Publicatieblad
van de Europese Unie

NL
L-serie

2024/1366

24.5.2024

GEDELEGEERDE VERORDENING (EU) 2024/1366 VAN DE COMMISSIE

van 11 maart 2024

tot aanvulling van Verordening (EU) 2019/943 van het Europees Parlement en de Raad door middel van de vaststelling van een netcode inzake sectorspecifieke regels voor met cyberbeveiliging samenhangende aspecten van grensoverschrijdende elektriciteitsstromen

(Voor de EER relevante tekst)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2019/943 van het Europees Parlement en de Raad van 5 juni 2019 betreffende de interne markt voor elektriciteit ([1]), en met name artikel 59, lid 2, punt e),

Overwegende hetgeen volgt:

(1) Het beheer van cyberbeveiligingsrisico's is van cruciaal belang voor het behoud van de voorzieningszekerheid van elektriciteit en voor het waarborgen van een hoog niveau van cyberbeveiliging in de elektriciteitssector.

(2) Digitalisering en cyberbeveiliging zijn van doorslaggevend belang voor de verlening van essentiële diensten en als zodanig van strategisch belang voor kritieke energie-infrastructuur.

(3) Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad ([2]) omvat maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie. Verordening (EU) 2019/941 van het Europees Parlement en de Raad ([3]) vormt een aanvulling op Richtlijn (EU) 2022/2555 door te waarborgen dat cyberbeveiligingsincidenten in de elektriciteitssector naar behoren als een risico worden aangemerkt en dat de maatregelen daartegen naar behoren in de risicoparaatheidsplannen worden opgenomen. Verordening (EU) 2019/943 vormt een aanvulling op Richtlijn (EU) 2022/2555 en Verordening (EU) 2019/941 door specifieke regels voor de elektriciteitssector op het niveau van de Unie vast te stellen. Bovendien vormt deze gedelegeerde verordening een aanvulling op Richtlijn (EU) 2022/2555 met betrekking tot de elektriciteitssector, waar het grensoverschrijdende elektriciteitsstromen betreft.

(4) In een context van verbonden gedigitaliseerde elektriciteitssystemen kunnen de preventie en het beheer van elektriciteitscrises in verband met cyberaanvallen niet als een uitsluitend nationale taak worden beschouwd. Het potentieel van efficiëntere en goedkopere maatregelen moet middels samenwerking op regionaal en op Unieniveau ten volle worden benut. Daarom zijn een gemeenschappelijk regelgevingskader en beter gecoördineerde procedures nodig om te waarborgen dat de lidstaten en andere partijen doeltreffend grensoverschrijdend kunnen samenwerken, in een geest van meer transparantie, vertrouwen en solidariteit tussen de lidstaten en de instanties die bevoegd zijn voor elektriciteit en cyberbeveiliging.

(5) Het beheer van cyberbeveiligingsrisico's binnen het toepassingsgebied van deze verordening vereist een gestructureerd proces dat onder meer de aanmerking van risico's voor grensoverschrijdende elektriciteitsstromen als gevolg van cyberaanvallen, de daarmee verband houdende operationele processen en perimeters, en de bijbehorende cyberbeveiligingscontroles en verificatiemechanismen omvat. Het tijdsbestek voor het hele proces omspant verscheidene jaren, en met elke stap moet worden toegewerkt naar een hoog gemeenschappelijk niveau van cyberbeveiliging in de sector en een beperking van cyberbeveiligingsrisico's. Alle deelnemers aan het proces moeten zich inspannen om de methoden zo spoedig mogelijk, en in ieder geval binnen de in deze verordening vastgestelde termijnen te ontwikkelen en daarover overeenstemming te bereiken.

([1]) PB L 158 van 14.6.2019, blz. 54.

([2]) Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972, en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-Richtlijn) (PB L 333 van 27.12.2022, blz. 80).

([3]) Verordening (EU) 2019/941 van het Europees Parlement en de Raad van 5 juni 2019 betreffende risicoparaatheid in de elektriciteitssector en tot intrekking van Richtlijn 2005/89/EG (PB L 158 van 14.6.2019, blz. 1).

(6) De cyberbeveiligingsrisicobeoordelingen op het niveau van de Unie, de lidstaten, de regio's en de entiteiten krachtens deze verordening kunnen worden beperkt tot beoordelingen naar aanleiding van cyberaanvallen in de zin van Verordening (EU) 2022/2554 van het Europees Parlement en de Raad ([4]), met uitsluiting van bijvoorbeeld fysieke aanvallen, natuurrampen en onderbrekingen vanwege het verlies van faciliteiten of personele middelen. Uniebrede en regionale risico's met betrekking tot fysieke aanvallen of natuurrampen op het gebied van elektriciteit vallen reeds onder andere bestaande Uniewetgeving, zoals artikel 5 van Verordening (EU) 2019/941 of Verordening (EU) 2017/1485 van de Commissie ([5]) tot vaststelling van richtsnoeren betreffende het beheer van elektriciteitstransmissiesystemen. In dezelfde zin heeft Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad ([6]) betreffende de weerbaarheid van kritieke entiteiten tot doel de kwetsbaarheden van kritieke entiteiten te verminderen en de fysieke weerbaarheid van kritieke entiteiten te versterken, en zij omvat alle relevante natuurlijke en door de mens veroorzaakte risico's die van invloed kunnen zijn op de verlening van essentiële diensten, waaronder ongevallen, natuurrampen, noodsituaties op het gebied van de volksgezondheid zoals pandemieën, en hybride dreigingen of andere antagonistische dreigingen, waaronder terroristische misdrijven, criminele infiltratie en sabotage.

(7) Het begrip "entiteiten met zeer belangrijke impact en entiteiten met kritieke impact" in deze verordening is van fundamenteel belang voor de bepaling van het toepassingsgebied van entiteiten die onderworpen zijn aan de verplichtingen uit hoofde van deze verordening. De in verschillende bepalingen beschreven risicogebaseerde aanpak is bedoeld voor het in kaart brengen van voor grensoverschrijdende elektriciteitsstromen relevante processen, ondersteunende activa en entiteiten die deze beheren. Afhankelijk van de mate waarin mogelijke cyberaanvallen van invloed zijn op hun activiteiten inzake grensoverschrijdende elektriciteitsstromen, kunnen die entiteiten worden beschouwd als "entiteiten met zeer belangrijke impact" of "entiteiten met kritieke impact". Artikel 3 van Richtlijn (EU) 2022/2555 bepaalt de begrippen "essentiële en belangrijke entiteiten" en de criteria om entiteiten van die categorieën aan te duiden. Hoewel vele ervan tegelijkertijd zullen worden beschouwd en aangeduid als "essentieel" in de zin van artikel 3 van Richtlijn (EU) 2022/2555 en als entiteit met zeer belangrijke impact of met kritieke impact overeenkomstig artikel 24 van deze verordening, hebben de in deze verordening vastgestelde criteria alleen betrekking op hun rol en impact in de elektriciteitsprocessen die van invloed zijn op grensoverschrijdende stromen, los van de criteria van artikel 3 van Richtlijn (EU) 2022/2555.

(8) De entiteiten die binnen het toepassingsgebied van deze verordening vallen en die als entiteiten met zeer belangrijke impact of met kritieke impact overeenkomstig artikel 24 van deze verordening worden beschouwd en onder de verplichtingen daarvan vallen, zijn in de eerste plaats entiteiten met rechtstreekse gevolgen voor grensoverschrijdende elektriciteitsstromen in de EU.

(9) Deze verordening maakt gebruik van bestaande mechanismen en instrumenten die reeds in andere wetgeving zijn vastgesteld, om de efficiëntie te waarborgen en overlappingen bij de verwezenlijking van de doelstellingen te voorkomen.

(10) Bij de toepassing van deze verordening moeten de lidstaten, de relevante instanties en de systeembeheerders rekening houden met de overeengekomen Europese normen en technische specificaties van de Europese normalisatieorganisaties en handelen conform de Uniewetgeving betreffende het in de handel brengen of in gebruik nemen van onder die Uniewetgeving vallende producten.

([4]) Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (PB L 333 van 27.12.2022, blz. 1).

([5]) Verordening (EU) 2017/1485 van de Commissie van 2 augustus 2017 tot vaststelling van richtsnoeren betreffende het beheer van elektriciteitstransmissiesystemen (PB L 220 van 25.8.2017, blz. 1).

([6]) Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad (PB L 333 van 27.12.2022, blz. 164).

(11) Met het oog op de beperking van cyberbeveiligingsrisico's is het noodzakelijk gedetailleerde regels vast te stellen voor de acties van en de samenwerking tussen belanghebbenden wier activiteiten betrekking hebben op met cyberbeveiliging samenhangende aspecten van grensoverschrijdende elektriciteitsstromen, teneinde de systeemveiligheid te waarborgen. Die organisatorische en technische regels moeten waarborgen dat de meeste elektriciteitsincidenten met een onderliggende oorzaak in cyberbeveiliging doeltreffend op operationeel niveau worden aangepakt. Er moet worden bepaald wat die belanghebbenden moeten doen om dergelijke crises te voorkomen en welke maatregelen zij kunnen treffen indien de systeembeheerregels alleen niet afdoende zijn. Daarom moet een gemeenschappelijk regelkader worden vastgesteld voor het voorkomen, voorbereiden en beheren van gelijktijdige elektriciteitscrises met een onderliggende oorzaak in cyberbeveiliging. Dat leidt tot meer transparantie in de voorbereidingsfase en gedurende een gelijktijdige elektriciteitscrisis en zorgt ervoor dat maatregelen in samenwerking met de voor cyberbeveiliging bevoegde instanties in de lidstaten gecoördineerd en doeltreffend worden getroffen. De lidstaten en de betrokken entiteiten moeten worden verplicht op regionaal niveau en, in voorkomend geval, bilateraal samen te werken in een geest van solidariteit. Deze samenwerking en die regels zijn bedoeld om de risicoparaatheid op het gebied van cyberbeveiliging tegen lagere kosten te verbeteren, mede conform de doelstellingen van Richtlijn (EU) 2022/2555. Het lijkt ook nodig de interne elektriciteitsmarkt te versterken door het vertrouwen tussen de lidstaten te vergroten, met name door het risico van onnodige inperking van grensoverschrijdende elektriciteitsstromen te mitigeren, zodat het risico van negatieve overloopeffecten op aangrenzende lidstaten wordt beperkt.

(12) De voorzieningszekerheid van elektriciteit veronderstelt een doeltreffende samenwerking tussen de lidstaten, de instellingen, organen, bureaus en agentschappen van de Unie, en de belanghebbenden. Distributiesysteembeheerders en transmissiesysteembeheerders spelen een sleutelrol bij het waarborgen van een veilig, betrouwbaar en efficiënt elektriciteitssysteem overeenkomstig de artikelen 31 en 40 van Richtlijn (EU) 2019/944 van het Europees Parlement en de Raad ([7]). De verschillende regulerende instanties en andere relevante nationale bevoegde instanties spelen ook een belangrijke rol bij het waarborgen en monitoren van de cyberbeveiliging in de elektriciteitsvoorziening, als onderdeel van hun taken uit hoofde van de Richtlijnen (EU) 2019/944 en (EU) 2022/2555. De lidstaten moeten een bestaande of nieuwe entiteit aanwijzen als hun nationale bevoegde instantie voor de uitvoering van deze verordening, met als doel de transparante en inclusieve deelname van alle betrokken partijen, de efficiënte voorbereiding en correcte uitvoering ervan, en de samenwerking tussen de verschillende belanghebbenden en de bevoegde instanties op het gebied van elektriciteit en cyberbeveiliging te waarborgen, alsook de preventie en evaluatie achteraf van elektriciteitscrises met een onderliggende oorzaak in cyberbeveiliging en de uitwisseling van informatie daarover te vergemakkelijken.

(13) Indien een entiteit met zeer belangrijke impact of met kritieke impact diensten verleent in meer dan één lidstaat, of haar zetel of andere vestiging of een vertegenwoordiger in een lidstaat heeft, maar haar netwerk- en informatiesystemen in een of meer andere lidstaten heeft, moeten die lidstaten hun respectieve bevoegde autoriteiten stimuleren zich in te spannen om samen te werken en elkaar waar nodig bij te staan.

(14) De lidstaten moeten waarborgen dat de bevoegde instanties over de nodige bevoegdheden beschikken met betrekking tot entiteiten met zeer belangrijke impact of met kritieke impact om de naleving van deze verordening te bevorderen. Deze bevoegdheden moeten de bevoegde instanties in staat stellen inspecties ter plaatse en toezicht op locatie uit te voeren. Dit kan steekproefsgewijze controles omvatten, alsook regelmatige audits, gerichte beveiligingsaudits op basis van risicobeoordelingen of beschikbare risicogerelateerde informatie en beveiligingsscans op basis van objectieve, niet-discriminatoire, billijke en transparante risicobeoordelingscriteria, zoals verzoeken om informatie ter beoordeling van de door de entiteit getroffen cyberbeveiligingsmaatregelen. Die informatie moet gedocumenteerde cyberbeveiligingsbeleidsmaatregelen, toegangsgegevens, stukken of inlichtingen omvatten die nodig zijn voor het verrichten van de toezichthoudende werkzaamheden, alsmede een bewijs van de uitvoering van het cyberbeveiligingsbeleid, zoals de resultaten van door een gekwalificeerde auditor uitgevoerde beveiligingsaudits en de bijbehorende bewijsstukken.

([7]) Richtlijn (EU) 2019/944 van het Europees Parlement en de Raad van 5 juni 2019 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en tot wijziging van Richtlijn 2012/27/EU (herschikking) (PB L 158 van 14.6.2019, blz. 125).

(15) Ter voorkoming van hiaten of overlappingen van verplichtingen inzake risicobeheer op het gebied van cyberbeveiliging die aan entiteiten met zeer belangrijke impact of met kritieke impact worden opgelegd, moeten de nationale autoriteiten overeenkomstig Richtlijn (EU) 2022/2555 en de bevoegde instanties overeenkomstig deze verordening samenwerken bij de uitvoering van de maatregelen voor het beheer van cyberbeveiligingsrisico's en het toezicht op de naleving van die maatregelen op nationaal niveau. De naleving door een entiteit van de in deze verordening vastgestelde vereisten inzake risicobeheer op het gebied van cyberbeveiliging kan door overeenkomstig Richtlijn (EU) 2022/2555 bevoegde autoriteiten worden beschouwd als het waarborgen van de naleving van de overeenkomstige vereisten van die richtlijn, en vice versa.

(16) Voor een gemeenschappelijke aanpak van gelijktijdige preventie en beheersing van elektriciteitscrises moeten de lidstaten een gemeenschappelijke opvatting vormen over de definitie van een gelijktijdige elektriciteitscrisis en het moment waarop een cyberaanval daarin een belangrijke factor vertegenwoordigt. Met name moet de coördinatie tussen de lidstaten en de betrokken entiteiten worden vereenvoudigd met het oog op het tegengaan van een situatie waarin vanwege een cyberaanval een potentieel risico van een significant tekort aan elektriciteit of een onmogelijkheid van het leveren aan afnemers ervan bestaand of ophanden is.

(17) In overweging 1 van Verordening (EU) 2019/881 van het Europees Parlement en de Raad ([8]) wordt de cruciale rol onderkend die netwerk- en informatiesystemen alsmede elektronischecommunicatienetwerken en -diensten spelen om de economieën draaiende te houden in essentiële sectoren zoals energie, en in overweging 44 wordt toegelicht dat het Agentschap van de Europese Unie voor cyberbeveiliging ("Enisa") moet overleggen met het Agentschap voor de samenwerking tussen energieregulators ("ACER").

(18) Bij Verordening (EU) 2019/943 worden specifieke verantwoordelijkheden met betrekking tot cyberbeveiliging toegekend aan transmissiesysteembeheerders ("TSB's") en distributiesysteembeheerders ("DSB's"). Hun Europese verenigingen, namelijk het Europees netwerk van TSB's voor elektriciteit ("ENTSB voor elektriciteit") en de Europese entiteit voor DSB's ("EU DSB-entiteit"), stimuleren overeenkomstig respectievelijk de artikelen 30 en 55 van die verordening cyberbeveiliging in samenwerking met relevante autoriteiten en gereglementeerde entiteiten.

(19) Een gemeenschappelijke aanpak voor de preventie en het beheer van gelijktijdige elektriciteitscrises met een onderliggende oorzaak in cyberbeveiliging vereist ook dat alle belanghebbenden geharmoniseerde methoden en definities gebruiken om risico's in verband met de cyberbeveiliging van de elektriciteitsvoorziening aan te duiden. Ook moet doeltreffend kunnen worden vergeleken hoe goed zij en hun buren op dat gebied presteren. Daarom moeten de processen en de rollen en verantwoordelijkheden worden vastgesteld voor de ontwikkeling en actualisering van risicobeheersmethoden, classificatieschalen voor incidenten en cyberbeveiligingsmaatregelen die zijn aangepast aan de cyberbeveiligingsrisico's met gevolgen voor de grensoverschrijdende elektriciteitsstromen.

(20) De lidstaten zijn via de voor deze verordening aangewezen bevoegde instantie verantwoordelijk voor het aanduiden van de entiteiten die voldoen aan de criteria om als entiteiten met zeer belangrijke impact of met kritieke impact te worden aangemerkt. Om verschillen tussen de lidstaten in dat opzicht weg te werken en rechtszekerheid te bieden met betrekking tot de maatregelen voor het beheer van cyberbeveiligingsrisico's en de rapportageverplichtingen voor alle relevante entiteiten, moeten er criteria worden vastgesteld om te bepalen welke entiteiten binnen het toepassingsgebied van deze verordening vallen. Die criteria moeten worden vastgesteld en regelmatig worden bijgewerkt door middel van het ontwikkelings- en vaststellingsproces van de in deze verordening bepaalde voorwaarden en methoden.

(21) Deze verordening laat het Unierecht inzake specifieke regels voor de certificering van ICT-producten, -diensten en -processen, met name Verordening (EU) 2019/881 met betrekking tot het kader voor de opstelling van Europese regelingen voor cyberbeveiligingscertificering onverlet. In het kader van de onderhavige verordening moeten ICT-producten ook technische apparaten en software omvatten waarmee rechtstreekse interactie met het elektrotechnisch netwerk mogelijk is, met name industriële regelsystemen die voor energietransmissie, energiedistributie en energieproductie, en voor het verzamelen en doorgeven van gerelateerde informatie kunnen worden gebruikt. De bepalingen moeten waarborgen dat de aan te schaffen ICT-producten, -diensten en -processen aan de relevante beveiligingsdoelstellingen van artikel 51 van Verordening (EU) 2019/881 voldoen.

([8]) Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (PB L 151 van 7.6.2019, blz. 15).

(22) Uit recente cyberaanvallen blijkt dat entiteiten steeds vaker het doelwit van aanvallen op de toeleveringsketen worden. Dergelijke aanvallen op de toeleveringsketen hebben niet alleen gevolgen voor individuele entiteiten binnen het toepassingsgebied, maar kunnen ook als een waterval doorwerken in grotere aanvallen op entiteiten waarop zij in het elektriciteitsnet zijn aangesloten. Daarom zijn bepalingen en aanbevelingen toegevoegd om de cyberbeveiligingsrisico's ten aanzien van processen betreffende de toeleveringsketen, met name aanbestedingen, met gevolgen voor de grensoverschrijdende elektriciteitsstromen, te mitigeren.

(23) Aangezien de uitbuiting van kwetsbaarheden in netwerk- en informatiesystemen aanzienlijke verstoringen van de energievoorziening en schade voor de economie en consumenten kan veroorzaken, moeten die kwetsbaarheden snel in kaart worden gebracht en verholpen om de risico's te beperken. Om de doeltreffende uitvoering van deze verordening te vergemakkelijken, moeten de relevante entiteiten en bevoegde instanties samenwerken om te oefenen en activiteiten te testen die daartoe geschikt worden geacht, met inbegrip van informatie-uitwisseling over cyberdreigingen, cyberaanvallen, kwetsbaarheden, instrumenten en methoden, tactieken, technieken en procedures, crisisbeheersingsparaatheid op het gebied van cyberbeveiliging en andere oefeningen. Aangezien de technologie voortdurend evolueert en de digitalisering van de elektriciteitssector snel vordert, mag de uitvoering van de vastgestelde bepalingen niet in de weg staan van innovatie noch belemmering vormen voor de toegang tot de elektriciteitsmarkt en het daarmee samenhangende gebruik van innovatieve oplossingen die tot de efficiëntie en de duurzaamheid van het elektriciteitssysteem bijdragen.

(24) De met het oog op het toezicht op de uitvoering van deze verordening verzamelde informatie moet redelijkerwijs worden beperkt op "need-to-know"-basis. Belanghebbenden moeten een haalbare en passende termijn krijgen om dergelijke informatie in te dienen. Dubbele kennisgeving moet worden vermeden.

(25) De bescherming van cyberbeveiliging stopt niet aan de grenzen van de Unie. Voor een veilig systeem is de betrokkenheid van aangrenzende derde landen vereist. De Unie en haar lidstaten moeten ernaar streven aangrenzende derde landen waarvan de elektriciteitsinfrastructuur op het Europese net is aangesloten, te ondersteunen bij de toepassing van cyberbeveiligingsregels die gelijksoortig zijn aan deze verordening.

(26) Om de veiligheidscoördinatie in een vroeg stadium te verbeteren en toekomstige bindende voorwaarden en methoden te testen, moeten het ENTSB voor elektriciteit, de EU DSB-entiteit en de bevoegde instanties onmiddellijk na de inwerkingtreding van deze verordening beginnen met de ontwikkeling van niet-bindende richtsnoeren. Die richtsnoeren zullen dienen als basis voor de ontwikkeling van de toekomstige voorwaarden en methoden. Tegelijkertijd moeten de bevoegde instanties entiteiten aanwijzen als kandidaten voor entiteiten met zeer belangrijke impact of met kritieke impact om een begin te maken met het vrijwillig nakomen van die verplichtingen.

(27) Deze verordening is opgesteld in nauwe samenwerking met ACER, Enisa, het ENTSO voor elektriciteit, de EU DSB-entiteit en andere belanghebbenden teneinde op transparante en participatieve wijze doeltreffende, evenwichtige en evenredige regels vast te stellen.

(28) Deze verordening vormt een aanvulling op en een versterking van de crisisbeheersingsmaatregelen conform het EU-kader voor respons op cybercrises, zoals benoemd in Aanbeveling (EU) 2017/1584 van de Commissie ([9]). Een cyberaanval kan ook leiden tot, bijdragen tot of samenvallen met een elektriciteitscrisis in de zin van artikel 2, punt 9, van Verordening (EU) 2019/941 met gevolgen voor grensoverschrijdende elektriciteitsstromen. Een zodanige elektriciteitscrisis kan leiden tot een gelijktijdige elektriciteitscrisis in de zin van artikel 2, punt 10, van Verordening (EU) 2019/941. Een dergelijk incident kan ook gevolgen hebben voor andere sectoren die van de voorzieningszekerheid van elektriciteit afhankelijk zijn. Indien een dergelijk incident escaleert tot een grootschalig cyberbeveiligingsincident in de zin van artikel 16 van Richtlijn (EU) 2022/2555, moeten de onderdelen van dat artikel, waarbij het Europees netwerk van verbindingsorganisaties voor cybercrises ("EU-CyCLONe") wordt opgericht, worden toegepast. Voor crisisbeheer op Unieniveau moeten de relevante partijen zich baseren op de geïntegreerde Unieregeling politieke crisisrespons ("IPCR-regeling") overeenkomstig Uitvoeringsbesluit (EU) 2018/1993 van de Raad ([10]).

(29) Deze verordening laat het de bevoegdheid van de lidstaten onverlet om de nodige maatregelen te nemen ter bescherming van de wezenlijke belangen van hun beveiliging, ter vrijwaring van de openbare orde en veiligheid en om het onderzoek, de opsporing en de vervolging van strafbare feiten mogelijk te maken, met inachtneming van het recht van de Unie. Overeenkomstig artikel 346 VWEU mag geen enkele lidstaat verplicht worden inlichtingen te verstrekken waarvan de openbaarmaking naar zijn mening strijdig is met wezenlijke veiligheidsbelangen.

([9]) Aanbeveling (EU) 2017/1584 van de Commissie van 13 september 2017 inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises (PB L 239 van 19.9.2017, blz. 36).

([10]) Uitvoeringsbesluit (EU) 2018/1993 van de Raad van 11 december 2018 inzake de geïntegreerde EU-regeling politieke crisisrespons (PB L 320 van 17.12.2018, blz. 28).

(30) Hoewel deze verordening in beginsel van toepassing is op entiteiten die activiteiten verrichten op het gebied van de elektriciteitsproductie van kerncentrales, kunnen sommige van deze activiteiten verband houden met de nationale veiligheid.

(31) Het Uniegegevensbeschermingsrecht en het Unieprivacyrecht moet van toepassing zijn op de verwerking van persoonsgegevens uit hoofde van deze verordening. Meer bepaald laat deze verordening Verordening (EU) 2016/679 van het Europees Parlement en de Raad ([11]), Richtlijn 2002/58/EG van het Europees Parlement en de Raad ([12]) en Verordening (EU) 2018/1725 van het Europees Parlement en de Raad ([13]) onverlet. Deze verordening moet derhalve onder meer de werkzaamheden en bevoegdheden onverlet laten van de autoriteiten die bevoegd zijn om toezicht te houden op de naleving van het toepasselijke Uniegegevensbeschermingsrecht en het Unieprivacyrecht.

(32) Gezien het belang van internationale samenwerking op het gebied van cyberbeveiliging moeten de bevoegde instanties die verantwoordelijk zijn voor het verrichten van de hun krachtens deze verordening toegewezen en door de lidstaten aangeduide werkzaamheden, aan internationale samenwerkingsnetwerken kunnen deelnemen. Daarom moeten de bevoegde instanties voor het verrichten van hun werkzaamheden inlichtingen, met inbegrip van persoonsgegevens, kunnen uitwisselen met de bevoegde instanties van derde landen, mits is voldaan aan de voorwaarden van het Uniegegevensbeschermingsrecht inzake de doorgifte van persoonsgegevens aan derde landen, onder meer die van artikel 49 van Verordening (EU) 2016/679.

(33) De verwerking van persoonsgegevens, voor zover noodzakelijk en evenredig met het oog op de beveiliging van activa door entiteiten met zeer belangrijke impact of met kritieke impact, kan als rechtmatig worden beschouwd op grond van het feit dat een dergelijke verwerking volgt uit een wettelijke verplichting waaraan de verwerkingsverantwoordelijke onderworpen is overeenkomstig artikel 6, lid 1, punt c), en artikel 6, lid 3, van Verordening (EU) 2016/679. De verwerking van persoonsgegevens kan ook noodzakelijk zijn voor de behartiging van de gerechtvaardigde belangen van entiteiten met zeer belangrijke impact of met kritieke impact, alsook van leveranciers van beveiligingstechnologieën en -diensten die namens die entiteiten optreden, op grond van artikel 6, lid 1, punt f), van Verordening (EU) 2016/679, onder meer wanneer een dergelijke verwerking noodzakelijk is voor regelingen voor het delen van cyberbeveiligingsinformatie of de vrijwillige melding van relevante informatie overeenkomstig deze verordening. Maatregelen met betrekking tot de preventie, opsporing, identificatie, indamming en analyse van cyberaanvallen en de reactie erop, maatregelen om het bewustzijn met betrekking tot specifieke cyberdreigingen te vergroten, uitwisseling van inlichtingen in het kader van herstel van de kwetsbaarheid en gecoördineerde openbaarmaking van de kwetsbaarheid, de vrijwillige uitwisseling van informatie over die cyberaanvallen, alsmede cyberdreigingen en kwetsbaarheden, indicatoren voor aantasting, tactieken, technieken en procedures, cyberbeveiligingswaarschuwingen en configuratiehulpmiddelen kunnen de verwerking vereisen van bepaalde categorieën persoonsgegevens, zoals IP-adressen, uniforme resources locators (URL's), domeinnamen, e-mailadressen en, voor zover hieruit persoonsgegevens blijken, tijdstempels. De verwerking van persoonsgegevens door de bevoegde instanties, de centrale contactpunten en de CSIRT's kan een wettelijke verplichting vormen of noodzakelijk worden geacht voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen op grond van artikel 6, lid 1, punt c) of e), en artikel 6, lid 3, van Verordening (EU) 2016/679, of voor de behartiging van een gerechtvaardigd belang van de entiteiten met zeer belangrijke impact of met kritieke impact, in de zin van artikel 6, lid 1, punt f), van die verordening. Voorts kunnen in het nationale recht regels worden vastgesteld die het de bevoegde instanties, de centrale contactpunten en de CSIRT's, voor zover noodzakelijk en evenredig ten behoeve van het waarborgen van de beveiliging van netwerk- en informatiesystemen van entiteiten met zeer belangrijke impact of met kritieke impact, toelaten om bijzondere categorieën van persoonsgegevens te verwerken overeenkomstig artikel 9 van Verordening (EU) 2016/679, met name door passende en specifieke maatregelen te treffen ter bescherming van de grondrechten en de belangen van natuurlijke personen, met inbegrip van technische beperkingen op het hergebruik van dergelijke gegevens en het gebruik van geavanceerde beveiligings- en privacybeschermingsmaatregelen, zoals pseudonimisering, of versleuteling wanneer anonimisering het nagestreefde doel aanzienlijk kan beïnvloeden.

([11]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1).

([12]) Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37).

([13]) Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39).

(34) Persoonsgegevens komen vaak in gevaar als gevolg van cyberaanvallen. In dat verband moeten de bevoegde instanties samenwerken en inlichtingen uitwisselen over alle relevante aangelegenheden met de in Verordening (EU) 2016/679 en Richtlijn 2002/58/EG bedoelde instanties.

(35) Overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 is de Europese Toezichthouder voor gegevensbescherming geraadpleegd, en op 17 november 2023 heeft hij een advies uitgebracht,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

HOOFDSTUK I

ALGEMENE BEPALINGEN

Artikel 1

Voorwerp

Bij deze verordening wordt een netcode vastgesteld die sectorspecifieke voorschriften bevat voor met cyberbeveiliging samenhangende aspecten van grensoverschrijdende elektriciteitsstromen, regels over gemeenschappelijke minimumvereisten, planning, toezicht, rapportage en crisisbeheer.

Artikel 2

Toepassingsgebied

1. Deze verordening is van toepassing op met cyberbeveiliging samenhangende aspecten van grensoverschrijdende elektriciteitsstromen in de activiteiten van de volgende entiteiten, indien deze overeenkomstig artikel 24 zijn aangemerkt als entiteiten met zeer belangrijke impact of met kritieke impact:

a) elektriciteitsbedrijven in de zin van artikel 2, punt 57, van Richtlijn (EU) 2019/944;

b) benoemde elektriciteitsmarktbeheerders ("NEMO") in de zin van artikel 2, punt 8, van Richtlijn (EU) 2019/943;

c) georganiseerde markten in de zin van artikel 2, lid 4, van Uitvoeringsverordening (EU) nr. 1348/2014 van de Commissie ([14]) die transacties regelen met betrekking tot producten die van belang zijn voor grensoverschrijdende elektriciteitsstromen;

d) aanbieders van kritieke ICT-diensten als bedoeld in artikel 3, punt 9;

e) het ENTSB voor elektriciteit, opgericht krachtens artikel 28 van Verordening (EU) 2019/943;

f) de EU DSB-entiteit, opgericht krachtens artikel 52 van Verordening (EU) 2019/943;

g) balanceringsverantwoordelijken in de zin van artikel 2, punt 14, van Verordening (EU) 2019/943;

h) exploitanten van laadpunten in de zin van bijlage I bij Richtlijn (EU) 2022/2555;

i) regionale coördinatiecentra, opgericht krachtens artikel 35 van Verordening (EU) 2019/943;

j) aanbieders van beheerde beveiligingsdiensten in de zin van artikel 6, punt 40, van Richtlijn (EU) 2022/2555;

k) iedere andere entiteit of derde waaraan overeenkomstig deze verordening bevoegdheden zijn gedelegeerd of toegewezen.

2. De volgende autoriteiten zijn, in het kader van hun huidige opdracht, verantwoordelijk voor het verrichten van de in deze verordening toegewezen werkzaamheden:

a) het Agentschap van de Europese Unie voor de samenwerking tussen energieregulators ("ACER"), opgericht bij Verordening (EU) 2019/942 van het Europees Parlement en de Raad ([15]);

b) nationale bevoegde instanties die belast zijn met het verrichten van de werkzaamheden die hun uit hoofde van deze verordening zijn toegewezen en door de lidstaten zijn aangeduid overeenkomstig artikel 4, ofwel "bevoegde instantie";

c) nationale regelgevende instanties ("NRI's") die door elke lidstaat zijn aangewezen overeenkomstig artikel 57, lid 1, van Richtlijn (EU) 2019/944;

([14]) Uitvoeringsverordening (EU) nr. 1348/2014 van de Commissie van 17 december 2014 inzake de informatieverstrekking overeenkomstig artikel 8, leden 2 en 6, van Verordening (EU) nr. 1227/2011 van het Europees Parlement en de Raad betreffende de integriteit en transparantie van de groothandelsmarkt voor energie (PB L 363 van 18.12.2014, blz. 121).

([15]) Verordening (EU) 2019/942 van het Europees Parlement en de Raad van 5 juni 2019 tot oprichting van een Agentschap van de Europese Unie voor de samenwerking tussen energieregulators (PB L 158 van 14.6.2019, blz. 22).

d) bevoegde instanties voor risicoparaatheid ("RP-NCA's"), opgericht overeenkomstig artikel 3 van Verordening (EU) 2019/941;

e) computer security incident response teams ("CSIRT's"), zoals aangewezen of opgericht overeenkomstig artikel 10 van Richtlijn (EU) 2022/2555;

f) bevoegde instanties, verantwoordelijk voor cyberbeveiliging ("CS-NCA's"), zoals aangewezen of opgericht overeenkomstig artikel 8 van Richtlijn (EU) 2022/2555;

g) het Agentschap van de Europese Unie voor cyberbeveiliging, opgericht overeenkomstig Verordening (EU) 2019/881;

h) iedere andere entiteit of derde waaraan overeenkomstig artikel 4, lid 3, bevoegdheden zijn gedelegeerd of toegewezen.

3. Deze verordening is ook van toepassing op alle entiteiten die niet in de Unie zijn gevestigd, maar die diensten verlenen aan entiteiten in de Unie, mits zij door de bevoegde instanties overeenkomstig artikel 24, lid 2, als entiteiten met zeer belangrijke impact of met kritieke impact zijn aangemerkt.

4. Deze verordening laat de verantwoordelijkheid van de lidstaten onverlet om de nationale veiligheid te beschermen en hun bevoegdheid om andere essentiële staatsfuncties te beschermen, waaronder de verdediging van de territoriale integriteit van de staat en de handhaving van de openbare orde.

5. Deze verordening laat de verantwoordelijkheid van de lidstaten onverlet om de nationale veiligheid te beschermen met betrekking tot activiteiten op het gebied van de productie van elektriciteit uit kerncentrales, met inbegrip van activiteiten binnen de nucleaire waardeketen, overeenkomstig de Verdragen.

6. Entiteiten, de bevoegde instanties, de centrale contactpunten op entiteitsniveau en de CSIRT's verwerken persoonsgegevens voor zover dat nodig is voor de toepassing van deze verordening en overeenkomstig Verordening (EU) 2016/679, en met name berust een dergelijke verwerking op artikel 6 daarvan.

Artikel 3

Definities

De volgende definities zijn van toepassing:

1) "actief": informatie, software of hardware in de netwerk- en informatiesystemen, materieel of immaterieel, die van waarde is voor een persoon, een organisatie of een overheid;

2) "bevoegde instantie voor risicoparaatheid": de overeenkomstig artikel 3 van Verordening (EU) 2019/941 opgerichte bevoegde instantie;

3) "computer security incident response team": een team dat verantwoordelijk is voor de behandeling van risico's en incidenten overeenkomstig artikel 10 van Richtlijn (EU) 2022/2555;

4) "actief met kritieke impact": een actief dat noodzakelijk is om een proces met kritieke impact uit te voeren;

5) "entiteit met kritieke impact": een entiteit die een proces met kritieke impact uitvoert en door de bevoegde instanties overeenkomstig artikel 24 is aangemerkt;

6) "perimeter van kritieke impact": een door een in artikel 2, lid 1, bedoelde entiteit gedefinieerde perimeter die alle activa met kritieke impact omvat en op welk punt de toegang tot die activa kan worden gecontroleerd, en die het toepassingsgebied definieert waarop geavanceerde cyberbeveiligingscontroles van toepassing zijn;

7) "proces met kritieke impact": een bedrijfsproces dat wordt uitgevoerd door een entiteit waarvoor de impactindices voor de cyberbeveiliging van elektriciteit boven de drempel voor kritieke impact liggen;

8) "drempel voor kritieke impact": de waarden van de in artikel 19, lid 3, punt b), bedoelde impactindices voor de cyberbeveiliging van elektriciteit, waarboven een cyberaanval op een bedrijfsproces een kritieke verstoring van grensoverschrijdende elektriciteitsstromen veroorzaakt;

9) "aanbieder van kritieke ICT-diensten": een entiteit die een ICT-dienst of een ICT-proces aanbiedt die of dat noodzakelijk is voor een proces met kritieke impact of een proces met zeer belangrijke impact dat van invloed is op de met cyberbeveiliging samenhangende aspecten van grensoverschrijdende elektriciteitsstromen en dat, indien het in gevaar komt, een cyberaanval kan veroorzaken met gevolgen boven de drempel voor kritieke impact of voor zeer belangrijke impact;

10) "grensoverschrijdende elektriciteitsstroom": een grensoverschrijdende stroom in de zin van artikel 2, punt 3, van Verordening (EU) 2019/943;

11) "cyberaanval": een incident in de zin van artikel 3, punt 14, van Verordening (EU) 2022/2554;

12) "cyberbeveiliging": cyberbeveiliging in de zin van artikel 2, punt 1, van Verordening (EU) 2019/881;

13) “cyberbeveiligingscontrole”: de acties of procedures om cyberbeveiligingsrisico’s te vermijden, op te sporen, tegen te gaan of tot een minimum te beperken;

14) “cyberbeveiligingsincident”: een incident in de zin van artikel 6, punt 6, van Richtlijn (EU) 2022/2555;

15) “cyberbeveiligingsbeheersysteem”: het beleid, de procedures, de richtsnoeren en de bijbehorende middelen en activiteiten, gezamenlijk beheerd door een entiteit, ter bescherming van haar informatieactiva tegen cyberdreigingen, waarbij de beveiliging van het netwerk en de informatiesystemen van een organisatie stelselmatig wordt vastgesteld, uitgevoerd, geëxploiteerd, gemonitord, geëvalueerd, onderhouden en verbeterd;

16) “operationeel centrum voor cyberbeveiliging”: een speciaal centrum waar een technisch team van een of meer deskundigen, ondersteund door cyberbeveiligingsystemen, beveiligingstaken uitvoert (diensten van het operationeel centrum voor cyberbeveiliging), zoals de reactie op cyberaanvallen en de behandeling van fouten in de beveiligings-configuratie, beveiligingsmonitoring, loganalyse en cyberaanvaldetectie;

17) “cyberdreiging”: een cyberdreiging in de zin van artikel 2, punt 8, van Verordening (EU) 2019/881;

18) “kwetsbaarheidsbeheer op het gebied van cyberbeveiliging”: de praktijk om kwetsbaarheden in kaart te brengen en aan te pakken;

19) “entiteit”: een entiteit in de zin van artikel 6, punt 38, van Richtlijn (EU) 2022/2555;

20) “vroegtijdige waarschuwing”: de informatie die nodig is om aan te geven of het significante incident veroorzaakt wordt geacht door onrechtmatige of kwaadwillige handelingen, en of het grensoverschrijdende gevolgen kan hebben;

21) “impactindex voor de cyberbeveiliging van elektriciteit” (“ECII”): een index of classificatieschema waarin de mogelijke gevolgen van cyberaanvallen voor bedrijfsprocessen voor grensoverschrijdende elektriciteitsstromen worden gerangschikt;

22) “Europese cyberbeveiligingscertificeringsregeling”: een regeling in de zin van artikel 2, punt 9, van Verordening (EU) 2019/881;

23) “entiteit met zeer belangrijke impact”: een entiteit die een proces met zeer belangrijke impact uitvoert en door de bevoegde instanties overeenkomstig artikel 24 is aangemerkt;

24) “proces met zeer belangrijke impact”: een bedrijfsproces dat wordt uitgevoerd door een entiteit waarvoor de impactindices voor de cyberbeveiliging van elektriciteit boven de drempel voor zeer belangrijke impact liggen;

25) “actief met zeer belangrijke impact”: een actief dat noodzakelijk is om een proces met zeer belangrijke impact uit te voeren;

26) “drempel voor zeer belangrijke impact”: de waarden van de in artikel 19, lid 3, punt b), bedoelde impactindices voor de cyberbeveiliging van elektriciteit, waarboven een geslaagde cyberaanval op een proces een zeer belangrijke verstoring van grensoverschrijdende elektriciteitsstromen veroorzaakt;

27) “perimeter van zeer belangrijke impact”: een door een in artikel 2, lid 1, bedoelde entiteit gedefinieerde perimeter die alle activa met zeer belangrijke impact omvat en op welk punt de toegang tot die activa kan worden gecontroleerd, en die het toepassingsgebied definieert waarop minimale cyberbeveiligingscontroles van toepassing zijn;

28) “ICT-product”: een ICT-product in de zin van artikel 2, punt 12, van Verordening (EU) 2019/881;

29) “ICT-dienst”: een ICT-dienst in de zin van artikel 2, punt 13, van Verordening (EU) 2019/881;

30) “ICT-proces”: een ICT-proces in de zin van artikel 2, punt 14, van Verordening (EU) 2019/881;

31) “legacy-systeem”: een legacy-ICT-systeem in de zin van artikel 3, punt 3, van Verordening (EU) 2022/2554;

32) “nationaal centraal contactpunt”: het centrale contactpunt dat door iedere lidstaat is aangewezen of ingesteld overeenkomstig artikel 8, lid 3, van Richtlijn (EU) 2022/2555;

33) “NIS-cybercrisisbeheerautoriteiten”: de autoriteiten die zijn aangewezen of ingesteld overeenkomstig artikel 9, punt 1, van Richtlijn (EU) 2022/2555;

34) “opsteller”: een entiteit die informatie-uitwisseling, informatiedeling of informatieopslag opstelt;

35) “aanbestedingsspecificaties”: de specificaties die entiteiten vaststellen voor de aanbesteding van nieuwe of geactualiseerde ICT-producten, -processen of -diensten;

36) “vertegenwoordiger”: een in de Unie gevestigde natuurlijke of rechtspersoon die uitdrukkelijk is aangewezen om op te treden namens een entiteit met zeer belangrijke impact of met kritieke impact die niet in de Unie is gevestigd, maar diensten levert aan entiteiten in de Unie en die door een bevoegde instantie of een CSIRT kan worden aangesproken in de plaats van de entiteit met zeer belangrijke impact of met kritieke impact zelf ten aanzien van de verplichtingen van die entiteit uit hoofde van deze verordening;

37) “risico”: een risico in de zin van artikel 6, punt 9, van Richtlijn (EU) 2022/2555;

38) “risicoimpactmatrix”: een matrix die bij een risicobeoordeling wordt gebruikt om het resulterende risicoimpactniveau per beoordeeld risico te bepalen;

39) “gelijktijdige elektriciteitscrisis”: een elektriciteitscrisis in de zin van artikel 2, punt 10, van Verordening (EU) 2019/941;

40) “centraal contactpunt op entiteitsniveau”: centraal contactpunt op entiteitsniveau zoals aangemerkt krachtens artikel 38, lid 1, punt c);

41) “belanghebbende”: een partij die belang heeft bij het welslagen en de voortdurende werking van een organisatie of proces, zoals werknemers, bestuurders, aandeelhouders, regelgevers, organisaties, leveranciers en klanten;

42) “norm”: een norm in de zin van artikel 2, punt 1, van Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad ([16]);

43) “systeembeheersregio”: de systeembeheersregio’s in de zin van bijlage I bij ACER-besluit 05-2022 inzake de definitie van systeembeheersregio’s, vastgesteld overeenkomstig artikel 36 van Verordening (EU) 2019/943;

44) “systeembeheerders”: “distributiesysteembeheerder” (“DSB”) en “transmissiesysteembeheerder” (“TSB”) in de zin van de artikelen 2, punten 29 en 35, van Richtlijn (EU) 2019/944;

45) “Uniebreed proces met kritieke impact”: een proces in de elektriciteitssector, waarbij mogelijk meerdere entiteiten betrokken zijn, waarbij de mogelijke gevolgen van een cyberaanval kritiek kunnen worden geacht bij de uitvoering van de Uniebrede cyberbeveiligingsrisicobeoordeling;

46) “Uniebreed proces met zeer belangrijke impact”: een proces in de elektriciteitssector, waarbij mogelijk meerdere entiteiten betrokken zijn, waarbij de mogelijke gevolgen van een cyberaanval zeer belangrijk kunnen worden geacht bij de uitvoering van de Uniebrede cyberbeveiligingsrisicobeoordeling;

47) “actief uitgebuite nog niet verholpen kwetsbaarheid”: een kwetsbaarheid die nog niet openbaar is gemaakt en nog niet is verholpen, en waarvoor er betrouwbare aanwijzingen zijn dat een partij een kwaadaardige code in een systeem heeft uitgevoerd zonder toestemming van de systeemeigenaar;

48) “kwetsbaarheid”: een kwetsbaarheid in de zin van artikel 6, punt 15, van Richtlijn (EU) 2022/2555.

Artikel 4

Bevoegde instantie

1. Elke lidstaat wijst zo spoedig mogelijk en in elk geval uiterlijk 13 december 2024 een nationale overheidsinstantie of een nationale regelgevende instantie aan om de bij deze verordening daaraan toegewezen werkzaamheden te verrichten (“bevoegde instantie”). Tot het moment dat de bevoegde instantie belast is met de verrichting van de werkzaamheden uit hoofde van deze verordening, verricht de overeenkomstig artikel 57, lid 1, van Richtlijn (EU) 2019/944 door elke lidstaat aangewezen regelgevende instantie de werkzaamheden van de bevoegde instantie overeenkomstig deze verordening.

2. De lidstaten stellen de Commissie, ACER, Enisa, de bij artikel 14 van Richtlijn (EU) 2022/2555 opgerichte NIS-samenwerkingsgroep en de bij artikel 1 van het besluit van de Commissie van 15 november 2012 ([17]) opgerichte Coördinatiegroep voor elektriciteit onverwijld in kennis van, en delen hun de naam en de contactgegevens van hun overeenkomstig lid 1 aangewezen bevoegde instantie en alle latere wijzigingen daarvan mee.

([16]) Verordening (EU) nr. 1025/2012 van het Europees Parlement en de Raad van 25 oktober 2012 betreffende Europese normalisatie, tot wijziging van de Richtlijnen 89/686/EEG en 93/15/EEG van de Raad alsmede de Richtlijnen 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG en 2009/105/EG van het Europees Parlement en de Raad en tot intrekking van Beschikking 87/95/EEG van de Raad en Besluit nr. 1673/2006/EG van het Europees Parlement en de Raad (PB L 316 van 14.11.2012, blz. 12).

([17]) Besluit van de Commissie van 15 november 2012 betreffende de oprichting van een Coördinatiegroep voor elektriciteit (2012/C 353/02) (PB C 353 van 17.11.2012, blz. 2).

3. De lidstaten kunnen hun bevoegde instantie machtigen aan andere nationale instanties werkzaamheden te delegeren, met uitzondering van de in artikel 5 genoemde werkzaamheden. Iedere bevoegde instantie houdt toezicht op de toepassing van deze verordening door de instanties waaraan zij werkzaamheden heeft gedelegeerd. De bevoegde instantie deelt de naam, de contactgegevens, de toegewezen werkzaamheden en alle latere wijzigingen daarvan van de instanties waaraan een taak is gedelegeerd, aan de Commissie, ACER, de Coördinatiegroep voor elektriciteit, Enisa en de NIS-samenwerkingsgroep mee.

Artikel 5

Samenwerking tussen instanties en organen op nationaal niveau

De bevoegde instanties coördineren en zorgen voor passende samenwerking tussen de bevoegde instanties, verantwoordelijk voor cyberbeveiliging, de cybercrisisbeheerautoriteiten, de NRI's, de bevoegde instanties voor risicoparaatheid en CSIRT's met het oog op de naleving van de toepasselijke verplichtingen van deze verordening. De bevoegde instanties werken ook samen met andere organen of instanties, zoals bepaald door iedere lidstaat, om efficiënte procedures te waarborgen en overlapping van werkzaamheden en verplichtingen te voorkomen. De bevoegde instanties kunnen de respectieve NRI's opdragen ACER om advies te vragen overeenkomstig artikel 8, lid 3.

Artikel 6

Voorwaarden of methoden of plannen

1. De TSB's ontwikkelen, in samenwerking met de EU DSB-entiteit, voorstellen voor de voorwaarden of methoden overeenkomstig lid 2, of voor plannen overeenkomstig lid 3.

2. De volgende voorwaarden of methoden, alsmede wijzigingen daarvan, worden ter goedkeuring voorgelegd aan alle bevoegde instanties:

a) de beoordelingsmethoden voor cyberbeveiligingsrisico's overeenkomstig artikel 18, lid 1;

b) het uitgebreide beoordelingsverslag over grensoverschrijdende cyberbeveiligingsrisico's voor elektriciteit overeenkomstig artikel 23;

c) de minimale en geavanceerde cyberbeveiligingscontroles overeenkomstig artikel 29, en het afzetten van cyberbeveiligingscontroles voor elektriciteit tegen normen overeenkomstig artikel 34, met inbegrip van minimale en geavanceerde cyberbeveiligingscontroles in de toeleveringsketen overeenkomstig artikel 33;

d) een aanbeveling voor aanbestedingen op het gebied van cyberbeveiliging overeenkomstig artikel 35;

e) de methode voor een classificatieschema van cyberaanvallen overeenkomstig artikel 37, lid 8.

3. De voorstellen voor de regionale plannen ter beperking van cyberbeveiligingsrisico's overeenkomstig artikel 22 moeten worden goedgekeurd door alle bevoegde instanties van de betrokken systeembeheersregio.

4. De voorstellen voor de in lid 2 genoemde voorwaarden en methoden of voor de in lid 3 genoemde plannen omvatten een voorgesteld tijdschema voor de uitvoering en een beschrijving van het verwachte effect op de doelstellingen van deze verordening.

5. De EU DSB-entiteit kan de betrokken TSB's tot drie weken vóór het verstrijken van de termijn een met redenen omkleed advies sturen om het voorstel voor de voorwaarden of methoden of voor de plannen bij de bevoegde instanties in te dienen. De voor het voorstel voor de voorwaarden of methoden of voor de plannen verantwoordelijke TSB's nemen het met redenen omklede advies van de EU DSB-entiteit in aanmerking voordat het ter goedkeuring aan de bevoegde instanties wordt voorgelegd. De TSB's verstrekken een motivering indien het advies van de EU DSB-entiteit niet in aanmerking is genomen.

6. Bij de gezamenlijke ontwikkeling van de voorwaarden en methoden en de plannen werken de deelnemende TSB's nauw samen. Met de hulp van het ENTSB voor elektriciteit en in samenwerking met de EU DSB-entiteit informeren de TSB's de bevoegde instanties en ACER regelmatig over de voortgang van de ontwikkeling van de voorwaarden of methoden, en van de plannen.

Artikel 7

Stemregels in de TSB's

1. Indien de TSB's die over voorstellen voor voorwaarden of methoden besluiten, geen overeenstemming kunnen bereiken, nemen zij een besluit met gekwalificeerde meerderheid van stemmen. Een gekwalificeerde meerderheid voor dergelijke voorstellen wordt als volgt berekend:

a) TSB's die ten minste 55 % van de lidstaten vertegenwoordigen, en

b) TSB's die lidstaten vertegenwoordigen die ten minste 65 % van de bevolking van de Unie vertegenwoordigen.

2. Een blokkerende minderheid voor besluiten over in artikel 6, lid 2, genoemde voorstellen voor voorwaarden of methoden omvat TSB's die minimaal vier lidstaten vertegenwoordigen; als er geen blokkerende minderheid is, wordt de gekwalificeerde meerderheid geacht te zijn bereikt.

3. Indien TSB's van een systeembeheersregio die over in artikel 6, lid 2, genoemde voorstellen voor plannen besluiten, geen overeenstemming kunnen bereiken en indien de betrokken systeembeheersregio uit meer dan vijf lidstaten bestaat, nemen de TSB's een besluit bij gekwalificeerde meerderheid van stemmen. Een gekwalificeerde meerderheid voor de in artikel 6, lid 2, genoemde voorstellen vereist de volgende meerderheid:

a) TSB's die ten minste 72 % van de betrokken lidstaten vertegenwoordigen, en

b) TSB's die lidstaten vertegenwoordigen die ten minste 65 % van de bevolking van het betrokken gebied vertegenwoordigen.

4. Een blokkerende minderheid voor besluiten inzake voorstellen voor plannen omvat ten minste het minimumaantal TSB's dat meer dan 35 % van de bevolking van de deelnemende lidstaten vertegenwoordigt, plus TSB's die ten minste één extra betrokken lidstaat vertegenwoordigen; als er geen blokkerende minderheid is, wordt de gekwalificeerde meerderheid geacht te zijn bereikt.

5. Voor besluiten van de TSB over voorstellen voor voorwaarden of methoden overeenkomstig artikel 6, lid 2, wordt per lidstaat één stem toegekend. Als er op het grondgebied van een lidstaat meer dan één TSB is, verdeelt die lidstaat de stembevoegdheden over de TSB's.

6. Indien de TSB's, in samenwerking met de EU DSB-entiteit, niet binnen de in deze verordening vastgestelde termijnen bij de relevante bevoegde instanties een eerste of een gewijzigd voorstel voor voorwaarden of methoden of voor plannen indienen, verstrekken zij de relevante bevoegde instanties en ACER de betrokken ontwerpen van de voorwaarden of methoden, of van de plannen. Zij lichten toe waarom er geen overeenkomst is bereikt. De bevoegde instanties treffen gezamenlijk de passende maatregelen om de vereiste voorwaarden of methoden of de vereiste plannen vast te stellen. Dit kan bijvoorbeeld geschieden door overeenkomstig dit lid te verzoeken om wijzigingen in de ontwerpen, door die ontwerpen te herzien en aan te vullen, of, indien er geen ontwerpen zijn ingediend, door de vereiste voorwaarden of methoden of de vereiste plannen vast te stellen en goed te keuren.

Artikel 8

Indiening van voorstellen bij de bevoegde instanties

1. De TSB's dienen de voorstellen voor voorwaarden of methoden of voor plannen ter goedkeuring in bij de relevante bevoegde instanties binnen de in de artikelen 18, 23, 29, 33, 34, 35 en 37 vastgestelde termijnen. De bevoegde instanties kunnen deze termijnen in uitzonderlijke omstandigheden gezamenlijk verlengen, met name in gevallen waarin een termijn niet kan worden gehaald als gevolg van omstandigheden buiten de macht van TSB's of van de EU DSB-entiteit.

2. Voorstellen voor voorwaarden, methoden of plannen overeenkomstig lid 1 worden ter informatie bij ACER ingediend op hetzelfde moment dat zij bij de bevoegde instanties worden ingediend.

3. Op gezamenlijk verzoek van de NRI's brengt ACER binnen een termijn van zes maanden na ontvangst van de voorstellen voor voorwaarden of methoden, of voor plannen, daarover advies uit en stelt het de NRI's en de bevoegde instanties in kennis van zijn advies. De NRI's, de CS-NCA's en alle andere als bevoegde instantie aangewezen instanties plegen onderling overleg voordat de NRI's ACER om advies verzoeken. ACER kan in zijn advies aanbevelingen opnemen. ACER raadpleegt Enisa alvorens advies uit te brengen over de in artikel 6, lid 2, genoemde voorstellen.

4. De bevoegde instanties plegen overleg en werken nauw samen om overeenstemming te bereiken over de voorgestelde voorwaarden, methoden of plannen. Alvorens de voorwaarden of methoden of de plannen goed te keuren, herzien en vervolledigen zij de voorstellen indien nodig, na raadpleging van het ENTSB voor elektriciteit en de EU DSB-entiteit, om te waarborgen dat de voorstellen in overeenstemming zijn met deze verordening en bijdragen tot een hoog gemeenschappelijk niveau van cyberbeveiliging in de hele Unie.

5. De bevoegde instanties nemen, binnen een termijn van zes maanden na ontvangst daarvan door de relevante bevoegde instantie of, in voorkomend geval, door de laatste betrokken relevante bevoegde instantie, een besluit over de voorwaarden of methoden of over de plannen.

6. Indien ACER een advies uitbrengt, nemen de relevante bevoegde instanties dat advies in aanmerking en nemen zij hun besluiten binnen een termijn van zes maanden na ontvangst van het advies van ACER.

7. Indien de bevoegde instanties gezamenlijk een wijziging van de voorgestelde voorwaarden of methoden of van de plannen verlangen om die goed te keuren, ontwikkelen de TSB's, in samenwerking met de EU DSB-entiteit, een voorstel tot wijziging. De TSB's dienen binnen een termijn van twee maanden na het verzoek van de bevoegde instanties het gewijzigde voorstel ter goedkeuring in. De bevoegde instanties nemen binnen een termijn van twee maanden na de indiening een besluit over de gewijzigde voorwaarden of methoden, of over de gewijzigde plannen.

8. Indien de bevoegde instanties binnen de in lid 5 of lid 7 bedoelde termijn geen overeenstemming hebben kunnen bereiken, stellen zij de Commissie daarvan in kennis. De Commissie kan passende maatregelen treffen om de vereiste voorwaarden of methoden of plannen te doen vaststellen.

9. De TSB's publiceren, met de hulp van het ENTSB voor elektriciteit en de EU DSB-entiteit, de voorwaarden of methoden of de plannen op hun website na goedkeuring door de relevante bevoegde instanties, tenzij die informatie overeenkomstig artikel 47 als vertrouwelijk wordt beschouwd.

10. De bevoegde instanties kunnen de TSB's en de EU DSB-entiteit gezamenlijk verzoeken om voorstellen tot wijziging van de goedgekeurde voorwaarden of methoden, of van de goedgekeurde plannen, en een termijn bepalen voor de indiening van die voorstellen. De TSB's kunnen, in samenwerking met de EU DSB-entiteit, ook ambtshalve wijzigingen voorstellen aan de bevoegde instanties. De voorstellen tot wijziging van de voorwaarden of methoden, of voor wijzigingen van de plannen, worden ontwikkeld en goedgekeurd volgens de procedure van dit artikel.

11. Ten minste om de drie jaar na de eerste vaststelling van de respectieve voorwaarden of methoden, of de respectieve vastgestelde plannen, evalueren de TSB's in samenwerking met de EU DSB-entiteit de doeltreffendheid van de vastgestelde voorwaarden of methoden, of van de vastgestelde plannen, en brengen onverwijld verslag uit aan de bevoegde instanties en ACER over de resultaten van de beoordeling.

Artikel 9

Overleg

1. Met de hulp van het ENTSB voor elektriciteit en in samenwerking met de EU DSB-entiteit raadplegen de TSB's de belanghebbenden, waaronder ACER, Enisa en de bevoegde instantie van iedere lidstaat, over de ontwerpvoorstellen voor de in artikel 6, lid 2, genoemde voorwaarden of methoden en voor de in artikel 6, lid 3, genoemde plannen. De duur van de raadpleging bedraagt ten minste één maand.

2. De in artikel 6, lid 2, genoemde voorstellen voor voorwaarden of methoden die door de TSB's, in samenwerking met de EU DSB-entiteit, zijn ingediend, worden bekendgemaakt en ter raadpleging voorgelegd op het niveau van de Unie. De in artikel 6, lid 3, genoemde voorstellen voor plannen die door de relevante TSB's, in samenwerking met de EU DSB-entiteit, op regionaal niveau zijn ingediend, worden ten minste op regionaal niveau ter raadpleging voorgelegd.

3. Met de hulp van het ENTSB voor elektriciteit, en de EU DSB-entiteit die verantwoordelijk is voor het voorstel voor de voorwaarden of methoden of voor de plannen, houden de TSB's afdoende rekening met de standpunten van de belanghebbenden zoals die naar voren komen uit de raadplegingen overeenkomstig lid 1, voordat het ter goedkeuring aan de regelgevende instantie wordt voorgelegd. In alle gevallen wordt bij de indiening van een voorstel voor voorwaarden of methoden een deugdelijke rechtvaardiging voor het al dan niet in dat voorstel opnemen van de uit de raadpleging voortgekomen standpunten gegeven; deze rechtvaardiging wordt tijdig, voorafgaand aan of gelijktijdig met het voorstel voor voorwaarden of methoden, bekendgemaakt.

Artikel 10

Betrokkenheid van belanghebbenden

ACER organiseert, in nauwe samenwerking met het ENTSB voor elektriciteit en de EU DSB-entiteit, dat belanghebbenden betrokken kunnen worden, onder meer door regelmatige bijeenkomsten met belanghebbenden om problemen in kaart te brengen en verbeteringen voor te stellen in verband met de uitvoering van deze verordening.

Artikel 11

Verhaal van kosten

1. De door de TSB's en de DSB's gedragen kosten die onderworpen zijn aan nettariefregulering en voortvloeien uit de in deze verordening vastgestelde verplichtingen, met inbegrip van de door het ENTSB voor elektriciteit en de EU DSB-entiteit gedragen kosten, worden door de relevante NRI van iedere lidstaat beoordeeld.

2. Kosten die als redelijk, doelmatig en evenredig worden beoordeeld, worden verhaald door middel van nettarieven of andere passende mechanismen, zoals bepaald door de desbetreffende NRI.

3. Op verzoek van de relevante NRI's verstrekken de in lid 1 bedoelde TSB's en DSB's binnen een redelijke, door de NRI bepaalde termijn de informatie om de beoordeling van de gemaakte kosten te vergemakkelijken.

Artikel 12

Toezicht

1. ACER houdt toezicht op de uitvoering van deze verordening overeenkomstig artikel 32, lid 1, van Verordening (EU) 2019/943 en artikel 4, lid 2, van Verordening (EU) 2019/942. Bij de uitvoering van dit toezicht kan ACER met Enisa samenwerken en kan het het ENTSB voor elektriciteit en de EU DSB-entiteit om steun verzoeken. ACER informeert de Coördinatiegroep voor elektriciteit en de NIS-samenwerkingsgroep regelmatig over de uitvoering van deze verordening.

2. ACER publiceert ten minste om de drie jaar na de inwerkingtreding van deze verordening een verslag om:

a) de stand van de uitvoering van de toepasselijke maatregelen voor het beheer van cyberbeveiligingsrisico's te evalueren met betrekking tot de entiteiten met zeer belangrijke impact en de entiteiten met kritieke impact;

b) na te gaan of aanvullende regels inzake gemeenschappelijke vereisten, planning, toezicht, rapportage en crisisbeheersing nodig kunnen zijn om risico's voor de elektriciteitssector te voorkomen, en

c) verbeterpunten voor de herziening van deze verordening vast te stellen, of onontgonnen terreinen en nieuwe prioriteiten te bepalen die zich als gevolg van technologische ontwikkelingen kunnen voordoen.

3. Uiterlijk 13 juni 2025 kan ACER, in samenwerking met Enisa en na raadpleging van het ENTSB voor elektriciteit en de EU DSB-entiteit, richtsnoeren uitvaardigen over de relevante informatie die voor toezichtsdoeleinden aan ACER wordt meegedeeld, alsook over het proces en de regelmaat van de verzameling, op basis van de overeenkomstig lid 5 vastgestelde prestatie-indicatoren.

4. De bevoegde entiteit kan toegang krijgen tot de relevante informatie waarover ACER beschikt en die het overeenkomstig dit artikel heeft verzameld.

5. ACER stelt in samenwerking met Enisa en met de steun van het ENTSB voor elektriciteit en de EU DSB-entiteit niet-bindende prestatie-indicatoren vast voor de beoordeling van de operationele betrouwbaarheid in verband met de met cyberbeveiliging samenhangende aspecten van grensoverschrijdende elektriciteitsstromen.

6. De in artikel 2, lid 1, genoemde entiteiten dienen bij ACER de informatie in die ACER nodig heeft om de in lid 2 genoemde werkzaamheden te verrichten.

Artikel 13

Benchmarking

1. Uiterlijk 13 juni 2025 stelt ACER, in samenwerking met Enisa, een niet-bindende gids voor cyberbeveiligingsbenchmarking op. In de gids wordt aan de NRI's uitgelegd wat de beginselen zijn van benchmarking van de uitgevoerde cyberbeveiligingscontroles overeenkomstig lid 2, met inachtneming van de kosten van de uitvoering van de controles en de doeltreffendheid van de functie van de processen, producten, diensten, systemen en oplossingen om dergelijke controles uit te voeren. ACER houdt rekening met bestaande benchmarkverslagen bij het opstellen van de niet-bindende gids voor cyberbeveiligingsbenchmarking. ACER legt de niet-bindende gids voor cyberbeveiligingsbenchmarking ter informatie aan de NRI's voor.

2. Binnen twaalf maanden na de opstelling van de benchmarkinggids overeenkomstig lid 1 voeren de NRI's een benchmarkinganalyse uit om na te gaan of de huidige investeringen in cyberbeveiliging:

a) de risico's met gevolgen voor grensoverschrijdende elektriciteitsstromen beperken;

b) de gewenste resultaten opleveren en efficiëntiewinst opleveren voor de ontwikkeling van elektriciteitssystemen;

c) efficiënt zijn en in de algemene aankoop van activa en diensten geïntegreerd zijn.

3. Voor de benchmarkinganalyse kunnen de NRI's de door ACER opgestelde niet-bindende gids voor cyberbeveiligingsbenchmarking in aanmerking nemen, en beoordelen zij in het bijzonder:

a) de gemiddelde uitgaven in verband met cyberbeveiliging ter beperking van risico's met gevolgen voor grensoverschrijdende elektriciteitsstromen, met name met betrekking tot entiteiten met zeer belangrijke impact en entiteiten met kritieke impact;

b) in samenwerking met het ENTSB voor elektriciteit en de EU DSB-entiteit, de gemiddelde prijzen van cyberbeveiligingsdiensten, -systemen en -producten die in grote mate bijdragen tot de verbetering en het onderhoud van de maatregelen voor het beheer van cyberbeveiligingsrisico's in de verschillende systeembeheersregio's;

c) het bestaan en de mate van vergelijkbaarheid van de kosten en functies van cyberbeveiligingsdiensten, -systemen en -oplossingen die geschikt zijn voor de uitvoering van deze verordening, waarbij mogelijke maatregelen in kaart worden gebracht om de efficiëntie van de uitgaven te bevorderen, met name als investeringen in cyberbeveiligingstechnologie nodig kunnen zijn.

4. Informatie met betrekking tot benchmarkinganalyses wordt behandeld en verwerkt conform de vereisten inzake gegevensclassificatie van deze verordening, de minimale cyberbeveiligingscontroles en het beoordelingsverslag over grensoverschrijdende cyberbeveiligingsrisico's voor elektriciteit. De in de leden 2 en 3 bedoelde benchmarkanalyse wordt niet openbaar gemaakt.

5. Onverminderd de vertrouwelijkheidsvereisten van artikel 47 en de noodzaak om de veiligheid te beschermen van entiteiten die onder deze verordening vallen, wordt de in de leden 2 en 3 bedoelde benchmarkanalyse gedeeld met alle NRI's, alle bevoegde instanties, ACER, Enisa en de Commissie.

Artikel 14

Overeenkomsten met TSB's van buiten de Unie

1. Binnen 18 maanden na de inwerkingtreding van deze verordening streven de TSB's van een aan een derde land grenzende systeembeheersregio ernaar overeenkomsten te sluiten met TSB's van het aangrenzende derde land die aan het toepasselijke Unierecht voldoen en waarin de basis voor samenwerking op het gebied van de bescherming van cyberbeveiliging en de samenwerkingsregelingen op het gebied van cyberbeveiliging met die TSB's worden vastgelegd.

2. De TSB's stellen de bevoegde instantie in kennis van de overeenkomstig lid 1 gesloten overeenkomsten.

Artikel 15

Wettelijke vertegenwoordigers

1. Entiteiten die geen vestiging in de Unie hebben maar wel diensten verlenen aan entiteiten in de Unie en overeenkomstig artikel 24, lid 6, zijn aangemerkt als entiteiten met zeer belangrijke impact of met kritieke impact, wijzen binnen drie maanden na de kennisgeving schriftelijk een vertegenwoordiger in de Unie aan en stellen de kennisgevende bevoegde instantie daarvan in kennis.

2. Deze vertegenwoordiger wordt gemachtigd om door een bevoegde instantie of een CSIRT in de Unie te worden benaderd, naast of in plaats van de entiteit met zeer belangrijke impact of met kritieke impact ten aanzien van de verplichtingen van de entiteit uit hoofde van deze verordening. De entiteit met zeer belangrijke impact of met kritieke impact verleent haar wettelijke vertegenwoordiger de nodige bevoegdheden en voldoende middelen om een efficiënte en tijdige samenwerking met de relevante bevoegde instanties of CSIRT's te waarborgen.

3. De vertegenwoordiger is gevestigd in een van de lidstaten waar de entiteit haar diensten aanbiedt. Deze entiteit wordt geacht onder de jurisdictie te vallen van de lidstaat waar de vertegenwoordiger is gevestigd. Entiteiten met zeer belangrijke impact of met kritieke impact delen de naam, het postadres, het e-mailadres en het telefoonnummer van hun wettelijke vertegenwoordiger mee aan de bevoegde instantie in de lidstaat waar die wettelijke vertegenwoordiger verblijft of gevestigd is.

4. De aangewezen wettelijke vertegenwoordiger kan aansprakelijk worden gesteld voor de niet-naleving van verplichtingen uit hoofde van deze verordening, onverminderd de aansprakelijkheid van en de gerechtelijke stappen die tegen de entiteiten met zeer belangrijke impact of met kritieke impact kunnen worden ondernomen.

5. Bij ontstentenis van een aangewezen vertegenwoordiger binnen de Unie uit hoofde van dit artikel kan iedere lidstaat waar de entiteit diensten verricht, gerechtelijke stappen ondernemen tegen de entiteit wegens niet-nakoming van de verplichtingen uit hoofde van deze verordening.

6. De aanwijzing van een wettelijke vertegenwoordiger binnen de Unie krachtens lid 1 vormt geen vestiging in de Unie.

Artikel 16

Samenwerking tussen het ENTSB voor elektriciteit en de EU DSB-entiteit

1. Het ENTSB voor elektriciteit en de EU DSB-entiteit werken samen bij het uitvoeren van cyberbeveiligingsrisicobeoordelingen overeenkomstig de artikelen 19 en 21, en met name bij de volgende werkzaamheden:

a) de ontwikkeling van de beoordelingsmethoden voor cyberbeveiligingsrisico's overeenkomstig artikel 18, lid 1;

b) de ontwikkeling van het uitgebreide beoordelingsverslag over grensoverschrijdende cyberbeveiligingsrisico's voor elektriciteit overeenkomstig artikel 23;

c) de ontwikkeling van het gemeenschappelijke cyberbeveiligingskader voor elektriciteit overeenkomstig hoofdstuk III;

d) de ontwikkeling van de aanbeveling voor aanbestedingen op het gebied van cyberbeveiliging overeenkomstig artikel 35;

e) de ontwikkeling van de methode voor een classificatieschema van cyberaanvallen overeenkomstig artikel 37, lid 8,

f) de ontwikkeling van de voorlopige impactindex voor de cyberbeveiliging van elektriciteit ("ECII") overeenkomstig artikel 48, lid 1, punt a);

g) de ontwikkeling van de voorlopige geconsolideerde lijst van entiteiten met zeer belangrijke impact of entiteiten met kritieke impact overeenkomstig artikel 48, lid 3;

h) de ontwikkeling van de voorlopige lijst van Uniebrede processen met zeer belangrijke impact of met kritieke impact overeenkomstig artikel 48, lid 4;

i) de ontwikkeling van de voorlopige lijst van Europese en internationale normen en controles overeenkomstig artikel 48, lid 6;

j) de uitvoering van de Uniebrede cyberbeveiligingsrisicobeoordeling overeenkomstig artikel 19;

k) de uitvoering van de regionale cyberbeveiligingsrisicobeoordeling overeenkomstig artikel 21;

l) de definitie van de regionale plannen ter beperking van cyberbeveiligingsrisico's overeenkomstig artikel 22;

m) de ontwikkeling van richtsnoeren inzake Europese cyberbeveiligingscertificeringsregelingen voor ICT-producten, -diensten en -processen overeenkomstig artikel 36;

n) de ontwikkeling van richtsnoeren voor de uitvoering van deze verordening in overleg met ACER en Enisa.

2. De samenwerking tussen het ENTSB voor elektriciteit en de EU DSB-entiteit kan de vorm aannemen van een werkgroep voor cyberbeveiligingsrisico's.

3. Het ENTSB voor elektriciteit en de EU DSB-entiteit informeren ACER, Enisa, de NIS-samenwerkingsgroep en de Coördinatiegroep voor elektriciteit regelmatig over de voortgang bij de uitvoering van de Uniebrede en regionale cyberbeveiligingsrisicobeoordelingen overeenkomstig de artikelen 19 en 21.

Artikel 17

Samenwerking tussen ACER en de bevoegde instanties

ACER zal, in samenwerking met iedere bevoegde instantie:

1) toezicht houden op de uitvoering van maatregelen voor het beheer van cyberbeveiligingsrisico's overeenkomstig artikel 12, lid 2, punt a), en de rapportageverplichtingen uit hoofde van de artikelen 27 en 39;

2) toezicht houden op het vaststellingsproces en de uitvoering van de voorwaarden, methoden en van de plannen overeenkomstig artikel 6, leden 2 en 3. De samenwerking tussen ACER, Enisa en iedere bevoegde instantie kan de vorm aannemen van een toezichtsorgaan voor cyberbeveiligingsrisico's.

HOOFDSTUK II

RISICOBEOORDELING EN AANDUIDING VAN DE RELEVANTE CYBERBEVEILIGINGSRISICO'S

Artikel 18

Beoordelingsmethoden voor cyberbeveiligingsrisico's

1. Uiterlijk 13 maart 2025 dienen de TSB's, met de hulp van het ENTSB voor elektriciteit, in samenwerking met de EU DSB-entiteit en na overleg met de NIS-samenwerkingsgroep, een voorstel in voor de beoordelingsmethoden voor cyberbeveiligingsrisico's op het niveau van de Unie, op regionaal niveau en op het niveau van de lidstaten.

2. De beoordelingsmethoden voor cyberbeveiligingsrisico's op het niveau van de Unie, op regionaal niveau en op het niveau van de lidstaten omvatten:

a) een lijst van cyberdreigingen die in aanmerking moeten worden genomen, met inbegrip van ten minste de volgende bedreigingen voor de toeleveringsketen:

   i) ernstige en onverwachte verstoringen van de toeleveringsketen;

   ii) de onbeschikbaarheid van ICT-producten, -diensten of -processen van de toeleveringsketen;

iii) door partijen in de toeleveringsketen geïnitieerde cyberaanvallen;

iv) het lekken van gevoelige informatie via de toeleveringsketen, inclusief toeleveringsketenmonitoring;

v) de installatie van kwetsbaarheden of achterdeurtjes in ICT-producten, -diensten of -processen door partijen in de toeleveringsketen;

b) de criteria om de impact van cyberbeveiligingsrisico's als hoog of kritiek te beoordelen aan de hand van vastgestelde drempels voor gevolgen en waarschijnlijkheid;

c) een aanpak voor de analyse van de cyberbeveiligingsrisico's van legacy-systemen, de watervaleffecten van cyberaanvallen en de realtime aard van netbeheersystemen;

d) een aanpak voor de analyse van de cyberbeveiligingsrisico's in verband met de afhankelijkheid van één leverancier van ICT-producten, -diensten of -processen.

3. De beoordelingsmethoden voor cyberbeveiligingsrisico's op het niveau van de Unie, op regionaal niveau en op het niveau van de lidstaten beoordelen de cyberbeveiligingsrisico's aan de hand van dezelfde risicoimpactmatrix. De risicoimpactmatrix:

a) meet de gevolgen van cyberaanvallen aan de hand van de volgende criteria:

i) verlies van belasting;

ii) lagere elektriciteitsopwekking;

iii) capaciteitsverlies in de primaire frequentiereserve;

iv) verlies van capaciteit voor het operationele herstel van een elektriciteitsnet zonder een beroep te doen op het externe transmissienet voor herstel na een volledige of gedeeltelijke stillegging (een z.g. "blackstart");

v) de verwachte duur van een elektriciteitsstoring met gevolgen voor afnemers, in combinatie met de schaal van de niet-beschikbaarheid in aantallen afnemers, en

vi) andere kwantitatieve of kwalitatieve criteria die redelijkerwijs kunnen dienen als indicator voor de impact van een cyberaanval op grensoverschrijdende elektriciteitsstromen;

b) meet de waarschijnlijkheid van een incident als de frequentie van cyberaanvallen per jaar.

4. In de beoordelingsmethoden voor cyberbeveiligingsrisico's op het niveau van de Unie wordt beschreven hoe de ECII-waarden voor drempels voor zeer belangrijke impact of voor kritieke impact zullen worden vastgesteld. Aan de hand van de ECII kunnen entiteiten met behulp van de in lid 2, punt b), bedoelde criteria de gevolgen van de risico's voor hun bedrijfsproces inschatten tijdens bedrijfseffectbeoordelingen die zij overeenkomstig artikel 26, lid 4, punt c), i), uitvoeren.

5. Het ENTSB voor elektriciteit stelt, in overleg met de EU DSB-entiteit, de Coördinatiegroep voor elektriciteit in kennis van de voorstellen voor de beoordelingsmethoden voor cyberbeveiligingsrisico's die overeenkomstig lid 1 worden ontwikkeld.

Artikel 19

Uniebrede cyberbeveiligingsrisicobeoordelingen

1. Binnen negen maanden na de goedkeuring van de beoordelingsmethoden voor cyberbeveiligingsrisico's overeenkomstig artikel 8 en vervolgens om de drie jaar voert het ENTSB voor elektriciteit, in samenwerking met de EU DSB-entiteit en in overleg met de NIS-samenwerkingsgroep, onverminderd artikel 22 van Richtlijn (EU) 2022/2555, een Uniebrede cyberbeveiligingsrisicobeoordeling uit en stelt het een ontwerp van Uniebreed beoordelingsverslag over cyberbeveiligingsrisico's op. Daartoe wordt gebruikgemaakt van de overeenkomstig artikel 18 ontwikkelde en overeenkomstig artikel 8 goedgekeurde methoden om de mogelijke gevolgen van cyberaanvallen die de operationele veiligheid van het elektriciteitssysteem aantasten en grensoverschrijdende elektriciteitsstromen verstoren, in kaart te brengen, te analyseren en te beoordelen. Bij de Uniebrede cyberbeveiligingsrisicobeoordeling wordt de juridische, financiële of reputatieschade van cyberaanvallen niet in aanmerking genomen.

2. Het Uniebrede beoordelingsverslag over cyberbeveiligingsrisico's bevat de volgende elementen:

a) de Uniebrede processen met zeer belangrijke impact en de Uniebrede processen met kritieke impact;

b) een risicoimpactmatrix die entiteiten en de bevoegde instanties moeten gebruiken bij de beoordeling van het cyberbeveiligingsrisico dat is opgemerkt in de cyberbeveiligingsrisicobeoordeling op lidstaatniveau, uitgevoerd overeenkomstig artikel 20, en in de cyberbeveiligingsrisicobeoordeling op entiteitsniveau overeenkomstig artikel 26, lid 2, punt b).

3. Met betrekking tot de Uniebrede processen met zeer belangrijke impact en de Uniebrede processen met kritieke impact bevat het Uniebrede beoordelingsverslag over cyberbeveiligingsrisico's:

a) een beoordeling van de mogelijke gevolgen van een cyberaanval aan de hand van de maatstaven die zijn gedefinieerd in de cyberbeveiligingsrisicobeoordelingmethode die is ontwikkeld overeenkomstig artikel 18, leden 2, 3 en 4, en goedgekeurd op grond van artikel 8;

b) de drempels voor de ECII en de drempels voor zeer belangrijke impact of voor kritieke impact die de bevoegde instanties overeenkomstig artikel 24, leden 1 en 2, gebruiken om entiteiten met zeer belangrijke impact of met kritieke impact aan te merken die betrokken zijn bij Uniebrede processen met zeer belangrijke impact en bij Uniebrede processen met kritieke impact.

4. Het ENTSB voor elektriciteit dient, in samenwerking met de EU DSB-entiteit, het ontwerp van het Uniebrede beoordelingsverslag over cyberbeveiligingsrisico's met de resultaten van de Uniebrede cyberbeveiligingsrisicobeoordeling bij ACER in voor advies. ACER brengt binnen drie maanden na ontvangst van het ontwerpverslag advies uit. Het ENTSB voor elektriciteit en de EU DSB-entiteit houden bij het voltooien van dat verslag zo veel mogelijk rekening met het advies van ACER.

5. Binnen drie maanden na ontvangst van het advies van ACER stelt het ENTSB voor elektriciteit, in samenwerking met de EU DSB-entiteit, ACER, de Commissie, Enisa en de bevoegde instanties in kennis van het definitieve Uniebrede beoordelingsverslag over cyberbeveiligingsrisico's.

Artikel 20

Cyberbeveiligingsrisicobeoordelingen op het niveau van de lidstaten

1. Iedere bevoegde instantie voert een cyberbeveiligingsrisicobeoordeling op lidstaatniveau uit voor alle entiteiten met zeer belangrijke impact of met kritieke impact in haar lidstaat aan de hand van de overeenkomstig artikel 18 ontwikkelde en overeenkomstig artikel 8 goedgekeurde methoden. In de cyberbeveiligingsrisicobeoordeling op lidstaatniveau worden de risico's van cyberaanvallen die de operationele veiligheid van het elektriciteitssysteem aantasten en grensoverschrijdende elektriciteitsstromen verstoren, in kaart gebracht en geanalyseerd. Bij de cyberbeveiligingsrisicobeoordeling op lidstaatniveau wordt de juridische, financiële of reputatieschade van cyberaanvallen niet in aanmerking genomen.

2. Binnen 21 maanden na de kennisgeving van de entiteiten met zeer belangrijke impact of met kritieke impact overeenkomstig artikel 24, lid 6, en vervolgens om de drie jaar, en na raadpleging van de CS-NCA voor elektriciteit, verstrekt iedere bevoegde instantie, ondersteund door het CSIRT, een beoordelingsverslag over cyberbeveiligingsrisico's op lidstaatniveau aan het ENTSB voor elektriciteit en de EU DSB-entiteit, dat per bedrijfsproces met zeer belangrijke impact of met kritieke impact de volgende informatie bevat:

a) de uitvoeringsstatus van de minimale en geavanceerde cyberbeveiligingscontroles overeenkomstig artikel 29;

b) een lijst van alle cyberaanvallen die in de voorgaande drie jaar zijn gemeld overeenkomstig artikel 38, lid 3;

c) een samenvatting van de informatie over cyberdreigingen die in de voorgaande drie jaar zijn gemeld overeenkomstig artikel 38, lid 6;

d) per Uniebreed proces met zeer belangrijke impact of met kritieke impact, een inschatting van de risico's van een inbreuk op de vertrouwelijkheid, de integriteit en de beschikbaarheid van informatie en de relevante activa;

e) indien nodig, een lijst van aanvullende entiteiten die zijn aangemerkt als entiteiten met zeer belangrijke impact of met kritieke impact overeenkomstig artikel 24, leden 1, 2, 3 en 5.

3. In het beoordelingsverslag over cyberbeveiligingsrisico's op lidstaatniveau wordt rekening gehouden met het overeenkomstig artikel 10 van Verordening (EU) 2019/941 opgestelde risicoparaatheidsplan van de lidstaat.

4. De informatie in het beoordelingsverslag over cyberbeveiligingsrisico's op lidstaatniveau overeenkomstig lid 2, punten a) tot en met d), wordt niet gekoppeld aan specifieke entiteiten of activa. Het beoordelingsverslag over cyberbeveiligingsrisico's op lidstaatniveau bevat ook een risicobeoordeling van de tijdelijke afwijkingen die door de bevoegde instanties in de lidstaten zijn verleend overeenkomstig artikel 30.

5. Het ENTSB voor elektriciteit en de EU DSB-entiteit kunnen de bevoegde instanties om aanvullende informatie verzoeken met betrekking tot de in lid 2, punten a) en c), genoemde werkzaamheden.

6. De bevoegde instanties waarborgen dat de door hen verstrekte informatie nauwkeurig en juist is.

Artikel 21

Regionale cyberbeveiligingsrisicobeoordelingen

1. Het ENTSB voor elektriciteit voert, in samenwerking met de EU DSB-entiteit en in overleg met het betrokken regionale coördinatiecentrum, een regionale cyberbeveiligingsrisicobeoordeling uit voor iedere systeembeheersregio aan de hand van de overeenkomstig artikel 19 ontwikkelde en overeenkomstig artikel 8 goedgekeurde methoden, om de risico's van cyberaanvallen die de operationele veiligheid van het elektriciteitssysteem aantasten en grensoverschrijdende elektriciteitsstromen verstoren, in kaart te brengen, te analyseren en te evalueren. Bij de regionale cyberbeveiligingsrisicobeoordelingen wordt de juridische, financiële of reputatieschade van cyberaanvallen niet in aanmerking genomen.

2. Binnen 30 maanden na de kennisgeving van de entiteiten met zeer belangrijke impact of met kritieke impact overeenkomstig artikel 24, lid 6, en vervolgens om de drie jaar, stelt het ENTSB voor elektriciteit, in samenwerking met de EU DSB-entiteit en in overleg met de NIS-samenwerkingsgroep, per systeembeheersregio een regionaal beoordelingsverslag over cyberbeveiligingsrisico's op.

3. In het regionale beoordelingsverslag over cyberbeveiligingsrisico's wordt de relevante informatie in de Uniebrede beoordelingsverslagen over cyberbeveiligingsrisico's en in de beoordelingsverslagen over cyberbeveiligingsrisico's op lidstaatniveau in aanmerking genomen.

4. In het regionale beoordelingsverslag over cyberbeveiligingsrisico's worden de overeenkomstig artikel 6 van Verordening (EU) 2019/941 aangemerkte regionale elektriciteitscrisesscenario's met betrekking tot cyberbeveiliging in aanmerking genomen.

Artikel 22

Regionale plannen ter beperking van cyberbeveiligingsrisico's

1. Binnen 36 maanden na de kennisgeving van de entiteiten met zeer belangrijke impact of met kritieke impact overeenkomstig artikel 24, lid 6, en uiterlijk 13 juni 2031, en vervolgens om de drie jaar, ontwikkelen de TSB's, met de hulp van het ENTSB voor elektriciteit, in samenwerking met de EU DSB-entiteit en in overleg met de regionale coördinatiecentra en de NIS-samenwerkingsgroep, per systeembeheersregio een regionaal plan ter beperking van cyberbeveiligingsrisico's over cyberbeveiligingsrisico's.

2. De regionale plannen ter beperking van cyberbeveiligingsrisico's omvatten;

a) de minimale en geavanceerde cyberbeveiligingscontroles die entiteiten met zeer belangrijke impact of met kritieke impact in de systeembeheersregio moeten toepassen;

b) de resterende cyberbeveiligingsrisico's in de systeembeheersregio's na toepassing van de in punt a) bedoelde controles.

3. Het ENTSB voor elektriciteit dient de regionale plannen ter beperking van risico's in bij de relevante transmissiesysteembeheerders, de bevoegde instanties en de Coördinatiegroep voor elektriciteit. De Coördinatiegroep voor elektriciteit kan wijzigingen aanbevelen.

4. De TSB's actualiseren, met de hulp van het ENTSB voor elektriciteit, in samenwerking met de EU DSB-entiteit en in overleg met de NIS-samenwerkingsgroep, de regionale plannen ter beperking van cyberbeveiligingsrisico's om de drie jaar, tenzij de omstandigheden tot een frequentere actualisering nopen.

Artikel 23

Uitgebreid beoordelingsverslag over grensoverschrijdende cyberbeveiligingsrisico's voor elektriciteit

1. Binnen 40 maanden na de kennisgeving van de entiteiten met zeer belangrijke impact of met kritieke impact overeenkomstig artikel 24, lid 6, en vervolgens om de drie jaar, verstrekken de TSB's, met de hulp van het ENTSB voor elektriciteit, in samenwerking met de EU DSB-entiteit en in overleg met de NIS-samenwerkingsgroep, aan de Coördinatiegroep voor elektriciteit een verslag over het resultaat van de beoordeling van cyberbeveiligingsrisico's met betrekking tot grensoverschrijdende elektriciteitsstromen (het "uitgebreide beoordelingsverslag over grensoverschrijdende cyberbeveiligingsrisico's voor elektriciteit").

2. Het uitgebreide beoordelingsverslag over grensoverschrijdende cyberbeveiligingsrisico's voor elektriciteit wordt gebaseerd op het Uniebrede beoordelingsverslag over cyberbeveiligingsrisico's, de beoordelingsverslagen over cyberbeveiligingsrisico's op lidstaatniveau en de regionale beoordelingsverslagen over cyberbeveiligingsrisico's, en bevat de volgende informatie:

a) de lijst van Uniebrede processen met zeer belangrijke impact of met kritieke impact die zijn aangeduid in het Uniebrede beoordelingsverslag over cyberbeveiligingsrisico's overeenkomstig artikel 19, lid 2, punt a), met inbegrip van de inschatting van de waarschijnlijkheid en de impact van cyberbeveiligingsrisico's die voor de regionale beoordelingsverslagen over cyberbeveiligingsrisico's zijn geëvalueerd overeenkomstig artikel 21, lid 2, en artikel 19, lid 3, punt a);

b) actuele cyberdreigingen, met bijzondere aandacht voor opkomende dreigingen en risico's voor het elektriciteitssysteem;

c) cyberaanvallen voor de vorige periode op Unieniveau met een kritisch overzicht van de gevolgen die dergelijke cyberaanvallen zouden kunnen hebben voor grensoverschrijdende elektriciteitsstromen;

d) een algemene stand van de uitvoering van de cyberbeveiligingsmaatregelen;

e) de stand van de uitvoering van de informatiestromen overeenkomstig de artikelen 37 en 38;

f) een lijst van informatie of specifieke criteria voor de classificatie van informatie overeenkomstig artikel 46;

g) vastgestelde en gesignaleerde risico's die kunnen voortvloeien uit een onveilig beheer van de toeleveringsketen;

h) resultaten en geaccumuleerde ervaringen van overeenkomstig artikel 44 georganiseerde regionale en regio-overschrijdende cyberbeveiligingsoefeningen;

i) een analyse van de ontwikkeling van de algemene grensoverschrijdende cyberbeveiligingsrisico's in de elektriciteitssector sinds de recentste regionale cyberbeveiligingsrisicobeoordelingen;

j) andere informatie die van belang kan zijn om mogelijke verbeteringen van deze verordening of de noodzaak van een herziening van deze verordening of van de instrumenten ervan vast te stellen, en

k) geaggregeerde en geanonimiseerde informatie over afwijkingen overeenkomstig artikel 30, lid 3.

3. De in artikel 2, lid 1, genoemde entiteiten kunnen bijdragen tot de ontwikkeling van het uitgebreide beoordelingsverslag over grensoverschrijdende cyberbeveiligingsrisico's voor elektriciteit, met inachtneming van de vertrouwelijkheid van de informatie overeenkomstig artikel 47. Met de hulp van het ENTSB voor elektriciteit en in samenwerking met de EU DSB-entiteit raadplegen de TSB's deze entiteiten in een vroeg stadium.

4. Op het uitgebreide beoordelingsverslag over grensoverschrijdende cyberbeveiligingsrisico's voor elektriciteit zijn de regels inzake de bescherming van de uitwisseling van informatie van toepassing, overeenkomstig artikel 46. Onverminderd artikel 10, lid 4, en artikel 47, lid 4, publiceren het ENTSB voor elektriciteit en de EU DSB-entiteit een openbare versie van dat verslag, die geen voor de in artikel 2, lid 1, genoemde entiteiten schadelijke informatie bevat. De openbare versie van dit verslag wordt alleen gepubliceerd met de instemming van de NIS-samenwerkingsgroep en de Coördinatiegroep voor elektriciteit. Het ENTSB voor elektriciteit is, in overleg met de EU DSB-entiteit, verantwoordelijk voor het opstellen en publiceren van de openbare versie van het verslag.

Artikel 24

Aanmerking van entiteiten met zeer belangrijke impact of met kritieke impact

1. Iedere bevoegde instantie stelt, aan de hand van de ECII en de drempels voor zeer belangrijke impact of voor kritieke impact in het Uniebrede beoordelingsverslag over cyberbeveiligingsrisico's overeenkomstig artikel 19, lid 3, punt b), vast welke entiteiten met zeer belangrijke impact of met kritieke impact in haar lidstaat betrokken zijn bij de Uniebrede processen met zeer belangrijke impact of met kritieke impact. De bevoegde instanties kunnen een entiteit in hun lidstaat om informatie verzoeken om de ECII-waarden voor die entiteit te bepalen. Indien de vastgestelde ECII van een entiteit boven de drempel voor zeer belangrijke impact of voor kritieke impact ligt, wordt de aangemerkte entiteit vermeld in het in artikel 20, lid 2, bedoelde beoordelingsverslag over cyberbeveiligingsrisico's op lidstaatniveau.

2. Iedere bevoegde instantie stelt, aan de hand van de ECII en de drempels voor zeer belangrijke impact of voor kritieke impact in het Uniebrede beoordelingsverslag over cyberbeveiligingsrisico's overeenkomstig artikel 19, lid 3, punt b), vast welke entiteiten met zeer belangrijke impact of met kritieke impact, voor zover zij in de Unie actief zijn, niet in de Unie gevestigd zijn. De bevoegde instantie kan een niet in de Unie gevestigde entiteit om informatie verzoeken om de ECII-waarden voor die entiteit te bepalen.

3. Iedere bevoegde instantie kan aanvullende entiteiten in haar lidstaat aanmerken als entiteiten met zeer belangrijke impact of met kritieke impact indien aan de volgende criteria is voldaan:

a) de entiteit maakt deel uit van een groep entiteiten waarvoor een aanzienlijk risico bestaat dat zij tegelijkertijd door een cyberaanval worden getroffen;

b) de geaggregeerde ECII voor de groep entiteiten ligt boven de drempel voor zeer belangrijke impact of voor kritieke impact.

4. Indien een bevoegde instantie overeenkomstig lid 3 aanvullende entiteiten aanmerkt, worden alle processen bij deze entiteiten waarvoor de voor de groep geaggregeerde ECII boven de drempel voor zeer belangrijke impact ligt, beschouwd als processen met zeer belangrijke impact, en worden alle processen bij deze entiteiten waarvoor de voor de groep geaggregeerde ECII de drempels voor kritieke impact overschrijden, beschouwd als processen met kritieke impact.

5. Indien een bevoegde instantie in meer dan één lidstaat entiteiten als bedoeld in lid 3, punt a), aanmerkt, stelt zij de andere bevoegde instanties, het ENTSB voor elektriciteit en de EU DSB-entiteit daarvan in kennis. Het ENTSB voor elektriciteit verstrekt, in samenwerking met de EU DSB-entiteit, op basis van de van alle bevoegde instanties ontvangen informatie, aan de bevoegde instanties een analyse van de aggregatie van entiteiten in meer dan één lidstaat die een gedistribueerde verstoring van de grensoverschrijdende elektriciteitsstromen kan veroorzaken en tot een cyberaanval kan leiden. Indien een groep entiteiten in verscheidene lidstaten wordt aangemerkt als een aggregatie waarvan de ECII hoger is dan de drempel voor zeer belangrijke impact of met kritieke impact, merken alle betrokken bevoegde instanties de entiteiten in die groep aan als entiteiten met zeer belangrijke impact of voor kritieke impact voor hun respectieve lidstaat, op basis van de geaggregeerde ECII voor de groep entiteiten, en worden de aangemerkte entiteiten in het Uniebrede beoordelingsverslag over cyberbeveiligingsrisico's opgenomen.

6. Binnen negen maanden nadat zij door het ENTSB voor elektriciteit en de EU DSB-entiteit in kennis zijn gesteld van het Uniebrede beoordelingsverslag over cyberbeveiligingsrisico's overeenkomstig artikel 19, lid 5, en in ieder geval uiterlijk 13 juni 2028, stelt iedere bevoegde instantie de entiteiten op de lijst ervan in kennis dat zij in haar lidstaat zijn aangemerkt als entiteit met zeer belangrijke impact of entiteit met kritieke impact.

7. Indien een dienstverlener bij een bevoegde instantie wordt aangemeld als aanbieder van kritieke ICT-diensten overeenkomstig artikel 27, punt c), stelt die bevoegde instantie de bevoegde instanties van de lidstaten op wier grondgebied diens zetel of vertegenwoordiger is gevestigd, daarvan in kennis. De laatstgenoemde bevoegde instantie stelt de dienstverlener ervan in kennis dat hij als aanbieder van kritieke diensten is aangemerkt.

Artikel 25

Nationale verificatieregelingen

1. De bevoegde instanties kunnen een nationale verificatieregeling opzetten om na te gaan of de overeenkomstig artikel 24, lid 1, aangemerkte entiteiten met kritieke impact uitvoering hebben gegeven aan het nationale wetgevingskader, zoals opgenomen in de verwijzingsmatrix in de zin van artikel 34. De nationale verificatieregeling kan gebaseerd zijn op een inspectie door de bevoegde instantie, op onafhankelijke veiligheidsaudits of op wederzijdse collegiale toetsingen door entiteiten met kritieke impact in dezelfde lidstaat onder toezicht van de bevoegde instantie.

2. Indien een bevoegde instantie besluit een nationaal verificatiesysteem op te zetten, zorgt die bevoegde instantie ervoor dat de verificatie wordt uitgevoerd aan de hand van de volgende vereisten:

a) partijen die de collegiale toetsing, audit of inspectie uitvoeren, moeten onafhankelijk zijn van de te verifiëren entiteit met kritieke impact en mogen geen belangenconflicten hebben;

b) het personeel dat de collegiale toetsing, audit of inspectie uitvoert, moet aantoonbare kennis hebben van:

   i) cyberbeveiliging in de elektriciteitssector;

   ii) cyberbeveiligingsbeheersystemen;

   iii) auditbeginselen;

   iv) cyberbeveiligingsrisicobeoordelingen;

   v) het gemeenschappelijke cyberbeveiligingskader voor elektriciteit;

   vi) het nationale wet- en regelgevingskader en de voor de verificatie relevante Europese en internationale normen;

   vii) de voor de verificatie relevante processen met kritieke impact;

c) de partij die de collegiale toetsing, audit of inspectie uitvoert, moet voldoende tijd krijgen om die activiteiten uit te voeren;

d) de partij die de collegiale toetsing, audit of inspectie uitvoert, moet passende maatregelen treffen om de tijdens de verificatie verzamelde informatie te beschermen conform het vertrouwelijkheidsniveau ervan, en

e) collegiale toetsingen, audits of inspecties moeten ten minste eenmaal per jaar worden uitgevoerd en ten minste om de drie jaar de volledige reikwijdte van de verificatie omvatten.

3. Indien een bevoegde instantie besluit een nationale verificatieregeling op te zetten, brengt zij jaarlijks verslag uit aan ACER over de frequentie waarmee zij inspecties in het kader van die regeling heeft uitgevoerd.

Artikel 26

Beheer van cyberbeveiligingsrisico's op entiteitsniveau

1. Iedere door de bevoegde instanties overeenkomstig artikel 24, lid 1, aangemerkte entiteit met zeer belangrijke impact of met kritieke impact voert cyberbeveiligingsrisicobeheer uit voor al haar activa in haar perimeter van zeer belangrijke impact of van kritieke impact. Iedere entiteit met zeer belangrijke impact of met kritieke impact voert om de drie jaar risicobeheer uit dat de fasen van lid 2 omvat.

2. Iedere entiteit met zeer belangrijke impact of met kritieke impact baseert haar cyberbeveiligingsrisicobeheer op een aanpak die gericht is op de bescherming van haar netwerk- en informatiesystemen en de volgende fasen omvat:

a) contextbepaling;

b) cyberbeveiligingsrisicobeoordelingen op entiteitsniveau;

c) behandeling van cyberbeveiligingsrisico's;

d) aanvaarding van cyberbeveiligingsrisico's.

3. Tijdens de contextbepalingsfase moet iedere entiteit met zeer belangrijke impact of met kritieke impact:

a) het toepassingsgebied van de cyberbeveiligingsrisicobeoordeling definiëren, met inbegrip van de door het ENTSB voor elektriciteit en de EU DSB-entiteit aangemerkte processen met zeer belangrijke impact of met kritieke impact, en andere processen die het doelwit kunnen zijn van cyberaanvallen met zeer belangrijke impact of met kritieke impact voor grensoverschrijdende elektriciteitsstromen, en

b) de criteria voor de evaluatie en de aanvaarding van risico's vaststellen overeenkomstig de risicoimpactmatrix die entiteiten en bevoegde instanties gebruiken om de cyberbeveiligingsrisico's te beoordelen volgens de door het ENTSB voor elektriciteit en de EU DSB-entiteit overeenkomstig artikel 19, lid 2, ontwikkelde beoordelingsmethoden voor cyberbeveiligingsrisico's op het niveau van de Unie, op regionaal niveau en op lidstaatniveau.

4. Tijdens de cyberbeveiligingsrisicobeoordelingsfase moet iedere entiteit met zeer belangrijke impact of met kritieke impact:

a) cyberbeveiligingsrisico's in beeld brengen door rekening te houden met:

i) alle activa die de Uniebrede processen met zeer belangrijke impact of met kritieke impact ondersteunen, met een beoordeling van de mogelijke gevolgen voor grensoverschrijdende elektriciteitsstromen indien de activa in gevaar komen;

ii) mogelijke cyberdreigingen, met inachtneming van de cyberdreigingen die zijn vastgesteld in het recentste in artikel 23 bedoelde uitgebreide beoordelingsverslag over grensoverschrijdende cyberbeveiligingsrisico's voor elektriciteit en dreigingen in de toeleveringsketen;

iii) kwetsbaarheden, met inbegrip van kwetsbaarheden in legacy-systemen;

iv) mogelijke scenario's voor cyberaanvallen, waaronder cyberaanvallen die de operationele veiligheid van het elektriciteitssysteem aantasten en grensoverschrijdende elektriciteitsstromen verstoren;

v) relevante risico-evaluaties en -beoordelingen op het niveau van de Unie, met inbegrip van gecoördineerde risicobeoordelingen van kritieke toeleveringsketens overeenkomstig artikel 22 van Richtlijn (EU) 2022/2555, en

vi) bestaande uitgevoerde controles;

b) de waarschijnlijkheid en de gevolgen van de in punt a) aangemerkte cyberbeveiligingsrisico's analyseren en het cyberbeveiligingsrisiconiveau bepalen aan de hand van de risicoimpactmatrix die is gebruikt ter beoordeling van de cyberbeveiligingsrisico's volgens de door de TSB's, met de hulp van het ENTSB voor elektriciteit en in samenwerking met de EU DSB-entiteit overeenkomstig artikel 19, lid 2, ontwikkelde beoordelingsmethoden voor cyberbeveiligingsrisico's op het niveau van de Unie, op regionaal niveau en op lidstaatniveau;

c) activa classificeren op basis van de mogelijke gevolgen als de cyberbeveiliging in gevaar komt, en de perimeter van zeer belangrijke impact of van kritieke impact bepalen aan de hand van de volgende stappen:

i) voor alle onder de cyberbeveiligingsrisicobeoordeling vallende processen een bedrijfseffectbeoordeling uitvoeren aan de hand van de ECII;

ii) een proces als proces met zeer belangrijke impact of met kritieke impact classificeren als de ECII boven de drempel voor zeer belangrijke impact respectievelijk kritieke impact ligt;

iii) bepalen welke activa met zeer belangrijke impact of met kritieke impact nodig zijn als activa voor processen met zeer belangrijke impact respectievelijk kritieke impact;

iv) de perimeters van zeer belangrijke impact of van kritieke impact definiëren die alle activa met zeer belangrijke impact respectievelijk kritieke impact bevatten, zodat de toegang tot die perimeters kan worden gecontroleerd;

d) cyberbeveiligingsrisico's evalueren door ze te rangschikken aan de hand van risicobeoordelingscriteria en risicoaanvaardingscriteria als bedoeld in lid 3, punt b).

5. Tijdens de fase van de behandeling van cyberbeveiligingsrisico's stelt iedere entiteit met zeer belangrijke impact of met kritieke impact een risicobeperkingsplan op entiteitsniveau op door de risicobehandelingsopties te selecteren die geschikt zijn om de risico's te beheren en de resterende risico's vast te stellen.

6. Tijdens de fase van de aanvaarding van cyberbeveiligingsrisico's beslist iedere entiteit met zeer belangrijke impact of met kritieke impact of zij het resterende risico aanvaardt op basis van de in lid 3, punt b), vastgestelde risicoaanvaardingscriteria.

7. Iedere entiteit met zeer belangrijke impact of met kritieke impact registreert de in lid 1 in kaart gebrachte activa in een activa-inventaris. Die activa-inventaris maakt geen deel uit van het risicobeoordelingsverslag.

8. De bevoegde instantie kan de in die inventaris opgenomen activa tijdens inspecties onderzoeken.

Artikel 27

Rapportage over risicobeoordelingen op entiteitsniveau

Iedere entiteit met zeer belangrijke impact of met kritieke impact verstrekt de bevoegde instanties binnen twaalf maanden na de kennisgeving van de entiteiten met zeer belangrijke impact of met kritieke impact overeenkomstig artikel 24, lid 6, en vervolgens om de drie jaar, een verslag met de volgende informatie:

1) een lijst van controles die zijn geselecteerd voor het risicobeperkingsplan op entiteitsniveau overeenkomstig artikel 26, lid 5, met de huidige uitvoeringsstatus per controle;

2) per Uniebreed proces met zeer belangrijke impact of met kritieke impact, een inschatting van het risico van een inbreuk op de vertrouwelijkheid, de integriteit en de beschikbaarheid van informatie en de relevante activa. De inschatting van dit risico vindt plaats aan de hand van de in artikel 19, lid 2, bedoelde risicoimpactmatrix;

3) een lijst van aanbieders van kritieke ICT-diensten voor hun processen met kritieke impact.

HOOFDSTUK III

GEMEENSCHAPPELIJK CYBERBEVEILIGINGSKADER VOOR ELEKTRICITEIT

Artikel 28

Samenstelling, werking en evaluatie van het gemeenschappelijke cyberbeveiligingskader voor elektriciteit

1. Het gemeenschappelijke cyberbeveiligingskader voor elektriciteit bestaat uit de volgende controles en het volgende cyberbeveiligingsbeheersysteem:

a) de minimale cyberbeveiligingscontroles, ontwikkeld overeenkomstig artikel 29;

b) de geavanceerde cyberbeveiligingscontroles, ontwikkeld overeenkomstig artikel 29;

c) de verwijzingsmatrix, ontwikkeld overeenkomstig artikel 34, waarmee de in de punten a) en b) bedoelde controles worden afgezet tegen geselecteerde Europese en internationale normen en nationale wet- of regelgevingskaders;

d) het cyberbeveiligingsbeheersysteem, opgezet overeenkomstig artikel 32.

2. Alle entiteiten met zeer belangrijke impact passen de minimale cyberbeveiligingscontroles krachtens lid 1, punt a), toe binnen hun perimeters van zeer belangrijke impact.

3. Alle entiteiten met kritieke impact passen de geavanceerde cyberbeveiligingscontroles krachtens lid 1, punt b), toe binnen hun perimeters van kritieke impact.

4. Binnen zeven maanden na de indiening van het eerste ontwerp van Uniebreed beoordelingsverslag over cyberbeveiligingsrisico's overeenkomstig artikel 19, lid 4, wordt het in lid 1 bedoelde gemeenschappelijke cyberbeveiligingskader voor elektriciteit aangevuld met de overeenkomstig artikel 33 ontwikkelde minimale en geavanceerde cyberbeveiligingscontroles in de toeleveringsketen.

Artikel 29

Minimale en geavanceerde cyberbeveiligingscontroles

1. Binnen zeven maanden na de indiening van het eerste ontwerp van Uniebreed risicobeoordelingsverslag inzake cyberbeveiliging overeenkomstig artikel 19, lid 4, ontwikkelen de TSB's, met de hulp van het ENTSB voor elektriciteit en in samenwerking met de EU DSB-entiteit, een voorstel voor minimale en geavanceerde cyberbeveiligingscontroles.

2. Binnen zes maanden na de opstelling van een regionaal risicobeoordelingsverslag inzake cyberbeveiliging overeenkomstig artikel 21, lid 2, stellen de TSB's, met de hulp van het ENTSB voor elektriciteit en in samenwerking met de EU DSB-entiteit, aan de bevoegde instantie een wijziging van de minimale en geavanceerde cyberbeveiligingscontroles voor. Het voorstel wordt gedaan overeenkomstig artikel 8, lid 10, en neemt de in de regionale risicobeoordeling aangeduide risico's in aanmerking.

3. De minimale en geavanceerde cyberbeveiligingscontroles zijn verifieerbaar door middel van deelname aan een nationale verificatieregeling overeenkomstig de procedure van artikel 31, of door middel van door een derde overeenkomstig artikel 25, lid 2, uitgevoerde onafhankelijke veiligheidsaudits.

4. De overeenkomstig lid 1 ontwikkelde initiële minimale en geavanceerde cyberbeveiligingscontroles zijn gebaseerd op de risico's die zijn vastgesteld in het in artikel 19, lid 5, bedoelde Uniebrede risicobeoordelingsverslag inzake cyberbeveiliging. De overeenkomstig lid 2 ontwikkelde gewijzigde minimale en geavanceerde cyberbeveiligingscontroles zijn gebaseerd op het in artikel 21, lid 2, bedoelde regionale risicobeoordelingsverslag inzake cyberbeveiliging.

5. De minimale cyberbeveiligingscontroles omvatten controles om uitgewisselde informatie te beschermen overeenkomstig artikel 46.

6. Binnen twaalf maanden na de goedkeuring van de minimale en geavanceerde cyberbeveiligingscontroles overeenkomstig artikel 8, lid 5, en na een actualisering overeenkomstig artikel 8, lid 10, passen de entiteiten die in artikel 2, lid 1, zijn genoemd en die overeenkomstig artikel 24 als entiteiten met zeer belangrijke impact of entiteit met kritieke impact zijn aangemerkt, tijdens de opstelling van het risicobeperkingsplan op entiteitsniveau overeenkomstig artikel 26, lid 5, de minimale cyberbeveiligingscontroles binnen de perimeter van zeer belangrijke impact, en de geavanceerde cyberbeveiligingscontroles binnen de perimeter van kritieke impact toe.

Artikel 30

Afwijkingen van de minimale en geavanceerde cyberbeveiligingscontroles

1. De in artikel 2, lid 1, genoemde entiteiten kunnen de respectieve bevoegde instantie verzoeken een afwijking toe te kennen van de verplichting om de in artikel 29, lid 6, bedoelde minimale en geavanceerde cyberbeveiligingscontroles toe te passen. De bevoegde instantie kan een zodanige afwijking toestaan op een van de volgende gronden:

a) in uitzonderlijke omstandigheden, indien de entiteit kan aantonen dat de kosten van de uitvoering van de passende cyberbeveiligingscontroles aanzienlijk hoger zijn dan de voordelen. Om de entiteiten te helpen kunnen ACER en het ENTSB voor elektriciteit in samenwerking met de EU DSB-entiteit gezamenlijk richtsnoeren ontwikkelen voor het ramen van de kosten van cyberbeveiligingscontroles;

b) indien de entiteit een risicobehandelingsplan op entiteitsniveau verstrekt dat de cyberbeveiligingsrisico's door middel van alternatieve controles beperkt tot een niveau dat aanvaardbaar is overeenkomstig de in artikel 26, lid 3, punt b), genoemde risicoaanvaardingscriteria.

2. Binnen drie maanden na ontvangst van het in lid 1 bedoelde verzoek besluit de bevoegde instantie of een afwijking van de minimale en geavanceerde cyberbeveiligingscontroles wordt toegekend. Afwijkingen van de minimale of geavanceerde cyberbeveiligingscontroles worden toegekend voor maximaal drie jaar, met de mogelijkheid van verlenging.

3. Geaggregeerde en geanonimiseerde informatie voor de toegekende afwijkingen wordt opgenomen als bijlage bij het in artikel 23 bedoelde uitgebreide beoordelingsverslag over grensoverschrijdende cyberbeveiligingsrisico's voor elektriciteit. Het ENTSB voor elektriciteit en de EU DSB-entiteit werken de lijst, indien nodig, gezamenlijk bij.

Artikel 31

Verificatie van het gemeenschappelijke cyberbeveiligingskader voor elektriciteit

1. Uiterlijk 24 maanden na de vaststelling van de in artikel 28, lid 1, punten a), b) en c), bedoelde controles en het opzetten van het in punt d) van dat artikel bedoelde cyberbeveiligingsbeheersysteem kan iedere overeenkomstig artikel 24, lid 1, aangemerkte entiteit met kritieke impact op verzoek van de bevoegde instantie aantonen dat zij het cyberbeveiligingsbeheersysteem en de minimale of geavanceerde cyberbeveiligingscontroles in acht neemt.

2. Iedere entiteit met kritieke impact voldoet aan de in lid 1 bedoelde verplichting door middel van door een derde uitgevoerde onafhankelijke veiligheidsaudits overeenkomstig artikel 25, lid 2, of door middel van deelname aan een nationale verificatieregeling overeenkomstig artikel 25, lid 1.

3. Het verifiëren of een entiteit met kritieke impact het cyberbeveiligingsbeheersysteem en de minimale of geavanceerde cyberbeveiligingscontroles in acht neemt, omvat alle activa binnen de perimeter van kritieke impact van de entiteit met kritieke impact.

4. Het verifiëren of een entiteit met kritieke impact het cyberbeveiligingsbeheersysteem en de minimale of geavanceerde cyberbeveiligingscontroles in acht neemt, wordt regelmatig herhaald, uiterlijk 36 maanden na het einde van de eerste verificatie, en vervolgens om de drie jaar.

5. Iedere overeenkomstig artikel 24 bedoelde entiteit met kritieke impact toont aan dat zij de in artikel 28, lid 1, punten a), b) en c), bedoelde controles en het opzetten van het in punt d) van dat lid bedoelde cyberbeveiligingsbeheersysteem naleeft, door middel van een verslag aan de bevoegde instantie over het resultaat van de nalevingsverificatie.

Artikel 32

Cyberbeveiligingsbeheersysteem

1. Binnen 24 maanden nadat een entiteit door de bevoegde instantie ervan in kennis is gesteld dat zij overeenkomstig artikel 24, lid 6, als entiteit met zeer belangrijke impact of met kritieke impact is aangemerkt, zet iedere entiteit met zeer belangrijke impact of met kritieke impact een cyberbeveiligingsbeheersysteem op en evalueert dat vervolgens om de drie jaar, om:

a) het toepassingsgebied van het cyberbeveiligingsbeheersysteem te bepalen, met inachtneming van de interfaces met en afhankelijkheden van andere entiteiten;

b) te waarborgen dat het gehele hogere management op de hoogte is van de toepasselijke wettelijke verplichtingen en door middel van tijdige besluiten en snelle reacties actief bijdraagt tot de implementatie van het cyberbeveiligingsbeheersysteem;

c) te waarborgen dat de middelen die noodzakelijk zijn voor het cyberbeveiligingsbeheersysteem beschikbaar zijn;

d) een cyberbeveiligingsbeleid vast te stellen dat wordt gedocumenteerd en meegedeeld binnen de entiteit en aan partijen die door de beveiligingsrisico's worden getroffen;

e) verantwoordelijkheden toe te wijzen en mee te delen voor rollen die voor cyberbeveiliging van belang zijn;

f) cyberbeveiligingsrisicobeheer op entiteitsniveau uit te voeren in de zin van artikel 26;

g) de middelen vast te stellen en te leveren die nodig zijn voor de implementatie, het onderhoud en de voortdurende verbetering van het cyberbeveiligingsbeheersysteem, met inachtneming van de benodigde competentie in en kennis van cyberbeveiligingsmiddelen;

h) te bepalen welke interne en externe communicatie relevant is voor cyberbeveiliging;

i) gedocumenteerde informatie met betrekking tot het cyberbeveiligingsbeheersysteem te creëren, bij te werken en te controleren;

j) de prestaties en de doeltreffendheid van het cyberbeveiligingsbeheersysteem te evalueren;

k) met geplande tussenpozen interne audits uit te voeren om te waarborgen dat het cyberbeveiligingsbeheersysteem doeltreffend wordt geïmplementeerd en onderhouden;

l) de implementatie van het cyberbeveiligingsbeheersysteem op gezette tijden te evalueren, en te controleren of, en te corrigeren indien middelen en activiteiten niet conform het beleid, de procedures en de richtsnoeren van het cyberbeveiligingsbeheersysteem zijn.

2. Het toepassingsgebied van het cyberbeveiligingsbeheersysteem omvat alle activa binnen de perimeter van zeer belangrijke impact of van kritieke impact van de entiteit met zeer belangrijke impact of met kritieke impact.

3. Zonder een bepaald type technologie op te leggen of te bevoordelen, moedigen de bevoegde instanties het gebruik aan van Europese of internationale normen en specificaties met betrekking tot beheersystemen en die van belang zijn voor de beveiliging van netwerk- en informatiesystemen.

Artikel 33

Minimale en geavanceerde cyberbeveiligingscontroles in de toeleveringsketen

1. Binnen zeven maanden na de indiening van het eerste ontwerp van Uniebreed beoordelingsverslag over cyberbeveiligingsrisico's overeenkomstig artikel 19, lid 4, ontwikkelen de TSB's, met de hulp van het ENTSB voor elektriciteit en in samenwerking met de EU DSB-entiteit, een voorstel voor minimale en geavanceerde cyberbeveiligingscontroles in de toeleveringsketen die de in het Uniebrede beoordelingsverslag over cyberbeveiligingsrisico's aangemerkte risico's in de toeleveringsketen mitigeren, ter aanvulling van de overeenkomstig artikel 29 ontwikkelde minimale en geavanceerde cyberbeveiligingscontroles. De minimale en geavanceerde cyberbeveiligingscontroles in de toeleveringsketen worden samen met de minimale en geavanceerde cyberbeveiligingscontroles overeenkomstig artikel 29 ontwikkeld. De minimale en geavanceerde cyberbeveiligingscontroles in de toeleveringsketen hebben betrekking op de gehele levenscyclus van alle ICT-producten, -diensten en -processen binnen de perimeter van zeer belangrijke impact of van kritieke impact van een entiteit met zeer belangrijke impact of met kritieke impact. De NIS-samenwerkingsgroep wordt geraadpleegd bij de ontwikkeling van het voorstel voor minimale en geavanceerde cyberbeveiligingscontroles in de toeleveringsketen.

2. De minimale cyberbeveiligingscontroles in de toeleveringsketen bestaan uit controles voor entiteiten met zeer belangrijke impact of met kritieke impact die:

a) aanbevelingen bevatten voor de aanschaf van ICT-producten, -diensten en -processen betreffende cyberbeveiligingsspecificaties, die ten minste betrekking hebben op:

   i) het antecedentenonderzoek van het personeel van de leverancier dat betrokken is bij de toeleveringsketen en te maken heeft met gevoelige informatie of toegang heeft tot de activa met zeer belangrijke of kritieke impact van de entiteit. Antecedentenonderzoeken kunnen een controle van de identiteit en de achtergrond van het personeel of de contractanten van een entiteit omvatten overeenkomstig het nationale recht en de nationale procedures en het toepasselijke Unierecht, met inbegrip van Verordening (EU) 2016/679 en Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad ([18]). Antecedentenonderzoeken zijn evenredig en strikt beperkt tot wat noodzakelijk is. Zij worden uitsluitend uitgevoerd om een mogelijk veiligheidsrisico voor de betrokken entiteit te beoordelen. Zij moeten in verhouding staan tot de bedrijfsvereisten, de classificatie van de informatie waartoe toegang moet worden verkregen en de gepercipieerde risico's, en kunnen worden uitgevoerd door de entiteit zelf, door een externe onderneming die een screening uitvoert of door middel van een onderzoek door de overheid;

   ii) de processen voor een veilig en gecontroleerd ontwerp, en een veilige en gecontroleerde ontwikkeling en productie van ICT-producten, -diensten en -processen, ter bevordering van het ontwerp en de ontwikkeling van ICT-producten, -diensten en -processen, met inbegrip van passende technische cyberbeveiligingsmaatregelen;

   iii) het ontwerp van netwerk- en informatiesystemen waarin apparaten niet worden vertrouwd, zelfs als zij zich binnen een veilige perimeter bevinden, de verificatie van alle ontvangen verzoeken vereisen en het principe van het minste voorrecht toepassen;

   iv) de toegang van de leverancier tot de activa van de entiteit;

([18]) Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (PB L 119 van 4.5.2016, blz. 89).

v) de contractuele verplichtingen van de leverancier om de toegang tot gevoelige informatie van de entiteit te beschermen en te beperken;

vi) de onderliggende aanbestedingsspecificaties voor cyberbeveiliging voor onderaannemers van de leverancier;

vii) de traceerbaarheid van de toepassing van de cyberbeveiligingsspecificaties vanaf de ontwikkeling via productie tot de levering van ICT-producten, -diensten of -processen;

viii) de ondersteuning van beveiligingsupdates gedurende de gehele levensduur van ICT-producten, -diensten of -processen;

ix) het recht om de cyberbeveiliging in de ontwerp-, ontwikkelings- en productieprocessen van de leverancier te controleren;

x) een beoordeling van het risicoprofiel van de leverancier;

b) van dergelijke entiteiten verlangen dat zij rekening houden met de in punt a) bedoelde aanbestedingsaanbevelingen bij het sluiten van overeenkomsten met leveranciers, samenwerkingspartners en andere partijen in de toeleveringsketen, met betrekking tot gewone leveringen van ICT-producten, -diensten en -processen, alsmede met onvoorziene gebeurtenissen en omstandigheden zoals beëindiging en overgang van de overeenkomst in geval van nalatigheid van de contractpartner;

c) van dergelijke entiteiten verlangen dat zij rekening houden met de resultaten van overeenkomstig artikel 22, lid 1, van Richtlijn (EU) 2022/2555 uitgevoerde relevante gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens;

d) criteria bevatten voor het selecteren en contracteren van leveranciers die aan de in punt a) vermelde cyberbeveiligingsspecificaties kunnen voldoen en een cyberbeveiligingsniveau hebben dat passend is voor de cyberbeveiligingsrisico's van de door de leverancier geleverde ICT-producten, -diensten of -processen;

e) criteria omvatten om de leveringsbronnen voor ICT-producten, -diensten en -processen te diversifiëren en het risico van afhankelijkheid van één leverancier te verminderen;

f) criteria omvatten om de cyberbeveiligingsspecificaties voor de interne operationele processen van leveranciers tijdens de gehele levenscyclus per ICT-product, -dienst en -proces regelmatig te monitoren, te evalueren of te controleren.

3. Voor de cyberbeveiligingsspecificaties in de in lid 2, punt a), bedoelde aanbeveling voor aanbestedingen op het gebied van cyberbeveiliging gebruiken entiteiten met zeer belangrijke impact of met kritieke impact overeenkomstig artikel 35, lid 4, de aanbestedingsbeginselen conform Richtlijn 2014/24/EU van het Europees Parlement en de Raad ([19]), of stellen zij hun eigen specificaties vast op basis van de resultaten van de cyberbeveiligingsrisicobeoordeling op entiteitsniveau.

4. De geavanceerde cyberbeveiligingscontroles in de toeleveringsketen omvatten controles voor entiteiten met kritieke impact om tijdens aanbestedingen na te gaan of ICT-producten, -diensten en -processen die als activa met kritieke impact zullen dienstdoen, aan de cyberbeveiligingsspecificaties voldoen. Het ICT-product, de ICT-dienst of het ICT-proces wordt geverifieerd door middel van een in artikel 31 bedoelde Europese cyberbeveiligingscertificeringsregeling of door middel van door de entiteit geselecteerde en georganiseerde verificatieactiviteiten. De omvang en de dekking van de verificatieactiviteiten moet voldoende zijn om de zekerheid te bieden dat het ICT-product, de ICT-dienst of het ICT-proces kan worden gebruikt om de bij de risicobeoordeling op entiteitsniveau vastgestelde risico's te mitigeren. De entiteit met kritieke impact documenteert de stappen ter beperking van de vastgestelde risico's.

5. De minimale en geavanceerde cyberbeveiligingscontroles in de toeleveringsketen zijn van toepassing op de aanschaf van relevante ICT-producten, -diensten en -processen. De minimale en geavanceerde cyberbeveiligingscontroles in de toeleveringsketen zijn van toepassing op aanbestedingsprocedures in de entiteiten die overeenkomstig artikel 24 als entiteiten met zeer belangrijke impact of met kritieke impact zijn aangemerkt, vanaf zes maanden na de vaststelling of de actualisering van de in artikel 29 bedoelde minimale en geavanceerde cyberbeveiligingscontroles.

([19]) Richtlijn 2014/24/EU van het Europees Parlement en de Raad van 26 februari 2014 betreffende het plaatsen van overheidsopdrachten en tot intrekking van Richtlijn 2004/18/EG (PB L 94 van 28.3.2014, blz. 65).

6. Binnen zes maanden na de opstelling van een regionaal risicobeoordelingsverslag inzake cyberbeveiliging overeenkomstig artikel 21, lid 2, stellen de TSB's, met de hulp van het ENTSB voor elektriciteit en in samenwerking met de EU DSB-entiteit, aan de bevoegde instantie een wijziging van de minimale en geavanceerde cyberbeveiligingscontroles in de toeleveringsketen voor. Het voorstel wordt gedaan overeenkomstig artikel 8, lid 10, en neemt de in de regionale risicobeoordeling aangeduide risico's in aanmerking.

Artikel 34

Verwijzingsmatrix voor cyberbeveiligingscontroles voor elektriciteit tegenover de normen

1. Binnen zeven maanden na de indiening van het eerste ontwerp van Uniebreed beoordelingsverslag over cyberbeveiligingsrisico's overeenkomstig artikel 19, lid 4, ontwikkelen de TSB's, met de hulp van het ENTSB voor elektriciteit, in samenwerking met de EU DSB-entiteit en in overleg met Enisa, een voorstel voor een matrix om de in artikel 28, lid 1, punten a) en b), bedoelde controles af te zetten tegen geselecteerde Europese en internationale normen en tegen relevante technische specificaties ("de verwijzingsmatrix"). Het ENTSB voor elektriciteit en de EU DSB-entiteit documenteren de mate van gelijkwaardigheid van de verschillende controles aan de hand van de in artikel 28, lid 1, punten a) en b), omschreven controles.

2. De bevoegde instanties kunnen voor het ENTSB voor elektriciteit en de EU DSB-entiteit de in artikel 28, lid 1, punten a) en b), bedoelde controles afzetten tegen de desbetreffende nationale wet- of regelgevingskaders, met inbegrip van de relevante nationale normen van de lidstaten overeenkomstig artikel 25 van Richtlijn (EU) 2022/2555. Indien de bevoegde instantie van een lidstaat een dergelijke matrix verstrekt, integreren het ENTSB voor elektriciteit en de EU DSB-entiteit dit nationale overzicht in de verwijzingsmatrix.

3. Binnen zes maanden na de opstelling van een regionaal risicobeoordelingsverslag inzake cyberbeveiliging overeenkomstig artikel 21, lid 2, stellen de TSB's, met de hulp van het ENTSB voor elektriciteit, in samenwerking met de EU DSB-entiteit en in overleg met Enisa, aan de bevoegde instantie een wijziging van de verwijzingsmatrix voor. Het voorstel wordt gedaan overeenkomstig artikel 8, lid 10, en neemt de in de regionale risicobeoordeling aangeduide risico's in aanmerking.

HOOFDSTUK IV

AANBEVELINGEN VOOR AANBESTEDINGEN OP HET GEBIED VAN CYBERBEVEILIGING

Artikel 35

Aanbevelingen voor aanbestedingen op het gebied van cyberbeveiliging

1. In een werkprogramma dat steeds na de goedkeuring van een regionaal risicobeoordelingsverslag inzake cyberbeveiliging wordt opgesteld en geactualiseerd, ontwikkelen de TSB's, met de hulp van het ENTSB voor elektriciteit en in samenwerking met de EU DSB-entiteit, niet-bindende aanbevelingen voor aanbestedingen op het gebied van cyberbeveiliging die entiteiten met zeer belangrijke impact of met kritieke impact kunnen gebruiken als basis voor de aanbesteding van ICT-producten, -diensten en -processen binnen de perimeters van zeer belangrijke impact of kritieke impact. Dit programma omvat:

a) een beschrijving en classificatie van de soorten ICT-producten, -diensten en -processen die worden gebruikt door entiteiten met zeer belangrijke impact of met kritieke impact binnen de perimeter van zeer belangrijke impact of kritieke impact;

b) een lijst van de soorten ICT-producten, -diensten en -processen waarvoor niet-bindende cyberbeveiligingsaanbevelingen worden opgesteld op basis van de relevante regionale beoordelingsverslagen over cyberbeveiligingsrisico's en de prioriteiten van entiteiten met zeer belangrijke impact of met kritieke impact.

2. Het ENTSB voor elektriciteit verstrekt, in samenwerking met de EU DSB-entiteit, aan ACER binnen zes maanden na de vaststelling of actualisering van het regionale beoordelingsverslag over cyberbeveiligingsrisico's een samenvatting van dat werkprogramma.

3. De TSB's streven er, met de hulp van het ENTSB voor elektriciteit en in samenwerking met de EU DSB-entiteit, naar dat tussen de systeembeheersregio's gebruik wordt gemaakt van dezelfde of vergelijkbare niet-bindende aanbevelingen voor aanbestedingen op het gebied van cyberbeveiliging, opgesteld op basis van de relevante regionale beoordelingsverslagen over cyberbeveiligingsrisico's. De aanbevelingen voor aanbestedingen op het gebied van cyberbeveiliging omvatten ten minste de in artikel 33, lid 2, punt a), bedoelde specificaties. Indien mogelijk worden de specificaties uit Europese en internationale normen gekozen.

4. Met de hulp van het ENTSB voor elektriciteit en in samenwerking met de EU DSB-entiteit, waarborgen de TSB's dat deze aanbevelingen voor aanbestedingen op het gebied van cyberbeveiliging:

a) voldoen aan de aanbestedingsbeginselen krachtens Richtlijn 2014/24/EU, en

b) verenigbaar zijn en rekening houden met de recentste beschikbare Europese cyberbeveiligingscertificeringsregelingen voor ICT-producten, -diensten en -processen.

Artikel 36

Richtsnoeren voor het gebruik van Europese cyberbeveiligingscertificeringsregelingen voor de aanschaf van ICT-producten, -diensten en -processen

1. De overeenkomstig artikel 35 opgestelde niet-bindende aanbevelingen voor aanbestedingen op het gebied van cyberbeveiliging kunnen sectorspecifieke richtsnoeren inzake het gebruik van Europese cyberbeveiligingscertificeringsregelingen bevatten, als een geschikte regeling beschikbaar is voor een type ICT-product, -dienst of -proces dat door entiteiten met kritieke impact wordt gebruikt, onverminderd het kader voor de vaststelling van Europese cyberbeveiligingscertificeringsregelingen overeenkomstig artikel 46 van Verordening (EU) 2019/881.

2. De TSB's werken, met de hulp van het ENTSB voor elektriciteit en in samenwerking met de EU DSB-entiteit, nauw samen met Enisa bij het verstrekken van sectorspecifieke richtsnoeren die overeenkomstig lid 1 in niet-bindende aanbevelingen voor aanbestedingen op het gebied van cyberbeveiliging zijn opgenomen.

HOOFDSTUK V

INFORMATIESTROMEN, CYBERAANVALLEN EN CRISISBEHEERSING

Artikel 37

Regels voor het delen van informatie

1. Met betrekking tot ontvangen informatie over een te melden cyberaanval, zal de bevoegde instantie:

a) het vertrouwelijkheidsniveau van die informatie beoordelen en de entiteit onverwijld en uiterlijk 24 uur na ontvangst ervan in kennis stellen van het resultaat van haar beoordeling;

b) trachten een aan andere bevoegde instanties in de Unie gemelde vergelijkbare cyberaanval op te zoeken, om de in het kader van de te melden cyberaanval ontvangen informatie te vergelijken met informatie die in het kader van andere cyberaanvallen is verstrekt, en bestaande informatie te verrijken en de respons op het gebied van cyberbeveiliging te versterken en te coördineren;

c) verantwoordelijk zijn voor de verwijdering van bedrijfsgeheimen en de anonimisering van informatie overeenkomstig de desbetreffende nationale en Unieregels;

d) de informatie onverwijld en uiterlijk 24 uur na ontvangst van een te melden cyberaanval delen met de nationale centrale contactpunten, de CSIRT's en alle overeenkomstig artikel 4 aangewezen bevoegde instanties in andere lidstaten, en deze instanties en organen regelmatig geactualiseerde informatie verstrekken;

e) de informatie over de cyberaanval, na anonimisering en verwijdering van bedrijfsgeheimen overeenkomstig lid 1, punt c), onverwijld en uiterlijk 24 uur na ontvangst van de in lid 1, punt a), bedoelde informatie verspreiden onder entiteiten met zeer belangrijke impact of met kritieke impact in haar lidstaat, en regelmatig geactualiseerde informatie verstrekken, zodat de entiteiten hun verdediging doeltreffend kunnen organiseren;

f) de rapporterende entiteit met zeer belangrijke impact of met kritieke impact kunnen verzoeken de informatie over de te melden cyberaanval op een veilige manier verder te verspreiden onder andere entiteiten die getroffen kunnen worden, om situationeel bewustzijn bij de elektriciteitssector op te wekken en te voorkomen dat zich een risico voordoet dat tot een grensoverschrijdend cyberincident op het gebied van elektriciteit kan escaleren;

g) na anonimisering en verwijdering van bedrijfsgeheimen een samenvattend verslag met Enisa delen, met de informatie over de cyberaanval.

2. Met betrekking tot kennis van een actief uitgebuite nog niet verholpen kwetsbaarheid, zal een CSIRT:

a) die kennis onverwijld met Enisa delen via een passend beveiligd kanaal voor informatie-uitwisseling, tenzij in ander Unierecht anders is bepaald;

b) de betrokken entiteit ondersteunen om van de fabrikant of leverancier een doeltreffend, gecoördineerd en snel beheer van de actief uitgebuite nog niet verholpen kwetsbaarheid of doeltreffende en efficiënte risicobeperkende maatregelen te ontvangen;

c) de beschikbare informatie delen met de verkoper, en waar mogelijk, de fabrikant of leverancier verzoeken een lijst op te stellen van CSIRT's in de lidstaten die bij de actief uitgebuite nog niet verholpen kwetsbaarheid betrokken zijn en op de hoogte moeten worden gebracht;

d) de beschikbare informatie delen met de in het vorige punt bedoelde CSIRT's, op "need-to-know"-basis;

e) eventuele mitigatiestrategieën en -maatregelen met betrekking tot de gemelde actief uitgebuite nog niet verholpen kwetsbaarheid delen.

3. Met betrekking tot kennis van een actief uitgebuite nog niet verholpen kwetsbaarheid, zal een bevoegde instantie:

a) na afstemming met de CSIRT's in haar lidstaat eventuele mitigatiestrategieën en -maatregelen met betrekking tot de gemelde actief uitgebuite nog niet verholpen kwetsbaarheid delen;

b) de informatie delen met een CSIRT in de lidstaat waar de actief uitgebuite nog niet verholpen kwetsbaarheid is gemeld.

4. Indien de bevoegde instantie kennis krijgt van een nog niet verholpen kwetsbaarheid, zonder dat er aanwijzingen zijn dat die al actief wordt uitgebuit, werkt zij onverwijld met het CSIRT met het oog op de gecoördineerde bekendmaking van kwetsbaarheden als bedoeld in artikel 12, lid 1, van Richtlijn (EU) 2022/2555.

5. Indien een CSIRT informatie over cyberdreigingen ontvangt van een of meer entiteiten met zeer belangrijke impact of met kritieke impact overeenkomstig artikel 38, lid 6, verspreidt het team die informatie of alle andere informatie die van belang is voor het voorkomen, opsporen, reageren op of beperken van het gerelateerde risico voor entiteiten met zeer belangrijke impact of met kritieke impact in zijn lidstaat en, in voorkomend geval, onverwijld en uiterlijk vier uur na ontvangst van de informatie onder alle betrokken CSIRT's en zijn nationale centrale contactpunt.

6. Indien een bevoegde instantie van een of meer entiteiten met zeer belangrijke impact of met kritieke impact kennis krijgt van informatie met betrekking tot cyberdreigingen, stuurt zij die informatie door naar het CSIRT voor de toepassing van lid 5.

7. Na overeenstemming tussen de betrokken bevoegde instanties kunnen zij de verantwoordelijkheden uit hoofde van de leden 3 en 4 met betrekking tot een of meer entiteiten met zeer belangrijke impact of met kritieke impact die in meer dan een lidstaat actief zijn, geheel of gedeeltelijk delegeren aan een andere bevoegde instantie in een van die lidstaten.

8. De TSB's ontwikkelen, met de hulp van het ENTSB voor elektriciteit en in samenwerking met de EU DSB-entiteit, uiterlijk 13 juni 2025 een methode voor een classificatieschema van cyberaanvallen. De TSB's kunnen, met de hulp van het ENTSB voor elektriciteit en de EU DSB-entiteit, de bevoegde instanties verzoeken Enisa en hun instanties die bevoegd zijn voor cyberbeveiliging te raadplegen met het oog op bijstand bij de ontwikkeling van een dergelijk classificatieschema. De methode biedt een rangschikking van de ernst van een cyberaanval volgens vijf niveaus, waarbij de twee hoogste niveaus "hoog" en "kritiek" zijn. De rangschikking wordt gebaseerd op een beoordeling van de volgende parameters:

a) de potentiële gevolgen, met inachtneming van de blootgestelde activa en perimeters, zoals bepaald overeenkomstig artikel 26, lid 4, punt c), en

b) de ernst van de cyberaanval.

9. Uiterlijk 13 juni 2026 voert het ENTSB voor elektriciteit, in samenwerking met de EU DSB-entiteit, een haalbaarheidsstudie uit om de mogelijkheid en de financiële kosten te beoordelen voor de ontwikkeling van een gemeenschappelijk instrument waarmee alle entiteiten informatie kunnen delen met de relevante nationale instanties.

10. In de haalbaarheidsstudie wordt aandacht besteed aan de mogelijkheid dat een dergelijk gemeenschappelijk instrument:

a) ondersteuning biedt aan entiteiten met zeer belangrijke impact of met kritieke impact middels relevante veiligheidsgerelateerde informatie voor de exploitatie van grensoverschrijdende elektriciteitsstromen, zoals bijna-realtime meldingen van cyberaanvallen, vroegtijdige waarschuwingen in verband met cyberbeveiliging en niet-openbaargemaakte kwetsbaarheden betreffende het elektriciteitssysteem gebruikte apparatuur;

b) wordt onderhouden in een geschikte en hoogst betrouwbare omgeving;

c) gegevens kan verzamelen van entiteiten met zeer belangrijke impact of met kritieke impact en zorgt voor het eenvoudiger verwijderen van vertrouwelijke informatie en anonimiseren van gegevens en voor een snelle verspreiding ervan onder entiteiten met zeer belangrijke impact of met kritieke impact.

11. Het ENTSB voor elektriciteit zal, in samenwerking met de EU DSB-entiteit:

a) Enisa en de NIS-samenwerkingsgroep, de nationale centrale contactpunten en de vertegenwoordigers van de belangrijkste belanghebbenden raadplegen bij de beoordeling van de haalbaarheid;

b) de resultaten van de haalbaarheidsstudie aan ACER en de NIS-samenwerkingsgroep voorleggen.

12. Het ENTSB voor elektriciteit kan, in samenwerking met de EU DSB-entiteit, initiatieven van entiteiten met zeer belangrijke impact of met kritieke impact analyseren en faciliteren om dergelijke instrumenten voor informatie-uitwisseling te beoordelen en te testen.

Artikel 38

Rol van entiteiten met zeer belangrijke impact of met kritieke impact bij het delen van informatie

1. De entiteiten met zeer belangrijke impact of met kritieke impact:

a) stellen voor alle middelen binnen hun overeenkomstig artikel 26, lid 4, punt c), bepaalde cyberbeveiligingsperimeter ten minste de capaciteiten van het operationeel centrum voor cyberbeveiliging vast om:

   i) te waarborgen dat de relevante netwerk- en informatiesystemen en toepassingen beveiligingslogbestanden produceren voor het toezicht op de beveiliging, zodat anomalieën kunnen worden opgespoord en informatie over cyberaanvallen kan worden verzameld;

   ii) toezicht op de beveiliging te houden, met inbegrip van het opsporen van hacks en het beoordelen van kwetsbaarheden van netwerk- en informatiesystemen;

   iii) alle binnen hun verantwoordelijkheid en capaciteiten vereiste maatregelen te onderzoeken en, indien nodig, te treffen, ter bescherming van de entiteit;

   iv) deel te nemen aan de in dit artikel beschreven verzameling en uitwisseling van informatie;

b) mogen deze capaciteiten krachtens punt a) geheel of gedeeltelijk aanschaffen via aanbieders van beheerde beveiligingsdiensten. Entiteiten met zeer belangrijke impact of met kritieke impact blijven verantwoordelijk voor de aanbieders van beheerde beveiligingsdiensten en houden toezicht op hun werkzaamheden;

c) wijzen een centraal contactpunt op entiteitsniveau aan met het oog op het delen van informatie.

2. Enisa kan niet-bindende richtsnoeren uitvaardigen betreffende het vaststellen van dergelijke capaciteiten of het uitbesteden van de dienst aan aanbieders van beheerde beveiligingsdiensten, als onderdeel van de in artikel 6, lid 2, van Verordening (EU) 2019/881 omschreven taak.

3. Onverwijld en uiterlijk vier uur nadat zij zich ervan bewust is geworden dat het incident moet worden gemeld, deelt een entiteit met zeer belangrijke impact of met kritieke impact de relevante informatie met betrekking tot een te melden cyberaanval met haar CSIRT's en met haar bevoegde instantie.

4. Informatie met betrekking tot een cyberaanval wordt geacht gemeld te worden indien de cyberaanval door de getroffen entiteit wordt beoordeeld met het niveau "hoog" of "kritiek" overeenkomstig de methode voor een classificatieschema van cyberaanvallen van artikel 37, lid 8. Het overeenkomstig lid 1, punt c), aangewezen centrale contactpunt op entiteitsniveau deelt de classificatie van incidenten mee.

5. Indien entiteiten met zeer belangrijke impact of met kritieke impact relevante informatie met betrekking tot actief uitgebuite nog niet verholpen kwetsbaarheden aan een CSIRT melden, kan het CSIRT die informatie doorgeven aan zijn bevoegde instantie. Afhankelijk van de gevoeligheid van de gemelde informatie kan het CSIRT om gegronde cyberbeveiligingsoverwegingen de informatie onder zich houden of de toezending ervan uitstellen.

6. Iedere entiteit met zeer belangrijke impact of met kritieke impact verstrekt haar CSIRT's onverwijld alle informatie met betrekking tot een te melden cyberdreiging die een grensoverschrijdend effect kan hebben. Informatie met betrekking tot een cyberdreiging wordt geacht gemeld te worden indien aan ten minste een van de volgende voorwaarden is voldaan:

a) de informatie biedt relevante inlichtingen voor andere entiteiten met zeer belangrijke impact of met kritieke impact om de gevolgen van het risico te voorkomen, op te sporen, erop te reageren of te mitigeren;

b) de opgespoorde technieken, tactieken en procedures die bij een aanval worden gebruikt, leiden tot informatie zoals gecompromitteerde URL- of IP-adressen, hashes of andere attributen die van belang zijn om meer inzicht in de aanval te krijgen;

c) een cyberdreiging kan verder worden beoordeeld en begrepen aan de hand van aanvullende informatie van dienstverleners of derden die niet onder deze verordening vallen.

7. Iedere entiteit met zeer belangrijke impact of met kritieke impact specificeert bij het delen van informatie op grond van dit artikel het volgende:

a) dat de informatie wordt ingediend overeenkomstig deze verordening;

b) of de informatie betrekking heeft op:

   i) een te melden cyberaanval als bedoeld in lid 3;

   ii) actief uitgebuite nog niet verholpen kwetsbaarheden die niet algemeen bekend zijn, als bedoeld in lid 4;

   iii) een te melden cyberdreiging als bedoeld in lid 5;

c) in het geval van een te melden cyberaanval, het niveau van de cyberaanval overeenkomstig de methode voor een classificatieschema van cyberaanvallen van artikel 37, lid 8, en informatie die tot deze classificatie heeft geleid, met inbegrip van ten minste de zwaarte van de cyberaanval.

8. Indien een entiteit met zeer belangrijke impact of met kritieke impact een significant incident meldt overeenkomstig artikel 23 van Richtlijn (EU) 2022/2555 en de melding van incidenten uit hoofde van dat artikel relevante informatie bevat zoals vereist krachtens lid 3 van dit artikel, geldt de rapportage van de entiteit krachtens artikel 23, lid 1, van die richtlijn als rapportage van informatie krachtens lid 3 van dit artikel.

9. Iedere entiteit met zeer belangrijke impact of met kritieke impact brengt verslag uit aan haar bevoegde instantie of het CSIRT door duidelijk aan te geven welke specifieke informatie alleen met de bevoegde instantie of het CSIRT mag worden gedeeld, in gevallen waarin de informatie-uitwisseling een bron van een cyberaanval zou kunnen zijn. Iedere entiteit met zeer belangrijke impact of met kritieke impact mag een niet-vertrouwelijke versie van de informatie aan het bevoegde CSIRT verstrekken.

Artikel 39

Opsporing van cyberaanvallen en behandeling van gerelateerde informatie

1. Entiteiten met zeer belangrijke impact of met kritieke impact ontwikkelen de nodige capaciteiten om gedetecteerde cyberaanvallen aan te pakken, met de benodigde steun van de betrokken bevoegde instantie, het ENTSB voor elektriciteit en de EU DSB-entiteit. De entiteiten met zeer belangrijke impact of met kritieke impact kunnen worden ondersteund door het CSIRT dat in hun respectieve lidstaat is aangewezen als onderdeel van de bij artikel 11, lid 5, punt a), van Richtlijn (EU) 2022/2555 aan de CSIRT's toegewezen taak. Entiteiten met zeer belangrijke impact of met kritieke impact voeren doeltreffende processen in om cyberaanvallen die gevolgen zullen of kunnen hebben voor grensoverschrijdende elektriciteitsstromen in kaart te brengen, te classificeren en erop te reageren, om de gevolgen tot een minimum te beperken.

2. Indien een cyberaanval gevolgen heeft voor grensoverschrijdende elektriciteitsstromen, werken de centrale contactpunten op entiteitsniveau van getroffen entiteiten met zeer belangrijke impact of met kritieke impact samen om informatie uit te wisselen, onder de coördinatie van de bevoegde instantie van de lidstaat waar de cyberaanval voor het eerst is gemeld.

3. Entiteiten met zeer belangrijke impact of met kritieke impact:

a) waarborgen dat hun eigen centrale contactpunt op entiteitsniveau op "need-to-know"-basis toegang heeft tot de informatie die zij via hun bevoegde instantie van het nationale centrale contactpunt hebben ontvangen;

b) tenzij reeds geschied overeenkomstig artikel 3, lid 4, van Richtlijn (EU) 2022/2555, stellen de bevoegde instantie van de lidstaat waar zij zijn gevestigd en het nationale centrale contactpunt in kennis van een lijst van hun centrale contactpunten voor cyberbeveiliging op entiteitsniveau:

   i) waarvan die bevoegde instantie en het nationale centrale contactpunt kunnen verwachten dat zij informatie over te melden cyberaanvallen ontvangen;

   ii) waaraan de bevoegde instanties en nationale centrale contactpunten informatie moeten verstrekken;

c) stellen procedures voor het beheer van cyberaanvallen op, met inbegrip van rollen en verantwoordelijkheden, werkzaamheden en reacties op basis van de waarneembare evolutie van de cyberaanval binnen de perimeters van zeer belangrijke impact en kritieke impact;

d) testen de algemene procedures voor het beheer van cyberaanvallen ten minste ieder jaar door middel van ten minste één scenario dat rechtstreeks of onrechtstreeks van invloed is op grensoverschrijdende elektriciteitsstromen. Die jaarlijkse test kan worden uitgevoerd door entiteiten met zeer belangrijke impact of met kritieke impact tijdens de reguliere oefeningen als bedoeld in artikel 43. Elke responsactiviteit op een live-cyberaanval van ten minste niveau 2 overeenkomstig de methode voor een classificatieschema van cyberaanvallen van artikel 37, lid 8, en met een onderliggende oorzaak in cyberbeveiliging, kan dienen als een jaarlijkse test van het responsplan voor cyberaanvallen.

4. De in lid 1 bedoelde werkzaamheden kunnen door de lidstaten ook aan de regionale coördinatiecentra worden gedelegeerd overeenkomstig artikel 37, lid 2, van Verordening (EU) 2019/943.

Artikel 40

Crisisbeheer

1. Indien de bevoegde instantie vaststelt dat een elektriciteitscrisis verband houdt met een cyberaanval met gevolgen voor meer dan één lidstaat, richten de bevoegde instanties van de getroffen lidstaten, de CS-NCA's, de RP-NCA en de NIS-cybercrisisbeheerautoriteiten van de getroffen lidstaten gezamenlijk een ad-hocgroep voor grensoverschrijdende crisiscoördinatie op.

2. De ad-hocgroep voor grensoverschrijdende crisiscoördinatie:

a) coördineert de efficiënte opzoeking en verdere verspreiding van alle relevante cyberbeveiligingsinformatie onder de bij het crisisbeheersingsproces betrokken entiteiten;

b) organiseert de communicatie tussen alle door de crisis getroffen entiteiten en de bevoegde instanties om overlappingen te verminderen en de efficiëntie van de analyses en technische reacties te vergroten om de gelijktijdige elektriciteitscrises met een onderliggende oorzaak in cyberbeveiliging op te lossen;

c) verstrekt, in samenwerking met de bevoegde CSIRT's, aan de door het incident getroffen entiteiten de vereiste deskundigheid, met inbegrip van operationeel advies over de uitvoering van mogelijke risicobeperkende maatregelen;

d) informeert de Commissie en de Coördinatiegroep voor elektriciteit en houdt die regelmatig op de hoogte van de status van het incident, met inachtneming van de beschermingsbeginselen van artikel 46;

e) wint advies in bij relevante instanties, organen of entiteiten die de elektriciteitscrisis kunnen helpen beperken.

3. Indien de cyberaanval wordt aangemerkt, of naar verwachting zal worden aangemerkt als een grootschalig cyberbeveiligingsincident, stelt de ad-hocgroep voor grensoverschrijdende crisiscoördinatie de nationale cybercrisisbeheerautoriteiten overeenkomstig artikel 9, lid 1, van Richtlijn (EU) 2022/2555 in de door het incident getroffen lidstaten, evenals de Commissie en EU-CyCLONe onmiddellijk daarvan in kennis. In een dergelijke situatie ondersteunt de ad-hocgroep voor grensoverschrijdende crisiscoördinatie EU-CyCLONe met betrekking tot sectorspecifieke kenmerken.

4. Entiteiten met zeer belangrijke impact of met kritieke impact ontwikkelen en beschikken over capaciteit, interne richtsnoeren, paraatheidsplannen en personeel om deel te nemen aan het opsporen en beperken van grensoverschrijdende crises. De entiteit met zeer belangrijke impact of met kritieke impact die door een gelijktijdige elektriciteitscrisis wordt getroffen, onderzoekt de onderliggende oorzaak van een dergelijke crisis in samenwerking met haar bevoegde instantie om te bepalen in hoeverre de crisis verband houdt met een cyberaanval.

5. De in lid 4 bedoelde werkzaamheden kunnen door de lidstaten ook aan de regionale coördinatiecentra worden gedelegeerd overeenkomstig artikel 37, lid 2, van Verordening (EU) 2019/943.

Artikel 41

Crisisbeheer- en -responsplannen op het gebied van cyberbeveiliging

1. Binnen 24 maanden na de kennisgeving aan ACER van het Uniebrede beoordelingsverslag over cyberbeveiligingsrisico's ontwikkelt ACER, in nauwe samenwerking met Enisa, het ENTSB voor elektriciteit, de EU DSB-entiteit, de CS-NCA's, de bevoegde instanties, de RP-NCA's, de NRI's en de nationale NIS-cybercrisisbeheerautoriteiten, een crisisbeheer- en -responsplan op het gebied van cyberbeveiliging op Unieniveau voor de elektriciteitssector.

2. Binnen twaalf maanden na de opstelling door ACER van het crisisbeheer- en -responsplan op het gebied van cyberbeveiliging op Unieniveau voor de elektriciteitssector overeenkomstig lid 1 ontwikkelt iedere bevoegde instantie een nationaal crisisbeheer- en -responsplan op het gebied van cyberbeveiliging op Unieniveau voor grensoverschrijdende elektriciteitsstromen, met inachtneming van het crisisbeheerplan op het gebied van cyberbeveiliging op Unieniveau en het overeenkomstig artikel 10 van Verordening (EU) 2019/941 opgestelde nationale risicoparaatheidsplan. Dit plan is in overeenstemming met het plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons overeenkomstig artikel 9, lid 4, van Richtlijn (EU) 2022/2555. De bevoegde instantie zorgt voor coördinatie met de entiteiten met zeer belangrijke impact of met kritieke impact en met de RP-NCA in haar lidstaat.

3. Het krachtens artikel 9, lid 4, van Richtlijn (EU) 2022/2555 vereiste nationale plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons wordt beschouwd als een nationaal crisisbeheerplan op het gebied van cyberbeveiliging uit hoofde van dit artikel indien het bepalingen inzake crisisbeheer- en -respons voor grensoverschrijdende elektriciteitsstromen bevat.

4. De in de leden 1 en 2 bedoelde werkzaamheden kunnen door de lidstaten ook aan de regionale coördinatiecentra worden gedelegeerd overeenkomstig artikel 37, lid 2, van Verordening (EU) 2019/943.

5. Entiteiten met zeer belangrijke impact of met kritieke impact waarborgen dat hun crisisbeheerprocessen op het gebied van cyberbeveiliging:

a) beschikken over compatibele procedures voor de behandeling van grensoverschrijdende incidenten op het gebied van cyberbeveiliging in de zin van artikel 6, lid 8, van Richtlijn (EU) 2022/2555, die formeel in hun crisisbeheerplannen zijn opgenomen;

b) deel uitmaken van de algemene crisisbeheeractiviteiten.

6. Binnen twaalf maanden na de kennisgeving van de entiteiten met zeer belangrijke impact of met kritieke impact overeenkomstig artikel 24, lid 6, en vervolgens om de drie jaar, ontwikkelen entiteiten met zeer belangrijke impact of met kritieke impact een crisisbeheerplan op entiteitsniveau voor cyberbeveiligingscrises, dat in hun algemene crisisbeheerplannen wordt opgenomen. Dit bevat ten minste de volgende gegevens:

a) de regels voor de afkondiging van de crisis als bedoeld in artikel 14, leden 2 en 3, van Verordening (EU) 2019/941;

b) duidelijke rollen en verantwoordelijkheden voor crisisbeheer, inclusief de rol van andere relevante entiteiten met zeer belangrijke impact of met kritieke impact;

c) actuele contactgegevens en regels voor communicatie en informatie-uitwisseling tijdens een crisissituatie, met inbegrip van de verbinding met de CSIRT's.

7. De maatregelen voor crisisbeheer overeenkomstig artikel 21, lid 2, punt c), van Richtlijn (EU) 2022/2555 worden beschouwd als een crisisbeheerplan op entiteitsniveau voor de elektriciteitssector uit hoofde van dit artikel indien het alle in lid 6 genoemde vereisten omvat.

8. De crisisbeheerplannen worden getest tijdens de in de artikelen 43, 44 en 45 bedoelde cyberbeveiligingsoefeningen.

9. De entiteiten met zeer belangrijke impact of met kritieke impact nemen hun crisisbeheerplannen op entiteitsniveau op in hun bedrijfscontinuïteitsplannen voor de processen met zeer belangrijke impact of met kritieke impact. De crisisbeheerplannen op entiteitsniveau omvatten:

a) de processen die afhankelijk zijn van de beschikbaarheid, de integriteit en de betrouwbaarheid van IT-diensten;

b) alle bedrijfscontinuïteitslocaties, met inbegrip van de locaties voor hardware en software;

c) alle interne rollen en verantwoordelijkheden die verband houden met bedrijfscontinuïteitsprocessen.

10. De entiteiten met zeer belangrijke impact of met kritieke impact actualiseren hun crisisbeheerplannen op entiteitsniveau ten minste om de drie jaar en als dat nodig is.

11. ACER actualiseert het overeenkomstig lid 1 opgestelde crisisbeheer- en -responsplan op het gebied van cyberbeveiliging op Unieniveau voor de elektriciteitssector ten minste om de drie jaar en als dat nodig is.

12. Iedere bevoegde instantie actualiseert de overeenkomstig lid 2 opgestelde nationale crisisbeheer- en -responsplannen op het gebied van cyberbeveiliging voor grensoverschrijdende elektriciteitsstromen ten minste om de drie jaar en als dat nodig is.

13. De entiteiten met zeer belangrijke impact of met kritieke impact testen hun bedrijfscontinuïteitsplannen ten minste om de drie jaar of na grote veranderingen in een proces met kritieke impact. Het resultaat van de testen van het bedrijfscontinuïteitsplan wordt gedocumenteerd. Entiteiten met zeer belangrijke impact of met kritieke impact kunnen de test van hun bedrijfscontinuïteitsplan in de cyberbeveiligingsoefeningen opnemen.

14. De entiteiten met zeer belangrijke impact of met kritieke impact actualiseren hun bedrijfscontinuïteitsplan als dat nodig is en ten minste om de drie jaar, met inachtneming van het resultaat van de test.

15. Indien bij een test tekortkomingen in het bedrijfscontinuïteitsplan worden vastgesteld, corrigeert de entiteit met zeer belangrijke impact of met kritieke impact deze tekortkomingen binnen 180 kalenderdagen na de test en voert zij een nieuwe test uit om aan te tonen dat de corrigerende maatregelen doeltreffend zijn.

16. Indien een entiteit met zeer belangrijke impact of met kritieke impact de tekortkomingen niet binnen 180 kalenderdagen kan corrigeren, vermeldt zij de redenen daarvoor in het verslag dat overeenkomstig artikel 27 aan haar bevoegde instantie moet worden verstrekt.

Artikel 42

Capaciteit voor vroegtijdige waarschuwing op het gebied van cyberbeveiliging voor de elektriciteitssector

1. De bevoegde instanties werken samen met Enisa om capaciteit voor vroegtijdige waarschuwing op het gebied van cyberbeveiliging voor de elektriciteitssector ("ECEAC") te ontwikkelen als onderdeel van de ondersteuning van de lidstaten overeenkomstig artikel 6, lid 2, en artikel 7, van Verordening (EU) 2019/881.

2. De ECEAC stelt Enisa in staat om bij het verrichten van de in artikel 7, lid 7, van Verordening (EU) 2019/881 genoemde werkzaamheden:

a) vrijwillig gedeelde informatie te verzamelen bij:

   i) de CSIRT's en de bevoegde instanties;

   ii) de in artikel 2 genoemde entiteiten;

   iii) andere entiteiten die op vrijwillige basis relevante informatie willen delen;

b) de verzamelde informatie te beoordelen en te classificeren;

c) de informatie te beoordelen waartoe Enisa toegang heeft voor het in kaart brengen van cyberrisicovoorwaarden en van relevante indicatoren voor aspecten van grensoverschrijdende elektriciteitsstromen;

d) omstandigheden en indicatoren vast te stellen die vaak met cyberaanvallen in de elektriciteitssector gepaard gaan;

e) te bepalen of verdere analyses moeten worden uitgevoerd en preventieve maatregelen moeten worden getroffen door middel van een aanduiding en een beoordeling van de risicofactoren;

f) de bevoegde instanties in kennis te stellen van de vastgestelde risico's en de aanbevolen preventieve maatregelen die specifiek zijn voor de betrokken entiteiten;

g) alle in artikel 2 genoemde relevante entiteiten in kennis te stellen van de resultaten van de overeenkomstig de punten b), c), en d), beoordeelde informatie;

h) de relevante informatie periodiek op te nemen in het situationeel bewustzijnverslag, dat wordt uitgebracht overeenkomstig artikel 7, lid 6, van Verordening (EU) 2019/881;

i) waar mogelijk, uit de verzamelde informatie toepasselijke gegevens af te leiden die een aanwijzing vormen dat er sprake is van een mogelijke veiligheidsinbreuk of cyberaanval ("inbreukindicatoren").

3. De CSIRT's verspreiden de van Enisa ontvangen informatie onverwijld onder de betrokken entiteiten, binnen hun in artikel 11, lid 3, punt b), van Richtlijn (EU) 2022/2555 omschreven taken.

4. ACER houdt toezicht op de doeltreffendheid van de ECEAC. Enisa staat ACER bij door alle nodige informatie te verstrekken, overeenkomstig artikel 6, lid 2, en artikel 7, lid 1, van Verordening (EU) 2019/881. De analyse van deze monitoringactiviteit maakt deel uit van het toezicht overeenkomstig artikel 12.

HOOFDSTUK VI

KADER VOOR CYBERBEVEILIGINGSOEFENINGEN OP HET GEBIED VAN ELEKTRICITEIT

Artikel 43

Cyberbeveiligingsoefeningen op het niveau van de entiteit en van de lidstaten

1. Uiterlijk 31 december van het jaar na de kennisgeving van entiteiten met kritieke impact, en vervolgens om de drie jaar, voert elke entiteit met kritieke impact een cyberbeveiligingsoefening uit, met inbegrip van een of meer scenario's met cyberaanvallen die rechtstreeks of onrechtstreeks van invloed zijn op grensoverschrijdende elektriciteitsstromen en verband houden met de tijdens de cyberbeveiligingsrisicobeoordelingen op het niveau van de lidstaten en entiteiten overeenkomstig de artikelen 20 en 27 vastgestelde risico's.

2. In afwijking van lid 1 kan de RP-NCA, na raadpleging van de bevoegde instantie en de relevante cybercrisisbeheerautoriteit zoals aangewezen of opgericht overeenkomstig artikel 9 van Richtlijn (EU) 2022/2555, besluiten een cyberbeveiligingsoefening op het niveau van de lidstaat te organiseren overeenkomstig lid 1, in plaats van een cyberbeveiligingsoefening op het niveau van de entiteit uit te voeren. Ter zake informeert de bevoegde instantie:

a) alle entiteiten met kritieke impact van zijn lidstaat, de NRI, de CSIRT's en de CS-NCA, uiterlijk 30 juni van het jaar voorafgaand aan de cyberbeveiligingsoefening op entiteitsniveau;

b) elke entiteit die aan de cyberbeveiligingsoefening op lidstaatniveau deelneemt, uiterlijk zes maanden voordat de oefening plaatsvindt.

3. Met de technische ondersteuning van haar CSIRT's organiseert de RP-NCA, onafhankelijk of in het kader van een andere cyberbeveiligingsoefening in die lidstaat, de in lid 2 beschreven cyberbeveiligingsoefening op het niveau van de lidstaat. Teneinde die oefeningen te kunnen groeperen, kan de RP-NCA de in lid 1 bedoelde cyberbeveiligingsoefening op lidstaatniveau met één jaar uitstellen.

4. De cyberbeveiligingsoefeningen op het niveau van de entiteit en van de lidstaten zijn in overeenstemming met de nationale kaders voor cyberbeveiligingscrisisbeheer overeenkomstig artikel 9, lid 4, punt d), van Richtlijn (EU) 2022/2555.

5. Uiterlijk 31 december 2026 en vervolgens om de drie jaar stelt het ENTSB voor elektriciteit, in samenwerking met de EU DSB-entiteit, een oefeningmodel beschikbaar om de in lid 1 bedoelde cyberbeveiligingsoefeningen op het niveau van de entiteit en van de lidstaat te houden. In dit model wordt rekening gehouden met de resultaten van de recentste cyberbeveiligingsrisicobeoordelingen op het niveau van de entiteit en van de lidstaten en worden belangrijke succescriteria opgenomen. Het ENTSB voor elektriciteit en de EU DSB-entiteit betrekken ACER en Enisa bij de ontwikkeling van dit model.

Artikel 44

Regionale of regio-overschrijdende cyberbeveiligingsoefeningen

1. Uiterlijk 31 december 2029 en vervolgens om de drie jaar organiseert het ENTSB voor elektriciteit, in samenwerking met de EU DSB-entiteit, in elke systeembeheersregio een regionale cyberbeveiligingsoefening. De entiteiten met kritieke impact in de systeembeheersregio nemen deel aan de regionale cyberbeveiligingsoefening. Het ENTSB voor elektriciteit kan, in samenwerking met de EU DSB-entiteit, in plaats van een regionale cyberbeveiligingsoefening in hetzelfde tijdsbestek in meer dan één systeembeheersregio een regio-overschrijdende cyberbeveiligingsoefening organiseren. Bij de oefening worden andere bestaande op Unieniveau ontwikkelde cyberbeveiligingsrisicobeoordelingen en -scenario's in aanmerking genomen.

2. Enisa ondersteunt het ENTSB voor elektriciteit en de EU DSB-entiteit bij de voorbereiding en de organisatie van de cyberbeveiligingsoefening op regionaal of regio-overschrijdend niveau.

3. Zes maanden voordat de oefening plaatsvindt, informeert het ENTSB voor elektriciteit, in overleg met de EU DSB-entiteit, de entiteiten met kritieke impact die aan de regionale of regio-overschrijdende cyberbeveiligingsoefening deelnemen.

4. De organisator van een regelmatige cyberbeveiligingsoefening op Unieniveau overeenkomstig artikel 7, lid 5, van Verordening (EU) 2019/881, of van een verplichte cyberbeveiligingsoefening met betrekking tot de elektriciteitssector binnen dezelfde geografische perimeter, kan het ENTSB voor elektriciteit en de EU DSB-entiteit uitnodigen om deel te nemen. In dergelijke gevallen is de verplichting van lid 1 niet van toepassing, mits alle entiteiten met kritieke impact in de systeembeheersregio aan dezelfde oefening deelnemen.

5. Indien het ENTSB voor elektriciteit en de EU DSB-entiteit deelnemen aan een in lid 4 bedoelde cyberbeveiligingsoefening, kunnen zij de in lid 1 bedoelde regionale of regio-overschrijdende cyberbeveiligingsoefening met één jaar uitstellen.

6. Uiterlijk 31 december 2027 en vervolgens om de drie jaar stelt het ENTSB voor elektriciteit, in samenwerking met de EU DSB-entiteit, een oefeningmodel beschikbaar om de regionale of regio-overschrijdende cyberbeveiligingsoefeningen te houden. In dit model wordt rekening gehouden met de resultaten van de recentste cyberbeveiligingsrisicobeoordelingen op het regionaal niveau en worden belangrijke succescriteria opgenomen. Het ENTSB voor elektriciteit raadpleegt de Commissie en kan advies inwinnen bij ACER, Enisa en het Joint Research Centre over de organisatie en de uitvoering van de regionale en regio-overschrijdende cyberbeveiligingsoefeningen.

Artikel 45

Resultaat van cyberbeveiligingsoefeningen op entiteits-, lidstaat-, regionaal of regio-overschrijdend niveau

1. Op verzoek van een entiteit met kritieke impact nemen aanbieders van kritieke diensten deel aan de in artikel 43, leden 1 en 2, en artikel 44, lid 1, bedoelde cyberbeveiligingsoefeningen als zij diensten verlenen aan de entiteit met kritieke impact op een gebied dat binnen het toepassingsgebied van de betreffende cyberbeveiligingsoefening valt.

2. Met het advies van Enisa indien daarom wordt verzocht overeenkomstig artikel 7, lid 5, van Verordening (EU) 2019/881, analyseren en voltooien de organisatoren van de in artikel 43, leden 1 en 2, en artikel 44, lid 1, bedoelde cyberbeveiligingsoefeningen de desbetreffende cyberbeveiligingsoefening door middel van een aan alle deelnemers gericht verslag met een samenvatting van de lessen. Dat verslag bevat:

a) de oefenscenario's, de vergaderverslagen, de belangrijkste standpunten, de successen en de geleerde lessen op alle niveaus van de elektriciteitswaardeketen;

b) of de belangrijkste succescriteria zijn vervuld;

c) een lijst van aanbevelingen voor entiteiten die deelnemen aan de relevante cyberbeveiligingsoefening om de processen, procedures, bijbehorende governancemodellen en bestaande contractuele afspraken met aanbieders van kritieke diensten te corrigeren, aan te passen of te wijzigen.

3. Op verzoek van het CSIRT-netwerk, de NIS-samenwerkingsgroep of EU-CyCLONe delen de organisatoren van de in artikel 43, leden 1 en 2, en artikel 44, lid 1, bedoelde cyberbeveiligingsoefeningen het resultaat van de desbetreffende cyberbeveiligingsoefening. De organisatoren delen de in lid 2, punten a) en b), bedoelde informatie met alle aan de oefeningen deelnemende entiteiten. De organisatoren delen de in lid 2, punt c), bedoelde lijst van aanbevelingen uitsluitend met de in de aanbevelingen genoemde entiteiten.

4. De organisatoren van de in artikel 43, leden 1 en 2, en artikel 44, lid 1, bedoelde cyberbeveiligingsoefeningen houden na afloop regelmatig overleg met de aan de oefeningen deelnemende entiteiten over de uitvoering van aanbevelingen uit hoofde van lid 2, punt c).

HOOFDSTUK VII

BESCHERMING VAN INFORMATIE

Artikel 46

Beginselen voor de bescherming van uitgewisselde informatie

1. De in artikel 2, lid 1, genoemde entiteiten waarborgen dat de krachtens deze verordening verstrekte, ontvangen, uitgewisselde of doorgegeven informatie alleen toegankelijk is op "need-to-know"-basis en overeenkomstig de toepasselijke Unie- en nationale voorschriften inzake informatiebeveiliging.

2. De in artikel 2, lid 1, genoemde entiteiten waarborgen dat de krachtens deze verordening verstrekte, ontvangen, uitgewisselde of doorgegeven informatie gedurende de gehele levenscyclus van die informatie wordt verwerkt en gevolgd en dat deze pas na anonimisering aan het einde van de levenscyclus mag worden vrijgegeven.

3. De in artikel 2, lid 1, genoemde entiteiten waarborgen dat alle nodige organisatorische en technische beschermingsmaatregelen zijn getroffen om de vertrouwelijkheid, de integriteit, de beschikbaarheid en de onweerlegbaarheid van de krachtens deze verordening verstrekte, ontvangen, uitgewisselde of doorgegeven informatie te waarborgen en te beschermen, onafhankelijk van de gebruikte middelen. De beschermingsmaatregelen:

a) zijn evenredigheid;

b) houden rekening met cyberbeveiligingsrisico's in verband met bekende oude en opkomende bedreigingen voor informatie in het kader van deze verordening;

c) zijn voor zover mogelijk gebaseerd op nationale, Europese of internationale normen en beste praktijken;

d) worden gedocumenteerd.

4. De in artikel 2, lid 1, genoemde entiteiten waarborgen dat wie toegang wordt verleend tot krachtens deze verordening verstrekte, ontvangen, uitgewisselde of doorgegeven informatie, wordt geïnformeerd over de op entiteitsniveau geldende veiligheidsvoorschriften en de maatregelen en procedures die voor de bescherming van informatie van belang zijn. Die entiteiten waarborgen dat de betrokken persoon de verantwoordelijkheid aanvaardt om de informatie te beschermen volgens de instructies tijdens de briefing.

5. De in artikel 2, lid 1, genoemde entiteiten waarborgen dat de toegang tot krachtens deze verordening verstrekte, ontvangen, uitgewisselde of doorgegeven informatie beperkt is tot personen:

a) die op basis van hun functie toegang mogen hebben tot die informatie, binnen de uitvoering van de toegewezen werkzaamheden;

b) van wie de entiteit de ethische en integriteitsbeginselen heeft kunnen beoordelen, en voor wie er geen bewijs is van een negatief resultaat uit een achtergrondcontrole bij een beoordeling van de betrouwbaarheid van de persoon conform de beste praktijken en standaardbeveiligingsvereisten van de entiteit en, indien nodig, de nationale wet- en regelgeving.

6. De in artikel 2, lid 1, genoemde entiteiten hebben schriftelijke toestemming van de natuurlijke of rechtspersoon die de informatie oorspronkelijk heeft opgesteld of verstrekt, alvorens die informatie te verstrekken aan een buiten het toepassingsgebied van deze verordening vallende derde.

7. Een in artikel 2, lid 1, genoemde entiteit kan van mening zijn dat deze informatie moet worden gedeeld zonder aan de leden 1 en 4 te voldoen, om een gelijktijdige elektriciteitscrisis met een onderliggende oorzaak in cyberbeveiliging of een grensoverschrijdende crisis binnen de Unie in een andere sector te voorkomen. In dat geval zal die entiteit:

a) de bevoegde instantie raadplegen en toestemming verkrijgen om die informatie te delen;

b) die informatie anonimiseren, met behoud van de elementen die nodig zijn om het publiek te informeren over een dreigend en ernstig risico voor grensoverschrijdende elektriciteitsstromen en de mogelijke mitigerende maatregelen;

c) de identiteit beschermen van de opsteller en de entiteiten die informatie krachtens deze verordening hebben verwerkt.

8. In afwijking van lid 6 kunnen de bevoegde instanties krachtens deze verordening verstrekte, ontvangen, uitgewisselde of doorgegeven informatie verstrekken aan een niet in artikel 2, lid 1, genoemde derde zonder schriftelijke voorafgaande toestemming van de opsteller van de informatie, maar de opsteller wordt wel zo spoedig mogelijk daarvan op de hoogte gebracht. Alvorens krachtens deze verordening verstrekte, ontvangen, uitgewisselde of doorgegeven informatie bekend te maken aan een niet in artikel 2, lid 1, genoemde derde, zorgt de betrokken bevoegde instantie er in redelijkheid voor dat de betrokken derde van de geldende veiligheidsvoorschriften op de hoogte is en waarborgt zij met een redelijk niveau van zekerheid dat de betrokken derde de ontvangen informatie kan beschermen overeenkomstig de leden 1 tot en met 5. De bevoegde instantie anonimiseert dergelijke informatie met behoud van de elementen die nodig zijn om het grote publiek te informeren over een dreigend en ernstig risico voor grensoverschrijdende elektriciteitsstromen en mogelijke mitigerende maatregelen, en om de identiteit van de opsteller van de informatie te beschermen. In dat geval beschermt de niet in artikel 2, lid 1, genoemde derde de ontvangen informatie overeenkomstig reeds op entiteitsniveau geldende regels of, indien dit niet mogelijk is, overeenkomstig de regels en instructies van de relevante bevoegde instantie.

9. Dit artikel is niet van toepassing op niet in artikel 2, lid 1, genoemde entiteiten die overeenkomstig lid 6 informatie ontvangen. In dat geval is lid 7 van toepassing, of kan de bevoegde instantie die entiteit schriftelijke instructies verstrekken die moeten worden toegepast in gevallen waarin overeenkomstig deze verordening informatie is ontvangen.

Artikel 47

Vertrouwelijkheid van informatie

1. Alle krachtens deze verordening verstrekte, ontvangen, uitgewisselde of doorgegeven informatie valt onder het in de leden 2 tot en met 5 bedoelde beroepsgeheim en onder artikel 65 van Verordening (EU) 2019/943. Alle informatie die met het oog op de uitvoering van deze verordening is verstrekt, ontvangen, uitgewisseld of doorgegeven tussen de in artikel 2, lid 1, genoemde entiteiten, wordt beschermd, met inachtneming van het vertrouwelijkheidsniveau van de informatie dat door de opsteller is toegepast.

2. Het beroepsgeheim geldt voor de in artikel 2 genoemde entiteiten.

3. De CS-NCA's, de NRI's, de RP-NCA's en de CSIRT's wisselen alle informatie uit die nodig is om hun werkzaamheden te verrichten.

4. Alle informatie die wordt ontvangen, uitgewisseld of doorgegeven tussen de in artikel 2, lid 1, genoemde entiteiten met het oog op de toepassing van artikel 23, wordt geanonimiseerd en geaggregeerd.

5. Informatie die beroepshalve is ontvangen door een onder deze verordening vallende entiteit of instantie, mag aan geen enkele andere persoon of instantie worden bekendgemaakt, onverminderd de gevallen die onder de nationale wetgeving, onder deze verordening of onder andere toepasselijke Uniewetgeving vallen.

6. Onverminderd de nationale of Uniewetgeving mag een instantie, entiteit of natuurlijke persoon die krachtens deze verordening informatie ontvangt, die informatie niet gebruiken voor andere doeleinden dan de uitvoering van haar werkzaamheden uit hoofde van deze verordening.

7. ACER vaardigt, na raadpleging van Enisa, alle bevoegde instanties, het ENTSB voor elektriciteit en de EU DSB-entiteit uiterlijk 13 juni 2025 richtsnoeren uit met betrekking tot mechanismen voor alle in artikel 2, lid 1, genoemde entiteiten met het oog op de uitwisseling van informatie, en met name geplande communicatiestromen, en methoden om informatie te anonimiseren en te aggregeren met het oog op de uitvoering van dit artikel.

8. Krachtens Unie- en nationale voorschriften vertrouwelijke informatie wordt alleen met de Commissie en andere bevoegde instanties uitgewisseld indien dat nodig is voor de toepassing van deze verordening. Er wordt uitsluitend informatie uitgewisseld die nodig is voor en evenredig is met het doel van die uitwisseling. Bij de uitwisseling van informatie wordt de vertrouwelijkheid van die informatie gewaarborgd en worden de veiligheids- en commerciële belangen van entiteiten met zeer belangrijke impact of met kritieke impact beschermd.

HOOFDSTUK VIII

SLOTBEPALINGEN

Artikel 48

Tijdelijke bepalingen

1. Tot het moment van de goedkeuring van de in artikel 6, lid 2, bedoelde voorwaarden of methoden of de in artikel 6, lid 3, bedoelde plannen, ontwikkelt het ENTSB voor elektriciteit, in samenwerking met de EU DSB-entiteit, niet-bindende richtsnoeren inzake de volgende kwesties:

a) een voorlopige impactindex voor de cyberbeveiliging van elektriciteit overeenkomstig lid 2;

b) een voorlopige lijst van Uniebrede processen met zeer belangrijke impact of met kritieke impact overeenkomstig lid 4, en

c) een voorlopige lijst van Europese en internationale normen en krachtens nationale wetgeving vereiste controles die van belang zijn voor met cyberbeveiliging samenhangende aspecten van grensoverschrijdende elektriciteitsstromen overeenkomstig lid 6.

2. Uiterlijk 13 oktober 2024 stelt het ENTSB voor elektriciteit, in samenwerking met de EU DSB-entiteit, een aanbeveling op voor een voorlopige ECII. Het ENTSB voor elektriciteit stelt, in samenwerking met de EU DSB-entiteit, de bevoegde instanties in kennis van de aanbevolen voorlopige ECII.

3. Vier maanden na ontvangst van de aanbevolen voorlopige ECII, of uiterlijk 13 februari 2025, duiden de bevoegde instanties op basis van de aanbevolen ECII kandidaten voor entiteiten met zeer belangrijke impact of met kritieke impact in hun lidstaat aan en stellen een voorlopige lijst op van entiteiten met zeer belangrijke impact of met kritieke impact. De op de voorlopige lijst opgenomen entiteiten met zeer belangrijke impact of met kritieke impact kunnen op basis van het voorzorgsbeginsel vrijwillig hun verplichtingen krachtens deze verordening nakomen. Uiterlijk 13 maart 2025 stellen de bevoegde instanties de in de voorlopige lijst genoemde entiteiten ervan in kennis dat zij zijn aangemerkt als entiteit met zeer belangrijke impact of met kritieke impact.

4. Uiterlijk 13 december 2024 stelt het ENTSB voor elektriciteit, in samenwerking met de EU DSB-entiteit, een voorlopige lijst van Uniebrede entiteiten met zeer belangrijke impact of met kritieke impact op. De overeenkomstig lid 3 aangemelde entiteiten die besluiten hun krachtens deze verordening vastgestelde verplichtingen op basis van het voorzorgsbeginsel vrijwillig na te komen, gebruiken de voorlopige lijst van processen met zeer belangrijke impact of met kritieke impact om de voorlopige perimeter van zeer belangrijke impact of van kritieke impact vast te stellen en om te bepalen welke activa in de eerste cyberbeveiligingsrisicobeoordeling op entiteitsniveau moeten worden opgenomen.

5. Uiterlijk 13 september 2024 verstrekt iedere bevoegde instantie in de zin van artikel 4, lid 1, aan het ENTSB voor elektriciteit en de EU DSB-entiteit een lijst van haar voor de met cyberbeveiliging samenhangende aspecten van grensoverschrijdende elektriciteitsstromen toepasselijke nationale wetgeving.

6. Uiterlijk 13 juni 2025 stelt het ENTSB voor elektriciteit, in samenwerking met de EU DSB-entiteit, een voorlopige lijst op van Europese en internationale normen en krachtens nationale wetgeving vereiste controles die van belang zijn voor met cyberbeveiliging samenhangende aspecten van grensoverschrijdende elektriciteitsstromen, met inachtneming van de door de bevoegde instanties verstrekte informatie.

7. De voorlopige lijst van Europese en internationale normen en controles omvat:

a) Europese en internationale normen en nationale wetgeving met richtsnoeren voor methoden voor cyberbeveiligingsrisicobeheer op entiteitsniveau, en

b) cyberbeveiligingscontroles die gelijkwaardig zijn aan de controles die naar verwachting deel zullen uitmaken van de minimale en geavanceerde cyberbeveiligingscontroles.

8. Het ENTSB voor elektriciteit en de EU DSB-entiteit nemen bij het opstellen van de voorlopige lijst van normen de standpunten van Enisa en ACER in aanmerking. Het ENTSB voor elektriciteit en de EU DSB-entiteit publiceren de overgangslijst van Europese en internationale normen en controles op hun websites.

9. Het ENTSB voor elektriciteit en de EU DSB-entiteit raadplegen Enisa en ACER over de voorstellen voor niet-bindende richtsnoeren overeenkomstig lid 1.

10. Tot het moment dat de minimale en geavanceerde cyberbeveiligingscontroles overeenkomstig artikel 29 zijn ontwikkeld en overeenkomstig artikel 8 zijn vastgesteld, streven de in artikel 2, lid 1, genoemde entiteiten ernaar geleidelijk de overeenkomstig lid 1 ontwikkelde niet-bindende richtsnoeren toe te passen.

Artikel 49

Inwerkingtreding

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Brussel, 11 maart 2024.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN