2024/1366

2024.5.24.

A BIZOTTSÁG (EU) 2024/1366 FELHATALMAZÁSON ALAPULÓ RENDELETE

(2024. március 11.)

az (EU) 2019/943 európai parlamenti és tanácsi rendeletnek a határkeresztező villamosenergia-áramlás kiberbiztonsági szempontjaira vonatkozó ágazatspecifikus szabályokról szóló üzemi és kereskedelmi szabályzat létrehozása révén történő kiegészítéséről

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a villamos energia belső piacáról szóló, 2019. június 5-i (EU) 2019/943 európai parlamenti és tanácsi rendeletre ([1]) és különösen annak 59. cikke (2) bekezdésének e) pontjára,

mivel:

(1) A kiberbiztonsági kockázatok kezelése elengedhetetlen a villamosenergia-ellátás biztonságának fenntartásához és a villamosenergia-ágazat magas szintű kiberbiztonságának biztosításához.

(2) A digitalizáció és a kiberbiztonság döntő fontosságú az alapvető szolgáltatások nyújtása szempontjából, és ezért a kritikus energetikai infrastruktúra számára stratégiai jelentőséggel bír.

(3) Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve ([2]) a kiberbiztonságnak az egész Unióban egységesen magas szintjét biztosító intézkedéseket állapít meg. Az (EU) 2019/941 európai parlamenti és tanácsi rendelet ([3]) kiegészíti az (EU) 2022/2555 irányelvet annak biztosítása révén, hogy a kiberbiztonsági eseményeket megfelelően, kockázatként azonosítsák, és a kezelésükre teendő intézkedések megfelelően szerepeljenek a kockázati készültségi tervekben. Az (EU) 2019/943 rendelet kiegészíti az (EU) 2022/2555 irányelvet és az (EU) 2019/941 rendeletet azáltal, hogy uniós szinten egyedi szabályokat állapít meg a villamosenergia-ágazatra vonatkozóan. Ez a felhatalmazáson alapuló rendelet továbbá kiegészíti az (EU) 2022/2555 irányelv villamosenergia-ágazatra vonatkozó rendelkezéseit, amennyiben határkeresztező villamosenergia-áramlásról van szó.

(4) Az összekapcsolt digitalizált villamosenergia-rendszerek összefüggésében a kibertámadásokkal kapcsolatos villamosenergia-ellátási válságok megelőzése és kezelése nem tekinthető kizárólag nemzeti feladatnak. A regionális és uniós együttműködés révén hatékonyabb és kevésbé költséges intézkedéseket kell kidolgozni az abban rejlő lehetőségek maradéktalan kiaknázása céljából. Ezért közös szabályozási keretre és jobban összehangolt eljárásokra van szükség annak biztosítása érdekében, hogy a tagállamok és más szereplők hatékonyan, határokon átívelő módon működjenek együtt, a tagállamok, valamint a villamos energiáért és a kiberbiztonságért felelős illetékes hatóságok közötti fokozott átláthatóság, bizalom és szolidaritás szellemében.

(5) Az e rendelet hatálya alá tartozó kiberbiztonsági kockázatkezeléshez strukturált folyamatra van szükség, amely magában foglalja többek között a kibertámadásokból eredő, a határkeresztező villamosenergia-áramlást érintő kockázatok azonosítását, a kapcsolódó működési folyamatokat és hatásköröket, valamint a megfelelő kiberbiztonsági ellenőrzéseket és hitelesítési mechanizmusokat. Bár a teljes folyamat időkerete több év, minden egyes lépésének hozzá kell járulnia az ágazat magas szintű, közös kiberbiztonságához és a kiberbiztonsági kockázatok csökkentéséhez. A folyamat valamennyi résztvevőjének minden tőle telhetőt meg kell tennie annak érdekében, hogy indokolatlan késedelem nélkül, de legkésőbb az e rendeletben meghatározott határidőkön belül, a lehető leghamarabb kidolgozza és elfogadja a módszertanokat.

([1]) HL L 158., 2019.6.14., 54. o.

([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 (NIS 2 irányelv) (HL L 333., 2022.12.27., 80. o.).

([3]) Az Európai Parlament és a Tanács (EU) 2019/941 rendelete (2019. június 5.) a villamosenergia-ágazati kockázatokra való felkészülésről és a 2005/89/EK irányelv hatályon kívül helyezéséről (HL L 158., 2019.6.14., 1. o.).

(6) Az e rendeletben szereplő uniós, tagállami, regionális és szervezeti szintű kiberbiztonsági kockázatértékelések az (EU) 2022/2554 európai parlamenti és tanácsi rendeletben ([4]) meghatározott kibertámadásokból eredő kockázatokra korlátozódhatnak, kizárva ezért például a fizikai támadásokat, a természeti katasztrófákat és a létesítmények vagy emberi erőforrások kiesése miatti üzemszüneteket. A villamos energia területét érintő fizikai támadásokhoz vagy természeti katasztrófákhoz kapcsolódó uniós szintű és regionális kockázatokat más meglévő uniós jogszabályok – többek között az (EU) 2019/941 rendelet 5. cikke vagy a villamosenergia-átviteli hálózat üzemeltetésére vonatkozó iránymutatás megalkotásáról szóló (EU) 2017/1485 bizottsági rendelet ([5]) – már szabályozzák. Hasonlóképpen, a kritikus szervezetek rezilienciájáról szóló (EU) 2022/2557 európai parlamenti és tanácsi irányelv ([6]) célja a kritikus szervezetek sérülékenységeinek csökkentése és fizikai rezilienciájának megerősítése, és kiterjed minden olyan releváns természeti és ember okozta kockázatra, amely hatással lehet az alapvető szolgáltatások nyújtására, beleértve a baleseteket, a természeti katasztrófákat, a népegészségügyi szükséghelyzeteket, így például a világjárványokat és a hibrid fenyegetéseket vagy egyéb ellenséges fenyegetéseket, ideértve a terrorista bűncselekményeket, a bűnözés beszivárgását és a szabotázst.

(7) A „nagy hatású és kritikus hatású szervezetek” e rendeletben szereplő fogalma alapvető fontosságú az e rendeletben ismertetett kötelezettségek hatálya alá tartozó szervezetek körének meghatározásához. A különböző rendelkezésekben felvázolt kockázatalapú megközelítés célja azon folyamatok, támogató eszközök és az ezeket működtető szervezetek azonosítása, amelyek hatással vannak a határkeresztező villamosenergia-áramlásra. Azon hatás mértékétől függően, amelyet az esetleges kibertámadások gyakorolnak az említett szervezeteknek a határkeresztező villamosenergia-áramlásokkal összefüggő műveleteire, e szervezetek „nagy hatásúnak” vagy „kritikus hatásúnak” tekinthetők. Az (EU) 2022/2555 irányelv 3. cikke meghatározza az alapvető és fontos szervezetek fogalmát, valamint az e kategóriákba tartozó szervezetek azonosításának kritériumait. Míg ezek közül sok szervezet egyidejűleg az (EU) 2022/2555 irányelv 3. cikke értelmében vett „alapvető” szervezetnek, e rendelet 24. cikke értelmében pedig nagy hatású vagy kritikus hatású szervezetnek minősül és ilyenként kell azonosítani, az e rendeletben meghatározott kritériumok csak a határkeresztező áramlásokat érintő villamosenergia-folyamatokban betöltött szerepükre és hatásukra vonatkoznak, az (EU) 2022/2555 irányelv 3. cikkében meghatározott kritériumok figyelembevétele nélkül.

(8) Az e rendelet hatálya alá tartozó, az e rendelet 24. cikke értelmében nagy hatásúnak vagy kritikus hatásúnak minősülő és az említett cikkben megállapított kötelezettségek hatálya alá tartozó szervezetek elsősorban azok, amelyek közvetlen hatást gyakorolnak az EU-n belüli határkeresztező villamosenergia-áramlásokra.

(9) Ez a rendelet felhasználja a más jogszabályokban már létrehozott meglévő mechanizmusokat és eszközöket annak érdekében, hogy a célkitűzések elérése során biztosítsa a hatékonyságot, és elkerülje az átfedéseket.

(10) E rendelet alkalmazása során a tagállamoknak, az érintett hatóságoknak és a rendszerüzemeltetőknek figyelembe kell venniük az európai szabványügyi szervezetek által elfogadott európai szabványokat és műszaki előírásokat, továbbá az uniós jogszabályok hatálya alá tartozó termékek forgalomba hozatalára vagy üzembe helyezésére vonatkozó uniós jogszabályokkal összhangban kell eljárniuk.

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

([5]) A Bizottság (EU) 2017/1485 rendelete (2017. augusztus 2.) a villamosenergia-átviteli hálózat üzemeltetésére vonatkozó iránymutatás megalkotásáról (HL L 220., 2017.8.25., 1. o.).

([6]) 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.).

(11) A kiberbiztonsági kockázatok csökkentése érdekében részletes szabálykönyvet kell létrehozni, amely szabályozza a határkeresztező villamosenergia-áramlások kiberbiztonsági szempontjait érintő tevékenységeket folytató érdekelt felek fellépéseit és a közöttük zajló együttműködést, a rendszerbiztonság biztosítása céljából. Ezeknek a szervezeti és technikai szabályoknak kell biztosítaniuk, hogy a kiberbiztonsági kiváltó okokból eredő villamosenergia-biztonsági események többségét operatív szinten hatékonyan kezeljék. Meg kell határozni, hogy az érintett érdekelt feleknek mit kell tenniük az ilyen válságok megelőzése érdekében, és milyen intézkedéseket hozhatnak akkor, ha a rendszerüzemeltetési szabályok önmagukban már nem elegendőek. Ezért közös szabályozási keretet kell létrehozni arra vonatkozóan, hogy miként lehet megelőzni a kiberbiztonsági kiváltó okokból eredő, egyidejű villamosenergia-ellátási válságokat, felkészülni rájuk és kezelni e válságokat. Ez nagyobb átláthatóságot biztosít az előkészítési szakaszban és az egyidejű villamosenergia-ellátási válság idején, és biztosítja, hogy az intézkedéseket a tagállamok illetékes kiberbiztonsági hatóságaival együtt, összehangolt és hatékony módon hozzák meg. A tagállamok és az érintett szervezetek számára elő kell írni, hogy regionális szinten és adott esetben kétoldalúan, a szolidaritás szellemében működjenek együtt. Ezen együttműködés és szabályok célja, hogy alacsonyabb költségek mellett a kiberbiztonsági kockázatokra való jobb felkészültséget érjenek el, összhangban az (EU) 2022/2555 irányelv célkitűzéseivel is. Szükségesnek tűnik továbbá a belső villamosenergia-piac megerősítése a tagállamok közötti bizalom erősítése, különösen a határkeresztező villamosenergia-áramlást érintő indokolatlan korlátozás kockázatának mérséklése révén, ami ezáltal csökkenti a szomszédos tagállamokra gyakorolt negatív továbbgyűrűző hatások kockázatát.

(12) A villamosenergia-ellátás biztonsága megköveteli a tagállamok, uniós intézmények, szervek, hivatalok és ügynökségek, valamint az érdekelt felek közötti hatékony együttműködést. Az elosztórendszer-üzemeltetők és az átvitelirendszer-üzemeltetők az (EU) 2019/944 európai parlamenti és tanácsi irányelv ([7]) 31. és 40. cikkével összhangban kulcsszerepet játszanak a biztonságos, megbízható és hatékony villamosenergia-rendszer biztosításában. A különböző szabályozó hatóságok és más érintett illetékes nemzeti hatóságok az (EU) 2019/944 és az (EU) 2022/2555 irányelv által rájuk ruházott feladataik részeként szintén fontos szerepet játszanak a villamosenergia-ellátás kiberbiztonságának biztosításában és nyomon követésében. A tagállamoknak az e rendelet végrehajtása terén illetékes nemzeti hatóságként ki kell jelölniük egy meglévő vagy új szervezetet azzal a céllal, hogy biztosítsák valamennyi érintett szereplő átlátható és inkluzív részvételét, a rendelet hatékony előkészítését és megfelelő végrehajtását, a villamos energia és a kiberbiztonság terén a különböző érdekelt felek és illetékes hatóságok közötti együttműködést, valamint hogy megkönnyítsék a kiberbiztonsági kiváltó okokból eredő villamosenergia-ellátási válságok megelőzését és utólagos értékelését, valamint az ezekkel kapcsolatos információcserét.

(13) Amennyiben egy nagy hatású vagy kritikus hatású szervezet egynél több tagállamban nyújt szolgáltatásokat, vagy székhelye, egyéb telephelye vagy képviselője valamely tagállamban van, de hálózati és információs rendszerei egy vagy több másik tagállamban találhatók, e tagállamoknak arra kell ösztönözniük illetékes hatóságaikat, hogy tegyenek meg minden tőlük telhetőt annak érdekében, hogy szükség esetén együttműködjenek egymással és segítsék egymást.

(14) A tagállamoknak az e rendeletnek való megfelelés előmozdítása érdekében biztosítaniuk kell, hogy az illetékes hatóságok a nagy hatású és kritikus hatású szervezetek tekintetében rendelkezzenek a szükséges hatáskörökkel. E hatásköröknek lehetővé kell tenniük az illetékes hatóságok számára, hogy helyszíni ellenőrzéseket és helyszínen kívüli felügyeletet végezzenek. Ez magában foglalhatja a véletlenszerű ellenőrzéseket, a rendszeres auditok elvégzését, a kockázatértékelésen alapuló célzott biztonsági ellenőrzéseket vagy a rendelkezésre álló, objektív, megkülönböztetésmentes, tisztességes és átlátható kockázatértékelési kritériumokon alapuló biztonsági átvilágításokat, amelyek a szervezet által elfogadott kiberbiztonsági intézkedések értékeléséhez szükséges információk bekérésére is kiterjedhetnek. Ezeknek az információknak magukban kell foglalniuk a dokumentált kiberbiztonsági szabályzatokat, a hozzáférési adatokat, dokumentumokat vagy a felügyeleti feladataik ellátásához szükséges információkat, valamint a kiberbiztonsági szabályzatok végrehajtásának bizonyítékait, például a képesített ellenőr által végzett biztonsági auditok eredményeit és az azok alapjául szolgáló bizonyítékokat.

([7]) Az Európai Parlament és a Tanács (EU) 2019/944 irányelve (2019. június 5.) a villamos energia belső piacára vonatkozó közös szabályokról és a 2012/27/EU irányelv módosításáról (HL L 158., 2019.6.14., 125. o.).

(15) A nagy hatású és kritikus hatású szervezetekre rótt kiberbiztonsági kockázatkezelési kötelezettségek közötti hézagok vagy átfedések elkerülése érdekében az (EU) 2022/2555 irányelv szerinti nemzeti hatóságoknak és az e rendelet szerinti illetékes hatóságoknak együtt kell működniük a kiberbiztonsági kockázatkezelési intézkedések végrehajtása és az ezen intézkedéseknek való megfelelés nemzeti szintű felügyelete terén. Ha egy szervezet megfelel az e rendeletben meghatározott kiberbiztonsági kockázatkezelési követelményeknek, az (EU) 2022/2555 irányelv szerinti illetékes hatóságok úgy tekinthetik, hogy az biztosítja az említett irányelvben meghatározott megfelelő követelményeknek való megfelelést, vagy fordítva.

(16) Az egyidejű villamosenergia-ellátási válságok megelőzésére és kezelésére vonatkozó közös megközelítés megköveteli, hogy a tagállamok közös egyetértésre jussanak azzal kapcsolatban, hogy miből áll az egyidejű villamosenergia-ellátási válság, és hogy a kibertámadás mikor számít fontos tényezőnek. Különösen meg kell könnyíteni a tagállamok és az érintett szervezetek közötti koordinációt az olyan helyzetek kezelése érdekében, amikor fennáll vagy fenyeget a jelentős villamosenergia-hiány vagy a fogyasztók villamosenergia-ellátása lehetetlenségének potenciális kockázata, és ez kibertámadásnak tulajdonítható.

(17) Az (EU) 2019/881 európai parlamenti és tanácsi rendelet ([8]) (1) preambulumbekezdése elismeri, hogy a hálózati és információs rendszerek és a távközlési hálózatok és szolgáltatások létfontosságú szerepet töltenek be a gazdaság olajozott működésének biztosításában olyan meghatározó ágazatokban, mint az energiaügy, míg a (44) preambulumbekezdés kifejti, hogy az Európai Uniós Kiberbiztonsági Ügynökségnek (ENISA) kapcsolatot kell kialakítania az Energiaszabályozók Európai Uniós Együttműködési Ügynökségével (ACER).

(18) Az (EU) 2019/943 rendelet konkrét kiberbiztonsági feladatokat ruház az átvitelirendszer-üzemeltetőkre és az elosztórendszer-üzemeltetőkre. Európai szövetségeik, nevezetesen a villamosenergia-piaci átvitelirendszer-üzemeltetők európai hálózata (a továbbiakban: villamosenergia-piaci ENTSO) és az elosztórendszer-üzemeltetők európai szervezete (a továbbiakban: EU DSO) az említett rendelet 30., illetve 55. cikke értelmében az érintett hatóságokkal és szabályozott szervezetekkel együttműködve előmozdítják a kiberbiztonságot.

(19) A kiberbiztonsági kiváltó okokból eredő, egyidejű villamosenergia-ellátási válságok megelőzésére és kezelésére vonatkozó közös megközelítés azt is megköveteli, hogy valamennyi érdekelt fél harmonizált módszereket és fogalommeghatározásokat alkalmazzon a villamosenergia-ellátás kiberbiztonságával kapcsolatos kockázatok azonosítására. Azt is megköveteli, hogy képesek legyenek hatékonyan összehasonlítani, hogy ők és szomszédaik mennyire teljesítenek jól ezen a területen. Ezért meg kell határozni a határkeresztező villamosenergia-áramlást érintő kiberbiztonsági kockázatokhoz igazított kockázatkezelési módszerek, eseményminősítési skálák és kiberbiztonsági intézkedések kidolgozására és aktualizálására szolgáló folyamatokat, szerepeket és felelősségi köröket.

(20) A tagállamok az e rendelet tekintetében kijelölt illetékes hatóságon keresztül felelősek azon szervezetek azonosításáért, amelyek megfelelnek a nagy hatású és kritikus hatású szervezetnek minősítés kritériumainak. A tagállamok között e tekintetben mutatkozó eltérések kiküszöbölése, valamint az összes érintett szervezet vonatkozásában a kiberbiztonsági kockázatkezelési intézkedések és a jelentéstételi kötelezettségek tekintetében, a jogbiztonság biztosítása érdekében egy olyan kritériumrendszert kell megállapítani, amely meghatározza az e rendelet hatálya alá tartozó szervezeteket. Ezeket a kritériumokat meg kell határozni és rendszeresen aktualizálni kell az e rendeletben meghatározott feltételek és módszertanok kidolgozása és elfogadása révén.

(21) E rendelet rendelkezései nem sérthetik az információs és kommunikációs technológiai (IKT) termékek, az IKT-szolgáltatások és az IKT-folyamatok tanúsítására vonatkozó különös szabályokat előíró uniós jogot, különösen az európai kiberbiztonsági tanúsítási rendszerek létrehozásának kerete tekintetében az (EU) 2019/881 rendeletet. E rendelet összefüggésében az IKT-termékeknek magukban kell foglalniuk az elektrotechnikai hálózattal való közvetlen interakciót lehetővé tevő műszaki eszközöket és szoftvereket is, különösen az energiaátvitelre, az energiaelosztásra és az energiatermelésre, valamint a kapcsolódó információk gyűjtésére és továbbítására használható ipari vezérlőrendszereket. A rendelkezéseknek biztosítaniuk kell, hogy a beszerzendő IKT-termékek, IKT-szolgáltatások és IKT-folyamatok teljesítsék az (EU) 2019/881 rendelet 51. cikkében foglalt releváns biztonsági célkitűzéseket.

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

(22) A közelmúltbeli kibertámadások azt mutatják, hogy a szervezetek egyre inkább az ellátási láncok ellen elkövetett támadások célpontjává válnak. Az ellátási láncok ellen elkövetett támadások nemcsak az e rendelet hatálya alá tartozó egyes szervezetekre gyakorolnak hatást, hanem továbbgyűrűző hatást gyakorolhatnak az olyan szervezetek elleni nagyobb támadásokra is, amelyekhez a villamosenergia-hálózatban csatlakoznak. Ezért a szöveg olyan rendelkezésekkel és ajánlásokkal egészült ki, amelyek elősegítik az ellátási lánccal összefüggő folyamatokhoz – különösen a közbeszerzéshez – kapcsolódó kiberbiztonsági kockázatok enyhítését, és amelyek hatással vannak a határkeresztező villamosenergia-áramlásokra.

(23) mivel a hálózati és információs rendszerek sérülékenységeinek kiaknázása az energiaellátásban jelentős zavarokat, a gazdaságnak és a fogyasztóknak pedig jelentős károkat okozhat, ezeket a sebezhetőségeket a kockázatok csökkentése érdekében gyorsan fel kell tárni és orvosolni kell. E rendelet eredményes végrehajtásának elősegítése érdekében az érintett szervezeteknek és illetékes hatóságoknak együtt kell működniük az e célból megfelelőnek ítélt tevékenységek gyakorlása és tesztelése érdekében, beleértve a kiberfenyegetésekre, kibertámadásokra, sérülékenységekre, eszközökre és módszerekre, taktikákra, technikákra és eljárásokra, kiberbiztonsági válságkezelési felkészültségre és egyéb gyakorlatokra vonatkozó információcserét. Mivel a technológia folyamatosan fejlődik, és a villamosenergia-ágazat digitalizációja gyors ütemben halad, az elfogadott rendelkezések végrehajtása nem veszélyeztetheti az innovációt, és nem akadályozhatja a villamosenergia-piachoz való hozzáférést, valamint a villamosenergia-rendszer hatékonyságához és fenntarthatóságához hozzájáruló innovatív megoldások későbbi alkalmazását.

(24) Az e rendelet végrehajtásának nyomon követése céljából gyűjtött információkat a szükséges ismeret elvének értelmében észszerű mértékben korlátozni kell. Az érdekelt felek számára teljesíthető és hatékony határidőket kell biztosítani az ilyen információk benyújtására. El kell kerülni a kettős értesítést.

(25) A kiberbiztonsági védelem nem ér véget az Unió határain. Biztonságos rendszer létrehozásához a szomszédos harmadik országok bevonására is szükség van. Az Uniónak és tagállamainak törekedniük kell arra, hogy támogassák az e rendeletben meghatározottakhoz hasonló kiberbiztonsági szabályok alkalmazásában azokat a szomszédos harmadik országokat, amelyek villamosenergia-infrastruktúrája az európai hálózathoz csatlakozik.

(26) A biztonsági koordináció mielőbbi javítása, valamint a jövőbeli kötelező feltételek és módszertanok tesztelése érdekében a villamosenergia-piaci ENTSO-nak, az EU DSO-nak és az illetékes hatóságoknak közvetlenül e rendelet hatálybalépését követően meg kell kezdeniük egy nem kötelező erejű iránymutatás kidolgozását. Ez az iránymutatás alapul szolgál majd a jövőbeli feltételek és módszertanok kidolgozásához. Ezzel párhuzamosan az illetékes hatóságoknak azonosítaniuk kell azokat a szervezeteket, amelyek nagy és kritikus hatású szervezetté minősíthetők és önkéntes alapon kezdik meg a kötelezettségek teljesítését.

(27) Ez a rendelet az Energiaszabályozók Európai Uniós Együttműködési Ügynökségével (ACER), az ENISA-val, a villamosenergia-piaci ENTSO-val, az EU DSO-val és egyéb érdekelt felekkel való szoros együttműködés keretében került kidolgozásra a hatékony, kiegyensúlyozott és arányos szabályok átlátható és a részvételt elősegítő módon történő elfogadása érdekében.

(28) Ez a rendelet kiegészíti és megerősíti az (EU) 2017/1584 bizottsági ajánlásban ([9]) meghatározott uniós kiberbiztonsági válságreagálási keretben megállapított válságkezelési intézkedéseket. Egy esetleges kibertámadás az (EU) 2019/941 rendelet 2. cikkének 9. pontjában meghatározott villamosenergia-ellátási válságot is okozhat, hozzájárulhat ahhoz, vagy egybeeshet azzal, amely befolyásolhatja a határkeresztező villamosenergia-áramlást. Ez a villamosenergia-ellátási válság az (EU) 2019/941 rendelet 2. cikkének 10. pontjában meghatározott egyidejű villamosenergia-ellátási válsághoz vezethet. Egy ilyen biztonsági esemény egyéb, a villamosenergia-ellátás biztonságától függő ágazatokra is hatással lehet. Amennyiben egy ilyen esemény az (EU) 2022/2555 irányelv 16. cikke értelmében vett nagyszabású kiberbiztonsági eseménnyé eszkalálódik, az említett cikknek az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatának (a továbbiakban: EU-CyCLONe) létrehozásáról szóló rendelkezéseit kell alkalmazni. Az uniós szintű válságkezelés során az érintett feleknek az (EU) 2018/1993 tanácsi végrehajtási határozat ([10]) szerinti uniós politikai szintű integrált válságelhárítási mechanizmusra (IPCR-mechanizmus) kell támaszkodniuk.

(29) Ez a rendelet nem érinti a tagállamok azon hatáskörét, hogy az uniós joggal összhangban meghozzák alapvető biztonsági érdekeik védelme, a közrend és a közbiztonság védelme, valamint a bűncselekmények kivizsgálásának, felderítésének és üldözésének lehetővé tétele érdekében szükséges intézkedéseket. Az EUMSZ 346. cikke értelmében egyetlen tagállam sem köteles olyan információt szolgáltatni, amelynek közlését ellentétesnek tartja alapvető biztonsági érdekeivel.

([9]) 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.).

([10]) 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.).

(30) Jóllehet ez a rendelet elvben az atomerőművekből származó villamos energia előállításával kapcsolatos tevékenységeket végző szervezetekre is alkalmazandó, e tevékenységek némelyike nemzetbiztonsági vonatkozású lehet.

(31) A személyes adatok e rendelet szerinti bármely kezelésére alkalmazni kell az adatvédelemre és a magánélet védelmére vonatkozó uniós jogot. Ez a rendelet nem érinti különösen az (EU) 2016/679 európai parlamenti és tanácsi rendeletet ([11]), a 2002/58/EK európai parlamenti és tanácsi irányelvet ([12]) és az (EU) 2018/1725 európai parlamenti és tanácsi rendeletet ([13]). Ez a rendelet ezért nem érintheti többek között az adatvédelemre és a magánélet védelmére vonatkozó, alkalmazandó uniós jognak való megfelelés nyomon követése terén illetékes hatóságok feladatait és hatásköreit.

(32) Tekintettel a kiberbiztonsággal kapcsolatos nemzetközi együttműködés fontosságára, az e rendelet alapján rájuk ruházott feladatok végrehajtásáért felelős és a tagállamok által kijelölt illetékes hatóságok számára lehetővé kell tenni, hogy részt vegyenek a nemzetközi együttműködési hálózatokban. Ezért az illetékes hatóságok számára feladataik ellátása céljából lehetővé kell tenni, hogy információkat – többek között személyes adatokat – cseréljenek harmadik országok illetékes hatóságaival, feltéve, hogy teljesülnek a személyes adatok harmadik országokba történő továbbítására vonatkozó uniós adatvédelmi jog szerinti, többek között az (EU) 2016/679 rendelet 49. cikkében foglalt feltételek.

(33) A személyes adatok kezelése – az eszközök biztonságának a nagy hatású vagy kritikus hatású szervezetek általi biztosítása céljából szükséges és arányos mértékben – jogszerűnek tekinthető azon az alapon, hogy az adatkezelés az (EU) 2016/679 rendelet 6. cikke (1) bekezdésének c) pontjában és 6. cikkének (3) bekezdésében foglalt követelményekkel összhangban megfelel az adatkezelőre vonatkozó jogi kötelezettségnek. A személyes adatok kezelése a nagy hatású vagy kritikus hatású szervezetek, valamint az e szervezetek nevében eljáró, biztonsági technológiákat és szolgáltatásokat nyújtó szolgáltatók jogos érdekei miatt is szükséges lehet az (EU) 2016/679 rendelet 6. cikke (1) bekezdésének f) pontja értelmében, ideértve azt az esetet is, amikor az adatkezelés kiberbiztonsági információmegosztási megállapodásokhoz vagy a releváns információk e rendelettel összhangban történő önkéntes bejelentéséhez szükséges. A kibertámadások megelőzésével, észlelésével, azonosításával, megfékezésével, elemzésével és az azokra való reagálással kapcsolatos intézkedések, a konkrét kiberfenyegetésekkel kapcsolatos tudatosság növelését célzó intézkedések, a sérülékenységek elhárításával és az összehangolt közzététellel kapcsolatos információmegosztás, valamint az ezekre a kibertámadásokra, valamint a kiberfenyegetésekre és sérülékenységekre, a fertőzöttségi mutatókra, taktikákra, technikákra és eljárásokra, kiberbiztonsági figyelmeztetésekre és konfigurációs eszközökre vonatkozó önkéntes információmegosztás szükségessé teheti a személyes adatok bizonyos kategóriáinak, például IP-címeknek, egységes forrásazonosítóknak (URL-ek), doménneveknek, e-mail-címeknek, és – amennyiben személyes adatokat fednek fel – időbélyegzőknek a kezelését. A személyes adatok illetékes hatóságok, egyedüli kapcsolattartó pontok és CSIRT-ek általi kezelése az (EU) 2016/679 rendelet 6. cikke (1) bekezdésének c) vagy e) pontja és 6. cikkének (3) bekezdése értelmében jogi kötelezettségnek minősülhet, vagy közérdekűnek vagy szükségesnek tekinthető az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához vagy a nagy hatású vagy kritikus hatású szervezeteknek az említett rendelet 6. cikke (1) bekezdésének f) pontjában említett jogos érdekének érvényesítéséhez. Ezen túlmenően a nemzeti jog megállapíthat olyan szabályokat, amelyek lehetővé teszik az illetékes hatóságok, az egyedüli kapcsolattartó pontok és a CSIRT-ek számára, hogy a nagy hatású vagy kritikus hatású szervezetek hálózati és információs rendszerei biztonságának biztosítása céljából szükséges és arányos mértékben az (EU) 2016/679 rendelet 9. cikkével összhangban kezeljék a személyes adatok különleges kategóriáit, különösen azáltal, hogy megfelelő és konkrét intézkedéseket írnak elő a természetes személyek alapvető jogainak és érdekeinek védelme érdekében, beleértve az ilyen adatok további felhasználására vonatkozó technikai korlátozásokat, valamint a legkorszerűbb biztonsági és adatvédelmi intézkedések alkalmazását, például az álnevesítést vagy titkosítást, amennyiben az anonimizálás jelentősen befolyásolhatja a kitűzött célt.

([11]) Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.).

([12]) Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv) (HL L 201., 2002.7.31., 37. o.).

([13]) Az Európai Parlament és a Tanács (EU) 2018/1725 rendelete (2018. október 23.) a természetes személyeknek a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelése tekintetében való védelméről és az ilyen adatok szabad áramlásáról, valamint a 45/2001/EK rendelet és az 1247/2002/EK határozat hatályon kívül helyezéséről (HL L 295., 2018.11.21., 39. o.).

(34) A kibertámadások következtében sok esetben személyes adatok kerülnek veszélybe. Ebben az összefüggésben az illetékes hatóságoknak minden releváns kérdésben együtt kell működniük és információt kell cserélniük az (EU) 2016/679 rendeletben és a 2002/58/EK irányelvben említett hatóságokkal.

(35) Az európai adatvédelmi biztossal az (EU) 2018/1725 rendelet 42. cikkének (1) bekezdésével összhangban konzultációra került sor, és a biztos 2023. november 17-én véleményt nyilvánított.

ELFOGADTA EZT A RENDELETET:

I. FEJEZET

ÁLTALÁNOS RENDELKEZÉSEK

1. cikk

Tárgy

Ez a rendelet létrehozza az üzemi és kereskedelmi szabályzatot, amely ágazatspecifikus szabályokat állapít meg a határkeresztező villamosenergia-áramlások kiberbiztonsági szempontjaira vonatkozóan, ideértve a közös minimumkövetelményekre, a tervezésre, a nyomon követésre, a jelentéstételre és a válságkezelésre vonatkozó szabályokat.

2. cikk

Hatály

(1) Ez a rendelet a határkeresztező villamosenergia-áramlás kiberbiztonsági szempontjaira alkalmazandó a következő szervezetek tevékenységei során, amennyiben e szervezetek a 24. cikkel összhangban nagy hatású vagy kritikus hatású szervezetnek minősülnek:

a) az (EU) 2019/944 irányelv 2. cikke 57. pontjában meghatározott villamosenergia-ipari vállalkozások;

b) az (EU) 2019/943 rendelet 2. cikkének 8. pontjában meghatározott kijelölt villamosenergiapiac-üzemeltetők;

c) az 1348/2014/EU bizottsági végrehajtási rendelet ([14]) 2. cikkének 4. pontjában meghatározott szervezett kereskedési helyek vagy „szervezett piacok”, amelyek a határkeresztező villamosenergia-áramlás szempontjából releváns termékekkel kapcsolatos ügyleteket bonyolítanak le;

d) az e rendelet 3. cikkének 9. pontjában említett kritikus IKT-szolgáltatók;

e) az (EU) 2019/943 rendelet 28. cikke alapján létrehozott villamosenergia-piaci ENTSO;

f) az (EU) 2019/943 rendelet 52. cikke alapján létrehozott EU DSO;

g) az (EU) 2019/943 rendelet 2. cikkének 14. pontjában meghatározott mérlegkörfelelősök;

h) az (EU) 2022/2555 irányelv I. mellékletében meghatározott elektromos töltőpontok üzemeltetői;

i) az (EU) 2019/943 rendelet 35. cikke alapján létrehozott regionális koordinációs központok;

j) az (EU) 2022/2555 irányelv 6. cikkének 40. pontjában meghatározott irányított biztonsági szolgáltatók (MSSP);

k) bármely más szervezet vagy harmadik fél, amelyre e rendelet alapján feladatokat ruháztak.

(2) Aktuális megbízatásuk részeként a következő hatóságok felelősek az e rendeletben meghatározott feladatok végrehajtásáért:

a) az (EU) 2019/942 európai parlamenti és tanácsi rendelettel ([15]) létrehozott Energiaszabályozók Európai Uniós Együttműködési Ügynöksége (ACER);

b) az e rendelet alapján rájuk ruházott feladatok végrehajtásáért felelős és a tagállamok által a 4. cikk alapján kijelölt illetékes nemzeti hatóságok vagy „illetékes hatóság”;

c) az egyes tagállamok által az (EU) 2019/944 irányelv 57. cikkének (1) bekezdése alapján kijelölt nemzeti szabályozó hatóságok;

([14]) A Bizottság 1348/2014/EU végrehajtási rendelete (2014. december 17.) a nagykereskedelmi energiapiacok integritásáról és átláthatóságáról szóló 1227/2011/EU európai parlamenti és tanácsi rendelet 8. cikke (2) és (6) bekezdésének végrehajtására irányuló adatszolgáltatásról (HL L 363., 2014.12.18., 121. o.).

([15]) Az Európai Parlament és a Tanács (EU) 2019/942 rendelete (2019. június 5.) az Energiaszabályozók Európai Uniós Együttműködési Ügynökségének létrehozásáról (HL L 158., 2019.6.14., 22. o.).

d) az (EU) 2019/941 rendelet 3. cikke alapján létrehozott, a kockázati készültség tekintetében illetékes hatóságok;

e) az (EU) 2022/2555 irányelv 10. cikke alapján kijelölt vagy létrehozott számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek);

f) az (EU) 2022/2555 irányelv 8. cikke alapján kijelölt vagy létrehozott, kiberbiztonságért felelős illetékes hatóságok;

g) az (EU) 2019/881 rendelet alapján létrehozott Európai Uniós Kiberbiztonsági Ügynökség;

h) bármely más hatóság vagy harmadik fél, amelyre 4. cikk (3) bekezdése alapján feladatokat ruháztak.

(3) Ez a rendelet minden olyan szervezetre is alkalmazandó, amely nem az Unióban telepedett le, de az Unióban működő szervezeteknek nyújt szolgáltatásokat, feltéve, hogy azokat az illetékes hatóságok a 24. cikk (2) bekezdésével összhangban nagy vagy kritikus hatású szervezetként azonosították.

(4) Ez a rendelet nem érinti a tagállamoknak a nemzetbiztonság védelmével kapcsolatos felelősségét és az egyéb alapvető állami funkciók védelmére vonatkozó hatáskörét, beleértve az állam területi integritásának biztosítását és a közrend fenntartását.

(5) Ez a rendelet nem érinti a tagállamok azon felelősségét, hogy a Szerződésekkel összhangban megvédjék a nemzetbiztonságot az atomerőművekből származó villamos energia termelésével kapcsolatos tevékenységek tekintetében, beleértve a nukleáris értékláncon belüli tevékenységeket is.

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

3. cikk

Fogalommeghatározások

A következő fogalommeghatározásokat kell alkalmazni:

1. „eszköz”: a hálózati és információs rendszerek minden olyan – fizikai vagy immateriális – információja, szoftvere vagy hardvere, amely egy egyén, szervezet vagy kormány számára értéket képvisel;

2. „kockázati készültség tekintetében illetékes hatóság”: az (EU) 2019/941 rendelet 3. cikke alapján kijelölt illetékes hatóság;

3. „számítógép-biztonsági eseményekre reagáló csoport”: az (EU) 2022/2555 irányelv 10. cikk értelmében a kockázatok és események kezeléséért felelős csoport;

4. „kritikus hatású eszköz”: kritikus hatású folyamat végrehajtásához szükséges eszköz;

5. „kritikus hatású szervezet”: olyan szervezet, amely kritikus hatású folyamatot hajt végre, és amelyet az illetékes hatóságok a 24. cikkel összhangban ilyenként azonosítanak;

6. „kritikus hatású hatókör”: a 2. cikk (1) bekezdésében említett szervezet által meghatározott hatókör, amely magában foglalja az összes kritikus hatású eszközt, és amelyben az ezen eszközökhöz való hozzáférés ellenőrizhető, és amely a fejlett kiberbiztonsági ellenőrzések hatókörét meghatározza;

7. „kritikus hatású folyamat”: olyan szervezet által végzett üzleti folyamat, amelynek esetében a villamos energia kiberbiztonsági hatásmutatói meghaladják a kritikus hatásra vonatkozó küszöbértéket;

8. „kritikus hatásra vonatkozó küszöbérték”: a 19. cikk (3) bekezdésének b) pontjában említett, a villamos energia kiberbiztonsági hatásmutatóinak azon értékei, amelyek felett az üzleti folyamatokra irányuló kibertámadás kritikus zavarokat okoz a határkeresztező villamosenergia-áramlásban;

9. „kritikus IKT-szolgáltató”: olyan szervezet, amely olyan IKT-szolgáltatást vagy IKT-folyamatot nyújt, amely a határkeresztező villamosenergia-áramlás kiberbiztonsági szempontjait érintő kritikus hatású vagy nagy hatású folyamathoz szükséges, és amely veszélyeztetés esetén olyan kibertámadást okozhat, amelynek hatása meghaladja a kritikus hatásra vagy nagy hatásra vonatkozó küszöbértéket;

10. „határkeresztező villamosenergia-áramlás”: az (EU) 2019/943 rendelet 2. cikkének 3. pontjában meghatározott határkeresztező áramlás;

11. „kibertámadás”: az (EU) 2022/2554 rendelet 14. cikkének 3. pontjában meghatározott biztonsági esemény;

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

13. „kiberbiztonsági ellenőrzés”: a kiberbiztonsági kockázatok elkerülése, észlelése, ellensúlyozása vagy minimalizálása céljából végrehajtott intézkedések vagy eljárások;

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

15. „kiberbiztonsági irányítási rendszer”: valamely szervezet által együttesen kezelt politikák, eljárások, iránymutatások, valamint a kapcsolódó erőforrások és tevékenységek, amelyek célja, hogy a szervezet információs eszközeit megvédje a kiberfenyegetésekkel szemben, és amelynek során szisztematikusan létrehozzák, megvalósítják, működtetik, nyomon követik, felülvizsgálják, fenntartják és javítják a szervezet hálózati és információs rendszereinek biztonságát;

16. „kiberbiztonsági műveleti központ”: olyan külön erre a célra létrehozott központ, ahol egy vagy több szakértőből álló, kiberbiztonsági informatikai rendszerek által támogatott technikai csoport biztonsági vonatkozású feladatokat (kiberbiztonsági műveleti központi [CSOC] szolgáltatások) lát el, mint például a kibertámadások és a biztonsági konfigurációs hibák kezelése, a biztonsági nyomon követés, naplóelemzés és a kibertámadások észlelése;

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

18. „kiberbiztonsági sérülékenység-menedzsment”: a sérülékenységek azonosításának és kezelésének gyakorlata;

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

20. „korai figyelmeztető jelzés”: annak jelzéséhez szükséges információ, hogy a jelentős biztonsági eseményt gyaníthatóan jogellenes vagy rosszindulatú cselekmény okozta-e, illetve hogy járhat-e határokon átnyúló hatással;

21. „a villamos energia kiberbiztonsági hatásmutatója” (ECII): olyan mutató vagy besorolási skála, amely rangsorolja a kibertámadásoknak a határkeresztező villamosenergia-áramlásokkal kapcsolatos üzleti folyamatokra gyakorolt lehetséges következményeit;

22. „európai kiberbiztonsági tanúsítási rendszer”: az (EU) 2019/881 rendelet 2. cikkének 9. pontjában meghatározott rendszer;

23. „nagy hatású szervezet”: olyan szervezet, amely nagy hatású folyamatot hajt végre, és amelyet az illetékes hatóságok a 24. cikkel összhangban ilyenként azonosítanak;

24. „nagy hatású folyamat”: olyan szervezet által végzett bármely üzleti folyamat, amelynek esetében a villamos energia kiberbiztonsági hatásmutatói meghaladják a nagy hatásra vonatkozó küszöbértéket;

25. „nagy hatású eszköz”: nagy hatású folyamat végrehajtásához szükséges eszköz;

26. „nagy hatásra vonatkozó küszöbérték”: a 19. cikk (3) bekezdésének b) pontjában említett, a villamos energia kiberbiztonsági hatásmutatóinak azon értékei, amelyek felett a valamely folyamatra irányuló sikeres kibertámadás nagy zavarokat okoz a határkeresztező villamosenergia-áramlásokban;

27. „nagy hatású hatókör”: a 2. cikk (1) bekezdésében felsorolt bármely szervezet által meghatározott hatókör, amely magában foglalja az összes nagy hatású eszközt, és amelyben az ezen eszközökhöz való hozzáférés ellenőrizhető, és amely a minimális kiberbiztonsági ellenőrzések hatókörét meghatározza;

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

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

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

31. „elavult rendszer”: az (EU) 2022/2554 rendelet 3. cikkének 3. pontjában meghatározott elavult IKT-rendszer;

32. „nemzeti egyedüli kapcsolattartó pont”: az egyes tagállamok által az (EU) 2022/2555 irányelv 8. cikkének (3) bekezdése alapján kijelölt vagy létrehozott egyedüli kapcsolattartó pont;

33. „kiberválságok kezelésével foglalkozó hatóságok”: az (EU) 2022/2555 irányelv 9. cikkének 1. pontja alapján kijelölt vagy létrehozott hatóságok;

34. „kezdeményező”: olyan szervezet, amely információcserét, információmegosztást vagy információtárolási eseményt kezdeményez;

35. „közbeszerzési kiírási feltételek”: azok a kiírási feltételek, amelyeket a szervezetek új vagy aktualizált IKT-termékek, IKT-folyamatok vagy IKT-szolgáltatások beszerzéséhez határoznak meg;

36. „képviselő”: az Unióban letelepedett természetes vagy jogi személy, akit vagy amelyet kifejezetten arra jelöltek ki, hogy egy, nem az Unióban letelepedett, de uniós szervezetek részére szolgáltatásokat nyújtó, nagy vagy kritikus hatású szervezet nevében eljárjon, és akihez vagy amelyhez az illetékes hatóság vagy a CSIRT a nagy vagy kritikus hatású szervezet helyett fordulhat az adott szervezetnek az e rendelet szerinti kötelezettségei tekintetében;

37. „kockázat”: az (EU) 2022/2555 irányelv 6. cikkének 9. pontjában meghatározott kockázat;

38. „kockázati hatásmátrix”: a kockázatértékelés során az egyes értékelt kockázatokhoz kapcsolódó kockázati hatásszint meghatározására használt mátrix;

39. „egyidejű villamosenergia-ellátási válság”: az (EU) 2019/941 rendelet 2. cikkének 10. pontjában meghatározott villamosenergia-ellátási válság;

40. „szervezeti szintű egyedüli kapcsolattartó pont”: a 38. cikk (1) bekezdés c) pontja értelmében kijelölt, szervezeti szintű egyedüli kapcsolattartó pont;

41. „érdekelt fél”: bármely olyan fél, amely érdekelt egy szervezet vagy folyamat sikerességében és folyamatos működésében, mint például az alkalmazottak, igazgatók, részvényesek, szabályozók, egyesületek, beszállítók és ügyfelek;

42. „szabvány”: az 1025/2012/EU európai parlamenti és tanácsi rendelet ([16]) 2. cikke 1. pontjában meghatározott szabvány;

43. „rendszerüzemeltetési régió”: az (EU) 2019/943 rendelet 36. cikkével összhangban létrehozott, a rendszerüzemeltetési régiók meghatározásáról szóló 05–2022. számú ACER-határozat I. mellékletében meghatározott rendszerüzemeltetési régiók;

44. „rendszer-üzemeltetők”: az (EU) 2019/944 irányelv 2. cikkének 29. pontjában és 2. cikkének 35. pontjában meghatározott elosztórendszer-üzemeltető és átvitelirendszer-üzemeltető;

45. „az Unió egészére kiterjedő kritikus hatású folyamat”: minden olyan villamosenergia-ágazati folyamat, amelyben esetleg több szervezet vesz részt, és amely esetében a kibertámadás lehetséges hatása az uniós szintű kiberbiztonsági kockázatértékelés elvégzése során kritikusnak tekinthető;

46. „az Unió egészére kiterjedő nagy hatású folyamat”: bármely villamosenergia-ágazati folyamat, amelyben esetleg több szervezet vesz részt, és amely esetében a kibertámadás lehetséges hatása az uniós szintű kiberbiztonsági kockázatértékelés elvégzése során nagynak tekinthető;

47. „kijavítatlan, aktívan kihasznált sérülékenység”: olyan sérülékenység, amelyet még nem hoztak nyilvánosságra és nem javítottak ki, és amelyre vonatkozóan megbízható bizonyíték van arra, hogy egy szereplő rosszindulatú kódot futtatott egy rendszerben a rendszer tulajdonosának engedélye nélkül;

48. „sérülékenység”: az (EU) 2022/2555 irányelv 6. cikkének 15. pontjában meghatározott sérülékenység.

4. cikk

Illetékes hatóság

(1) A lehető leghamarabb, de legkésőbb 2024. december 13-án minden tagállam kijelöli az e rendeletben ráruházott feladatok végrehajtásáért felelős nemzeti kormányzati vagy szabályozó hatóságot (a továbbiakban: illetékes hatóság). Amíg az illetékes hatóságot nem bízzák meg az e rendelet szerinti feladatok ellátásával, az egyes tagállamok által az (EU) 2019/944 irányelv 57. cikkének (1) bekezdése alapján kijelölt szabályozó hatóság látja el az e rendelet értelmében vett illetékes hatóság feladatait.

(2) A tagállamok haladéktalanul értesítik a Bizottságot, az ACER-t, az ENISA-t, az (EU) 2022/2555 irányelv 14. cikke alapján létrehozott hálózat- és információbiztonsági együttműködési csoportot és a 2012. november 15-i bizottsági határozat ([17]) 1. cikke alapján létrehozott villamosenergia-ügyi koordinációs csoportot, és közlik velük az e cikk (1) bekezdése szerint kijelölt illetékes hatóságuk nevét és elérhetőségét, valamint ezen adatok minden későbbi változását.

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

([17]) A Bizottság határozata (2012. november 15.) a villamosenergia-ügyi koordinációs csoport felállításáról (2012/C 353/02) (HL C 353., 2012.11.17., 2. o.).

(3) A tagállamok engedélyezhetik illetékes hatóságuk számára, hogy az e rendeletben rábízott feladatokat – az 5. cikkben felsorolt feladatok kivételével – más nemzeti hatóságokra ruházza át. Minden illetékes hatóság nyomon követi e rendelet azon hatóságok általi alkalmazását, amelyekre feladatokat ruházott át. Az illetékes hatóság közli a Bizottsággal, az ACER-rel, a villamosenergia-ügyi koordinációs csoporttal, az ENISA-val és a Kiberbiztonsági Együttműködési Csoporttal azon hatóságok nevét, elérhetőségét, hozzárendelt feladatait és azok későbbi változásait, amelyekre feladatokat ruházott át.

5. cikk

Együttműködés a nemzeti szintű érintett hatóságok és szervek között

Az illetékes hatóságok az e rendeletben meghatározott releváns kötelezettségek teljesítése céljából koordinálják és biztosítják a kiberbiztonságért felelős illetékes hatóságok, a kiberválságok kezelésével foglalkozó hatóságok, a nemzeti szabályozó hatóságok, a kockázatokra való felkészültségért felelős illetékes hatóságok és a CSIRT-ek közötti megfelelő együttműködést. Az illetékes hatóságok a hatékony eljárások biztosítása, valamint a feladatok és kötelezettségek megkettőzésének elkerülése érdekében az egyes tagállamok által megnevezett egyéb szervekkel vagy hatóságokkal is egyeztetnek. Az illetékes hatóságok utasíthatják az érintett nemzeti szabályozó hatóságokat, hogy kérjék ki az ACER véleményét a 8. cikk (3) bekezdése szerint.

6. cikk

Feltételek vagy módszertanok vagy tervek

(1) Az átvitelirendszer-üzemeltetők az EU DSO-val együttműködve javaslatokat dolgoznak ki a (2) bekezdés szerinti feltételekre vagy módszertanokra, illetve a (3) bekezdés szerinti tervekre vonatkozóan.

(2) A következő feltételeket vagy módszertanokat és azok módosításait valamennyi illetékes hatóságnak jóvá kell hagynia:

a) a 18. cikk (1) bekezdése szerinti kiberbiztonsági kockázatértékelési módszertanok;

b) a 23. cikk szerinti, a határkeresztező villamos energia kiberbiztonsági kockázatértékeléséről szóló átfogó jelentés;

c) a 29. cikk szerinti minimális és fejlett kiberbiztonsági ellenőrzések, a 34. cikk szerinti, a villamos energia kiberbiztonsági ellenőrzéseinek a szabványok alapján történő feltérképezés, beleértve a 33. cikk szerinti, minimális és fejlett kiberbiztonsági ellenőrzéseket;

d) a 35. cikk szerinti kiberbiztonsági beszerzési ajánlás;

e) a 37. cikk (8) bekezdése szerinti, a kibertámadások besorolási skálájának módszertana.

(3) A 22. cikk szerinti regionális kiberbiztonsági kockázatcsökkentési tervekre vonatkozó javaslatokat az érintett rendszerüzemeltetési régió valamennyi illetékes hatóságának jóvá kell hagynia.

(4) A (2) bekezdésben felsorolt feltételekre, módszertanokra vagy a (3) bekezdésben felsorolt tervekre vonatkozó javaslatok tartalmazzák a végrehajtásuk javasolt időkeretét és az e rendelet célkitűzéseire gyakorolt várható hatásuk leírását.

(5) Az EU DSO a feltételekre vagy módszertanokra, illetve a tervekre vonatkozó javaslat illetékes hatóságokhoz történő benyújtására megadott határidő előtt legkésőbb 3 héttel indokolással ellátott véleményt adhat ki az érintett átvitelirendszer-üzemeltetőknek. A feltételekre vagy módszertanokra, illetve a tervekre vonatkozó javaslatért felelős átvitelirendszer-üzemeltetők az illetékes hatóságok általi jóváhagyás céljából történő benyújtás előtt figyelembe veszik az EU DSO indokolással ellátott véleményét. Az átvitelirendszer-üzemeltetők indoklást adnak arról, ha az EU DSO véleményét nem veszik figyelembe.

(6) A feltételek, módszertanok és tervek közös kidolgozása során a részt vevő átvitelirendszer-üzemeltetők szorosan együttműködnek egymással. Az átvitelirendszer-üzemeltetők a villamosenergia-piaci ENTSO segítségével és az EU DSO-val együttműködve rendszeresen tájékoztatják az illetékes hatóságokat és az ACER-t a feltételek vagy módszertanok, illetve a tervek kidolgozásának előrehaladásáról.

7. cikk

A szavazás szabályai az átvitelirendszer-üzemeltetőknél

(1) Amennyiben a feltételekre vagy módszertanokra vonatkozó javaslatokról döntő átvitelirendszer-üzemeltetők nem tudnak megállapodásra jutni, minősített többségi szavazással döntenek. Az ilyen javaslatok esetében a minősített többséget a következőképpen kell kiszámítani:

a) a tagállamok legalább 55 %-át képviselő átvitelirendszer-üzemeltetők; valamint

b) az Unió népességének legalább 65 %-át magukban foglaló tagállamokat képviselő átvitelirendszer-üzemeltetők.

(2) A 6. cikk (2) bekezdésében felsorolt feltételekre vagy módszertanokra vonatkozó javaslatokról való döntés tekintetében a blokkoló kisebbségnek legalább négy tagállamot képviselő átvitelirendszer-üzemeltetőket szükséges magában foglalnia; ennek hiányában úgy kell tekinteni, hogy sikerült elérni a minősített többséget.

(3) Amennyiben egy rendszerüzemeltetési régióban a 6. cikk (2) bekezdésében felsorolt tervekre vonatkozó javaslatokról döntő átvitelirendszer-üzemeltetők nem tudnak megállapodásra jutni, és amennyiben az érintett rendszerüzemeltetési régió több mint öt tagállamból áll, az átvitelirendszer-üzemeltetők minősített többségi szavazással döntenek. A 6. cikk (2) bekezdésében felsorolt javaslatok tekintetében a minősített többséghez a következő szükséges:

a) az érintett tagállamok legalább 72 %-át képviselő átvitelirendszer-üzemeltetők; valamint

b) az érintett régió népességének legalább 65 %-át magukban foglaló tagállamokat képviselő átvitelirendszer-üzemeltetők.

(4) A tervekkel kapcsolatos javaslatokra vonatkozó döntések tekintetében a blokkoló kisebbségnek legalább a részt vevő tagállamok lakosságának több mint 35 %-át plusz legalább egy további tagállamot képviselő átvitelirendszer-üzemeltetők minimális számát kell magában foglalnia; ennek hiányában úgy kell tekinteni, hogy sikerült elérni a minősített többséget.

(5) A feltételekre vagy módszertanokra vonatkozó javaslatokról a 6. cikk (2) bekezdésének megfelelően döntő átvitelirendszer-üzemeltetők számára tagállamonként egy szavazatot kell biztosítani. Ha egy tagállam területén egynél több átvitelirendszer-üzemeltető működik, a tagállam megosztja közöttük a szavazati jogot.

(6) Ha az átvitelirendszer-üzemeltetők az EU DSO-val együttműködve az e rendeletben meghatározott határidőkön belül nem nyújtják be a feltételekre vagy módszertanokra, illetve tervekre vonatkozó eredeti vagy módosított javaslatot az érintett illetékes hatóságoknak, akkor az érintett illetékes hatóságok és az ACER rendelkezésére bocsátják a feltételek vagy módszertanok, illetve a tervek vonatkozó tervezetét. Magyarázatot kell adniuk arra, hogy miért nem sikerült megállapodásra jutniuk. Az illetékes hatóságok közösen megteszik a megfelelő lépéseket az előírt feltételek vagy módszertanok, illetve az előírt tervek elfogadása érdekében. Ez történhet például a tervezetek e bekezdés szerinti módosításának bekérésével, a tervezetek felülvizsgálatával és kiegészítésével, vagy tervezet hiányában az előírt feltételek vagy módszertanok, illetve tervek meghatározásával és jóváhagyásával.

8. cikk

A javaslatok illetékes hatóságokhoz történő benyújtása

(1) Az átvitelirendszer-üzemeltetők a feltételekre vagy módszertanokra, illetve a tervekre vonatkozó javaslatokat a 18., 23., 29., 33., 34., 35. és 37. cikkben meghatározott határidőkön belül benyújtják az érintett illetékes hatóságoknak. Az illetékes hatóságok kivételes körülmények között közösen meghosszabbíthatják ezeket a határidőket, különösen azokban az esetekben, amikor a határidő az átvitelirendszer-üzemeltetők vagy az EU DSO-n hatáskörén kívül álló körülmények miatt nem teljesíthető.

(2) Az (1) bekezdés szerinti feltételekre, módszertanokra vagy tervekre vonatkozó javaslatokat az illetékes hatóságokhoz történő benyújtásukkal egyidejűleg tájékoztatásul az ACER-hez is be kell nyújtani.

(3) A nemzeti szabályozó hatóságok közös kérésére az ACER a feltételekre vagy módszertanokra, illetve a tervekre vonatkozó javaslatok kézhezvételétől számított hat hónapon belül véleményt ad ki a feltételekre vagy módszertanokra, illetve a tervekre vonatkozó javaslatról, és véleményéről értesíti a nemzeti szabályozó hatóságokat és az illetékes hatóságokat. A nemzeti szabályozó hatóságok, a kiberbiztonságért felelős illetékes hatóságok és más jellegű, illetékes hatóságként kijelölt hatóságok egyeztetnek egymással, mielőtt a nemzeti szabályozó hatóságok véleményt kérnének az ACER-től. Az ACER e véleményében ajánlásokat is megfogalmazhat. Az ACER konzultál az ENISA-val, mielőtt véleményt adna ki a 6. cikk (2) bekezdésében felsorolt javaslatokról.

(4) Az illetékes hatóságok konzultálnak, szorosan együttműködnek és egyeztetnek egymással annak érdekében, hogy megállapodásra jussanak a javasolt feltételekről, módszertanokról vagy tervekről. A feltételek vagy módszertanok, illetve a tervek jóváhagyása előtt szükség esetén – a villamosenergia-piaci ENTSO-val és az EU DSO-val folytatott konzultációt követően – felülvizsgálják és kiegészítik a javaslatokat annak biztosítása érdekében, hogy a javaslatok összhangban legyenek e rendelettel, és az egész Unióban hozzájáruljanak a kiberbiztonság egységesen magas szintjéhez.

(5) Az illetékes hatóságok a feltételek vagy módszertanok, illetve a tervek érintett illetékes hatóság vagy – adott esetben – az utolsó érintett illetékes hatóság általi kézhezvételétől számított hat hónapon belül határoznak e feltételekről vagy módszertanokról, illetve e tervekről.

(6) Amennyiben az ACER véleményt ad ki, az érintett illetékes hatóságok figyelembe veszik ezt a véleményt, és az ACER véleményének kézhezvételétől számított hat hónapon belül döntést hoznak.

(7) Amennyiben az illetékes hatóságok közösen kérik a javasolt feltételek vagy módszertanok, illetve tervek módosítását azok jóváhagyása érdekében, az átvitelirendszer-üzemeltetők az EU DSO-val együttműködve javaslatot dolgoznak ki a feltételek vagy módszertanok, illetve a tervek módosítására. Az átvitelirendszer-üzemeltetők a módosított javaslatot az illetékes hatóságok kérésétől számított két hónapon belül nyújtják be jóváhagyásra. Az illetékes hatóságok a benyújtástól számított két hónapon belül határoznak a módosított feltételekről és módszertanokról, illetve tervekről.

(8) Amennyiben az illetékes hatóságok az (5) vagy (7) bekezdésben említett határidőn belül nem tudnak megállapodásra jutni, erről tájékoztatják a Bizottságot. A Bizottság megfelelő lépéseket tehet, hogy lehetővé tegye az előírt feltételek vagy módszertanok, illetve tervek elfogadását.

(9) Az átvitelirendszer-üzemeltetők – a villamosenergia-piaci ENTSO és az EU DSO segítségével – az érintett illetékes hatóságok jóváhagyását követően honlapjukon közzéteszik a feltételeket vagy módszertanokat, illetve terveket, kivéve, ha ezek az információk a 47. cikkel összhangban bizalmasnak minősülnek.

(10) Az illetékes hatóságok közösen kérhetik az átvitelirendszer-üzemeltetőktől és az EU DSO-tól a jóváhagyott feltételek vagy módszertanok, illetve a jóváhagyott tervek módosítására irányuló javaslatokat, és határidőt határozhatnak meg e javaslatok benyújtására. Az átvitelirendszer-üzemeltetők az EU DSO-val együttműködve saját kezdeményezésükre is javasolhatnak módosításokat az illetékes hatóságoknak. A feltételek vagy módszertanok, illetve a tervek módosítására irányuló javaslatokat az e cikkben meghatározott eljárásnak megfelelően kell kidolgozni és jóváhagyni.

(11) A vonatkozó feltételek vagy módszertanok, illetve a vonatkozó elfogadott tervek első elfogadását követően az átvitelirendszer-üzemeltetők az EU DSO-val együttműködve legalább háromévente felülvizsgálják az elfogadott feltételek vagy módszertanok, illetve az elfogadott tervek hatékonyságát, és indokolatlan késedelem nélkül jelentést tesznek az illetékes hatóságoknak és az ACER-nek a felülvizsgálat eredményeiről.

9. cikk

Konzultáció

(1) Az átvitelirendszer-üzemeltetők a villamosenergia-piaci ENTSO segítségével és az EU DSO-val együttműködve konzultálnak az érdekelt felekkel, köztük az ACER-rel, az ENISA-val és az egyes tagállamok illetékes hatóságaival a 6. cikk (2) bekezdésében felsorolt feltételekre vagy módszertanokra, és a 6. cikk (3) bekezdésében említett tervekre vonatkozó javaslattervezetekről. A konzultáció időtartama nem lehet kevesebb egy hónapnál.

(2) Az átvitelirendszer-üzemeltetők által az EU DSO-val együttműködésben benyújtott, a 6. cikk (2) bekezdésében felsorolt feltételekre vagy módszertanokra vonatkozó javaslatokat közzé kell tenni és uniós szintű konzultációra kell bocsátani. Az érintett átvitelirendszer-üzemeltetők által az EU DSO-val együttműködésben regionális szinten benyújtott, a 6. cikk (3) bekezdésében felsorolt tervekre vonatkozó javaslatokat legalább regionális szintű konzultációra kell bocsátani.

(3) Az átvitelirendszer-üzemeltetők a villamosenergia-piaci ENTSO és a feltételekre, módszertanokra vagy tervekre vonatkozó javaslatért felelős EU DSO segítségével kellően figyelembe veszik az érdekelt feleknek az (1) bekezdéssel összhangban folytatott konzultációk során kifejtett véleményét, mielőtt azokat szabályozási jóváhagyásra benyújtanák. Valamennyi esetben kellően alátámasztott indoklást kell kidolgozni arra vonatkozóan, hogy a konzultációs során kifejtett vélemények miért szerepelnek vagy nem szerepelnek a benyújtott dokumentumokban, és kellő időben közzé kell tenni a feltételekre vagy módszertanokra vonatkozó javaslat előtt vagy azzal egyidejűleg.

10. cikk

Az érdekelt felek bevonása

Az ACER a villamosenergia-piaci ENTSO-val és az EU DSO-val szoros együttműködésben megszervezi az érdekelt felek bevonását, többek között rendszeres találkozókat szervez az érdekelt felekkel a problémák azonosítása és az e rendelet végrehajtásával kapcsolatos javítások érdekében.

11. cikk

Költségek megtérítése

(1) Az átvitelirendszer-üzemeltetők és az elosztórendszer-üzemeltetők által viselt, a hálózati díjakra vonatkozó szabályozás hatálya alá tartozó és az e rendeletben meghatározott kötelezettségekből eredő költségeket, beleértve a villamosenergia-piaci ENTSO és az EU DSO által viselt költségeket is, az egyes tagállamok illetékes nemzeti szabályozó hatóságai értékelik.

(2) Az észszerűnek, hatékonynak és arányosnak minősített költségeket hálózati díjakon vagy más megfelelő mechanizmusokon keresztül kell megtéríteni, az érintett nemzeti szabályozó hatóság által meghatározottak szerint.

(3) Az érintett nemzeti szabályozó hatóságok kérésére az (1) bekezdésben említett átvitelirendszer-üzemeltetők és elosztórendszer-üzemeltetők a nemzeti szabályozó hatóság által meghatározott észszerű határidőn belül rendelkezésre bocsátják a felmerült költségek értékelésének megkönnyítéséhez szükséges információkat.

12. cikk

Nyomon követés

(1) Az ACER az (EU) 2019/943 rendelet 32. cikkének (1) bekezdésével és az (EU) 2019/942 rendelet 4. cikkének (2) bekezdésével összhangban nyomon követi e rendelet végrehajtását. E nyomon követés során az ACER együttműködhet az ENISA-val, és támogatást kérhet a villamosenergia-piaci ENTSO-tól és az EU DSO-tól. Az ACER rendszeresen tájékoztatja a villamosenergia-ügyi koordinációs csoportot és a Kiberbiztonsági Együttműködési Csoportot e rendelet végrehajtásáról.

(2) Az ACER e rendelet hatálybalépését követően legalább háromévente jelentést tesz közzé, hogy:

a) megvizsgálja az alkalmazandó kiberbiztonsági kockázatkezelési intézkedések végrehajtásának állapotát a nagy hatású és kritikus hatású szervezetek tekintetében;

b) meghatározza, hogy szükség lehet-e további szabályokra a közös követelményekre, a tervezésre, a nyomon követésre, a jelentéstételre és a válságkezelésre vonatkozóan a villamosenergia-ágazatot érintő kockázatok megelőzése érdekében; valamint

c) az e rendelet felülvizsgálata céljából azonosítsa a javításra szoruló területeket, vagy meghatározza a technológiai fejlődés következtében esetlegesen felmerülő, le nem fedett területeket és új prioritásokat.

(3) 2025. június 13-án az ACER az ENISA-val együttműködve, valamint a villamosenergia-piaci ENTSO-val és az EU DSO-val folytatott konzultációt követően az (5) bekezdéssel összhangban meghatározott teljesítménymutatók alapján iránymutatást adhat ki az ACER-rel a nyomon követés céljából közlendő releváns információkról, valamint az adatgyűjtés folyamatáról és gyakoriságáról.

(4) Az illetékes hatóságok hozzáférhetnek az ACER birtokában lévő releváns információkhoz, amelyeket az ACER e cikkel összhangban gyűjtött össze.

(5) Az ACER az ENISA-val együttműködve, valamint a villamosenergia-piaci ENTSO és az EU DSO támogatásával nem kötelező erejű teljesítménymutatókat ad ki a határkeresztező villamosenergia-áramlás kiberbiztonsági szempontjaival kapcsolatos működési megbízhatóság értékelése céljából.

(6) Az e rendelet 2. cikkének (1) bekezdésében felsorolt szervezetek benyújtják az ACER-nek a (2) bekezdésben felsorolt feladatok ellátásához szükséges információkat.

13. cikk

Összehasonlító teljesítményértékelés

(1) Az ACER az ENISA-val együttműködve 2025. június 13-án nem kötelező erejű kiberbiztonsági teljesítményértékelési útmutatót dolgoz ki. Az útmutató ismerteti a nemzeti szabályozó hatóságokkal a végrehajtott kiberbiztonsági ellenőrzések e cikk (2) bekezdése szerinti összehasonlító teljesítményértékelésének elveit, figyelembe véve az ellenőrzések végrehajtásának költségeit és az ilyen ellenőrzések végrehajtásához használt folyamatok, termékek, szolgáltatások, rendszerek és megoldások által betöltött funkció hatékonyságát. Az ACER a nem kötelező erejű kiberbiztonsági teljesítményértékelési útmutató kidolgozásakor figyelembe veszi a meglévő teljesítményértékelési jelentéseket. Az ACER tájékoztatás céljából benyújtja a nem kötelező erejű kiberbiztonsági teljesítményértékelési útmutatót a nemzeti szabályozó hatóságoknak.

(2) Az (1) bekezdés szerinti teljesítményértékelési útmutató kidolgozását követő 12 hónapon belül a nemzeti szabályozó hatóságok teljesítményértékelési elemzést végeznek annak értékelésére, hogy a jelenlegi kiberbiztonsági beruházások:

a) csökkentik-e a határkeresztező villamosenergia-áramlásokat érintő kockázatokat;

b) a kívánt eredményt nyújtják-e és a növelik-e a hatékonyságot a villamosenergia-rendszerek fejlesztése terén;

c) hatékonyak-e, és beépülnek-e az eszközök és szolgáltatások általános beszerzésébe.

(3) A teljesítményértékelési elemzés céljából a nemzeti szabályozó hatóságok figyelembe vehetik az ACER által kidolgozott, nem kötelező erejű kiberbiztonsági teljesítményértékelési útmutatót és különösen a következőket értékelik:

a) a határkeresztező villamosenergia-áramlásokra hatást gyakorló kockázatok mérséklése céljából a kiberbiztonsággal kapcsolatban keletkezett átlagos kiadások, különös tekintettel a nagy hatású és kritikus hatású szervezetekre;

b) a villamosenergia-piaci ENTSO-val és az EU DSO-val együttműködve azon kiberbiztonsági szolgáltatások, rendszerek és termékek átlagárai, amelyek nagymértékben hozzájárulnak a kiberbiztonsági kockázatkezelési intézkedések javításához és fenntartásához a különböző rendszerüzemeltetési régiókban;

c) az e rendelet végrehajtására alkalmas kiberbiztonsági szolgáltatások, rendszerek és megoldások költségeinek és funkcióinak megléte és összehasonlíthatóságának szintje, meghatározva a kiadások hatékonyságának növeléséhez szükséges lehetséges intézkedéseket, különösen azokban az esetekben, amikor kiberbiztonsági technológiai beruházásokra lehet szükség.

(4) A teljesítményértékelési elemzéssel kapcsolatos információkat e rendelet adatbesorolási követelményeinek, a minimális kiberbiztonsági ellenőrzéseknek és a határkeresztező villamos energia kiberbiztonsági kockázatértékeléséről szóló jelentésnek megfelelően kell kezelni és feldolgozni. A (2) és (3) bekezdésben említett összehasonlító teljesítményértékelési elemzés nem hozható nyilvánosságra.

(5) A 47. cikkben foglalt titoktartási követelmények és az e rendelet rendelkezéseinek hatálya alá tartozó szervezetek biztonságának védelme szükségességének sérelme nélkül, az e cikk (2) és (3) bekezdésében említett összehasonlító teljesítményértékelési elemzést meg kell osztani minden nemzeti szabályozó hatósággal, minden illetékes hatósággal, az ACER-rel, az ENISA-val és a Bizottsággal.

14. cikk

Megállapodások az Unión kívüli átvitelirendszer-üzemeltetőkkel

(1) E rendelet hatálybalépésétől számított 18 hónapon belül a harmadik országgal szomszédos rendszerüzemeltetési régiók átvitelirendszer-üzemeltetői arra törekednek, hogy a szomszédos harmadik ország átvitelirendszer-üzemeltetőivel olyan megállapodásokat kössenek, amelyek összhangban vannak a vonatkozó uniós joggal, és amelyek meghatározzák az említett átvitelirendszer-üzemeltetőkkel a kiberbiztonsági védelemmel kapcsolatban folytatott együttműködés és a velük kötött kiberbiztonsági együttműködési megállapodások alapját.

(2) Az átvitelirendszer-üzemeltetők tájékoztatják az illetékes hatóságot az (1) bekezdés alapján megkötött megállapodásokról.

15. cikk

Jogi képviselők

(1) Azok a szervezetek, amelyek nem az Unióban telepedtek le, de az Unióban működő szervezeteknek nyújtanak szolgáltatásokat, és amelyek értesítés kaptak arról, hogy a 24. cikk (6) bekezdésének megfelelően nagy hatású vagy kritikus hatású szervezetnek minősülnek, az értesítéstől számított három hónapon belül írásban kijelölnek egy uniós képviselőt, és ennek megfelelően tájékoztatják az értesítő illetékes hatóságot.

(2) Ezt a képviselőt azzal a céllal kell megbízni, hogy az illetékes hatóság vagy a CSIRT a nagy vagy a kritikus hatású szervezet mellett vagy helyett e képviselőhöz fordulhasson az adott szervezetnek az e rendelet szerinti kötelezettségei tekintetében. A nagy hatású vagy kritikus hatású szervezet biztosítja jogi képviselője számára az érintett illetékes hatóságokkal vagy CSIRT-ekkel való hatékony és időben történő együttműködés biztosításához szükséges hatásköröket és elegendő erőforrást.

(3) A jogi képviselő azon tagállamok egyikében telepedett le, amelyben a szervezet szolgáltatásokat nyújt. A szervezetet a képviselő letelepedése szerinti tagállam joghatósága alá tartozónak kell tekinteni. A nagy hatású vagy kritikus hatású szervezetek tájékoztatják azon tagállam illetékes hatóságát a jogi képviselőjük nevéről, postai címéről, e-mail-címéről és telefonszámáról, ahol a jogi képviselő lakóhellyel vagy letelepedési hellyel rendelkezik.

(4) A kijelölt jogi képviselő felelősségre vonható az e rendeletben előírt kötelezettségeknek való meg nem felelés esetén, a nagy hatású vagy kritikus hatású szervezetek felelősségének és az ellenük indítható jogi eljárások sérelme nélkül.

(5) Az Unióban e cikk alapján kijelölt képviselő hiányában bármely olyan tagállam, amelyben a szervezet szolgáltatást nyújt, jogi lépéseket tehet a szervezet ellen az e rendeletből eredő kötelezettségek be nem tartása miatt.

(6) Az Unión belüli jogi képviselő (1) bekezdés alapján történő kinevezése nem minősül Unión belüli letelepedésnek.

16. cikk

Együttműködés a villamosenergia-piaci ENTSO és az EU DSO között

(1) A villamosenergia-piaci ENTSO és az EU DSO együttműködik a 19. cikk és a 21. cikk szerinti kiberbiztonsági kockázatértékelések elvégzésében, különös tekintettel a következő feladatokra:

a) a 18 cikk (1) bekezdése szerinti kiberbiztonsági kockázatértékelési módszerek kidolgozása;

b) a 23. cikk szerinti, a határkeresztező villamos energia kiberbiztonsági kockázatértékeléséről szóló átfogó jelentés kidolgozása;

c) a III. fejezet szerinti, a villamos energia közös kiberbiztonsági keretének kidolgozása;

d) a 35. cikk szerinti kiberbiztonsági beszerzési ajánlás kidolgozása;

e) a 37 cikk (8) bekezdése szerinti, a kibertámadások besorolási skálája módszertanának kidolgozása;

f) a 48. cikk (1) bekezdése szerinti, a villamos energia ideiglenes kiberbiztonsági hatásmutatójának (a továbbiakban: ECII) kidolgozása;

g) a nagy hatású és kritikus hatású szervezetek 48. cikk (3) bekezdése szerinti, egységes szerkezetben foglalt ideiglenes jegyzékének kidolgozása;

h) az egész Unióra kiterjedő, nagy hatású és kritikus hatású folyamatok 48. cikk (4) bekezdése szerinti ideiglenes jegyzékének kidolgozása;

i) az európai és nemzetközi szabványok és ellenőrzések 48. cikk (6) bekezdése szerinti ideiglenes jegyzékének kidolgozása;

j) a 19. cikk szerinti, az egész Unióra kiterjedő kiberbiztonsági kockázatértékelés elvégzése;

k) a 21. cikk szerinti regionális kiberbiztonsági kockázatértékelések elvégzése;

l) a 22. cikk szerinti regionális kiberbiztonsági kockázatcsökkentési tervek meghatározása;

m) a 36. cikk szerinti, az IKT-termékekre, IKT-szolgáltatásokra és IKT-folyamatokra vonatkozó európai kiberbiztonsági tanúsítási rendszerekről szóló iránymutatás kidolgozása;

n) e rendelet végrehajtására vonatkozó iránymutatások kidolgozása az ACER-rel és az ENISA-val konzultálva.

(2) A villamosenergia-piaci ENTSO és az EU DSO közötti együttműködés történhet kiberbiztonsági kockázatokkal foglalkozó munkacsoport formájában.

(3) A villamosenergia-piaci ENTSO és az EU DSO rendszeresen tájékoztatja az ACER-t, az ENISA-t, a Kiberbiztonsági Együttműködési Csoportot és a villamosenergia-ügyi koordinációs csoportot a 19. és a 21. cikk szerinti, az egész Unióra kiterjedő és a regionális kiberbiztonsági kockázatértékelések végrehajtása terén elért eredményekről.

17. cikk

Együttműködés az ACER és az illetékes hatóságok között

Az ACER az egyes illetékes hatóságokkal együttműködve:

1. nyomon követi a 12. cikk (2) bekezdésének a) pontja szerinti kiberbiztonsági kockázatkezelési intézkedések, valamint a 27. és a 39. cikk szerinti jelentéstételi kötelezettségek végrehajtását; valamint

2. nyomon követi a 6. cikk (2) és (3) bekezdése szerinti feltételek, módszertanok vagy tervek elfogadási folyamatát és végrehajtását. Az ACER, az ENISA és az egyes illetékes hatóságok közötti együttműködés történhet a kiberbiztonsági kockázatot nyomon követő szervezet formájában.

II. FEJEZET

KOCKÁZATÉRTÉKELÉS ÉS A RELEVÁNS KIBERBIZTONSÁGI KOCKÁZATOK AZONOSÍTÁSA

18. cikk

A kiberbiztonsági kockázatértékelés módszertanai

(1) 2025. március 13-án az átvitelirendszer-üzemeltetők a villamosenergia-piaci ENTSO segítségével, az EU DSO-val együttműködve és a Kiberbiztonsági Együttműködési Csoporttal folytatott konzultációt követően javaslatot nyújtanak be az uniós, regionális és tagállami szintű kiberbiztonsági kockázatértékelési módszertanokra vonatkozóan.

(2) Az uniós, regionális és tagállami szintű kiberbiztonsági kockázatértékelési módszertanok a következőket tartalmazzák:

a) a vizsgálandó kiberfenyegetések listája, beleértve legalább a következő, az ellátási láncot érintő fenyegetéseket:

   i. az ellátási lánc súlyos és váratlan sérülése;

   ii. IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok hiányoznak az ellátási láncból;

iii. az ellátási lánc szereplőin keresztül kezdeményezett kibertámadások;

iv. érzékeny információk kiszivárogtatása az ellátási láncon keresztül, az ellátási lánc nyomon követését is beleértve;

v. gyengeségek vagy hátsó ajtók beépítése az IKT-termékekbe, az IKT-szolgáltatásokba vagy az IKT-folyamatokba az ellátási lánc szereplőin keresztül.

b) a kiberbiztonsági kockázatok magas vagy kritikus hatásának értékelésére szolgáló kritériumok, a következményekre és a valószínűségre vonatkozóan meghatározott küszöbértékek alkalmazásával;

c) az örökölt rendszerekből eredő kiberbiztonsági kockázatok, a kibertámadások lépcsőzetes hatásai és a hálózatot működtető rendszerek valós idejű jellegének elemzésére szolgáló megközelítés;

d) az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok egyetlen beszállítójától való függőségből eredő kiberbiztonsági kockázatok elemzésére szolgáló megközelítés.

(3) Az uniós, regionális és tagállami szintű kiberbiztonsági kockázatértékelési módszertanok ugyanazon kockázati hatásmátrix alkalmazásával értékelik a kiberbiztonsági kockázatokat. A kockázati hatásmátrix:

a) a kibertámadások következményeit a következő kritériumok alapján méri:

i. terheléskiesés;

ii. a villamosenergia-termelés csökkenése;

iii. kapacitásvesztés az elsődleges frekvenciatartalékban;

iv. teljes vagy részleges leállás után az elektromos hálózat működésének külső szállítóhálózat igénybevétele nélkül történő helyreállításához szükséges kapacitás kiesése (más néven „black start”);

v. a fogyasztókat érintő elektromos üzemszünet várható időtartama, az üzemszünetnek a fogyasztók számában kifejezett mértékével együtt; valamint

vi. bármely más mennyiségi vagy minőségi kritérium, amely észszerűen jelezheti a kibertámadásnak a határkeresztező villamosenergia-áramlásokra gyakorolt hatását.

b) a biztonsági esemény valószínűségének mérése a kibertámadások évenkénti gyakoriságaként.

(4) Az uniós szintű kiberbiztonsági kockázatértékelési módszerek ismertetik, hogy hogyan határozzák meg a nagy hatású és a kritikus hatású küszöbértékek ECII-értékeit. Az ECII lehetővé teszi a szervezetek számára, hogy a 26. cikk (4) bekezdése c) pontjának i. alpontja szerint elvégzett üzleti hatásvizsgálatok során a (2) bekezdés b) pontjában említett kritériumok segítségével felbecsüljék a kockázatok üzleti folyamataikra gyakorolt hatását.

(5) A villamosenergia-piaci ENTSO az EU DSO-val egyeztetve tájékoztatja a villamosenergia-ügyi koordinációs csoportot az (1) bekezdés szerint kidolgozott kiberbiztonsági kockázatértékelési módszerekre vonatkozó javaslatokról.

19. cikk

Az egész Unióra kiterjedő kiberbiztonsági kockázatértékelés

(1) A 8. cikk szerinti kiberbiztonsági kockázatértékelési módszertanok jóváhagyását követő 9 hónapon belül, majd azt követően háromévente a villamosenergia-piaci ENTSO az EU DSO-val együttműködve és a Kiberbiztonsági Együttműködési Csoporttal konzultálva – az (EU) 2022/2555 irányelv 22. cikkének sérelme nélkül – az egész Unióra kiterjedő kiberbiztonsági kockázatértékelést végez, és elkészíti az egész Unióra kiterjedő kiberbiztonsági kockázatértékelési jelentés tervezetét. E célból a villamosenergia-rendszer üzembiztonságát befolyásoló és a határkeresztező villamosenergia-áramlást megzavaró kibertámadások lehetséges következményeinek azonosítására, elemzésére és értékelésére a 18. cikk alapján kidolgozott és a 8. cikk alapján jóváhagyott módszereket fogják használni. Az egész Unióra kiterjedő kiberbiztonsági kockázatértékelés nem veszi figyelembe a kibertámadások által okozott jogi, pénzügyi vagy a hírnévben keletkezett károkat.

(2) Az egész Unióra kiterjedő kiberbiztonsági kockázatértékelési jelentés a következő elemeket tartalmazza:

a) az egész Unióra kiterjedő, nagy hatású folyamatok és az egész Unióra kiterjedő kritikus hatású folyamatok;

b) a szervezetek és az illetékes hatóságok kockázati hatásmátrixot használnak 20. cikk értelmében végzett tagállami kiberbiztonsági kockázatértékelésben és a 26. cikk (2) bekezdésének b) pontja értelmében végzett szervezetszintű kiberbiztonsági kockázatértékelésben azonosított kiberbiztonsági kockázat értékeléséhez.

(3) Az egész Unióra kiterjedő nagy hatású folyamatok és az egész Unióra kiterjedő kritikus hatású folyamatok tekintetében az egész Unióra kiterjedő kiberbiztonsági kockázatértékelési jelentés a következőket tartalmazza:

a) a kibertámadás lehetséges következményeinek értékelése a 18. cikk (2), (3) és (4) bekezdése alapján kidolgozott és a 8. cikk szerint jóváhagyott kiberbiztonsági kockázatértékelési módszertanban meghatározott mérőszámok felhasználásával;

b) az ECII, valamint a nagy hatású és kritikus hatású küszöbértékek, amelyeket az illetékes hatóságok a 24. cikk (1) és (2) bekezdése alapján használnak az egész Unióra kiterjedő nagy hatású folyamatokban és az egész Unióra kiterjedő kritikus hatású folyamatokban részt vevő, nagy hatású és kritikus hatású szervezetek azonosítására.

(4) A villamosenergia-piaci ENTSO az EU DSO-val együttműködve véleményezésre benyújtja az ACER-hez az egész Unióra kiterjedő kiberbiztonsági kockázatértékelési jelentés tervezetét és az egész Unióra kiterjedő kiberbiztonsági kockázatértékelés eredményeit. Az ACER a jelentéstervezet kézhezvételétől számított három hónapon belül véleményt ad ki a jelentéstervezetről. A villamosenergia-piaci ENTSO és az EU DSO a jelentés véglegesítésekor a lehető legnagyobb mértékben figyelembe veszi az ACER véleményét.

(5) Az ACER véleményének kézhezvételétől számított három hónapon belül a villamosenergia-piaci ENTSO az EU DSO-val együttműködve értesíti az ACER-t, a Bizottságot, az ENISA-t és az illetékes hatóságokat az egész Unióra kiterjedő, végleges kiberbiztonsági kockázatértékelési jelentésről.

20. cikk

Tagállami kiberbiztonsági kockázatértékelés

(1) Minden illetékes hatóság tagállami kiberbiztonsági kockázatértékelést végez a tagállamában található valamennyi nagy hatású és kritikus hatású szervezetre vonatkozóan, a 18. cikk alapján kidolgozott és a 8. cikk alapján jóváhagyott módszertanok alkalmazásával. A tagállami kiberbiztonsági kockázatértékelés azonosítja és elemzi a villamosenergia-rendszer üzembiztonságát érintő kibertámadások azon kockázatait, amelyek zavart okozhatnak a határkeresztező villamosenergia-áramlásokban. A tagállami kiberbiztonsági kockázatértékelés nem veszi figyelembe a kibertámadások által okozott jogi, pénzügyi vagy a hírnévben keletkezett károkat.

(2) A nagy és kritikus hatású szervezeteknek a 24. cikk (6) bekezdése szerinti bejelentését követő 21 hónapon belül és azt követően háromévente, valamint a villamos energia terén a kiberbiztonságért felelős illetékes hatóságokkal folytatott konzultációt követően minden illetékes hatóság – a CSIRT támogatásával – tagállami kiberbiztonsági kockázatértékelési jelentést nyújt be a villamosenergia-piaci ENTSO-nak és az EU DSO-nak, amely minden egyes nagy hatású és kritikus hatású üzleti folyamatra vonatkozóan tartalmazza a következő információkat:

a) a 29. cikk szerinti minimális és fejlett kiberbiztonsági ellenőrzések végrehajtásának állapota;

b) a 38. cikk (3) bekezdése alapján az előző három évben bejelentett valamennyi kibertámadás jegyzéke;

c) a 38. cikk (6) bekezdése alapján az előző három évben bejelentett kiberfenyegetésekkel kapcsolatos információk összefoglalása;

d) minden uniós szintű, nagy hatású vagy kritikus hatású folyamat esetében az információk és a releváns eszközök bizalmas jellegének, integritásának és elérhetőségének veszélyeztetésével kapcsolatos kockázatok becslése;

e) szükség esetén a 24. cikk (1), (2), (3) és (5) bekezdése értelmében nagy vagy kritikus hatásúként azonosított további szervezetek jegyzéke.

(3) A tagállami kiberbiztonsági kockázatértékelési jelentés figyelembe veszi a tagállamnak az (EU) 2019/941 rendelet 10. cikke alapján létrehozott kockázati készültségi tervét.

(4) A (2) bekezdés a)–d) pontja szerinti tagállami kiberbiztonsági kockázatértékelési jelentésben szereplő információk nem kapcsolhatók konkrét szervezetekhez vagy eszközökhöz. A tagállami kiberbiztonsági kockázatértékelési jelentés tartalmazza a tagállamok illetékes hatóságai által a 30. cikk alapján megadott ideiglenes eltérések kockázatértékelését is.

(5) A villamosenergia-piaci ENTSO és az EU DSO további információkat kérhet az illetékes hatóságoktól a második albekezdés a) és c) pontjában meghatározott feladatokkal kapcsolatban.

(6) Az illetékes hatóságok biztosítják, hogy az általuk szolgáltatott információk pontosak és helyesek legyenek.

21. cikk

Regionális kiberbiztonsági kockázatértékelés

(1) A villamosenergia-piaci ENTSO – az EU DSO-val együttműködve és az érintett regionális koordinációs központtal konzultálva – a 19. cikk alapján kidolgozott és a 8. cikk alapján jóváhagyott módszertanok alkalmazásával regionális kiberbiztonsági kockázatértékelést végez minden rendszerüzemeltetési régióra vonatkozóan a villamosenergia-rendszer üzembiztonságát befolyásoló és a határkeresztező villamosenergia-áramlást megzavaró kibertámadások kockázatainak azonosítása, elemzése és értékelése céljából. A regionális kiberbiztonsági kockázatértékelések nem veszik figyelembe a kibertámadások által okozott jogi, pénzügyi vagy a hírnévben keletkezett károkat.

(2) A nagy hatású és kritikus hatású szervezeteknek a 24. cikk (6) bekezdése szerinti bejelentését követő 30 hónapon belül és azt követően háromévente a villamosenergia-piaci ENTSO – az EU DSO-val együttműködve és a Kiberbiztonsági Együttműködési Csoporttal konzultálva – minden rendszerüzemeltetési régióra vonatkozóan regionális kiberbiztonsági kockázatértékelési jelentést készít.

(3) A regionális kiberbiztonsági kockázatértékelési jelentés figyelembe veszi az egész Unióra kiterjedő kiberbiztonsági kockázatértékelési jelentésekben és a tagállami kiberbiztonsági kockázatértékelési jelentésekben szereplő releváns információkat.

(4) A regionális kiberbiztonsági kockázatértékelés figyelembe veszi az (EU) 2019/941 rendelet 6. cikke szerint azonosított, kiberbiztonsággal kapcsolatos regionális villamosenergia-ellátási válságforgatókönyveket.

22. cikk

Regionális kiberbiztonsági kockázatcsökkentési tervek

(1) A nagy és kritikus hatású szervezeteknek a 24. cikk (6) bekezdése szerinti bejelentését követő 36 hónapon belül és, de legkésőbb 2031. június 13-án, majd azt követően háromévente az átvitelirendszer-üzemeltetők a villamosenergia-piaci ENTSO segítségével, az EU DSO-val együttműködve, valamint a regionális koordinációs központokkal és a Kiberbiztonsági Együttműködési Csoporttal konzultálva regionális kiberbiztonsági kockázatcsökkentési tervet dolgoznak ki minden rendszerüzemeltetési régióra vonatkozóan.

(2) A regionális kiberbiztonsági kockázatcsökkentési tervek a következőket tartalmazzák:

a) a nagy hatású és kritikus hatású szervezetek által a rendszerüzemeltetési régióban alkalmazandó minimális és fejlett kiberbiztonsági ellenőrzések;

b) az a) pontban említett ellenőrzések alkalmazását követően a rendszerüzemeltetési régiókban fennmaradó kiberbiztonsági kockázatok.

(3) A villamosenergia-piaci ENTSO benyújtja a regionális kockázatcsökkentési terveket az érintett átvitelirendszer-üzemeltetőknek, az illetékes hatóságoknak és a villamosenergia-ügyi koordinációs csoportnak. A villamosenergia-ügyi koordinációs csoport módosításokat javasolhat.

(4) Az átvitelirendszer-üzemeltetők a villamosenergia-piaci ENTSO segítségével, az EU DSO-val együttműködve és a Kiberbiztonsági Együttműködési Csoporttal konzultálva háromévente aktualizálják a regionális kockázatcsökkentési terveket, kivéve, ha a körülmények ennél gyakoribb aktualizálást tesznek szükségessé.

23. cikk

A határkeresztező villamos energia kiberbiztonsági kockázatértékeléséről szóló átfogó jelentés

(1) A nagy és kritikus hatású szervezeteknek a 24. cikk (6) bekezdése szerinti bejelentését követő 40 hónapon belül és azt követően háromévente az átvitelirendszer-üzemeltetők a villamosenergia-piaci ENTSO segítségével, az EU DSO-val együttműködve és a Kiberbiztonsági Együttműködési Csoporttal konzultálva jelentést nyújtanak be a villamosenergia-ügyi koordinációs csoportnak a határkeresztező villamosenergia-áramlásokkal kapcsolatos kiberbiztonsági kockázatértékelés eredményéről (a továbbiakban: a határkeresztező villamos energia kiberbiztonsági kockázatértékeléséről szóló átfogó jelentés).

(2) A határkeresztező villamos energia kiberbiztonsági kockázatértékeléséről szóló átfogó jelentés az Unió egészére kiterjedő kiberbiztonsági kockázatértékelési jelentésen, a tagállami kiberbiztonsági kockázatértékelési jelentéseken és a regionális kiberbiztonsági kockázatértékelési jelentéseken alapul, és tartalmazza a következő információkat:

a) az egész Unióra kiterjedő kiberbiztonsági kockázatértékelési jelentésben a 19. cikk (2) bekezdésének a) pontjával összhangban azonosított, uniós szintű nagy hatású és kritikus hatású folyamatok jegyzéke, beleértve a 21. cikk (2) bekezdése és a 19. cikk (3) bekezdésének a) pontja szerint a regionális kiberbiztonsági kockázatértékelési jelentésekben értékelt kiberbiztonsági kockázatok valószínűségének és hatásának becslését;

b) aktuális kiberfenyegetések, különös tekintettel a villamosenergia-rendszert érintő új fenyegetésekre és kockázatokra;

c) az előző időszakot érintő, uniós szintű kibertámadások, kritikus áttekintést nyújtva arról, hogy az ilyen kibertámadások hogyan befolyásolhatták a határkeresztező villamosenergia-áramlásokat;

d) a kiberbiztonsági intézkedések végrehajtásának általános állapota;

e) a 37. és 38. cikk szerinti információáramlás megvalósításnak állapota;

f) az információk jegyzéke vagy az információk besorolására vonatkozó konkrét kritériumok a 46. cikk szerint;

g) azonosított és kiemelt kockázatok, amelyek az ellátási lánc nem biztonságos irányításából származhatnak;

h) a 44. cikk szerint szervezett regionális és régiók közötti kiberbiztonsági gyakorlatok eredményei és tapasztalatai;

i) a villamosenergia-ágazatban a legutóbbi regionális kiberbiztonsági kockázatértékelések óta a határokon átnyúló általános kiberbiztonsági kockázatok alakulásának elemzése;

j) bármely egyéb információ, amely hasznos lehet e rendelet lehetséges javításainak, illetve az e rendelet vagy az abban foglalt bármely eszköz felülvizsgálata szükségességének megállapításához; valamint

k) a 30. cikk (3) bekezdése alapján engedélyezett eltérésekre vonatkozó összesített és anonimizált információk.

(3) A 2. cikk (1) bekezdésében felsorolt szervezetek – a 47. cikkel összhangban az információk bizalmas jellegének tiszteletben tartása mellett – hozzájárulhatnak a határkeresztező villamos energia kiberbiztonsági kockázatértékeléséről szóló átfogó jelentés kidolgozásához. Az átvitelirendszer-üzemeltetők a villamosenergia-piaci ENTSO segítségével és az EU DSO-val együttműködve már a korai szakaszban konzultálnak ezekkel a szervezetekkel.

(4) A határkeresztező villamos energia kiberbiztonsági kockázatértékeléséről szóló átfogó jelentésre a 46. cikk szerinti, az információcsere védelmére vonatkozó szabályokat kell alkalmazni. A 10. cikk (4) bekezdésének és a 47. cikk (4) bekezdésének sérelme nélkül a villamosenergia-piaci ENTSO és az EU DSO közzéteszi a jelentés olyan nyilvános változatát, amely nem tartalmazhat olyan információkat, amelyek kárt okozhatnak a 2. cikk (1) bekezdésében felsorolt szervezeteknek. E jelentés nyilvános változata csak a Kiberbiztonsági Együttműködési Csoport és a villamosenergia-ügyi koordinációs csoport beleegyezésével tehető közzé. A villamosenergia-piaci ENTSO az EU DSO-val egyeztetve felel a jelentés nyilvános változatának összeállításáért és közzétételéért.

24. cikk

A nagy hatású és kritikus hatású szervezetek azonosítása

(1) A 19. cikk (3) bekezdésének b) pontja szerinti, az egész Unióra kiterjedő kiberbiztonsági kockázatértékelési jelentésben szereplő ECII, továbbá a nagy hatásra és kritikus hatásra vonatkozó küszöbértékek felhasználásával minden illetékes hatóság azonosítja a tagállama azon nagy hatású és kritikus hatású szervezeteit, amelyek részt vesznek az uniós szintű nagy hatású és kritikus hatású folyamatokban. Az illetékes hatóságok információt kérhetnek a tagállamukban lévő szervezettől az adott szervezet ECII-értékeinek meghatározásához. Ha egy szervezet meghatározott ECII-je meghaladja a nagy hatásra vagy kritikus hatásra vonatkozó küszöbértéket, az így azonosított szervezetet fel kell tüntetni a 20. cikk (2) bekezdésében említett tagállami kiberbiztonsági kockázatértékelési jelentésben.

(2) A 19. cikk (3) bekezdésének b) pontja szerinti, az egész Unióra kiterjedő kiberbiztonsági kockázatértékelési jelentésben szereplő ECII, valamint a nagy hatásra és kritikus hatásra vonatkozó küszöbértékek felhasználásával minden illetékes hatóság azonosítja az Unióban nem letelepedett, nagy hatású és kritikus hatású szervezeteket, amennyiben azok az Unióban tevékenykednek. Az illetékes hatóság információt kérhet az Unióban nem letelepedett szervezettől az adott szervezet ECII-értékeinek meghatározásához.

(3) Minden illetékes hatóság a tagállamában további szervezeteket azonosíthat nagy hatású vagy kritikus hatású szervezetként, amennyiben teljesülnek a következő kritériumok:

a) a szervezet olyan szervezetek csoportjának része, amelyek esetében jelentős a kockázata annak, hogy egyidejű kibertámadás sújthatja őket;

b) a szervezetek csoportjára vonatkozóan aggregált ECII meghaladja a nagy hatásra vagy kritikus hatásra vonatkozó küszöbértéket.

(4) Ha az illetékes hatóság a (3) bekezdéssel összhangban további szervezeteket azonosít, e szervezetek valamennyi olyan folyamatát, amelyek esetében a csoporton belül összesített ECII meghaladja a nagy hatásra vonatkozó küszöbértéket, nagy hatású folyamatnak kell tekinteni, és e szervezetek valamennyi olyan folyamatát, amelyek esetében a csoporton belül összesített ECII meghaladja a kritikus hatásra vonatkozó küszöbértékeket, kritikus hatású folyamatnak kell tekinteni.

(5) Ha egy illetékes hatóság egynél több tagállamban azonosít a (3) bekezdés a) pontjában említett szervezeteket, tájékoztatja erről a többi illetékes hatóságot, a villamosenergia-piaci ENTSO-t és az EU DSO-t. A villamosenergia-piaci ENTSO az EU DSO-val együttműködve – az összes illetékes hatóságtól kapott információk alapján – elemzést nyújt be az illetékes hatóságoknak az egynél több tagállamban működő olyan szervezetek összesítéséről, amelyek megosztott zavart okozhatnak a határkereszteződő villamosenergia-áramlásban, és kibertámadáshoz vezethetnek. Amennyiben szervezetek több tagállamban működő csoportját olyan összesítésként azonosítanak, amelynek ECII-je meghaladja a nagy hatásra vagy kritikus hatásra vonatkozó küszöbértéket, az érintett illetékes hatóságok az ilyen csoporthoz tartozó szervezeteket a szervezetcsoport összesített ECII-je alapján saját tagállamuk tekintetében nagy hatású vagy kritikus hatású szervezetként azonosítják, és az így azonosított szervezeteket fel kell sorolni az egész Unióra kiterjedő kiberbiztonsági kockázatértékelési jelentésben.

(6) Minden illetékes hatóság az azt követő kilenc hónapon belül, hogy a villamosenergia-piaci ENTSO és az EU DSO értesítette a 19. cikk (5) bekezdése szerinti, az egész Unióra kiterjedő kiberbiztonsági kockázatértékelési jelentésről, de legkésőbb 2028. június 13-án értesíti az említett felsorolásban szereplő szervezeteket arról, hogy a tagállamában nagy hatású vagy kritikus hatású szervezetként azonosították őket.

(7) Amennyiben egy szolgáltatót a 27. cikk c) pontja értelmében kritikus IKT-szolgáltatóként jelentenek be az illetékes hatóságnak, az illetékes hatóság értesíti erről azon tagállamok illetékes hatóságait, amelyek területén a szolgáltató székhelye vagy képviselője található. Ez utóbbi illetékes hatóság értesíti a szolgáltatót arról, hogy kritikus szolgáltatóként azonosították.

25. cikk

Nemzeti hitelesítési rendszerek

(1) Az illetékes hatóságok nemzeti hitelesítési rendszert hozhatnak létre annak megerősítése céljából, hogy a 24. cikk (1) bekezdése szerint azonosított kritikus hatású szervezetek végrehajtották-e a 34. cikkben említett feltérképezési mátrixban szereplő nemzeti jogszabályi keretet. A nemzeti hitelesítési rendszer alapulhat az illetékes hatóság által végzett ellenőrzésen, független biztonsági ellenőrzéseken vagy az ugyanazon tagállamban működő, az illetékes hatóság által felügyelt, kritikus hatású szervezetek által végzett kölcsönös szakmai vizsgálatokon.

(2) Ha egy illetékes hatóság nemzeti hitelesítési rendszer létrehozása mellett dönt, gondoskodik arról, hogy a hitelesítés a következő követelményeknek megfelelően történjen:

a) a szakmai vizsgálatot, auditot vagy ellenőrzést végző bármely fél független a hitelesítés tárgyát képező kritikus hatású szervezettől, és nem állhat fenn összeférhetetlenség;

b) a szakmai vizsgálatot, auditot vagy ellenőrzést végző személyzetnek igazolható ismeretekkel kell rendelkeznie a következőkről:

   i. kiberbiztonság a villamosenergia-ágazatban;

   ii. kiberbiztonsági irányítási rendszerek;

   iii. az auditálás elvei;

   iv. kiberbiztonsági kockázatértékelés;

   v. a villamos energia közös kiberbiztonsági kerete;

   vi. a nemzeti jogszabályi és szabályozási keret, valamint a hitelesítés hatókörébe tartozó európai és nemzetközi szabványok;

   vii. a hitelesítés hatókörébe tartozó kritikus hatású folyamatok.

c) a szakmai vizsgálatot, auditot vagy ellenőrzést végző fél számára elegendő időt kell biztosítani e tevékenységek elvégzésére;

d) a szakmai vizsgálatot, auditot vagy ellenőrzést végző fél megteszi a megfelelő intézkedéseket a hitelesítés során gyűjtött információk védelme érdekében, a titoktartás szintjének megfelelően; valamint

e) a szakmai vizsgálatokat, auditokat vagy ellenőrzéseket évente legalább egyszer el kell végezni, és azok legalább háromévente a teljes hitelesítési körre kiterjednek.

(3) Ha egy illetékes hatóság nemzeti hitelesítési rendszer létrehozása mellett dönt, évente jelentést tesz az ACER-nek arról, hogy a rendszer keretében milyen gyakran folytatott ellenőrzéseket.

26. cikk

Szervezeti szinten végzett kiberbiztonsági kockázatkezelés

(1) Minden egyes, az illetékes hatóságok által a 24. cikk (1) bekezdése szerint azonosított nagy hatású és kritikus hatású szervezet kiberbiztonsági kockázatkezelést végez a nagy hatású és kritikus hatású hatókörébe tartozó valamennyi eszközére vonatkozóan. Minden nagy hatású és kritikus hatású szervezet háromévente kockázatkezelést végez, amely tartalmazza a (2) bekezdésben említett szakaszokat.

(2) Minden nagy hatású és kritikus hatású szervezet kiberbiztonsági kockázatkezelését olyan megközelítésre alapozza, amelynek célja a szervezet hálózati és információs rendszereinek védelme, és amely a következő szakaszokból áll:

a) összefüggések megállapítása;

b) szervezeti szinten végzett kiberbiztonsági kockázatértékelés;

c) kiberbiztonsági kockázatkezelés;

d) kiberbiztonsági kockázatok elfogadása.

(3) Az összefüggések megállapításának szakaszában minden nagy hatású és kritikus hatású szervezet:

a) meghatározza a kiberbiztonsági kockázatértékelés hatókörét, beleértve a villamosenergia-piaci ENTSO és az EU DSO által azonosított nagy hatású és kritikus hatású folyamatokat, valamint más olyan folyamatokat, amelyek a határkeresztező villamosenergia-áramlásokra nagy hatást vagy kritikus hatást gyakorló kibertámadások célpontjai lehetnek; valamint

b) meghatározza a kockázatértékelés és a kockázatelfogadás kritériumait a szervezetek és az illetékes hatóságok által a 19. cikk (2) bekezdésével összhangban kidolgozott uniós, regionális és tagállami szintű kiberbiztonsági kockázatértékelési módszertanokban a kiberbiztonsági kockázatok értékeléséhez felhasználandó kockázati hatásmátrixnak megfelelően.

(4) A kiberbiztonsági kockázatértékelés szakaszában minden nagy hatású és kritikus hatású szervezet:

a) azonosítja a kiberbiztonsági kockázatokat a következők figyelembevételével:

i. az uniós szintű nagy hatású és kritikus hatású folyamatokat támogató valamennyi eszköz, az eszköz veszélyeztetése esetén a határkeresztező villamosenergia-áramlásokra gyakorolt esetleges hatás értékelésével;

ii. lehetséges kiberfenyegetések, figyelembe véve a 23. cikkben említett, a határkeresztező villamos energia kiberbiztonsági kockázatértékeléséről szóló legújabb átfogó jelentésben azonosított kiberfenyegetéseket és az ellátási lánccal kapcsolatos fenyegetéseket;

iii. sérülékenységek, beleértve az örökölt rendszerek sérülékenységeit is;

iv. lehetséges kibertámadási forgatókönyvek, beleértve a villamosenergia-rendszer üzembiztonságát érintő és a határkeresztező villamosenergia-áramlásokat zavaró kibertámadásokat;

v. releváns kockázatértékelések és uniós szinten végzett értékelések, beleértve a kritikus ellátási láncok koordinált kockázatértékelését az (EU) 2022/2555 irányelv 22. cikkével összhangban; valamint

vi. meglévő végrehajtott ellenőrzések.

b) elemzi az a) pontban azonosított kiberbiztonsági kockázatok valószínűségét és következményeit, és meghatározza a kiberbiztonsági kockázati szintet a kiberbiztonsági kockázatok értékeléséhez használt, az átvitelirendszer-üzemeltetők által a 19. cikk (2) bekezdésével összhangban a villamosenergia-piaci ENTSO segítségével és az EU DSO-val együttműködésben kidolgozott uniós, regionális és tagállami szintű kiberbiztonsági kockázatértékelési módszertanokban a kiberbiztonsági kockázatok értékelésére szolgáló kockázati hatásmátrix felhasználásával;

c) osztályozza az eszközöket a kiberbiztonság veszélyeztetésének lehetséges következményei szerint, továbbá a következő lépések alapján meghatározza a nagy hatású és kritikus hatású hatókört:

i. a kiberbiztonsági kockázatértékelés hatálya alá tartozó valamennyi folyamatra vonatkozóan üzleti hatásvizsgálatot végez az ECII felhasználásával;

ii. egy folyamatot nagy hatásúként vagy kritikus hatásúként sorol be, ha az ECII meghaladja a nagy, illetve a kritikus hatásra vonatkozó küszöbértéket;

iii. az összes nagy hatású és kritikus hatású eszközt a nagy hatású, illetve a kritikus hatású folyamatokhoz szükséges eszközként határozza meg;

iv. meghatározza az összes nagy hatású, illetve kritikus hatású eszközt tartalmazó nagy hatású és kritikus hatókört annak érdekében, hogy a hatókörökbe való bejutás ellenőrizhető legyen.

d) értékeli a kiberbiztonsági kockázatokat azáltal, hogy a (3) bekezdés b) pontjában említett kockázatértékelési kritériumok és kockázatelfogadási kritériumok alapján rangsorolja azokat.

(5) A kiberbiztonsági kockázatkezelési szakaszban minden egyes nagy hatású és kritikus hatású szervezet szervezeti szintű kockázatcsökkentési tervet készít, amelyben kiválasztja a kockázatok kezeléséhez megfelelő kockázatkezelési lehetőségeket és azonosítja a fennmaradó kockázatokat.

(6) A kiberbiztonsági kockázatok elfogadásának szakaszában minden nagy hatású és kritikus hatású szervezet eldönti, hogy a (3) bekezdés b) pontjában meghatározott kockázatelfogadási kritériumok alapján elfogadja-e a fennmaradó kockázatot.

(7) Minden nagy hatású és kritikus hatású szervezet eszközleltárban tartja nyilván az (1) bekezdésben meghatározott eszközöket. Ez az eszközleltár nem része a kockázatértékelési jelentésnek.

(8) Az illetékes hatóság az ellenőrzések során megvizsgálhatja a leltárban szereplő eszközöket.

27. cikk

Jelentéstétel a szervezeti szinten végzett kockázatértékelésről

Minden nagy hatású és kritikus hatású szervezet a nagy és kritikus hatású szervezeteknek a 24. cikk (6) bekezdése szerinti bejelentését követő 12 hónapon belül, majd azt követően háromévente jelentést nyújt be az illetékes hatóságnak, amely a következő információkat tartalmazza:

1. a 26. cikk (5) bekezdése alapján a szervezeti szintű kockázatcsökkentési tervhez kiválasztott ellenőrzések listája, az egyes ellenőrzések aktuális végrehajtási állapotával együtt;

2. minden uniós szintű, nagy hatású vagy kritikus hatású folyamat esetében az információk és a releváns eszközök bizalmas jellegének, integritásának és elérhetőségének veszélyeztetésével kapcsolatos kockázatok becslése. E kockázat becslését a 19. cikk (2) bekezdésében szereplő kockázati hatásmátrixnak megfelelően kell megadni;

3. a kritikus hatású folyamataik szempontjából kritikus IKT-szolgáltatók jegyzéke.

III. FEJEZET

A VILLAMOS ENERGIA KÖZÖS KIBERBIZTONSÁGI KERETE

28. cikk

A villamos energia közös kiberbiztonsági keretének összetétele, működése és felülvizsgálata

(1) A villamos energia közös kiberbiztonsági kerete a következő ellenőrzésekből és kiberbiztonsági irányítási rendszerből áll:

a) a 29. cikkel összhangban kidolgozott minimális kiberbiztonsági ellenőrzések;

b) a 29. cikkel összhangban kidolgozott fejlett kiberbiztonsági ellenőrzések;

c) az a) és b) pontban említett ellenőrzéseket a kiválasztott európai és nemzetközi szabványokhoz és nemzeti jogszabályi vagy szabályozási keretekhez képest feltérképező, a 34. cikkel összhangban kidolgozott feltérképezési mátrix;

d) a 32. cikk alapján létrehozott kiberbiztonsági irányítási rendszer.

(2) Nagy hatású hatókörén belül valamennyi nagy hatású szervezet alkalmazza az (1) bekezdés a) pontja szerinti minimális kiberbiztonsági ellenőrzéseket.

(3) Kritikus hatású hatókörén belül valamennyi kritikus hatású szervezet alkalmazza az (1) bekezdés b) pontja szerinti fejlett kiberbiztonsági ellenőrzéseket.

(4) A 19. cikk (4) bekezdése szerinti, az egész Unióra kiterjedő kiberbiztonsági kockázatértékelési jelentés első tervezetének benyújtását követő 7 hónapon belül az (1) bekezdésben említett, a villamos energia közös kiberbiztonsági keretét ki kell egészíteni az ellátási láncon belül a 33. cikknek megfelelően elvégzett minimális és fejlett kiberbiztonsági ellenőrzésekkel.

29. cikk

Minimális és fejlett kiberbiztonsági ellenőrzések

(1) A 19. cikk (4) bekezdése szerinti, az egész Unióra kiterjedő kiberbiztonsági kockázatértékelési jelentés első tervezetének benyújtását követő 7 hónapon belül az átvitelirendszer-üzemeltetők a villamosenergia-piaci ENTSO segítségével és az EU DSO-val együttműködve javaslatot dolgoznak ki a minimális és fejlett kiberbiztonsági ellenőrzésekre vonatkozóan.

(2) A 21. cikk (2) bekezdése szerinti regionális kiberbiztonsági kockázatértékelési jelentések elkészítését követő 6 hónapon belül az átvitelirendszer-üzemeltetők a villamosenergia-piaci ENTSO segítségével és az EU DSO-val együttműködve javaslatot tesznek az illetékes hatóságnak a minimális és fejlett kiberbiztonsági ellenőrzések módosítására. A javaslat a 8. cikk (10) bekezdésével összhangban készül, és figyelembe veszi a regionális kockázatértékelés során azonosított kockázatokat.

(3) A minimális és fejlett kiberbiztonsági ellenőrzések hitelesíthetők valamely nemzeti hitelesítési rendszerben való részvétel alapján, a 31. cikkben meghatározott eljárással összhangban vagy a 25. cikk (2) bekezdésében felsorolt követelményeknek megfelelően, független harmadik fél által végzett biztonsági auditok elvégzésével.

(4) Az (1) bekezdés szerint kidolgozott, eredeti minimális és fejlett kiberbiztonsági ellenőrzések a 19. cikk (5) bekezdésében említett, az egész Unióra kiterjedő kiberbiztonsági kockázatértékelési jelentésben azonosított kockázatokon alapulnak. A (2) bekezdés szerint kidolgozott módosított minimális és fejlett kiberbiztonsági ellenőrzések a 21. cikk (2) bekezdésében említett regionális kiberbiztonsági kockázatértékelési jelentésen alapulnak.

(5) A minimális kiberbiztonsági ellenőrzések magukban foglalják a 46. cikk alapján megosztott információk védelmét szolgáló ellenőrzéseket.

(6) 12 hónappal a minimális és fejlett kiberbiztonsági ellenőrzéseknek a 8. cikk (5) bekezdése szerinti jóváhagyását vagy a 8. cikk (10) bekezdése szerinti aktualizálását követően a 2. cikk (1) bekezdésében felsorolt és a 24. cikk értelmében kritikus hatású vagy nagy hatású szervezetként azonosított szervezetek a 26. cikk (5) bekezdése szerinti, a szervezeti szintű kockázatcsökkentési terv kidolgozása során a nagy hatású hatókörön belül minimális kiberbiztonsági ellenőrzést, a kritikus hatású hatókörön belül pedig fejlett kiberbiztonsági ellenőrzést végeznek.

30. cikk

Eltérések a minimális és fejlett kiberbiztonsági ellenőrzésektől

(1) A 2. cikk (1) bekezdésében felsorolt szervezetek kérhetik az érintett illetékes hatóságtól, hogy engedélyezze a 29. cikk (6) bekezdésében említett minimális és fejlett kiberbiztonsági ellenőrzések alkalmazására irányuló kötelezettségüktől való eltérést. Az illetékes hatóság az alábbi indokok egyike alapján engedélyezheti az eltérést:

a) kivételes körülmények között, ha a szervezet bizonyítani tudja, hogy a megfelelő kiberbiztonsági ellenőrzések végrehajtásának költségei jelentősen meghaladják az előnyöket. Az ACER és a villamosenergia-piaci ENTSO az elosztórendszer-üzemeltetők szervezetével együttműködve közösen iránymutatást dolgozhat ki a kiberbiztonsági ellenőrzések költségeinek becslésére, hogy így segítse a szervezeteket;

b) ha a szervezet olyan szervezeti szintű kockázatkezelési tervet nyújt be, amely alternatív ellenőrzések alkalmazásával a 26. cikk (3) bekezdésének b) pontjában említett kockázatelfogadási kritériumoknak megfelelően elfogadható szintre csökkenti a kiberbiztonsági kockázatokat.

(2) Az (1) bekezdésben említett kérelem kézhezvételétől számított három hónapon belül minden illetékes hatóság határoz arról, hogy engedélyezhető-e a minimális és fejlett kiberbiztonsági ellenőrzésektől való eltérés. A minimális vagy fejlett kiberbiztonsági ellenőrzésektől való eltérés legfeljebb három évre engedélyezhető és meghosszabbítható.

(3) Az engedélyezett eltérésekre vonatkozó összesített és anonimizált információkat a 23. cikkben említett, a határkeresztező villamos energia kiberbiztonsági kockázatértékeléséről szóló legújabb átfogó jelentéshez csatolt mellékletként kell szerepeltetni. A villamosenergia-piaci ENTSO és az EU DSO szükség esetén közösen aktualizálja a felsorolást.

31. cikk

A villamos energia közös kiberbiztonsági keretének hitelesítése

(1) Legkésőbb 24 hónappal a 28. cikk (1) bekezdésének a), b) és c) pontjában említett ellenőrzések elfogadását és az ugyanazon cikk d) pontjában említett kiberbiztonsági irányítási rendszer létrehozását követően a 24. cikk (1) bekezdése szerint azonosított valamennyi kritikus hatású szervezetnek képesnek kell lennie arra, hogy az illetékes hatóság kérésére igazolja a kiberbiztonsági irányítási rendszernek és a minimális vagy fejlett kiberbiztonsági ellenőrzéseknek való megfelelését.

(2) Minden kritikus hatású szervezet a 25. cikk (2) bekezdésében felsorolt követelményekkel összhangban független harmadik fél által végzett biztonsági auditokkal vagy a 25. cikk (1) bekezdése szerinti nemzeti hitelesítési rendszerben való részvétellel teljesíti az (1) bekezdésben említett kötelezettséget.

(3) A kritikus hatású szervezet kritikus hatású hatókörén belüli valamennyi eszközre kiterjed annak hitelesítése, hogy a kritikus hatású szervezet megfelel-e a kiberbiztonsági irányítási rendszernek és a minimális vagy fejlett kiberbiztonsági ellenőrzéseknek.

(4) Annak hitelesítését, hogy a kritikus hatású szervezet megfelel-e a kiberbiztonsági irányítási rendszernek és a minimális vagy fejlett kiberbiztonsági ellenőrzéseknek, legkésőbb az első hitelesítés végét követő 36 hónapon belül, majd azt követően háromévente rendszeresen meg kell ismételni.

(5) Valamennyi, a 24. cikknek megfelelően meghatározott kritikus hatású szervezet oly módon igazolja azt, hogy megfelel a 28. cikk (1) bekezdésének a), b) és c) pontjában említett ellenőrzéseknek, valamint ugyanazon cikk d) pontjában említett kiberbiztonsági irányítási rendszer létrehozásának, hogy jelentést tesz az illetékes hatóságnak a megfelelés hitelesítésének eredményéről.

32. cikk

Kiberbiztonság-irányítási rendszer

(1) 24 hónapon belül azt követően, hogy az illetékes hatóság értesítette őket arról, hogy a 24. cikk (6) bekezdésének megfelelően nagy hatású vagy kritikus hatású szervezetnek minősülnek, minden nagy hatású és kritikus hatású szervezet kiberbiztonsági irányítási rendszert hoz létre, és azt követően háromévente felülvizsgálja e rendszert, hogy:

a) meghatározza a kiberbiztonsági irányítási rendszer hatókörét, figyelembe véve a más szervezetekkel való kapcsolódási pontokat és függőségeket;

b) biztosítsa, hogy teljes felső vezetése tájékoztatást kapjon a vonatkozó jogi kötelezettségekről, és kellő időben hozott döntések és gyors reakciók segítségével aktívan hozzájáruljon a kiberbiztonsági irányítási rendszer végrehajtásához;

c) biztosítsa, hogy a kiberbiztonsági irányítási rendszerhez szükséges erőforrások rendelkezésre állnak;

d) kiberbiztonsági szabályzatot alakítson ki, amelyet dokumentál és közzétesz a szervezeten belül, valamint a biztonsági kockázatok által érintett felek részére;

e) kijelölje és közölje a kiberbiztonság szempontjából fontos szerepekkel kapcsolatos felelősségi köröket;

f) a 26. cikkben meghatározott szervezeti szintű kiberbiztonsági kockázatkezelést végezzen;

g) meghatározza és biztosítja a kiberbiztonsági irányítási rendszer végrehajtásához, karbantartásához és folyamatos fejlesztéséhez szükséges erőforrásokat, figyelembe véve a kiberbiztonsági erőforrások szükséges hozzáértését és ismereteit;

h) meghatározza a kiberbiztonság szempontjából releváns belső és külső kommunikációt;

i) létrehozza, frissítse és ellenőrizze a kiberbiztonsági irányítási rendszerrel kapcsolatban dokumentált információkat;

j) értékelje a kiberbiztonsági irányítási rendszer teljesítményét és hatékonyságát;

k) tervezett időközönként belső auditokat végezzen a kiberbiztonsági irányítási rendszer hatékony végrehajtásának és fenntartásának biztosítása érdekében;

l) tervezett időközönként felülvizsgálja a kiberbiztonsági irányítási rendszer végrehajtását; továbbá ellenőrizze és korrigálja az erőforrásoknak és tevékenységeknek a kiberbiztonsági irányítási rendszer szabályzatainak, eljárásainak és iránymutatásainak való meg nem felelését.

(2) A kiberbiztonsági irányítási rendszer hatálya kiterjed a nagy hatású és kritikus hatású szervezet nagy hatású és kritikus hatású hatókörébe tartozó valamennyi eszközre.

(3) Az illetékes hatóságok egy adott technológiatípus használatának előírása vagy előnyben részesítése nélkül ösztönzik az irányítási rendszerekkel kapcsolatos, valamint a hálózati és információs rendszerek biztonsága szempontjából releváns európai vagy nemzetközi szabványok és előírások alkalmazását.

33. cikk

Minimális és fejlett kiberbiztonsági ellenőrzések az ellátási láncban

(1) A 19. cikk (4) bekezdése szerinti, az egész Unióra kiterjedő kiberbiztonsági kockázatértékelési jelentés első tervezetének benyújtását követő 7 hónapon belül az átvitelirendszer-üzemeltetők a villamosenergia-piaci ENTSO segítségével és az EU DSO-val együttműködve javaslatot dolgoznak ki az ellátási lánc azon minimális és fejlett kiberbiztonsági ellenőrzéseire vonatkozóan, amelyek mérséklik az egész Unióra kiterjedő kiberbiztonsági kockázatértékelésekben azonosított, ellátási láncra vonatkozó kockázatokat, és kiegészítik a 29. cikk szerint kidolgozott minimális és fejlett kiberbiztonsági ellenőrzéseket. Az ellátási láncon belüli minimális és fejlett kiberbiztonsági ellenőrzéseket a 29. cikk szerinti minimális és fejlett kiberbiztonsági ellenőrzésekkel együtt kell kidolgozni. Az ellátási láncban a minimális és fejlett kiberbiztonsági ellenőrzések kiterjednek a nagy hatású vagy kritikus hatású szervezet nagy hatású vagy kritikus hatású hatókörébe tartozó valamennyi IKT-termék, IKT-szolgáltatás és IKT-folyamat teljes életciklusára. Az ellátási lánc minimális és fejlett kiberbiztonsági ellenőrzésére vonatkozó javaslat kidolgozása során konzultálni kell a Kiberbiztonsági Együttműködési Csoporttal.

(2) Az ellátási lánc minimális kiberbiztonsági ellenőrzései a nagy hatású és kritikus hatású szervezetek azon ellenőrzéseiből állnak, amelyek:

a) kiberbiztonsági előírásokra hivatkozó ajánlásokat tartalmaznak az IKT-termékek, az IKT-szolgáltatások és IKT-folyamatok beszerzésére vonatkozóan, legalább a következőkre kiterjedően:

   i. a beszállítónak az ellátási láncban érintett és érzékeny információkkal foglalkozó vagy a szervezet nagy hatású vagy kritikus hatású eszközeihez való hozzáféréssel rendelkező személyzetének háttérellenőrzése. A háttérellenőrzés magában foglalhatja a szervezetnél dolgozó munkatársak vagy szerződéses vállalkozók személyazonosságának és hátterének ellenőrzését a nemzeti joggal és eljárásokkal, valamint a vonatkozó és alkalmazandó uniós joggal, többek között az (EU) 2016/679 rendelettel és az (EU) 2016/680 európai parlamenti és tanácsi irányelvvel ([18]) összhangban. A háttérellenőrzéseknek arányosnak kell lenniük, és szigorúan a szükséges mértékre kell korlátozódniuk. Azokat kizárólag az érintett szervezetet érintő potenciális biztonsági kockázat értékelése céljából kell elvégezni. Arányosnak kell lenniük az üzleti követelményekkel, a megtekintendő információk besorolásával és az érzékelt kockázatokkal, és maga a szervezet, egy átvilágítást végző külső vállalat által vagy kormányzati klíring révén is elvégezhetők;

   ii. az IKT-termékek, IKT-szolgáltatások és IKT-folyamatok biztonságos és ellenőrzött tervezésére, fejlesztésére és gyártására szolgáló folyamatok, amelyek elősegítik az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok tervezését és fejlesztését, beleértve a kiberbiztonságot biztosító megfelelő technikai intézkedéseket;

   iii. az olyan hálózati és információs rendszerek kialakítása, amelyekben az eszközök még akkor sem tekinthetők megbízhatónak, ha biztonságos hatókörön belül vannak, az összes kapott megkeresés ellenőrzését szükségessé teszi, és a legkisebb jogosultság elvét alkalmazza;

   iv. a beszállítónak a szervezet eszközeihez való hozzáférése;

([18]) Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről (HL L 119., 2016.5.4., 89. o.).

v. a beszállítót érintő, a szervezet érzékeny információinak védelmét és az azokhoz való hozzáférés korlátozását szolgáló szerződéses kötelezettségek;

vi. az ezeket alátámasztó kiberbiztonsági beszerzési előírások a beszállító alvállalkozói számára;

vii. a kiberbiztonsági előírások alkalmazásának nyomon követhetősége az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok fejlesztésétől a gyártáson át a szállításig;

viii. a biztonsági frissítések támogatása az IKT-termékek, IKT-szolgáltatások vagy IKT-folyamatok teljes élettartama alatt;

ix. a kiberbiztonság auditálásához való jog a szállító tervezési, fejlesztési és gyártási folyamataiban; valamint

x. a beszállító kockázati profiljának értékelése.

b) előírja az ilyen szervezetek számára, hogy vegyék figyelembe az a) albekezdésben említett közbeszerzési ajánlásokat a beszállítókkal, az együttműködő partnerekkel és az ellátási láncban részt vevő más felekkel kötött szerződések megkötésekor, amelyek kiterjednek az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok szokásos szállítására, valamint az olyan nem kívánt eseményekre és körülményekre, mint a szerződéses partner gondatlansága esetén a szerződések felmondása és átruházása;

c) előírja az ilyen szervezetek számára, hogy vegyék figyelembe a kritikus ellátási láncokra vonatkozóan az (EU) 2022/2555 irányelv 22. cikkének (1) bekezdésével összhangban elvégzett összehangolt biztonsági kockázatértékelések eredményeit;

d) kritériumokat tartalmaz az a) pontban meghatározott kiberbiztonsági előírásoknak megfelelő és a beszállító által szállított IKT-termék, IKT-szolgáltatás vagy IKT-folyamatok kiberbiztonsági kockázatainak megfelelő kiberbiztonsági szinttel rendelkező beszállítók kiválasztására és a velük való szerződéskötésre vonatkozóan;

e) az IKT-termékek, az IKT-szolgáltatások és az IKT-folyamatok beszerzési forrásainak diverzifikálására, valamint a vállalkozóhoz kötöttség kockázatának csökkentésére vonatkozó kritériumokat tartalmaz;

f) az egyes IKT-termékek, IKT-szolgáltatások és IKT-folyamatok teljes életciklusa során rendszeresen meghatározza a beszállítók belső működési folyamataira vonatkozó kiberbiztonsági előírások nyomon követésére, felülvizsgálatára vagy auditálására vonatkozó kritériumokat.

(3) A (2) bekezdés a) pontjában említett kiberbiztonsági beszerzési ajánlásban szereplő kiberbiztonsági előírások tekintetében a nagy hatású vagy kritikus hatású szervezetek a 2014/24/EU európai parlamenti és tanácsi irányelv ([19]) szerinti közbeszerzési elveket alkalmazzák a 35. cikk (4) bekezdésével összhangban, vagy a szervezeti szintű kiberbiztonsági kockázatértékelés eredményei alapján saját előírásokat határoznak meg.

(4) Az ellátási lánc fejlett kiberbiztonsági ellenőrzései magukban foglalják a kritikus hatású szervezetekre vonatkozó ellenőrzéseket a beszerzés során annak ellenőrzése céljából, hogy a kritikus hatású eszközként használt IKT-termékek, IKT-szolgáltatások és IKT-folyamatok megfelelnek-e a kiberbiztonsági előírásoknak. Az IKT-terméket, IKT-szolgáltatást vagy IKT-folyamatot a 31. cikkben említett európai kiberbiztonsági tanúsítási rendszeren keresztül vagy a szervezet által kiválasztott és szervezett hitelesítési tevékenységek segítségével kell hitelesíteni. A hitelesítési tevékenységek részletessége és hatóköre elegendő annak biztosításához, hogy az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat felhasználható legyen a szervezeti szintű kockázatértékelésben azonosított kockázatok csökkentésére. A kritikus hatású szervezet dokumentálja az azonosított kockázatok csökkentése érdekében tett lépéseket.

(5) A releváns IKT-termékek, IKT-szolgáltatások és IKT-folyamatok beszerzésére az ellátási lánc minimális és fejlett kiberbiztonsági ellenőrzései alkalmazandók. Az ellátási lánc minimális és fejlett kiberbiztonsági ellenőrzéseit a 24. cikk értelmében kritikus hatású és nagy hatású szervezetként azonosított szervezetek beszerzési folyamataira a 29. cikkben említett minimális és fejlett kiberbiztonsági ellenőrzések elfogadását vagy aktualizálását követő hat hónap elteltével kell elkezdeni alkalmazni.

([19]) 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.).

(6) A 21. cikk (2) bekezdése szerinti regionális kiberbiztonsági kockázatértékelési jelentések elkészítését követő 6 hónapon belül az átvitelirendszer-üzemeltetők a villamosenergia-piaci ENTSO segítségével és az EU DSO-val együttműködve javaslatot tesznek az illetékes hatóságnak a minimális és fejlett kiberbiztonsági ellenőrzések módosítására az ellátási láncban. A javaslat a 8. cikk (10) bekezdésével összhangban készül, és figyelembe veszi a regionális kockázatértékelés során azonosított kockázatokat.

34. cikk

A villamos energia kiberbiztonsági ellenőrzéseinek a szabványok alapján történő feltérképezésére szolgáló mátrix

(1) A 19. cikk (4) bekezdése szerinti, az egész Unióra kiterjedő kiberbiztonsági kockázatértékelési jelentés első tervezetének benyújtását követő 7 hónapon belül az átvitelirendszer-üzemeltetők a villamosenergia-piaci ENTSO segítségével és az EU DSO-val együttműködve, továbbá az ENISA-val konzultálva javaslatot dolgoznak ki a 28. cikk (1) bekezdésének a) és b) pontjában meghatározott ellenőrzéseknek a kiválasztott európai és nemzetközi szabványokhoz és a vonatkozó műszaki előírásokhoz viszonyított feltérképezésére szolgáló mátrixra (a továbbiakban: feltérképezési mátrix). A villamosenergia-piaci ENTSO és az EU DSO dokumentálja a különböző ellenőrzések és a 28. cikk (1) bekezdésének a) és b) pontjában meghatározott ellenőrzések egyenértékűségét.

(2) Az illetékes hatóságok a villamosenergia-piaci ENTSO és az EU DSO rendelkezésére bocsáthatják a 28. cikk (1) bekezdésének a) és b) pontjában meghatározott ellenőrzések feltérképezését a kapcsolódó nemzeti jogszabályi vagy szabályozási keretekre való hivatkozással, beleértve az (EU) 2022/2555 irányelv 25. cikke szerinti vonatkozó tagállami nemzeti szabványokat is. Ha egy tagállam illetékes hatósága ilyen feltérképezést bocsát rendelkezésre, a villamosenergia-piaci ENTSO és az EU DSO ezt a nemzeti feltérképezést integrálja a feltérképezési mátrixba.

(3) A 21. cikk (2) bekezdése szerinti regionális kiberbiztonsági kockázatértékelési jelentések elkészítését követő 6 hónapon belül az átvitelirendszer-üzemeltetők a villamosenergia-piaci ENTSO segítségével és az EU DSO-val együttműködve, továbbá az ENISA-val konzultálva javaslatot tesznek az illetékes hatóságnak a feltérképezési mátrix módosítására. A javaslat a 8. cikk (10) bekezdésével összhangban készül, és figyelembe veszi a regionális kockázatértékelés során azonosított kockázatokat.

IV. FEJEZET

KIBERBIZTONSÁGI BESZERZÉSI AJÁNLÁSOK

35. cikk

Kiberbiztonsági beszerzési ajánlások

(1) Az átvitelirendszer-üzemeltetők – a villamosenergia-piaci ENTSO segítségével és az EU DSO-val együttműködésben – a regionális kiberbiztonsági kockázatértékelési jelentés elfogadásakor kidolgozandó és aktualizálandó munkaprogramban nem kötelező erejű kiberbiztonsági beszerzési ajánlásokat dolgoznak ki, amelyeket a nagy hatású és kritikus hatású szervezetek felhasználhatnak IKT-termékek, IKT-szolgáltatások és IKT-folyamatok beszerzésének alapjául a nagy hatású és kritikus hatású hatókörökön belül. E munkaprogram a következőket tartalmazza:

a) a nagy hatású és kritikus hatású szervezetek által a nagy hatású és kritikus hatású hatókörökön belül használt IKT-termékek, IKT-szolgáltatások és IKT-folyamatok típusainak leírása és besorolása;

b) azon IKT-termékek, IKT-szolgáltatások és IKT-folyamatok típusainak jegyzéke, amelyekre vonatkozóan az adott regionális kiberbiztonsági kockázatértékelési jelentések, valamint a nagy hatású és kritikus hatású szervezetek prioritásai alapján nem kötelező erejű kiberbiztonsági ajánlásokat kell kidolgozni.

(2) A villamosenergia-piaci ENTSO az EU DSO-val együttműködve a regionális kiberbiztonsági kockázatértékelési jelentés elfogadását vagy aktualizálását követő 6 hónapon belül benyújtja az ACER-nek az említett munkaprogram összefoglalóját.

(3) Az átvitelirendszer-üzemeltetők a villamosenergia-piaci ENTSO segítségével és az EU DSO-val együttműködve törekednek annak biztosítására, hogy a vonatkozó regionális kiberbiztonsági kockázatértékelés alapján kidolgozott, nem kötelező erejű kiberbiztonsági beszerzési ajánlások az egyes rendszerüzemeltetési régiók között hasonlóak vagy összehasonlíthatók legyenek. A kiberbiztonsági beszerzési ajánlások legalább a 33. cikk (2) bekezdésének a) pontjában említett előírásokra kiterjednek. Amennyiben lehetséges, az előírásokat európai és nemzetközi szabványokból kell kiválasztani.

(4) Az átvitelirendszer-üzemeltetők a villamosenergia-piaci ENTSO segítségével és az EU DSO-val együttműködve biztosítják, hogy a kiberbiztonsági beszerzési ajánlások:

a) megfeleljenek a 2014/24/EU irányelv szerinti közbeszerzési elveknek; valamint

b) kompatibilisek legyenek az IKT-termék, az IKT-szolgáltatás vagy az IKT-folyamat szempontjából releváns legújabb rendelkezésre álló európai kiberbiztonsági tanúsítási rendszerekkel, és figyelembe vegyék azokat.

36. cikk

Iránymutatás az európai kiberbiztonsági tanúsítási rendszerek IKT-termékek, IKT-szolgáltatások és IKT-folyamatok beszerzésére való alkalmazásához

(1) A 35. cikk alapján kidolgozott, nem kötelező erejű kiberbiztonsági beszerzési ajánlások tartalmazhatnak ágazatspecifikus iránymutatást az európai kiberbiztonsági tanúsítási rendszerek használatához, amennyiben a kritikus hatású szervezetek által használt IKT-termék, IKT-szolgáltatás vagy IKT-folyamat tekintetében megfelelő rendszer áll rendelkezésre, az (EU) 2019/881 rendelet 46. cikke szerinti, az európai kiberbiztonsági tanúsítási rendszerek létrehozására vonatkozó keret sérelme nélkül.

(2) Az átvitelirendszer-üzemeltetők a villamosenergia-piaci ENTSO segítségével és az EU DSO-val együttműködve szorosan együttműködnek az ENISA-val az (1) bekezdés szerinti, nem kötelező erejű kiberbiztonsági beszerzési ajánlásokban foglalt ágazatspecifikus iránymutatások kidolgozása során.

V. FEJEZET

INFORMÁCIÓÁRAMLÁS, KIBERTÁMADÁSOK ÉS VÁLSÁGKEZELÉS

37. cikk

Az információmegosztás szabályai

(1) Ha egy illetékes hatóság bejelentendő kibertámadással kapcsolatos információt kap, az említett illetékes hatóság:

a) értékeli az információ bizalmas jellegének mértékét, és indokolatlan késedelem nélkül, de legkésőbb az információ kézhezvételétől számított 24 órán belül tájékoztatja a szervezetet az értékelésének eredményéről;

b) kísérletet tesz arra, hogy az Unióban más illetékes hatóságoknak bejelentett hasonló kibertámadást találjon annak érdekében, hogy a bejelentendő kibertámadással összefüggésben kapott információkat összekapcsolja az egyéb kibertámadásokkal összefüggésben szolgáltatott információkkal, és ily módon gazdagítsa a meglévő információkat, megerősítse és koordinálja a kiberbiztonsági válaszlépéseket;

c) felelős az üzleti titkok eltávolításáért és az információk anonimizálásáért a vonatkozó nemzeti és uniós szabályokkal összhangban;

d) indokolatlan késedelem nélkül, de legkésőbb 24 órával a bejelentendő kibertámadás kézhezvételét követően megosztja az információkat a nemzeti egyedüli kapcsolattartó pontokkal, a CSIRT-ekkel és a többi tagállamban a 4. cikk szerint kijelölt valamennyi illetékes hatósággal, továbbá rendszeresen naprakész információkkal látja el ezeket a hatóságokat vagy szerveket;

e) az üzleti titkok (1) bekezdés c) pontja szerinti anonimizálását és eltávolítását követően indokolatlan késedelem nélkül, de legkésőbb az (1) bekezdés a) pontja szerinti információ kézhezvételét követő 24 órán belül továbbítja a kibertámadásra vonatkozó információkat a saját tagállamában található kritikus hatású és nagy hatású szervezeteknek, és rendszeresen naprakész információkat szolgáltat, amelyek lehetővé teszik a szervezetek számára, hogy hatékonyan megszervezzék védelmüket;

f) felkérheti a nagy hatású vagy kritikus hatású szervezetet, hogy a bejelentendő kibertámadásra vonatkozó információkat biztonságos módon terjessze az esetlegesen érintett más szervezetek részére azzal a céllal, hogy fokozza a villamosenergia-ágazat helyzetismeretét, és megelőzze a határkeresztező villamos energiát érintő kiberbiztonsági esemény során esetlegesen eszkalálódó kockázat bekövetkezését;

g) az üzleti titkok anonimizálását és eltávolítását követően a kibertámadásra vonatkozó információkat tartalmazó összefoglaló jelentést oszt meg az ENISA-val.

(2) Ha a CSIRT kijavítatlan, aktívan kihasznált sérülékenységről szerez tudomást, akkor:

a) megfelelően biztonságos információcsere-csatornán keresztül haladéktalanul megosztja azt az ENISA-val, kivéve, ha más uniós jogszabály másként rendelkezik;

b) támogatja az érintett szervezetet abban, hogy a gyártó vagy a szolgáltató biztosítsa részére a kijavítatlan, aktívan kihasznált sérülékenység hatékony, összehangolt és gyors kezelését vagy hatékony és eredményes enyhítő intézkedéseket;

c) megosztja a rendelkezésre álló információkat az értékesítővel, és lehetőség szerint felkéri a gyártót vagy a szolgáltatót, hogy azonosítsa a kijavítatlan, aktívan kihasznált sérülékenység által érintett tagállamokban működő CSIRT-ek jegyzékét, amelyeket tájékoztatni kell;

d) megosztja a rendelkezésre álló információkat az előző pontban azonosított CSIRT-ekkel a szükséges ismeret elve alapján;

e) megosztja a bejelentett kijavítatlan, aktívan kihasznált sérülékenységgel kapcsolatos mérséklési stratégiákat és intézkedéseket, amennyiben vannak ilyenek.

(3) Ha az illetékes hatóság kijavítatlan, aktívan kihasznált sérülékenységről szerez tudomást, akkor:

a) a saját tagállamában működő CSIRT-ekkel egyeztetve megosztja a bejelentett kijavítatlan, aktívan kihasznált sérülékenységre vonatkozó mérséklési stratégiákat és intézkedéseket, amennyiben vannak ilyenek;

b) megosztja az információkat annak a tagállamnak a CSIRT-jével, ahol a kijavítatlan, aktívan kihasznált sérülékenységet bejelentették.

(4) Ha az illetékes hatóság kijavítatlan sérülékenységről szerez tudomást anélkül, hogy azt bizonyíthatóan aktívan kihasználnák, indokolatlan késedelem nélkül egyeztet a CSIRT-tel a sérülékenységeknek az (EU) 2022/2555 irányelv 12. cikkének (1) bekezdésében meghatározott, összehangolt közzététele céljából.

(5) Ha a CSIRT a 38. cikk (6) bekezdése alapján kiberfenyegetésekkel kapcsolatos információkat kap egy vagy több nagy hatású vagy kritikus hatású szervezettől, akkor indokolatlan késedelem nélkül, de legkésőbb az információ kézhezvételétől számított négy órán belül továbbítja ezeket az információkat vagy bármely más, a kapcsolódó kockázat megelőzése, felderítése, kezelése vagy csökkentése szempontjából fontos információt a tagállamában található kritikus hatású és nagy hatású szervezetek, valamint adott esetben valamennyi érintett CSIRT és a tagállama nemzeti egyedüli kapcsolattartó pontjának részére.

(6) Ha egy illetékes hatóság egy vagy több nagy hatású vagy kritikus hatású szervezettől származó, kiberfenyegetésekkel kapcsolatos információról szerez tudomást, az (5) bekezdés alkalmazásában továbbítja ezeket az információkat a CSIRT-nek.

(7) Az illetékes hatóságok – az érintett illetékes hatóságok közötti megállapodást követően – az egynél több tagállamban működő egy vagy több nagy hatású vagy kritikus hatású szervezetre vonatkozó, (3) és (4) bekezdés szerinti felelősségi köröket részben vagy egészben átruházhatják az érintett tagállamok valamelyikében működő másik illetékes hatóságra.

(8) Az átvitelirendszer-üzemeltetők a villamosenergia-piaci ENTSO segítségével és az EU DSO-val együttműködve 2025. június 13-án kidolgozzák a kibertámadások besorolási skálájának módszertanát. Az átvitelirendszer-üzemeltetők a villamosenergia-piaci ENTSO és az EU DSO segítségével felkérhetik az illetékes hatóságokat, hogy konzultáljanak az ENISA-val és a kiberbiztonságért felelős illetékes hatóságaikkal az ilyen besorolási skála kidolgozásához nyújtandó segítség céljából. A módszertan 5 szintbe sorolja be a kibertámadás súlyosságát, amelyek közül a két legmagasabb szint a „magas” és a „kritikus”. A besorolás a következő paraméterek értékelésén alapul:

a) az esetleges hatás, figyelembe véve a 26. cikk (4) bekezdésének c) pontjával összhangban meghatározott, kitett eszközöket és hatóköröket; valamint

b) a kibertámadás súlyossága.

(9) 2026. június 13-án a villamosenergia-piaci ENTSO az EU DSO-val együttműködésben megvalósíthatósági tanulmányt készít egy olyan közös eszköz kifejlesztésének lehetősége és a szükséges pénzügyi költségek felmérése céljából, amely lehetővé teszi valamennyi szervezet számára, hogy információkat osszon meg az érintett nemzeti hatóságokkal.

(10) A megvalósíthatósági tanulmány foglalkozik annak lehetőségével, hogy egy ilyen közös eszköz:

a) támogassa a kritikus hatású és nagy hatású szervezeteket a határkeresztező villamosenergia-áramlások műveleteire vonatkozó releváns, biztonsági vonatkozású információkkal, mint például a kibertámadások közel valós idejű bejelentése, a kiberbiztonsági kérdésekkel kapcsolatos korai riasztások és a villamosenergia-rendszerben használt berendezések nyilvánosságra nem hozott sebezhetőségei;

b) megfelelő és rendkívül megbízható környezetben működjön;

c) tegye lehetővé a kritikus hatású és nagy hatású szervezetektől történő adatgyűjtést, és segítse elő a bizalmas információk eltávolítását és az adatok anonimizálását, valamint azok gyors terjesztését a kritikus hatású és nagy hatású szervezetek felé.

(11) A villamosenergia-piaci ENTSO az EU DSO-val együttműködve:

a) a megvalósíthatóság értékelése során konzultál az ENISA-val és a Kiberbiztonsági Együttműködési Csoporttal, a nemzeti egyedüli kapcsolattartókkal és a fő érdekelt felek képviselőivel;

b) benyújtja a megvalósíthatósági tanulmány eredményeit az ACER-nek és a Kiberbiztonsági Együttműködési Csoportnak.

(12) A villamosenergia-piaci ENTSO az EU DSO-val együttműködve elemezheti és elősegítheti a kritikus hatású és nagy hatású szervezetek által az ilyen információmegosztási eszközök értékelésére és tesztelésére javasolt kezdeményezéseket.

38. cikk

A nagy hatású és kritikus hatású szervezetek szerepe az információmegosztásban

(1) Minden nagy hatású és kritikus hatású szervezet:

a) a 26. cikk (4) bekezdésének c) pontja szerint meghatározott kiberbiztonsági hatókörébe tartozó valamennyi eszköz tekintetében létrehozza legalább a CSOC-képességeket, hogy:

i. biztosítsa, hogy az érintett hálózati és információs rendszerek és alkalmazások biztonsági naplókat készítsenek a biztonsági nyomon követéshez, ami lehetővé teszi az anomáliák észlelését és a kibertámadásokkal kapcsolatos információk gyűjtését;

ii. biztonsági nyomon követést végezzen, beleértve a hálózati és információs rendszerekbe történő behatolások észlelését és e rendszerek sebezhetőségeinek értékelését;

iii. elemezzen és szükség esetén meghozzon minden, a felelősségi körébe és kapacitásába tartozó olyan intézkedést, amely a szervezet védelme érdekében szükséges;

iv. részt vegyen az e cikkben leírt információgyűjtésben és -megosztásban.

b) jogosult arra, hogy az a) pont szerinti képességek egészét vagy egy részét MSSP-ken keresztül szerezze be. A kritikus hatású és nagy hatású szervezetek továbbra is felelősek az MSSP-kért, és felügyelik azok törekvéseit;

c) egyetlen kapcsolattartó pontot jelöl ki szervezeti szinten az információmegosztás céljára.

(2) Az ENISA az (EU) 2019/881 rendelet 6. cikkének (2) bekezdésében meghatározott feladata részeként nem kötelező erejű iránymutatást adhat ki az ilyen képességek létrehozásáról vagy a szolgáltatásnak az MSSP-k részére történő alvállalkozásba adásáról.

(3) Minden kritikus hatású és nagy hatású szervezet indokolatlan késedelem nélkül, de legkésőbb négy órával azt követően, hogy tudomást szerzett arról, hogy a biztonsági esemény bejelentendő, megosztja a bejelentendő kibertámadással kapcsolatos releváns információkat a CSIRT-jeivel és illetékes hatóságával.

(4) A kibertámadással kapcsolatos információk akkor minősülnek bejelentendőnek, ha a kibertámadásnak az érintett szervezet általi értékelése azt állapítja meg, hogy a kibertámadások 37. cikk (8) bekezdése szerinti besorolási skálája alapján a támadás kritikussága a „nagytól" „kritikusig" terjed. A biztonsági események besorolását az (1) bekezdés c) pontja szerint kijelölt szervezeti szintű egyedüli kapcsolattartó pont közli.

(5) Amennyiben a kritikus hatású és nagy hatású szervezetek kijavítatlan, aktívan kihasznált sérülékenységekkel kapcsolatos releváns információkat jelentenek be a CSIRT-nek, ez utóbbi továbbíthatja ezeket az információkat az illetékes hatóságnak. A bejelentett információk érzékenységének mértékére tekintettel a CSIRT indokolt kiberbiztonsági okokból visszatarthatja az információt vagy késleltetheti annak továbbítását.

(6) Minden kritikus hatású és nagy hatású szervezet indokolatlan késedelem nélkül a CSIRT-jei rendelkezésére bocsát minden olyan bejelentendő kiberfenyegetéssel kapcsolatos információt, amelynek határokon átnyúló hatása lehet. A kiberfenyegetéssel kapcsolatos információk akkor minősülnek bejelentendőnek, ha az alábbi feltételek közül legalább egy teljesül:

a) releváns információkat nyújt más kritikus hatású és nagy hatású szervezetek számára a kockázat megelőzéséhez, felderítéséhez, kezeléséhez vagy hatásának enyhítéséhez;

b) a támadással összefüggésben alkalmazott azonosított technikák, taktikák és eljárások olyan információkhoz vezetnek, mint például a sérült URL-címek vagy IP-címek, hashek vagy bármely más, a támadás kontextusba helyezése és korrelálása szempontjából hasznos attribútum;

c) a kiberfenyegetés az e rendelet hatálya alá nem tartozó szolgáltatók vagy harmadik felek által nyújtott további információkkal tovább értékelhető és kontextusba helyezhető.

(7) Az e cikk szerinti információmegosztás során minden kritikus hatású szervezet és nagy hatású szervezet meghatározza a következőket:

a) hogy az információkat e rendelet alapján nyújtották-e be;

b) az információk a következőkre vonatkoznak-e:

   i. a (3) bekezdésben említett bejelentendő kibertámadás;

   ii. a (4) bekezdésben említett, nyilvánosan nem ismert, kijavítatlan, aktívan kihasznált sérülékenységek;

   iii. az (5) bekezdésben említett bejelentendő kiberfenyegetés;

c) bejelentendő kibertámadás esetén a kibertámadás szintje a kibertámadásoknak a 37. cikk (8) bekezdésében említett besorolási skála módszertana szerint, valamint az e besorolás alapjául szolgáló információk, beleértve legalább a kibertámadás kritikusságát.

(8) Amennyiben egy kritikus vagy nagy hatású szervezet az (EU) 2022/2555 irányelv 23. cikke alapján jelent be jelentős biztonsági eseményt, és az említett cikk szerinti eseménybejelentés az e cikk (3) bekezdésében előírt releváns információkat tartalmaz, a szervezetnek az említett irányelv 23. cikkének (1) bekezdése szerinti bejelentése az e cikk (3) bekezdése szerinti információbejelentésnek minősül.

(9) Minden kritikus hatású és nagy hatású szervezet jelentést tesz illetékes hatóságának vagy CSIRT-jének, amelyben egyértelműen meghatározza azokat a konkrét információkat, amelyeket csak abban az esetben lehet megosztani az illetékes hatósággal vagy a CSIRT-tel, ha az információmegosztás kibertámadás forrása lehet. Minden kritikus hatású és nagy hatású szervezetnek jogában áll az információk betekinthető változatát az illetékes CSIRT rendelkezésére bocsátani.

39. cikk

Kibertámadások felderítése és a kapcsolódó információk kezelése

(1) A kritikus hatású és nagy hatású szervezetek az érintett illetékes hatóság, a villamosenergia-piaci ENTSO és az EU DSO részéről kapott szükséges támogatással alakítják ki a felderített kibertámadások kezeléséhez szükséges képességeket. A kritikus hatású és nagy hatású szervezeteket – az (EU) 2022/2555 irányelv 11. cikke (5) bekezdésének a) pontja által a CSIRT-ekre ruházott feladat részeként – támogathatja az adott tagállamban kijelölt CSIRT. A kritikus hatású és nagy hatású szervezetek a kibertámadások hatásának minimalizálása érdekében hatékony eljárásokat vezetnek be az olyan kibertámadások azonosítására, besorolására és az azokra való reagálásra, amelyek hatással lesznek vagy hatással lehetnek a határkeresztező villamosenergia-áramlásokra.

(2) Ha a kibertámadás hatással van a határkeresztező villamosenergia-áramlásokra, az érintett kritikus hatású és nagy hatású szervezeteknek a szervezeti szintű egyedüli kapcsolattartó pontjai együttműködnek egymással az információk megosztása érdekében, amely együttműködést annak a tagállamnak az illetékes hatósága koordinál, amelyben a kibertámadást először jelentették.

(3) A kritikus hatású és nagy hatású szervezetek:

a) biztosítják, hogy saját, szervezeti szintű egyedüli kapcsolattartó pontjuk a szükséges ismeret elve alapján hozzáférjen azokhoz az információkhoz, amelyeket a nemzeti egyedüli kapcsolattartó ponttól az illetékes hatóságukon keresztül kaptak;

b) amennyiben erre az (EU) 2022/2555 irányelv 3. cikkének (4) bekezdése alapján még nem került sor, értesítik a székhelyük szerinti tagállam illetékes hatóságát és a nemzeti egyedüli kapcsolattartó pontot a szervezeti szintű kiberbiztonsági egyedüli kapcsolattartó pontjaik jegyzékével együtt:

   i. amelytől a szóban forgó illetékes hatóság és nemzeti egyedüli kapcsolattartó pont várhatóan bejelentendő kibertámadásokat fog kapni;

   ii. amelynek az illetékes hatóságoknak és a nemzeti egyedüli kapcsolattartó pontoknak esetleg információt kell szolgáltatniuk.

c) kibertámadás-kezelési eljárásokat hoznak létre a kibertámadásokra vonatkozóan, beleértve a szerepeket és felelősségi köröket, feladatokat és reakciókat a kibertámadásnak a kritikus hatású és nagy hatású hatókörökön belül megfigyelhető alakulása alapján;

d) legalább évente tesztelik az átfogó kibertámadás-kezelési eljárásokat, legalább egy olyan forgatókönyv tesztelésével, amely közvetlenül vagy közvetve érinti a határkeresztező villamosenergia-áramlásokat. Ezt az éves tesztet a kritikus hatású és nagy hatású szervezetek is elvégezhetik a 43. cikkben említett rendszeres gyakorlatok során. A kibertámadásokra való reagálási terv éves tesztjeként szolgálhat minden olyan éles kibertámadásra való reagálási tevékenység, amelynek következménye a 37. cikk (8) bekezdésében említett kibertámadás-besorolási skála módszertana szerint legalább 2. fokozatú és a kiberbiztonsági kiváltó okkal rendelkezik.

(4) Az (1) bekezdésben említett feladatokat a tagállamok az (EU) 2019/943 rendelet 37. cikkének (2) bekezdésével összhangban a regionális koordinációs központokra is átruházhatják.

40. cikk

Válságkezelés

(1) Amennyiben az illetékes hatóság megállapítja, hogy a villamosenergia-ellátási válság olyan kibertámadáshoz kapcsolódik, amely egynél több tagállamot érint, az érintett tagállamok illetékes hatóságai, a kiberbiztonságért felelős illetékes hatóságok, a kockázati készültség tekintetében illetékes hatóságok és a kiberválságok kezelésével foglalkozó hatóságok közösen hoznak létre egy határokon átnyúló eseti válságkoordinációs csoportot.

(2) A határokon átnyúló eseti válságkoordinációs csoport:

a) koordinálja az összes releváns kiberbiztonsági információ hatékony lekérdezését és a válságkezelési folyamatban részt vevő szervezetek részére történő további terjesztését;

b) megszervezi a válság által érintett valamennyi szervezet és az illetékes hatóságok közötti kommunikációt az átfedések csökkentése, valamint az elemzések és a technikai válaszlépések hatékonyságának növelése érdekében, a kiberbiztonsági kiváltó okkal rendelkező egyidejű villamosenergia-ellátási válságok orvoslása érdekében;

c) az illetékes CSIRT-ekkel együttműködve biztosítja a szükséges szakértelmet, beleértve a biztonsági esemény által érintett szervezetek számára a lehetséges kockázatcsökkentő intézkedések végrehajtásával kapcsolatos operatív tanácsadást is;

d) értesíti a Bizottságot és a villamosenergia-ügyi koordinációs csoportot és rendszeres tájékoztatást ad részükre a biztonsági esemény állásáról, a 46. cikkben meghatározott védelmi elvek szerint;

e) tanácsot kér az érintett hatóságoktól, ügynökségektől vagy szervezetektől, amelyek segíthetnek a villamosenergia-ellátási válság enyhítésében.

(3) Amennyiben a kibertámadás nagyszabású kiberbiztonsági eseménynek minősül vagy várhatóan annak fog minősülni, a határokon átnyúló eseti válságkoordinációs csoport haladéktalanul tájékoztatja az esemény által érintett tagállamok kiberválságok kezelésével foglalkozó nemzeti hatóságait az (EU) 2022/2555 irányelv 9. cikkének (1) bekezdésével összhangban, valamint a Bizottságot és az EU CyCLONe-t. Ilyen helyzetben a határokon átnyúló eseti válságkoordinációs csoport támogatja az EU CyCLONe-t az ágazati sajátosságok tekintetében.

(4) A kritikus hatású és nagy hatású szervezetek képességekkel, belső iránymutatásokkal, felkészültségi tervekkel és olyan munkatársakkal rendelkeznek, akik részt vehetnek a határokon átnyúló válságok felderítésében és enyhítésében. Az egyidejű villamosenergia-ellátási válság által érintett kritikus hatású vagy nagy hatású szervezet az illetékes hatóságával együttműködve kivizsgálja a válság kiváltó okát annak meghatározása érdekében, hogy a válság milyen mértékben kapcsolódik kibertámadáshoz.

(5) A (4) bekezdés szerinti feladatokat a tagállamok az (EU) 2019/943 rendelet 37. cikkének (2) bekezdésével összhangban a regionális koordinációs központokra is átruházhatják.

41. cikk

Kiberbiztonsági válságkezelési és -reagálási tervek

(1) Az egész Unióra kiterjedő kockázatértékelési jelentésnek az ACER részére történő benyújtását követő 24 hónapon belül az ACER az ENISA-val, a villamosenergia-piaci ENTSO-val, az EU DSO-val, a kiberbiztonságért felelős illetékes hatóságokkal, az illetékes hatóságokkal, a kockázati készültség tekintetében illetékes hatóságokkal, a nemzeti szabályozó hatóságokkal és a nemzeti kiberbiztonsági válságkezelési hatóságokkal szorosan együttműködve uniós szintű kiberbiztonsági válságkezelési és -reagálási tervet dolgoz ki a villamosenergia-ágazatra vonatkozóan.

(2) A villamosenergia-ágazatra vonatkozó uniós szintű kiberbiztonsági válságkezelési és -reagálási tervnek az ACER általi, az (1) bekezdés szerinti kidolgozását követő 12 hónapon belül minden illetékes hatóság nemzeti kiberbiztonsági válságkezelési és -reagálási tervet dolgoz ki a határkeresztező villamosenergia-áramlásokra vonatkozóan, figyelembe véve az uniós szintű kiberbiztonsági válságkezelési tervet és az (EU) 2019/941 rendelet 10. cikkével összhangban kidolgozott nemzeti kockázati készültségi tervet. E terv összhangban áll az (EU) 2022/2555 irányelv 9. cikkének (4) bekezdése szerinti nagyszabású kiberbiztonsági eseményekre és válságelhárításra vonatkozó tervvel. Az illetékes hatóság egyeztet a kritikus hatású és nagy hatású szervezetekkel és a saját tagállamában működő, a kockázati készültség tekintetében illetékes hatósággal.

(3) Az (EU) 2022/2555 irányelv 9. cikkének (4) bekezdése alapján előírt, a nagyszabású kiberbiztonsági események és válságok elhárítására szolgáló nemzeti tervet e cikk értelmében nemzeti kiberbiztonsági válságkezelési tervnek kell tekinteni, ha a határkeresztező villamosenergia-áramlásokra vonatkozó válságkezelési és -reagálási rendelkezéseket tartalmaz.

(4) Az (1) és (2) bekezdésben felsorolt feladatokat a tagállamok az (EU) 2019/943 rendelet 37. cikkének (2) bekezdésével összhangban a regionális koordinációs központokra is átruházhatják.

(5) A kritikus hatású és nagy hatású szervezetek biztosítják, hogy kiberbiztonsággal kapcsolatos válságkezelési folyamataik:

a) rendelkezzenek az (EU) 2022/2555 irányelv 6. cikkének 8. pontjában meghatározott, összeegyeztethető, határokon átnyúló kiberbiztonsági események kezelésére szolgáló eljárásokkal, amelyeket hivatalosan beépítettek válságkezelési terveikbe;

b) az általános válságkezelési tevékenységek részét képezzék.

(6) A nagy és kritikus hatású szervezeteknek a 24. cikk (6) bekezdése szerinti értesítését követő 12 hónapon belül, majd azt követően háromévente a kritikus hatású és a nagy hatású szervezetek a kiberbiztonsággal kapcsolatos válságokra vonatkozó, szervezeti szintű válságkezelési tervet dolgoznak ki, amelyet beépítenek az általános válságkezelési tervükbe. A terv tartalmazza legalább az alábbiakat:

a) a válsághelyzet bejelentésére vonatkozó szabályok, amelyeket az (EU) 2019/941 az rendelet 14. cikkének (2) és (3) bekezdése állapít meg;

b) egyértelmű szerepek és felelősségi körök a válságkezelésben, beleértve az egyéb releváns kritikus hatású és nagy hatású szervezetek szerepét is;

c) naprakész kapcsolattartási információk, valamint a válsághelyzet alatti kommunikációra és információmegosztásra vonatkozó szabályok, beleértve a CSIRT-ekkel való kapcsolatot is.

(7) Az (EU) 2022/2555 irányelv 21. cikke (2) bekezdésének c) pontja szerinti válságkezelési intézkedéseket az e cikk szerinti, a villamosenergia-ágazatra vonatkozó szervezetszintű válságkezelési tervnek kell tekinteni, ha a (6) bekezdésben felsorolt valamennyi követelményt tartalmazza.

(8) A válságkezelési terveket a 43., 44. és 45. cikkben említett kiberbiztonsági gyakorlatok során kell tesztelni.

(9) A kritikus hatású és nagy hatású szervezetek a kritikus hatású és nagy hatású folyamatokra vonatkozó üzletmenet-folytonossági terveikbe a szervezeti szintű válságkezelési terveiket is beépítik. A szervezeti szintű válságkezelési tervek a következőket tartalmazzák:

a) az IT-szolgáltatások rendelkezésre állásától, integritásától és megbízhatóságától függő folyamatok;

b) minden üzletmenet-folytonossági helyszín, a hardver és szoftver helyét is beleértve;

c) az üzletmenet-folytonossági folyamatokhoz kapcsolódó valamennyi belső szerep és felelősség.

(10) A kritikus hatású és nagy hatású szervezetek legalább háromévente, továbbá szükség esetén aktualizálják szervezeti szintű válságkezelési terveiket.

(11) Az ACER legalább háromévente, továbbá szükség esetén aktualizálja a villamosenergia-ágazatra vonatkozóan az (1) bekezdés szerint kidolgozott uniós szintű kiberbiztonsági válságkezelési és -reagálási tervet.

(12) Minden illetékes hatóság legalább háromévente, továbbá szükség esetén aktualizálja a (2) bekezdés szerint kidolgozott, a határkeresztező villamosenergia-áramlásokra vonatkozó nemzeti kiberbiztonsági válságkezelési és -reagálási tervet.

(13) A kritikus hatású és nagy hatású szervezetek legalább háromévente vagy a kritikus hatású folyamat jelentős változásait követően tesztelik üzletmenet-folytonossági terveiket. Az üzletmenet-folytonossági terv tesztelésének eredményét dokumentálni kell. A kritikus hatású és nagy hatású szervezetek a kiberbiztonsági gyakorlatokba belefoglalhatják üzletmenet-folytonossági tervük tesztelését.

(14) A kritikus hatású és nagy hatású szervezetek szükség esetén, és – a teszt eredményének figyelembevételével – legalább háromévente frissítik üzletmenet-folytonossági tervüket.

(15) Ha a teszt hiányosságokat tár fel az üzletmenet-folytonossági tervben, a kritikus hatású és nagy hatású szervezet a tesztelést követő 180 naptári napon belül korrigálja ezeket a hiányosságokat, és új tesztelést végez a korrekciós intézkedések hatékonyságának bizonyítása érdekében.

(16) Amennyiben egy kritikus hatású vagy nagy hatású szervezet 180 naptári napon belül nem tudja kijavítani a hiányosságokat, ennek okait fel kell tüntetnie az illetékes hatóságához a 27. cikknek megfelelően benyújtandó jelentésben.

42. cikk

Korai kiberbiztonsági riasztási képességek a villamosenergia-ágazat számára

(1) Az illetékes hatóságok az (EU) 2019/881 rendelet 6. cikkének (2) és (7) bekezdése értelmében a tagállamoknak nyújtott segítség részeként együttműködnek az ENISA-val a villamosenergia-kiberbiztonsági korai riasztási képességek (ECEAC) fejlesztése érdekében.

(2) Az ECEAC lehetővé teszi az ENISA számára, hogy az (EU) 2019/881 rendelet 7. cikkének (7) bekezdésében felsorolt feladatok ellátása során:

a) önkéntesen megosztott információkat gyűjtsön a következőktől:

   i. CSIRT-ek, illetékes hatóságok;

   ii. az e rendelet 2. cikkében felsorolt szervezetek;

   iii. bármely más szervezet, amely a releváns információkat önkéntes alapon kívánja megosztani.

b) értékeli és osztályozza az összegyűjtött információkat;

c) értékeli azokat az információkat, amelyekhez az ENISA hozzáfér a kiberkockázati feltételek és a határkeresztező villamosenergia-áramlás szempontjaira vonatkozó releváns mutatók azonosításához;

d) azonosítja azokat a feltételeket és mutatókat, amelyek gyakran korrelálnak a villamosenergia-ágazaton belüli kibertámadásokkal;

e) meghatározza, hogy szükség van-e további elemzésekre és megelőző intézkedésekre a kockázati tényezők értékelése és azonosítása révén;

f) tájékoztatja az illetékes hatóságokat az azonosított kockázatokról és az érintett szervezetekre vonatkozóan javasolt megelőző intézkedésekről;

g) tájékoztatja a 2. cikkben felsorolt valamennyi érintett szervezetet az e bekezdés b), c) és d) pontjával összhangban értékelt információk eredményeiről;

h) rendszeres időközönként belefoglalja a releváns információkat az (EU) 2019/881 rendelet 7. cikkének (6) bekezdésével összhangban kiadott helyzetismereti jelentésbe;

i) amennyiben lehetséges, az összegyűjtött információkból levezeti azokat az alkalmazandó adatokat, amelyek a biztonság esetleges megsértésére vagy kibertámadásra utalnak (a továbbiakban: fertőzöttségi mutató).

(3) A CSIRT-ek az (EU) 2022/2555 irányelv 11. cikke (3) bekezdésének b) pontjában meghatározott feladataik keretében haladéktalanul továbbítják az érintett szervezeteknek az ENISA-tól kapott információkat.

(4) Az ACER nyomon követi az ECEAC hatékonyságát. Az ENISA az (EU) 2019/881 rendelet 6. cikkének (2) bekezdése és 7. cikkének (1) bekezdése értelmében minden szükséges információ rendelkezésre bocsátásával segíti az ACER-t. E nyomonkövetési tevékenység elemzése az e rendelet 12. cikke szerinti nyomon követés részét képezi.

VI. FEJEZET

A VILLAMOS ENERGIÁRA VONATKOZÓ KIBERBIZTONSÁGI GYAKORLAT KERETE

43. cikk

Szervezeti és tagállami szintű kiberbiztonsági gyakorlatok

(1) A kritikus hatású szervezetek bejelentését követő év december 31-ig, majd azt követően háromévente minden kritikus hatású szervezet kiberbiztonsági gyakorlatot végez, amely magában foglal egy vagy több, a határkeresztező villamosenergia-áramlásokat közvetlenül vagy közvetve érintő, valamint a 20. és a 27. cikk szerinti, tagállami és szervezeti szintű kiberbiztonsági kockázatértékelések során azonosított kockázatokhoz kapcsolódó kibertámadásokra vonatkozó forgatókönyvet.

(2) Az (1) bekezdéstől eltérve, a kockázati készültség tekintetében illetékes hatóság az illetékes hatósággal és az (EU) 2022/2555 irányelvben a 9. cikk szerint kijelölt vagy létrehozott érintett kibervválságkezelő hatósággal folytatott konzultációt követően dönthet úgy, hogy a szervezeti szintű kiberbiztonsági gyakorlat helyett az (1) bekezdésben leírtak szerinti, tagállami szintű kiberbiztonsági gyakorlatot szervez. E tekintetben az illetékes hatóság tájékoztatja a következőket:

a) tagállamának valamennyi kritikus hatású szervezetét, a nemzeti szabályozó hatóságot, a CSIRT-eket és a kiberbiztonságért felelős illetékes hatóságot legkésőbb a szervezeti szintű kiberbiztonsági gyakorlatot megelőző év június 30-ig;

b) minden olyan szervezetet, amely legkésőbb 6 hónappal a gyakorlat előtt részt vesz a tagállami szintű kiberbiztonsági gyakorlatban.

(3) A kockázati készültség tekintetében illetékes hatóság a CSIRT-jei technikai támogatásával tagállami szinten önállóan vagy az adott tagállamban folytatott eltérő kiberbiztonsági gyakorlat keretében szervezi meg a (2) bekezdésben leírt kiberbiztonsági gyakorlatot. E gyakorlatok csoportosítása érdekében a kockázati készültség tekintetében illetékes hatóság egy évvel elhalaszthatja az (1) bekezdésben említett tagállami szintű kiberbiztonsági gyakorlatot.

(4) A szervezeti és tagállami szintű kiberbiztonsági gyakorlatok összhangban állnak az (EU) 2022/2555 irányelv 9. cikke (4) bekezdésének d) pontja szerinti nemzeti kiberbiztonsági válságelhárítási keretekkel.

(5) A villamosenergia-piaci ENTSO 2026. december 31-én és azt követően háromévente az EU DSO-val együttműködve rendelkezésre bocsátja a gyakorlatok forgatókönyvének mintáját az (1) bekezdésben említett szervezeti és tagállami szintű kiberbiztonsági gyakorlatok elvégzéséhez. Ez a minta figyelembe veszi a szervezet és a tagállamok szintjén legutóbb elvégzett kiberbiztonsági kockázatértékelést, és kulcsfontosságú sikerkritériumokat tartalmaz. A villamosenergia-piaci ENTSO és az EU DSO bevonja az ACER-t és az ENISA-t e minta kidolgozásába.

44. cikk

Regionális vagy régiók közötti kiberbiztonsági gyakorlatok

(1) A villamosenergia-piaci ENTSO 2029. december 31-én és azt követően háromévente az EU DSO-val együttműködve minden rendszerüzemeltetési régióban regionális kiberbiztonsági gyakorlatot szervez. A rendszerüzemeltetési régióban működő kritikus hatású szervezetek részt vesznek a regionális kiberbiztonsági gyakorlatban. A villamosenergia-piaci ENTSO az EU DSO-val együttműködve regionális kiberbiztonsági gyakorlat helyett több rendszerüzemeltető régióban is szervezhet régiók közötti kiberbiztonsági gyakorlatot ugyanabban az időkeretben. A gyakorlat során figyelembe kell venni az uniós szinten kidolgozott egyéb meglévő kiberbiztonsági kockázatértékeléseket és forgatókönyveket is.

(2) Az ENISA támogatja a villamosenergia-piaci ENTSO-t és az EU DSO-t a regionális vagy régiók közötti kiberbiztonsági gyakorlat előkészítésében és megszervezésében.

(3) A villamosenergia-piaci ENTSO az EU DSO-val egyeztetve hat hónappal a gyakorlat előtt tájékoztatja azokat a kritikus hatású szervezeteket, amelyek részt vesznek a regionális vagy régiók közötti kiberbiztonsági gyakorlatban.

(4) Az (EU) 2019/881 rendelet 7. cikkének (5) bekezdése szerinti rendszeres uniós szintű kiberbiztonsági gyakorlat vagy az ugyanazon földrajzi területen belüli, villamosenergia-ágazattal kapcsolatos bármely kötelező kiberbiztonsági gyakorlat szervezője felkérheti a villamosenergia-piaci ENTSO-t és az EU DSO-t a részvételre. Ilyen esetekben az (1) bekezdésben foglalt kötelezettség nem alkalmazandó, feltéve, hogy a rendszerüzemeltetési régió valamennyi kritikus hatású szervezete részt vesz ugyanabban a gyakorlatban.

(5) Ha a villamosenergia-piaci ENTSO és az EU DSO részt vesz a (4) bekezdésben említett kiberbiztonsági gyakorlatban, egy évvel elhalaszthatja az (1) bekezdésben említett regionális vagy régiók közötti kiberbiztonsági gyakorlatot.

(6) A villamosenergia-piaci ENTSO 2027. december 31-én és azt követően háromévente az EU DSO-val egyeztetve a regionális és régiók közötti kiberbiztonsági gyakorlatok elvégzéséhez rendelkezésre bocsátja e gyakorlatok mintáját. Ez a minta figyelembe veszi a regionális szinten legutóbb elvégzett kiberbiztonsági kockázatértékelést, és kulcsfontosságú sikerkritériumokat tartalmaz. A villamosenergia-piaci ENTSO konzultál a Bizottsággal, és tanácsot kérhet az ACER-től, az ENISA-tól és a Közös Kutatóközponttól a regionális és régiók közötti kiberbiztonsági gyakorlatok megszervezésével és végrehajtásával kapcsolatban.

45. cikk

A szervezeti, tagállami, regionális vagy régiók közötti kiberbiztonsági gyakorlatok eredménye

(1) A kritikus hatású szervezet kérésére a kritikus szolgáltatók részt vesznek a 43. cikk (1) és (2) bekezdésében és a 44. cikk (1) bekezdésében említett kiberbiztonsági gyakorlatokban, amennyiben a vonatkozó kiberbiztonsági gyakorlat hatókörének megfelelő területen nyújtanak a kritikus hatású szervezet részére szolgáltatásokat.

(2) A 43. cikk (1) és (2) bekezdésében és a 44. cikk (1) bekezdésében említett kiberbiztonsági gyakorlatok szervezői – kérésükre az ENISA által nyújtott tanácsadással és az (EU) 2019/881 rendelet 7. cikkének (5) bekezdésével összhangban – a tanulságokat összefoglaló, valamennyi résztvevőnek címzett jelentésben elemzik és véglegesítik a vonatkozó kiberbiztonsági gyakorlatot. A jelentés a következőket tartalmazza:

a) a gyakorlatok forgatókönyvei, az ülésekről szóló jelentések, főbb álláspontok, sikerek és a levont tanulságok a villamosenergia-értéklánc bármely szintjén;

b) teljesültek-e a fő sikerkritériumok;

c) a kiberbiztonsági gyakorlatban részt vevő szervezetek számára a kiberbiztonsági válságkezelési folyamatok, eljárások, kapcsolódó irányítási modellek és a kritikus szolgáltatókkal fennálló szerződéses kötelezettségek helyesbítésére, kiigazítására vagy megváltoztatására vonatkozó ajánlások jegyzéke.

(3) A CSIRT-hálózat, a Kiberbiztonsági Együttműködési Csoport vagy az EU CyCLONe kérésére a 43. cikk (1) és (2) bekezdésében és a 44. cikk (1) bekezdésében említett kiberbiztonsági gyakorlatok szervezői megosztják a vonatkozó kiberbiztonsági gyakorlat eredményeit. A szervezők megosztják a gyakorlatokban részt vevő minden egyes szervezettel az e cikk (2) bekezdésének a) és b) pontjában említett információkat. A szervezők az említett bekezdés c) pontjában említett ajánlások jegyzékét kizárólag azokkal a szervezettekkel osztják meg, amelyek az ajánlások címzettjei.

(4) A 43. cikk (1) és (2) bekezdésében és a 44. cikk (1) bekezdésében említett kiberbiztonsági gyakorlatok szervezői rendszeresen nyomon követik a gyakorlatokban részt vevő szervezetekkel együtt az e cikk (2) bekezdésének c) pontja szerinti ajánlások végrehajtását.

VII. FEJEZET

INFORMÁCIÓVÉDELEM

46. cikk

A megosztott információk védelmének elvei

(1) A 2. cikk (1) bekezdésében felsorolt szervezetek biztosítják, hogy az e rendelet alapján szolgáltatott, kapott, megosztott vagy továbbított információk csak a szükséges ismeret elve alapján és az információbiztonságra vonatkozó uniós és nemzeti szabályokkal összhangban legyenek hozzáférhetők.

(2) A 2. cikk (1) bekezdésében felsorolt szervezetek biztosítják, hogy az e rendelet alapján szolgáltatott, kapott, megosztott vagy továbbított információkat az említett információk teljes életciklusa alatt kezeljék és nyomon kövessék, és hogy ezeket az információkat életciklusuk végén csak anonimizálás után lehessen kiadni.

(3) A 2. cikk (1) bekezdésében felsorolt szervezetek biztosítják, hogy az e rendelet alapján szolgáltatott, kapott, megosztott vagy továbbított információk bizalmas jellegének, integritásának, rendelkezésre állásának és letagadhatatlanságának biztosításához és védelméhez szükséges szervezeti és technikai jellegű védelmi intézkedések – az alkalmazott eszközöktől függetlenül – rendelkezésre álljanak. A védelmi intézkedések:

a) arányosak;

b) figyelembe veszik az olyan ismert múltbeli és újonnan megjelenő fenyegetésekkel kapcsolatos kiberbiztonsági kockázatokat, amelyeknek az ilyen információk e rendelettel összefüggésben ki lehetnek téve;

c) a lehetőségekhez mérten nemzeti, európai vagy nemzetközi szabványokon és bevált gyakorlatokon alapulnak;

d) dokumentálva vannak.

(4) A 2. cikk (1) bekezdésében felsorolt szervezetek biztosítják, hogy az e rendelet alapján szolgáltatott, kapott, megosztott vagy továbbított információkhoz való hozzáféréssel rendelkező személyek tájékoztatást kapjanak a szervezet szintjén alkalmazandó biztonsági szabályokról, valamint az információk védelmével kapcsolatos intézkedésekről és eljárásokról. Ezek a szervezetek biztosítják, hogy az érintett személy a tájékoztatás során kapott utasításnak megfelelően tisztában legyen az információk védelméért őt terhelő felelősséggel.

(5) A 2. cikk (1) bekezdésében felsorolt szervezetek biztosítják, hogy az e rendelet alapján szolgáltatott, kapott, megosztott vagy továbbított információkhoz való hozzáférés azokra a személyekre korlátozódjon:

a) akik beosztásuk alapján és a rájuk bízott feladatok végrehajtására korlátozódóan jogosultak hozzáférni ezekhez az információkhoz;

b) akik esetében a szervezet értékelni tudta az etikai és feddhetetlenségi elveket, és akikre vonatkozóan nincs bizonyíték arra, hogy az egyén megbízhatóságának a szervezet bevált gyakorlataival és standard biztonsági követelményeivel, valamint szükség esetén a nemzeti jogszabályokkal és rendelkezésekkel összhangban történő értékelése céljából végzett háttérellenőrzés során negatív eredmény született volna.

(6) A 2. cikk (1) bekezdésében felsorolt szervezetek rendelkeznek az információt eredetileg létrehozó vagy szolgáltató természetes vagy jogi személy írásbeli hozzájárulásával, mielőtt az információt olyan harmadik fél rendelkezésére bocsátanák, amely nem tartozik e rendelet hatálya alá.

(7) A 2. cikk (1) bekezdésében felsorolt szervezetek fontolóra vehetik, hogy ezeket az információkat e cikk (1) és (4) bekezdésének való megfelelés nélkül osszák meg annak érdekében, hogy megelőzzék a kiberbiztonsági kiváltó okokból eredő, egyidejű villamosenergia-ellátási válságot vagy az Unión belüli, határokon átnyúló válságot egy másik ágazatban. Ebben az esetben a szervezet:

a) konzultál az illetékes hatósággal, és megszerzi az illetékes hatóságnak az ilyen információk megosztására irányuló engedélyét;

b) anonimizálja ezeket az információkat anélkül, hogy elvesznének a nyilvánosságnak a határkeresztező villamosenergia-áramlást fenyegető közvetlen és súlyos kockázatról és a lehetséges kockázatcsökkentő intézkedésekről való tájékoztatásához szükséges elemek;

c) óvja a kezdeményező és az ilyen információkat e rendelet alapján kezelő szervezetek kilétét.

(8) E cikk (6) bekezdésétől eltérve, az illetékes hatóságok a 2. cikk (1) bekezdésben nem felsorolt harmadik fél részére szolgáltathatnak az e rendelet alapján szolgáltatott, kapott, megosztott vagy továbbított információkat az információ kezdeményezőjének előzetes írásbeli hozzájárulása nélkül, de erről a lehető leghamarabb tájékoztatják a kezdeményezőt. Az e rendelet alapján szolgáltatott, kapott, megosztott vagy továbbított információnak a 2. cikk (1) bekezdésében nem felsorolt harmadik fél részére történő felfedése előtt az érintett illetékes hatóság észszerűen biztosítja, hogy az érintett harmadik fél tisztában legyen a hatályos biztonsági szabályokkal, és észszerű biztosítékot szerez arra vonatkozóan, hogy az érintett harmadik fél e cikk (1)–(5) bekezdésével összhangban képes megvédeni a kapott információkat. Az illetékes hatóság anonimizálja ezeket az információkat anélkül, hogy elvesznének a nyilvánosságnak a határkeresztező villamosenergia-áramlásokat fenyegető súlyos kockázatról és a lehetséges kockázatcsökkentő intézkedésekről való tájékoztatásához szükséges elemek, és óvja az információ kezdeményezőjének kilétét. Ebben az esetben a 2. cikk (1) bekezdésében nem felsorolt harmadik fél a kapott információkat a szervezet szintjén már hatályban lévő rendelkezéseknek megfelelően, vagy ha ez nem lehetséges, az érintett illetékes hatóság rendelkezéseinek és utasításainak megfelelően védi.

(9) Ez a cikk nem alkalmazandó azokra a 2. cikk (1) bekezdésében nem felsorolt szervezetekre, amelyek e cikk (6) bekezdése alapján kapják a szóban forgó információkat. Ebben az esetben e cikk (7) bekezdését kell alkalmazni, vagy az illetékes hatóság írásbeli rendelkezéseket írhat elő e szervezet számára, amelyeket azokban az esetekben kell alkalmazni, ha az információkat e rendelet alapján kapták.

47. cikk

Az információk bizalmas kezelése

(1) Az e rendelet alapján nyújtott, kapott, megosztott vagy továbbított információkra az e rendelet e cikkének (2)–(5) bekezdésében meghatározott szakmai titoktartási feltételek és az (EU) 2019/943 rendelet 65. cikkében meghatározott követelmények vonatkoznak. Az e rendelet 2. cikkében felsorolt szervezetek között e rendelet végrehajtása céljából szolgáltatott, kapott, megosztott vagy továbbított információkat védeni kell, figyelembe véve az információk bizalmasságának a kezdeményező által alkalmazott mértékét.

(2) A 2. cikkben felsorolt szervezeteket szakmai titoktartási kötelezettség terheli.

(3) A kiberbiztonságért felelős illetékes hatóságok, a nemzeti szabályozó hatóságok, a kockázati készültség tekintetében illetékes hatóságok és a CSIRT-ek megosztják a feladataik ellátásához szükséges valamennyi információt.

(4) A 2. cikk (1) bekezdésében felsorolt szervezetek között a 23. cikk végrehajtása céljából szolgáltatott, megosztott vagy továbbított információkat anonimizálni és összesíteni kell.

(5) Az e rendelet hatálya alá tartozó szervezetek vagy hatóságok által a feladataik ellátása során kapott bizalmas információkat nem adhatják ki semmilyen más szervezetnek vagy hatóságnak, kivéve a nemzeti törvények, az e rendelet egyéb rendelkezései, vagy az egyéb vonatkozó uniós jogszabályok hatálya alá tartozó esetekben.

(6) A nemzeti vagy uniós jogszabályok sérelme nélkül az a hatóság, szervezet vagy természetes személy, aki e rendelet alapján kap információt, azt kizárólag az e rendelet szerinti feladatai ellátására használhatja fel.

(7) Az ACER az ENISA-val, az összes illetékes hatósággal, a villamosenergia-piaci ENTSO-val és az EU-DSO-val folytatott konzultációt követően 2025. június 13-én iránymutatásokat ad ki az e cikk végrehajtása céljából a 2. cikk (1) bekezdésében felsorolt valamennyi szervezet közötti információcsere mechanizmusairól, különösen a tervezett kommunikációs folyamatokról, valamint az információk anonimizálásának és összesítésének módszereiről.

(8) Az uniós és nemzeti szabályok értelmében bizalmasnak minősülő információk csak akkor osztandók meg a Bizottsággal és más releváns hatóságokkal, amennyiben e rendelet alkalmazásához szükséges az ilyen információcsere. Az információcsere a célja szempontjából szükséges és arányos mértékre korlátozódik. Az információcsere megőrzi ezen információk bizalmas jellegét, és védi a kritikus hatású vagy nagy hatású szervezetek biztonsági és kereskedelmi érdekeit.

VIII. FEJEZET

ZÁRÓ RENDELKEZÉSEK

48. cikk

Átmeneti rendelkezések

(1) A 6. cikk (2) bekezdésében említett feltételek vagy módszertanok vagy a 6. cikk (3) bekezdésében említett tervek jóváhagyásáig a villamosenergia-piaci ENTSO az EU DSO-val együttműködve nem kötelező erejű iránymutatást dolgoz ki a következő kérdésekre vonatkozóan:

a) az e cikk (2) bekezdése szerinti, a villamos energia ideiglenes kiberbiztonsági hatásmutatója (a továbbiakban: ECII);

b) az egész Unióra kiterjedő, nagy hatású és kritikus hatású folyamatok e cikk (4) bekezdése szerinti ideiglenes jegyzéke; valamint

c) az e cikk (6) bekezdése szerinti, a határkeresztező villamosenergia-áramlás kiberbiztonsági szempontjai számára releváns európai és nemzetközi szabványok és a nemzeti jogszabályok által előírt ellenőrzések ideiglenes jegyzéke.

(2) A villamosenergia-piaci ENTSO 2024. október 13-án az EU DSO-val együttműködve ajánlást dolgoz ki az ideiglenes ECII-re vonatkozóan. A villamosenergia-piaci ENTSO az EU DSO-val együttműködve értesíti az illetékes hatóságokat az ajánlott ideiglenes ECII-ről.

(3) Az illetékes hatóságok az ajánlott ideiglenes ECII kézhezvételétől számított négy hónapon belül, vagy legkésőbb 2025. február 13-án az ajánlott ECII alapján azonosítják a tagállamukban a nagy hatású és kritikus hatású szervezetek jelöltjeit, és elkészítik a nagy hatású és kritikus hatású szervezetek ideiglenes jegyzékét. Az ideiglenes jegyzékben azonosított nagy hatású és kritikus hatású szervezetek az elővigyázatosság elve alapján önkéntesen teljesíthetik az e rendeletben meghatározott kötelezettségeiket. Az illetékes hatóságok 2025. március 13-án értesítik az ideiglenes jegyzékben azonosított szervezeteket arról, hogy nagy hatású vagy kritikus hatású szervezetként azonosították őket.

(4) A villamosenergia-piaci ENTSO 2024. december 13-án az EU DSO-val együttműködve kidolgozza az egész Unióra kiterjedő, nagy hatású és kritikus hatású folyamatok ideiglenes jegyzékét. A (3) bekezdés szerint értesített azon szervezetek, amelyek önkéntesen úgy döntenek, hogy az elővigyázatosság elve alapján teljesítik az e rendeletben meghatározott kötelezettségeiket, a nagy hatású és kritikus hatású folyamatok ideiglenes jegyzékét használják a nagy hatású és kritikus hatású folyamatok ideiglenes hatókörének meghatározásához, valamint annak meghatározásához, hogy mely eszközök szerepeljenek a szervezet szintjén végzett első kiberbiztonsági kockázatértékelésben.

(5) A 4. cikk (1) bekezdése szerinti valamennyi illetékes hatóság 2024. szeptember 13-án benyújtja a villamosenergia-piaci ENTSO-nak és az EU DSO-nak a határkeresztező villamosenergia-áramlás kiberbiztonsági szempontjai számára releváns nemzeti jogszabályainak jegyzékét.

(6) A villamosenergia-piaci ENTSO az EU DSO-val együttműködve 2025. június 13-án elkészíti a határkeresztező villamosenergia-áramlás kiberbiztonsági szempontjai számára releváns, a nemzeti jogszabályokban előírt európai és nemzetközi szabványok és ellenőrzések ideiglenes jegyzékét, figyelembe véve az illetékes hatóságok által szolgáltatott információkat.

(7) Az európai és nemzetközi szabványok és ellenőrzések ideiglenes jegyzéke a következőket tartalmazza:

a) olyan európai és nemzetközi szabványok és nemzeti jogszabályok, amelyek iránymutatást nyújtanak a szervezeti szintű kiberbiztonsági kockázatkezelés módszertanára vonatkozóan; valamint

b) a várhatóan a minimális és fejlett kiberbiztonsági ellenőrzések részét képező ellenőrzésekkel egyenértékű kiberbiztonsági ellenőrzések.

(8) A villamosenergia-piaci ENTSO és az EU DSO figyelembe veszi az ENISA és az ACER véleményét a szabványok ideiglenes jegyzékének véglegesítésekor. A villamosenergia-piaci ENTSO és az EU DSO honlapján közzéteszi az európai és nemzetközi szabványok és ellenőrzések ideiglenes jegyzékét.

(9) A villamosenergia-piaci ENTSO és az EU DSO konzultál az ENISA-val és az ACER-rel az (1) bekezdés alapján kidolgozott, nem kötelező erejű iránymutatásra irányuló javaslatokról.

(10) A minimális és fejlett kiberbiztonsági ellenőrzéseknek a 29. cikk szerinti kidolgozásáig és a 8. cikk szerinti elfogadásáig a 2. cikk (1) bekezdésében felsorolt valamennyi szervezet törekszik az (1) bekezdés alapján kidolgozott, nem kötelező erejű iránymutatás fokozatos alkalmazására.

49. 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 Brüsszelben, 2024. március 11-én.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN