EURÓPAI
BIZOTTSÁG

Brüsszel, 2023.9.13.
C(2023) 6068 final

A BIZOTTSÁG KÖZLEMÉNYE

A Bizottság iránymutatása az (EU) 2022/2555 irányelv (NIS 2 irányelv) 4. cikke (1) és (2) bekezdésének alkalmazásáról

I. Bevezetés

1. Az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről szóló, 2022. december 14-i (EU) 2022/2555 európai parlamenti és tanácsi irányelv (NIS 2 irányelv)[1] 4. cikkének (3) bekezdése értelmében a Bizottság 2023. július 17-ig iránymutatásokat ad ki, amelyekben pontosítja az irányelv 4. cikke (1) és (2) bekezdésének alkalmazását.

2. Ez az iránymutatás pontosítja az említett rendelkezések alkalmazását, amelyek az (EU) 2022/2555 irányelv, valamint a kiberbiztonsági kockázatkezelési intézkedésekkel vagy a biztonsági események jelentésére vonatkozó követelményekkel foglalkozó jelenlegi és jövőbeli ágazatspecifikus uniós jogi aktusok közötti kapcsolatra vonatkoznak. Az iránymutatás függeléke felsorolja azokat az ágazatspecifikus uniós jogi aktusokat, amelyek a Bizottság megítélése szerint az (EU) 2022/2555 irányelv 4. cikkének hatálya alá tartoznak. Az a tény, hogy valamely jogi aktus nem szerepel az említett függelékben, nem feltétlenül jelenti azt, hogy nem tartozik az említett rendelkezés hatálya alá.

3. Az (EU) 2022/2555 irányelv 4. cikke (3) bekezdésének harmadik mondata alkalmazásában a Bizottság ezen iránymutatás elfogadása előtt figyelembe vette az együttműködési csoport és az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) észrevételeit.

4. Ez az iránymutatás nem érinti az uniós jognak az Európai Unió Bírósága általi értelmezését.

II. Az ágazatspecifikus uniós jogi aktusok kiberbiztonsági követelményeinek egyenértékűsége

5. Az (EU) 2022/2555 irányelv 4. cikkének (1) bekezdése úgy rendelkezik, hogy 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 említett irányelvben meghatározott kötelezettségekkel, akkor az (EU) 2022/2555 irányelv vonatkozó rendelkezései – beleértve az említett irányelv VII. fejezetében meghatározott, a felügyeletre és a végrehajtásra vonatkozó rendelkezéseket – nem alkalmazandók az említett szervezetekre. Az említett rendelkezés előírja továbbá, hogy amennyiben az ágazatspecifikus uniós jogi aktusok hatálya nem terjed ki az (EU) 2022/2555 irányelv hatálya alá tartozó, adott ágazatban működő valamennyi szervezetre, az említett irányelv vonatkozó rendelkezései továbbra is alkalmazandók azokra a szervezetekre, amelyek nem tartoznak az említett ágazatspecifikus uniós jogi aktusok hatálya alá.

II.1. Kiberbiztonsági kockázatkezelési követelmények

[1] HL L 333., 2022.12.27., 80. o.

6. Az (EU) 2022/2555 irányelv 4. cikke (2) bekezdésének a) pontja úgy rendelkezik, hogy az alapvető vagy fontos szervezetek által az ágazatspecifikus uniós jogi aktusok értelmében elfogadandó kiberbiztonsági kockázatkezelési intézkedéseket hatásukban egyenértékűnek kell tekinteni az (EU) 2022/2555 irányelvben meghatározott kötelezettségekkel, amennyiben ezek az intézkedések hatásukban legalább egyenértékűek az említett irányelv 21. cikkének (1) és (2) bekezdésében megállapítottakkal. Annak értékelésekor, hogy a kiberbiztonsági kockázatkezelési intézkedésekről szóló ágazatspecifikus uniós jogi aktusban foglalt követelmények hatásukban legalább egyenértékűek-e az (EU) 2022/2555 irányelv 21. cikkének (1) és (2) bekezdésében megállapítottakkal, az adott ágazatspecifikus uniós jogi aktusban foglalt követelményeknek meg kell felelniük legalább az említett rendelkezések követelményeinek, vagy túl kell mutatniuk rajtuk, ami annyit jelent, hogy az ágazatspecifikus rendelkezések tartalmilag részletesebbek lehetnek az (EU) 2022/2555 irányelv megfelelő rendelkezéseihez képest.

7. Az (EU) 2022/2555 irányelv 21. cikke (1) bekezdésének első albekezdése értelmében a tagállamoknak biztosítaniuk kell, 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. Ezeknek az intézkedéseknek kockázatalapúnak kell lenniük, és képesnek kell lenniük arra, hogy megelőzzék vagy minimalizálják a biztonsági események hatását. Az (EU) 2022/2555 irányelv 21. cikke (1) bekezdésének második albekezdése meghatározza, hogyan kell értékelni az ilyen intézkedések arányosságát[2]. Az (EU) 2022/2555 irányelv 21. cikkének (1) bekezdésében meghatározott kötelezettség, amely előírja az alapvető és fontos szervezetek számára, hogy megfelelő és arányos kiberbiztonsági kockázatkezelési intézkedéseket hozzanak, az érintett szervezet valamennyi műveletére és szolgáltatására vonatkozik, nem csak a szervezet által nyújtott konkrét információtechnológiai (IT) eszközökre vagy kritikus szolgáltatásokra.

8. Annak értékelésekor, hogy egy ágazatspecifikus uniós jogi aktus egyenértékű-e az (EU) 2022/2555 irányelv vonatkozó kiberkockázat-kezelési rendelkezéseivel, az értékelés során különös jelentőséget kell tulajdonítani annak a kérdésnek, hogy az adott jogi aktusban szereplő biztonsági kötelezettségek tartalmaznak-e a hálózati és információs rendszerek biztonságának biztosítására szolgáló intézkedéseket. Az (EU) 2022/2555 irányelv 6. cikke 2. pontjában szereplő fogalommeghatározás szerint a 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. A „rendelkezésre állás”, „hitelesség”, „sértetlenség” és „bizalmasság” kifejezés e fogalommeghatározásban

[2] Lásd még az (EU) 2022/2555 irányelv (78), (81) és (82) preambulumbekezdését.

való használata mind a négy, a hálózati és információs rendszerek biztonságával kapcsolatos védelmi célra vonatkozik. Az (EU) 2022/2555 irányelv 6. cikkének 1. pontjában meghatározott „hálózati és információs rendszerek” kifejezés magában foglalja az elektronikus hírközlő hálózatokat [3] ; minden olyan eszközt vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportját, amelyek közül egy vagy több valamely program alapján digitális adatok automatikus kezelését végzi; és az ilyen elektronikus hírközlő hálózatok által a működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatokat. Következésképpen az ágazatspecifikus uniós jogi aktus által előírt biztonsági intézkedéseknek ki kell terjedniük a szervezet tevékenységei során használt hardverre, belső vezérlőprogramra és szoftverre is.

9. Egy ágazatspecifikus uniós jogi aktusnak az (EU) 2022/2555 irányelv 21. cikkének (1) és (2) bekezdésében foglalt követelményekkel való egyenértékűségének értékelésekor további fontos szempont, hogy az említett jogi aktusban előírt kiberbiztonsági kockázatkezelési intézkedéseknek az „összes veszélyre kiterjedő megközelítésen” kell alapulniuk. Mivel a hálózati és információs rendszerek biztonságát fenyegető veszélyek különböző eredetűek lehetnek, bármilyen típusú esemény negatív hatással lehet a szervezet hálózati és információs rendszereire, és potenciálisan biztonsági eseményhez vezethet. Ezért a szervezet által hozott kiberbiztonsági kockázatkezelési intézkedéseknek nemcsak a szervezet hálózati és információs rendszereit, hanem e rendszerek fizikai környezetét is védeniük kell minden olyan eseménytől, például szabotázstól, lopástól, tűztől, árvíztől, telekommunikációs hibától vagy feszültség-kimaradástól, vagy jogosulatlan fizikai hozzáféréstől, amely veszélyeztetheti a hálózati és információs rendszerek által tárolt, továbbított vagy feldolgozott adatok, illetve az általuk kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét vagy bizalmasságát. Következésképpen az ágazatspecifikus uniós jogi aktusban előírt kiberbiztonsági kockázatkezelési intézkedéseknek kifejezetten foglalkozniuk kell a hálózati és információs rendszerek fizikai és környezeti biztonságával a rendszerhibák, emberi hibák, rosszindulatú cselekmények vagy természeti jelenségek tekintetében[4].

10. Az (EU) 2022/2555 irányelv 21. cikkének (2) bekezdése előírja továbbá, hogy a kiberbiztonsági kockázatkezelési intézkedéseknek magukban kell foglalniuk az említett rendelkezés (2) bekezdésének a)–j) pontjában felsorolt egyedi biztonsági követelményeket. Ezek a követelmények olyan intézkedésekre terjednek ki, mint a kockázatelemzési és az informatikai rendszerek biztonságára vonatkozó szabályzatok, a biztonsági események kezelése, az üzletmenet-folytonosság, a válságkezelés, az ellátási lánc biztonsága, valamint a kriptográfia és adott esetben a titkosítás használatára vonatkozó szabályzatok és eljárások. Az (EU) 2022/2555 irányelv 21. cikke (5) bekezdésének második albekezdése értelmében a Bizottság felhatalmazást kap arra, hogy

[3] Az Európai Elektronikus Hírközlési Kódex létrehozásáról szóló, 2018. december 11-i (EU) 2018/1972 európai parlamenti és tanácsi irányelv (HL L 321., 2018.12.17., 36. o.) 2. cikkének (1) bekezdése.

[4] Lásd az (EU) 2022/2555 irányelv (79) preambulumbekezdését.

végrehajtási jogi aktusokat fogadjon el, amelyekben meghatározza az említett irányelv 21. cikkének (2) bekezdésében említett biztonsági intézkedések technikai és módszertani követelményeit, valamint szükség esetén ágazati 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 2024. október 17-ig végrehajtási jogi aktusokat fogad el az (EU) 2022/2555 irányelv 21. cikkének (2) bekezdésében említett biztonsági intézkedések technikai és módszertani követelményeiről. A végrehajtási jogi aktusok részletesebben meghatározzák az alap-jogiaktusban meghatározott fő végrehajtási feltételeket és kritériumokat, anélkül, hogy érintenék e jogi aktus lényegét[5].

II.2. Jelentéstételi követelmények

11. Az (EU) 2022/2555 irányelv 4. cikke (2) bekezdésének b) pontja úgy rendelkezik, hogy a jelentős biztonsági események bejelentésére vonatkozó jelentéstételi követelményeket hatásukban egyenértékűnek kell tekinteni az említett irányelvben foglalt kötelezettségekkel, amennyiben egy ágazatspecifikus uniós jogi aktus előírja a biztonsági eseményekre vonatkozó bejelentésekhez való azonnali – adott esetben automatikus és közvetlen – hozzáférést a számítógép-biztonsági eseményekre reagáló csoportok (a továbbiakban: CSIRT-ek), az illetékes hatóságok vagy az egyedüli kapcsolattartó pontok számára, és ha a jelentős biztonsági események bejelentésére vonatkozó követelmények hatásukban legalább egyenértékűek az (EU) 2022/2555 irányelv 23. cikkének (1)–(6) bekezdésében megállapítottakkal.

12. Mivel egy ágazatspecifikus uniós jogi aktus jelentős biztonsági események bejelentésére vonatkozó követelményeinek hatásukban legalább egyenértékűeknek kell lenniük az (EU) 2022/2555 irányelv 23. cikkének (1)–(6) bekezdésében meghatározott követelményekkel ahhoz, hogy az adott jogi aktus az említett irányelvben foglalt jelentéstételi kötelezettségek helyett alkalmazandó legyen, az irányelv 23. cikkének (1)–(6) bekezdésében meghatározott követelmények különösen fontosak az egyenértékűség értékelése szempontjából. Az (EU) 2022/2555 irányelv 23. cikkének (1)–(6) bekezdése részletesebben meghatározza, hogy kinek, milyen határidőn belül, és milyen információtartalommal kell bejelenteni a biztonsági eseményeket. Ezeket az alábbi alszakaszok ismertetik részletesebben:

II.2.1. A jelentős biztonsági események jelentése a CSIRT-eknek, az illetékes hatóságoknak és a szolgáltatások igénybe vevőinek

13. Az (EU) 2022/2555 irányelv 23. cikke (1) bekezdése első albekezdésének első mondata előírja az alapvető és fontos szervezetek számára, hogy indokolatlan késedelem nélkül értesítsék a CSIRT-jüket vagy adott esetben az illetékes hatóságukat minden jelentős

[5] Lásd az alábbi dokumentumot: Nem kötelező erejű kritériumok az Európai Unió működéséről szóló szerződés 290. és 291. cikkének alkalmazásához – 2019. június 18., D fejezet (Az alap-jogiaktust végrehajtó további szabályok) (2019/C 223/01), C 223/1, 2019.7.3.

biztonsági eseményről. Az (EU) 2022/2555 irányelv 23. cikke (1) bekezdése első albekezdésének második mondata előírja az alapvető és fontos szervezetek számára, hogy adott esetben indokolatlan késedelem nélkül értesítsék a szolgáltatásaikat igénybe vevőket azokról a jelentős biztonsági eseményekről, amelyek valószínűleg hátrányosan érintik az említett szolgáltatások nyújtását.

14. Míg az (EU) 2022/2555 irányelv 6. cikkének 6. pontja nagyon tágan határozza meg a biztonsági esemény fogalmát – 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 –, az említett irányelv 23. cikkének (1) bekezdése csak a jelentős biztonsági események esetében ír elő jelentési kötelezettséget. Egy biztonsági esemény akkor jelentős, ha súlyos működési zavart okozott vagy képes okozni a szolgáltatásokban, vagy pénzügyi veszteséget okozott vagy képes okozni az érintett szervezetnek (23. cikk (3) bekezdés a) pont), vagy a biztonsági esemény jelentős vagyoni vagy nem vagyoni kár okozásával más természetes vagy jogi személyeket érintett vagy képes érinteni (23. cikk (3) bekezdés b) pont).

15. Az (EU) 2022/2555 irányelv (101) preambulumbekezdése egyértelművé teszi, hogy a biztonsági események jelentésének az érintett szervezet által elvégzett első értékelésen kell alapulnia. Ennek az első értékelésnek figyelembe kell vennie többek között az érintett hálózati és információs rendszereket és különösen fontosságukat a szervezet szolgáltatásainak nyújtásában, a kiberfenyegetés súlyosságát és műszaki jellemzőit, minden kihasznált mögöttes sérülékenységet, valamint a szervezet hasonló biztonsági eseményekkel kapcsolatos tapasztalatait. Annak meghatározásában, hogy a szolgáltatás működési zavara súlyos-e, fontos szerepet játszhatnak olyan mutatók, mint a szolgáltatás működésére gyakorolt hatás mértéke, a biztonsági esemény időtartama vagy a szolgáltatások érintett igénybe vevőinek száma.

16. Az (EU) 2022/2555 irányelv 23. cikke (11) bekezdésének második albekezdése értelmében a Bizottság felhatalmazást kap arra, hogy végrehajtási jogi aktusokat fogadjon el, amelyekben részletesebben meghatározza azokat az eseteket, amikor egy biztonsági esemény jelentősnek tekintendő. 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 ilyen végrehajtási jogi aktusokat fogad el. A végrehajtási jogi aktusok részletesebben meghatározzák az alap-jogiaktusban meghatározott fő végrehajtási feltételeket és kritériumokat, anélkül, hogy érintenék e jogi aktus lényegét[6].

[6] Lásd az alábbi dokumentumot: Nem kötelező erejű kritériumok az Európai Unió működéséről szóló szerződés 290. és 291. cikkének alkalmazásához – 2019. június 18., D fejezet (Az alap-jogiaktust végrehajtó további szabályok) (2019/C 223/01), C 223/1, 2019.7.3.

II.2.2. A jelentős biztonsági események jelentésének többlépcsős megközelítése és időkerete

17. Az (EU) 2022/2555 irányelv többlépcsős megközelítést határoz meg a jelentős biztonsági események jelentésére vonatkozóan, amely magában foglalja a korai előrejelzést, a biztonsági események bejelentését és a zárójelentést. Ez a három elem adott esetben kiegészíthető időközi jelentésekkel és az elért eredményekről szóló jelentéssel.

18. A többlépcsős megközelítés célja, hogy biztosítsa a megfelelő egyensúlyt egyrészt a gyors bejelentések – amelyek segítenek enyhíteni a jelentős biztonsági események potenciális terjedését, és lehetővé teszik az alapvető és fontos szervezetek számára, hogy segítségnyújtást kérjenek –, másrészt pedig az olyan mélyreható jelentések között, amelyek értékes tanulságokat vonnak le az egyes biztonsági eseményekből, és idővel javítják az egyes szervezetek és teljes ágazatok kiberrezilienciáját[7].

19. A többlépcsős megközelítés szerint az alapvető és fontos szervezeteknek először indokolatlan késedelem nélkül, de legkésőbb a jelentős biztonsági eseményről való tudomásszerzéstől számított 24 órán belül korai előrejelzést kell benyújtaniuk az illetékes CSIRT-nek vagy hatóságnak. Ezt követően e szervezeteknek indokolatlan késedelem nélkül, de legkésőbb a jelentős biztonsági eseményről való tudomásszerzéstől számított 72 órán belül be kell nyújtaniuk a biztonsági esemény bejelentését. Ezt követően az illetékes CSIRT vagy hatóság időközi jelentést kérhet. Végezetül, legkésőbb a biztonsági esemény bejelentésétől számított egy hónapon belül zárójelentést kell benyújtani az illetékes CSIRT-nek vagy hatóságnak, kivéve, ha a biztonsági esemény akkor még folyamatban van, amely esetben az esemény kezelését követő egy hónapon belül eredményjelentést és zárójelentést kell benyújtani.

20. Az (EU) 2022/2555 irányelv 23. cikke (4) bekezdésének második albekezdésében meghatározott, a biztonsági eseményekre vonatkozó bejelentésre a bizalmi szolgáltatók tekintetében eltérő időkeret vonatkozik. Ezeknek a szolgáltatóknak indokolatlan késedelem nélkül, de minden esetben a jelentős biztonsági eseményről való tudomásszerzéstől számított 24 órán belül jelenteniük kell a bizalmi szolgáltatásaik nyújtásával kapcsolatos jelentős biztonsági eseményeket.

II.2.3. A jelentős biztonsági események CSIRT-eknek vagy illetékes hatóságoknak való bejelentésére vonatkozó kötelezettség tartalma

21. Általános szabályként az (EU) 2022/2555 irányelv 23. cikke (1) bekezdése első albekezdésének harmadik mondata értelmében minden tagállamnak biztosítania kell, hogy az alapvető és fontos szervezetek jelentsenek többek között minden olyan információt, amely lehetővé teszi az illetékes CSIRT vagy adott esetben az illetékes hatóság számára, hogy meghatározza a biztonsági esemény határokon átnyúló hatásait. Ezt a jelentéstételi kötelezettség tartalmára vonatkozó követelményt az (EU) 2022/2555

[7] Lásd az (EU) 2022/2555 irányelv (101) preambulumbekezdését.

irányelv 23. cikkének (4) bekezdése részletezi, amely meghatározza a többlépcsős megközelítést.

22. A 23. cikk (4) bekezdésének a) pontja értelmében a korai előrejelzésben adott esetben fel kell tüntetni, hogy a jelentős biztonsági eseményt vélhetően jogellenes vagy rosszindulatú cselekmény okozta-e, és hogy lehet-e (lehetséges-e) határokon átnyúló hatása. Az (EU) 2022/2555 irányelv (102) preambulumbekezdése szerint a korai előrejelzésnek csak azokat az információkat kell tartalmaznia, amelyek szükségesek ahhoz, hogy az illetékes CSIRT-ek vagy hatóságok értesüljenek a jelentős biztonsági eseményről, és lehetővé tegyék az érintett szervezet számára, hogy szükség esetén segítséget kérjen.

23. A biztonsági eseményre vonatkozó bejelentésnek adott esetben tartalmaznia kell a korai előrejelzés részeként benyújtott információk frissítését. Ezenkívül tartalmaznia kell a jelentős biztonsági esemény első értékelését, beleértve a biztonsági esemény súlyosságát és hatását, valamint – amennyiben rendelkezésre állnak – a fertőzöttségi mutatóit.

24. Amennyiben időközi jelentést kérnek, annak tartalmaznia kell a vonatkozó helyzetjelentést. A zárójelentésnek tartalmaznia kell a biztonsági esemény részletes leírását, beleértve annak súlyosságát és hatását, a biztonsági eseményt valószínűleg kiváltó fenyegetés vagy kiváltó ok típusát, az alkalmazott és folyamatban lévő mérséklési intézkedéseket, valamint adott esetben a biztonsági esemény határokon átnyúló hatását.

II.2.4. Azonnali hozzáférés a biztonsági eseményekre vonatkozó bejelentésekhez

25. Az (EU) 2022/2555 irányelv 4. cikke (2) bekezdésének b) pontja úgy rendelkezik, hogy az említett irányelv helyett a bejelentési követelmények tekintetében alkalmazandó ágazatspecifikus uniós jogi aktusnak azonnali hozzáférést kell biztosítania az (EU) 2022/2555 irányelv szerinti CSIRT-ek, illetékes hatóságok vagy egyedüli kapcsolattartó pontok számára az ágazatspecifikus uniós jogi aktussal összhangban benyújtott, a biztonsági eseményekre vonatkozó bejelentésekhez. Az (EU) 2022/2555 irányelv (24) preambulumbekezdésének megfelelően az ilyen azonnali hozzáférés különösen akkor biztosítható, ha indokolatlan késedelem nélkül továbbítják a biztonsági eseményekre vonatkozó bejelentéseket a CSIRT-nek, az illetékes hatóságnak vagy az egyedüli kapcsolattartó pontnak.

26. Azonnali hozzáférés automatikus és közvetlen eszközökkel biztosítható, amelyeket a tagállamoknak adott esetben be kell vezetniük. Az automatikus és közvetlen jelentéstételi mechanizmus biztosítja az információk szisztematikus és azonnali megosztását a CSIRT-ekkel, az illetékes hatóságokkal vagy az egyedüli kapcsolattartó pontokkal a biztonsági eseményekre vonatkozó bejelentések kezelésével kapcsolatban. A tagállamok egyedüli kapcsolattartó pontot is használhatnak, amelynek meg kell felelnie az ágazatspecifikus uniós jogi aktusnak, egyszerűsítenie kell a jelentéstételt, és végre kell hajtania az automatikus és közvetlen jelentéstételi mechanizmust.

27. Annak értékelésekor, hogy egy ágazatspecifikus uniós jogi aktusban a jelentős biztonsági események bejelentésére vonatkozóan meghatározott követelmények hatásukban legalább egyenértékűek-e az (EU) 2022/2555 irányelv 23. cikkének (1)–(6) bekezdésében megállapítottakkal, az adott ágazatspecifikus uniós jogi aktusban foglalt követelményeknek meg kell felelniük legalább a 23. cikk (1)–(6) bekezdésében foglalt követelményeknek, vagy az említett rendelkezéseknél részletesebbnek kell lenniük. A követelményeknek az (EU) 2022/2555 irányelvnek megfelelően bejelentendő biztonsági események típusára kell vonatkozniuk, figyelembe véve különösen a szolgáltatások igénybe vevőit, a tartalmat és az alkalmazandó időkereteket.

III. Az egyenértékűség következményei

III.1. Felügyelet és végrehajtás

28. Amennyiben az ágazatspecifikus uniós jogi aktusok hatásukban legalább egyenértékűek az (EU) 2022/2555 irányelvben meghatározott kötelezettségekkel, nemcsak az említett irányelvnek a kiberbiztonsági kockázatkezelési intézkedések elfogadására vagy a jelentős biztonsági események bejelentésére vonatkozó kötelezettségről szóló releváns rendelkezései nem alkalmazandók, hanem az (EU) 2022/2555 irányelv VII. fejezetében a felügyeletre és végrehajtásra vonatkozóan meghatározott rendelkezések sem.

29. Az (EU) 2022/2555 irányelv (25) preambulumbekezdése kifejti, hogy a hatásukban legalább egyenértékű ágazatspecifikus uniós jogi aktusok előírhatják, hogy az említett jogi aktusok szerinti illetékes hatóságok a kiberbiztonsági kockázatkezeléssel vagy bejelentési kötelezettségekkel kapcsolatos felügyeleti és végrehajtási hatásköreiket az (EU) 2022/2555 irányelv szerinti illetékes hatóságok támogatásával gyakorolják. Az érintett illetékes hatóságok e célból együttműködési megállapodásokat hozhatnak létre, beleértve a felügyeleti tevékenységek koordinálásával kapcsolatos eljárásokat, a nemzeti joggal összhangban végzett vizsgálatokra és helyszíni ellenőrzésekre vonatkozó eljárásokat, valamint a felügyelettel és a végrehajtással kapcsolatos releváns információk illetékes hatóságok közötti cseréjére szolgáló mechanizmusokat. A releváns információk cseréjére szolgáló ilyen mechanizmus magában foglalhatja az illetékes hatóságok által az (EU) 2022/2555 irányelv alapján kért kiberjellegű információkhoz való hozzáférést.

III.2. Nemzeti kiberbiztonsági stratégia

30. Az (EU) 2022/2555 irányelv 7. cikkének (1) bekezdése értelmében minden tagállamnak nemzeti kiberbiztonsági stratégiát kell elfogadnia. A nemzeti kiberbiztonsági stratégia valamely tagállam koherens kerete, amely meghatározza a kiberbiztonság területén követendő stratégiai célokat és prioritásokat és az e célkitűzések és prioritások megvalósításához szükséges irányítási intézkedéseket az adott tagállamban (lásd az (EU) 2022/2555 irányelv 6. cikkének (4) bekezdését). A kiberbiztonsági stratégiának tartalmaznia kell többek között az (EU) 2022/2555 irányelv I. és II. mellékletében meghatározott ágazatokra vonatkozó célokat és prioritásokat. A stratégiának emellett tartalmaznia kell az említett célok és prioritások elérésére szolgáló irányítási keretet,

beleértve az (EU) 2022/2555 irányelv 7. cikkének (2) bekezdésében említett szakpolitikákat.

31. Az (EU) 2022/2555 irányelv 7. cikke (1) bekezdésének c) pontja előírja továbbá, hogy a nemzeti kiberbiztonsági stratégiának tartalmaznia kell a releváns érdekelt felek szerepét és felelősségi körét nemzeti szinten tisztázó irányítási keretet, amely alapul szolgál az (EU) 2022/2555 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.

32. Ezért az (EU) 2022/2555 irányelv 7. cikke értelmében vett kiberbiztonsági stratégia elfogadására vonatkozó követelmény nem vonatkozik sem az említett irányelv 21. és 23. cikke alapján az alapvető és fontos szervezetek esetében előírt kiberbiztonsági követelményekre, sem a VII. fejezetben a felügyeletükre és végrehajtásukra vonatkozóan az irányelv 4. cikkének (1) és (2) bekezdésében előírtak szerint meghatározott rendelkezésekre. A 7. cikk vonatkozó rendelkezését továbbra is alkalmazni kell azon ágazatok, alágazatok és szervezettípusok tekintetében, amelyekre vonatkozóan léteznek az (EU) 2022/2555 irányelv 4. cikke értelmében vett ágazatspecifikus uniós jogi aktusok.

III.3. A CSIRT-ek kijelölése

33. Az (EU) 2022/2555 irányelv 10. cikke (1) bekezdésének megfelelően a tagállamoknak ki kell jelölniük vagy létre kell hozniuk egy vagy több CSIRT-et, amelyeknek ki kell terjedniük legalább az irányelv I. és II. mellékletben említett ágazatokra, alágazatokra és szervezettípusokra, így beleértve azokat az ágazatokat, alágazatokat és szervezettípusokat is, amelyekre vonatkozóan léteznek ágazatspecifikus uniós jogi aktusok. A CSIRT-ek általában az (EU) 2022/2555 irányelv 11. cikkének (3) bekezdésében meghatározott feladataikat is ellátják e tekintetben, kivéve, ha az ágazatspecifikus uniós jogi aktusok konkrét feladatokat határoznak meg.

III.4. Nemzeti kiberbiztonsági válságkezelési keretek és az EU-CyCLONe

34. Az (EU) 2022/2555 irányelv 9. cikkének (1) bekezdése értelmében a tagállamoknak ki kell jelölniük vagy létre kell hozniuk a nagyszabású kiberbiztonsági események és válságok kezeléséért felelős egy vagy több kiberbiztonsági válságkezelési hatóságot. Az említett irányelv 6. cikkének 7. pontja értelmében a nagyszabású kiberbiztonsági esemény olyan biztonsági esemény, amely olyan mértékű zavart okoz, amely meghaladja valamely tagállamnak az arra való reagálása képességét, vagy amely legalább két tagállamra jelentős hatást gyakorol. Az (EU) 2022/2555 irányelv 9. cikkének (4) bekezdése értelmében a tagállamoknak el kell fogadniuk egy, a nagyszabású kiberbiztonsági események és válságok elhárítására szolgáló nemzeti tervet is, amelyben meghatározzák a nagyszabású kiberbiztonsági események és válságok kezelésének célkitűzéseit és szabályait. Ennek a tervnek többek között meg kell határoznia a kiberválságok kezelésére szolgáló eljárásokat – beleértve azok integrálását az általános nemzeti válságkezelési keretbe és az információcserére szolgáló csatornákba –, valamint az érintett állami és

magán érdekelt felek, valamint az érintett infrastruktúra azonosítását. A kiberválságok kezelésére szolgáló ilyen eljárások, illetve az érintett állami és magán érdekelt felek, valamint az érintett infrastruktúra között ágazatspecifikus eljárások és érdekelt felek is szerepelhetnek.

35. Az (EU) 2022/2555 irányelv 16. cikke létrehozza az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatát (EU-CyCLONe) 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.

36. Mivel a kiberbiztonsági válságkezelési keretekről szóló 9. cikk és az EU-CyCLONe-ról szóló 16. cikk nem érinti az (EU) 2022/2555 irányelv 21. és 23. cikke alapján a szervezetek vonatkozásában előírt kiberbiztonsági követelményeket vagy a VII. fejezetben meghatározott, az említett irányelv 4. cikkének (1) és (2) bekezdésében előírt felügyeletet és végrehajtást, a 9. és 16. cikket teljes egészében alkalmazni kell az ágazatokra, annak ellenére, hogy vannak a 4. cikk értelmében vett ágazatspecifikus uniós jogi aktusok. Ennek eredményeként a tagállamoknak ki kell jelölniük vagy létre kell hozniuk az ágazatspecifikus uniós jogi aktusok hatálya alá tartozó ágazatokban előforduló nagyszabású kiberbiztonsági események és válságok kezeléséért felelős egy vagy több kiberbiztonsági válságkezelési hatóságot. Ezen túlmenően az ágazatspecifikus uniós jogi aktusok hatálya alá tartozó ágazatokat nem szabad figyelmen kívül hagyni a nagyszabású kiberbiztonsági események és válságok elhárítására szolgáló nemzeti terv elfogadásakor. Végezetül, az EU-CyCLONe-nak el kell látnia az (EU) 2022/2555 irányelv 16. cikkében foglalt feladatait azon ágazatok tekintetében, amelyekben a szervezetek ágazatspecifikus uniós jogi aktusok hatálya alá tartoznak.

III.5. A 3. cikk (3) és (4) bekezdése, a 20. cikk, valamint a 27. cikk (2) és (3) bekezdése alkalmazásának kizárása

37. Az (EU) 2022/2555 irányelv 3. cikkének (3) bekezdése értelmében a tagállamoknak össze kell állítaniuk az irányelv hatálya alá tartozó alapvető és fontos szervezetek, valamint doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek jegyzékét. A 27. cikk (2) bekezdése értelmében a tagállamok előírják az említett irányelv 27. cikkének (1) bekezdésében említett szervezetek számára, hogy bizonyos információkat nyújtsanak be az illetékes hatóságoknak. Mivel e rendelkezések célja az (EU) 2022/2555 irányelv hatálya alá tartozó szervezetek egyértelmű áttekintésének biztosítása az irányelv hatálya alá tartozó alapvető és fontos szervezetek felügyeletének támogatása érdekében, ebből következik, hogy ezek a rendelkezések nem alkalmazandók azokra a szervezetekre, amelyekre a kiberbiztonsági kockázatkezelési és jelentéstételi követelmények tekintetében valamely ágazatspecifikus uniós jogi aktus alkalmazandó. Ez nem zárja ki, hogy a tagállamok ezeket a szervezeteket felvegyék a jegyzékbe.

Az (EU) 2022/2555 irányelv 20. cikkének (1) bekezdése értelmében az alapvető és fontos szervezetek vezető testületeinek jóvá kell hagyniuk az e szervezetek által a 21. cikknek

való megfelelés érdekében tett kiberbiztonsági kockázatkezelési intézkedéseket, felügyelniük kell annak végrehajtását, és felelősségre vonhatók az említett cikk szervezetek általi megsértéséért. Az említett irányelv 20. cikkének (2) bekezdése értelmében 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. Mivel az (EU) 2022/2555 irányelv 20. cikkéből eredő kötelezettségek szervesen kapcsolódnak az említett irányelv 21. cikkében foglalt követelményekhez, a 20. cikk következésképpen nem alkalmazandó az említett irányelv 4. cikke értelmében vett, a kiberbiztonsági kockázatkezelési követelmények tekintetében alkalmazandó ágazatspecifikus uniós jogi aktusok esetében.

FÜGGELÉK: Ágazatspecifikus uniós jogi aktusok

Az (EU) 2022/2554 rendelet (a digitális működési rezilienciáról szóló jogszabály)[1]

1. Az (EU) 2022/2554 rendelet (a digitális működési rezilienciáról szóló rendelet, DORA-rendelet) 1. cikkének (2) bekezdése úgy rendelkezik, hogy az (EU) 2022/2555 irányelv és az azt átültető megfelelő nemzeti szabályok hatálya alá tartozó pénzügyi szervezetek tekintetében az (EU) 2022/2554 rendelet az (EU) 2022/2555 irányelv 4. cikkének alkalmazásában ágazatspecifikus uniós jogi aktusnak minősül. Ez az állítás tükröződik az (EU) 2022/2555 irányelv (28) preambulumbekezdésében, amely kimondja, hogy a DORA-rendeletet az (EU) 2022/2555 irányelv vonatkozásában a pénzügyi szervezetek tekintetében ágazatspecifikus uniós jogi aktusnak kell tekinteni. Következésképpen az (EU) 2022/2555 irányelvben előírt rendelkezések helyett az (EU) 2022/2554 rendeletnek az információs és kommunikációs technológiai (IKT) kockázatkezelésre (a 6. és azt követő cikkek), az IKT-vel kapcsolatos biztonsági események kezelésére és különösen a jelentős IKT-vonatkozású biztonsági események bejelentésére (a 17. és azt követő cikkek), valamint a digitális működési rezilienciára vonatkozó tesztekre (a 24. és azt követő cikkek), az információmegosztási megállapodásokra (25. cikk) és a harmadik féltől eredő IKT-kockázatokra (a 28. és azt követő cikkek) vonatkozó rendelkezéseit kell alkalmazni. A tagállamok ezért nem alkalmazhatják az (EU) 2022/2555 irányelv kiberbiztonsági kockázatkezelésre és jelentéstételi kötelezettségekre, valamint felügyeletre és végrehajtásra vonatkozó rendelkezéseit az (EU) 2022/2554 rendelet hatálya alá tartozó pénzügyi szervezetekre.

2. E tekintetben a pénzügyi szervezetek az (EU) 2022/2554 rendelet 2. cikke (1) bekezdésének a)–t) pontjában említett szervezeteknek minősülnek. A pénzügyi szervezetként az (EU) 2022/2554 rendelet hatálya alá, illetve alapvető vagy fontos szervezetként az (EU) 2022/2555 irányelv hatálya alá tartozó szervezettípusok közé tartoznak a hitelintézetek, a kereskedési helyszínek és a központi szerződő felek. Mivel fontos fenntartani az (EU) 2022/2555 irányelv szerinti szoros kapcsolatot és információcserét a pénzügyi ágazattal, az európai felügyeleti hatóságok és az (EU) 2022/2554 rendelet szerinti illetékes hatóságok kérhetik az együttműködési csoport tevékenységeiben való részvételt[2], az információcserét és az együttműködést az (EU) 2022/2555 irányelv szerinti egyedüli kapcsolattartó pontokkal, CSIRT-ekkel és illetékes hatóságokkal[3]. Az (EU) 2022/2554 rendelet szerint illetékes hatóságoknak továbbítaniuk kell az IKT-vel kapcsolatos jelentős biztonsági események és adott esetben a jelentős kiberfenyegetések részleteit az (EU) 2022/2555 irányelv szerinti CSIRT-eknek, illetékes hatóságoknak vagy egyedüli kapcsolattartó pontoknak is. Ez a biztonsági eseményekre vonatkozó bejelentésekhez való azonnali hozzáférés és azok közvetlenül vagy egy egyedüli kapcsolattartó pont révén történő továbbítása biztosításával érhető el. A CSIRT-

[1] Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról (HL L 333., 2022.12.27., 1. o.).

[2] Az (EU) 2022/2555 irányelv 14. cikkének (3) bekezdése és az (EU) 2022/2554 rendelet 47. cikkének (1) bekezdése.

[3] Lásd az (EU) 2022/2555 irányelv (28) preambulumbekezdését.

eknek képesnek kell lenniük arra, hogy tevékenységeik során lefedjék a pénzügyi ágazatot[4]. A tagállamoknak továbbra is bele kell foglalniuk a pénzügyi ágazatot a kiberbiztonsági stratégiáikba. A nemzeti kiberbiztonsági válságkezelési keretekre (az (EU) 2022/2555 irányelv 9. cikke) és az EU-CyCLONe-ra (az (EU) 2022/2555 irányelv 16. cikke) vonatkozó rendelkezéseket továbbra is alkalmazni kell az (EU) 2022/2554 rendelet hatálya alá tartozó szervezetekre.

[4] Ugyanott.