MÓDOSÍTÁSOK 001-001
előterjesztette: Ipari, Kutatási és Energiaügyi Bizottság

Jelentés
Lina Gálvez Muñoz **A9-0426/2023**
A kiberszolidaritásról szóló jogszabály

Rendeleti javaslat (COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Módosítás 1

AZ EURÓPAI PARLAMENT MÓDOSÍTÁSAI*

a Bizottság javaslatához

2023/0109 (COD)

Javaslat

AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE

a kiberbiztonsági fenyegetések és események észlelése, valamint az azokra való felkészülés és reagálás céljából az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról *és az (EU) 2021/694 rendelet módosításáról*

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 173. cikke (3) bekezdésére és 322. cikke (1) bekezdésének a) pontjára,

---

* Módosítások: az új vagy módosított szöveget félkövér dőlt betűtípus, a törléseket pedig a ▌ jel mutatja.

tekintettel az Európai Bizottság javaslatára,

a jogalkotási aktus tervezete nemzeti parlamenteknek való megküldését követően,

tekintettel a Számvevőszék véleményére[1],

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére[2],

tekintettel a Régiók Bizottságának véleményére[3],

rendes jogalkotási eljárás keretében,

mivel:

(1) Az információs és kommunikációs technológiák alkalmazása és az azoktól való függés alapvetően fontos ***szemponttá vált, de ezzel egyidejűleg a gazdasági tevékenységek és a demokrácia valamennyi ágazatában lehetséges sebezhetőségeket eredményezett***, mivel az európai közigazgatási szervek, vállalatok és polgárok ágazatok közötti és határokon átnyúló összekapcsoltságának és egymástól való függésének mértéke minden eddiginél nagyobb méreteket ölt.

(2) A módszereket és hatásokat tekintve a kiberbiztonsági események ***nagyságrendje, gyakorisága és hatása egyre számottevőbb Unió-szerte és globális szinten is,*** ideértve az ellátási láncok ellen elkövetett, kiberkémkedést, zsarolóvírusokkal való fenyegetést vagy zavarkeltést célzó támadásokat. E jelenségek komoly veszélyt jelentenek a hálózati és információs rendszerek működésére nézve. Tekintettel a fenyegetettségi helyzet gyorsan változó jellegére, ***a gazdaságokban és demokráciákban,*** a kritikus infrastruktúrákban ***Unió-szerte*** jelentős fennakadásokat vagy károkat okozó esetleges nagyszabású kiberbiztonsági események veszélye az EU kiberbiztonsági keretének minden szintjén fokozott felkészültséget igényel. Ez a veszély túlmutat az Ukrajna elleni orosz katonai agresszión, és tekintettel a jelenlegi geopolitikai feszültségekben közreműködő, államközeli ***és*** bűnözői ▌ körök sokféleségére, valószínűleg nem fog alábbhagyni. Az ilyen események akadályozhatják a közszolgáltatások nyújtását és a gazdasági tevékenységek folytatását – többek között a kritikus, illetve a kiemelten kritikus ágazatokban –, jelentős pénzügyi veszteségeket idézhetnek elő, alááshatják a felhasználók bizalmát, jelentős károkat okozhatnak az Unió gazdaságában, és akár egészségügyi vagy az emberi életet veszélyeztető következményekkel is járhatnak. Ezenkívül a kiberbiztonsági események kiszámíthatatlanok, mivel gyakran igen rövid időn belül alakulnak ki és eszkalálódnak, nem korlátozódnak egy adott földrajzi területre, hiszen több országot érintően egyidejűleg is előfordulhatnak vagy gyorsan terjedhetnek. ***Ezért szoros és összehangolt együttműködésre van szükség a közszféra, a magánszektor, a tudományos körök, a civil társadalom és a média között. Emellett az Unió reagálását össze kell hangolni a nemzetközi intézményekkel, valamint a megbízható és hasonlóan gondolkodó nemzetközi partnerekkel. A megbízható és hasonlóan gondolkodó nemzetközi partnerek olyan országok, amelyek a nemzetközi együttműködési keretekkel és megállapodásokkal összhangban osztják az Unió demokratikus értékeit, az emberi jogok iránti elkötelezettségét, a hatékony multilateralizmust és a szabályokon alapuló rendet. A megbízható és hasonlóan gondolkodó nemzetközi partnerekkel való együttműködés és a rendszerszintű riválisokkal szembeni védelem biztosítása érdekében a közbeszerzésről szóló***

---

1 HL C […]., […], […]. o.
2 HL C , , . o.
3 HL C , , . o.

többoldalú megállapodásban (GPA-ban) nem részes harmadik országokban letelepedett szervezetek nem vehetnek részt az e rendelet szerinti közbeszerzésekben.

(3) Szükséges a digitalizált gazdaság egészét tekintve megerősíteni az uniós ipari és szolgáltatási ágazat versenyhelyzetét, és a digitális egységes piac kiberbiztonsági szintjének megerősítése révén előmozdítani e szektorok digitális átalakulását. Az Európa jövőjéről szóló konferencia[1] három különböző javaslatában is szerepelt az ajánlás, miszerint növelni kell a polgárok, a vállalkozások, ***különösen*** a ***mikrovállalkozások, a kis- és középvállalkozások (kkv-k), köztük az induló innovatív***vállalkozások és a kritikus infrastruktúrákat működtető szervezetek **–** ***köztük a helyi és regionális önkormányzatok*** – rezilienciáját a növekvő kiberbiztonsági fenyegetésekkel szemben, amelyek pusztító társadalmi és gazdasági hatásokkal járhatnak. Ezért olyan infrastruktúrákba és szolgáltatásokba***, valamint a kiberbiztonsági készségek fejlesztéséhez szükséges képességek kiépítésébe*** történő beruházásokra van szükség, amelyek támogatják a kiberbiztonsági fenyegetések és események mielőbbi észlelését és az azokra való gyorsabb reagálást, továbbá a tagállamoknak segítségre van szükségük ahhoz, hogy jobban felkészüljenek és hatékonyabban reagáljanak a jelentős és nagyszabású kiberbiztonsági eseményekre. Az Uniónak e területeken is meg kell erősítenie képességeit, különösen a kiberbiztonsági fenyegetésekkel és eseményekkel kapcsolatos adatok gyűjtése és elemzése tekintetében.

(3a) A kibertámadások célpontjai gyakran helyi, regionális vagy nemzeti közszolgáltatások és infrastruktúrák. A helyi önkormányzatok pénzügyi és emberi erőforrásaik hiánya miatt a kibertámadások legsérülékenyebb célpontjai közé tartoznak. Ezért különösen fontos, hogy a helyi szintű döntéshozók tudatában legyenek annak, hogy növelniük kell a digitális rezilienciát, növelniük kell a kibertámadások hatásának csökkentésére irányuló kapacitásukat, és meg kell ragadniuk az e rendelet által kínált lehetőségeket.

(4) Az Unió már számos intézkedést hozott a kritikus infrastruktúrák és a kritikus szervezetek kiberbiztonsági kockázatokkal szembeni sebezhetőségének csökkentése és fokozott rezilienciája érdekében, ezek közé tartozik különösen az (EU) 2022/2555 európai parlamenti és tanácsi irányelv[2], az (EU) 2017/1584 bizottsági ajánlás[3], a 2013/40/EU európai parlamenti és tanácsi irányelv[4] és az (EU) 2019/881 európai parlamenti és tanácsi rendelet[5]. Ezen túlmenően a kritikus infrastruktúrák

---

1 https://futureu.europa.eu/en/

2 Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (HL L 333., 2022.12.27.).

3 A Bizottság (EU) 2017/1584 ajánlása (2017. szeptember 13.) a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról (HL L 239., 2017.9.19., 36. o.).

4 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.).

5 Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU

rezilienciájának megerősítését célzó összehangolt uniós megközelítésről szóló tanácsi ajánlás felkéri a tagállamokat, hogy hozzanak sürgős és hatékony intézkedéseket, továbbá hogy folytassanak lojális, hatékony, szolidáris és összehangolt együttműködést egymással, a Bizottsággal és más érintett hatóságokkal, valamint az érintett szervezetekkel a belső piacon az alapvető szolgáltatások nyújtásához használt kritikus infrastruktúrák fokozott rezilienciája érdekében.

(5) A növekvő kiberbiztonsági kockázatok és az általánosságban összetett fenyegetettségi helyzet okán – amely egyértelműen azzal a kockázattal jár, hogy a kiberbiztonsági események gyorsan tovagyűrűzhetnek az egyik tagállamból a másikba, illetve valamely harmadik országból az Unióba – a kiberbiztonsági fenyegetések és események eredményesebb észlelése, és az azokra való hatékonyabb felkészülés**,** reagálás***, valamint az azokat követő helyreállítás*** érdekében meg kell erősíteni az uniós szintű szolidaritást. Az Európai Unió kiberbiztonsági helyzetének javításáról szóló tanácsi következtetésekben a tagállamok felkérték a Bizottságot, hogy nyújtson be javaslatot egy új Kiberbiztonsági Vészhelyzeti Alapra vonatkozóan[1].

(6) Az EU kibervédelmi politikájáról szóló, 2022. november 10-én elfogadott közös közlemény[2] bejelentette az uniós kiberszolidaritási kezdeményezést, amelynek céljai a következők: a biztonsági műveleti központok (a továbbiakban: SOC-k) alkotta uniós ***hálózat*** kiépítésének előmozdítása révén a közös uniós észlelési, helyzetismereti és reagálási képességek megerősítése, a megbízható szolgáltatók szolgáltatásait igénybe vevő uniós szintű kiberbiztonsági tartalék fokozatos kiépítésének támogatása, valamint a kritikus szervezetek uniós kockázatértékeléseken alapuló tesztelése az esetleges sebezhetőségek tekintetében.

(7) Unió-szerte meg kell erősíteni a kiberbiztonsági fenyegetések és események észlelését és helyzetismeretét, valamint a tagállamok és az Unió jelentős és nagyszabású kiberbiztonsági eseményekre való felkészültségét***, azok megelőzését és az arra való reagálást*** szolgáló képességeinek javítása révén meg kell erősíteni a szolidaritást is. Ezért a közös észlelési és helyzetismereti képességek kialakítása és fejlesztése érdekében ki kell építeni a biztonsági műveleti központok páneurópai ***hálózatát*** (a továbbiakban: Európai Kiberpajzs), ***megerősítve az Unió veszélyfelderítési és információmegosztási képességeit***. Létre kell hozni a kiberbiztonsági vészhelyzeti mechanizmust, amely támogatja a tagállamokat a jelentős és nagyszabású kiberbiztonsági eseményekre való felkészülésben, reagálásban és az azonnali helyreállításban. Létre kell hozni a kiberbiztonsági események felülvizsgálati mechanizmusát konkrét jelentős vagy nagyszabású kiberbiztonsági események felülvizsgálata és értékelése céljából. Ezek az intézkedések nem érintik az Európai Unió működéséről szóló szerződés (EUMSZ) 107. és 108. cikkét.

(8) E célkitűzések elérése érdekében bizonyos területeket érintően módosítani kell az

---

rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (HL L 151., 2019.6.7., 15. o.).

[1] A Tanács következtetései az Európai Unió kiberbiztonsági helyzetének javításáról, amelyet a Tanács a 2022. május 23-i ülésén jóváhagyott (9364/22).

[2] Közös közlemény az Európai Parlamentnek és a Tanácsnak – Az EU kibervédelmi politikája, JOIN(2022)0049.

(EU) 2021/694 európai parlamenti és tanácsi rendeletet[1] is. Konkrétabban, e rendeletnek módosítania kell az (EU) 2021/694 rendeletet annak érdekében, hogy a Digitális Európa program 3. sz. egyedi célkitűzését kiegészítse az Európai Kiberpajzshoz és a kiberbiztonsági vészhelyzeti mechanizmushoz kapcsolódó új operatív célkitűzésekkel, amelynek célja a digitális egységes piac rezilienciájának, integritásának és megbízhatóságának garantálása, a kibertámadások és -fenyegetések nyomon követésére és az azokra való reagálásra szolgáló képességek megerősítése, valamint a kiberbiztonsággal kapcsolatos, határokon átnyúló együttműködés megerősítése. Ezenfelül meg kell állapítani azokat az egyedi feltételeket, amelyek mellett pénzügyi támogatás nyújtható az említett intézkedésekhez, és meg kell határozni a célkitűzések eléréséhez szükséges irányítási és koordinációs mechanizmusokat is. Az (EU) 2021/694 rendelet egyéb módosításai ismertetik az új operatív célkitűzések keretében javasolt intézkedéseket, valamint az új operatív célkitűzések végrehajtásának nyomon követésére szolgáló mérhető mutatókat.

(9) Az e rendelet szerinti intézkedések finanszírozásáról az (EU) 2021/694 rendelet rendelkezik, amely változatlanul a Digitális Európa program 3. sz. egyedi célkitűzésében foglalt intézkedések releváns alap-jogiaktusának számít. Az (EU) 2021/694 rendelet alkalmazandó rendelkezéseivel összhangban a vonatkozó munkaprogramok határozzák meg az egyes intézkedések egyedi részvételi feltételeit.

(9a) A geopolitikai fejlemények és a növekvő kiberfenyegetési helyzet (EPP 52) fényében, valamint az e rendeletben meghatározott intézkedések – különösen az európai kiberbiztonsági pajzs és a kiberbiztonsági szükséghelyzeti mechanizmus – 2027 utáni folytonosságának és továbbfejlesztésének biztosítása érdekében a 2028–2034 közötti időszakra szóló többéves pénzügyi keretben külön költségvetési sort kell biztosítani. A tagállamoknak kötelezettséget kell vállalniuk arra, hogy támogatják a kiberfenyegetések és -események Unió-szerte történő csökkentéséhez és a szolidaritás megerősítéséhez szükséges valamennyi intézkedést.

(10) Erre a rendeletre az Európai Parlament és a Tanács által az EUMSZ 322. cikke alapján elfogadott horizontális költségvetési szabályok alkalmazandók. E szabályokat ***az (EU, Euratom) 2018/1046 európai parlamenti és tanácsi rendelet***[2] állapítja meg, és e szabályok meghatározzák különösen az uniós költségvetés elkészítésére és végrehajtására vonatkozó eljárást, továbbá rendelkeznek a pénzügyi szereplők felelősségével kapcsolatos ellenőrzésekről. Az EUMSZ 322. cikke alapján elfogadott szabályok az uniós költségvetés védelmét szolgáló, az (EU, Euratom) 2020/2092 európai parlamenti és tanácsi rendeletben meghatározott általános feltételrendszert is

---

1 Az Európai Parlament és a Tanács (EU) 2021/694 rendelete (2021. április 29.) a Digitális Európa program létrehozásáról és az (EU) 2015/2240 határozat hatályon kívül helyezéséről (HL L 166., 2021.5.11., 1. o.).

2 Az Európai Parlament és a Tanács (EU, Euratom) 2018/1046 rendelete (2018. július 18.) az Unió általános költségvetésére alkalmazandó pénzügyi szabályokról, az 1296/2013/EU, az 1301/2013/EU, az 1303/2013/EU, az 1304/2013/EU, az 1309/2013/EU, az 1316/2013/EU, a 223/2014/EU és a 283/2014/EU rendelet és az 541/2014/EU határozat módosításáról, valamint a 966/2012/EU, Euratom rendelet hatályon kívül helyezéséről (HL L 193., 2018.7.30., 1. o.).
ELI: ***http://data.europa.eu/eli/reg/2018/1046/oj).***

magukban foglalják[1].

(11) A hatékony és eredményes pénzgazdálkodás érdekében egyedi szabályokat kell megállapítani a fel nem használt kötelezettségvállalási és kifizetési előirányzatok átvitelére vonatkozóan. Az uniós költségvetés évenkénti meghatározására vonatkozó elv tiszteletben tartása mellett e rendeletnek a kiberbiztonsági környezet kiszámíthatatlan, rendkívüli és egyedi jellege miatt rendelkeznie kell arról, hogy a fel nem használt források ***az (EU, Euratom) 2018/1046*** rendeletben meghatározottakon felül is átvihetők legyenek, ezáltal maximalizálva a kiberbiztonsági vészhelyzeti mechanizmus azon képességét, hogy támogassa a tagállamokat a kiberfenyegetések elleni hatékony küzdelemben.

(11a) Az e rendelettel létrehozott kiberbiztonsági szükséghelyzeti mechanizmus és az uniós kiberbiztonsági tartalék új kezdeményezések, amelyeket nem irányoztak elő a 2021–2027-es időszakra vonatkozó többéves pénzügyi keret létrehozása során, és e kezdeményezések finanszírozásának célja, hogy a lehető legkisebbre korlátozza a Digitális Európa program egyéb prioritásaira fordított finanszírozás csökkentését. Az uniós kiberbiztonsági tartalékra szánt pénzügyi források összegét ezért csökkenteni kell, és azt elsősorban a többéves pénzügyi keret felső határai alatt rendelkezésre álló mozgástérből kell lehívni, vagy a többéves pénzügyi keret nem tematikus speciális eszközein keresztül kell mozgósítani. A meglévő programok forrásainak elkülönítését vagy átcsoportosítását a lehető legalacsonyabb szinten kell tartani annak érdekében, hogy megvédjék a meglévő programokat, különösen az Erasmus+ programot a negatív hatásoktól, és biztosítsák, hogy ezek a programok elérhessék kitűzött céljaikat.

(12) A kiberbiztonsági fenyegetések és események eredményesebb megelőzése és értékelése, az azokra való hatékonyabb reagálás***, valamint az azokat követő helyreállítás*** érdekében átfogóbb ismereteket kell kialakítani az Unió területén található stratégiai eszközöket és kritikus infrastruktúrákat fenyegető veszélyekről, beleértve azok földrajzi elhelyezkedését, összekapcsoltságát és az ezen infrastruktúrákat érintő kibertámadások lehetséges hatásait is. ***A potenciális kiberfenyegetések azonosítására, enyhítésére és megelőzésére irányuló proaktív megközelítés magában foglalja az előrehaladott, tartós fenyegetések megállításához szükséges fejlett felderítési képességek fokozott kapacitását. A fenyegetésekkel kapcsolatos hírszerzési információk a potenciális fenyegetések és kockázatok megértése érdekében gyűjtött, elemzett és értelmezett információk. A hatalmas mennyiségű adat elemzésével és összekapcsolásával olyan mintákat, tendenciákat és fertőzöttségi mutatókat tárnak fel, amelyek rosszindulatú tevékenységekre vagy sebezhetőségekre deríthetnek fényt.*** Ki kell építeni a biztonsági műveleti központok ***hálózatát*** (a továbbiakban: Európai Kiberpajzs), amelyet olyan interoperabilitás jellemezte, határokon átnyúló platformok alkotnak, amelyek mindegyike több nemzeti biztonsági műveleti központot tömörít. Ennek a korszerű technológiákra támaszkodó fejlett adatgyűjtési és -elemzési eszközöket használó, a kiberfenyegetések észlelésére és kezelésére irányuló képességeket javító, és valós idejű helyzetismeretet biztosító infrastruktúrának a nemzeti és uniós kiberbiztonsági érdekeket és igényeket kell szolgálnia. ***A nemzeti biztonsági műveleti központ egy központosított kapacitás,***

[1] ***Az Európai Parlament és a Tanács (EU, Euratom) 2020/2092 rendelete (2020. december 16.) az uniós költségvetés védelmét szolgáló általános feltételrendszerről*** *(HL L 433I., 2020.12.22., 1. o.)* ***ELI: http://data.europa.eu/eli/reg/2020/2092/oj).***

amely képes a fenyegetésekkel kapcsolatos hírszerzési információk folyamatos gyűjtésére és a nemzeti joghatóság alá tartozó szervezetek kiberbiztonsági helyzetének javítására a kiberbiztonsági fenyegetések megelőzése, észlelése és elemzése révén. Az infrastruktúra a kiberbiztonsági fenyegetések és események fokozott észlelését hivatott előmozdítani, és ezáltal kiegészíteni és támogatni az Unión belüli válságkezelésért felelős uniós szervezeteket és hálózatokat, nevezetesen az (EU) 2022/2555 európai parlamenti és tanácsi irányelvben[1] meghatározott Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatát (a továbbiakban: EU-CyCLONe).

(13) ***A Kiberpajzsban való részvétel érdekében minden tagállamnak ki kell jelölnie*** egy nemzeti szintű közjogi szervet, amelynek feladata az adott tagállamban a kiberfenyegetés-észlelési és információmegosztási tevékenységek koordinálása. ***A Bizottság arra ösztönzi a tagállamokat, hogy építsék be a nemzeti biztonsági műveleti központ kapacitásait a már meglévő kiberstruktúrájukba és -irányításukba, hogy ne hozzanak létre további irányítási szinteket, és hangolják össze e rendeletet a már meglévő jogalkotási aktusokkal, többek között az (EU) 2022/2555 irányelvvel.*** Ezeknek a nemzeti biztonsági műveleti központoknak nemzeti szinten referenciapontként és átjáróként kell szolgálniuk ***a magán- és állami szervezetek, különösen a nemzeti biztonsági műveleti központok Európai Kiberpajzsban való részvételéhez,*** és biztosítaniuk kell, hogy az állami és magánszervezetektől származó, kiberfenyegetésekkel kapcsolatos információkat nemzeti szinten hatékonyan és egységesen osszák meg és gyűjtsék össze. ***A nemzeti biztonsági műveleti központoknak meg kell erősíteniük az állami és a magánszervezetek közötti együttműködést és információmegosztást, hogy megszüntethessék a jelenleg létező kommunikációs silókat. Ennek során támogathatják adatcseremodellek létrehozását, valamint meg kell könnyíteniük és ösztönözniük kell az információk megbízható és biztonságos környezetben történő megosztását. Az állami és magánszervezetek közötti szoros és összehangolt együttműködés központi szerepet játszik az Unió kiberbiztonsági rezilienciájának megerősítésében.***

(14) Az Európai Kiberpajzs részeként több határokon átnyúló biztonsági műveleti központot (a továbbiakban: határokon átnyúló SOC) kell létrehozni. A határokon átnyúló fenyegetések észlelése, valamint az információmegosztás és -kezelés előnyeinek teljes körű kiaknázása érdekében e központoknak legalább három tagállam nemzeti biztonsági műveleti központjából kell állniuk. A határokon átnyúló biztonsági műveleti központok általános célkitűzése a kiberbiztonsági fenyegetések elemzésére, megelőzésére és észlelésére szolgáló kapacitások megerősítése, valamint a magas színvonalú hírszerzési***információk előállításának támogatása, beleértve az esetleges rosszindulatú feltörésekre, újonnan kifejlesztett rosszindulatú fenyegetésekre és a sebezhetőségek kihasználására vonatkozó adatok és információk gyűjtését és megosztását, amelyeket még nem vetettek be kiberbiztonsági események során, valamint a kiberbiztonsági fenyegetésekkel kapcsolatos elemzési erőfeszítések, különösen a különböző köz- vagy magánforrásokból származó adatok megosztása, valamint a legkorszerűbb eszközök megosztása és közös használata révén, valamint***

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

a tagállamok közötti operatív együttműködéssel kapcsolatos ügyekben a felderítési, elemzési és megelőzési képességeknek az ENISA támogatásával történő közös fejlesztése révén. ***A határokon átnyúló biztonsági műveleti központoknak meg kell könnyíteniük és ösztönözniük kell az információk megbízható és biztonságos környezetben történő megosztását, és*** a meglévő biztonsági műveleti központokra, számítógép-biztonsági eseményekre reagáló csoportokra (a továbbiakban: CSIRT) és más érintett szereplőkre támaszkodva és azokat kiegészítve új további kapacitást kell biztosítaniuk.

(15) Nemzeti szinten a kiberfenyegetések nyomon követését, észlelését és elemzését jellemzően az állami és magánszervezetek biztonsági műveleti központjai biztosítják a CSIRT-ekkel együttműködve. Emellett a CSIRT-ek az (EU) 2022/2555 irányelvvel összhangban a CSIRT-ek hálózata keretében folytatnak információcserét. A határokon átnyúló biztonsági műveleti központoknak olyan új ***kapacitást kell kialakítaniuk, amely oly módon épül be a már létező kiberbiztonsági infrastruktúrába, különösen a CSIRT-ek hálózatába***, hogy összegyűjti és megosztja az állami és magánszervezetektől, ***különösen azok biztonsági műveleti központjaiból származó,*** kiberbiztonsági fenyegetésekkel kapcsolatos adatokat, majd szakértői elemzések, közösen beszerzett infrastruktúrák és a legkorszerűbb eszközök révén növeli az ilyen adatok értékét, valamint hozzájárul ***az Unió technológiai szuverenitásához, nyitott stratégiai autonómiájához, versenyképességéhez és rezilienciájához, valamint egy jelentős kiberbiztonsági ökoszisztéma kialakításához, többek között megbízható és hasonlóan gondolkodó nemzetközi partnerekkel együttműködésben***. .

(16) A határokon átnyúló biztonsági műveleti központoknak olyan központi pontként kell működniük, amely lehetővé teszi a releváns adatok és kiberfenyegetettségi információk kiterjedt gyűjtését, és a szóban forgó információk különféle szereplők (pl. hálózatbiztonsági vészhelyzeteket elhárító csoportok (CERT), CSIRT-ek, információmegosztó és -elemző központok (ISAC), kritikus infrastruktúrák üzemeltetői) közötti széles körű terjesztését ***a jelenleg létező kommunikációs silók megszüntetésének megkönnyítése érdekében***. ***Ennek során a határokon átnyúló biztonsági műveleti központok támogathatnák az Unión belüli adatcsere-modellek létrehozását is.*** A határokon átnyúló biztonsági műveleti központok résztvevői közötti információcsere kiterjedhet a hálózatokból és érzékelőkből származó adatokra, a kiberfenyegetettségi információk hírcsatornáira, a fertőzöttségi mutatókra, valamint a kiberbiztonsági eseményekre, fenyegetésekre és sebezhetőségekre vonatkozó, kontextusba helyezett információkra, ***beleértve az esetleges rosszindulatú feltörésekre, az újonnan kifejlesztett rosszindulatú fenyegetésekre és kizsákmányolásokra vonatkozó adatok és információk gyűjtését és megosztását, amelyeket még nem vetettek be kiberbiztonsági eseményekre, valamint elemzési erőfeszítésekre***. Emellett a határokon átnyúló biztonsági műveleti központoknak együttműködési megállapodásokat kell kötniük más határokon átnyúló biztonsági műveleti központokkal is.

(17) Az érintett hatóságok közösen kialakított helyzetismerete elengedhetetlen előfeltétele a jelentős és nagyszabású kiberbiztonsági eseményekkel kapcsolatos uniós szintű felkészültségnek és koordinációnak. A nagyszabású kiberbiztonsági események és válsághelyzetek operatív szintű összehangolt kezelésének támogatása, valamint a releváns információk tagállamok és az Unió intézményei, szervei, hivatalai és ügynökségei közötti rendszeres cseréjének biztosítása érdekében az (EU) 2022/2555 irányelv létrehozta az EU-CyCLONe-t. A nagyszabású kiberbiztonsági eseményekre

és válsághelyzetekre való összehangolt reagálásról szóló (EU) 2017/1584 ajánlás valamennyi érintett szereplő feladataival foglalkozik. Az (EU) 2022/2555 irányelv emlékeztet továbbá a Bizottságnak az 1313/2013/EU európai parlamenti és tanácsi határozattal[1] létrehozott uniós polgári védelmi mechanizmussal (a továbbiakban: UCPM) kapcsolatos feladataira, valamint arra, hogy a Bizottság feladata az is, hogy elemző jelentéseket készítsen az (EU) 2018/1993 ***tanácsi*** végrehajtási határozat[2] szerinti uniós politikai szintű integrált válságelhárítási mechanizmus (a továbbiakban: IPCR-mechanizmus) számára. Ezért azokban az esetekben, amikor a határokon átnyúló biztonsági műveleti központok potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményről szereznek információkat, releváns információkat kell szolgáltatniuk az EU-CyCLONe, a CSIRT-ek hálózata és a Bizottság számára, ***az (EU) 2022/2555 irányelvvel összhangban***. A helyzettől függően a megosztandó információk közé tartozhatnak különösen a technikai információk, a támadó vagy potenciális támadó jellegére és szándékaira vonatkozó információk, valamint a potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményekkel kapcsolatos magasabb szintű, nem technikai jellegű információk. Ebben az összefüggésben kellő figyelmet kell fordítani a szükséges ismeret elvére és a megosztott információk potenciálisan érzékeny jellegére.

(18) Az Európai Kiberpajzsban részt vevő szervezeteknek gondoskodniuk kell az egymás közötti magas szintű interoperabilitásról, beleértve adott esetben az adatformátumokat, a taxonómiát, az adatkezelésre és az adatelemzésre szolgáló eszközöket, valamint a biztonságos kommunikációs csatornákat, az alkalmazási réteg minimális biztonsági szintjét, a helyzetismereti jelzőrendszert és a mutatókat. A kiberbiztonsági események technikai okait és hatásait leíró helyzetjelentések egységes taxonómiájának és sablonjának elfogadása kapcsán figyelembe kell venni az események bejelentésével kapcsolatban az (EU) 2022/2555 irányelv végrehajtásával összefüggésben már folyamatban lévő munkát.

(19) Annak érdekében, hogy a különböző forrásokból származó, kiberbiztonsági fenyegetésekkel kapcsolatos adatcserére széles körben és megbízható környezetben kerülhessen sor, az Európai Kiberpajzsban részt vevő szervezeteket korszerű és rendkívül biztonságos eszközökkel, berendezésekkel és infrastruktúrákkal kell felszerelni***, valamint képzett személyzettel kell ellátni.*** Ez várhatóan lehetővé teszi a közös észlelési képességek javítását és a hatóságok és az érintett szervezetek időben történő figyelmeztetését, különösen a legkorszerűbb mesterségesintelligencia- és adatelemzési technológiák alkalmazásával.

(20) Az Európai Kiberpajzs az adatgyűjtésnek, -megosztásnak és -cserének köszönhetően várhatóan meg fogja erősíteni az Unió technológiai szuverenitását, ***nyitott stratégiai autonómiáját, versenyképességét és rezilienciáját, valamint egy jelentős uniós kiberbiztonsági ökoszisztémát***. A kiváló minőségű gondozott adatok összevonása minden bizonnyal hozzájárul a fejlett mesterségesintelligencia- és adatelemzési technológiák fejlesztéséhez is. ***A mesterséges intelligencia akkor a leghatékonyabb,***

---

1 ***Az Európai Parlament és a Tanács 1313/2013/EU határozata (2013. december 17.) az uniós polgári védelmi mechanizmusról (EGT-vonatkozású szöveg) (HL L 347., 2013.12.20., 924. o., ELI:*** http://data.europa.eu/eli/dec/2013/1313/oj***).***

2 ***A Tanács (EU) 2018/1993 végrehajtási határozata (2018. december 11.) az uniós politikai szintű integrált válságelhárítási mechanizmusról (HL L 320., 2018.12.17., 28. o.), ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).***

ha ember által végzett elemzéssel párosítják. Ezért a képzett munkaerő továbbra is elengedhetetlen a jó minőségű adatok összegyűjtéséhez. Ezt az Európai Kiberpajzsnak az (EU) 2021/1173 tanácsi rendelettel[1] létrehozott páneurópai nagy teljesítményű számítástechnikai infrastruktúrával való összekapcsolása révén kell elősegíteni.

(21) Jóllehet az Európai Kiberpajzs polgári projekt, a kibervédelmi közösség számára is előnyt jelenthetnek a kritikus infrastruktúrák védelmére kifejlesztett, erősebb polgári észlelési és helyzetismereti képességek. A határokon átnyúló biztonsági műveleti központoknak a Bizottság és az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont (a továbbiakban: ECCC) támogatásával, valamint az Unió külügyi és biztonságpolitikai főképviselőjének (a továbbiakban: főképviselő) közreműködésével a kibervédelmi közösséggel való együttműködés érdekében ***célzott hozzáférési feltételeket, biztosítékokat,*** protokollokat és szabványokat – többek között ellenőrzési és biztonsági feltételeket – kell fokozatosan kidolgozniuk***, tiszteletben tartva a kezdeményezések polgári jellegét és a finanszírozás rendeltetését, ezáltal felhasználva a védelmi közösség rendelkezésére álló forrásokat***. Az Európai Kiberpajzsnak a főképviselővel szoros együttműködésben ***és a jogok és szabadságok teljes körű tiszteletben tartása mellett*** folytatott fejlesztését olyan szemléletnek kell kísérnie, amely lehetővé teszi a kibervédelmi közösségen belüli információmegosztásért felelős hálózatokkal és platformokkal való együttműködést.

(22) Az Európai Kiberpajzs résztvevői közötti információmegosztásnak meg kell felelnie a meglévő jogi követelményeknek, különösen az uniós és nemzeti adatvédelmi jogszabályoknak, valamint az információcserére irányadó uniós versenyjogi szabályoknak. Amennyiben személyes adatok kezelésére is szükség van, az információ címzettjének olyan technikai és szervezeti intézkedéseket kell végrehajtania, amelyek védik az érintettek jogait és szabadságait, és amint az adatok a megjelölt célból már nem szükségesek, meg kell azokat semmisítenie, majd tájékoztatnia kell az adatokat rendelkezésre bocsátó szervet arról, hogy az adatokat megsemmisítették.

(23) Az EUMSZ 346. cikkének sérelme nélkül az uniós vagy nemzeti ***jogszabályok*** értelmében bizalmas információk cseréjét az információcsere célja szempontjából releváns és azzal arányos információkra kell korlátozni. A szóban forgó információcsere során meg kell őrizni az információk bizalmas jellegét, és a kereskedelmi és üzleti titkok teljes körű tiszteletben tartása mellett óvni kell az érintett szervezetek biztonsági és kereskedelmi érdekeit.

(24) Tekintettel arra, hogy a tagállamokat érintő kiberbiztonsági események egyre nagyobb kockázatot jelentenek és egyre gyakoribbak, létre kell hozni egy válsághelyzetek kezelését célzó támogatási eszközt, amely javítja az Unió jelentős és nagyszabású kiberbiztonsági eseményekkel szembeni rezilienciáját, és a felkészültséghez, a reagáláshoz és az alapvető szolgáltatások azonnali helyreállításához nyújtott vészhelyzeti pénzügyi támogatás révén kiegészíti a tagállamok intézkedéseit. Ennek az eszköznek lehetővé kell tennie a meghatározott körülmények közötti és egyértelmű feltételek melletti gyors és tényleges segítségnyújtást, valamint a források

[1] A Tanács (EU) 2021/1173 rendelete (2021. július 13.) az európai nagy teljesítményű számítástechnikával foglalkozó közös vállalkozás létrehozásáról és az (EU) 2018/1488 rendelet hatályon kívül helyezéséről (HL L 256., 2021.7.19., 3. o., ***ELI: http://data.europa.eu/eli/reg/2021/1173/oj***).

felhasználásának részletes nyomon követését és értékelését. Míg a kiberbiztonsági események és válsághelyzetek megelőzése, valamint az azokra való felkészülés és reagálás elsősorban a tagállamok feladata, a kiberbiztonsági vészhelyzeti mechanizmus az Európai Unióról szóló szerződés (a továbbiakban: EUSZ) 3. cikkének (3) bekezdésével összhangban előmozdítja a tagállamok közötti szolidaritást.

(25) Jelentős és nagyszabású ***sürgősségi*** kiberbiztonsági eseményekre való reagálás alkalmával és az eseményt követő azonnali helyreállítás során a kiberbiztonsági vészhelyzeti mechanizmusnak a tagállami intézkedéseket és erőforrásokat, valamint a rendelkezésre álló egyéb támogatási lehetőségeket – például az Európai Uniós Kiberbiztonsági Ügynökség (a továbbiakban: ENISA) által a megbízatásával összhangban nyújtott szolgáltatásokat, a CSIRT-ek hálózata nyújtotta összehangolt reagálást és segítséget, az EU-CyCLONe mérséklési támogatását, valamint a tagállamok közötti, többek között az EUSZ 42. cikkének (7) bekezdésével összefüggésben az állandó strukturált együttműködés (PESCO) kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportjai és a hibrid fenyegetéseket kezelő uniós gyorsreagálású csapatai[1] keretében nyújtott kölcsönös segítségnyújtást – kiegészítve kell támogatnia a tagállamokat. A mechanizmusnak az igényekre reagálva biztosítania kell, hogy Unió-szerte és harmadik országokban speciális eszközök álljanak rendelkezésre, amelyek támogatják a kiberbiztonsági eseményekre való felkészültséget és reagálást.

(26) Ez az eszköz nem érinti a válságelhárítás uniós szintű összehangolására szolgáló eljárásokat és kereteket, így különösen az uniós polgári védelmi mechanizmust[2], az uniós politikai szintű integrált válságelhárítási mechanizmust[3], sem az (EU) 2022/2555 irányelvet. Hozzájárulhat ugyanakkor az EUSZ 42. cikkének (7) bekezdésével összefüggésben vagy az EUMSZ 222. cikkében meghatározott helyzetekben végrehajtott intézkedésekhez, illetve kiegészítheti azokat. Ezen eszköz használatát adott esetben össze kell hangolni a kiberdiplomáciai eszköztár intézkedéseinek végrehajtásával is.

(27) Az e rendelet alapján biztosított segítségnyújtásnak támogatnia kell a tagállamok által nemzeti szinten hozott intézkedéseket, és ki kell egészítenie azokat. E célból biztosítani kell a Bizottság, az ENISA és az érintett tagállam közötti szoros együttműködést és konzultációt. Amikor valamely tagállam támogatást kér a kiberbiztonsági vészhelyzeti mechanizmus keretében, meg kell adnia a támogatás iránti igényét alátámasztó releváns információkat.

(28) Az (EU) 2022/2555 irányelv előírja a tagállamok számára, hogy jelöljenek ki vagy hozzanak létre egy vagy több, kiberválságok kezelésével foglalkozó hatóságot, és biztosítsák, hogy azok megfelelő forrásokkal rendelkezzenek a rájuk ruházott feladatok hatékony és eredményes ellátásához. Előírja továbbá a tagállamok számára,

---

1 A Tanács (KKBP) 2017/2315 határozata (2017. december 11.) az állandó strukturált együttműködés (PESCO) létrehozásáról és a részt vevő tagállamok jegyzékének meghatározásáról.

2 Az Európai Parlament és a Tanács 1313/2013/EU határozata (2013. december 17.) az uniós polgári védelmi mechanizmusról (HL L 347., 2013.12.20., 924. o.).

3 Uniós politikai szintű integrált válságelhárítási mechanizmus (IPCR-mechanizmus) és a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról szóló, 2017. szeptember 13-i (EU) 2017/1584 bizottsági ajánlással összhangban.

hogy meghatározzák azon képességeket, eszközöket és eljárásokat, amelyek válság esetén alkalmazhatók, valamint hogy fogadjanak el nemzeti szintű nagyszabású kiberbiztonsági esemény- és válságelhárítási tervet, amelyben meghatározzák a nagyszabású kiberbiztonsági események és válsághelyzetek kezelésének célkitűzéseit és szabályait. A tagállamoknak továbbá létre kell hozniuk egy vagy több CSIRT-et, amelyek feladata a biztonsági események egy jól meghatározott folyamat szerinti kezelése, amely kiterjed legalább az említett irányelv hatálya alá tartozó ágazatokra, alágazatokra és szervezettípusokra, és biztosítaniuk kell, hogy hogy minden CSIRT megfelelő erőforrásokkal rendelkezzen feladatai hatékony ellátásához. Ez a rendelet nem érinti a Bizottság szerepét annak biztosításában, hogy a tagállamok megfeleljenek az (EU) 2022/2555 irányelvben foglalt kötelezettségeknek. A kiberbiztonsági vészhelyzeti mechanizmusnak segítséget kell nyújtania a felkészültség megerősítésére irányuló intézkedésekhez, valamint a jelentős és nagyszabású kiberbiztonsági események hatásának enyhítését, az azonnali helyreállítás támogatását és/vagy az alapvető szolgáltatások működésének helyreállítását célzó, kiberbiztonsági eseményekre való reagálással kapcsolatos intézkedésekhez.

(29) A következetes megközelítés előmozdítása, valamint az Unió és belső piaca biztonságának megerősítése érdekében a felkészültségi intézkedések részeként támogatást kell nyújtani az (EU) 2022/2555 irányelv alapján azonosított, kiemelten kritikus ágazatokban működő szervezetek kiberbiztonságának összehangolt teszteléséhez és értékeléséhez. E célból a Bizottságnak az ENISA támogatásával és az (EU) 2022/2555 irányelvvel létrehozott Kiberbiztonsági Együttműködési Csoporttal együttműködésben rendszeresen azonosítania kell azokat az érintett ágazatokat vagy alágazatokat, amelyeket az uniós szinten összehangolt tesztelés összefüggésében pénzügyi támogatásra jogosultnak kell minősíteni. Az ágazatokat vagy alágazatokat az (EU) 2022/2555 irányelv I. mellékletéből („A kiemelten kritikus ágazatok”) kell kiválasztani. Az összehangolt tesztelésnek közös kockázati forgatókönyveken és módszereken kell alapulnia. Az ágazatok kiválasztása és a kockázati forgatókönyvek kidolgozása során figyelembe kell venni a vonatkozó uniós szintű kockázatértékeléseket és kockázati forgatókönyveket, többek között a párhuzamosságok elkerülése végett, például az Európai Unió kiberbiztonsági helyzetének javításáról szóló tanácsi következtetésekben a Bizottsághoz, a főképviselőhöz és a Kiberbiztonsági Együttműködési Csoporthoz intézett felkérés szerinti, az érintett polgári és katonai szervekkel és ügynökségekkel, valamint a már működő hálózatokkal – többek között az EU-CyCLONe-nal – koordinációban elvégzendő kockázatértékeléssel és kidolgozandó kiberbiztonsági szempontú kockázati forgatókönyvvel, vagy a távközlési hálózatokra és infrastruktúrákra vonatkozóan a nevers-i közös miniszteri felhívás nyomán a Kiberbiztonsági Együttműködési Csoport által, a Bizottság és az ENISA támogatásával, az Európai Elektronikus Hírközlési Szabályozók Testületével (BEREC) együttműködésben elvégzendő kockázatértékeléssel, vagy az (EU) 2022/2555 irányelv 22. cikke alapján elvégzendő összehangolt kockázatértékelésekkel, illetve az (EU) 2022/2554 európai parlamenti és tanácsi rendeletben előírt digitális működési reziliencia tesztelésével[1]. Az ágazatok kiválasztásakor figyelembe kell venni a kritikus infrastruktúrák

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

rezilienciájának megerősítését célzó összehangolt uniós megközelítésről szóló tanácsi ajánlást is.

(30) Emellett a kiberbiztonsági vészhelyzeti mechanizmusnak támogatást kell nyújtania más felkészültségi intézkedésekhez, és támogatnia kell a felkészültséget más olyan ágazatokban, amelyekre nem terjed ki a kiemelten kritikus ágazatokban működő szervezetek összehangolt tesztelése. A szóban forgó intézkedések különböző típusú nemzeti szintű felkészültségi tevékenységeket foglalhatnak magukban.

(31) A kiberbiztonsági vészhelyzeti mechanizmusnak emellett támogatást kell nyújtania a jelentős és nagyszabású kiberbiztonsági események hatásának enyhítését, az azonnali helyreállítás támogatását és az alapvető szolgáltatások működésének helyreállítását célzó, kiberbiztonsági eseményekre való reagálással kapcsolatos intézkedésekhez. Adott esetben ki kell egészítenie az uniós polgári védelmi mechanizmust, biztosítva a kiberbiztonsági események polgárokra gyakorolt hatásaira való reagálás átfogó megközelítését.

(32) A kiberbiztonsági vészhelyzeti mechanizmusnak támogatást kell biztosítania azokban az esetekben, amikor a tagállamok segítséget nyújtanak egy jelentős vagy nagyszabású kiberbiztonsági esemény által érintett tagállamnak, többek között az (EU) 2022/2555 irányelv 15. cikkében meghatározott CSIRT-ek hálózata révén. A segítséget nyújtó tagállamok számára lehetővé kell tenni, hogy kérelmeket nyújtsanak be a szakértői csoportok kölcsönös segítségnyújtás keretében történő kiküldésével kapcsolatos költségek fedezésére. Az elszámolható költségek közé tartozhatnak a kiberbiztonsági szakértők utazási, szállás- és napidíjköltségei.

(33) Fokozatosan létre kell hozni egy uniós szintű kiberbiztonsági tartalékot, amely az irányított biztonsági szolgáltatások magánszolgáltatói által nyújtott szolgáltatásokból áll, amelyek jelentős vagy nagyszabású kiberbiztonsági események alkalmával támogatják a reagálást és az azonnali helyreállítási intézkedéseket. Az uniós kiberbiztonsági tartaléknak biztosítania kell a szolgáltatások rendelkezésre állását és készenlétét, ***ugyanakkor meg kell erősítenie az Unió rezilienciáját, beleértve a kkv-nak minősülő, európai irányítású biztonsági szolgáltatók részvételét, és biztosítania kell a kiberbiztonsági ökoszisztéma – különösen a mikrovállalkozások, a kkv-k és az induló innovatív vállalkozások – létrehozását, a legkorszerűbb technológiák – például a felhővel és a mesterséges intelligenciával kapcsolatos technológiák – fejlesztésére irányuló kutatásba és innovációba (K+I) történő beruházásokkal együtt***. ***A megbízható szolgáltatók, köztük a kkv-k számára lehetővé kell tenni, hogy a fenti kritériumok teljesítése érdekében együttműködjenek egymással.*** Az uniós kiberbiztonsági tartalék szolgáltatásai a nemzeti hatóságokat hivatottak támogatni abban, hogy a saját nemzeti szintű intézkedéseik kiegészítéseként segítséget nyújtsanak a kritikus vagy kiemelten kritikus ágazatokban működő érintett szervezeteknek. Ezért a kiberbiztonsági tartalék keretében ösztönözni kell a kutatásba és innovációba történő beruházásokat e technológiák fejlesztésének fellendítése érdekében. Szükség esetén a megbízható szolgáltatókkal és a kiberbiztonsági tartalék potenciális felhasználóival közös gyakorlatokat lehet végezni a tartalék hatékony működésének biztosítása érdekében. Az uniós kiberbiztonsági tartalék keretében nyújtott támogatás kérelmezésekor a tagállamoknak meg kell határozniuk az érintett szervezetnek nemzeti szinten nyújtott támogatást, amelyet figyelembe kell venni a tagállami kérelem értékelésekor. Az uniós kiberbiztonsági tartalék szolgáltatásai hasonló feltételek mellett az uniós intézményeknek, szerveknek***, hivataloknak*** és ügynökségeknek is támogatást nyújthatnak. ***A Bizottságnak biztosítania kell a***

tagállamok bevonását és a velük folytatott széles körű információcserét a hasonló kezdeményezésekkel való átfedések elkerülése érdekében, többek között az Észak-atlanti Szerződés Szervezetén (NATO) belül.

(34) Az uniós kiberbiztonsági tartalék keretében szolgáltatásokat nyújtó magánszolgáltatók kiválasztása céljából meg kell határozni az e szolgáltatók kiválasztására irányuló ajánlati felhívásban szereplő minimumkritériumokat, biztosítva, hogy a tagállami hatóságok és a kritikus vagy kiemelten kritikus ágazatokban működő szervezetek igényei teljesüljenek.***Ösztönözni kell a regionális és helyi szinten aktív kisebb szolgáltatók részvételét.***

(35) Az uniós kiberbiztonsági tartalék létrehozásának előmozdítása érdekében a Bizottság fontolóra vehetné, hogy felkérje az ENISA-t, hogy az (EU) 2019/881 rendelet alapján dolgozzon ki egy javasolt tanúsítási rendszert a kiberbiztonsági vészhelyzeti mechanizmus hatálya alá tartozó területeken nyújtott irányított biztonsági szolgáltatásokra vonatkozóan. ***Az e rendelkezésből eredő további feladatok ellátása érdekében az ENISA-nak megfelelő, kiegészítő finanszírozásban kell részesülnie.***

(36) E rendelet azon célkitűzéseinek támogatása érdekében, amelyek a közös helyzetismeret előmozdítására, az Unió rezilienciájának fokozására és a jelentős és nagyszabású kiberbiztonsági eseményekre való hatékony reagálás lehetővé tételére irányulnak, lehetővé kell tenni, hogy egy adott jelentős vagy nagyszabású kiberbiztonsági esemény kapcsán az EU-CyCLONe, a CSIRT-ek hálózata vagy a Bizottság felkérje az ENISA-t, hogy vizsgálja felül és értékelje a fenyegetéseket, a sebezhetőségeket és a mérséklési intézkedéseket. Az esemény felülvizsgálatának és értékelésének befejeztével az ENISA-nak az érintett érdekelt felekkel, többek között a magánszektor, a tagállamok, a Bizottság és más érintett uniós intézmények, szervek***,*** ***hivatalok*** és ügynökségek képviselőivel együttműködésben eseményértékelési jelentést kell készítenie. Ami a magánszektort illeti, az ENISA a szakosodott szolgáltatókkal – többek között az irányított biztonsági megoldások szolgáltatóival és értékesítőivel – folytatott információcserét szolgáló csatornákat fejleszt ki annak érdekében, hogy hozzájáruljon az ENISA azon küldetéséhez, hogy Unió-szerte egységesen magas szintű kiberbiztonságot érjen el. Az érdekelt felekkel – többek között a magánszektorral – folytatott együttműködésre építve a konkrét kiberbiztonsági eseményekkel kapcsolatos eseményértékelési jelentésnek arra kell irányulnia, hogy bekövetkezte után értékelje az esemény okait, hatásait és az azzal kapcsolatos mérséklési intézkedéseket. Különös figyelmet kell fordítani az e rendeletben előírt legmagasabb szintű szakmai feddhetetlenség, pártatlanság és szükséges technikai szakértelem feltételeinek megfelelő irányított biztonsági szolgáltatók által megosztott információkra és tapasztalatokra. A jelentést az EU-CyCLONe-nak, a CSIRT-ek hálózatának és a Bizottságnak kell benyújtani, amelyeknek azt munkájuk során figyelembe kell venniük. Ha az esemény harmadik országgal kapcsolatos, a Bizottságnak meg kell osztania a jelentést a főképviselővel.

(37) Figyelembe véve a kiberbiztonsági támadások kiszámíthatatlan jellegét és azt, hogy azok gyakran nem korlátozódnak egy adott földrajzi területre, és így a tovagyűrűzés magas kockázatát hordozzák magukban, a szomszédos országok rezilienciájának és a jelentős és nagyszabású kiberbiztonsági eseményekre való hatékony reagálási képességüknek a megerősítése hozzájárul az Unió egészének védelméhez. Ezért a Digitális Európa programhoz társult harmadik országok is részesülhetnek az uniós kiberbiztonsági tartalékból nyújtott támogatásban, amennyiben erről a Digitális Európa programban való részvételükről kötött társulási megállapodás rendelkezik. A

társult harmadik országok a vonatkozó partnerségek és finanszírozási eszközök keretében részesülnek az Unió nyújtotta finanszírozásból. A támogatásnak ki kell terjednie a jelentős vagy nagyszabású kiberbiztonsági eseményekre való reagálás és az eseményt követő azonnali helyreállítás területén nyújtott szolgáltatásokra. Az e rendeletben az uniós kiberbiztonsági tartalékra és a megbízható szolgáltatókra vonatkozóan meghatározott feltételeket alkalmazni kell a Digitális Európa programhoz társult harmadik országoknak nyújtott támogatásokra.

(37a) Harmadik országok az e rendelet szerinti erőforrásokhoz és támogatáshoz az uniós kiberbiztonsági tartalékból származó biztonsági eseményekre való reagálási támogatás felhasználásával férhetnek hozzá. Emellett szükség lehet harmadik országokból – többek között a Digitális Európa programhoz társult harmadik országokból vagy más nemzetközi partnerországokból – és NATO-tagoktól származó eseményreagálási szolgáltatókra az uniós kiberbiztonsági tartalékon belüli konkrét szolgáltatások nyújtásához. Az (EU, Euratom) 2018/1046 rendelettől eltérve, az Unió technológiai szuverenitásának, nyitott stratégiai autonómiájának, versenyképességének és rezilienciájának megerősítése, valamint az Unió stratégiai eszközeinek, érdekeinek és biztonságának védelme érdekében az olyan harmadik országokban letelepedett szervezetek számára, amelyek nem részes felei a közbeszerzésről szóló többoldalú megállapodásnak, és amelyeket nem vetettek alá az (EU) 2019/452 európai parlamenti[1] és tanácsi rendelet értelmében vett átvilágításnak, valamint szükség esetén kockázatcsökkentő intézkedéseknek, az e rendeletben meghatározott célkitűzések figyelembevételével nem engedélyezhető a részvétel. E rendelet külső dimenziójának összhangban kell állnia a Digitális Európa program keretében létrejött társulási megállapodásban foglalt rendelkezésekkel. A jogalkotó hatóságok részvételével nyilvános ellenőrzésnek kell alávetni a harmadik országok részvételét annak biztosítása érdekében, hogy a polgárok részt vehessenek a folyamatban.

(38) Ezen rendelet végrehajtása egységes feltételeinek biztosítása érdekében a Bizottságra végrehajtási hatásköröket kell ruházni a következők tekintetében: a határokon átnyúló biztonsági műveleti központok közötti interoperabilitás feltételeinek meghatározása; a potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményekkel kapcsolatos információknak a határokon átnyúló biztonsági műveleti központok és az uniós szervezetek közötti megosztására vonatkozó eljárási szabályok meghatározása; az Európai Kiberpajzs biztonságát garantáló technikai követelmények meghatározása; az uniós kiberbiztonsági tartalékhoz szükséges reagálási szolgáltatások típusainak és számának meghatározása; valamint az uniós kiberbiztonsági tartalék támogatási szolgáltatásainak allokációjára vonatkozó részletes szabályok pontosítása. Ezeket a végrehajtási hatásköröket a 182/2011/EU európai parlamenti és tanácsi rendeletnek megfelelően kell gyakorolni*.

---

* ***Az Európai Parlament és a Tanács 182/2011/EU rendelete (2011. február 16.) a Bizottság végrehajtási hatásköreinek gyakorlására vonatkozó tagállami ellenőrzési***

---

[1] Az Európai Parlament és a Tanács (EU) 2019/452 rendelete (2019. március 19.) az Unióba irányuló közvetlen külföldi befektetések átvilágítási keretének létrehozásáról (HL L 79. I, 2019.3.21., 1. o., ELI:. http://data.europa.eu/eli/reg/2019/452/oj).

mechanizmusok szabályainak és általános elveinek megállapításáról (HL L 55., 2011.2.28., 13. o., ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(38a) Az európai kiberbiztonsági pajzs és a kiberbiztonsági vészhelyzeti mechanizmus hatékony végrehajtásához elengedhetetlen a képzett személyzet, amely képes megbízhatóan, a legmagasabb normáknak megfelelően biztosítani a releváns kiberbiztonsági szolgáltatásokat. Ezért aggályos, hogy az Unió szakemberhiánnyal szembesül, amelyet a képzett szakemberek hiánya jellemez, miközben gyorsan változó fenyegetettségi helyzettel néz szembe, amint azt a Kiberkészségek Akadémiájáról szóló, 2023. április 18-i bizottsági közlemény is elismeri. Fontos áthidalni ezt a szakemberhiányt a különböző érdekelt felek – többek között a magánszektor, a tudományos körök, a tagállamok, a Bizottság és az ENISA – közötti együttműködés és koordináció erősítésével minden területen, az oktatásba és képzésbe való beruházás, a köz- és magánszféra közötti partnerségek fejlesztése, a kutatási és innovációs kezdeményezések támogatása, a közös szabványok kidolgozása és kölcsönös elismerése, valamint a kiberbiztonsági készségek tanúsítása terén, többek között a kiberbiztonsági készségek európai keretrendszerén keresztül. Ez várhatóan megkönnyíti a kiberbiztonsági szakemberek Unión belüli mobilitását is. E rendeletnek a sokszínűbb kiberbiztonsági munkaerő előmozdítására kell irányulnia. A kiberbiztonsági készségek fejlesztését célzó valamennyi intézkedéshez biztosítékokra van szükség az „agyelszívás” és a munkavállalói mobilitást fenyegető kockázat elkerülése érdekében.

(38b) Unió-szerte meg kell erősíteni a speciális, interdiszciplináris és általános készségeket és kompetenciákat, különös tekintettel a nőkre, mivel a kiberbiztonság terén továbbra is fennáll a nemek közötti szakadék, lévén a nők globális átlagos jelenléte 20%. A nőknek jelen kell lenniük és részt kell venniük a digitális jövő és annak irányításának kialakításában.

(38c) A kiberbiztonság területén a kutatás és innováció (K+I) megerősítésének célja az Unió rezilienciájának és nyitott stratégiai autonómiájának növelése. Hasonlóképpen fontos szinergiákat teremteni a kutatási és innovációs programokkal, valamint a meglévő eszközökkel és intézményekkel, továbbá meg kell erősíteni a különböző érdekelt felek – többek között a magánszektor, a civil társadalom, a tudományos körök, a tagállamok, a Bizottság és az ENISA – közötti együttműködést és koordinációt;

(38d) E rendeletnek hozzá kell járulnia a digitális évtizedben érvényre juttatandó digitális jogokról és elvekről szóló európai nyilatkozatban foglalt, a demokráciáink, az emberek, a vállalkozások és a közintézmények érdekeinek kiberbiztonsági kockázatokkal és kiberbűnözéssel, többek között adatvédelmi incidensekkel, valamint személyazonosság-lopással vagy -manipulációval szembeni védelméhez kapcsolódó kötelezettségvállaláshoz. E rendelet alkalmazásának hozzá kell járulnia más – például a mesterséges intelligenciára, az adatvédelemre és az adatok szabályozására vonatkozó – jogszabályok végrehajtásának javításához is a kiberbiztonság és a kiberreziliencia tekintetében.

(38e) E rendelet sikeres végrehajtása szempontjából kulcsfontosságú a kiberbiztonsági kultúra erősítése, amely a biztonságot – beleértve a digitális környezet biztonságát is – a közjavak egyikének tekinti. Ezért a demokráciáink és alapvető értékeink védelmét garantáló további eszközként a polgárok bevonását és tudatosságának növelését célzó intézkedéseket kell kidolgozni.

(38f) E rendelet egyes nem alapvető fontosságú elemeinek kiegészítése érdekében a Bizottságot fel kell hatalmazni arra, hogy az EUMSZ 290. cikkével összhangban jogi aktusokat fogadjon el a határokon átnyúló biztonsági műveleti központok közötti átjárhatóság feltételeinek meghatározása, az egyrészről a határokon átnyúló biztonsági műveleti központok, másrészről az EU-CyCLONe, a CSIRT-ek hálózata és a Bizottság közötti információcserére vonatkozó eljárási szabályok meghatározása, az uniós kiberbiztonsági tartalékhoz szükséges reagálási szolgáltatások típusainak és számának meghatározása, valamint az uniós kiberbiztonsági tartalék támogatási szolgáltatásainak allokációjára vonatkozó részletes szabályok pontosítása céljából. Különösen fontos, hogy a Bizottság előkészítő munkája során megfelelő konzultációkat folytasson, többek között szakértői szinten, és hogy e konzultációkra a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásnak* megfelelően kerüljön sor. Így különösen a felhatalmazáson alapuló jogi aktusok előkészítésében való egyenlő részvétel biztosítása érdekében az Európai Parlament és a Tanács a tagállamok szakértőivel egyidejűleg kap kézhez minden dokumentumot, és szakértőik rendszeresen részt vehetnek a Bizottság felhatalmazáson alapuló jogi aktusok előkészítésével foglalkozó szakértői csoportjainak ülésein.

**** HL L 123., 2016.5.12., 1. o., ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.***

(39) Mivel e rendelet ***céljait, nevezetesen az Unió kiberfenyegetés-megelőzési, -felderítési, -reagálási és -helyreállítási képességeinek megerősítését, valamint a kommunikációs silót megszüntető általános keret létrehozását a tagállamok nem tudják kielégítően megvalósítani, hanem*** azok uniós szinten ***jobban*** megvalósíthatók. Az Unió ezért intézkedéseket fogadhat el az Európai Unióról szóló szerződés 5. cikkében foglalt szubszidiaritási és arányossági elvnek megfelelően. ***Az említett cikkben foglalt arányossági elvnek megfelelően ez*** a rendelet nem lépi túl az e cél eléréséhez szükséges mértéket,

ELFOGADTA EZT A RENDELETET:

I. fejezet

ÁLTALÁNOS CÉLKITŰZÉSEK, TÁRGY ÉS FOGALOMMEGHATÁROZÁSOK

1. cikk

A rendelet tárgya és céljai

(1) Ez a rendelet intézkedéseket állapít meg a kiberbiztonsági fenyegetések és események észlelésére, valamint az azokra való felkészülésre és reagálásra irányuló uniós képességek megerősítésére, különösen a következő intézkedések révén:

a) a biztonsági műveleti központok páneurópai ***hálózatának*** kiépítése (Európai Kiberpajzs) a közös észlelési és helyzetismereti képességek kialakítása és fejlesztése érdekében;

b) kiberbiztonsági vészhelyzeti mechanizmus létrehozása, amely támogatja a tagállamokat a jelentős és nagyszabású kiberbiztonsági eseményekre való felkészülésben, reagálásban és az eseményt követő azonnali helyreállításban;

c) a kiberbiztonsági események európai felülvizsgálati mechanizmusának létrehozása konkrét jelentős vagy nagyszabású kiberbiztonsági események felülvizsgálata és értékelése céljából.

(2) E rendelet célja az uniós szintű szolidaritás megerősítése a következő egyedi célkitűzések révén:

a) ***a kiberfenyegetések és -események közös uniós észlelésének és helyzetismeretének megerősítése, lehetővé téve ezáltal az Unió és a tagállamok ipari kapacitásának támogatását a kiberbiztonsági ágazatban, valamint az uniós ipar, különösen a mikrovállalkozások, a kkv-k – köztük az induló innovatív vállalkozások – és a szolgáltatási ágazatok versenyhelyzetének megerősítése a digitális gazdaságban, valamint hozzájárulás az Unió technológiai szuverenitásához, versenyképességéhez és rezilienciájához az ágazatban, megerősítve a kiberbiztonsági ökoszisztémát az erős uniós képességek biztosítása érdekében, többek között a nemzetközi partnerekkel együttműködésben;***

b) a kritikus és a kiemelten kritikus ágazatokban működő szervezetek felkészültségének megerősítése Unió-szerte, valamint a szolidaritás megerősítése a jelentős vagy nagyszabású kiberbiztonsági eseményekre való közös reagálási kapacitások kialakítása révén, többek között a Digitális Európa programhoz társult harmadik országok számára kiberbiztonsági eseményekre való reagáláshoz nyújtott uniós támogatással;

c) az Unió rezilienciájának fokozása és a hatékony reagáláshoz való hozzájárulás a jelentős vagy nagyszabású kiberbiztonsági események felülvizsgálata és értékelése révén, beleértve a levont tanulságokat és adott esetben az ajánlásokat is.

ca) a munkavállalók készségeinek, know-how-képességeinek és kompetenciáinak összehangolt módon történő fejlesztése a kiberbiztonság biztosítása és a Kiberkészségek Akadémiájával való szinergiák megteremtése érdekében.

(3) E rendelet nem érinti a tagállamoknak a nemzetbiztonsággal, a közbiztonsággal, valamint a bűncselekmények megelőzésével, kivizsgálásával, felderítésével és büntetőeljárás alá vonásával kapcsolatos elsődleges felelősségét.

2. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

(-1a) „nemzeti biztonsági műveleti központ” vagy „nemzeti SOC”: olyan központosított nemzeti kapacitás, amely a 4. cikkel összhangban folyamatosan összegyűjti és elemzi a kiberfenyegetésekkel kapcsolatos hírszerzési információkat, és javítja a kiberbiztonsági helyzetet;

(1) **„határokon átnyúló biztonsági műveleti központ”** *vagy* **„határokon átnyúló SOC”**: olyan több országra kiterjedő platform, amely ***az 5. cikkel összhangban*** összehangolt hálózati struktúrában egyesíti a nemzeti biztonsági műveleti központokat;

(2) „**közjogi szerv**”: a 2014/24/EU európai parlamenti és tanácsi irányelv 2. cikke (1) bekezdésének 4. pontjában meghatározott közjogi ***intézmények***[1];

(3) „**üzemeltetési konzorcium**”: konzorcium, amelyet a nemzeti biztonsági műveleti központok által képviselt részt vevő államok alkotnak, ***amelyet az 5. cikkel összhangban a nemzeti biztonsági műveleti központok képviselnek***;

(4) „szervezet”: az (EU) 2022/2555 irányelv 6. cikkének 38. pontjában meghatározott szervezet;

(4a) „kritikus szervezet”: az (EU) 2022/2557 európai parlamenti és tanácsi irányelv 2. cikkének 1. pontjában meghatározott kritikus szervezet[2].

(5) „**kritikus vagy kiemelten kritikus ágazatokban működő szervezetek**”: az (EU) 2022/2555 irányelv I. és II. mellékletében felsorolt ágazatokban működő szervezetek;

(5a) „biztonsági esemény kezelése”: az (EU) 2022/2555 irányelv 6. cikkének 8. pontjában meghatározott eseménykezelés;

(5b) „kockázat”: az (EU) 2022/2555 rendelet 6. cikkének 9. pontjában meghatározott kockázat;

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

(6a) „jelentős kiberfenyegetés”: az (EU) 2022/2555 irányelv 6. cikkének 11. pontjában meghatározott jelentős kiberfenyegetés;

(7) „jelentős kiberbiztonsági esemény”: az (EU) 2022/2555 irányelv 23. cikkének (3) bekezdésében meghatározott kritériumoknak megfelelő kiberbiztonsági esemény;

(8) „nagyszabású kiberbiztonsági esemény”: az (EU) 2022/2555 irányelv 6. cikkének 7. pontjában meghatározott esemény;

(9) „felkészültség”: egy jelentős vagy nagyszabású kiberbiztonsági eseményre való hatékony és gyors reagálást biztosító, előre meghozott kockázatértékelési és nyomonkövetési intézkedések eredményeként kialakult készenlét és képesség;

(10) „reagálás”: jelentős vagy nagyszabású kiberbiztonsági esemény alkalmával, illetve ilyen esemény során vagy után hozott intézkedés az esemény azonnali és rövid távú káros következményeinek kezelése érdekében;

(10a) „irányított biztonsági szolgáltatásokat nyújtó szolgáltató”: az (EU) 2022/2555 irányelv 6. cikkének 40. pontjában meghatározott irányított szolgáltató;

(11) „**irányított biztonsági szolgáltatásokat nyújtó szolgáltatók**”: e rendelet 16. cikkével összhangban ***az uniós kiberbiztonsági tartalékba való felvételre kiválasztott*** irányított biztonsági szolgáltatásokat nyújtó szolgáltatók.

---

[1] Az Európai Parlament és a Tanács 2014/24/EU irányelve (2014. február 26.) a közbeszerzésről és a 2004/18/EK irányelv hatályon kívül helyezéséről (HL L 94., 2014.3.28., 65. o.).

[2] ***Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről (HL L 333., 2022.12.27., 164. o.,***
ELI: http://data.europa.eu/eli/dir/2022/2557/oj).

II. fejezet

EURÓPAI KIBERPAJZS

3. cikk

Az Európai Kiberpajzs létrehozása

(1) Létre kell hozni a biztonsági műveleti központok ***hálózatát*** (a továbbiakban: „Európai Kiberpajzs”) hogy fejlett képességeket fejlesszenek ki az Unió számára a kiberfenyegetésekkel kapcsolatos adatok észlelésére, elemzésére és feldolgozására, valamint az Unión belüli biztonsági események ***megelőzésére***. A pajzsot az összes nemzeti biztonsági műveleti központ (a továbbiakban: nemzeti SOC) és határokon átnyúló biztonsági műveleti központ (a továbbiakban: határokon átnyúló SOC) alkotja.

Az Európai Kiberpajzsot végrehajtó intézkedéseket a Digitális Európa programból nyújtott finanszírozással kell támogatni, és az (EU) 2021/694 rendelettel és különösen annak 3. egyedi célkitűzésével összhangban kell végrehajtani.

(2) Az Európai Kiberpajzs:

a) a különböző forrásokból származó kiberfenyegetésekre és biztonsági eseményekre vonatkozó adatok összegyűjtése és megosztása a határokon átnyúló SOC-okon keresztül ***és adott esetben információcsere a CSIRT-ek hálózatával;***

b) a legkorszerűbb eszközök, nevezetesen a mesterséges intelligencia és az adatelemzési technológiák alkalmazásával magas színvonalú, hasznosítható információkat és kiberfenyegetettségi információkat állít elő;

c) hozzájárul a fokozott védelemhez és a kiberfenyegetésekre való hatékonyabb reagáláshoz, ***többek között azáltal, hogy konkrét ajánlásokat fogalmaz meg a szervezetek számára***;

d) Unió-szerte hozzájárul a kiberfenyegetések gyorsabb észleléséhez és a helyzetismerethez;

e) szolgáltatásokat és tevékenységeket nyújt az Unió kiberbiztonsági közössége számára, többek között hozzájárul a fejlett mesterséges intelligenciát és adatelemzést szolgáló eszközök ***fejlesztéséhez***.

A pajzsot az (EU) 2021/1173 rendelet alapján létrehozott páneurópai nagy teljesítményű számítástechnikai infrastruktúrával együttműködésben kell kialakítani.

4. cikk

Nemzeti biztonsági műveleti központok

(1) Az Európai Kiberpajzsban való részvétel lehetőségének érdekében minden tagállamnak ki

kell jelölnie legalább egy nemzeti biztonsági műveleti központot. A nemzeti biztonsági műveleti központ egy állami szerv ***központosított kapacitása***. ***Amennyiben lehetséges, a nemzeti SOC-okat be kell építeni a CSIRT-ekbe vagy más meglévő kiberbiztonsági infrastruktúrákba és irányításba.***

Képesnek kell lennie arra, hogy nemzeti szintű referenciapontként és átjáróként szolgáljon más állami és magánszervezetek, ***különösen azok nemzeti SOC-jai*** számára a kiberbiztonsági fenyegetésekre és eseményekre vonatkozó információk gyűjtése és elemzése, ***valamint adott esetben ezen információknak az adott tagállam CSIRT-jei hálózatának tagjaival való megosztása***, és a valamely határokon átnyúló biztonsági műveleti központhoz való hozzájárulás tekintetében. Fel kell szerelni a kiberbiztonsági fenyegetések és események ***megelőzésére***, észlelésére, valamint a kapcsolódó adatok összesítésére és elemzésére alkalmas legkorszerűbb technológiákkal.

A nemzeti biztonsági műveleti központ vagy CSIRT a kritikus fontosságú szervezet számára szolgáltatást nyújtó, irányított biztonsági szolgáltatóktól kérheti a nemzeti kritikus fontosságú szervezeteik telemetriai, szenzor- vagy naplózási adatait. Ezeket az adatokat az uniós adatvédelmi joggal összhangban és kizárólag azzal a céllal kell megosztani, hogy támogassák a nemzeti SOC-ot vagy CSIRT-et a kiberbiztonsági fenyegetések és események felderítésében és megelőzésében.

(2) Az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont (a továbbiakban: „ECCC”) részvételi szándék kifejezésére való felhívás nyomán ***választhatja*** ki azokat a nemzeti biztonsági műveleti központokat, amelyek részt vesznek az ECCC-vel közösen bonyolított eszköz- és infrastruktúra-beszerzésben. Az ECCC támogatást ítélhet oda a kiválasztott nemzeti biztonsági műveleti központoknak az említett eszközök és infrastruktúrák működtetésének finanszírozására. Az uniós pénzügyi hozzájárulás az eszközök és infrastruktúrák beszerzési költségeinek legfeljebb 50 %-át és a működési költségek legfeljebb 50 %-át fedezi, a fennmaradó költségek pedig a tagállamra hárulnak. Az eszközök és infrastruktúrák beszerzésére irányuló eljárás megindítása előtt az ECCC és a nemzeti biztonsági műveleti központ az eszközök és infrastruktúrák használatát szabályozó üzemeltetési és használati megállapodást köt.

(3) A (2) bekezdés szerint kiválasztott nemzeti biztonsági műveleti központ kötelezettséget vállal arra, hogy az eszközök és infrastruktúrák beszerzésétől vagy a támogatás odaítélésétől számított két éven belül – attól függően, hogy melyik következik be előbb – pályázik határokon átnyúló biztonsági műveleti központban való részvételre. Ha egy nemzeti biztonsági műveleti központ a szóban forgó időpontig nem válik valamely határokon átnyúló biztonsági műveleti központ résztvevőjévé, akkor e rendelet alapján nem jogosult további uniós támogatásra.

5. cikk

Határokon átnyúló biztonsági műveleti központok

(1) A nemzeti biztonsági műveleti központok által képviselt, a kiberbiztonsági események észlelését és a fenyegetések nyomon követését célzó tevékenységek összehangolására kötelezettséget vállaló, legalább három tagállamból álló üzemeltetési konzorcium jogosult részt venni a határokon átnyúló biztonsági műveleti központ létrehozására irányuló fellépésekben. ***Valamely határokon átnyúló biztonsági műveleti központot úgy kell kialakítani, hogy észlelje és elemezze a kiberfenyegetéseket, megelőzze az incidenseket és***

támogassa a magas színvonalú hírszerzési információk előállítását, különösen a különböző – köz- és magánforrásokból származó – adatok cseréje, valamint a legkorszerűbb eszközök megosztása, valamint a kiberfelderítési, -elemzési, -megelőzési és -védelmi képességek megbízható és biztonságos környezetben történő közös fejlesztése révén.

(2) Az ECCC részvételi szándék kifejezésére való felhívás nyomán választhatja ki azt az üzemeltetési konzorciumot, amely részt vesz az ECCC-vel közösen bonyolított eszköz- és infrastruktúra-beszerzésben. Az ECCC támogatást ítélhet oda az üzemeltetési konzorciumnak az említett eszközök és infrastruktúrák működtetésének finanszírozására. Az uniós pénzügyi hozzájárulás az eszközök és infrastruktúrák beszerzési költségeinek legfeljebb 75 %-át és a működési költségek legfeljebb 50 %-át fedezi, a fennmaradó költségek pedig az üzemeltetési konzorciumra hárulnak. Az eszközök és infrastruktúrák beszerzésére irányuló eljárás megindítása előtt az ECCC és az üzemeltetési konzorcium az eszközök és infrastruktúrák használatát szabályozó üzemeltetési és használati megállapodást köt.

(2a) Az (EU, Euratom) 2018/1046 rendelet 176. cikkétől eltérve azok a harmadik országokban letelepedett szervezetek, amelyek nem részes felei a közbeszerzésről szóló megállapodásnak, nem vehetnek részt az eszközök és infrastruktúrák közös beszerzésében.

(3) Az üzemeltetési konzorcium tagjai írásos konzorciumi megállapodást kötnek, amely meghatározza az üzemeltetési és használati megállapodás végrehajtásának belső szabályait.

(4) A határokon átnyúló biztonsági műveleti központot jogi szempontból a koordináló biztonsági műveleti központként eljáró nemzeti biztonsági műveleti központ, vagy ha jogi személyiséggel rendelkezik, az üzemeltetési konzorcium képviseli. A koordináló biztonsági műveleti központ felel az üzemeltetési és használati megállapodásban, valamint az e rendeletben foglalt követelmények teljesítéséért.

6. cikk

Együttműködés és információmegosztás a *határokon átnyúló* SOC-okon belül és azok között

(1) Az üzemeltetési konzorcium tagjai a határokon átnyúló biztonsági műveleti központ keretében folytatják egymás között a releváns információk cseréjét, beleértve a kiberfenyegetésekre, a majdnem bekövetkezett eseményekre, a sebezhetőségekre, a technikákra és eljárásokra, a fertőzöttségi mutatókra, az ellenséges taktikákra vonatkozó információkat, az elkövetővel kapcsolatos információkat, a kiberbiztonsági figyelmeztetéseket, valamint a kibertámadások észlelésére szolgáló biztonságieszköz-konfigurációkra vonatkozó ajánlásokat, amennyiben az említett információmegosztás:

a) ***javítja a kiberfenyegetésekkel kapcsolatos hírszerzési információk cseréjét a nemzeti és határokon átnyúló SOC-k és az ágazati ISAC-ok között a fenyegetések megelőzése, felderítése vagy mérséklése céljából;***

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 sebezhetőség 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) Az 5. cikk (3) bekezdésében említett írásbeli konzorciumi megállapodásban meg kell határozni a következőket:

a) az (1) bekezdésben említett jelentős ▌ adatok megosztására vonatkozó kötelezettségvállalás, valamint a szóban forgó információcsere feltételei;

b) irányítási keret, amely minden résztvevőt az információk megosztására ösztönöz;

c) célértékek a fejlett mesterséges intelligenciát és adatelemzést szolgáló eszközök fejlesztéséhez való hozzájárulás tekintetében.

(3) A határokon átnyúló biztonsági műveleti központok ***közötti és az ágazati információmegosztó és -elemző központokkal*** folytatott információcsere ösztönzése érdekében a határokon átnyúló biztonsági műveleti központoknak magas szintű interoperabilitást kell biztosítaniuk egymás között ***és – amennyiben lehetséges – az ágazati információmegosztó és -elemző központokkal.*** A határokon átnyúló biztonsági műveleti központok ***és az ágazati információmegosztó és -elemző központok*** közötti interoperabilitás megkönnyítése érdekében ***az információmegosztási szabványok és protokollok harmonizálhatók a nemzetközi szabványokkal és az ágazat bevált gyakorlataival. Ösztönözni kell a kiberinfrastruktúrák, -szolgáltatások és -eszközök közös beszerzését is. Ezenkívül*** az ECCC-vel és az ENISA-val folytatott konzultációt követően ***a Bizottság ...[e rendelet hatálybalépésétől számított hat hónap]-ig felhatalmazást kap a 20a. cikknek megfelelően felhatalmazáson alapuló jogi aktusok elfogadására e rendelet kiegészítése céljából, a szóban forgó interoperabilitás feltételeinek meghatározásával a határokon átnyúló biztonsági műveleti központokkal szoros együttműködésben, valamint a nemzetközi szabványok és az ágazati bevált gyakorlatok alapján.***

(4) A határokon átnyúló biztonsági műveleti központok együttműködési megállapodásokat kötnek egymással, ***és adott esetben az ágazati információmegosztó és -elemző központokkal***, amelyekben meghatározzák a határokon átnyúló platformok közötti információmegosztás ***és interoperabilitás*** elveit, ***figyelembe véve az (EU) 2022/2555 irányelv szerinti, már meglévő releváns információmegosztási mechanizmusokat. Adott esetben a határokon átnyúló biztonsági műveleti központok együttműködési megállapodásokat kötnek az ágazati információmegosztó és -elemző központokkal. A lehetséges vagy folyamatban lévő nagyszabású kiberbiztonsági incidensekkel összefüggésben az információmegosztási mechanizmusoknak meg kell felelniük az (EU) 2022/2555 irányelv vonatkozó rendelkezéseinek.***

7. cikk

Együttműködés és információmegosztás a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT) hálózatával

(1) Ha a határokon átnyúló biztonsági műveleti központok ***megosztott helyzetfelismerés céljából*** információkhoz jutnak egy potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményről, ***a koordinációt végző biztonsági műveleti központ*** a releváns információkat az (EU) 2022/2555 irányelv szerinti válságkezelési szerepük ***és eljárásaik*** figyelembevételével indokolatlan késedelem nélkül eljuttatja ***saját CSIRT-jének vagy illetékes hatóságának***, ***amelyek erről jelentést tesznek*** az EU-CyCLONe-nak, a CSIRT-ek hálózatának, a Bizottságnak ***és az ENISA-nak. Ez a bekezdés nem ró további kötelezettségeket a köz- vagy magánjogi szervezetekre arra vonatkozóan, hogy az (EU) 2022/2555 irányelvben meghatározott kötelezettségek teljesítése érdekében közöljenek egy potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményt.***

(2) A Bizottság ***felhatalmazást kap arra, hogy a CSIRT-hálózattal folytatott konzultációt követően a 20a. cikknek megfelelően felhatalmazáson alapuló*** jogi aktusokat ***fogadjon el abból a célból, hogy az e cikk*** (1) bekezdésében előírt információmegosztásra vonatkozó eljárási szabályok ***meghatározása révén és az (EU) 2022/2555 irányelvvel összhangban kiegészítse ezt a rendeletet***.

8. cikk

Biztonság

(1) Az Európai Kiberpajzsban részt vevő tagállamok gondoskodnak az Európai Kiberpajzs infrastruktúrájának magas szintű ***titkosságáról***, adatbiztonságáról és fizikai biztonságáról, biztosítják, hogy az infrastruktúrát megfelelő irányítás és ellenőrzés révén megvédjék a fenyegetésektől, továbbá biztosítják az infrastruktúra és a rendszerek – többek között az infrastruktúrán keresztül kicserélt adatok – biztonságát is.

(2) Az Európai Kiberpajzsban részt vevő tagállamok gondoskodnak arról, hogy az Európai Kiberpajzs keretében nem tagállami közjogi szerveknek minősülő szervezetekkel folytatott információmegosztás ne érintse hátrányosan az Unió biztonsági érdekeit.

(3) A Bizottság végrehajtási jogi aktusokat fogadhat el, amelyekben technikai követelményeket állapít meg a tagállamok számára az (1) és (2) bekezdés szerinti kötelezettségeik teljesítéséhez. Ezeket a végrehajtási jogi aktusokat az e rendelet 21. cikkének (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni. ***Meg kell felelniük az (EU) 2022/2555 és az (EU) 2022/2557 irányelvnek.*** A Bizottság ***végrehajtási jogi aktusaiban*** – a főképviselő támogatásával –a katonai szereplőkkel való együttműködés megkönnyítése érdekében figyelembe veszi a vonatkozó védelmi szintű biztonsági előírásokat.

III. fejezet

KIBERBIZTONSÁGI VÉSZHELYZETI MECHANIZMUS

9. cikk

A *kiberbiztonsági* vészhelyzeti mechanizmus létrehozása

(1) Létrejön a ***kiberbiztonsági*** vészhelyzeti mechanizmus, amelynek célja az Unió súlyos kiberbiztonsági fenyegetésekkel szembeni rezilienciájának javítása, valamint a szolidaritás szellemében a jelentős és nagyszabású kiberbiztonsági események rövid távú hatásaira való felkészülés és e hatások enyhítése (a továbbiakban: mechanizmus).

(2) A ▌ mechanizmust végrehajtó intézkedéseket a Digitális Európa programból nyújtott finanszírozással kell támogatni, és az (EU) 2021/694 rendelettel és különösen annak 3. egyedi célkitűzésével összhangban kell végrehajtani.

10. cikk

Intézkedéstípusok

(1) A mechanizmus a következő intézkedéstípusokat támogatja:

a) felkészültségi intézkedések, amelyek magukban foglalják a kiemelten kritikus ágazatokban működő szervezetek Unió-szerte összehangolt felkészültségi tesztelését;

b) a jelentős és nagyszabású kiberbiztonsági eseményekre való reagálást és az eseményt követő azonnali helyreállítást támogató reagálási intézkedések, amelyeket a 12. cikk alapján létrehozott uniós kiberbiztonsági tartalékban részt vevő, ***irányított biztonsági szolgáltatásokat*** nyújtó, megbízható szolgáltatók biztosítanak;

c) kölcsönös segítségnyújtási intézkedések, amelyek magukban foglalják az egyik tagállam nemzeti hatóságai által egy másik tagállamnak nyújtott segítséget, különösen az (EU) 2022/2555 irányelv 11. cikke (3) bekezdésének f) pontjában előírtak szerint.

(1a) A mechanizmus elindítását követően a Bizottság évente értékeli azt, és közzétesz egy a mechanizmus pozitív és negatív hatásáról szóló jelentést, beleértve azt is, hogy szükség van-e további együttműködési vagy képzési követelményekre.

11. cikk

A szervezetek összehangolt felkészültségi tesztelése

(1) A szervezetek 10. cikk (1) bekezdésének a) pontjában említett összehangolt felkészültségi tesztelésének Unió-szerte történő támogatása céljából a Bizottság a Kiberbiztonsági Együttműködési Csoporttal és az ENISA-val folytatott konzultációt követően azonosítja az (EU) 2022/2555 irányelv I. mellékletében felsorolt kiemelten kritikus ágazatokon belüli érintett ágazatokat vagy alágazatokat, amelyek szervezetei a meglévő és tervezett összehangolt kockázatértékelések és rezilienciatesztek figyelembevételével ***az (EU) 2022/2555 irányelv I. mellékletében felsorolt, a kiemelten kritikus ágazatokhoz tartozó szervezetekre vonatkozóan megállapított szabályokkal összhangban*** felkészültségi tesztelés alá vonhatók.

(2) A Kiberbiztonsági Együttműködési Csoport a Bizottsággal, az ENISA-val, a főképviselővel, ***valamint az (1) bekezdés szerinti koordinált felkészültségi tesztelésnek alávetett szervezetekkel*** együttműködve közös kockázati forgatókönyveket és módszereket dolgoz ki az összehangolt ***felkészültségi*** tesztelési gyakorlatokhoz, ***amelyek összehangolt munkatervvel zárulnak. Az összehangolt felkészültségi tesztelésnek alávetett szervezetek korrekciós tervet dolgoznak ki és hajtanak végre, amely végrehajtja a felkészültségi tesztekből származó ajánlásokat.***

A Kiberbiztonsági Együttműködési Csoport tájékoztatást nyújthat az ágazatoknak vagy alágazatoknak az összehangolt felkészültségi tesztelési gyakorlatok során történő rangsorolásához.

12. cikk

Az uniós kiberbiztonsági tartalék létrehozása

(1) Létre kell hozni az uniós kiberbiztonsági tartalékot annak érdekében, hogy jelentős vagy nagyszabású kiberbiztonsági események alkalmával a (3) bekezdésben említett felhasználók segítséget kapjanak a reagáláshoz vagy a reagálás támogatásához, valamint az ilyen eseményeket követő azonnali helyreállításhoz.

Amennyiben nyilvánvaló, hogy a beszerzett szolgáltatásokat nem lehet teljes mértékben

felhasználni jelentős vagy nagy horderejű eseményekre való reagáláshoz nyújtott támogatás céljára, e szolgáltatásokat kivételes esetben az ajánlatkérő szerv átalakíthatja az események kezelésére szolgáló gyakorlatokká vagy képzésekké, és kérésre a felhasználók rendelkezésére bocsáthatja azokat.

(2) Az uniós kiberbiztonsági tartalék a 16. cikkben meghatározott kritériumoknak megfelelően kiválasztott, ***irányított biztonsági szolgáltatásokat*** nyújtó, megbízható szolgáltatók eseményreagálási szolgáltatásaiból áll össze. Az ***uniós kiberbiztonsági tartalék*** előzetes kötelezettségvállalás keretében rendelkezésre bocsátott szolgáltatásokat tartalmaz. A szolgáltatásoknak valamennyi tagállamban igénybe vehetőnek kell lenniük, ***és meg kell erősíteniük az Unió technológiai szuverenitását, nyitott stratégiai autonómiáját, versenyképességét és rezilienciáját a kiberbiztonsági ágazatban, többek között azáltal, hogy Unió-szerte fellendítik az innovációt a digitális egységes piacon.***

(3) Az uniós kiberbiztonsági tartalék szolgáltatásainak felhasználói közé a következők tartoznak:

a) az (EU) 2022/2555 irányelv 9. cikkének (1) és (2) bekezdésében említett, kiberválságok kezelésével foglalkozó tagállami hatóságok és az említett irányelv 10. cikkében említett CSIRT-ek;

b) Az ***(EU).../2023 európai parlamenti és tanácsi rendelet[1] 3. cikkének (1) bekezdésében említett uniós intézmények, szervek és ügynökségek és a CERT-EU***.

(4) A (3) bekezdés a) pontjában említett felhasználóknak az uniós kiberbiztonsági tartalék szolgáltatásait kell igénybe venniük a kritikus vagy kiemelten kritikus ágazatokban működő szervezeteket érintő jelentős vagy nagyszabású biztonsági eseményekre való reagáláshoz vagy a reagálás támogatásához, valamint az ilyen eseményeket követő azonnali helyreállításhoz.

(5) A Bizottság általános felelősséggel tartozik az uniós kiberbiztonsági tartalék végrehajtásáért. A Bizottság ***a NIS 2 koordinációs csoporttal egyeztetve és*** a (3) bekezdésben említett felhasználók igényeivel összhangban határozza meg az uniós kiberbiztonsági tartalék prioritásait és alakulását, továbbá felügyeli annak végrehajtását, és biztosítja az e rendelet szerinti egyéb támogatási intézkedésekkel, valamint az egyéb uniós intézkedésekkel és programokkal való kiegészítő jelleget, következetességet, szinergiákat és kapcsolatokat.

(6) A Bizottság hozzájárulási megállapodások révén részben vagy egészben megbízza az ENISA-t az uniós kiberbiztonsági tartalék működtetésével és igazgatásával.

(7) Annak érdekében, hogy támogassa a Bizottságot az uniós kiberbiztonsági tartalék létrehozásában, az ENISA – a tagállamokkal és a Bizottsággal, ***valamint adott esetben az irányított biztonsági szolgáltatókkal és a kiberbiztonsági ágazat egyéb képviselőivel*** folytatott konzultációt követően – feltérképezi a szükséges szolgáltatásokat, ***beleértve a kiberbiztonsági munkaerő szükséges készségeit és kapacitását.*** Az ENISA a Bizottsággal, ***az irányított biztonsági szolgáltatókkal és adott esetben a kiberbiztonsági ágazat egyéb képviselőivel*** folytatott konzultációt követően hasonló feltérképezést készít az uniós kiberbiztonsági tartalék keretében a 17. cikk alapján támogatásra jogosult harmadik országok szükségleteinek azonosítása érdekében. A Bizottság adott esetben konzultál a főképviselővel, ***és tájékoztatja a Tanácsot a harmadik országok szükségleteiről.***

---

[1] ***(EU).../2023 rendelet az uniós intézmények, szervek, hivatalok és ügynökségek egységesen magas szintű kiberbiztonságát biztosító intézkedések meghatározásáról (HL C, 2023. o., ELI: ...).***

(8) A Bizottság ***felhatalmazást kap arra, hogy a 20a. cikknek megfelelően felhatalmazáson alapuló jogi aktusokat fogadjon el abból a célból, hogy kiegészítse ezt a rendeletet*** az uniós kiberbiztonsági tartalékhoz szükséges reagálási szolgáltatások típusainak és számának ***meghatározása révén***. ▌..

13. cikk

Az uniós kiberbiztonsági tartalékból nyújtott támogatás iránti kérelmek

(1) A 12. cikk (3) bekezdésében említett felhasználók szolgáltatásokat kérhetnek az uniós kiberbiztonsági tartalékból a jelentős vagy nagyszabású kiberbiztonsági eseményekre való reagálás és az eseményt követő azonnali helyreállítás támogatása érdekében.

(2) Ahhoz, hogy a 12. cikk (3) bekezdésében említett felhasználók támogatást – beleértve a közvetlen technikai segítségnyújtást és az eseményre való reagálást, valamint az eseményt követő azonnali helyreállítási erőfeszítéseket segítő egyéb erőforrásokat – kapjanak az uniós kiberbiztonsági tartalékból, intézkedéseket kell hozniuk annak érdekében, hogy enyhítsék a támogatás iránti kérelem tárgyát képező esemény hatásait.

(3) Az e rendelet 12. cikke (3) bekezdésének a) pontjában említett felhasználók támogatás iránti kérelmeit a tagállam által az (EU) 2022/2555 irányelv 8. cikkének (3) bekezdésével összhangban kijelölt vagy létrehozott egyedüli kapcsolattartó ponton keresztül kell továbbítani a Bizottságnak és az ENISA-nak.

(4) A tagállamok tájékoztatják a CSIRT-ek hálózatát és adott esetben az EU-CyCLONe-t az e cikk szerinti, kiberbiztonsági eseményekre való reagáláshoz és azonnali helyreállításhoz támogatást igénylő kérelmeikről.

(5) A kiberbiztonsági eseményekre való reagáláshoz és azonnali helyreállításhoz támogatást igénylő kérelmek a következőket tartalmazzák:

a) megfelelő információk az érintett szervezetről és a kiberbiztonsági esemény lehetséges hatásairól, valamint a kért támogatás tervezett felhasználásáról, beleértve a becsült szükségletek megjelölését is;

b) a (2) bekezdésben említett, a támogatás iránti kérelem tárgyát képező esemény hatásainak enyhítése érdekében hozott intézkedésekre vonatkozó információk;

c) az érintett szervezet rendelkezésére álló egyéb támogatási formákra vonatkozó információk, beleértve az eseményreagálási és az azonnali helyreállítási szolgáltatásokra vonatkozó szerződéses megállapodásokat, valamint az ilyen típusú kiberbiztonsági eseményekre potenciálisan kiterjedő biztosítási szerződéseket.

(6) Az ENISA a Bizottsággal és a Kiberbiztonsági Együttműködési Csoporttal együttműködve sablont dolgoz ki az uniós kiberbiztonsági tartalékból nyújtott támogatás iránti kérelmek benyújtásának megkönnyítésére.

(7) A Bizottság ***felhatalmazást kap arra, hogy a 20a. cikknek megfelelően felhatalmazáson alapuló jogi aktusokat fogadjon el abból a célból, hogy kiegészítse ezt a rendeletet azáltal,*** hogy részletesebben ***meghatározza*** az uniós kiberbiztonsági tartalékot támogató szolgáltatások elosztására vonatkozó részletes szabályokat. ▌

14. cikk

Az uniós kiberbiztonsági tartalékból nyújtott támogatás végrehajtása

(1) Az uniós kiberbiztonsági tartalékból nyújtott támogatás iránti kérelmeket a Bizottság az ENISA közreműködésével vagy a 12. cikk (6) bekezdése szerinti hozzájárulási megállapodásokban meghatározottak szerint értékeli, és a választ ***indokolatlan késedelem nélkül, de legkésőbb 24 órán belül*** továbbítja a 12. cikk (3) bekezdésében említett felhasználóknak.

(2) Több párhuzamos megkeresés esetén a kérelmek rangsorolásához adott esetben a következő kritériumokat kell figyelembe venni:

a) a kiberbiztonsági esemény súlyossága;

b) az érintett szervezet típusa, e tekintetben nagyobb prioritást élveznek az (EU) 2022/2555 irányelv 3. cikkének (1) bekezdésében meghatározott alapvető szervezeteket érintő kiberbiztonsági események;

c) az érintett tagállam(ok)ra vagy felhasználókra gyakorolt lehetséges hatás;

d) a kiberbiztonsági esemény ***kiterjedése***, lehetséges határokon átnyúló jellege és annak kockázata, hogy tovagyűrűzhet más tagállamokra vagy felhasználókra;

e) a felhasználó által a reagálás elősegítése érdekében hozott intézkedések és az azonnali helyreállítási erőfeszítések a 13. cikk (2) bekezdésében és a 13. cikk (5) bekezdésének b) pontjában említettek szerint.

(3) Az uniós kiberbiztonsági tartalék szolgáltatásait a szolgáltató és az uniós kiberbiztonsági tartalékból támogatásban részesülő felhasználó közötti egyedi megállapodásokkal összhangban kell nyújtani. E megállapodásoknak tartalmazniuk kell felelősségre vonatkozó feltételeket is ***és a megállapodásban részes felek által az adott szolgáltatás nyújtásához szükségesnek ítélt egyéb rendelkezéseket.***

(4) A (3) bekezdésben említett megállapodásoknak az ENISA által a tagállamokkal ***és adott esetben az uniós kiberbiztonsági tartalék egyéb felhasználóival*** folytatott konzultációt követően készített sablonokon ***kell*** alapulniuk.

(5) A Bizottság és az ENISA nem visel szerződéses felelősséget az uniós kiberbiztonsági tartalék végrehajtása keretében nyújtott szolgáltatások nyomán harmadik feleknek okozott károkért, ***kivéve a szolgáltató alkalmazásának értékelése során elkövetett súlyos gondatlanság eseteit, vagy ha a Bizottság vagy az ENISA a 14. cikk (3) bekezdése szerint az uniós kiberbiztonsági tartalék felhasználói.***

(6) A támogatási intézkedés befejezését követő egy hónapon belül a felhasználók összefoglaló jelentést nyújtanak be a Bizottságnak, az ENISA-nak, ***a CSIRT-ek hálózatának és adott esetben az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatának*** a nyújtott szolgáltatásról, az elért eredményekről és a levont tanulságokról. Amennyiben a felhasználó a 17. cikkben meghatározott harmadik országból származik, a szóban forgó jelentést meg kell osztani a főképviselővel.
A jelentésnek tiszteletben kell tartania az érzékeny vagy minősített adatok védelmére vonatkozó uniós és nemzeti jogszabályokat.

(7) A Bizottság ***rendszeresen és évente legalább kétszer*** jelentést tesz a Kiberbiztonsági Együttműködési Csoportnak a támogatás felhasználásáról és eredményeiről. ***Az érzékeny vagy minősített adatok védelmére vonatkozó uniós és nemzeti jogszabályokkal összhangban védenie kell a bizalmas információkat.***

15. cikk

Koordináció a válságkezelési mechanizmusokkal

(1) Azokban az esetekben, amikor a jelentős vagy nagyszabású kiberbiztonsági események az 1313/2013/EU határozatban[1] meghatározott katasztrófák nyomán alakulnak ki, vagy ilyen katasztrófát okoznak, az ilyen eseményekre való reagáláshoz az e rendelet alapján nyújtott támogatásnak azok sérelme nélkül ki kell egészítenie az 1313/2013/EU határozat szerinti intézkedéseket.

(2) Ha olyan nagyszabású, határokon átnyúló kiberbiztonsági esemény következik be, amely kiváltja az uniós politikai szintű integrált válságelhárítási mechanizmus (a továbbiakban: IPCR-mechanizmus) alkalmazását, a kiberbiztonsági eseményhez való reagáláshoz az e rendelet szerint nyújtott támogatást az IPCR-mechanizmus szerinti vonatkozó protokollokkal és eljárásokkal összhangban kell kezelni.

(3) A főképviselővel folytatott konzultáció alapján a ***kiberbiztonsági*** vészhelyzeti mechanizmus keretében nyújtott támogatás kiegészítheti a közös kül- és biztonságpolitika, valamint a közös biztonság- és védelempolitika keretében – többek között a kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok révén – nyújtott segítséget. Kiegészítheti továbbá az egyik tagállam által egy másik tagállamnak az ***EUMSZ*** 42. cikkének (7) bekezdésével összefüggésben nyújtott segítséget, vagy hozzájárulhat ahhoz.

(4) A ***kiberbiztonsági*** vészhelyzeti mechanizmus keretében nyújtott támogatás az EUMSZ 222. cikkében említett helyzetekben az Unió és a tagállamok közötti közös reagálás részét képezheti.

16. cikk

Megbízható szolgáltatók

(1) Az uniós kiberbiztonsági tartalék létrehozását célzó közbeszerzési eljárások során az ajánlatkérő szerv az (EU, Euratom) 2018/1046 rendeletben meghatározott elvekkel és a következő elvekkel összhangban jár el:

a) biztosítja, hogy az uniós kiberbiztonsági tartalék olyan szolgáltatásokat foglaljon magában, amelyek valamennyi tagállamban igénybe vehetők, figyelembe véve különösen az ilyen szolgáltatások nyújtására vonatkozó nemzeti követelményeket, beleértve a tanúsítást, illetve az akkreditációt is;

b) biztosítja az Unió és tagállamai alapvető biztonsági érdekeinek védelmét;

c) biztosítja, hogy az uniós kiberbiztonsági tartalék uniós hozzáadott értéket képviseljen azáltal, hogy hozzájárul az (EU) 2021/694 rendelet 3. cikkében meghatározott célkitűzésekhez, így többek között előmozdítsa a kiberbiztonsági készségek fejlesztését az EU-ban, ***valamint a nemek közötti egyensúly elérését az ágazatban, és megerősítve az Unió technológiai szuverenitását, nyitott stratégiai autonómiáját, versenyképességét és rezilienciáját.***

(2) Az uniós kiberbiztonsági tartalékhoz kapcsolódó szolgáltatások beszerzése során az ajánlatkérő szervnek a következő kiválasztási szempontokat kell belefoglalnia a közbeszerzési dokumentumokba:

[1] Az Európai Parlament és a Tanács 1313/2013/EU határozata (2013. december 17.) az uniós polgári védelmi mechanizmusról (HL L 347., 2013.12.20., 924. o.).

a) a szolgáltatónak bizonyítania kell, hogy személyzete a saját területén a legmagasabb szintű szakmai feddhetetlenséggel, függetlenséggel, felelősséggel és a tevékenységek elvégzéséhez szükséges műszaki szakértelemmel rendelkezik, továbbá biztosítania kell a szakértelem állandóságát/folytonosságát, valamint a szükséges technikai erőforrásokat;

b) a szolgáltatónak, leányvállalatainak és alvállalkozóinak olyan kerettel kell rendelkezniük, amely védi a szolgáltatással kapcsolatos érzékeny információkat, különösen a bizonyítékokat, a megállapításokat és a jelentéseket, és megfelel az EU-minősített adatok védelmére vonatkozó uniós biztonsági szabályoknak;

c) a szolgáltatónak elegendő bizonyítékot kell szolgáltatnia arra vonatkozóan, hogy irányítási struktúrája átlátható, és valószínűleg nem veszélyezteti pártatlanságát és szolgáltatásai minőségét, illetve nem okoz összeférhetetlenséget;

d) a szolgáltatónak megfelelő biztonsági tanúsítvánnyal kell rendelkeznie, legalább azon személyek tekintetében, akiket a szolgáltatásnyújtásban alkalmazni kíván;

e) a szolgáltatónak megfelelő biztonsági szintű informatikai rendszerekkel kell rendelkeznie;

f) a szolgáltatónak rendelkeznie kell a kért szolgáltatás támogatásához szükséges ***naprakész*** hardver- és szoftvertechnikai berendezésekkel, ***és adott esetben meg kell felelnie az (EU).../... európai parlamenti és tanácsi rendeletnek[1] (2022/0272(COD))***

g) a szolgáltatónak bizonyítékot kell szolgáltatnia arra vonatkozóan, hogy tapasztalattal rendelkezik az érintett nemzeti hatóságoknak, illetve a kritikus vagy kiemelten kritikus ágazatokban működő szervezeteknek nyújtott hasonló szolgáltatások terén;

h) a szolgáltatónak képesnek kell lennie arra, hogy a szolgáltatást rövid időn belül nyújtsa abban a tagállamban, illetve azokban a tagállamokban, ahol a szolgáltatást biztosítani tudja;

i) a szolgáltatónak képesnek kell lennie arra, hogy a szolgáltatást azon tagállam(ok) helyi nyelvén – ***vagy az uniós intézmények valamelyik munkanyelvén*** – nyújtsa, ahol a szolgáltatást nyújtani tudja;

j) amint életbe lép az (EU) 2019/881 rendelet ***szerinti***, irányított biztonsági szolgáltatásokra vonatkozó ***európai kiberbiztonsági*** tanúsítási rendszer, a szolgáltatónak ***a rendszer elfogadásától számított két éven belül*** az említett rendszerrel összhangban tanúsítást kell szereznie.

ja) a szolgáltatónak képesnek kell lennie arra, hogy a szolgáltatást önállóan, nem pedig csomag részeként nyújtsa, ezáltal biztosítva a felhasználó azon lehetőségét, hogy másik szolgáltatóra váltson;

jb) a 12. cikk (1) bekezdésének alkalmazásában a szolgáltató a pályázati ajánlatba belefoglalja a fel nem használt eseményreagálási szolgáltatások gyakorlatokká vagy képzésekké való átalakításának lehetőségét;

jc) a szolgáltatónak az Unióban, társult országban vagy a Kereskedelmi Világszervezet keretében a közbeszerzésről szóló megállapodás (GPA) részét képező harmadik országban kell letelepednie és ügyvezetési struktúráival rendelkeznie.

---

[1] Az Európai Parlament és a Tanács (EU) […] rendelete [...] (HL L..., ELI: …).

jd) a szolgáltató nem tartozhat olyan nem társult harmadik ország vagy nem társult harmadik országbeli szervezet ellenőrzése alá, amely nem részes fele a GPA-nak, vagy – alternatív megoldásként – az (EU) 2019/452 rendelet szerinti átvilágítás és szükség esetén mérséklési intézkedések hatálya alá tartozik, figyelembe véve az e rendeletben meghatározott célkitűzéseket.

17. cikk

Harmadik országoknak nyújtott támogatás

(1) Az uniós kiberbiztonsági tartalék nyújtotta támogatást harmadik országok is kérelmezhetik, ha a velük kötött társulási megállapodás a Digitális Európa programban való részvételükről ekképpen rendelkezik.

(2) Az uniós kiberbiztonsági tartalékból nyújtott támogatásnak összhangban kell lennie e rendelettel, és meg kell felelnie az (1) bekezdésben említett társulási megállapodásokban meghatározott bármely egyedi feltételnek.

(3) Az uniós kiberbiztonsági tartalék szolgáltatásainak igénybevételére jogosult társult harmadik országbeli felhasználók közé tartoznak az illetékes hatóságok, így például a CSIRT-ek és a kiberválságok kezelésével foglalkozó hatóságok.

(4) Az uniós kiberbiztonsági tartalékból támogatásra jogosult minden egyes harmadik ország kijelöl egy hatóságot, amely e rendelet alkalmazásában egyedüli kapcsolattartó pontként jár el.

(5) Mielőtt a harmadik országok bármilyen támogatást kapnának az uniós kiberbiztonsági tartalékból, tájékoztatják a Bizottságot és a főképviselőt kiberreziliencia- és kockázatkezelési képességeikről, beleértve legalább a jelentős vagy nagyszabású kiberbiztonsági eseményekre való felkészülés érdekében hozott nemzeti intézkedésekre vonatkozó információkat, valamint a felelős nemzeti szervezetekre – köztük a CSIRT-ekre vagy azokkal egyenértékű szervezetekre –, azok képességeire és a hozzájuk rendelt erőforrásokra vonatkozó információkat. Amennyiben e rendelet 13. és 14. cikkének rendelkezései a tagállamokra hivatkoznak, azok az (1) bekezdésben meghatározott harmadik országokra is alkalmazandók.

(6) A Bizottság ***indokolatlan késedelem nélkül értesíti a Tanácsot,*** és egyeztet a főképviselővel a beérkezett kérelmekről és az uniós kiberbiztonsági tartalékból harmadik országoknak nyújtott támogatás végrehajtásáról.

IV. fejezet

A KIBERBIZTONSÁGI ESEMÉNYEK FELÜLVIZSGÁLATI MECHANIZMUSA

18. cikk

A kiberbiztonsági események felülvizsgálati mechanizmusa

(1) A Bizottság, az EU-CyCLONe vagy a CSIRT-ek hálózatának kérésére az ENISA felülvizsgálja és értékeli az egy adott jelentős vagy nagyszabású kiberbiztonsági eseményhez kapcsolódó fenyegetéseket, sebezhetőségeket és mérséklési intézkedéseket. Egy adott kiberbiztonsági esemény felülvizsgálatának és értékelésének lezárultával az ENISA eseményértékelési jelentést nyújt be a CSIRT-ek hálózatának, az EU-CyCLONe-nak és a Bizottságnak, hogy támogassa őket – különösen az (EU) 2022/2555 irányelv 15. és 16.

cikkében foglalt – feladataik ellátásában. A Bizottság adott esetben megosztja a jelentést a főképviselővel.

(2) Az (1) bekezdésben említett eseményértékelési jelentés elkészítése érdekében az ENISA együttműködik valamennyi érdekelt féllel ***és visszajelzést gyűjt azoktól,*** beleértve a tagállamok, a Bizottság és más érintett uniós intézmények, szervek, ***hivatalok*** és ügynökségek, valamint ***a nemzeti és a határokon átnyúló biztonsági műveleti központokon belüli*** irányított biztonsági szolgáltatók képviselőit és a kiberbiztonsági szolgáltatások felhasználóit, ***kiegészítve olyan garanciákkal és nyomon követéssel, amelyek megfelelőek annak biztosításához, hogy a kiberbiztonsági szolgáltatási ágazat szereplői támogassák a levont tanulságokat és az azonosított legjobb gyakorlatokat.*** Az ENISA adott esetben együttműködik a jelentős vagy nagyszabású kiberbiztonsági események által érintett szervezetekkel is. Az eseményértékelés alátámasztása érdekében az ENISA más típusú érdekelt felekkel is konzultálhat. A konzultációba bevont képviselőknek jelezniük kell bármilyen esetleges összeférhetetlenséget.

(3) A jelentésnek ki kell terjednie az adott jelentős vagy nagyszabású kiberbiztonsági esemény felülvizsgálatára és elemzésére, beleértve a fő okokat, a sebezhetőségeket és a levont tanulságokat. A bizalmas információkat az érzékeny vagy minősített adatok védelmére vonatkozó uniós vagy nemzeti jogszabályokkal összhangban védenie kell. ***Nem tartalmazhat semmilyen részletet az aktívan kihasznált sebezhetőségekről, amelyek továbbra is orvosolatlanok.***

(3a) Az e cikk (1) bekezdésében említett jelentés tartalmazza az (EU) 2022/2555 irányelv 19. cikke alapján elvégzett szakértői értékelések tanulságait.

(4) A jelentés adott esetben ajánlásokat fogalmaz meg – ***többek között valamennyi érdekelt fél számára*** – az Unió kiberbiztonsági helyzetének javítása érdekében;

(5) Ha lehetséges, a jelentés egy változatát nyilvánosan hozzáférhetővé kell tenni. Ez a változat csak nyilvános információkat tartalmazhat.

V. fejezet

ZÁRÓ RENDELKEZESEK

19. cikk

Az (EU) 2021/694 rendelet módosításai

Az (EU) 2021/694 rendelet a következőképpen módosul:

(1) A 6. cikk a következőképpen módosul:

a) az (1) bekezdés a következőképpen módosul:

i. a szöveg a következő aa) ponttal egészül ki:

„aa) az Európai Kiberpajzs kialakításának támogatása, beleértve a nemzeti és a határokon átnyúló biztonsági műveleti központok platformjainak fejlesztését, telepítését és működtetését, amelyek hozzájárulnak az Unión belüli helyzetismerethez és az Unió kiberfenyegetettségi információszerző képességeinek megerősítéséhez;”.

ii. A szöveg a következő g) ponttal egészül ki:

a nemzeti erőforrásokat és képességeket, valamint az uniós szinten rendelkezésre álló egyéb támogatási formákat kiegészítő ***kiberbiztonsági*** vészhelyzeti mechanizmus létrehozása és működtetése annak érdekében, hogy támogassa a tagállamokat a jelentős kiberbiztonsági eseményekre való felkészülésben és reagálásban, ideértve az uniós kiberbiztonsági tartalék létrehozását is.”

b) a (2) bekezdés helyébe a következő szöveg lép:

„(2) A 3. sz. egyedi célkitűzés alá tartozó fellépéseket elsősorban az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózata révén kell végrehajtani, az (EU) 2021/887 európai parlamenti és tanácsi rendelettel* összhangban, kivéve az uniós kiberbiztonsági tartalékot végrehajtó fellépéseket, amelyeket a Bizottság és az ENISA hajt végre.

_____

*Az Európai Parlament és a Tanács (EU) 2021/887 rendelete (2021. május 20.) az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontnak és a nemzeti koordinációs központok hálózatának a létrehozásáról (HL L 202., 2021.6.8., 1. O., ***ELI: http://data.europa.eu/eli/reg/2021/887/oj)”*;**

(2) A 9. cikk a következőképpen módosul:

a) A (2) bekezdés b), c) és d) pontja helyébe a következő szöveg lép:

„b) 1 776 956 000 EUR a 2. sz. Mesterséges intelligencia egyedi célkitűzésre;

c) ***1 620 566 000*** EUR a 3. sz. Kiberbiztonság és bizalom egyedi célkitűzésre;

d) ***500 347 000***EUR a 4. sz. Fejlett digitális készségek egyedi célkitűzésre;”

aa) a szöveg a következő (2a) bekezdéssel egészül ki:

„(2a). A (2) bekezdés c) pontjában említett összeget elsősorban a program 6. cikke (1) bekezdésének a)–f) pontjában említett operatív célkitűzések elérésére kell felhasználni.”;

ab) a szöveg a következő új (2b) bekezdéssel egészül ki:

„(2b). Az uniós kiberbiztonsági tartalék létrehozására és végrehajtására szánt összeg nem haladhatja meg a 27 millió EUR-t az Unióban a kiberbiztonsági fenyegetések és események észlelése, valamint az azokra való felkészülés és reagálás céljából az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról szóló rendelet tervezett időtartamára.”;

b) a cikk a következő (8) bekezdéssel egészül ki:

„(8) Az (EU, Euratom) 2018/1046 rendelet 12. cikkének (4) bekezdésétől ***eltérve az uniós kiberbiztonsági tartalék végrehajtásával összefüggésben*** az e rendelet 6. cikke (1) bekezdésének g) pontjában meghatározott célkitűzések megvalósítására irányuló fellépésekre elkülönített, fel nem használt kötelezettségvállalási és kifizetési előirányzatok

automatikusan átvihetők a következő pénzügyi évre, és terhükre a következő év december 31-éig kötelezettségek vállalhatók és kifizetések teljesíthetők.

A Bizottság tájékoztatja a Parlamentet és a Tanácsot az (EU, Euratom) 2018/1046 rendelet 12. cikkének (6) bekezdésével összhangban átvitt előirányzatokról.

(3) A 14. cikk (2) bekezdésének helyébe a következő szöveg lép:

„(2) A program az ***(EU, Euratom) 2018/1046*** rendeletben megállapított bármely formában nyújthat finanszírozást, többek között különösen közbeszerzés mint elsődleges forma vagy vissza nem térítendő támogatások és pénzdíjak útján.

Amennyiben valamely fellépés célkitűzésének eléréséhez innovatív termékek és szolgáltatások beszerzésére van szükség, csak olyan kedvezményezetteknek ítélhető oda vissza nem térítendő támogatás, amelyek a 2014/24/EU27[27] és a 2014/25/EU28 európai parlamenti és tanácsi irányelv[28] által meghatározott ajánlatkérő szervek vagy közszolgáltató ajánlatkérők.

Amennyiben valamely fellépés célkitűzéseinek eléréséhez olyan innovatív áruk vagy szolgáltatások nyújtása szükséges, amelyek kereskedelmi forgalomban nagy volumenben még nem beszerezhetők, az ajánlatkérő szerv vagy a közszolgáltató ajánlatkérő engedélyezheti ugyanazon eljárás keretében több szerződés odaítélését is.

Kellően indokolt közbiztonsági okokból az ajánlatkérő szerv vagy a közszolgáltató ajánlatkérő követelheti, hogy a szerződés teljesítésének helye az Unió területén legyen kijelölve.

Az (EU) 2023***/…*** rendelet 12. cikkével létrehozott uniós kiberbiztonsági tartalékra vonatkozó közbeszerzési eljárások végrehajtáskor a Bizottság és az ENISA központi beszerző szervként járhat el a 10. cikkel összhangban a programhoz társult harmadik országok érdekében vagy nevében történő beszerzések során. A Bizottság és az ENISA nagykereskedőként is eljárhat áruk és szolgáltatások az említett harmadik országoknak történő vásárlása, készletezése, továbbértékesítése vagy adományozása révén, beleértve a bérbeadást is. Az (EU) ***…/…*** rendelet 169. cikkének (3) bekezdésétől eltérve egyetlen harmadik ország által benyújtott kérelem elegendő ahhoz, hogy a Bizottság vagy az ENISA megbízást kapjon eljárni.

Az (EU) 2023/***…***XX rendelet 12. cikkével létrehozott uniós kiberbiztonsági tartalékra vonatkozó közbeszerzési eljárások végrehajtásakor a Bizottság és az ENISA központi beszerző szervként járhat el az uniós intézmények, szervek és ügynökségek érdekében vagy nevében történő beszerzések során. A Bizottság és az ENISA nagykereskedőként is eljárhat áruk és szolgáltatások uniós intézményeknek, szerveknek és ügynökségeknek történő vásárlása, készletezése, továbbértékesítése vagy adományozása révén, beleértve a bérbeadást is. Az (EU) ***…/…*** rendelet 169. cikkének (3) bekezdésétől eltérve egyetlen uniós intézmény, szerv vagy ügynökség által benyújtott kérelem elegendő ahhoz, hogy a Bizottság vagy az ENISA megbízást kapjon eljárni.

A program vegyes finanszírozási műveletek keretében pénzügyi eszközök formájában is nyújthat finanszírozást. ’;

(4) A szöveg a következő 16a. cikkel egészül ki:

„***16a. cikk***

„Az (EU) 2023/XX rendelet 3. cikkével létrehozott Európai Kiberpajzsot végrehajtó intézkedések esetében az (EU) 2023/**…** rendelet 4. és 5. cikkében meghatározott szabályok alkalmazandók. Az e rendeletben, illetve az (EU) 2023/**…** rendelet 4. és 5. cikkében foglalt rendelkezések ütközése esetén az utóbbiak az irányadók és alkalmazandók az említett egyedi intézkedésekre.***”;***

(5) A 19. cikk helyébe a következő szöveg lép:

„A program keretében nyújtott vissza nem térítendő támogatásokat az ***(EU, Euratom) 2018/1046*** rendelet VIII. címével összhangban kell odaítélni és irányítani, és azok az ***(EU, Euratom) 2018/1046*** rendelet 190. cikkében megállapított társfinanszírozási elv sérelme nélkül az elszámolható költségek legfeljebb 100 %-át fedezhetik. Az ilyen támogatásokat az egyes egyedi célkitűzésekre vonatkozóan meghatározottak szerint kell odaítélni és irányítani.

A vissza nem térítendő támogatásként nyújtott támogatást az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont az***(EU, Euratom) 2018/1046***rendelet 195. cikke (1) bekezdésének d) pontjával összhangban közvetlenül, pályázati felhívás nélkül is odaítélheti az ***(EU) .../...*** rendelet 4. cikkében említett nemzeti biztonsági műveleti központoknak és az ***(EU) .../...*** rendelet 5. cikkében említett üzemeltetési konzorciumnak.

Az ***(EU) .../...*** rendelet 10. cikkében meghatározott ***kiberbiztonsági*** vészhelyzeti mechanizmushoz vissza nem térítendő támogatásként nyújtott támogatást az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont az ***(EU, Euratom) 2018/1046***rendelet 195. cikke (1) bekezdésének d) pontjával összhangban közvetlenül, pályázati felhívás nélkül is odaítélheti a tagállamoknak.

Az ***(EU) .../...*** rendelet 10. cikke (1) bekezdésének c) pontjában meghatározott intézkedések esetében az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont tájékoztatja a Bizottságot és az ENISA-t a tagállamok pályázati felhívás nélküli közvetlen támogatásra irányuló kérelmeiről.

Az ***(EU) .../...*** rendelet 10. cikkének c) pontjában meghatározott jelentős vagy nagyszabású kiberbiztonsági eseményre való reagáláshoz nyújtott kölcsönös segítségnyújtás támogatása céljából és az ***(EU, Euratom) 2018/1046*** rendelet 193. cikke (2) bekezdése második albekezdésének a) pontjával összhangban kellően indokolt esetekben a költségek akkor is elszámolhatónak tekinthetők, ha azok a vissza nem térítendő támogatás elnyerésére rányuló pályázat benyújtása előtt merültek fel.”

(6) Az (EU) 2021/694 rendelet I. és II. melléklete e rendelet mellékletének megfelelően módosul.

19a. cikk

További források az ENISA számára

Az ENISA-nak további forrásokat kell kapnia az e rendelet által ráruházott további feladatai ellátásához. Ez a kiegészítő támogatás, beleértve a finanszírozást is, nem veszélyeztetheti más uniós programok, különösen a Digitális Európa program célkitűzéseinek elérését.

20. cikk

Értékelés és felülvizsgálat

(1) A Bizottság [e rendelet alkalmazásának kezdőnapjától számított ***két*** év]-ig, ***majd azt követően kétévente értékeli*** az e rendeletben ***meghatározott intézkedések működését, és jelentést nyújt be*** az Európai Parlamentnek és a Tanácsnak.

(2) Az értékelés különösen a következőkre terjed ki:

a) a határokon átnyúló SOC-k használata és hozzáadott értéke, valamint az, hogy milyen mértékben járulnak hozzá a kiberfenyegetések felderítésének és az azokra való reagálásnak a felgyorsításához és a helyzetismerethez; a nemzeti SOC-ok aktív részvétele az Európai Kiberpajzsban, beleértve a létrehozott nemzeti és határokon átnyúló SOC-k számát, valamint azt, hogy milyen mértékben járult hozzá a magas színvonalú, megvalósítható információk és kiberfenyegetésekkel kapcsolatos hírszerzési információk előállításához és cseréjéhez; a közösen beszerzett kiberbiztonsági infrastruktúra vagy eszközök, illetve mindkettő száma és költsége; a határokon átnyúló SOC-k között és az ágazati ISAC-kkal kötött együttműködési megállapodások száma; a CSIRT-ek hálózatának bejelentett biztonsági események száma és annak a CSIRT-ek hálózatának munkájára gyakorolt hatása;

b) a kiberbiztonsági szükséghelyzeti mechanizmus pozitív és negatív működése, beleértve azt is, hogy szükség van-e további együttműködésre vagy képzési követelményekre;

c) e rendelet hozzájárulása az Unió rezilienciájának és nyílt stratégiai autonómiájának megerősítéséhez, az érintett iparágak, mikrovállalkozások, kkv-k, köztük az induló vállalkozások versenyképességének javításához, valamint a kiberbiztonsági készségek fejlesztéséhez az Unióban;

d) az uniós kiberbiztonsági tartalék felhasználása és hozzáadott értéke, beleértve az uniós kiberbiztonsági tartalék részét képező megbízható biztonsági szolgáltatók számát; a kiberbiztonsági eseményekre való reagálást támogató intézkedések száma, típusa, költségei és hatása, valamint azok felhasználói és szolgáltatói; az az átlagos időtartam, amely alatt a Bizottság tudomást vesz a biztonsági eseményekről, az uniós

kiberbiztonsági tartalékot bevetik és reagálnak a biztonsági eseményekre, illetve amely alatt a felhasználó helyreáll a biztonsági eseményt követően; az uniós kiberbiztonsági tartalék hatályát ki kell-e terjeszteni a biztonsági eseményekre való felkészülési szolgáltatásokra vagy a megbízható, irányított biztonsági szolgáltatókkal és az uniós kiberbiztonsági tartalék potenciális felhasználóival való közös gyakorlatokra hogy szükség esetén biztosítható legyen az uniós kiberbiztonsági tartalék hatékony működése;

e) e rendelet hozzájárulása a kiberbiztonsági ágazatban dolgozó munkaerő azon készségeinek és kompetenciáinak fejlesztéséhez és javításához, amelyek az Unió kiberbiztonsági fenyegetések és események észlelésére, megelőzésére, az azokra való reagálásra és az azokat követő helyreállításra irányuló képességének megerősítéséhez szükségesek;

f) e rendelet hozzájárulása a legkorszerűbb technológiák Unión belüli bevezetéséhez és fejlesztéséhez.

(3) Az (1) bekezdésben említett jelentések alapján a Bizottság adott esetben jogalkotási javaslatot nyújt be az Európai Parlamentnek és a Tanácsnak e rendelet módosítása céljából.

20a. 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 Bizottság 6. cikk (3) bekezdésében, 7. cikk (2) bekezdésében, 12. cikk (8) bekezdésében és 13. cikk (7) bekezdésében említett, felhatalmazáson alapuló jogi aktus elfogadására vonatkozó felhatalmazása ...éves időtartamra szól ...-tól/-től [az alap-jogiaktus hatálybalépésének időpontja vagy a társjogalkotók által megállapított bármely más időpont] kezdődő hatállyal. A Bizottság legkésőbb kilenc hónappal a …éves időtartam letelte előtt jelentést készít a felhatalmazásról. A felhatalmazás hallgatólagosan meghosszabbodik a korábbival megegyező időtartamra, amennyiben az Európai Parlament vagy a Tanács nem ellenzi a meghosszabbítást legkésőbb három hónappal minden egyes időtartam letelte előtt.

(3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja a 6. cikk (3) bekezdésében, a 7. cikk (2) bekezdésében, a 12. cikk (8) bekezdésében és a 13. cikk (7) bekezdésében említett felhatalmazást. A visszavonásról szóló határozat megszünteti az abban meghatározott felhatalmazást. A határozat az Európai Unió Hivatalos Lapjában való kihirdetését követő napon, vagy a benne megjelölt 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) Az 6. cikk (3) bekezdése, a 7. cikk (2) bekezdése, a 12. cikk (8) bekezdése vagy a 13. cikk (7) 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. Ez az időtartam az Európai Parlament vagy a Tanács kezdeményezésére [két hónappal] meghosszabbodik.

21. cikk

A bizottsági eljárás

(1) A Bizottságot az (EU) 2021/694 rendelettel létrehozott Digitális Európa programot koordináló bizottság segíti. Ez a bizottság a 182/2011/EU rendelet értelmében vett bizottságnak minősül.

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

22. cikk

Hatálybalépés

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

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt ....

az Európai Parlament részéről	*a Tanács részéről*
az elnök	*az elnök*

MELLÉKLET

Az (EU) 2021/694 rendelet a következőképpen módosul:

(1) Az I. mellékletben a „3. sz. egyedi célkitűzés – Kiberbiztonság és bizalom” szakasz/fejezet helyébe a következő szöveg lép:

sz. egyedi célkitűzés – Kiberbiztonság és bizalom

A program ösztönzi az Unió digitális gazdaságának, társadalmának és demokráciájának biztosításához szükséges alapvető kapacitások megerősítését, kiépítését és beszerzését azáltal, hogy megerősíti az Unió kiberbiztonsági ipari potenciálját és versenyképességét, valamint javítja a magán- és a közszektor arra irányuló képességét, hogy megvédje a polgárokat és a vállalkozásokat a kiberfenyegetésektől, többek között az (EU) 2016/1148 irányelv végrehajtásának támogatásával.

Ezen célkitűzés keretében a kezdeti és adott esetben a további fellépések a következőket foglalják magukban:

1. A tagállamokkal közös beruházások fejlett kiberbiztonsági berendezésekbe, infrastruktúrákba és know-how-ba, amelyek alapvető fontosságúak a kritikus infrastruktúrák és általában a digitális egységes piac védelméhez. Az ilyen közös beruházások körébe tartozhatnak a kvantum-létesítményekbe és a kiberbiztonságot szolgáló adatforrásokba, a kibertérbeli helyzetismeretbe – ***beleértve az Európai Kiberpajzsot alkotó nemzeti biztonsági műveleti központokat és a határokon átnyúló biztonsági műveleti központokat*** –, valamint egyéb olyan eszközökbe történő befektetések, amelyeket az állami és magánszektor rendelkezésére kell bocsátani egész Európában.

2. A meglévő technológiai kapacitások továbbfejlesztése és a tagállami kompetenciaközpontok hálózatba szervezése, valamint annak biztosítása, hogy ezen kapacitások reagáljanak a közszektorbeli és az ipari igényekre, többek között olyan termékek és szolgáltatások révén, amelyek megerősítik a kiberbiztonságot és bizalmat a digitális egységes piacon belül.

3. Hatékony és korszerű kiberbiztonsági és bizalmi szolgáltatások széles körű bevezetésének biztosítása a tagállamokban. Az ilyen bevezetésbe beletartozik a termékek biztonságának és védelmének megerősítése is, a tervezésüktől kezdve a kereskedelmi forgalmazásukig.

4. Támogatás a kiberbiztonsági készségek terén fennálló hiányok megszüntetéséhez – ***különös hangsúlyt helyezve a nemek egyensúlyának megvalósítására az ágazatban*** –, például a kiberbiztonsági készségeket célzó programok összhangba hozásával, azok konkrét ágazati szükségletekhez igazításával – ***beleértve az interdiszciplináris és az általános szempontokat is*** –, valamint a célzott specializált képzéshez való hozzáférés megkönnyítésével, ***hogy minden személy és minden terület számára lehetőséget biztosítson***

az e rendelet által biztosított lehetőségek kihasználására.

(5) A tagállamok közötti szolidaritás előmozdítása a jelentős kiberbiztonsági eseményekre való felkészülés és reagálás terén a kiberbiztonsági szolgáltatások határokon átnyúló bevezetése révén, beleértve a hatóságok közötti kölcsönös segítségnyújtás támogatását és a ***irányított biztonsági szolgáltatásokat*** nyújtó, megbízható szolgáltatókból álló uniós szintű tartalék létrehozását.”;

(2) A II. mellékletben a „3. sz. egyedi célkitűzés – Kiberbiztonság és bizalom” szakasz/fejezet helyébe a következő szöveg lép:

sz. egyedi célkitűzés – Kiberbiztonság és bizalom

3.1. ***A kiberbiztonsági pajzs részeként*** közösen beszerzett kiberbiztonsági infrastruktúrák és/vagy eszközök száma.

3.2. Az európai kiberbiztonsági létesítményekhez hozzáféréssel rendelkező felhasználók és felhasználói közösségek száma

3.3. A ***kiberbiztonsági*** vészhelyzeti mechanizmus keretében a kiberbiztonsági eseményekre való felkészültséget és reagálást támogató, ***végrehajtott*** intézkedések száma, ***típusa, költsége és hatása. Az, hogy a felhasználó milyen mértékben hajtotta végre a felkészültségi tesztekre vonatkozó ajánlásokat, valamint az az átlagos időtartam, amely alatt a Bizottság tudomást vesz a biztonsági eseményekről, az uniós kiberbiztonsági tartalékot bevetik és reagálnak a biztonsági eseményekre, illetve amely alatt a felhasználó helyzete helyreáll a biztonsági eseményt követően;***