Az Európai Unió
Hivatalos Lapja

L 237

64. évfolyam

Magyar nyelvű kiadás Jogszabályok

2021. július 5.

Tartalom

HU

II

(Nem jogalkotási aktusok)

AJÁNLÁSOK

A BIZOTTSÁG (EU) 2021/1086 AJÁNLÁSA

(2021. június 23.)

a közös kiberbiztonsági egység létrehozásáról

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 292. cikkére,

mivel:

(1) A kiberbiztonság elengedhetetlen eleme a sikeres gazdasági és a társadalmi digitális átalakulásnak. Az EU elkötelezett amellett, hogy példátlan mértékű beruházásokat fordítson arra, hogy megerősítse az emberek, a vállalkozások és a hatóságok digitális eszközök iránti bizalmát.

(2) A Covid19-világjárvány növelte a konnektivitás fontosságát, valamint Európának a stabil hálózati és információs rendszerektől való függőségét, és rámutatott arra, hogy a teljes ellátási láncnak védelmet kell biztosítani. A megbízható és biztonságos hálózati és információs rendszerek különösen fontosak a világjárvány elleni küzdelem élén álló szervezetek, például a kórházak, az egészségügyi hatóságok és az oltóanyaggyártók számára. Az ilyen szervezetek elleni nagy horderejű kibertámadások megelőzésére, észlelésére, okozásától való eltántorításra és elrettentésre, enyhítésére és az azokra való reagálásra irányuló uniós erőfeszítések összehangolásával emberéletek menthetők meg és megelőzhetők azok a próbálkozások, amelyek a világjárvány lehető leghamarabbi leküzdésére irányuló uniós törekvések meghiúsítását célozzák. Emellett az EU kibertámadások elleni védekezőképességének megerősítése hatékonyan hozzájárul a globális, nyitott, stabil és biztonságos kibertér előmozdításához.

(3) Tekintettel a kiberbiztonsági fenyegetések határokon átnyúló jellegére és az összetettebb, áthatóbb és célzott támadások gyakoriságának folyamatos növekedésére ([1]), az érintett kiberbiztonsági intézményeknek és szereplőknek a meglévő erőforrások kiaknázása és az erőfeszítések jobb összehangolása révén növelniük kell az ilyen fenyegetésekre és támadásokra való reagálási képességüket. Valamennyi érintett uniós szereplőnek készen kell állnia arra, hogy közösen reagáljon, és a szükséges ismeret elve (need to know) helyett a megosztás szükségességének (need to share) elve alapján cseréljen információt egymással.

(4) A tagállamok közötti kiberbiztonsági együttműködés – különösen az Együttműködési Csoport (Kiberbiztonsági Együttműködési Csoport) és az (EU) 2016/1148 európai parlamenti és tanácsi irányelv ([2]) alapján létrehozott, a számítógép-biztonsági eseményekre reagáló csoportok (a továbbiakban: CSIRT-ek) hálózata – révén elért jelentős eredmények ellenére még mindig nincs olyan közös uniós platform, ahol a különböző kiberbiztonsági közösségekben gyűjtött információkat hatékonyan és biztonságosan ki lehetne cserélni, illetve ahol a műveleti képességeket az érintett szereplők koordinálhatnák és mozgósíthatnák. Ennek következtében fennáll annak a kockázata, hogy a kiberfenyegetésekkel és a kiberbiztonsági eseményekkel elszigetelten foglalkoznak, ami korlátozott hatékonysághoz és fokozott sebezhetőséghez vezet. Nem létezik továbbá olyan uniós szintű csatorna, amely technikai és operatív együttműködést tenne lehetővé a magánszektorral, akár az információmegosztás, akár a biztonsági eseményekre való reagálás támogatása céljából.

([1]) ENISA, Fenyegetettségi helyzet – 2020; Europol, Az internetes szervezett bűnözés általi fenyegetettség 2020. évi értékelése (IOCTA)

([2]) Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19., 1. o.).

(5) A meglévő keretek és struktúrák, valamint a tagállamokban és az érintett uniós intézményeknél, szerveknél és hivataloknál rendelkezésre álló erőforrások és szakértelem szilárd alapot biztosítanak a kiberbiztonsági fenyegetésekre, eseményekre és válsághelyzetekre való kollektív reagáláshoz ([3]). Ez a meglévő struktúra műveleti szinten magában foglalja a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálás tervezetét ([4]) (a továbbiakban: az összehangolt reagálás tervezete), a CSIRT-hálózatot ([5]) és az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatát (a továbbiakban: EU-CyCLONe), a Bűnüldözési Együttműködés és Képzés Európai Ügynökségének (a továbbiakban: Europol) a Kiberbűnözés Elleni Európai Központját (a továbbiakban: EC3) és a kiberbűnözéssel foglalkozó közös munkacsoportját (a továbbiakban: J-CAT), valamint az uniós bűnüldözési vészhelyzet-elhárítási protokollját (a továbbiakban: EU LE ERP). A Kiberbiztonsági Együttműködési Csoport, az Európai Unió Helyzetelemző Központja (a továbbiakban: EU INTCEN), valamint az állandó strukturált együttműködés ([6]) (a továbbiakban: PESCO) keretében indított kiberdiplomáciai eszköztár ([7]) és kibervédelemmel kapcsolatos projektek szintén hozzájárulnak a különböző kiberbiztonsági közösségekben folytatott szakpolitikai és operatív együttműködéshez. Megerősített megbízatása értelmében az Európai Uniós Kiberbiztonsági Ügynökség (a továbbiakban: ENISA) feladata a hálózati és információs rendszerek, e rendszerek felhasználói és a kiberbiztonsági fenyegetések és események által érintett más személyek kiberbiztonságával kapcsolatos operatív együttműködés támogatása ([8]). A politikai szintű integrált válságelhárítási mechanizmus (a továbbiakban: IPCR) révén az EU képes koordinálni a súlyos válságokra – többek között a nagyszabású kibertámadásokra – adott politikai válaszlépéseit.

(6) Ugyanakkor még nem létezik olyan mechanizmus, amely a hálózati és információs rendszerek biztonságáért, a kiberbűnözés elleni küzdelemért, a kiberdiplomácia tevékenységek folytatásáért és adott esetben a válsághelyzetekben szükséges kibervédelemért felelős kiberbiztonsági közösségek közötti kölcsönös segítségnyújtásra és a meglévő erőforrások kiaknázására szolgálna. Olyan uniós szintű, átfogó mechanizmus sem létezik, amely elősegítené a közösségek közötti technikai és operatív együttműködést a helyzetismeret, a felkészültség és a reagálás tekintetében. Ezenkívül az Europolon és az EU INTCEN-en keresztül szinergiákat kellene kiépíteni a bűnüldöző, illetve a hírszerzési közösségekkel.

(7) A Bizottság, az Unió külügyi és biztonságpolitikai főképviselője (a továbbiakban: a főképviselő), a tagállamok és az érintett uniós intézmények, szervek és hivatalok elismerik, hogy az elmúlt években létrehozott, jelenleg használt uniós kiberbiztonsági architektúra erősségeinek, gyengeségeinek, hiányosságainak és átfedéseinek elemzése nagy jelentőséggel bír. Ezen elemzésre válaszul a Bizottság – a tagállamokkal konzultálva és a főképviselő bevonásával – kidolgozta a közös kiberbiztonsági egység koncepcióját, mely a biztonsági unióra vonatkozó stratégia ([9]), a digitális stratégia ([10]) és a kiberbiztonsági stratégia ([11]) fontos eleme.

([3]) Az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatát, az EU-CyCLONe-t a tagállamok hozták létre az összehangolt reagálás tervezetére vonatkozó ajánlásra adott válaszként. A nemzeti operatív és válságkezelési szakértőkből álló hálózat kodifikációját a Bizottság 2020 decemberében javasolta az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről szóló COM(2020) 823 final (2020/0359 [COD]) irányelv révén.

([4]) 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.).

([5]) Ez az ajánlás figyelembe veszi az összehangolt reagálás tervezetéhez kapcsolódó, 2020. évi operatív szintű szimulációs gyakorlaton (Blue OLEx) alapuló utólagos műveleti jelentést, és különösen a közös kiberbiztonsági egységről folytatott stratégiai szakpolitikai megbeszélés elnöki összefoglalóját.

([6]) Különösen a kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportokra, valamint a kiberbiztonság területén a kölcsönös segítségnyújtásra vonatkozó, Litvánia által koordinált PESCO-projekt és a Németország által koordinált, a Kiber- és az Információs Terület Koordinációs Központjára vonatkozó PESCO-projekt.

([7]) A Tanács 2017. június 19-i következtetései (9916/17) a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről („kiberdiplomáciai eszköztár").

([8]) Az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) szóló, 2019. április 17-i (EU) 2019/881 európai parlamenti és tanácsi rendelet (HL L 151., 2019.6.7., 15. o.) 7. cikke előírja, hogy az Ügynökségnek támogatnia kell a tagállamok, az uniós intézmények, szervek és hivatalok közötti, valamint az érdekeltek közötti operatív együttműködést. Ez magában foglalja a tagállamok támogatását a CSIRT-ek hálózatán belüli operatív együttműködésben, a biztonsági eseményekről és a kiberfenyegetésekről szóló, részletes uniós kiberbiztonsági technikai helyzetjelentés rendszeres elkészítését, valamint a nagy kiterjedésű, határokon átnyúló biztonsági eseményekre és válságokra uniós és tagállami szintű, együttműködésen alapuló válasz kidolgozásához való hozzájárulást. Emellett az ENISA hozzájárul az Európai Biztonsági és Védelmi Főiskola (a továbbiakban: EBVF) által nyújtott képzési tevékenységekhez is.

([9]) A Bizottság közleménye az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: A biztonsági unióra vonatkozó uniós stratégia, COM(2020) 605 final.

([10]) A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Európa digitális jövőjének megtervezése, COM(2020) 67 final.

([11]) Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az EU kiberbiztonsági stratégiája a digitális évtizedre, JOIN(2020) 18 final.

(8) Válsághelyzetekben a tagállamok számára lehetővé kell tenni, hogy támaszkodhassanak az Unió szolidaritására, amely összehangolt, többek között a négy kiberbiztonsági közösség, azaz a polgári, a bűnüldözési ([12]), a diplomáciai és adott esetben a védelmi közösség általi segítségnyújtás formájában valósul meg. Az egy vagy több közösség tagjai által végrehajtott beavatkozás mértéke a nagyszabású esemény vagy válság jellegétől, és következésképpen az arra való reagáláshoz szükséges ellenintézkedések típusától függhet. Kiberbiztonsági fenyegetések, események és válságok esetén a jól képzett szakértők és a technikai eszközök alapvető fontosságú erőforrások, melyek hozzájárulhatnak a súlyos károk elkerüléséhez és a károk hatékony helyreállításához. Ezért a közös kiberbiztonsági egység központi elmei az egyértelműen meghatározott technikai és műveleti képességek (elsősorban a szakértők és az eszközök) lesznek, melyek szükség esetén bevethetők lesznek a tagállamokban. E platform résztvevői egyedülálló helyzetben lesznek ahhoz, hogy az uniós kiberbiztonsági gyorsreagálású csoportokon keresztül támogassák és koordinálják ezeket a képességeket, miközben megfelelő szinergiákat építenek ki a PESCO keretében már meglévő kiberbiztonsági projektekkel.

(9) A közös kiberbiztonsági egység virtuális és fizikai platformot biztosít, melynek működéséhez nem szükséges egy további, önálló szerv létrehozása. Az egység felállítása nem érintheti a nemzeti kiberbiztonsági hatóságok és az érintett uniós szervek felelősségi köreit és hatásköreit. A közös kiberbiztonsági egységnek a résztvevők közötti egyetértési megállapodásokon kell alapulnia. Az uniós szervezetek és a tagállami hatóságok közötti biztonságos és gyors operatív és technikai együttműködés platformjaként a meglévő struktúrákra, erőforrásokra és képességekre kell épülnie, és azokhoz hozzáadott értéket kell nyújtania. Emellett össze kell fognia az összes – azaz a polgári, a bűnüldözési, a diplomáciai és a védelmi – kiberbiztonsági közösséget. A platform résztvevőinek operatív vagy támogató szerepet kell betölteniük. Az operatív szerepet betöltő résztvevők között szerepelnie kell az ENISA-nak, az Europolnak, az európai intézmények, szervek és hivatalok számítógépes vészhelyzeteket elhárító csoportjának (a továbbiakban: CERT-EU), a Bizottságnak, az Európai Külügyi Szolgálatnak (beleértve az INTCEN-t), a CSIRT-hálózatnak és az EU-CyCLONe-hálózatnak. A támogató szerepet betöltő résztvevők között pedig szerepelnie kell az Európai Védelmi Ügynökségnek (a továbbiakban: EDA), a kiberbiztonsági együttműködési csoport elnökének, a kiberkérdésekkel foglalkozó tanácsi horizontális munkacsoport elnökének, valamint az érintett PESCO-projektek egy-egy képviselőjének ([13]). Mivel a tagállamok rendelkeznek a nagyszabású kiberbiztonsági fenyegetésekre, eseményekre és válságokra való reagáláshoz szükséges műveleti képességekkel és hatáskörökkel, a platform résztvevőinek célkitűzéseik eléréséhez – a megfelelő uniós szervezetek segítségével – elsősorban ezekre a kapacitásokra kell támaszkodniuk.

(10) A közös kiberbiztonsági egység várhatóan új lendületet fog adni a 2017-ben az összehangolt reagálás tervezetével elindított folyamatnak. Folytatnia fogja az összehangolt reagálás tervezetben vázolt struktúra működőképessé tételét, és létrehozása meghatározó lépés lesz egy olyan európai kiberbiztonsági válságkezelési keret kidolgozása felé, amely lehetővé teszi a fenyegetések és kockázatok összehangolt és időben történő azonosítását, enyhítését és megválaszolását. Ezáltal a közös kiberbiztonsági egység segíteni fogja az EU-t a jelenlegi és a jövőbeli fenyegetésekre való reagálásban.

(11) A közös kiberbiztonsági egységben való részvétel révén az operatív és támogató szerepet betöltő résztvevőknek várhatóan lehetőségük fog nyílni arra, hogy az uniós kiberbiztonsági válságreagálási kerethez kapcsolódóan végzett tevékenységük részeként kapcsolatot építsenek az érdekelt felek szélesebb körével. Miközben megbízatásuk korlátain belül feladataikat ellátják, a résztvevők számára biztosítani kell, hogy a kiberbiztonsági fenyegetésekre és eseményekre minden szempontból jobban fel legyenek készülve, azokról átfogóbb helyzetismerettel rendelkezzenek, és a kiberbiztonsági szaktudás további forrásai is rendelkezésükre álljanak. A résztvevőknek például rendszeresen részt kell venniük a közösségek közötti gyakorlatokban, jól meghatározott szerepet kell betölteniük az uniós válságreagálási tervben, közös nyilvános kommunikáció révén növelniük kell fellépéseik láthatóságát, és operatív együttműködési megállapodásokat kell kötniük a magánszektorral. Ezzel párhuzamosan a közös kiberbiztonsági egységhez való hozzájárulás lehetővé fogja tenni a résztvevők számára a meglévő hálózatok, például a CSIRT-hálózat és az EU-CyCLONe-hálózat megerősítését, biztonságos információcserére szolgáló eszközöket és – pl. a biztonsági műveleti központok (a továbbiakban: SOC-k) révén – a biztonsági események jobb észlelését lehetővé tevő képességeket biztosít számukra, valamint lehetővé teszi, hogy kihasználják a rendelkezésre álló uniós műveleti képességeket.

(12) A közös kiberbiztonsági egység résztvevőinek a technikai és operatív együttműködésre kell összpontosítaniuk, melybe a közös műveletek is beletartoznak. A résztvevőknek a megbízatásuk által lehetővé tett mértékben hozzá kell járulniuk az ilyen együttműködéshez. Az együttműködésnek a folyamatban lévő erőfeszítésekre kell épülnie és azokat ki kell egészítenie. Az érintett együttműködés típusától függően azokba további résztvevők is bevonhatók.

([12]) Az igazságügyi együttműködés szempontjából is releváns.

([13]) Lásd az 5. lábjegyzetet. Az Európai Külügyi Szolgálat (a továbbiakban EKSZ) és az EDA – a PESCO titkárságaként betöltött szerepe révén – kapcsolatot tart a releváns PESCO-projektek koordinátoraival.

(13) A platformnak össze kell gyűjtenie a tagállamok és az uniós szervek technikai és operatív válságkezelési szakértőit abból a célból, hogy a meglévő képességek és szakértelem felhasználásával összehangolja a kiberbiztonsági fenyegetésekre, eseményekre és válsághelyzetekre való reagálást. A közös kiberbiztonsági egységben részt vevő szakértők a fizikai és a virtuális platform együttes használatával sokkal szélesebb támadási felület felügyeletére és védelmére lesznek képesek. E célból a résztvevőknek össze kell hangolniuk a határokon átnyúló biztonsági események és válságok esetén tett erőfeszítéseiket, valamint a platformon keresztül segítséget kell nyújtaniuk az incidens sújtotta országoknak.

(14) A közös kiberbiztonsági egység létrehozásához olyan fokozatos folyamatra van szükség, amely kiaknázza és konszolidálja az ezen ajánlásban említett, meglévő kereteket és struktúrákat, ideértve a tagállamok által vezetett fórumok keretében létrehozott együttműködési mechanizmusokat (pl. a CSIRT-ek hálózatát, az EU-CyCLONe-hálózatot, a kiberkérdésekkel foglalkozó tanácsi horizontális munkacsoportot, a J-CAT-et és a vonatkozó PESCO-projekteket), valamint az uniós intézmények, szervek és hivatalok oldalán az ENISA és a CERT-EU közötti, illetve az információcserével foglalkozó intézményközi kiberbiztonsági csoportban folytatott strukturált együttműködést. A hibrid fenyegetésekre vonatkozó, a polgári védelmi ([14]) és ágazatspecifikus ([15]) kereteket szintén be kell vonni. Hasonlóképpen strukturált kapcsolatot kell kialakítani az IPCR-rel ([16]). Ez lehetővé fogja tenni válság esetén az információk gyors és hatékony továbbítását a Tanácsban csoportosult politikai szintű döntéshozóknak.

(15) A közös kiberbiztonsági egység létrehozásának ezért egy fokozatos és átlátható folyamatnak kell lennie, amelynek a következő két évben le kell zajlania. Ezért az ezen ajánlásban meghatározott célkitűzéseket a mellékletben ismertetett négylépéses folyamattal kell elérni. Az első két lépésben a Bizottság által létrehozandó munkacsoport keretében el kell indítani az ENISA által szervezett és támogatott előkészítő folyamatot, amelyben uniós és tagállami szinten operatív és támogató szerepet betöltő résztvevők vesznek részt. Az előkészítő munkát a kölcsönös szerepvállalás, az inkluzivitás és a konszenzusépítés elveinek kell vezérelniük. Ösztönözni kell valamennyi résztvevőt a szerepvállalásra, lehetővé téve a különböző nézetek és álláspontok kifejtését, és törekedni kell az olyan megoldásokra, amelyek a lehető legszélesebb körű támogatást élvezik. Az igényektől függően és kellően indokolt feltételek alapján az ezen ajánlásban szereplő különböző lépések ütemterve módosítható.

(16) Az előkészítő folyamatnak az első lépés keretében a rendelkezésre álló releváns uniós műveleti képességek azonosításával és a résztvevők platformon belüli szerepeinek és felelősségi köreinek értékelésével kell kezdődnie. A második lépésnek a következőket kell magában foglalnia: a biztonsági események és válságok elhárítására irányuló uniós terv kidolgozása az összehangolt reagálás tervezetével ([17]) és az uniós bűnüldözési veszélyhelyzet-elhárítási protokollal összhangban, a felkészültséghez és a helyzetismerethez kapcsolódó tevékenységek bevezetése a kiberbiztonsági jogszabállyal és az Europol-rendelettel ([18]) összhangban, valamint a résztvevők platformon belüli szerepei és felelősségi körei értékelésének lezárása. A munkacsoportnak be kell nyújtania az értékelés eredményeit a Bizottsághoz és a főképviselőhöz, akik később megosztják az eredményeket a Tanáccsal. A Bizottságnak és a főképviselőnek együtt kell működniük annak érdekében, hogy hatáskörüknek megfelelően az említett értékelés alapján közös jelentést készítsenek, és fel kell kérniük a Tanácsot, hogy tanácsi következtetések útján hagyja jóvá a jelentést.

(17) A jóváhagyást követően a közös kiberbiztonsági egység működőképessé válik, utat nyitva a folyamat két hátralévő lépése előtt. A harmadik lépésben a résztvevőknek – a fizikai és a virtuális platformban rejlő lehetőségeket kihasználva – képessé kell válniuk a közös kiberbiztonsági egység keretében uniós gyorsreagálású csoportok bevetésére a biztonsági események és válságok elhárítására irányuló uniós tervben meghatározott eljárások szerint, és ezáltal hozzá kell járuljanak a biztonsági eseményekre való reagálás különböző aspektusaihoz (a nyilvános kommunikációtól a károk utólagos helyreállításáig). Végezetül a negyedik lépésben a magánszektor érdekelt feleit – köztük a kiberbiztonsági megoldások és szolgáltatások felhasználóit és szolgáltatóit – felkérik, hogy járuljanak hozzá a platform működéséhez, lehetővé téve a résztvevők számára, hogy javítsák az információmegosztást és hatékonyabbá tegyék az EU kiberbiztonsági fenyegetésekre és eseményekre való összehangolt reagálását.

([14]) Ezzel összefüggésben a közös kiberbiztonsági egységnek szinergiákat kell kialakítania az uniós polgári védelmi mechanizmussal (UCPM) annak érdekében, hogy fokozza Európa felkészültségét a kiberbiztonsági vetülettel is rendelkező összetett katasztrófákra és veszélyhelyzetekre, és javítsa az azokra való reagálást.

([15]) Mint például az (EU) 2021/xx európai parlamenti és tanácsi rendeletben* [DORA] előirányzott, pénzügyi szektorra vonatkozó keret.

([16]) Lásd az (5) preambulumbekezdést.

([17]) Lásd a 3. lábjegyzetet.

([18]) Az Európai Parlament és a Tanács (EU) 2016/794 rendelete (2016. május 11.) a Bűnüldözési Együttműködés Európai Uniós Ügynökségéről (Europol), valamint a 2009/371/IB, a 2009/934/IB, a 2009/935/IB, a 2009/936/IB és a 2009/968/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről (HL L 135., 2016.5.24., 53. o.).

(18) A négylépéses folyamat végén a résztvevőknek tevékenységi jelentést kell készíteniük az ajánlásban meghatározott négy lépés végrehajtása terén elért eredményekről, amelyben ismertetniük kell az elért eredményeket és a felmerülő kihívásokat, majd be kell nyújtaniuk a Bizottságnak és a főképviselőnek. E jelentés alapján a Bizottságnak és a főképviselőnek értékelnie kell az említett eredményeket, és következtetéseket kell levonnia a közös kiberbiztonsági egység jövőjére vonatkozóan.

(19) A Bizottságnak, az ENISA-nak, az Europolnak és a CERT-EU-nak az ezen ajánlás IV. szakaszában meghatározottak szerint igazgatási, pénzügyi és technikai támogatást kell nyújtania a közös kiberbiztonsági egység számára, a rendelkezésre álló költségvetés és emberi erőforrások függvényében. Az érintett uniós intézmények, szervek és hivatalok operatív kiberbiztonsági képességeinek megerősítése kulcsfontosságú lesz a közös kiberbiztonsági egység hatékony előkészítéséhez és fenntarthatóságához. A Bizottság biztosítani kívánja, hogy a CERT-EU esetében e hozzájárulás jogalapja az uniós intézmények, szervek és hivatalok számára kötelező közös kiberbiztonsági szabályokról szóló, 2021. októberi rendelet legyen.

(20) Tekintettel az (EU) 2019/881 rendelet (a továbbiakban: kiberbiztonsági jogszabály) szerinti megerősített megbízatására, az ENISA egyedülálló helyzetben van ahhoz, hogy megszervezze és támogassa a közös kiberbiztonsági egység előkészítését, valamint hogy hozzájáruljon annak működőképessé tételéhez. A kiberbiztonsági jogszabály rendelkezéseivel összhangban az ENISA jelenleg Brüsszelben irodát hoz létre a CERT-EU-val való strukturált együttműködés támogatása érdekében. Ez a strukturált együttműködés – melyben a kapcsolódó hivatalok is részt vesznek – hasznos keretet biztosít a közös kiberbiztonsági egység létrehozásának elősegítéséhez, beleértve egy olyan fizikai tér kialakítását, amelyet szükség esetén a résztvevők, illetve más érintett uniós intézmények, szervek és hivatalok személyzete rendelkezésére kell bocsátani. A fizikai platformot egy virtuális platformmal kell kombinálni, amely együttműködési és biztonságos információmegosztási eszközöket kínál. Ezek az eszközök ki fogják aknázni az európai kiberpajzs ([19]) — többek között az SOC-k és az ISAC-k – révén gyűjtött gazdag információkészletet.

(21) A Tanács által 2018-ban elfogadott, a súlyos, határokon átnyúló kibertámadásokra vonatkozó uniós bűnüldözési veszélyhelyzet-elhárítási protokoll központi szerepet biztosít az Europol Kiberbűnözés Elleni Európai Központjának (EC3) ([20]) az összehangolt reagálás tervezete keretében. Az említett protokoll lehetővé teszi az uniós bűnüldöző hatóságok számára, hogy határokon átnyúló, feltehetőleg rossz szándékú, nagyszabású kibertevékenységek esetén a hét minden napján 24 órában gyorsan reagáljanak és felmérjék a helyzetet, valamint hogy a határokon átnyúló biztonsági eseményekre való reagálás hatékony koordinálása érdekében biztonságosan és időben megosszák egymással a kritikus információkat. A protokoll tovább részleteket tartalmaz a többi uniós intézménnyel való együttműködésről, az egész EU-ra kiterjedő válságprotokollokról, valamint a magánszektorral folytatott válsághelyzeti együttműködésről. A bűnüldöző közösségnek adott esetben az Europol támogatásával hozzá kell járulnia a közös kiberbiztonsági egység munkájához azáltal, hogy a büntető igazságszolgáltatási keret követelményeivel és az alkalmazandó elektronikusbizonyíték-kezelési eljárásokkal összhangban megteszi a szükséges lépéseket a teljes nyomozási ciklus során. Az Europol az EC3 2013-as létrehozása óta operatív támogatást nyújt és elősegíti a kiberfenyegetések elleni operatív együttműködést. Az Europolnak megbízatásával és a „hírszerzésen alapuló bűnüldözés” megközelítéssel összhangban támogatnia kell a platformot, és fel kell használni minden, a szervezeten belül rendelkezésre álló szakértelemet, terméket, eszközt és szolgáltatást, amely releváns lehet az adott eseményre vagy válságra való reagálás szempontjából.

(22) Az információs rendszerek elleni támadásokról szóló 2013/40/EU irányelv többek között előírja a tagállamok számára egy olyan operatív nemzeti kapcsolattartó pont létrehozását, amely a hét minden napján 24 órában rendelkezésre áll az említett irányelvben meghatározott bűncselekményekkel kapcsolatos információcsere céljából. Az operatív nemzeti kapcsolattartó pontok hálózatának szintén hozzá kell járulnia a közös kiberbiztonsági egység munkájához azáltal, hogy adott esetben biztosítja a tagállami bűnüldöző hatóságok bevonását.

(23) Az uniós kiberdiplomáciai közösség hozzájárul a globális, nyitott, stabil és biztonságos kibertér előmozdításához és védelméhez, valamint az ezzel kapcsolatos rossz szándékú kibertevékenységek megelőzéséhez, az azoktól való elrettentéshez, illetve az azokra való reagáláshoz. Az EU 2017-ben létrehozta a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretét (a továbbiakban: kiberdiplomáciai eszköztár). Ez a keret a kiberdiplomáciára vonatkozó tágabb uniós szakpolitika részét képezi. Hozzájárul a konfliktusmegelőzéshez és a nemzetközi kapcsolatok stabilabbá tételéhez. Lehetővé teszi az EU és a tagállamok számára, hogy adott esetben a nemzetközi partnerekkel együttműködve valamennyi közös kül- és biztonságpolitikai (a továbbiakban: KKBP) intézkedést – a megvalósításukra vonatkozó eljárásokkal összhangban – felhasználják az együttműködés ösztönzésére, a fenyegetések mérséklésére, valamint a kibertérben az aktuális és lehetséges jövőbeli rosszindulatú magatartás befolyásolására. A kiberdiplomáciai közösségnek a közös kiberbiztonsági egység keretében kell együttműködnie a diplomáciai intézkedések teljes skálájának felhasználása, illetve a felhasználás támogatása révén, különösen a nyilvános kommunikáció tekintetében, és válság esetén a közös helyzetismeret és a harmadik országokkal való együttműködés előmozdításával.

([19]) JOIN(2020) 18 final, 1.2. szakasz.
([20]) A központot az (EU) 2016/794 rendelet hozta létre.

(24) A tervezetnek megfelelően a főképviselőnek – többek között az INTCEN-en keresztül – hozzá kell járulnia a közös kiberbiztonsági egység munkájához a meglévő és kialakulóban lévő fenyegetésekre vonatkozó, hírszerzési információkon alapuló közös helyzetismeret folyamatos meglétének biztosításával, beleértve az adott eseményhez kapcsolódóan szükséges stratégiai helyzetismeretet is.

(25) A kibervédelmi közösségen belül az EU és a tagállamok célja a kibervédelmi képességek bővítése, valamint az érintett uniós intézmények, szervek és hivatalok közötti, illetve a tagállamokkal kialakított és a tagállamok közötti további szinergiák, koordináció és együttműködés megerősítése, többek között a közös biztonság- és védelempolitikához (a továbbiakban: KBVP) kapcsolódó missziók és műveletek tekintetében. A közösség működését az uniós szintű kormányközi irányítás, a nemzeti katonai parancsnoki struktúrák és a katonai, illetve kettős felhasználású képességek és eszközök határozzák meg. Mivel a kibervédelmi közösség és a közös kiberbiztonsági egység jellegüket tekintve eltérőek, az információmegosztás lehetővé tétele érdekében speciális interfészeket kell kiépíteni ([21]).

(26) Az állandó strukturált együttműködés a Lisszaboni Szerződés ([22]) által bevezetett jogi keret, melyet 2017-ben hoztak létre az Unió keretén belül. A strukturált együttműködés eredményeként több PESCO-projekt jött létre a kiberbiztonság területén, amelyek hozzájárulnak a kibervédelemmel kapcsolatos együttműködés – mint például az információmegosztás, a képzés és az operatív támogatás – terén tett erőfeszítések fokozására vonatkozó 11. kötelezettségvállalás ([23]) teljesítéséhez. Az EKSZ, beleértve az Európai Unió Katonai Törzsét és az EDA-t, alkotja a PESCO titkárságát, amely az Unió keretén belül egyedüli kapcsolattartó pontként szolgál a PESCO-val kapcsolatos valamennyi kérdésben, ideértve a PESCO-projektekhez kapcsolódó támogató és koordináló feladatokat is (pl. az új projektjavaslatok értékelését, a projektekre vonatkozó eredményjelentések elkészítését stb.). A releváns PESCO-projektek képviselőinek támogatniuk kell a közös kiberbiztonsági egység munkáját, különösen a helyzetismeret és a felkészültség tekintetében.

(27) A közös kiberbiztonsági egységen keresztül a résztvevőknek megfelelő mértékben be kell vonniuk a magánszektor érdekelt feleit (ideértve a kiberbiztonsági megoldásokat és szolgáltatásokat nyújtó és felhasználó feleket is) ahhoz, hogy – az adatmegosztásra és az adatbiztonságra vonatkozó jogi keret kellő figyelembevétele mellett – támogathassák az európai kiberbiztonsági válságkezelési kerethez kapcsolódó munkát. A kiberbiztonsági szolgáltatóknak azáltal kell hozzájárulniuk a kezdeményezéshez, hogy megosztják a fenyegetettségi információkat, és a kiberbiztonsági eseményekre való reagálás szakértőinek biztosítása révén gyorsan növelik az egységnek a nagyszabású támadásokra és válságokra való reagálás céljából rendelkezésre álló kapacitását. Lehetővé kell tenni, hogy – elsősorban a kiberbiztonsági irányelv hatálya alá tartozó – kiberbiztonsági termékek és szolgáltatások felhasználói segítséget és tanácsot kérhessenek az uniós szintű információmegosztási és elemzési központokhoz (ISAC-khez) kapcsolódó, jelenleg még nem létező, strukturált csatornákon keresztül ([24]). A platform a nemzetközi partnerekkel folytatott együttműködés megerősítéséhez is hozzájárulhat.

(28) A helyzetismeret fejlesztéséhez és fenntartásához élvonalbeli behatolásészlelési és -megelőzési képességekre van szükség. A közös kiberbiztonsági egységnek a legkorszerűbb hálózatot kell használnia, amely képes elemezni azokat a rosszindulatú fenyegetéseket és eseményeket, melyek az Unió egész területén hatással lehetnek a kulcsfontosságú kommunikációs és információs rendszerekre. Ez azt jelenti, hogy – egyéb források mellett – a nemzeti, ágazati és határokon átnyúló SOC-k által felügyelt kommunikációs hálózatokból származó, fenyegetésekkel kapcsolatos információkat továbbítani kell a közös kiberbiztonsági egységnek annak érdekében, hogy a résztvevők jobban felmérhessék az EU fenyegetettségi helyzetét.

(29) Az esetlegesen bizalmas anyagokat is tartalmazó operatív információk cseréjének támogatása érdekében a platformnak megfelelően biztonságos kommunikációs csatornákat kell használnia. Ezek a csatornák a már meglévő infrastruktúrára is épülhetnek, például az Europol és a bűnüldöző közösség által használt Biztonságos Információcsere Hálózati Alkalmazásra (a továbbiakban: SIENA). A kiberbiztonsági stratégiában bejelentetteknek megfelelően az uniós intézmények, szervek és hivatalok által használt eszközöknek tiszteletben kell tartaniuk az információbiztonsági szabályokat, melyekre a Bizottság hamarosan javaslatot fog tenni.

([21]) Nevezetesen az EKSZ képviselete révén, hogy lehetővé váljon a kibervédelmi közösség megfelelő bevonása, mely önkéntes nemzeti hozzájárulásokon alapul.

([22]) Az EUSZ 42. cikkének (6) bekezdése, 46. cikke és 10. jegyzőkönyve.

([23]) A PESCO-ban részt vevő tagállamok 20 egyedi kötelezettségvállalást tesznek. Az egyes kötelezettségvállalások a PESCO-ról szóló, a Lisszaboni Szerződéshez csatolt 10. jegyzőkönyv 2. cikkében meghatározott öt kulcsterület szerint oszthatók fel.

([24]) Említésre méltó példa az olyan ISAC-kre, amelyek részt vehetnének a szóban forgó információmegosztásban az európai energiaipari információmegosztási és elemzési központ (EE-ISAC) és az európai pénzügyi intézetek információmegosztási és elemzési központja (FI-ISAC).

(30) A Bizottság – elsősorban a Digitális Európa programon keresztül – támogatni fogja a fizikai és virtuális platform létrehozásához, a biztonságos kommunikációs csatornák és képzési kapacitások kiépítéséhez és fenntartásához, valamint a felderítési képességek fejlesztéséhez és bevezetéséhez szükséges beruházásokat. Emellett az Európai Védelmi Alap hozzájárulhat a kulcsfontosságú kibervédelmi technológiák és képességek finanszírozásához, amelyek megerősítenék a nemzeti kibervédelmi felkészültséget,

ELFOGADTA EZT AZ AJÁNLÁST:

I. **AZ AJÁNLÁS CÉLJA**

1. Ezen ajánlás célja azoknak a folyamatoknak az azonosítása, amelyek a nagyszabású kiberbiztonsági események és válsághelyzetek megelőzésére, észlelésére, okozásától való eltántorításra és elrettentésre, enyhítésére és az azokra való reagálásra irányuló uniós erőfeszítéseknek egy kiberbiztonsági egységen keresztüli összehangolásához szükségesek. Ennek érdekében ez az ajánlás meghatározza azt a folyamatot, azokat a mérföldköveket és azt az ütemtervet is, amelyet a tagállamoknak és az érintett uniós intézményeknek, szerveknek és hivataloknak a platform létrehozása és fejlesztése tekintetében követniük kell.

2. A tagállamoknak és az érintett uniós intézményeknek, szerveknek és hivataloknak biztosítaniuk kell, hogy nagyszabású kiberbiztonsági események és válsághelyzetek esetén egy közös kiberbiztonsági egységen keresztül koordinálják erőfeszítéseiket, ami a tagállami hatóságok és az érintett uniós intézmények, szervek és hivatalok szakértelmén alapuló kölcsönös segítségnyújtást ([25]) tesz lehetővé. A közös kiberbiztonsági egységnek lehetővé kell tennie a résztvevők számára a magánszektorral való együttműködést is.

II. **FOGALOMMEGHATÁROZÁSOK**

3. Ezen ajánlás alkalmazásában:

a) „Kiberbiztonsági események és válságok elhárítására irányuló uniós terv”: a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról szóló, 2017. szeptember 13-i bizottsági ajánlás (a továbbiakban: az összehangolt reagálás tervezete) 1. pontjában ismertetett uniós kiberbiztonsági válságreagálási keret megvalósításához szükséges szerepkörök, módozatok és eljárások összessége.

b) „Kiberbiztonsági közösségek”: a tagállamokat és az érintett uniós intézményeket, szerveket és hivatalokat egyaránt képviselő, egymással együttműködő polgári, bűnüldözési, diplomáciai és védelmi csoportok, amelyek a kiberbiztonsággal kapcsolatos közös célok, érdekek és missziók érdekében információt cserélnek.

c) „Magánszektorbeli résztvevők”: kiberbiztonsági megoldásokat ([26]) és szolgáltatásokat ([27]) nyújtó vagy használó magánszektorbeli szervezetek képviselői.

d) „Nagyszabású esemény”: az (EU) 2016/1148 irányelv 4. cikkének 7. pontjában meghatározott olyan biztonsági esemény, amelynek legalább két tagállamban jelentős hatása van.

e) „Integrált uniós kiberbiztonsági helyzetjelentés”: a közös kiberbiztonsági egység résztvevőitől származó információkat összegző jelentés, amely az (EU) 2019/881 rendelet 7. cikkének (6) bekezdésében meghatározott uniós kiberbiztonsági technikai helyzetjelentésre épül.

f) „Uniós kiberbiztonsági gyorsreagálású csoport”: a tagállami számítógép-biztonsági eseményekre reagáló csoportokból származó, elismert kiberbiztonsági szakértőkből álló csoport, melynek munkáját az ENISA, a CERT-EU és az Europol támogatja, és amely készen áll arra, hogy távolról segítse a nagyszabású események és válsághelyzetek által érintett résztvevőket.

g) „Egyetértési megállapodások”: résztvevők közötti megállapodás, amely meghatározza az együttműködés szükséges módozatait, beleértve az uniós kiberbiztonsági gyorsreagálású csoportok létrehozásához és mozgósításához, valamint a kölcsönös segítségnyújtás lehetővé tételéhez szükséges eszközök és eljárások meghatározását is.

([25]) Az (EU) 2016/1148 irányelvben és az EUMSZ 222. cikkében meghatározott megközelítéssel és elvekkel összhangban. Az Európai Unióról szóló szerződés 42. cikke (7) bekezdésének sérelme nélkül.

([26]) Beleértve a szoftverforgalmazókat is.

([27]) Beleértve a fenyegetettségi információkat is.

III. A KÖZÖS KIBERBIZTONSÁGI EGYSÉG CÉLJA

4. A tagállamok és az érintett uniós intézmények, szervek és hivatalok feladata biztosítani, hogy a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre **összehangolt uniós válaszlépeseket** adjanak, és a károk helyreállítása is uniós szinten koordinált módon történjék. Ezeket a válaszlépéseket egyfelől az operatív résztvevők, nevezetesen az ENISA, az Europol, a CERT-EU, a Bizottság, az Európai Külügyi Szolgálat (beleértve az INTCEN-t), a CSIRT-hálózat, az EU-CyCLONe, másfelől a támogató résztvevők, nevezetesen a Kiberbiztonsági Együttműködési Csoport elnöke, a kiberkérdésekkel foglalkozó tanácsi horizontális munkacsoport elnöke, az Európai Védelmi Ügynökség és az idevágó PESCO-projektek ([28]) egy-egy képviselője közötti együttműködésben kell megtenni. Az operatív résztvevőknek képesnek kell lenniük arra, hogy a közös kiberbiztonsági egységen belül gyorsan és hatékonyan mozgósítsák a kölcsönös segítségnyújtáshoz szükséges operatív erőforrásokat. E célból a közös kiberbiztonsági egységen belül össze kell hangolni a kölcsönös segítségnyújtási mechanizmusokat, amennyiben egy vagy több tagállam ezt kéri.

5. A hatékonyan összehangolt válaszlépések érdekében a 4. pontban felsorolt operatív és támogató résztvevőknek képesnek kell lenniük arra, hogy megosszák egymással bevált módszereiket, kihasználják a **megosztott helyzetismeret** folyamatos meglétének előnyeit, és a megbízatásuk szerint lehetséges mértékben biztosítsák a **felkészültség** megfelelő szintjét. Ennek során figyelembe kell venniük a meglévő folyamatokat és a különböző kiberbiztonsági közösségek szakértelmét.

IV. A KÖZÖS KIBERBIZTONSÁGI EGYSÉG MŰKÖDÉSÉNEK MEGHATÁROZÁSA

6. A tagállamoknak és az érintett uniós intézményeknek, szerveknek és hivataloknak biztosítaniuk kell az alábbiak révén, hogy az ENISA hozzájárulására építve az (EU) 2019/881 rendelet 7. cikkének (7) bekezdésével összhangban a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre **összehangolt uniós válaszlépeseket** adjanak, és a károk helyreállítása is uniós szinten koordinált módon történjék:

a) **uniós kiberbiztonsági gyorsreagálású csoportok** létrehozása, képzése, tesztelése és összehangolt bevetése az (EU) 2019/881 rendelet 7. cikkének (4) bekezdésében és az (EU) 2016/794 rendelet 3. és 4. cikkében rejlő lehetőségeket kiaknázva;

b) egy olyan **virtuális és fizikai platform** összehangolt kiépítése, amely az ENISA és a CERT-EU közötti – az (EU) 2019/881 rendelet 7. cikkének (4) bekezdésében lefektetett – strukturált együttműködés alapján támogató infrastruktúraként hivatott szolgálni a résztvevők közötti műszaki és operatív együttműködéshez, valamint ahhoz, hogy összegyűjtsék a releváns személyzetet és egyéb erőforrásokat a résztvevőktől;

c) **az Unió** kiberbiztonsági közösségeiben ([29]) **rendelkezésre álló** azon **operatív és műszaki képességek nyilvántartásának** létrehozása és vezetése, amelyeket nagyszabású kiberbiztonsági események vagy válsághelyzetek esetén be lehet vetni;

d) jelentéstétel a Bizottságnak és a főképviselőnek az egyes kiberbiztonsági közösségeken belüli és az azok közötti **kiberbiztonsági operatív együttműködési tevékenységek** során szerzett tapasztalatokról.

7. A tagállamoknak és az érintett uniós intézményeknek, szerveknek és hivataloknak biztosítaniuk kell, hogy a közös kiberbiztonsági egység – az (EU) 2019/881 rendelet 7. cikkében és az (EU) 2016/794 rendelet 3. cikkében foglalt célkitűzéseket követve – gondoskodjon a **megosztott helyzetismeret** folyamatos meglétéről és a **felkészültségről** a kiberbiztonsági közösségek között vagy azokon belül a kibertérben kialakuló válsághelyzetekkel kapcsolatban. E célból a tagállamoknak és az érintett uniós intézményeknek, szerveknek és hivataloknak az (EU) 2019/881 és az (EU) 2016/794 rendelettel összhangban lehetővé kell tenniük a következő **támogató** műveletek végrehajtását:

a) **integrált uniós kiberbiztonsági helyzetjelentés** kidolgozása az összes releváns információ és fenyegetettségi információ összegyűjtése és elemzése révén;

b) megfelelő és biztonságos **eszközök** használata a résztvevők közötti és más szervezetekkel való gyors információmegosztás érdekében az (EU) 2019/881 rendelet 7. cikke (1) bekezdésével összhangban;

c) az ahhoz szükséges **információk és szakértelem cseréje**, hogy az Unió – az (EU) 2019/881 rendelet 7. cikkének (2) bekezdése szerint az ENISA támogatásával – felkészülten tudja kezelni a kibertérben kialakuló nagyszabású eseményeket és válsághelyzeteket;

d) a **kiberbiztonsági események és válságok elhárítására irányuló** nemzeti **tervek** ([30]) elfogadása és tesztelése az (EU) 2019/881 rendelet 7. cikkének (2), (5) és (7) bekezdésével összhangban;

([28]) Ezek a Kiber- és az Információs Terület Koordinációs Központjára (CIDCC), továbbá a kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportokra, valamint a kiberbiztonság területét érintő kölcsönös segítségnyújtásra (CRRT) vonatkozó projektek.

([29]) Adott esetben ideértve a kibervédelmi közösséget is.

([30]) Az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről szóló irányelv 7. cikkének (3) bekezdése alapján, COM(2020) 823 final, 2020/0359 (COD).

e) a **kiberbiztonsági események és válságok elhárítására irányuló uniós terv** kidolgozása, kezelése és tesztelése, többek között közösségek közötti gyakorlatok és képzések révén, az összehangolt reagálás tervezetére vonatkozó ajánlással összhangban és az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről szóló (EU) 2016/1148 irányelv felülvizsgálatára irányuló bizottsági javaslat ([31]) 7. cikkének (3) bekezdésére építve;

f) a résztvevők támogatása abban, hogy – az (EU) 2019/881 rendelet 7. cikkének (1) bekezdésével összhangban az ENISA segítségével – információmegosztási megállapodásokat, valamint operatív együttműködési megállapodásokat tudjanak kötni olyan **magánszektorbeli szervezetekkel**, amelyek többek között fenyegetettségi információkat szolgáltatnak és eseményreagálási szolgáltatásokat nyújtanak;

g) strukturált szinergiák kialakítása a nemzeti, ágazati és határokon átnyúló **megfigyelési és felderítési képességekkel**, különösen a biztonsági műveleti központokkal;

h) a résztvevők támogatása a nagyszabású biztonsági események és válsághelyzetek **kezelésében**, összhangban az ENISA-nak az (EU) 2019/881 rendelet 7. cikkében meghatározott támogató szerepével. Ez magában foglalja a közös helyzetismerethez való hozzájárulást, a diplomáciai fellépések támogatását, a politikai jellegű és a bűnügyi nyomozásokkal összefüggésben végzett attribúció támogatását, többek között az Europolon keresztül ([32]), a nyilvános kommunikáció összehangolását és a biztonsági események után a károk helyreállításának elősegítését.

8. A 6. és 7. pont végrehajtásához a tagállamoknak és az érintett uniós intézménynek, szerveknek és hivataloknak biztosítaniuk kell a következőket:

a) a közös kiberbiztonsági egység szervezeti szempontjainak, valamint a platformon belül az operatív és támogató résztvevők **szerepének és felelősségi körének** meghatározása a platform hatékony működésének érdekében az ezen ajánlás mellékletében meghatározott szempontokkal és elvekkel összhangban;

b) a 4. pontban említett résztvevők közötti együttműködés szükséges módozatait meghatározó **egyetértési megállapodások** megkötése.

9. Az (EU) 2019/881 rendelet 7. cikkének megfelelően az ENISA feladata, hogy a közös kiberbiztonsági egységen belül koordinálja, illetve támogassa a tagállamokat és az érintett uniós intézményeket, szerveket és hivatalokat, többek között a titkársági feladatok ellátásával, találkozók szervezésével, valamint a tagállami és az uniós szintű intézkedések végrehajtásához való hozzájárulással. Az ENISA-nak a találkozók megrendezésére biztonságos virtuális platformot és fizikai teret kell létrehoznia, és elő kell segítenie a szükséges végrehajtási intézkedéseket.

V. A KÖZÖS KIBERBIZTONSÁGI EGYSÉG LÉTREHOZÁSA

10. A tagállamoknak és az érintett uniós intézményeknek, szerveknek és hivataloknak biztosítaniuk kell, hogy a közös kiberbiztonsági egység **2022. június 30**-án az operatív szakaszba lépjen. Az operatív résztvevőknek addigra az uniós kiberbiztonsági gyorsreagálású csoportok megalapozásához elegendő műveleti képességet és szakértőt rendelkezésre kell bocsátaniuk. A fizikai és virtuális platformra vonatkozó terveknek előrehaladott állapotban kell lenniük.

11. A tagállamoknak és az érintett uniós intézményeknek, szerveknek és hivataloknak hozzá kell járulniuk a közös kiberbiztonsági egység működéséhez, és biztosítaniuk kell, hogy **2023. június 30**-ig teljeskörűen működőképessé váljon. Ehhez négy egymást követő lépést kell megtenni, amelyek a következő tevékenységek elvégzésére irányulnak:

a) első lépés: a közös kiberbiztonsági egység szervezeti szempontjainak értékelése és a rendelkezésre álló uniós műveleti képességek azonosítása **2021. december 31**-ig;

b) második lépés: a kiberbiztonsági események és a válságok elhárítására irányuló tervek kidolgozása és a közös felkészültségi tevékenységek bevezetése **2022. június 30**-ig;

c) harmadik lépés: a közös kiberbiztonsági egység működőképessé tétele **2022. december 31**-ig;

d) 4. lépés: a közös kiberbiztonsági egységen belüli együttműködés kiterjesztése magánszervezetekre és jelentéstétel az elért eredményekről **2023. június 30**-ig.

A négy egymást követő lépés keretében végrehajtandó részletesebb intézkedéseket ezen ajánlás melléklete tartalmazza.

([31]) COM(2020) 823 final

([32]) Összhangban az (EU) 2016/794 rendelettel.

12. Az első két lépés keretében az ENISA-nak meg kell szerveznie és támogatnia kell a közös kiberbiztonsági egység előkészítését. A Bizottság szolgálatainak munkacsoportot kell összehívniuk, amelyben az operatív és a támogató résztvevők közreműködnek az említett előkészítő munka befejezése érdekében. A Bizottság szolgálatainak ki kell nevezniük az egyik képviselőt a munkacsoport társelnökévé, és fel kell kérniük további társelnököknek egyfelől egy, a főképviselő által kinevezett képviselőt, akik saját hatáskörüknek megfelelően hozzájárulnak a napirendi pontokhoz, valamint másfelől egy, a tagállamok által választott képviselőt is.

13. A második lépés végére a munkacsoportnak le kell zárnia a közös kiberbiztonsági egység szervezeti szempontjainak, valamint az operatív résztvevők e platformon belüli szerepeinek és felelősségi köreinek értékelését. A munkacsoportnak be kell nyújtania az értékelés eredményeit a Bizottsághoz és a főképviselőhöz. A Bizottság és a főképviselő megosztják az értékelést a Tanáccsal. A Bizottság és a főképviselő az említett értékelés alapján közös jelentést készít, és felkéri a Tanácsot, hogy tanácsi következtetések útján hagyja jóvá a jelentést.

14. A közös kiberbiztonsági egységnek a harmadik lépéstől kezdve működőképesnek kell lennie.

15. Az ENISA-nak és a Bizottságnak gondoskodnia kell arról, hogy az uniós finanszírozási programok, elsősorban a Digitális Európa program keretében meglévő források – összhangban a megfelelő munkaprogramok létrehozására vonatkozó szabályokkal – felhasználásra kerüljenek annak érdekében, hogy a közös kiberbiztonsági egység résztvevői számára további képzési lehetőségeket, kommunikációs képességeket és biztonságos információmegosztási infrastruktúrát tegyenek elérhetővé, amely utóbbi lehetővé teszi a minősített információk cseréjét akár közösségeken átnyúlóan is.

VI. **FELÜLVIZSGÁLAT**

16. A tagállamoknak együtt kell működniük a Bizottsággal és a főképviselővel annak érdekében, hogy hatáskörüknek megfelelően **2025. június 30**-ig felmérjék a közös kiberbiztonsági egység eredményességét és hatékonyságát, aminek alapján következtetéseket lehet majd levonni a közös kiberbiztonsági egység jövőjét illetően. Ezen értékelés során figyelembe kell venni a fent említett négy lépés végrehajtását.

Kelt Brüsszelben, 2021. június 23-án.

a Bizottság részéről
Thierry BRETON
a Bizottság tagja

MELLÉKLET

A közös kiberbiztonsági egység létrehozásának lépései

Ez a melléklet részletesebben ismerteti a közös kiberbiztonsági egység létrehozásához és működőképessé tételéhez szükséges alapvető és támogató intézkedéseket.

1. *Első lépés: a közös kiberbiztonsági egység szervezeti szempontjainak értékelése és a rendelkezésre álló uniós műveleti képességek azonosítása*

ALAPVETŐ INTÉZKEDÉSEK

A közös kiberbiztonsági egység operatív résztvevőinek a Bizottság által az ENISA támogatásával létrehozott munkacsoportban össze kell gyűjteniük a meglévő műveleti képességekkel kapcsolatos információkat, többek között össze kell állítaniuk a rendelkezésre álló elismert szakemberek jegyzékét, feltüntetve szakterületüket, továbbá a biztonsági események kezelésére szolgáló eszközökre, funkciókra és módszerekre, a rendelkezésre álló képzési és gyakorlati portfóliókra, valamint a meglévő információs és hírszerzési elemzési termékekre vonatkozó információkat. Ezen információk alapján az operatív résztvevőknek össze kell állítaniuk egy **jegyzéket azon rendelkezésre álló uniós műveleti képességekről**, amelyeket kiberbiztonsági események vagy válsághelyzetek esetén be lehet vetni, különösen az uniós kiberbiztonsági gyorsreagálású csoportokon keresztül.

A munkacsoportnak értékelnie kell a közös kiberbiztonsági egység mint platform **szervezeti szempontjait**, valamint **az operatív résztvevők e platformon belüli szerepeit és felelősségi köreit**.

Annak érdekében, hogy átfogó képet lehessen nyerni a képességekről, és megállapodás jöhessen létre az eljárásokról, az első lépés keretében előirányzott alapvető intézkedéseket **2021. december 31-ig [6 hónappal az elfogadás után]** el kell végezni, és lehetőség szerint a támogató intézkedéseket is le kell zárni.

2. *Második lépés: a kiberbiztonsági események és válságok elhárítására irányuló tervek kidolgozása és a közös felkészültségi tevékenységek bevezetése*

ALAPVETŐ INTÉZKEDÉSEK

A munkacsoport operatív résztvevőinek a támogató résztvevőkkel egyeztetve el kell készíteniük a **kiberbiztonsági események és válságok elhárítására irányuló uniós tervet** az idevágó nemzeti tervek alapján. A kiberbiztonsági események és válságok elhárítására irányuló uniós tervnek tartalmaznia kell az uniós felkészültséggel kapcsolatos célkitűzéseket, a biztonságos információcsere azonosított eljárásait és csatornáit, beleértve az információkezelési módokat is, valamint a kölcsönös segítségnyújtási mechanizmus aktiválásának kritériumait, amelyek a biztonsági események kölcsönösen elfogadott osztályozási taxonómiáján és a rendelkezésre álló uniós képességek jegyzékén alapulnak.

A második lépés végére a munkacsoportnak le kell zárnia a közös kiberbiztonsági egység szervezeti szempontjainak, valamint az operatív résztvevők e platformon belüli szerepeinek és felelősségi köreinek értékelését. A munkacsoportnak be kell nyújtania az értékelés eredményeit a Bizottsághoz és a főképviselőhöz. A Bizottság és a főképviselő megosztja az értékelést a Tanáccsal. A Bizottságnak és a főképviselőnek együtt kell működniük annak érdekében, hogy hatáskörüknek megfelelően az említett értékelés alapján közös jelentést készítsenek, és felkérjék a Tanácsot, hogy tanácsi következtetések útján hagyja jóvá a jelentést.

TÁMOGATÓ INTÉZKEDÉSEK

A kiberbiztonsági események és válságok elhárítására irányuló uniós tervnek az idevágó nemzeti tervek fő elemeire kell épülnie. Az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről szóló irányelvre irányuló bizottsági javaslattal ([1]) összhangban a tagállamoknak nemzeti terveket kell elfogadniuk a kiberbiztonsági események és válságok elhárítására. A nemzeti terveknek, amelyek kölcsönös felülvizsgálat tárgyát képezhetik, a nagyszabású kiberbiztonsági események és válsághelyzetek kezelésével kapcsolatban célkitűzéseket és módszereket kell meghatározniuk. A nemzeti terveknek különösen a következőkre kell kitérniük:

a) a nemzeti felkészültségi intézkedések és tevékenységek célkitűzései;

b) az illetékes nemzeti hatóságok feladatai és felelősségei tagállami szinten;

c) nemzeti válságkezelési eljárások és információmegosztási csatornák;

d) a felkészültségi intézkedések azonosítása, beleértve a gyakorlatokat és a képzési tevékenységeket;

e) az érintett állami és magán érdekelt felek, valamint az érintett infrastruktúra azonosítása;

f) nemzeti eljárások és megállapodások az érintett nemzeti – köztük az összes kiberközösségért felelős – hatóságok és szervek között annak biztosítása érdekében, hogy a tagállam hatékonyan részt vegyen a nagyszabású kiberbiztonsági események és válságok uniós szintű összehangolt elhárításában és azt támogassa.

A tagállamok, valamint az uniós intézmények, szervek és hivatalok által szolgáltatott információk alapján az operatív résztvevőknek a közös kiberbiztonsági egység keretében a következő támogató intézkedéseket kell végrehajtaniuk:

a) az első uniós integrált helyzetjelentés elkészítése a kiberbiztonsági események és válságok elhárítására irányuló nemzeti tervek alapján;

([1]) COM(2020) 823 final, 2020/0359 (COD), Brüsszel, 2020.12.16.

b) kommunikációs képességek és biztonságos információmegosztási eszközök kialakítása;

c) a résztvevők közötti kölcsönös segítségnyújtásra vonatkozó jegyzőkönyvek elfogadásának elősegítése;

d) a közösségek közötti gyakorlatok és képzések megszervezése azon szakértők számára, akik szerepelnek a rendelkezésre álló uniós műveleti képességek jegyzékében;

e) a gyakorlatok koordinálására irányuló többéves terv kidolgozása.

Szükség esetén az operatív résztvevőknek konzultálniuk kell a támogató résztvevőkkel. Az ENISA-nak a Bizottság, az Europol és a CERT-EU támogatásával kommunikációs képességeket és biztonságos információmegosztási eszközöket kell kialakítania az információmegosztás lehetővé tétele érdekében.

Annak érdekében, hogy a szükséges tervek ki legyenek dolgozva, és a közös tevékenységeket el lehessen kezdeni, a második lépés keretében előirányzott alapvető intézkedéseket **2022. június 30-ig [6 hónappal az 1. lépés végét követően]** el kell végezni, és lehetőség szerint a támogató intézkedéseket is le kell zárni.

3. *Harmadik lépés: a közös kiberbiztonsági egység működőképessé tétele*

ALAPVETŐ INTÉZKEDÉSEK

Miután a Tanács jóváhagyta a második lépés keretében benyújtott jelentésről szóló bizottsági következtetéseket, az operatív résztvevők feladata, hogy a közös kiberbiztonsági egységen keretében koordinálják az **uniós kiberbiztonsági gyorsreagálású csoportok** bevetését, és létrehozzanak egy olyan **fizikai platformot**, amely lehetővé teszi a csapatok számára a technikai és operatív tevékenységek végzését. A második lépés keretében végzett előkészítő munka alapján a résztvevőknek véglegesíteniük kell a kiberbiztonsági események és válságok elhárítására irányuló uniós tervet. Az operatív résztvevőknek gondoskodniuk kell arról, hogy az uniós műveleti képességek jegyzékében szereplő szakértők és képességek rendelkezésre álljanak, és készek legyenek hozzájárulni az uniós kiberbiztonsági gyorsreagálású csoportok tevékenységéhez.

A kiberbiztonsági események és válságok elhárítására irányuló uniós terv végrehajtása érdekében a résztvevőknek éves munkaprogramot kell meghatározniuk.

TÁMOGATÓ INTÉZKEDÉSEK

A kiberdiplomáciai közösség támaszkodhat a közös kiberbiztonsági egységre a nyilvános kommunikáció összehangolása érdekében. A platform lehetővé teheti a résztvevők számára, hogy mind a politikai jellegű attribúcióhoz, mind a rendőrségi és igazságügyi szinten alkalmazott büntető igazságszolgáltatási keretrendszeren belüli attribúcióhoz hozzájáruljanak. Emellett megkönnyítheti a károk helyreállítását, és strukturált szinergiákat teremthet a nemzeti és határokon átnyúló megfigyelési és felderítési képességekkel.

A közös kiberbiztonsági egység működőképessé tételének érdekében a harmadik lépés keretében előirányzott alapvető intézkedéseket **2022. december 31-ig [6 hónappal a 2. lépés végét követően]** el kell végezni, és lehetőség szerint a támogató intézkedéseket is le kell zárni.

4. *Negyedik lépés: a közös kiberbiztonsági egységen belüli együttműködés kiterjesztése magánszervezetekre, valamint jelentéstétel az elért eredményekről*

ALAPVETŐ INTÉZKEDÉS

A közös kiberbiztonsági egység résztvevőinek tevékenységi **jelentést** kell készíteniük **az ajánlásban meghatározott négy lépés végrehajtása terén elért haladásról, mind az eredményeket, mind a felmerülő kihívásokat ismertetve**. A jelentésnek statisztikai információkat is magában kell foglalnia a négy lépés során végzett operatív együttműködési tevékenységekkel kapcsolatban. A jelentést be kell nyújtani a Bizottságnak és a főképviselőnek.

TÁMOGATÓ INTÉZKEDÉSEK

Az uniós kiberbiztonsági gyorsreagálású csoportok rendelkezésére álló képességek és információk bővítése érdekében a résztvevőknek biztosítaniuk kell, hogy a közös kiberbiztonsági egység támogassa az **információmegosztási és operatív együttműködési megállapodások** megkötését a **résztvevők** és az olyan **magánszektorbeli szervezetek** között, amelyek többek között fenyegetettségi információkat szolgáltatnak és eseményelhárítási szolgáltatásokat nyújtanak. Egyéb tevékenységek mellett biztosítaniuk kell továbbá, hogy a közös kiberbiztonsági egység támogassa a fenyegetettségről és sebezhető pontokról folytatott rendszeres párbeszédet és információmegosztási tevékenységeket a kiberbiztonsági megoldások felhasználóival, elsősorban azokkal, akik a kiberbiztonsági irányelv hatálya alá tartoznak, illetve részt vesznek az **uniós szintű információmegosztó és -elemző központok (ISAC)** munkájában.

A tagállamoknak elő kell segíteniük, hogy a területükön működő szervezetek, különösen a kiberbiztonsági irányelv hatálya alá tartozók, részt vehessenek az uniós szintű információmegosztó és -elemző központokkal folytatott köz-magán párbeszédekben, és hozzá tudjanak ezekhez járulni.

A magánszektor megfelelő részvételének garantálása érdekében a negyedik lépés keretében előirányzott alapvető intézkedéseket **2023. június 30-ig [6 hónappal a 3. lépés végét követően]** el kell végezni, és lehetőség szerint a támogató intézkedéseket is le kell zárni.

AZ UNIÓS MŰVELETI KÉPESSÉGEK GYORS MOZGÓSÍTÁSA

A KÉPESSÉGEKET BIZTOSÍTJÁK: operatív résztvevők

A KÉPESSÉGEKET IRÁNYÍTJÁK: a közös kiberbiztonsági egységen belül a résztvevők, az elfogadott szerepekkel és felelősségi körökkel összhangban

Lépés	Célkitűzés	Feladat	Alapvető intézkedés	Támogató intézkedés
1. lépés: meghatározás **2021. december 31-ig** [6 hónappal az elfogadás után]	FELKÉSZÜLTSÉG	**a képességek azonosítása**	**az operatív résztvevők összeállítják a rendelkezésre álló uniós műveleti képességek jegyzékét**	
2. lépés: előkészítés **2022. június 30-ig** [6 hónappal az 1. lépés végét követően]	FELKÉSZÜLTSÉG	**azon eljárások és intézkedések meghatározása, amelyekkel szükség esetén aktiválhatók a képességek**	**az operatív résztvevők elkészítik a kiberbiztonsági események és válságok elhárítására irányuló uniós tervet (uniós kiberbiztonsági válságreagálási keret az összehangolt reagálás tervezete szerint) az elfogadott nemzeti tervek alapján**	**az operatív résztvevők elkészítik az uniós kiberbiztonsági technikai helyzetjelentésen alapuló integrált uniós helyzetjelentéseket**
	FELKÉSZÜLTSÉG	**a képességeket fejlesztő gyakorlatok szervezése**		**a résztvevők közös gyakorlatokat és képzéseket szerveznek (a közösségeken átnyúlóan)** **a résztvevők a gyakorlatok koordinálására irányuló többéves tervet dolgoznak ki**
	HELYZETISMERET	**az információk és a támogatás iránti kérelmek megosztására szolgáló eszközök létrehozása**		**a résztvevők biztonságos és gyors információmegosztási eszközöket dolgoznak ki**
A KÖZÖS KIBERBIZTONSÁGI EGYSÉG MŰKÖDŐKÉPES a Bizottság által létrehozandó munkacsoport résztvevői által végzett előkészítő munka alapján				
3. lépés: bevetés **2022. december 31-ig** [6 hónappal a 2. lépés végét követően]	FELKÉSZÜLTSÉG	**azon eljárások, rendelkezések és egyetértési megállapodások elfogadása, amelyekkel szükség esetén aktiválhatók a képességek**	**az operatív résztvevők véglegesítik a kiberbiztonsági események és válságok elhárítására irányuló uniós tervet, és éves munkaprogramok révén meghatározzák végrehajtását**	**a résztvevők támogatják a nemzeti és határokon átnyúló megfigyelési és felderítési képességek, köztük a biztonsági műveleti központok létrehozását is**
	ÖSSZEHANGOLT VÁLASZLÉPÉSEK	**a képességek bevetése szükség esetén**	**az operatív résztvevők koordinálják a bevethető uniós kiberbiztonsági gyorsreagálású csoportokat a brüsszeli közös kiberbiztonsági egység virtuális és fizikai platformján keresztül**	**a résztvevők koordinálják a nyilvános kommunikációt, és hozzájárulnak mind a politikai, mind a büntető igazságszolgáltatás keretében történő attribúcióhoz**

4. lépés: kiterjesztés és jelentéstétel **2023. június 30-ig** [6 hónappal a 3. lépés végét követően]	HELYZETISMERET ÖSSZEHANGOLT VÁLASZLÉPÉSEK	**a méretezhetőség biztosítása a magánszektor bevonása révén, az újonnan felmerülő igények kielégítése érdekében**	**a résztvevők tevékenységi jelentést nyújtanak be az elért haladásról, mind az eredményeket, mind a felmerülő kihívásokat ismertetve, mindezt statisztikai információkkal alátámasztva**	**a résztvevők információmegosztási megállapodásokat, valamint operatív együttműködési megállapodásokat kötnek a kiberbiztonsági szolgáltatókkal** **a résztvevők információmegosztási megállapodásokat kötnek a kiberbiztonsági megoldások felhasználóival – elsősorban a kiberbiztonsági irányelv hatálya alá tartozó és az uniós szintű információmegosztó és -elemző központokban tevékenykedő felhasználókkal**

ISSN 1977-0731 (elektronikus kiadás)
ISSN 1725-5090 (nyomtatott kiadás)

Az Európai Unió
Kiadóhivatala
L-2985 Luxembourg
LUXEMBURG

HU