmozdítását és megkönnyítését;

d) a nyílt internet nyilvános alkotóelemei általános rendelkezésre állásának, sértetlenségének és bizalmasságának fenntartására vonatkozóan, beleértve adott esetben a tenger alatti kommunikációs kábelek kiberbiztonságát is;

e) a legkorszerűbb kiberbiztonsági kockázatkezelési intézkedések végrehajtását célzó megfelelő fejlett technológiák fejlesztésének és integrációjának előmozdítására;

f) a kiberbiztonsággal, a kiberbiztonsági készségekkel, a figyelemfelkeltéssel, valamint a kutatási és fejlesztési kezdeményezésekkel kapcsolatos oktatás és képzés, valamint a helyes kiberhigiéniai gyakorlatokkal és ellenőrzésekkel kapcsolatos, a polgárokat, az érdekelt feleket és a szervezeteket célzó iránymutatások előmozdítására és fejlesztésére;

g) a tudományos és kutatóintézetek támogatására a kiberbiztonsági eszközök és a biztonságos hálózati infrastruktúra fejlesztése, megerősítése és bevezetésének előmozdítása terén;

▼B

h) vonatkozó eljárások és megfelelő információmegosztási eszközök beépítésére a szervezetek közötti – az uniós jognak megfelelő – önkéntes kiberbiztonsági információmegosztás támogatása céljából;

i) a kis- és középvállalkozások – különösen az ezen irányelv hatálya alól kizárt kkv-k – alapszintű kiberbiztonsági ellenállóképességének és kiberhigiéniájának megerősítésére azok sajátos szükségleteihez igazodó, könnyen hozzáférhető iránymutatások és segítségnyújtás révén;

j) az aktív kiberbiztonság előmozdítására.

(3) A tagállamok az elfogadásuktól számított három hónapon belül értesítik a Bizottságot nemzeti kiberbiztonsági stratégiájukról. Ezen értesítésből a tagállamok kihagyhatják a nemzetbiztonságukkal kapcsolatos információkat.

(4) A tagállamok a fő teljesítménymutatók alapján rendszeresen, de legalább ötévente értékelik nemzeti kiberbiztonsági stratégiájukat, és szükség esetén aktualizálják azt. Az ENISA kérésre segítséget nyújt a tagállamoknak a nemzeti kiberbiztonsági stratégia és a stratégia értékelésére szolgáló fő teljesítménymutatók kidolgozásához vagy aktualizálásához annak érdekében, hogy összehangolja a stratégiát az ezen irányelvben megállapított követelményekkel és kötelezettségekkel.

8. cikk

Illetékes hatóságok és egyedüli kapcsolattartó pontok

(1) Minden tagállam kijelöl vagy létrehoz egy vagy több, a kiberbiztonságért és a VII. fejezetben említett felügyeleti feladatokért felelős illetékes hatóságot (a továbbiakban: illetékes hatóságok).

(2) Az (1) bekezdésben említett illetékes hatóságok nemzeti szinten nyomon követik ezen irányelv végrehajtását.

(3) Minden tagállam kijelöl vagy létrehoz egy egyedüli kapcsolattartó pontot. Amennyiben valamely tagállam az (1) bekezdés alapján csak egy illetékes hatóságot jelöl ki vagy hoz létre, ez az illetékes hatóság lesz a tagállam egyedüli kapcsolattartó pontja is.

(4) Minden egyes egyedüli kapcsolattartó pont összekötő feladatot lát el annak biztosítása érdekében, hogy tagállama hatóságai határokon átnyúlóan együttműködjenek a többi tagállam érintett hatóságaival és adott esetben a Bizottsággal és az ENISA-val, valamint az ágazatok közötti együttműködésnek a tagállama más illetékes nemzeti hatóságaival való biztosítása érdekében.

(5) A tagállamok biztosítják, hogy illetékes hatóságaik és egyedüli kapcsolattartó pontjaik elegendő erőforrással rendelkeznek a rájuk bízott feladatok hatékony és eredményes ellátásához és ezáltal ezen irányelv célkitűzéseinek teljesítéséhez.

(6) Minden tagállam indokolatlan késedelem nélkül értesíti a Bizottságot az (1) bekezdésben említett illetékes hatóságról és a (3) bekezdésben említett egyedüli kapcsolattartó pontról, az említett hatóságok feladatairól és azok minden későbbi változásáról. Minden tagállam nyilvánosságra hozza, hogy mely hatóság az illetékes hatósága. A Bizottság nyilvánosan elérhetővé teszi az egyedüli kapcsolattartó pontok jegyzékét.

▼B

9. cikk

Nemzeti kiberbiztonsági válságkezelési keretek

(1) Minden tagállam kijelöl vagy létrehoz egy vagy több illetékes hatóságot, amely felelős a nagyszabású kiberbiztonsági események és válságok kezeléséért (a továbbiakban: kiberválságok kezelésével foglalkozó hatóságok). A tagállamok biztosítják, hogy az említett hatóságok megfelelő forrásokkal rendelkezzenek a rájuk ruházott feladatok hatékony és eredményes ellátásához. A tagállamok biztosítják a koherenciát a meglévő általános nemzeti válságkezelési keretekkel.

(2) Amennyiben valamely tagállam az (1) bekezdés alapján egynél több, kiberválságok kezelésével foglalkozó hatóságot jelöl ki vagy hoz létre, egyértelműen meg kell jelölnie, hogy e hatóságok közül melyik látja el a koordinátor szerepét a nagyszabású kiberbiztonsági események és válságok kezelésében.

(3) Minden tagállam meghatározza azon képességeket, eszközöket és eljárásokat, amelyek válság esetén ezen irányelv alkalmazásában alkalmazhatók.

(4) Minden tagállam elfogad egy, a nagyszabású kiberbiztonsági események és válságok elhárítására szolgáló nemzeti tervet, amelyben meghatározza a nagyszabású kiberbiztonsági események és válságok kezelésének célkitűzéseit és szabályait. Az említett tervnek különösen a következőket kell meghatároznia:

a) a nemzeti felkészültségi intézkedések és tevékenységek célkitűzései;

b) a kiberválságok kezelésével foglalkozó hatóságok feladatai és felelősségei;

c) a kiberválságok 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 annak biztosítása érdekében, hogy a tagállam hatékonyan részt vegyen a nagyszabású kiberbiztonsági események és válságok uniós szintű összehangolt kezelésében és azt hatékonyan támogassa.

(5) Az (1) bekezdésben említett, kiberválságok kezelésével foglalkozó hatóság kijelölését vagy létrehozását követő három hónapon belül minden tagállam tájékoztatja a Bizottságot a hatóságáról és az azt érintő, minden későbbi változásról. A tagállamok benyújtják a Bizottságnak és az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatának (a továbbiakban: EU-CyCLONe) a nagyszabású kiberbiztonsági esemény- és válságelhárítási nemzeti terveikre vonatkozó, a (4) bekezdésben foglalt követelményekkel kapcsolatos releváns információkat az említett tervek elfogadását követő három hónapon belül. A tagállamok kihagyhatnak információkat, annyiban és amennyiben ez nemzetbiztonságuk szempontjából szükséges.

▼B

10. cikk

Számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek)

(1) Minden tagállam kijelöl vagy létrehoz egy vagy több CSIRT-et. A CSIRT-ek kijelölhetők vagy létrehozhatók egy illetékes hatóságon belül. A CSIRT-eknek meg kell felelniük a 11. cikk (1) bekezdésében meghatározott követelményeknek, legalább az I. és II. mellékletben említett ágazatokra, alágazatokra és szervezettípusokra ki kell terjedniük, és az események egy jól meghatározott folyamat szerinti kezeléséért kell felelniük.

(2) A tagállamok biztosítják, hogy minden CSIRT megfelelő erőforrásokkal rendelkezzen a 11. cikk (3) bekezdésében meghatározott feladatai hatékony végrehajtásához.

(3) A tagállamok biztosítják, hogy az alapvető és fontos szervezetekkel és más érintett érdekelt felekkel folytatott információcsere céljából minden CSIRT rendelkezzen megfelelő, biztonságos és reziliens kommunikációs és információs infrastruktúrával. E célból a tagállamok biztosítják, hogy minden CSIRT részt vegyen a biztonságos információmegosztó eszközök kiépítésében.

(4) A CSIRT-ek együttműködnek, és adott esetben a 29. cikkel összhangban releváns információkat cserélnek az alapvető és fontos szervezetek ágazati vagy ágazatközi csoportjaival.

(5) A CSIRT-ek részt vesznek a 19. cikkel összhangban szervezett szakértői értékelésekben.

(6) A tagállamok biztosítják, hogy a CSIRT-jeik hatékonyan, eredményesen és biztonságosan működjenek együtt a CSIRT-hálózatban.

(7) A CSIRT-ek együttműködési kapcsolatokat alakíthatnak ki harmadik országok nemzeti, számítógép-biztonsági eseményekre reagáló csoportjaival. Ezen együttműködési kapcsolatok részeként a tagállamok elősegítik a megfelelő információmegosztási protokollok – többek között a jelzőlámpa-protokoll (TLP) – használatával történő hatékony, eredményes és biztonságos információcserét harmadik országok nemzeti, számítógép-biztonsági eseményekre reagáló csoportjaival. A CSIRT-ek az uniós adatvédelmi joggal összhangban releváns információkat – többek között személyes adatokat – cserélhetnek harmadik országok nemzeti, számítógép-biztonsági eseményekre reagáló csoportjaival.

(8) A CSIRT-ek együttműködhetnek harmadik országok nemzeti, számítógép-biztonsági eseményekre reagáló csoportjaival vagy azokkal egyenértékű harmadik országbeli szervekkel különösen a célból, hogy kiberbiztonsági segítséget nyújtsanak részükre.

(9) Minden tagállam indokolatlan késedelem nélkül értesíti a Bizottságot az (1) bekezdésben említett CSIRT-ről és a 12. cikk (1) bekezdése értelmében koordinátorként kijelölt CSIRT-ről, az alapvető és fontos szervezetekkel összefüggő feladataikról, valamint az ezekkel kapcsolatos minden későbbi változásról.

(10) A tagállamok kérhetik az ENISA segítségét a CSIRT-jeik kialakításához.

▼B

11. cikk

A CSIRT-ekre vonatkozó követelmények, a CSIRT-ek technikai képességei és feladatai

(1) A CSIRT-eknek meg kell felelniük a következő követelményeknek:

a) a CSIRT-eknek a kritikus hibapontok kiküszöbölése révén biztosítaniuk kell a kommunikációs csatornáik magas szintű elérhetőségét, továbbá elérhetőségük és másokkal való kapcsolattartásuk céljára folyamatosan több eszközt kell fenntartaniuk; a CSIRT-eknek a kommunikációs csatornákat egyértelműen meg kell határozniuk, és azokat a felhasználóik és az együttműködési partnereik tudomására kell hozniuk;

b) a CSIRT-ek hivatali helyiségeit és a támogató információs rendszereket biztonságos helyszíneken kell elhelyezni;

c) a CSIRT-eknek megfelelő rendszerrel kell rendelkezniük a megkeresések kezelésére és továbbítására, különösen a hatékony és eredményes átadás megkönnyítése céljából;

d) a CSIRT-eknek biztosítaniuk kell műveleteik bizalmas jellegét és megbízhatóságát;

e) a CSIRT-eket elegendő személyzettel kell ellátni ahhoz, hogy szolgáltatásaik mindig rendelkezésre álljanak, és gondoskodniuk kell arról, hogy személyzetük megfelelően képzett legyen;

f) a CSIRT-eket redundáns rendszerekkel és tartalék munkaterülettel kell ellátni a szolgáltatásaik folyamatosságának biztosítása érdekében.

A CSIRT-ek részt vehetnek nemzetközi együttműködési hálózatokban.

(2) A tagállamok biztosítják, hogy CSIRT-jeik együttesen rendelkezzenek a (3) bekezdésben említett feladatok végrehajtásához szükséges technikai képességekkel. A tagállamok biztosítják, hogy elegendő erőforrást fordítsanak a CSIRT-jeikre a megfelelő személyzeti létszám biztosításához annak érdekében, hogy a CSIRT-ek fejleszthessék technikai képességeiket.

(3) A CSIRT-ek a következő feladatokat látják el:

a) a kiberfenyegetések, sérülékenységek és események nyomon követése és elemzése nemzeti szinten, valamint kérésre segítségnyújtás az érintett alapvető és fontos szervezetek számára a hálózataik és információs rendszereik valós idejű vagy közel valós idejű nyomon követése tekintetében;

b) a kiberfenyegetésekkel, a sérülékenységekkel és az eseményekkel kapcsolatos korai előrejelzések, riasztások, bejelentéstételek és információterjesztés az érintett alapvető és fontos szervezetek, valamint az illetékes hatóságok és az egyéb releváns érdekelt felek számára, lehetőség szerint közel valós időben;

c) reagálás az eseményekre és adott esetben segítségnyújtás az érintett alapvető és fontos szervezetek számára;

▼B

d) forenzikus adatok gyűjtése és elemzése, továbbá dinamikus kockázat- és eseményelemzés, valamint a kiberbiztonsággal kapcsolatos helyzetismeret biztosítása;

e) valamely alapvető vagy fontos szervezet kérésére az érintett szervezet hálózati és információs rendszerei proaktív átvizsgálásának biztosítása olyan sérülékenységek felderítése céljából, amelyek jelentős hatást gyakorolhatnak;

f) részvétel a CSIRT-hálózatban, valamint kapacitásaiknak és hatásköreiknek megfelelően kölcsönös segítségnyújtás a CSIRT-hálózat többi tagjának azok kérésére;

g) adott esetben a koordinátori szerep betöltése a sérülékenységeknek a 12. cikk (1) bekezdésében említett összehangolt közzététele céljából;

h) hozzájárulás a 10. cikk (3) bekezdése szerinti biztonságos információmegosztási eszközök bevezetéséhez.

A CSIRT-ek proaktív, behatolásmentes átvilágítást végezhetnek az alapvető és fontos szervezetek nyilvánosan hozzáférhető hálózati és információs rendszerein. Ezen átvilágítás célja a sérülékeny vagy nem biztonságosan konfigurált hálózati és információs rendszerek felderítése és az érintett szervezetek tájékoztatása. Ez az átvilágítás semmilyen negatív hatást nem gyakorolhat a szervezetek szolgáltatásainak működésére.

Az első albekezdésben említett feladatok végrehajtása során a CSIRT-ek kockázatalapú megközelítés alapján rangsorolhatnak bizonyos feladatokat.

(4) A CSIRT-ek együttműködési kapcsolatokat alakítanak ki a magánszektor érintett érdekelt feleivel ezen irányelv célkitűzéseinek elérése érdekében.

(5) A (4) bekezdésben említett együttműködés megkönnyítése érdekében a CSIRT-ek előmozdítják a közös vagy szabványosított gyakorlatok, osztályozási rendszerek és rendszertanok elfogadását és alkalmazását a következők tekintetében:

a) az események kezelésre vonatkozó eljárások;

b) válságkezelés; valamint

c) a sérülékenységeknek a 12. cikk (1) bekezdése szerinti összehangolt közzététele.

12. cikk

Sérülékenységek összehangolt közzététele és egy európai sérülékenység-adatbázis

(1) Minden tagállam kijelöli egyik CSIRT-jét koordinátorként a sérülékenységek összehangolt közzététele céljából. A koordinátorként kijelölt CSIRT megbízható közvetítőként jár el, szükség esetén megkönnyítve a sérülékenységet bejelentő természetes vagy jogi személy és a potenciálisan sérülékeny IKT-termékek vagy IKT-szolgáltatások gyártója vagy szolgáltatója közötti kapcsolattartást, bármely fél kérésére. A koordinátorként kijelölt CSIRT feladatai közé tartozik:

▼B

a) az érintett szervezetek azonosítása és a velük való kapcsolatfelvétel;

b) a sérülékenységet bejelentő természetes vagy jogi személyek segítése; és

c) a közzétételi ütemtervek megtárgyalása és a több szervezetet érintő sérülékenységek kezelése.

A tagállamok biztosítják, hogy a természetes vagy jogi személyek – kérésükre névtelenül – bejelenthessenek valamely sérülékenységet a koordinátorként kijelölt CSIRT-nek. A koordinátorként kijelölt CSIRT biztosítja, hogy a bejelentett sérülékenység tekintetében gondos nyomonkövetési intézkedések végrehajtására kerüljön sor, és biztosítja a sérülékenységet bejelentő természetes vagy jogi személy névtelenségét. Ha a bejelentett sérülékenység több tagállamban is jelentős hatást gyakorolhat a szervezetekre, az érintett tagállamok koordinátorként kijelölt CSIRT-jeinek adott esetben együtt kell működnie a többi koordinátorként kijelölt CSIRT-tel a CSIRT-hálózaton belül.

(2) Az ENISA az együttműködési csoporttal folytatott konzultációt követően kidolgozza és fenntartja az európai sérülékenység-adatbázist. E célból az ENISA létrehozza és fenntartja a megfelelő információs rendszereket, szabályzatokat és eljárásokat, valamint elfogadja az európai sérülékenység-adatbázis biztonságának és integritásának biztosításához szükséges műszaki és szervezeti intézkedéseket, különösen annak érdekében, hogy a szervezetek – függetlenül attól, hogy ezen irányelv hatálya alá tartoznak-e – és a hálózati és információs rendszereket biztosító beszállítóik számára lehetővé tegye az IKT-termékekben vagy az IKT-szolgáltatásokban található nyilvánosan ismert sérülékenységek önkéntes alapon történő közzétételét és nyilvántartását. Minden érdekelt fél számára hozzáférést kell biztosítani az európai sérülékenység-adatbázisban található sérülékenységekre vonatkozó információkhoz. Ezen adatbázisnak tartalmaznia kell:

a) a sérülékenységet leíró információkat;

b) az érintett IKT-terméket vagy IKT-szolgáltatásokat, valamint a sérülékenység súlyosságát azon körülmények szempontjából, amelyek között a sérülékenység kihasználható;

c) a kapcsolódó javítások elérhetőségét, valamint elérhető javítás hiányában az illetékes hatóságok vagy a CSIRT-ek által a sérülékeny IKT-termékek és IKT-szolgáltatások felhasználói számára a közzétett sérülékenységekből fakadó kockázatok mérséklésének módjáról kiadott útmutatást.

13. cikk

Nemzeti szintű együttműködés

(1) Ugyanazon tagállam illetékes hatóságai, egyedüli kapcsolattartó pontja, valamint CSIRT-jei – amennyiben különállóak – kötelesek együttműködni az ezen irányelvben meghatározott kötelezettségek végrehajtása tekintetében.

▼B

(2) A tagállamok biztosítják, hogy CSIRT-jeik vagy adott esetben illetékes hatóságaik a 23. cikk értelmében értesítést kapjanak a jelentős eseményekről, valamint a 30. cikk értelmében az eseményekről, kiberfenyegetésekről és majdnem bekövetkezett eseményekről.

(3) A tagállamok biztosítják, hogy CSIRT-jeik vagy adott esetben illetékes hatóságaik tájékoztassák egyedüli kapcsolattartó pontjukat az ezen irányelv alapján bejelentett eseményekről, kiberfenyegetésekről és majdnem bekövetkezett eseményekről.

(4) Annak érdekében, hogy biztosítsák az illetékes hatóságok, az egyedüli kapcsolattartó pontok és a CSIRT-ek feladatainak és kötelezettségeinek hatékony végrehajtását, a tagállamok az adott tagállamon belül lehetőség szerint biztosítják a megfelelő együttműködést az említett szervek és a bűnüldöző hatóságok, az adatvédelmi hatóságok, a 300/2008/EK és az (EU) 2018/1139 rendelet szerinti nemzeti hatóságok, a 910/2014/EU rendelet szerinti felügyeleti szervek, az (EU) 2022/2554 rendelet szerinti illetékes hatóságok, az (EU) 2018/1972 irányelv szerinti nemzeti szabályozó hatóságok, az (EU) 2022/2557 irányelv szerinti illetékes hatóságok, valamint az egyéb ágazatspecifikus uniós jogi aktusok szerinti illetékes hatóságok között.

(5) A tagállamok biztosítják, hogy az ezen irányelv szerinti illetékes hatóságaik és az (EU) 2022/2557 irányelv szerinti illetékes hatóságaik rendszeresen együttműködjenek és információt cseréljenek a kritikus szervezetek azonosításáról, a kockázatokról, a kiberfenyegetésekről és az eseményekről, továbbá az (EU) 2022/2557 irányelv szerint kritikus szervezetként azonosított alapvető szervezeteket érintő nem kiberbiztonsági kockázatokról, fenyegetésekről és eseményekről, valamint az említett kockázatokra, fenyegetésekre és eseményekre való reagálásként hozott intézkedésekről. A tagállamok biztosítják továbbá, hogy az ezen irányelv szerinti illetékes hatóságok és a 910/2014/EU rendelet, az (EU) 2022/2554 rendelet, valamint az (EU) 2018/1972 irányelv szerinti illetékes hatóságaik rendszeresen releváns információkat cseréljenek, többek között a releváns eseményekkel és kiberfenyegetésekkel kapcsolatban.

(6) A tagállamok a 23. és a 30. cikkben említett bejelentések tekintetében technikai eszközök révén egyszerűsítik a jelentéstételt.

III. FEJEZET

UNIÓS ÉS NEMZETKÖZI SZINTŰ EGYÜTTMŰKÖDÉS

14. cikk

Együttműködési csoport

(1) A tagállamok közötti stratégiai együttműködés és információcsere támogatása és megkönnyítése, valamint a bizalom erősítése érdekében együttműködési csoport kerül létrehozásra.

(2) Az együttműködési csoport feladatait a (7) bekezdésben említett kétéves munkaprogramok alapján látja el.

▼B

(3) Az együttműködési csoport a tagállamok, a Bizottság és az ENISA képviselőiből áll. Az Európai Külügyi Szolgálat megfigyelőként vesz részt az együttműködési csoport tevékenységeiben. Az európai felügyeleti hatóságok (a továbbiakban: EFH-k) és az (EU) 2022/2554 rendelet szerinti illetékes hatóságok az említett rendelet 47. cikkének (1) bekezdésével összhangban részt vehetnek az együttműködési csoport tevékenységeiben.

Adott esetben az együttműködési csoport meghívhatja az Európai Parlamentet és az érintett érdekelt felek képviselőit, hogy vegyenek részt a munkájában.

A titkárságot a Bizottság biztosítja.

(4) Az együttműködési csoport a következő feladatokat látja el:

a) iránymutatás nyújtása az illetékes hatóságok számára ezen irányelv átültetésével és végrehajtásával kapcsolatban;

b) iránymutatás nyújtása az illetékes hatóságok számára a sérülékenységek összehangolt közzétételére vonatkozó, a 7. cikk (2) bekezdésének c) pontjában említett szakpolitikák kidolgozásához és végrehajtásához;

c) az ezen irányelv végrehajtásával kapcsolatos bevált gyakorlatok és információk cseréje, többek között a kiberfenyegetések, az események, a sérülékenységek, a majdnem bekövetkezett események, a figyelemfelkeltő kezdeményezések, képzés, gyakorlatok és készségek, a kapacitásépítés, a szabványok és a műszaki előírások, valamint az alapvető és fontos szervezeteknek a 2. cikk (2) bekezdésének b)–e) pontja alapján történő azonosítása tekintetében;

d) tanácsadás és együttműködés a Bizottsággal a kialakítás alatt álló kiberbiztonsági szakpolitikai kezdeményezésekkel és az ágazatspecifikus kiberbiztonsági követelmények általános következetességével kapcsolatban;

e) tanácsadás és együttműködés a Bizottsággal az ezen irányelv alapján elfogadott felhatalmazáson alapuló vagy végrehajtási jogi aktusok tervezetével kapcsolatban;

f) bevált gyakorlatok és információk cseréje az érintett uniós intézményekkel, szervekkel, hivatalokkal és ügynökségekkel;

g) eszmecsere a kiberbiztonságra vonatkozó rendelkezéseket tartalmazó ágazatspecifikus uniós jogi aktusok végrehajtásáról;

h) adott esetben a 19. cikk (9) bekezdésében említett szakértői értékelésről szóló jelentések megvitatása, továbbá következtetések és ajánlások megfogalmazása;

i) a 22. cikk (1) bekezdésével összhangban a kritikus ellátási láncok összehangolt biztonsági kockázatértékelésének elvégzése;

▼B

j) a kölcsönös segítségnyújtás eseteinek megvitatása, beleértve a 37. cikkben említett, határokon átnyúló közös felügyeleti intézkedések tapasztalatait és eredményeit;

k) egy vagy több érintett tagállam kérésére a 37. cikkben említettek szerinti kölcsönös segítségnyújtás iránti konkrét megkeresések megvitatása;

l) stratégiai iránymutatás nyújtása a CSIRT-hálózat és az EU–CyCLONe számára konkrét felmerülő kérdésekben;

m) a CSIRT-hálózat és az EU-CyCLONe által levont tanulságok alapján eszmecsere a nagyszabású kiberbiztonsági eseményeket és válságokat követő nyomonkövetési intézkedésekre vonatkozó szakpolitikáról;

n) hozzájárulás a kiberbiztonsági képességekhez az egész Unióban a nemzeti tisztviselők cseréjének megkönnyítésével az illetékes hatóságok vagy CSIRT-ek munkatársait bevonó kapacitásépítő program révén;

o) rendszeres közös megbeszélések szervezése az Unió egész területéről érkező magánszférabeli érdekelt felekkel, hogy megvitassák az együttműködési csoport tevékenységeit, és információkat gyűjtsenek a felmerülő szakpolitikai kihívásokról;

p) a kiberbiztonsági gyakorlatokkal kapcsolatos munka megvitatása, ideértve az ENISA által végzett munkát is;

q) a 19. cikk (1) bekezdésében említett szakértői értékelések módszertanának és szervezeti szempontjainak megállapítása, valamint a 19. cikk (5) bekezdésével összhangban a tagállamok számára az önértékelési módszertan meghatározása a Bizottság és az ENISA segítségével, valamint a Bizottsággal és az ENISA-val együttműködésben a 19. cikk (6) bekezdésével összhangban a kijelölt kiberbiztonsági szakértők munkamódszereit alátámasztó magatartási kódexek kidolgozása;

r) a 40. cikkben említett felülvizsgálat céljából jelentések készítése a stratégiai szinten és a szakértői értékelésekből szerzett tapasztalatokról;

s) a kiberfenyegetések vagy -események, például a zsarolóvírusok aktuális helyzetének rendszeres megvitatása és értékelése.

Az együttműködési csoport benyújtja az első albekezdés r) pontjában említett jelentéseket a Bizottságnak, az Európai Parlamentnek és a Tanácsnak.

(5) A tagállamok biztosítják, hogy képviselőik hatékonyan, eredményesen és biztonságosan működnek együtt az együttműködési csoportban.

(6) Az együttműködési csoport műszaki jelentést kérhet a CSIRT-hálózattól kiválasztott témákról.

(7) Az együttműködési csoport 2024. február 1-ig, majd azt követően kétévente munkaprogramot állít össze a céljai és feladatai végrehajtása érdekében megvalósítandó intézkedésekről.

▼B

(8) A Bizottság végrehajtási jogi aktusokat fogadhat el, amelyek meghatározzák az együttműködési csoport működéséhez szükséges eljárási szabályokat.

Ezeket a végrehajtási jogi aktusokat a 39. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

A Bizottság a (4) bekezdés e) pontjával összhangban megosztja a szakértelmet és együttműködik az együttműködési csoporttal az e bekezdés első albekezdésében említett végrehajtási jogi aktusok tervezetével kapcsolatban.

(9) Az együttműködési csoport rendszeresen és mindenképpen évente legalább egy alkalommal ülésezik az (EU) 2022/2557 irányelv alapján létrehozott, a kritikus szervezetek rezilienciájával foglalkozó csoporttal a stratégiai együttműködés és az információcsere elősegítése és megkönnyítése érdekében.

15. cikk

A CSIRT-hálózat

(1) A bizalom fejlődéséhez való hozzájárulás és a tagállamok közötti gyors és hatékony operatív együttműködés előmozdítása érdekében létrehozásra kerül a nemzeti CSIRT-hálózat.

(2) A CSIRT-hálózat a 10. cikk alapján kijelölt vagy létrehozott CSIRT-ek, valamint az Unió intézményei, szervei és ügynökségei hálózatbiztonsági vészhelyzeteket elhárító csoportjának (CERT-EU) képviselőiből áll. A Bizottság megfigyelőként vesz részt a CSIRT-hálózatban. Az ENISA biztosítja a titkárságot, és aktívan segítséget nyújt a CSIRT-ek közötti együttműködéshez.

(3) A CSIRT-hálózat a következő feladatokat látja el:

a) információmegosztás a CSIRT-ek képességeiről;

b) a technológiák és a releváns intézkedések, szabályzatok, eszközök, eljárások, bevált gyakorlatok és keretek CSIRT-ek közötti megosztásának, átadásának és cseréjének megkönnyítése;

c) releváns információk cseréje az eseményekről, a majdnem bekövetkezett eseményekről, a kiberfenyegetésekről, a kockázatokról és a sérülékenységekről;

d) a kiberbiztonsági kiadványokkal és ajánlásokkal kapcsolatos információk cseréje;

e) az interoperabilitás biztosítása az információmegosztási előírások és protokollok tekintetében;

f) a CSIRT-hálózat valamely esemény által potenciálisan érintett tagjának kérésére az említett eseményre és a kapcsolódó kiberfenyegetésekre, kockázatokra és sérülékenységekre vonatkozó információk cseréje és azok megvitatása;

g) a CSIRT-hálózat tagjának kérésére az adott tagállam joghatósága alatt azonosított eseményre vonatkozó összehangolt válasz megvitatása és lehetőség szerint végrehajtása;

▼B

h) segítség nyújtása a tagállamoknak a határokon átnyúló események ezen irányelv szerinti kezelése érdekében;

i) együttműködés, a bevált gyakorlatok cseréje és segítségnyújtás a 12. cikk (1) bekezdése szerint koordinátorként kijelölt CSIRT-ek számára az olyan sérülékenységek összehangolt közzétételének kezelése tekintetében, amelyek több tagállamban is jelentős hatást gyakorolhatnak a szervezetekre;

j) az operatív együttműködés további formáinak megvitatása és meghatározása, beleértve a következők tekintetében:

i. a kiberfenyegetések és események kategóriái;

ii. korai előrejelzések;

iii. kölcsönös segítségnyújtás;

iv. a határokon átnyúló kockázatok és események elhárítása koordinálásának elvei és szabályai;

v. tagállami kérésre hozzájárulás a 9. cikk (4) bekezdésében említett nemzeti nagyszabású kiberbiztonsági esemény- és válságelhárítási tervhez;

k) az együttműködési csoport tájékoztatása a tevékenységeiről és az operatív együttműködésnek a j) pont szerint megvitatott további formáiról, és adott esetben iránymutatás kérése az operatív együttműködésre nézve;

l) a kiberbiztonsági gyakorlatok számbavétele, beleértve az ENISA által szervezetteket is;

m) valamely CSIRT kérésére az említett CSIRT képességeinek és felkészültségének megvitatása;

n) együttműködés és információcsere a regionális és uniós szintű biztonsági műveleti központokkal annak érdekében, hogy az egész Unióban javuljon az eseményekkel és a kiberfenyegetésekkel kapcsolatos közös helyzetismeret;

o) adott esetben a 19. cikk (9) bekezdésében említett szakértői értékelési jelentések megvitatása;

p) iránymutatások nyújtása az operatív gyakorlatok konvergenciájának megkönnyítése érdekében e cikk operatív együttműködésre vonatkozó rendelkezéseinek alkalmazása tekintetében.

(4) 2025. január 17-ig, majd azt követően kétévente a CSIRT-hálózat a 40. cikkben említett felülvizsgálat céljából értékeli az operatív együttműködés tekintetében elért előrehaladást, és jelentést fogad el. A jelentés következtetéseket von le és ajánlásokat fogalmaz meg a 19. cikkben említett, a nemzeti CSIRT-ekkel kapcsolatban végzett szakértői értékelések eredményei alapján. Ezt a jelentést be kell nyújtani az együttműködési csoportnak.

(5) A CSIRT-hálózat elfogadja saját eljárási szabályzatát.

(6) A CSIRT-hálózatnak és az EU-CyCLONe-nak meg kell állapodnia az eljárási szabályokról, és azok alapján együtt kell működniük.

▼B

16. cikk

Az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata (EU-CyCLONe)

(1) A nagyszabású kiberbiztonsági események és válságok operatív szintű összehangolt kezelésének támogatása, valamint a releváns információk tagállamok és az Unió intézményei, szervei, hivatalai és ügynökségei közötti rendszeres cseréjének biztosítása érdekében létrehozásra kerül az EU-CyCLONe.

(2) Az EU-CyCLONe a tagállamok kiberválságok kezelésével foglalkozó hatóságainak képviselőiből, valamint azokban az esetekben, amikor egy potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági esemény jelentős hatással van vagy valószínűleg jelentős hatást gyakorolhat az ezen irányelv hatálya alá tartozó szolgáltatásokra és tevékenységekre, a Bizottság képviselőiből áll. Más esetekben a Bizottság megfigyelőként vesz részt az EU-CyCLONe tevékenységeiben.

Az ENISA biztosítja az EU-CyCLONe titkárságát, támogatja a biztonságos információcserét, valamint szolgáltatja a tagállamok közötti együttműködés támogatásához szükséges eszközöket, ezáltal biztosítva a biztonságos információcserét.

Az EU-CyCLONe adott esetben az érintett érdekelt felek képviselőit is felkérheti, hogy megfigyelőként részt vegyenek a munkájában.

(3) Az EU-CyCLONe a következő feladatokat látja el:

a) a nagyszabású kiberbiztonsági események és válságok kezelésére való felkészültség szintjének növelése;

b) közös helyzetismeret kialakítása a nagyszabású kiberbiztonsági eseményekkel és válságokkal kapcsolatban;

c) a releváns nagyszabású kiberbiztonsági események és válságok következményeinek és hatásának értékelése, valamint javaslattétel lehetséges mérséklési intézkedésekre;

d) a nagyszabású kiberbiztonsági események és válságok kezelésének összehangolása és az ilyen eseményekkel és válságokkal kapcsolatos politikai szintű döntéshozatal támogatása;

e) valamely érintett tagállam kérésére a 9. cikk (4) bekezdésében említett nagyszabású nemzeti kiberbiztonsági eseményekre és válságokra való reagálási tervek megvitatása.

(4) Az EU-CyCLONe elfogadja eljárási szabályzatát.

(5) Az EU-CyCLONe rendszeresen jelentést tesz az együttműködési csoportnak a nagyszabású kiberbiztonsági események és válságok kezeléséről, valamint a tendenciákról, különös tekintettel az alapvető és fontos szervezetekre gyakorolt hatásukra.

▼B

(6) Az EU-CyCLONe együttműködik a CSIRT-hálózattal a 15. cikk (6) bekezdésében előírt megállapodás szerinti eljárási szabályok alapján.

(7) Az EU-CyCLONe 2024. július 17-ig, majd azt követően 18 havonta jelentést nyújt be az Európai Parlamentnek és a Tanácsnak munkája értékeléséről.

17. cikk

Nemzetközi együttműködés

Az Unió adott esetben nemzetközi megállapodásokat köthet az EUMSZ 218. cikkével összhangban harmadik országokkal vagy nemzetközi szervezetekkel, lehetővé téve és megszervezve részvételüket az együttműködési csoport, a CSIRT-hálózat és az EU-CyCLONe egyes tevékenységeiben. E megállapodásoknak meg kell felelniük az uniós adatvédelmi jognak.

18. cikk

Jelentés az uniós kiberbiztonsági helyzetről

(1) Az ENISA a Bizottsággal és az együttműködési csoporttal együttműködve kétéves jelentést ad ki az Unió kiberbiztonságának helyzetéről, és azt benyújtja és bemutatja az Európai Parlamentnek. A jelentést többek között géppel olvasható formátumban is elérhetővé kell tenni, és a következőket tartalmazza:

a) uniós szintű kiberbiztonsági kockázatértékelés, amely figyelembe veszi a kiberfenyegetettségi helyzetet;

b) a köz- és a magánszektorbeli kiberbiztonsági képességek egész Unióban megvalósított fejlesztésének értékelése;

c) a kiberbiztonsági tudatosság és a kiberhigiénia általános szintjének értékelése a polgárok és a szervezetek körében, beleértve a kis- és középvállalkozásokat is;

d) a 19. cikkben említett szakértői értékelések eredményének összesített értékelése;

e) kiberbiztonsági képességek és erőforrások érettségi szintjének összesített értékelése Unió-szerte, beleértve az ágazati szintűeket is, valamint a tagállamok nemzeti kiberbiztonsági stratégiái összehangolásának mértékére vonatkozó összesített értékelés.

(2) A jelentésnek konkrét szakpolitikai ajánlásokat kell tartalmaznia a hiányosságok kezelésére és a kiberbiztonság szintjének növelésére az Unió egész területén, valamint tartalmaznia kell az adott időszakra vonatkozó, az ENISA által az (EU) 2019/881 rendelet 7. cikkének (6) bekezdésével összhangban készített, az eseményekről és kiberfenyegetésekről szóló uniós kiberbiztonsági technikai helyzetjelentésekből származó megállapítások összefoglalását.

(3) Az ENISA a Bizottsággal, az együttműködési csoporttal és a CSIRT-hálózattal együttműködésben kidolgozza a módszertant, ezen belül az (1) bekezdés e) pontjában említett összesített értékelés releváns változóit, például a mennyiségi és minőségi indikátorokat.

▼B

19. cikk

Szakértői értékelés

(1) Az együttműködési csoport 2025. január 17-ig a Bizottság, az ENISA és adott esetben a CSIRT-hálózat segítségével kidolgozza a szakértői értékelések módszertanát és szervezeti vonatkozásait a közös tapasztalatokból való tanulás, a kölcsönös bizalom erősítése, a kiberbiztonság egységesen magas szintjének elérése, valamint az ezen irányelv végrehajtásához szükséges tagállami kiberbiztonsági képességek és szakpolitikák fejlesztése céljából. A szakértői értékelésekben való részvétel önkéntes. A szakértői értékelést kiberbiztonsági szakértők végzik. A kiberbiztonsági szakértőket legalább két, az értékelés alatt álló tagállamtól eltérő tagállamnak kell kijelölnie.

A szakértői értékelés a következők legalább egyikéből áll:

a) a 21. és 23. cikkben 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) a 37. cikkben említett kölcsönös segítségnyújtás végrehajtási szintje;

e) a 29. cikkben említett kiberbiztonsági információmegosztási megállapodások végrehajtási szintje;

f) határokon vagy ágazatokon átnyúló jellegű konkrét kérdések.

(2) Az (1) bekezdésben említett módszertannak objektív, megkülönböztetéstől mentes, igazságos és átlátható kritériumokat kell tartalmaznia, amelyek alapján a tagállamok kijelölik a szakértői értékelések elvégzésére jogosult kiberbiztonsági szakértőket. Az ENISA és a Bizottság megfigyelőként vesz részt a szakértői értékelésekben.

(3) A tagállamok az (1) bekezdés f) pontjában említett konkrét kérdéseket határozhatnak meg a szakértői értékelés céljából.

(4) Az (1) bekezdésben említett szakértői értékelés megkezdése előtt a tagállamok értesítik a részt vevő tagállamokat a szakértői értékelés hatóköréről, beleértve a (3) bekezdés alapján meghatározott konkrét kérdéseket is.

(5) A szakértői értékelés megkezdése előtt a szakértői értékelés alatt álló tagállamok önértékelést végezhetnek az értékelt szempontokról, és ezt az önértékelést átadhatják a kijelölt kiberbiztonsági szakértőknek. Az együttműködési csoport a Bizottság és az ENISA segítségével megállapítja a tagállamok önértékelésének módszertanát.

▼B

(6) A szakértői értékeléseknek részét képezik tényleges vagy virtuális helyszíni látogatások és a helyszínen kívüli információcsere. A jó együttműködés elvével összhangban a szakértői értékelés alatt álló tagállam – a bizalmas vagy minősített adatok védelmét szolgáló nemzeti vagy uniós jog sérelme nélkül, illetve az alapvető állami funkciók, például a nemzetbiztonság védelmének sérelme nélkül – a kijelölt kiberbiztonsági szakértőknek megadja az értékeléshez szükséges információkat. Az együttműködési csoport a Bizottsággal és az ENISA-val együttműködve megfelelő magatartási kódexeket dolgoz ki a kijelölt kiberbiztonsági szakértők munkamódszereinek alátámasztására. A szakértői értékelés során kapott információkat kizárólag erre a célra lehet felhasználni. A szakértői értékelésben részt vevő kiberbiztonsági szakértők semmilyen, az adott szakértői értékelés során kapott érzékeny vagy bizalmas információt nem közölhetnek harmadik személyekkel.

(7) A valamely tagállamban szakértői értékelésnek alávetett szempontokkal azonos szempontokat nem lehet az említett tagállamban további szakértői értékelésnek alávetni a szakértői értékelés lezárását követő két éven belül, kivéve, ha a tagállam azt kéri vagy arról az együttműködési csoport javaslata nyomán megállapodás született.

(8) A tagállamok biztosítják, hogy bármely, a kijelölt kiberbiztonsági szakértőket érintő összeférhetetlenség kockázatát a szakértői értékelés megkezdése előtt jelezzék a többi tagállamnak, az együttműködési csoportnak, a Bizottságnak és az ENISA-nak. A szakértői értékelés alatt álló tagállam a kijelölő tagállammal közölt, kellően megindokolt okokból kifogást emelhet egyes kiberbiztonsági szakértők kijelölésével szemben.

(9) A szakértői értékelésekben részt vevő kiberbiztonsági szakértők jelentést készítenek a szakértői értékelések eredményeiről és következtetéseiről. A szakértői értékelés alatt álló tagállamok észrevételeket tehetnek a rájuk vonatkozó jelentéstervezetekre vonatkozóan, és ezeket az észrevételeket csatolni kell a jelentésekhez. A jelentések ajánlásokat tartalmaznak, amelyek lehetővé teszik a helyzet javítását a szakértői értékelésben érintett szempontok területén. A jelentéseket adott esetben be kell nyújtani az együttműködési csoportnak és a CSIRT-hálózatnak. A szakértői értékelés alatt álló tagállam dönthet úgy, hogy jelentését vagy annak szerkesztett változatát nyilvánosan hozzáférhetővé teszi.

IV. FEJEZET

KIBERBIZTONSÁGI KOCKÁZATKEZELÉSI INTÉZKEDÉSEK ÉS JELENTÉSTÉTELI KÖTELEZETTSÉG

20. cikk

Irányítás

(1) A tagállamok biztosítják, hogy az alapvető és fontos szervezetek vezető testületei jóváhagyják az e szervezetek által a 21. cikknek való megfelelés érdekében tett kiberbiztonsági kockázatkezelési intézkedéseket, felügyeljék annak végrehajtását és felelősségre vonhatók legyenek az említett cikknek a szervezetek általi megsértéséért.

E bekezdés alkalmazása nem érinti a közintézményekre alkalmazandó felelősségi szabályokat és a köztisztviselők és a megválasztott vagy kinevezett tisztviselők felelősségét előíró nemzeti jogot.

▼B

(2) A tagállamok biztosítják, hogy az alapvető és fontos szervezetek vezető testületeinek tagjai számára kötelező legyen a képzéseken való részvétel, és ösztönzik az alapvető és fontos szervezeteket arra, hogy munkavállalóik számára rendszeresen hasonló képzéseket biztosítsanak annak érdekében, hogy elsajátítsák a kockázatok azonosításához és a kiberbiztonsági kockázatkezelési gyakorlatok, valamint azoknak a szervezet által nyújtott szolgáltatásokra gyakorolt hatása értékeléséhez szükséges tudást és készségeket.

21. cikk

A kiberbiztonsági kockázatkezelési intézkedések

(1) A tagállamok biztosítják, hogy az alapvető és fontos szervezetek megfelelő és arányos technikai, operatív és szervezési intézkedéseket hozzanak annak érdekében, hogy kezeljék azokat a kockázatokat, amelyek a működésük vagy szolgáltatásaik nyújtása során használt hálózati és információs rendszerek biztonságát fenyegetik, és megelőzzék vagy minimalizálják az eseményeknek a szolgáltatásaik igénybe vevőire és más szolgáltatásokra gyakorolt hatásait.

Figyelembe véve a legkorszerűbb és adott esetben a vonatkozó európai és nemzetközi szabványokat, valamint a végrehajtás költségeit, az első albekezdésben említett intézkedéseknek biztosítaniuk kell a hálózati és információs rendszerek biztonságának a felmerülő kockázatoknak megfelelő szintjét. Ezen intézkedések arányosságának értékelésekor megfelelően figyelembe kell venni a szervezet kockázatoknak való kitettségének mértékét, a szervezet méretét és az események előfordulásának valószínűségét, valamint azok súlyosságát, beleértve társadalmi és gazdasági hatásukat is.

(2) Az (1) bekezdésben említett intézkedéseknek egy minden veszélyre kiterjedő megközelítésen kell alapulniuk, amelynek célja a hálózati és információs rendszerek, valamint e rendszerek fizikai környezetének védelme az eseményekkel szemben, és legalább a következőket kell magukban foglalniuk:

a) kockázatelemzési és az informatikai rendszerek biztonságára vonatkozó szabályzatok;

b) eseménykezelés;

c) üzletmenet-folytonosság, például tartalékrendszerek kezelése, valamint katasztrófa utáni helyreállítás és válságkezelés;

d) az ellátási lánc biztonsága, ideértve az egyes szervezetek és közvetlen beszállítóik vagy szolgáltatóik közötti kapcsolatok biztonságával kapcsolatos szempontokat;

e) biztonság a hálózati és információs rendszerek beszerzésében, fejlesztésében és karbantartásában, beleértve a sérülékenységek kezelését és közzétételét;

f) szabályzatok és eljárások a kiberbiztonsági kockázatkezelési intézkedések hatékonyságának értékelésére;

g) alapvető kiberhigiéniai gyakorlatok és kiberbiztonsági képzés;

▼B

h) a kriptográfia és adott esetben a titkosítás használatára vonatkozó szabályzatok és eljárások;

i) humánerőforrás-biztonság, hozzáférés-ellenőrzési szabályzatok és eszközgazdálkodás;

j) adott esetben többtényezős hitelesítési vagy folyamatos hitelesítési megoldások, biztonságos hang-, video- és szöveges kommunikáció, valamint biztonságos vészhelyzeti kommunikációs rendszerek használata a szervezeten belül.

(3) A tagállamok biztosítják, hogy a szervezetek – amikor azt mérlegelik, hogy az e cikk (2) bekezdésének d) pontjában említett intézkedések közül melyek megfelelők – figyelembe vegyék az egyes közvetlen beszállítókra és szolgáltatókra jellemző sérülékenységeket, valamint a beszállítóik és szolgáltatóik termékeinek és kiberbiztonsági gyakorlatainak – többek között biztonságos fejlesztési eljárásaiknak – az általános minőségét. A tagállamok biztosítják továbbá, hogy a szervezetek – amikor azt mérlegelik, hogy az említett pontban említett intézkedések közül melyek megfelelők – kötelesek legyenek figyelembe venni a 22. cikk (1) bekezdésének megfelelően a kritikus ellátási láncok vonatkozásában elvégzett összehangolt biztonsági kockázatértékelések eredményeit.

(4) A tagállamok biztosítják, hogy az a szervezet, amely megállapítja, hogy nem felel meg a (2) bekezdésben előírt intézkedéseknek, indokolatlan késedelem nélkül meghozza az összes szükséges, megfelelő és arányos korrekciós intézkedést.

(5) 2024. október 17-ig a Bizottság végrehajtási jogi aktusokat fogad el, amelyekben meghatározza a (2) bekezdésben említett intézkedések technikai és módszertani követelményeit a DNS-szolgáltatók, a legfelső szintű doménnév-nyilvántartók, a felhőszolgáltatók, az adatközpont-szolgáltatók, a tartalomszolgáltató hálózati szolgáltatók, az irányított szolgáltatók, az irányított biztonsági szolgáltatók, az online piacterek, az online keresőprogramok és a közösségimédia-szolgáltatási platformok szolgáltatói, valamint a bizalmi szolgáltatók tekintetében.

A Bizottság végrehajtási jogi aktusokat fogadhat el, amelyekben az e bekezdés első albekezdésében említettektől eltérő alapvető és fontos szervezetek tekintetében meghatározza a (2) bekezdésben említett intézkedések technikai és módszertani követelményeit, valamint szükség esetén ágazati követelményeit.

Az e bekezdés első és második albekezdésében említett végrehajtási jogi aktusok előkészítése során a Bizottság a lehető legnagyobb mértékben követi az európai és nemzetközi szabványokat, valamint a vonatkozó műszaki előírásokat. A Bizottság a 14. cikk (4) bekezdésének e) pontjával összhangban megosztja a szakértelmet és együttműködik az együttműködési csoporttal és az ENISA-val a végrehajtási jogi aktusok tervezetével kapcsolatban.

Ezeket a végrehajtási jogi aktusokat a 39. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

22. cikk

A kritikus ellátási láncok uniós szintű összehangolt biztonsági kockázatértékelése

(1) Az együttműködési csoport a Bizottsággal és az ENISA-val együttműködve összehangolt biztonsági kockázatértékeléseket végezhet a kritikus IKT-szolgáltatások, IKT-rendszerek vagy IKT-termékek ellátási láncai tekintetében, figyelembe véve a technikai, és adott esetben a nem technikai kockázati tényezőket.

▼B

(2) A Bizottság az együttműködési csoporttal és az ENISA-val, valamint adott esetben az érdekelt felekkel folytatott konzultációt követően meghatározza azokat a kritikus IKT-szolgáltatásokat, IKT-rendszereket vagy IKT-termékeket, amelyekre az (1) bekezdésben említett összehangolt biztonsági kockázatértékelés vonatkozhat.

23. cikk

Jelentéstételi kötelezettség

(1) Minden tagállam biztosítja, hogy az alapvető és fontos szervezetek a (4) bekezdéssel összhangban indokolatlan késedelem nélkül értesítsék a CSIRT-jét vagy adott esetben az illetékes hatóságát minden olyan eseményről, amely jelentős hatással van a (3) bekezdésben említett szolgáltatásaik nyújtására (jelentős esemény). Adott esetben az érintett szervezetek indokolatlan késedelem nélkül értesítik a szolgáltatásaikat igénybe vevőket azon jelentős eseményekről, amelyek valószínűleg hátrányosan érintik az említett szolgáltatások nyújtását. Minden tagállam biztosítja, hogy ezek a szervezetek jelentsenek többek között minden olyan információt, amely lehetővé teszi a CSIRT vagy adott esetben az illetékes hatóság számára, hogy meghatározza az esemény határokon átnyúló hatásait. Pusztán a bejelentés következtében a bejelentő szervezetet többletfelelősség nem terhelheti.

Amennyiben az érintett szervezetek az első albekezdés szerint jelentős eseményről értesítik az illetékes hatóságot, a tagállam biztosítja, hogy az említett illetékes hatóság a kézhezvételt követően továbbítsa az értesítést a CSIRT-nek.

Határokon átnyúló vagy ágazatközi jelentős esemény esetén a tagállamok biztosítják, hogy egyedüli kapcsolattartó pontjaik kellő időben megkapják a (4) bekezdéssel összhangban bejelentett releváns információkat.

(2) Adott esetben a tagállamok biztosítják, hogy az alapvető és a fontos szervezetek indokolatlan késedelem nélkül közöljék a jelentős kiberfenyegetés által potenciálisan érintett szolgáltatásaik igénybe vevőivel azon intézkedéseket, illetve fenyegetést orvosló lehetőségeket, amelyeket a szolgáltatások igénybe vevői a fenyegetésre válaszul maguk megtehetnek, illetve amelyekkel élhetnek. Adott esetben a szervezetek az igénybe vevőket magáról a jelentős kiberfenyegetésről is tájékoztatják.

(3) Egy esemény akkor tekintendő jelentősnek, ha:

a) súlyos működési zavart okozott vagy képes okozni a szolgáltatásokban, vagy pénzügyi veszteséget okozott az érintett szervezetnek;

b) az esemény jelentős vagyoni vagy nem vagyoni kár okozásával más természetes vagy jogi személyeket érintett vagy képes érinteni.

(4) A tagállamok biztosítják, hogy az (1) bekezdés szerinti bejelentés céljából az érintett szervezetek benyújtsanak a CSIRT-nek vagy adott esetben az illetékes hatóságnak:

a) indokolatlan késedelem nélkül és minden esetben a jelentős eseményről való tudomásszerzéstől számított 24 órán belül egy korai előrejelzést, amelyben adott esetben fel kell tüntetni, hogy a jelentős eseményt vélhetően jogellenes vagy rosszindulatú cselekmény okozta-e és hogy lehet-e határokon átnyúló hatása;

▼B

b) indokolatlan késedelem nélkül és minden esetben a jelentős eseményről való tudomásszerzéstől számított 72 órán belül egy eseménybejelentést, amely adott esetben aktualizálja az a) pontban említett információkat, és tartalmazza a jelentős esemény első értékelését, beleértve annak súlyosságát és hatását, valamint – amennyiben rendelkezésre állnak – a fertőzöttségi mutatókat;

c) a CSIRT vagy adott esetben az illetékes hatóság kérésére közbenső helyzetjelentést;

d) zárójelentést, legkésőbb a b) pont szerinti eseménybejelentés benyújtását követő egy hónapon belül, amely tartalmazza a következőket:

i. az esemény részletes leírása, beleértve annak súlyosságát és hatását;

ii. az eseményt valószínűleg kiváltó fenyegetés vagy kiváltó ok típusa;

iii. alkalmazott és folyamatban lévő mérséklési intézkedések;

iv. adott esetben az esemény határokon átnyúló hatása;

e) abban az esetben, ha a d) pontban említett zárójelentés benyújtásának időpontjában folyamatban van az esemény, a tagállamok biztosítják, hogy az említett időpontban az érintett szervezetek benyújtsanak egy jelentést az addig elért eredményekről, az esemény általuk való kezelését követő egy hónapon belül pedig egy zárójelentést.

Az első albekezdés b) pontjától eltérve a bizalmi szolgáltató indokolatlan késedelem nélkül és minden esetben a jelentős eseményről való tudomásszerzést követő 24 órán belül értesíti a CSIRT-et vagy adott esetben az illetékes hatóságot a bizalmi szolgáltatásai nyújtására hatást gyakorló jelentős eseményekről.

(5) A CSIRT vagy az illetékes hatóság haladéktalanul és – ha lehetséges – a (4) bekezdés a) pontjában említett korai előrejelzés kézhezvételétől számított 24 órán belül választ ad – többek között egy kezdeti visszajelzést küld a jelentős eseményről – a bejelentő szervezetnek, valamint – a szervezet kérésére – útmutatást vagy operatív tanácsokat nyújt a lehetséges mérséklési intézkedések végrehajtásáról. Ha nem a CSIRT az (1) bekezdésben említett bejelentés első címzettje, az útmutatást az illetékes hatóság a CSIRT-tel együttműködve nyújtja. A CSIRT további technikai támogatást nyújt, ha az érintett szervezet ezt kéri. Ha a jelentős esemény gyaníthatóan büntetőjogi természetű, a CSIRT vagy az illetékes hatóság a jelentős esemény bűnüldöző hatóságoknak történő bejelentésére vonatkozóan is útmutatást ad.

(6) Adott esetben, és különösen, ha a jelentős esemény két vagy több tagállamot érint, a CSIRT, az illetékes hatóság vagy az egyedüli kapcsolattartó pont haladéktalanul tájékoztatja a jelentős eseményről a többi érintett tagállamot és az ENISA-t. Ezeknek az információknak tartalmazniuk kell a (4) bekezdéssel összhangban kapott információk típusát. Ennek során a CSIRT-nek, az illetékes hatóságnak vagy az egyedüli kapcsolattartó pontnak az uniós vagy nemzeti joggal összhangban meg kell óvniuk a szervezet biztonsági és üzleti érdekeit, valamint a benyújtott információk titkosságát.

▼B

(7) Ha a jelentős esemény megelőzéséhez vagy egy folyamatban lévő jelentős esemény kezeléséhez lakossági figyelemfelkeltés szükséges, vagy ha a jelentős esemény nyilvánosságra hozatala egyébként közérdek, a tagállam CSIRT-je vagy adott esetben az illetékes hatósága, és adott esetben a többi érintett tagállam CSIRT-jei vagy illetékes hatóságai az érintett szervezettel folytatott konzultációt követően tájékoztathatják a nyilvánosságot a jelentős eseményről, vagy ezt előírhatják a szervezet számára.

(8) A CSIRT vagy az illetékes hatóság kérésére az egyedüli kapcsolattartó pont az (1) bekezdés alapján kapott bejelentéseket továbbítja a többi érintett tagállam egyedüli kapcsolattartó pontjának.

(9) Az egyedüli kapcsolattartó pont háromhavonta összefoglaló jelentést nyújt be az ENISA-nak, amely névtelen és összesített adatokat tartalmaz az e cikk (1) bekezdésével és a 30. cikkel összhangban bejelentett jelentős eseményekről, eseményekről, kiberfenyegetésekről és majdnem bekövetkezett eseményekről. Az összehasonlítható információk szolgáltatásához való hozzájárulás érdekében az ENISA technikai útmutatást fogadhat el az összefoglaló jelentésbe belefoglalandó információk paramétereiről. Az ENISA hathavonta tájékoztatja az együttműködési csoportot és a CSIRT-hálózatot a beérkezett bejelentésekről tett megállapításairól.

(10) A CSIRT-ek vagy adott esetben az illetékes hatóságok az (EU) 2022/2557 irányelv alapján kritikus szervezetként azonosított szervezetek által az e cikk (1) bekezdésével és a 30. cikkel összhangban bejelentett jelentős eseményekről, eseményekről, kiberfenyegetésekről és a majdnem bekövetkezett eseményekről tájékoztatják az (EU) 2022/2557 irányelv szerinti illetékes hatóságokat.

(11) A Bizottság végrehajtási jogi aktusokat fogadhat el, amelyek meghatározzák az információk típusát, valamint az e cikk (1) bekezdése és a 30. cikk alapján benyújtott bejelentés és az e cikk (2) bekezdése alapján benyújtott értesítés formátumát és eljárását.

2024. október 17-ig a Bizottság a DNS-szolgáltatók, a legfelső szintű doménnév-nyilvántartók, a felhőszolgáltatók, az adatközpont-szolgáltatók, a tartalomszolgáltató hálózati szolgáltatók, az irányított szolgáltatók, az irányított biztonsági szolgáltatók, valamint az online piacterek, az online keresőprogramok és a közösségimédia-szolgáltatási platformok szolgáltatói tekintetében végrehajtási jogi aktusokat fogad el, amelyekben részletesebben meghatározza azokat az eseteket, amikor egy esemény a (3) bekezdésben említettek szerint jelentősnek tekintendő. A Bizottság elfogadhat ilyen végrehajtási jogi aktusokat más alapvető és fontos szervezetek tekintetében is.

A Bizottság a 14. cikk (4) bekezdésének e) pontjával összhangban megosztja a szakértelmet és együttműködik az együttműködési csoporttal az e bekezdés első és második albekezdésében említett végrehajtási jogi aktusok tervezetével kapcsolatban.

Ezeket a végrehajtási jogi aktusokat a 39. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

▼B

24. cikk

Az európai kiberbiztonsági tanúsítási rendszerek használata

(1) A 21. cikk egyes követelményeinek való megfelelés igazolása érdekében a tagállamok előírhatják az alapvető és fontos szervezetek számára, hogy bizonyos – az alapvető vagy fontos szervezet által fejlesztett, vagy harmadik felektől beszerzett – az (EU) 2019/881 rendelet 49. cikke alapján elfogadott európai kiberbiztonsági tanúsítási rendszerek által tanúsított IKT-termékeket, IKT-szolgáltatásokat és IKT-folyamatokat használjanak. Ezenkívül a tagállamok ösztönzik az alapvető és fontos szervezeteket, hogy vegyenek igénybe minősített bizalmi szolgáltatásokat.

(2) A Bizottság felhatalmazást kap arra, hogy a 38. cikknek megfelelően felhatalmazáson alapuló jogi aktusokat fogadjon el ezen irányelv kiegészítésére, meghatározva, hogy az alapvető és fontos szervezetek mely kategóriái számára kell előírni, hogy bizonyos, az (EU) 2019/881 rendelet 49. cikke alapján elfogadott európai kiberbiztonsági tanúsítási rendszerek keretében tanúsított IKT-termékeket, IKT-szolgáltatásokat és IKT-folyamatokat használjanak. Az említett felhatalmazáson alapuló jogi aktusokat abban az esetben kell elfogadni, ha elégtelen kiberbiztonsági szintet állapítanak meg, és azoknak végrehajtási időszakot kell előírniuk.

Az ilyen felhatalmazáson alapuló jogi aktusok elfogadása előtt a Bizottság az (EU) 2019/881 rendelet 56. cikkével összhangban hatásvizsgálatot végez és konzultációkat folytat.

(3) Amennyiben nem áll rendelkezésre megfelelő európai kiberbiztonsági tanúsítási rendszer e cikk (2) bekezdésének céljára, a Bizottság az együttműködési csoporttal és az európai kiberbiztonsági tanúsítási csoporttal folytatott konzultációt követően felkérheti az ENISA-t, hogy készítsen egy javasolt tanúsítási rendszert az (EU) 2019/881 rendelet 48. cikkének (2) bekezdése alapján.

25. cikk

Szabványosítás

(1) A 21. cikk (1) és (2) bekezdése konvergens végrehajtásának előmozdítása érdekében a tagállamok – anélkül, hogy előírnák vagy előnyben részesítenék egy adott típusú technológia alkalmazását – ösztönzik a hálózati és információs rendszerek biztonsága tekintetében releváns európai és nemzetközi szabványok és műszaki előírások alkalmazását.

(2) Az ENISA a tagállamokkal együttműködve és adott esetben az érintett érdekelt felekkel folytatott konzultációt követően tanácsokat és iránymutatásokat dolgoz ki az (1) bekezdéssel összefüggésben mérlegelendő technikai területekről, valamint a már meglévő szabványokról – beleértve a nemzeti szabványokat is –, amelyek lehetővé tennék az említett területek lefedését.

V. FEJEZET

JOGHATÓSÁG ÉS NYILVÁNTARTÁS

26. cikk

Joghatóság és területi elv

(1) Az ezen irányelv hatálya alá tartozó szervezeteket a letelepedésük szerinti tagállam joghatósága alá tartozónak kell tekinteni, kivéve:

▼B

a) a nyilvános elektronikus hírközlő hálózatok szolgáltatóit vagy a nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatókat, amelyeket úgy kell tekinteni, hogy a szolgáltatásnyújtásuk helye szerinti tagállam joghatósága alá tartoznak;

b) azokat a DNS-szolgáltatókat, legfelső szintű doménnév-nyilvántartókat és doménnév-nyilvántartási szolgáltatásokat nyújtó szervezeteket, felhőszolgáltatókat, adatközpont-szolgáltatókat, tartalomszolgáltató hálózati szolgáltatókat, irányított szolgáltatókat és irányított biztonsági szolgáltatókat, valamint az online piacterek, az online keresőprogramok és a közösségimédia-szolgáltatási platformok szolgáltatóit, amelyeket annak a tagállamnak a joghatósága alá tartozónak kell tekinteni, amelyben a (2) bekezdés alapján az Unióban üzleti tevékenységük fő helye található;

c) azokat a közigazgatási szerveket, amelyek az azokat létrehozó tagállam joghatósága alá tartozónak kell tekinteni.

(2) Ezen irányelv alkalmazásában úgy kell tekinteni, hogy az (1) bekezdés b) pontjában említett szervezet üzleti tevékenységének fő helye az Unióban abban a tagállamban van, ahol a kiberbiztonsági kockázatkezelési intézkedésekkel kapcsolatos döntéseket túlnyomórészt meghozzák. Ha ilyen tagállam nem határozható meg, vagy az ilyen döntéseket nem az Unióban hozzák meg, akkor úgy kell tekinteni, hogy az üzleti tevékenység fő helye abban a tagállamban található, ahol a kiberbiztonsági műveleteket végzik. Ha ilyen tagállam nem határozható meg, akkor az üzleti tevékenység fő helyét abban a tagállamban levőnek kell tekinteni, ahol az érintett szervezetnek az Unióban a legmagasabb munkavállalói létszámmal rendelkező telephelye van.

(3) Ha az (1) bekezdés b) pontjában említett szervezet nem az Unióban letelepedett, de az Unión belül kínál szolgáltatásokat, ki kell jelölnie egy képviselőt az Unióban. A képviselőnek azon tagállamok valamelyikében kell letelepedettnek lennie, ahol a szolgáltatásokat kínálják. Az ilyen szervezetet a képviselő letelepedése szerinti tagállam joghatósága alá tartozónak kell tekinteni. E bekezdés alapján az Unióban kijelölt képviselő hiányában bármely olyan tagállam, amelyben a szervezet szolgáltatásokat nyújt, jogi lépéseket tehet a szervezet ellen ezen irányelv megsértése miatt.

(4) A képviselő (1) bekezdés b) pontjában említett szervezet általi kijelölése nem érinti azokat a jogi lépéseket, amelyek maga a szervezet ellen kezdeményezhetők.

(5) Amennyiben egy tagállamhoz kölcsönös segítségnyújtás iránti megkeresés érkezik az (1) bekezdés b) pontjában említett szervezettel kapcsolatban, a megkeresés keretein belül felügyeleti és végrehajtási intézkedéseket hozhat azon érintett szervezettel kapcsolatban, amely a területén szolgáltatásokat nyújt vagy amelynek a hálózati és információs rendszere a területén található.

27. cikk

Az alapvető és fontos szervezetek nyilvántartása

(1) Az ENISA az egyedüli kapcsolattartó ponttól a (4) bekezdéssel összhangban kapott információk alapján létrehozza és fenntartja 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,

▼B

valamint az online piacterek, az online keresőprogramok és a közösségimédia-szolgáltatási platformok szolgáltatói nyilvántartását. Az ENISA kérésre hozzáférést enged az illetékes hatóságok számára az említett nyilvántartáshoz, ugyanakkor biztosítva adott esetben az információk bizalmas jellegének védelmét.

(2) A tagállamok előírják az (1) bekezdésben említett szervezetek számára, hogy 2025. január 17-ig nyújtsák be a következő információkat az illetékes hatóságoknak:

a) a szervezet neve;

b) adott esetben az I. vagy II. mellékletben említett érintett ágazat, alágazat és szervezettípus;

c) a szervezet üzleti tevékenysége fő helyének és egyéb Unión belüli jogszerű telephelyének, vagy ha az Unióban nem letelepedett, a 26. cikk (3) bekezdése szerint kijelölt képviselőjének a címe;

d) a szervezet és adott esetben a 26. cikk (3) bekezdése szerint kijelölt képviselőjének naprakész elérhetőségei, beleértve e-mail-címét és telefonszámát is;

e) azok a tagállamok, ahol a szervezet szolgáltatásokat nyújt; továbbá

f) a szervezet IP-tartományai.

(3) A tagállamok biztosítják, hogy az (1) bekezdésben említett szervezetek a (2) bekezdés alapján benyújtott adatokban bekövetkezett minden változást haladéktalanul, és minden esetben a változás időpontjától számított három hónapon belül bejelentsenek az illetékes hatóságnak.

(4) A (2) és (3) bekezdésben említett információk – a (2) bekezdés f) pontjában említett információkat ide nem értve – kézhezvételét követően az érintett tagállam egyedüli kapcsolattartó pontja indokolatlan késedelem nélkül továbbítja ezeket az információkat az ENISA-nak.

(5) Az e cikk (2) és (3) bekezdésében említett információkat adott esetben a 3. cikk (4) bekezdésének negyedik albekezdésében említett nemzeti mechanizmus révén kell benyújtani.

28. cikk

A doménnevek nyilvántartási adatainak adatbázisa

(1) A DNS biztonságához, stabilitásához és rezilienciájához való hozzájárulás céljából a tagállamok előírják, hogy a legfelső szintű doménnév-nyilvántartók és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek – a személyes adatnak minősülő adatok tekintetében az uniós adatvédelmi jogszabályoknak megfelelően – a kellő gondossággal, egy erre kijelölt adatbázisban gyűjtsék és kezeljék a pontos és teljes doménnév-nyilvántartási adatokat.

(2) A tagállamok az (1) bekezdés alkalmazásában előírják, hogy a doménnév-nyilvántartási adatok adatbázisai tartalmazzák a szükséges információkat a doménnevek tulajdonosai és a legfelső szintű domének alatt bejegyzett doménneveket kezelő kapcsolattartó pontok azonosításához és a velük való kapcsolatfelvételhez. Az ilyen információk magukban foglalják:

▼B

a) a doménnevet;

b) a nyilvántartásba vétel időpontját;

c) a regisztráló nevét, kapcsolattartási e-mail címét és telefonszámát;

d) a doménnevet kezelő kapcsolattartó pont kapcsolattartási e-mail címét és telefonszámát, amennyiben azok eltérnek a regisztrálóétól.

(3) A tagállamok előírják, hogy a legfelső szintű doménnév-nyilvántartók és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek rendelkezzenek szabályzatokkal és eljárásokkal – többek között ellenőrzési eljárásokkal – annak biztosítására, hogy az (1) bekezdésben említett adatbázisok pontos és teljes információkat tartalmazzanak. A tagállamok előírják, hogy az említett szabályzatokat és eljárásokat nyilvánosan hozzáférhetővé kell tenni.

(4) A tagállamok előírják, hogy a legfelső szintű doménnév-nyilvántartók és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek a doménnév nyilvántartásba vétele után indokolatlan késedelem nélkül nyilvánosan hozzáférhetővé tegyék azokat a doménnév-nyilvántartási adatokat, amelyek nem személyes adatok.

(5) A tagállamok előírják a legfelső szintű doménnév-nyilvántartók és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek számára, hogy a jogosult hozzáférés-igénylők jogszerű és kellően indokolt kérésére az uniós adatvédelmi jogszabályokkal összhangban betekintést biztosítsanak meghatározott doménnév-nyilvántartási adatokba. A tagállamok előírják a legfelső szintű doménnév-nyilvántartók és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek számára, hogy indokolatlan késedelem nélkül – de minden esetben a kézhezvételtől számított 72 órán belül – megválaszoljanak minden hozzáférési kérelmet. A tagállamok előírják, hogy az ilyen adatok nyilvánosságra hozatalára vonatkozó szabályzatokat és eljárásokat nyilvánosan hozzáférhetővé kell tenni.

(6) Az (1)–(5) bekezdésben megállapított kötelezettségeknek való megfelelés nem eredményezheti a doménnév-nyilvántartási adatok gyűjtésének megkettőzését. E célból a tagállamok előírják a legfelső szintű doménnév-nyilvántartók és a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek számára az egymással való együttműködést.

VI. FEJEZET

INFORMÁCIÓMEGOSZTÁS

29. cikk

Kiberbiztonsági információmegosztási megállapodások

(1) A tagállamok biztosítják, hogy az ezen irányelv hatálya alá tartozó szervezetek és adott esetben az ezen irányelv hatálya alá nem tartozó egyéb szervezetek önkéntes alapon megoszthassák egymással a vonatkozó kiberbiztonsági információkat, ideértve a kiberfenyegetésekre, a majdnem bekövetkezett eseményekre, a sérülékenységekre, a technikákra és eljárásokra, a fertőzöttségi mutatókra, az ellenséges taktikákra, az elkövetővel kapcsolatos információkra, a kiberbiztonsági figyelmeztetésekre, valamint a kibertámadások észlelésére szolgáló biztonságieszköz-konfigurációkra vonatkozó ajánlásokkal kapcsolatos információkat, amennyiben az említett információmegosztás:

▼B

a) célja, hogy megelőzze, észlelje az eseményeket, reagáljon azokra vagy az eseményeket követően helyreállítsa a működést, illetve mérsékelje az események hatását;

b) növeli a kiberbiztonság szintjét, különösen azáltal, hogy felhívja a figyelmet a kiberfenyegetésekre, korlátozza vagy gátolja az ilyen fenyegetések terjedési képességét, támogatja a védelmi képességek széles skáláját, a sérülékenység elhárítását és nyilvánosságra hozatalát, a fenyegetésészlelési, -korlátozási és -megelőzési technikákat, a mérséklési stratégiákat vagy az elhárítási és helyreállítási szakaszt, vagy előmozdítja az állami szervek és magánszervezetek közötti együttműködésen alapuló, kiberfenyegetésekkel kapcsolatos kutatásokat.

(2) A tagállamok biztosítják, hogy az információkat megosszák az alapvető és fontos szervezetek és adott esetben beszállítóik és szolgáltatóik közösségeiben. Az említett megosztást kiberbiztonsági információmegosztási megállapodások útján kell végrehajtani a megosztott információk potenciálisan érzékeny jellegét tiszteletben tartva.

(3) A tagállamok elősegítik az e cikk (2) bekezdésében említett kiberbiztonsági információmegosztási megállapodások létrehozását. Az ilyen megállapodások meghatározhatják az információmegosztási megállapodások működési elemeit – ideértve dedikált IKT-platformok és automatizálási eszközök használatát –, tartalmát és feltételeit. A tagállamok a hatóságok említett megállapodásokban való részvétele részleteinek meghatározása során feltételeket szabhatnak az illetékes hatóságok vagy a CSIRT-ek által rendelkezésre bocsátott információkra vonatkozóan. A tagállamok segítséget nyújtanak az említett megállapodások alkalmazásához az 7. cikk (2) bekezdésének g) pontjában említett szakpolitikájukkal összhangban.

(4) A tagállamok biztosítják, hogy az alapvető és fontos szervezetek az említett megállapodások megkötésekor értesítsék az illetékes hatóságokat a (2) bekezdésben említett kiberbiztonsági információmegosztási megállapodásokban való részvételükről, vagy adott esetben az említett megállapodások felmondásáról, a felmondás hatálybalépésekor.

(5) Az ENISA bevált gyakorlatok megosztásával és útmutatás nyújtásával segítséget nyújt a (2) bekezdésben említett kiberbiztonsági információmegosztási megállapodások létrehozásához.

30. cikk

A releváns információk önkéntes bejelentése

(1) A tagállamok biztosítják, hogy a 23. cikkben előírt értesítési kötelezettségen túlmenően a CSIRT-ekhez vagy adott esetben az illetékes hatóságokhoz önkéntes alapon be lehessen nyújtani bejelentéseket az alábbiak által:

a) alapvető és fontos szervezetek az események, a kiberfenyegetések és a majdnem bekövetkezett események tekintetében;

▼B

b) az a) pontban említettektől eltérő szervezetek – függetlenül attól, hogy ezen irányelv hatálya alá tartoznak-e – a jelentős események, a kiberfenyegetések és a majdnem bekövetkezett események tekintetében.

(2) A tagállamok az e cikk (1) bekezdésében említett bejelentéseket a 23. cikkben megállapított eljárásnak megfelelően dolgozzák fel. A tagállamok előnyben részesíthetik a kötelező bejelentések feldolgozását az önkéntes bejelentésekkel szemben.

Szükség esetén a CSIRT-ek és adott esetben az illetékes hatóságok átadják az egyedüli kapcsolattartó pontoknak az e cikk alapján kapott bejelentésekre vonatkozó információkat, biztosítva ugyanakkor a bejelentő szervezet által nyújtott információk bizalmas kezelését és megfelelő védelmét. A bűncselekmények megelőzésének, kivizsgálásának, felderítésének és büntetőeljárás alá vonásának sérelme nélkül, az önkéntes adatszolgáltatás nem eredményezhet a bejelentő szervezetre nézve olyan további kötelezettségeket, amelyek nem vonatkoztak volna rá, ha nem nyújtja be a bejelentést.

VII. FEJEZET

FELÜGYELET ÉS VÉGREHAJTÁS

31. cikk

A felügyelet és a végrehajtás általános szempontjai

(1) A tagállamok biztosítják, hogy az illetékes hatóságaik ténylegesen felügyeljék és megtegyék az ezen irányelvnek való megfelelés biztosításához szükséges intézkedéseket.

(2) A tagállamok engedélyezhetik az illetékes hatóságaik számára, hogy rangsorolják a felügyeleti feladatokat. Az ilyen rangsorolásnak kockázatalapú megközelítésen kell alapulnia. Ennek érdekében a 32. és 33. cikkben előírt felügyeleti feladataik ellátása keretében az illetékes hatóságok kialakíthatnak olyan felügyeleti módszereket, amelyek lehetővé teszik e feladatok kockázatalapú megközelítés alapján történő rangsorolását.

(3) Az illetékes hatóságok szorosan együttműködnek az (EU) 2016/679 rendelet szerinti felügyeleti hatóságokkal a személyes adatok megsértését eredményező események kezelése során, a felügyeleti hatóságok említett rendelet szerinti illetékességének és feladatainak sérelme nélkül.

(4) A nemzeti jogszabályi és intézményi keretek sérelme nélkül, a tagállamok biztosítják, hogy a közigazgatási szervek ezen irányelvnek való megfelelésének felügyelete és az ezen irányelv megsértésére tekintettel előírt végrehajtási intézkedések során az illetékes hatóságok rendelkezzenek az ahhoz szükséges megfelelő hatáskörökkel, hogy a felügyelet hatálya alá vont közigazgatási szervekkel szemben működési szempontból függetlenül végezhessék el ezen feladataikat. A tagállamok a nemzeti jogszabályi és intézményi keretekkel összhangban határozhatnak megfelelő, arányos és hatékony felügyeleti és végrehajtási intézkedések előírásáról e szervezetekkel szemben.

▼B

32. cikk

Az alapvető szervezetekre vonatkozó felügyeleti és végrehajtási intézkedések

(1) A tagállamok biztosítják, hogy az alapvető szervezetekre az ezen irányelvben megállapított kötelezettségek tekintetében előírt felügyeleti vagy végrehajtási intézkedések hatékonyak, arányosak és visszatartó erejűek legyenek, figyelembe véve az egyes konkrét esetek körülményeit.

(2) A tagállamok biztosítják, hogy az illetékes hatóságok az alapvető szervezetekkel kapcsolatos felügyeleti feladataik ellátása során hatáskörrel rendelkezzenek arra, hogy ezeknél a szervezeteknél elvégezzék legalább az alábbiakat:

a) képzett szakemberek által végrehajtott helyszíni ellenőrzések és távoli felügyeleti intézkedések, ideértve a véletlenszerű ellenőrzéseket is;

b) egy független szerv vagy illetékes hatóság által végzett, rendszeres és célzott biztonsági ellenőrzések;

c) eseti ellenőrzések, többek között ha azt jelentős esemény vagy ezen irányelvnek az alapvető szervezet általi megsértése indokolja;

d) objektív, megkülönböztetéstől mentes, méltányos és átlátható kockázatértékelési kritériumokon alapuló biztonsági vizsgálatok, amennyiben szükséges, az érintett szervezet együttműködésével;

e) az érintett szervezet által elfogadott kiberbiztonsági kockázatkezelési intézkedések –többek között a dokumentált kiberbiztonsági szabályzatok – értékeléséhez, valamint az információk illetékes hatóságok részére való, a 27. cikk alapján történő bejelentésére vonatkozó kötelezettség betartásának értékeléséhez szükséges tájékoztatás kérése;

f) a felügyeleti feladataik ellátásához szükséges adatokhoz, dokumentumokhoz és információkhoz való hozzáférés iránti kérelmek;

g) a kiberbiztonsági szabályzatok végrehajtására vonatkozó bizonyítékok, például a minősített ellenőr által végzett biztonsági ellenőrzések eredményei és a vonatkozó mögöttes bizonyítékok iránti kérelmek.

Az első albekezdés b) pontjában említett célzott biztonsági ellenőrzéseknek az illetékes hatóság vagy az ellenőrzött szervezet által végzett kockázatértékeléseken vagy más rendelkezésre álló, kockázattal kapcsolatos információkon kell alapulniuk.

A célzott biztonsági ellenőrzések eredményeit az illetékes hatóság rendelkezésére kell bocsátani. A független szerv által végzett ilyen célzott biztonsági ellenőrzés költségeit az ellenőrzött szervezet fizeti, kivéve azokban a kellően indokolt esetekben, amikor az illetékes hatóság másként határoz.

(3) A (2) bekezdés e), f) vagy g) pontja szerinti hatásköreik gyakorlása során az illetékes hatóságok közlik a megkeresés célját és meghatározzák a kért információkat.

(4) A tagállamok biztosítják, hogy az illetékes hatóságaik az alapvető szervezetekkel kapcsolatos végrehajtási hatásköreik gyakorlása során hatáskörrel rendelkezzenek legalább az alábbiakra:

▼B

a) figyelmeztetés kiadása ezen irányelv érintett szervezetek általi megsértéséről;

b) kötelező erejű utasítások – többek között az események megelőzéséhez vagy orvoslásához szükséges intézkedésekre, azok végrehajtási határidejére és a végrehajtással kapcsolatos adatszolgáltatásra vonatkozóan – vagy végzés elfogadása, amely előírja az érintett szervezetek számára, hogy orvosolják a feltárt hiányosságokat vagy ezen irányelv megsértését;

c) az érintett szervezetek kötelezése arra, hogy szüntessék meg az ezen irányelvet sértő magatartást, és tartózkodjanak a magatartás ismételt elkövetésétől;

d) az érintett szervezetek kötelezése arra, hogy meghatározott módon és határidőn belül biztosítsák, hogy kiberbiztonsági kockázatkezelési intézkedéseik megfeleljenek a 21. cikknek, és meghatározott módon és határidőn belül eleget tegyenek a 23. cikkben megállapított jelentéstételi kötelezettségeiknek;

e) az érintett szervezetek kötelezése arra, hogy azon természetes vagy jogi személyeket, akik vagy amelyek tekintetében szolgáltatásokat nyújtanak vagy tevékenységeket végeznek, és akiket vagy amelyeket egy jelentős kiberfenyegetés potenciálisan érinthet, tájékoztassák a fenyegetés jellegéről, valamint minden lehetséges védelmi vagy helyreállítási intézkedésről, amelyet e természetes vagy jogi személyek megtehetnek a fenyegetés elhárítására;

f) az érintett szervezetek kötelezése arra, hogy észszerű határidőn belül hajtsák végre a biztonsági ellenőrzés eredményeként adott ajánlásokat;

g) egy jól meghatározott feladatokkal ellátott ellenőrző tisztviselő kinevezése egy meghatározott időtartamra az érintett szervezetek 21. és 23. cikkben előírt kötelezettségei teljesítésének felügyeletére;

h) az érintett szervezetek kötelezése arra, hogy ezen irányelv megsértésének szempontjait meghatározott módon hozzák nyilvánosságra;

i) a 34. cikk szerinti közigazgatási bírság kiszabása vagy annak kérése az illetékes szervektől vagy bíróságoktól a nemzeti joggal összhangban, az e bekezdés a)–h) pontjában említett intézkedések mellett.

(5) Ha a (4) bekezdés a)–d) és f) pontja alapján elfogadott végrehajtási intézkedések eredménytelenek, a tagállamok biztosítják, hogy az illetékes hatóságaik jogosultak legyenek határidőt tűzni, amelyen belül az alapvető szervezet köteles a hiányosságok orvoslásához vagy az említett hatóságok követelményeinek való megfeleléshez szükséges intézkedések meghozatalára. Ha a kért intézkedést a kitűzött határidőn belül nem hozzák meg, a tagállamok biztosítják, hogy az illetékes hatóságaik hatáskörrel rendelkezzenek a következőkre:

a) a tanúsítás vagy az engedély ideiglenes felfüggesztése az alapvető szervezet által nyújtott releváns szolgáltatások vagy tevékenységek egészére vagy egy részére vonatkozóan, vagy a nemzeti joggal összhangban egy tanúsító vagy engedélyező szervezet, illetve egy bíróság erre való felkérése;

b) az érintett szervek, bíróságok felkérése arra, hogy a nemzeti joggal összhangban ideiglenesen tiltsák meg az alapvető szervezet vezérigazgatói vagy jogi képviseleti szintű vezetői feladatainak ellátásáért felelős bármely természetes személy számára, hogy az adott szervezetben vezetői feladatokat lásson el.

▼B

Az e bekezdés szerint kiszabott ideiglenes felfüggesztéseket vagy tiltásokat csak addig kell alkalmazni, amíg az érintett szervezet megteszi a szükséges intézkedéseket a hiányosságok orvoslására, vagy eleget tesz az illetékes hatóság azon követelményeinek, amelyek tekintetében az említett végrehajtási intézkedéseket alkalmazták. Az ilyen ideiglenes felfüggesztések vagy tiltások kiszabására megfelelő eljárási biztosítékok vonatkoznak, az uniós jog általános elveivel és a Chartával összhangban, ideértve a hatékony jogorvoslathoz és a tisztességes eljáráshoz való jogot, az ártatlanság vélelmét és a védelemhez való jogot.

Az e bekezdésben előírt végrehajtási intézkedések nem alkalmazhatók az ezen irányelv hatálya alá tartozó közigazgatási szervekre.

(6) A tagállamok biztosítják, hogy az alapvető szervezetért felelős vagy annak jogi képviseletében – képviseleti joga, a nevében történő döntéshozatal vagy az irányítás gyakorlásának joga alapján – eljáró természetes személy hatáskörrel rendelkezzen az ezen irányelvnek való megfelelés biztosítására. A tagállamok biztosítják, hogy e természetes személyek felelősségre vonhatók az ezen irányelvnek való megfelelés biztosítását szolgáló kötelezettségeik megsértéséért.

A közigazgatási szervek tekintetében e bekezdés nem érinti azon nemzeti jogot, amely a köztisztviselők és a megválasztott vagy kinevezett tisztviselők jogi felelősségét szabályozza.

(7) A (4) vagy (5) bekezdésben említett végrehajtási intézkedések bármelyikének meghozatala esetén az illetékes hatóságoknak tiszteletben kell tartaniuk a védelemhez való jogot, és figyelembe kell venniük a konkrét eset körülményeit, és legalább kellően figyelembe kell venniük az alábbiakat:

a) a jogsértés súlya és a megsértett rendelkezések jelentősége, azzal hogy többek között a következők minden esetben súlyos jogsértésnek minősülnek:

   i. ismételt jogsértések;

   ii. jelentős események bejelentésének vagy orvoslásának elmaradása;

   iii. a hiányosságok orvoslásának elmaradása az illetékes hatóságok kötelező erejű utasításait követően;

   iv. a jogsértés megállapítását követően az illetékes hatóság által elrendelt ellenőrzések vagy ellenőrzési tevékenységek akadályozása;

   v. hamis vagy súlyosan pontatlan információk közlése a 21. és 23. cikkben megállapított kiberbiztonsági kockázatkezelési intézkedésekkel vagy jelentéstételi kötelezettségekkel kapcsolatban;

b) a jogsértés időtartama;

c) az érintett szervezet által korábban elkövetett releváns jogsértések;

d) az okozott bármely vagyoni vagy nem vagyoni kár, beleértve bármely pénzügyi vagy gazdasági veszteséget, az egyéb szolgáltatásokra gyakorolt hatásokat és az érintett felhasználók számát;

▼B

e) a jogsértés elkövetőjének bármely szándékossága vagy gondatlansága;

f) a szervezet által a vagyoni vagy nem vagyoni kár megelőzésére vagy mérséklésére tett bármely intézkedések;

g) a jóváhagyott magatartási kódexek vagy jóváhagyott tanúsítási mechanizmusok betartása;

h) a felelősnek tartott természetes vagy jogi személyek illetékes hatóságokkal való együttműködésének szintje.

(8) Az illetékes hatóságok részletesen indokolják végrehajtási intézkedéseiket. Az ilyen intézkedések elfogadása előtt az illetékes hatóságok értesítik az érintett szervezeteket előzetes megállapításaikról. Emellett észszerű időt kell biztosítaniuk az említett szervezetek számára észrevételeik benyújtására, kivéve azokat a kellően indokolt eseteket, amikor az események megelőzésére vagy az azokra való reagálásra irányuló azonnali intézkedések máskülönben akadályokba ütköznének.

(9) A tagállamok biztosítják, hogy az ezen irányelv szerinti illetékes hatóságaik tájékoztassák az (EU) 2022/2557 irányelv szerinti, ugyanazon tagállambeli érintett illetékes hatóságokat arról, amikor gyakorolják azon felügyeleti és végrehajtási hatásköreiket, amelyek célja az (EU) 2022/2557 irányelv szerint kritikus szervezetként azonosított szervezet által ezen irányelvnek való megfelelés biztosítása. Adott esetben az (EU) 2022/2557 irányelv szerinti illetékes hatóságok előírhatják az ezen irányelv szerinti illetékes hatóságok számára, hogy gyakorolják felügyeleti és végrehajtási hatásköreiket az ezen irányelv hatálya alá tartozó, az (EU) 2022/2557 irányelv értelmében kritikus szervezetként azonosított szervezet tekintetében.

(10) A tagállamok biztosítják, hogy az ezen irányelv szerinti illetékes hatóságaik együttműködjenek az érintett tagállamnak az (EU) 2022/2554 rendelet szerinti illetékes hatóságaival. A tagállamok biztosítják különösen, hogy az ezen irányelv szerinti illetékes hatóságaik tájékoztassák az (EU) 2022/2554 rendelet 32. cikkének (1) bekezdése szerint létrehozott felvigyázási fórumot arról, amikor gyakorolják azon felügyeleti és végrehajtási hatásköreiket, amelyek célja annak biztosítása, hogy az ezen irányelv hatálya alá tartozó, az (EU) 2022/2554 rendelet 31. cikke szerint kritikus harmadik fél IKT-szolgáltatónak kijelölt alapvető szervezetek megfeleljenek ezen irányelvnek.

33. cikk

A fontos szervezetekre vonatkozó felügyeleti és végrehajtási intézkedések

(1) Ha bizonyítékokat, jelzést vagy információt kapnak arról, hogy egy fontos szervezet vélhetően nem felel meg ezen irányelvnek és különösen a 21. és 23. cikkének, a tagállamok biztosítják, hogy az illetékes hatóságok szükség esetén utólagos felügyeleti intézkedések révén intézkedjenek. A tagállamok biztosítják, hogy ezek az intézkedések hatékonyak, arányosak és visszatartó erejűek legyenek, figyelembe véve az egyes konkrét esetek körülményeit.

(2) A tagállamok biztosítják, hogy az illetékes hatóságok a fontos szervezetekkel kapcsolatos felügyeleti feladataik ellátása során hatáskörrel rendelkezzenek arra, hogy ezeknél a szervezeteknél elvégezzék legalább az alábbiakat:

▼B

a) képzett szakemberek által végrehajtott helyszíni ellenőrzések és távoli, utólagos felügyeleti intézkedések;

b) egy független szerv vagy illetékes hatóság által végzett célzott biztonsági ellenőrzések;

c) objektív, megkülönböztetéstől mentes, méltányos és átlátható kockázatértékelési kritériumokon alapuló biztonsági vizsgálatok, amennyiben szükséges, az érintett szervezet együttműködésével;

d) az érintett szervezet által elfogadott kiberbiztonsági kockázatkezelési intézkedések –többek között a dokumentált kiberbiztonsági szabályzatok – értékeléséhez, valamint az információk illetékes hatóságok részére való, a 27. cikk alapján történő bejelentésére vonatkozó kötelezettség betartásának értékeléséhez szükséges tájékoztatás kérése;

e) a felügyeleti feladataik ellátásához szükséges adatokhoz, dokumentumokhoz és információkhoz való hozzáférés iránti kérelmek;

f) a kiberbiztonsági szabályzatok végrehajtására vonatkozó bizonyítékok, például a minősített ellenőr által végzett biztonsági ellenőrzések eredményei és a vonatkozó mögöttes bizonyítékok iránti kérelmek.

Az első albekezdés b) pontjában említett célzott biztonsági ellenőrzéseknek az illetékes hatóság vagy az ellenőrzött szervezet által végzett kockázatértékeléseken vagy más rendelkezésre álló, kockázattal kapcsolatos információkon kell alapulniuk.

A célzott biztonsági ellenőrzések eredményeit az illetékes hatóság rendelkezésére kell bocsátani. A független szerv által végzett ilyen célzott biztonsági ellenőrzés költségeit az ellenőrzött szervezet fizeti, kivéve azokban a kellően indokolt esetekben, amikor az illetékes hatóság másként határoz.

(3) Hatásköreik (2) bekezdés d), e) vagy f) pontja szerinti gyakorlása során az illetékes hatóságok közlik a megkeresés célját és meghatározzák a kért tájékoztatást.

(4) A tagállamok biztosítják, hogy az illetékes hatóságok a fontos szervezetekkel kapcsolatos végrehajtási hatásköreik gyakorlása során hatáskörrel rendelkezzenek legalább az alábbiakra:

a) figyelmeztetés kiadása ezen irányelv érintett szervezetek általi megsértéséről;

b) kötelező erejű utasítások vagy végzés elfogadása, amelyek előírják az érintett szervezetek számára, hogy orvosolják a feltárt hiányosságokat vagy ezen irányelv megsértését;

c) az érintett szervezetek kötelezése arra, hogy szüntessék meg az ezen irányelvet sértő magatartást, és tartózkodjanak a magatartás ismételt elkövetésétől;

d) az érintett szervezetek kötelezése arra, hogy meghatározott módon és határidőn belül biztosítsák, hogy kiberbiztonsági kockázatkezelési intézkedéseik megfeleljenek a 21. cikknek, és meghatározott módon és határidőn belül eleget tegyenek a 23. cikkben megállapított jelentéstételi kötelezettségeiknek;

▼B

e) az érintett szervezetek kötelezése arra, hogy azon természetes vagy jogi személyeket, akik vagy amelyek tekintetében szolgáltatásokat nyújtanak vagy tevékenységeket végeznek, és akiket vagy amelyeket egy jelentős kiberfenyegetés potenciálisan érinthet, tájékoztassák a fenyegetés jellegéről, valamint minden lehetséges védelmi vagy helyreállítási intézkedésről, amelyet e természetes vagy jogi személyek megtehetnek a fenyegetés elhárítására;

f) az érintett szervezetek kötelezése arra, hogy észszerű határidőn belül hajtsák végre a biztonsági ellenőrzés eredményeként adott ajánlásokat;

g) az érintett szervezetek kötelezése arra, hogy ezen irányelv megsértésének szempontjait meghatározott módon hozzák nyilvánosságra;

h) a 34. cikk szerinti közigazgatási bírság kiszabása vagy annak kérése az illetékes szervektől vagy bíróságoktól a nemzeti joggal összhangban, az e bekezdés a)–g) pontjában említett intézkedések mellett.

(5) A 32. cikk (6), (7) és (8) bekezdését értelemszerűen alkalmazni kell az e cikkben a fontos szervezetekre vonatkozóan előírt felügyeleti és végrehajtási intézkedésekre is.

(6) A tagállamok biztosítják, hogy az ezen irányelv szerinti illetékes hatóságaik együttműködjenek az érintett tagállamnak az (EU) 2022/2554 rendelet szerinti illetékes hatóságaival. A tagállamok biztosítják különösen, hogy az ezen irányelv szerinti illetékes hatóságaik tájékoztassák az (EU) 2022/2554 rendelet 32. cikkének (1) bekezdése szerint létrehozott felvigyázási fórumot arról, amikor gyakorolják azon felügyeleti és végrehajtási hatásköreiket, amelyek célja annak biztosítása, hogy az ezen irányelv hatálya alá tartozó, az (EU) 2022/2554 rendelet 31. cikke szerint kritikus harmadik fél IKT-szolgáltatónak kijelölt fontos szervezetek megfeleljenek ezen irányelvnek.

34. cikk

Közigazgatási bírság alapvető és fontos szervezetekre történő kiszabásának általános feltételei

(1) A tagállamok biztosítják, hogy az ezen irányelv megsértésére tekintettel az alapvető és fontos szervezetekre e cikk szerint kiszabott közigazgatási bírságok hatékonyak, arányosak és visszatartó erejűek legyenek, figyelembe véve az egyes konkrét esetek körülményeit.

(2) A közigazgatási bírságot a 32. cikk (4) bekezdésének a)–h) pontjában, a 32. cikk (5) bekezdésében és a 33. cikk (4) bekezdésének a)–g) pontjában említett intézkedések mellett kell kiszabni.

(3) Az egyes esetekben a közigazgatási bírság kiszabásának és annak összegének eldöntésekor kellő figyelmet kell fordítani legalább a 32. cikk (7) bekezdésében előírt elemekre.

(4) A tagállamok biztosítják, hogy az alapvető szervezeteket – amennyiben megsértik a 21. vagy a 23. cikket – e cikk (2) és (3) bekezdésével összhangban legalább 10 000 000 EUR vagy, ha ez magasabb, legalább azon vállalkozás előző pénzügyi évi globális éves forgalma teljes összege 2%-ának megfelelő maximális összegű közigazgatási bírsággal sújtsák, amelyhez az alapvető szervezet tartozik.

▼B

(5) A tagállamok biztosítják, hogy a fontos szervezeteket – amennyiben megsértik a 21. vagy a 23. cikket – e cikk (2) és (3) bekezdésével összhangban legalább 7 000 000 EUR vagy, ha ez magasabb, legalább azon vállalkozás előző pénzügyi évi globális éves forgalma teljes összege 1,4%-ának megfelelő maximális összegű közigazgatási bírsággal sújtsák, amelyhez a fontos szervezet tartozik.

(6) A tagállamok rendelkezhetnek időszakos kényszerítő bírság kiszabásának hatásköréről annak érdekében, hogy egy alapvető vagy fontos szervezetet az illetékes hatóság korábbi határozatával összhangban ezen irányelv megsértésének megszüntetésére kényszerítsenek.

(7) Az illetékes hatóságok 32. és 33. cikk szerinti hatáskörének sérelme nélkül minden tagállam meghatározhat arra vonatkozó szabályokat, hogy közigazgatási bírság kiszabható-e és milyen mértékben a közigazgatási szervekre.

(8) Ha a tagállam jogrendszere nem rendelkezik közigazgatási bírságokról, az adott tagállam biztosítja, hogy e cikket oly módon alkalmazzák, hogy a bírságot az illetékes hatóság kezdeményezésére az illetékes nemzeti bíróság rója ki, ugyanakkor biztosítva e jogorvoslatok hatékonyságát és az illetékes hatóságok által kiszabott közigazgatási bírságokéval egyenértékű hatását. A kiszabott bírságoknak minden esetben hatékonynak, arányosnak és visszatartó erejűnek kell lenniük. A tagállamok 2024. október 17-ig értesítik a Bizottságot az e bekezdés alapján elfogadott jogszabályokról, valamint haladéktalanul értesítik a Bizottságot az ezeket érintő későbbi módosító jogszabályokról vagy módosításokról.

35. cikk

A személyes adatok megsértésével járó jogsértések

(1) Ha az illetékes hatóságoknak a felügyelet vagy a végrehajtás során a tudomásukra jut, hogy az ezen irányelv 21. és 23. cikkében megállapított kötelezettségeknek egy alapvető vagy fontos szervezet általi megsértése személyes adatok megsértésével járhat az (EU) 2016/679 rendelet 4. cikkének (12) bekezdésében meghatározottak szerint, amelyet az említett rendelet 33. cikke alapján be kell jelenteni, indokolatlan késedelem nélkül tájékoztatniuk kell az említett rendelet 55. vagy 56. cikkében említett felügyeleti hatóságokat.

(2) Amennyiben az (EU) 2016/679 rendelet 55. vagy 56. cikkében említett felügyeleti hatóságok az említett rendelet 58. cikke (2) bekezdésének i) pontja alapján közigazgatási bírságot szabnak ki, az illetékes hatóságok nem szabhatnak ki ezen irányelv 34. cikke szerinti közigazgatási bírságot az e cikk (1) bekezdésében említett olyan jogsértésért, amely ugyanazon magatartásból ered, mint amely az (EU) 2016/679 rendelet 58. cikke (2) bekezdésének i) pontja szerinti közigazgatási bírság tárgyát képezte. Az illetékes hatóságok azonban előírhatják az ezen irányelv 32. cikke (4) bekezdésének a)–h) pontjában, 32. cikkének (5) bekezdésében és 33. cikke (4) bekezdésének a)–g) pontjában előírt végrehajtási intézkedéseket.

(3) Ha az (EU) 2016/679 rendelet alapján illetékes felügyeleti hatóság az illetékes hatóság tagállamától eltérő tagállamban található, az illetékes hatóság tájékoztatja a saját tagállamában található felügyeleti hatóságot a személyes adatok (1) bekezdésben említett potenciális megsértéséről.

▼B

36. cikk

Szankciók

A tagállamok megállapítják az ezen irányelv alapján elfogadott nemzeti rendelkezések megsértése esetén alkalmazandó szankciókra vonatkozó szabályokat, és meghoznak minden szükséges intézkedést ezek végrehajtására. Az előírt szankcióknak hatékonyaknak, arányosaknak és visszatartó erejűeknek kell lenniük. A tagállamok e szabályokról és intézkedésekről 2025. január 17-ig értesítik a Bizottságot, és haladéktalanul tájékoztatják a Bizottságot az e szabályokat és intézkedéseket érintő minden későbbi módosításról.

37. cikk

Kölcsönös segítségnyújtás

(1) Ha egy szervezet egynél több tagállamban nyújt szolgáltatásokat, vagy egy vagy több tagállamban nyújt szolgáltatásokat, és hálózati és információs rendszerei egy vagy több másik tagállamban találhatók, az érintett tagállamok illetékes hatóságai szükség szerint együttműködnek és segítik egymást. Ez az együttműködés magában foglalja legalább a következőket:

a) az egyik tagállamban felügyeleti vagy végrehajtási intézkedéseket alkalmazó illetékes hatóságok az egyedüli kapcsolattartó ponton keresztül tájékoztatják a többi érintett tagállam illetékes hatóságait és konzultálnak velük a megtett felügyeleti és végrehajtási intézkedésekről;

b) az illetékes hatóság felkérhet egy másik illetékes hatóságot felügyeleti vagy végrehajtási intézkedések megtételére;

c) az illetékes hatóság egy másik illetékes hatóságtól származó indokolt kérelem kézhezvétele után – a saját erőforrásaihoz mérten arányos módon – kölcsönös segítséget nyújt a másik illetékes hatóság számára annak érdekében, hogy a felügyeleti vagy végrehajtási intézkedéseket hatékonyan, eredményesen és következetesen lehessen végrehajtani.

Az első albekezdés c) pontjában említett kölcsönös segítségnyújtás kiterjedhet az információkérésekre és a felügyeleti intézkedésekre, beleértve a helyszíni ellenőrzések, a távoli felügyelet vagy a célzott biztonsági ellenőrzések elvégzésére irányuló megkereséseket is. Az az illetékes hatóság, amelyhez segítségnyújtás iránti megkeresést intéztek, nem utasíthatja el a megkeresést, kivéve, ha megállapítást nyer, hogy nem rendelkezik hatáskörrel a kért segítség nyújtására, a kért segítség nem arányos az illetékes hatóság felügyeleti feladataival, vagy a megkeresés olyan információra vonatkozik, vagy olyan tevékenységeket foglal magában, amelyek közlése vagy végrehajtása ellentétes lenne az adott tagállam nemzetbiztonságának, közbiztonságának vagy védelmének alapvető érdekeivel. A megkeresés elutasítása előtt az illetékes hatóság konzultál a többi érintett illetékes hatósággal, valamint az érintett tagállamok egyikének kérésére a Bizottsággal és az ENISA-val.

▼B

(2) Adott esetben és közös megegyezéssel különböző tagállamok illetékes hatóságai közös felügyeleti intézkedéseket végezhetnek.

VIII. FEJEZET

FELHATALMAZASON ALAPULO ES VEGREHAJTASI JOGI AKTUSOK

38. cikk

A felhatalmazás gyakorlása

(1) A felhatalmazáson alapuló jogi aktusok elfogadására vonatkozóan a Bizottság részére adott felhatalmazás feltételeit ez a cikk határozza meg.

(2) A Bizottságnak a 24. cikk (2) bekezdésében említett, felhatalmazáson alapuló jogi aktus elfogadására vonatkozó felhatalmazása ötéves időtartamra szól, 2023. január 16-tól kezdődő hatállyal.

(3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja a 24. cikk (2) bekezdésében említett felhatalmazást. A visszavonásról szóló határozat megszünteti az abban meghatározott felhatalmazást. Ez a határozat az *Európai Unió Hivatalos Lapjában* való közzétételét követő napon vagy a határozatban meghatározott későbbi időpontban lép hatályba. A határozat nem érinti a már hatályban lévő, felhatalmazáson alapuló jogi aktusok érvényességét.

(4) A felhatalmazáson alapuló jogi aktus elfogadása előtt a Bizottság a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásban megállapított elvekkel összhangban konzultál az egyes tagállamok által kijelölt szakértőkkel.

(5) A Bizottság a felhatalmazáson alapuló jogi aktus elfogadását követően haladéktalanul és egyidejűleg értesíti arról az Európai Parlamentet és a Tanácsot.

(6) A 24. cikk (2) bekezdése értelmében elfogadott, felhatalmazáson alapuló jogi aktus csak akkor lép hatályba, ha az Európai Parlamentnek és a Tanácsnak a jogi aktusról való értesítését követő két hónapon belül sem az Európai Parlament, sem a Tanács nem emelt ellene kifogást, illetve ha az említett időtartam lejártát megelőzően mind az Európai Parlament, mind a Tanács arról tájékoztatta a Bizottságot, hogy nem fog kifogást emelni. Az Európai Parlament vagy a Tanács kezdeményezésére ez az időtartam két hónappal meghosszabbodik.

39. cikk

A bizottsági eljárás

(1) A Bizottságot egy bizottság segíti. Ez a bizottság a 182/2011/EU rendelet értelmében vett bizottságnak minősül.

▼B

(2) Az e bekezdésre történő hivatkozáskor a 182/2011/EU rendelet 5. cikkét kell alkalmazni.

(3) Ha a bizottság véleményét írásbeli eljárás útján kell beszerezni, ezt az eljárást eredmény hiányában meg kell szüntetni, ha a vélemény benyújtására előírt határidőn belül a bizottság elnöke így dönt, vagy a bizottság egyik tagja kéri.

IX. FEJEZET

ZARO RENDELKEZESEK

40. cikk

Felülvizsgálat

A Bizottság 2027. október 17-ig, majd azt követően 36 havonta felülvizsgálja ezen irányelv működését, és jelentést nyújt be az Európai Parlamentnek és a Tanácsnak. A jelentés különösen azt értékeli, hogy az érintett szervezetek mérete, és az I. és II. mellékletben említett ágazatok, alágazatok, valamint szervezettípusok mennyire relevánsak a gazdaság és a társadalom működése szempontjából a kiberbiztonság tekintetében. Ennek érdekében a stratégiai és operatív együttműködés további előmozdítása céljából a Bizottság figyelembe veszi az együttműködési csoport és a CSIRT-hálózat stratégiai és operatív szinten szerzett tapasztalatokról szóló jelentéseit. A jelentéshez szükség esetén jogalkotási javaslatot kell mellékelni.

41. cikk

Átültetés

(1) A tagállamok 2024. október 17-ig elfogadják és kihirdetik azokat a rendelkezéseket, amelyek szükségesek ahhoz, hogy ennek az irányelvnek megfeleljenek. Erről haladéktalanul tájékoztatják a Bizottságot.

Ezeket a rendelkezésket 2024. október 18-tól alkalmazzák.

(2) Amikor a tagállamok elfogadják az (1) bekezdésben említett rendelkezéseket, azokban hivatkozni kell erre az irányelvre, vagy azokhoz hivatalos kihirdetésük alkalmával ilyen hivatkozást kell fűzni. A hivatkozás módját a tagállamok határozzák meg.

42. cikk

A 910/2014/EU rendelet módosításai

A 910/2014/EU rendelet 19. cikkét 2024. október 18-i hatállyal el kell hagyni.

43.cikk

Az (EU) 2018/1972 irányelv módosítása

Az (EU) 2018/1972 irányelv 40. és 41. cikkét 2024. október 18-i hatállyal el kell hagyni.

▼B

44. cikk

Hatályon kívül helyezés

Az (EU) 2016/1148 irányelv 2024. október 18-i hatállyal hatályát veszti.

A hatályon kívül helyezett irányelvre történő hivatkozásokat ezen irányelvre való hivatkozásnak kell tekinteni és a III. mellékletben szereplő megfelelési táblázattal összhangban kell értelmezni.

45. cikk

Hatálybalépés

Ez az irányelv az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

46. cikk

Címzettek

Ennek az irányelvnek a tagállamok a címzettjei.

▼B

I. MELLÉKLET

A KIEMELTEN KRITIKUS ÁGAZATOK

Ágazat	Alágazat	Szervezet típusa
1. Energia	a) Villamos energia	— Az (EU) 2019/944 európai parlamenti és tanácsi irányelv [1] 2. cikkének 57. pontjában meghatározott villamosenergia-ipari vállalkozások, amelyek az említett irányelv 2. cikkének 12. pontjában meghatározott „ellátás” funkciót végzik
		— Az (EU) 2019/944 irányelv 2. cikkének 29. pontjában meghatározott elosztórendszer-üzemeltetők
		— Az (EU) 2019/944 irányelv 2. cikkének 35. pontjában meghatározott átvitelirendszer-üzemeltetők
		— Az (EU) 2019/944 irányelv 2. cikkének 38. pontjában meghatározott termelők
		— Az (EU) 2019/943 európai parlamenti és tanácsi rendelet [2] 2. cikkének 8. pontjában meghatározott kijelölt villamosenergiapiac-üzemeltetők — Az (EU) 2019/943 rendelet 2. cikkének 25. pontjában meghatározott, az (EU) 2019/944 irányelv 2. cikkének 18., 20. és 59. pontjában említett aggregálást, keresletoldali választ vagy energiatárolási szolgáltatást nyújtó piaci szereplők — Az elektromos töltőpont kezeléséért és üzemeltetéséért felelős jogalanyok, akik – többek között egy mobilitási szolgáltató nevében és megbízásából – elektromos töltési szolgáltatást nyújtanak végfelhasználók számára
	b) Távfűtés és -hűtés	— Az (EU) 2018/2001 európai parlamenti és tanácsi irányelv [3] 2. cikkének 19. pontjában meghatározott távfűtés vagy távhűtés üzemeltetői
	c) Olaj	— Az olajszállító csővezetékek üzemeltetői
		— Olajtermelő, finomító és kezelő létesítmények, tárolók üzemeltetői és szállításirendszer-üzemeltetők
		— A 2009/119/EK tanácsi irányelv [4] 2. cikkének f) pontjában meghatározott központi készletezőszervek
	d) Gáz	— A 2009/73/EK európai parlamenti és tanácsi irányelv [5] 2. cikkének 8. pontjában meghatározott ellátó vállalkozások
		— A 2009/73/EK irányelv 2. cikkének 6. pontjában meghatározott elosztórendszer-üzemeltetők
		— A 2009/73/EK irányelv 2. cikkének 4. pontjában meghatározott szállításirendszer-üzemeltetők
		— A 2009/73/EK irányelv 2. cikkének 10. pontjában meghatározott tárolásirendszer-üzemeltetők

▼B

Ágazat	Alágazat	Szervezet típusa
		— A 2009/73/EK irányelv 2. cikkének 12. pontjában meghatározott LNG-létesítmény rendszerüzemeltetők
		— A 2009/73/EK irányelv 2. cikkének 1. pontjában meghatározott földgázipari vállalkozások
		— A földgázfinomító és -kezelő létesítmények üzemeltetői
	e) Hidrogén	— A hidrogéntermelés, -tárolás és -szállítás üzemeltetői
2. Szállítás	a) Légi	— A 300/2008/EK rendelet 3. cikkének 4. pontjában említett – üzleti célra igénybe vett – légi fuvarozók
		— A 2009/12/EK európai parlamenti és tanácsi irányelv (6) 2. cikkének 2. pontjában meghatározott repülőtér-irányító szervezetek, az említett irányelv 2. cikkének 1. pontjában meghatározott repülőterek, a törzshálózathoz tartozó, az 1315/2013/EU európai parlamenti és tanácsi rendelet (7) II. mellékletének 2. szakaszában felsorolt repülőtereket is beleértve, valamint a repülőtereken található kapcsolódó létesítményeket üzemeltető szervezetek
		— Az 549/2004/EK európai parlamenti és tanácsi rendelet (8) 2. cikkének 1. pontjában meghatározott légiforgalmi irányító (ATC) szolgálatot ellátó forgalomirányítási üzemeltetők
	b) Vasúti	— A 2012/34/EU európai parlamenti és tanácsi irányelv (9) 3. cikkének 2. pontjában meghatározott pályahálózat-működtetők
		— A 2012/34/EU irányelv 3. cikkének 1. pontjában meghatározott vállalkozó vasúttársaságok, a kiszolgáló létesítményeknek az említett irányelv 3. cikkének 12. pontjában meghatározott üzemeltetőit is beleértve
	c) Vízi	— A 725/2004/EK európai parlamenti és tanácsi rendelet (10) I. mellékletében foglalt tengeri szállítás tekintetében meghatározott azon vállalkozások, amelyek belvízi, tengeri és part menti vízi személyszállítással, illetve vízi árufuvarozással foglalkoznak, ide nem értve azonban az e vállalkozások által üzemeltetett egyes hajókat

▼B

Ágazat	Alágazat	Szervezet típusa
		— A 2005/65/EK európai parlamenti és tanácsi irányelv ([11]) 3. cikkének 1. pontjában meghatározott kikötőket irányító szervezetek, a 725/2004/EK rendelet 2. cikkének 11. pontjában meghatározott kikötőlétesítményeiket is beleértve, valamint a kikötőkben található létesítményeket és berendezéseket üzemeltető szervezetek
		— A 2002/59/EK európai parlamenti és tanácsi irányelv ([12]) 3. cikkének o) pontjában meghatározott hajóforgalmi szolgálatok (VTS) üzemeltetői
	d) Közúti	— Az (EU) 2015/962 felhatalmazáson alapuló bizottsági rendelet ([13]) 2. cikkének 12. pontjában meghatározott, a forgalomirányításért felelős közúti hatóságok, azon közigazgatási szervek kivételével, amelyek általános tevékenységének nem alapvető része a forgalomszervezés vagy az intelligens közlekedési rendszerek üzemeltetése
		— A 2010/40/EU európai parlamenti és tanácsi irányelv ([14]) 4. cikkének 1. pontjában meghatározott intelligens közlekedési rendszerek üzemeltetői
3. Banki szolgáltatások		Az 575/2013/EU európai parlamenti és tanácsi rendelet ([15]) 4. cikkének 1. pontjában meghatározott hitelintézetek
4. Pénzügyi piaci infrastruktúrák		— A 2014/65/EU európai parlamenti és tanácsi irányelv ([16]) 4. cikkének 24. pontjában meghatározott kereskedési helyszínek működtetői
		— A 648/2012/EU európai parlamenti és tanácsi rendelet ([17]) 2. cikkének 1. pontjában meghatározott központi szerződő felek
5. Egészségügy		— A 2011/24/EU európai parlamenti és tanácsi irányelv ([18]) 3. cikkének g) pontjában meghatározott egészségügyi szolgáltatók
		— Az (EU) 2022/2371 európai parlamenti és tanácsi rendelet ([19]) 15. cikkében említett uniós referencialaboratóriumok
		— A 2001/83/EK európai parlamenti és tanácsi irányelv ([20]) 1. cikkének 2. pontjában említett gyógyszerek kutatásával és fejlesztésével foglalkozó szervezetek — A NACE Rev. 2. C nemzetgazdasági ágának 21. ágazatában említett gyógyszeralapanyagokat és gyógyszerkészítményeket gyártó szervezetek — Az (EU) 2022/123 európai parlamenti és tanácsi rendelet ([21]) 22. cikkének értelmében vett népegészségügyi szükséghelyzetben kritikus fontosságú orvostechnikai eszközöket (a népegészségügyi szükséghelyzet kritikus fontosságú eszközeinek jegyzéke) gyártó szervezetek

▼B

Ágazat	Alágazat	Szervezet típusa
6. Ivóvíz		Az (EU) 2020/2184 európai parlamenti és tanácsi irányelv ([22]) 2. cikke 1. pontjának a) alpontjában meghatározott, emberi fogyasztásra szánt víz szolgáltatói és elosztói, azokat az elosztókat kivéve, akik számára az emberi fogyasztásra szánt víz elosztása más áruk és termékek forgalmazásából álló általános tevékenységüknek nem alapvető része
7. Szennyvíz		A 91/271/EGK tanácsi irányelv ([23]) 2. cikkének 1, 2. és 3. pontjában meghatározott települési szennyvíz, háztartási szennyvíz, vagy ipari szennyvíz összegyűjtését, ártalmatlanítását vagy kezelését végző vállalkozások, azokat a vállalkozásokat kivéve, amelyek általános tevékenységének nem alapvető része a települési szennyvíz, háztartási szennyvíz vagy ipari szennyvíz összegyűjtése, ártalmatlanítása és kezelése
8. Digitális infrastruktúra		— Internetes exchange pont szolgáltatók
		— DNS-szolgáltatók, a gyökérnév-szerverek üzemeltetőit kivéve
		— Legfelső szintű doménnév-nyilvántartók
		— Felhőszolgáltatók
		— Adatközpont-szolgáltatók
		— Tartalomszolgáltató hálózati szolgáltatók
		— Bizalmi szolgáltatók
		— Nyilvános elektronikus hírközlési hálózatok szolgáltatói
		— Nyilvánosan elérhető elektronikus hírközlési szolgáltatásokat nyújtó szolgáltatók
9. IKT-szolgáltatások irányítása (vállalkozások között)		— Irányított szolgáltatók — Irányított biztonsági szolgáltatók
10. Közigazgatás		— A tagállam által a nemzeti joggal összhangban meghatározott, a központi kormányzathoz tartozó közigazgatási szervek
		— A tagállam által a nemzeti joggal összhangban meghatározott regionális szintű közigazgatási szervek

▼B

Ágazat	Alágazat	Szervezet típusa
11. Világűr		A tagállamok vagy magánfelek tulajdonában, kezelésében és üzemeltetésében lévő azon földi infrastruktúra üzemeltetői, amelyek támogatják az űralapú szolgáltatások nyújtását, kivéve a nyilvános elektronikus hírközlő hálózatok szolgáltatóit

(1) Az Európai Parlament és a Tanács (EU) 2019/944 irányelve (2019. június 5.) a villamos energia belső piacára vonatkozó közös szabályokról és a 2012/27/EU irányelv módosításáról (HL L 158., 2019.6.14., 125. o.).
(2) Az Európai Parlament és a Tanács (EU) 2019/943 rendelete (2019. június 5.) a villamos energia belső piacáról (HL L 158., 2019.6.14., 54. o.).
(3) Az Európai Parlament és a Tanács (EU) 2018/2001 irányelve (2018. december 11.) a megújuló energiaforrásokból előállított energia használatának előmozdításáról (HL L 328., 2018.12.21., 82. o.).
(4) A Tanács 2009/119/EK irányelve (2009. szeptember 14.) a tagállamok minimális kőolaj- és/vagy kőolajtermék-készletezési kötelezettségéről (HL L 265., 2009.10.9., 9. o.).
(5) Az Európai Parlament és a Tanács 2009/73/EK irányelve (2009. július 13.) a földgáz belső piacára vonatkozó közös szabályokról és a 2003/55/EK irányelv hatályon kívül helyezéséről (HL L 211., 2009.8.14., 94. o.).
(6) Az Európai Parlament és a Tanács 2009/12/EK irányelve (2009. március 11.) a repülőtéri díjakról (HL L 70., 2009.3.14., 11. o.).
(7) Az Európai Parlament és a Tanács 1315/2013/EU rendelete (2013. december 11.) a transzeurópai közlekedési hálózat fejlesztésére vonatkozó uniós iránymutatásokról és a 661/2010/EU határozat hatályon kívül helyezéséről (HL L 348., 2013.12.20., 1. o.).
(8) Az Európai Parlament és a Tanács 549/2004/EK rendelete (2004. március 10.) az egységes európai égbolt létrehozására vonatkozó keret megállapításáról (keretrendelet) (HL L 96., 2004.3.31., 1. o.; magyar nyelvű különkiadás, 7. fejezet, 8. kötet, 23. o.).
(9) Az Európai Parlament és a Tanács 2012/34/EU irányelve (2012. november 21.) az egységes európai vasúti térség létrehozásáról (HL L 343., 2012.12.14., 32. o.).
(10) Az Európai Parlament és a Tanács 725/2004/EK rendelete (2004. március 31.) a hajók és kikötői létesítmények biztonságának fokozásáról (HL L 129., 2004.4.29., 6. o.).
(11) Az Európai Parlament és a Tanács 2005/65/EK irányelve (2005. október 26.) a kikötővédelem fokozásáról (HL L 310., 2005.11.25., 28. o.).
(12) Az Európai Parlament és a Tanács 2002/59/EK irányelve (2002. június 27.) a közösségi hajóforgalomra vonatkozó megfigyelő és információs rendszer létrehozásáról és a 93/75/EGK irányelv hatályon kívül helyezéséről (HL L 208., 2002.8.5., 10. o.).
(13) A Bizottság (EU) 2015/962 felhatalmazáson alapuló rendelete (2014. december 18.) a 2010/40/EU európai parlamenti és tanácsi irányelvnek az EU egészére kiterjedő valós idejű forgalmi információs szolgáltatások nyújtása tekintetében történő kiegészítéséről (HL L 157., 2015.6.23., 21. o.).
(14) Az Európai Parlament és a Tanács 2010/40/EU irányelve (2010. július 7.) az intelligens közlekedési rendszereknek a közúti közlekedés területén történő kiépítésére, valamint a más közlekedési módokhoz való kapcsolódására vonatkozó keretről (HL L 207., 2010.8.6., 1. o.).
(15) Az Európai Parlament és a Tanács 575/2013/EU rendelete (2013. június 26.) a hitelintézetekre vonatkozó prudenciális követelményekről és a 648/2012/EU rendelet módosításáról (HL L 176., 2013.6.27., 1. o.).
(16) Az Európai Parlament és a Tanács 2014/65/EU irányelve (2014. május 15.) a pénzügyi eszközök piacairól, valamint a 2002/92/EK irányelv és a 2011/61/EU irányelv módosításáról (HL L 173., 2014.6.12., 349. o.).
(17) Az Európai Parlament és a Tanács 648/2012/EU rendelete (2012. július 4.) a tőzsdén kívüli származtatott ügyletekről, a központi szerződő felekről és a kereskedési adattárakról (HL L 201., 2012.7.27., 1. o.).
(18) Az Európai Parlament és a Tanács 2011/24/EU irányelve (2011. március 9.) a határon átnyúló egészségügyi ellátásra vonatkozó betegjogok érvényesítéséről (HL L 88., 2011.4.4., 45. o.).
(19) Az Európai Parlament és a Tanács (EU) 2022/2371 rendelete (2022. november 23.) a határokon át terjedő súlyos egészségügyi veszélyekről és az 1082/2013/EU határozat hatályon kívül helyezéséről (HL L 314., 2022.12.6., 26. o.).
(20) Az Európai Parlament és a Tanács 2001/83/EK irányelve (2001. november 6.) az emberi felhasználásra szánt gyógyszerek közösségi kódexéről (HL L 311., 2001.11.28., 67. o.).
(21) Az Európai Parlament és a Tanács (EU) 2022/123 rendelete (2022. január 25.) az Európai Gyógyszerügynökség által a gyógyszerek és orvostechnikai eszközök tekintetében a válsághelyzetekre való felkészültség és a válságkezelés terén betöltött szerep megerősítéséről (HL L 20., 2022.1.31., 1. o.).
(22) Az Európai Parlament és a Tanács (EU) 2020/2184 irányelve (2020. december 16.) az emberi fogyasztásra szánt víz minőségéről (HL L 435., 2020.12.23., 1. o.).
(23) A Tanács 91/271/EGK irányelve (1991. május 21.) a települési szennyvíz kezeléséről (HL L 135., 1991.5.30., 40. o.).

▼B

II. MELLÉKLET

EGYÉB KRITIKUS ÁGAZATOK

Ágazat	Alágazat	Szervezet típusa
1. Postai és futárszolgáltatások		A 97/67/EK irányelv 2. cikkének 1a. pontjában meghatározott postai szolgáltatók, beleértve a futárszolgáltatókat
2. Hulladékgazdálkodás		A 2008/98/EK európai parlamenti és tanácsi irányelv (1) 3. cikkének 9. pontjában meghatározott hulladékgazdálkodással foglalkozó vállalkozások, kivéve azokat a vállalkozásokat, amelyeknek nem a hulladékgazdálkodás a fő gazdasági tevékenységük
3. Vegyszerek gyártása, előállítása és forgalmazása		Az 1907/2006/EK európai parlamenti és tanácsi rendelet (2) 3. cikkének 9. és 14. pontjában említettek szerint anyagok gyártását, illetve anyagok vagy keverékek forgalmazását végző vállalkozások, továbbá az említett rendelet 3. cikkének 3. pontjában meghatározott árucikkeket ilyen anyagokból vagy keverékekből előállító vállalkozások
4. Élelmiszer-termelés, -feldolgozás és -forgalmazás		A 178/2002/EK európai parlamenti és tanácsi rendelet (3) 3. cikkének 2. pontjában meghatározott élelmiszer-vállalkozások, amelyek nagykereskedelemmel, ipari termeléssel és feldolgozással foglalkoznak
5. Gyártás	a) Orvostechnikai eszközök és in vitro diagnosztikai orvostechnikai eszközök gyártása	Az (EU) 2017/745 európai parlamenti és tanácsi rendelet (4) 2. cikkének 1. pontjában meghatározott orvostechnikai eszközöket, valamint az (EU) 2017/746 európai parlamenti és tanácsi rendelet (5) 2. cikkének 2. pontjában meghatározott in vitro diagnosztikai orvostechnikai eszközöket gyártó szervezetek, kivéve az e rendelet 1. melléklete 5. pontjának ötödik franciabekezdésében említett orvostechnikai eszközöket gyártó szervezeteket
	b) Számítógépek, elektronikai és optikai termékek gyártása	A NACE Rev. 2. C nemzetgazdasági ágának 26. ágazatában említett bármely gazdasági tevékenységet folytató vállalkozások
	c) Villamos berendezések gyártása	A NACE Rev. 2. C nemzetgazdasági ágának 27. ágazatában említett bármely gazdasági tevékenységet folytató vállalkozások

▼B

Ágazat	Alágazat	Szervezet típusa
	d) Máshova nem sorolt gépek és gépi berendezések gyártása	A NACE Rev. 2. C nemzetgazdasági ágának 28. ágazatában említett bármely gazdasági tevékenységet folytató vállalkozások
	e) Gépjárművek, pótkocsik és félpótkocsik gyártása	A NACE Rev. 2. C nemzetgazdasági ágának 29. ágazatában említett bármely gazdasági tevékenységet folytató vállalkozások
	f) Egyéb szállítóeszközök gyártása	A NACE Rev. 2. C nemzetgazdasági ágának 30. ágazatában említett bármely gazdasági tevékenységet folytató vállalkozások
6. Digitális szolgáltatók		— Online piacterek szolgáltatói
		— Online keresőmotorok szolgáltatói
		— A közösségimédia-szolgáltatási platform szolgáltatói
7. Kutatás		Kutatóhelyek

(1) Az Európai Parlament és a Tanács 2008/98/EK irányelve (2008. november 19.) a hulladékokról és egyes irányelvek hatályon kívül helyezéséről (HL L 312., 2008.11.22., 3. o.).
(2) Az Európai Parlament és a Tanács 1907/2006/EK rendelete (2006. december 18.) a vegyi anyagok regisztrálásáról, értékeléséről, engedélyezéséről és korlátozásáról (REACH), az Európai Vegyianyag-ügynökség létrehozásáról, az 1999/45/EK irányelv módosításáról, valamint a 793/93/EGK tanácsi rendelet, az 1488/94/EK bizottsági rendelet, a 76/769/EGK tanácsi irányelv, a 91/155/EGK, a 93/67/EGK, a 93/105/EK és a 2000/21/EK bizottsági irányelv hatályon kívül helyezéséről (HL L 396., 2006.12.30., 1. o.).
(3) Az Európai Parlament és a Tanács 178/2002/EK rendelete (2002. január 28.) az élelmiszerjog általános elveiről és követelményeiről, az Európai Élelmiszerbiztonsági Hatóság létrehozásáról és az élelmiszerbiztonságra vonatkozó eljárások megállapításáról (HL L 31., 2002.2.1., 1. o.).
(4) Az Európai Parlament és a Tanács (EU) 2017/745 rendelete (2017. április 5.) az orvostechnikai eszközökről, a 2001/83/EK irányelv, a 178/2002/EK rendelet és az 1223/2009/EK rendelet módosításáról, valamint a 90/385/EGK és a 93/42/EGK tanácsi irányelv hatályon kívül helyezéséről (HL L 117., 2017.5.5., 1. o.).
(5) Az Európai Parlament és a Tanács (EU) 2017/746 rendelete (2017. április 5.) az in vitro diagnosztikai orvostechnikai eszközökről, valamint a 98/79/EK irányelv és a 2010/227/EU bizottsági határozat hatályon kívül helyezéséről (HL L 117., 2017.5.5., 176. o.).

▼B

III. MELLÉKLET

MEGFELELÉSI TÁBLÁZAT

Az (EU) 2016/1148 irányelv	Ez az irányelv
1. cikk, (1) bekezdés	1. cikk, (1) bekezdés
1. cikk, (2) bekezdés	1. cikk, (2) bekezdés
1. cikk, (3) bekezdés	–
1. cikk, (4) bekezdés	2. cikk, (12) bekezdés
1. cikk, (5) bekezdés	2. cikk, (13) bekezdés
1. cikk, (6) bekezdés	2. cikk, (6) és (11) bekezdés
1. cikk, (7) bekezdés	4. cikk
2. cikk	2. cikk, (14) bekezdés
3. cikk	5. cikk
4. cikk	6. cikk
5. cikk	–
6. cikk	–
7. cikk, (1) bekezdés	7. cikk, (1) és (2) bekezdés
7. cikk, (2) bekezdés	7. cikk, (4) bekezdés
7. cikk, (3) bekezdés	7. cikk, (3) bekezdés
8. cikk, (1)–(5) bekezdés	8. cikk, (1)–(5) bekezdés
8. cikk, (6) bekezdés	13. cikk, (4) bekezdés
8. cikk, (7) bekezdés	8. cikk, (6) bekezdés
9. cikk, (1), (2) és (3) bekezdés	10. cikk, (1), (2) és (3) bekezdés
9. cikk, (4) bekezdés	10. cikk, (9) bekezdés
9. cikk, (5) bekezdés	10. cikk, (10) bekezdés
10. cikk, (1), (2) és (3) bekezdés, első albekezdés	13. cikk, (1), (2) és (3) bekezdés
10. cikk (3) bekezdés, második albekezdés	23. cikk (9) bekezdés
11. cikk, (1) bekezdés	14. cikk, (1) és (2) bekezdés
11. cikk, (2) bekezdés	14. cikk, (3) bekezdés
11. cikk, (3) bekezdés	14. cikk, (4) bekezdés, első albekezdés, a)–q) pont és s) pont és (7) bekezdés

▼B

Az (EU) 2016/1148 irányelv	Ez az irányelv
11. cikk, (4) bekezdés	14. cikk, (4) bekezdés, első albekezdés, r) pont és második albekezdés
11. cikk, (5) bekezdés	14. cikk, (8) bekezdés
12. cikk, (1)–(5) bekezdés	15. cikk, (1)–(5) bekezdés
13. cikk	17. cikk
14. cikk, (1) és (2) bekezdés	21. cikk, (1)–(4) bekezdés
14. cikk, (3) bekezdés	23. cikk, (1) bekezdés
14. cikk, (4) bekezdés	23. cikk, (3) bekezdés
14. cikk, (5) bekezdés	23. cikk, (5), (6) és (8) bekezdés
14. cikk, (6) bekezdés	23. cikk, (7) bekezdés
14. cikk, (7) bekezdés	23. cikk, (11) bekezdés
15. cikk, (1) bekezdés	31. cikk, (1) bekezdés
15. cikk, (2) bekezdés, első albekezdés, a) pont	32. cikk, (2) bekezdés, e) pont
15. cikk, (2) bekezdés, első albekezdés, b) pont	32. cikk, (2) bekezdés, g) pont
15. cikk, (2) bekezdés, második albekezdés	32. cikk, (3) bekezdés
15. cikk, (3) bekezdés	32. cikk, (4) bekezdés, b) pont
15. cikk, (4) bekezdés	31. cikk, (3) bekezdés
16. cikk, (1) és (2) bekezdés	21. cikk, (1)–(4) bekezdés
16. cikk, (3) bekezdés	23. cikk, (1) bekezdés
16. cikk, (4) bekezdés	23. cikk, (3) bekezdés
16. cikk, (5) bekezdés	–
16. cikk, (6) bekezdés	23. cikk, (6) bekezdés
16. cikk, (7) bekezdés	23. cikk, (7) bekezdés
16. cikk, (8) és (9) bekezdés	21. cikk, (5) bekezdés és 23. cikk (11) bekezdés
16. cikk, (10) bekezdés	–
16. cikk, (11) bekezdés	2. cikk, (1), (2) és (3) bekezdés
17. cikk, (1) bekezdés	33. cikk, (1) bekezdés
17. cikk, (2) bekezdés, a) pont	32. cikk, (2) bekezdés, e) pont
17. cikk, (2) bekezdés, b) pont	32. cikk, (4) bekezdés, b) pont

▼B

Az (EU) 2016/1148 irányelv	Ez az irányelv
17. cikk, (3) bekezdés	37. cikk, (1) bekezdés, a) és b) pont
18. cikk, (1) bekezdés	26. cikk, (1) bekezdés, b) pont és (2) bekezdés
18. cikk, (2) bekezdés	26. cikk, (3) bekezdés
18. cikk, (3) bekezdés	26. cikk, (4) bekezdés
19. cikk	25. cikk
20. cikk	30. cikk
21. cikk	36. cikk
22. cikk	39. cikk
23. cikk	40. cikk
24. cikk	–
25. cikk	41. cikk
26. cikk	45. cikk
27. cikk	46. cikk
I. melléklet, 1. pont	11. cikk, (1) bekezdés
I. melléklet, 2. pont, a) pont, i–iv. alpont	11. cikk, (2) bekezdés, a–d) pont
I. melléklet, 2. pont, a) pont, v. alpont	11. cikk, (2) bekezdés, f) pont
I. melléklet, 2. pont, b) pont	11. cikk, (4) bekezdés
I. melléklet, 2. pont, c) pont, i. és ii. alpont	11. cikk, (5) bekezdés, a) pont
II. melléklet	I. melléklet
III. melléklet, 1. és 2. pont	II. melléklet, 6. pont
III. melléklet, 3. pont	I. melléklet, 8. pont