Euroopan unionin
virallinen lehti

FI
L-sarja

2024/1366

24.5.2024

KOMISSION DELEGOITU ASETUS (EU) 2024/1366,

annettu 11 päivänä maaliskuuta 2024,

Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/943 täydentämisestä vahvistamalla verkkosääntö rajat ylittävien sähkönsiirtojen kyberturvanäkökohtia koskevista toimialakohtaisista säännöistä

(ETA:n kannalta merkityksellinen teksti)

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon sähkön sisämarkkinoista 5 päivänä kesäkuuta 2019 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/943 ([1]) ja erityisesti sen 59 artiklan 2 kohdan e alakohdan,

sekä katsoo seuraavaa:

(1) Kyberturvallisuusriskien hallinta on ratkaisevan tärkeää sähkön toimitusvarmuuden ylläpitämiseksi ja kyberturvallisuuden korkean tason varmistamiseksi sähköalalla.

(2) Digitalisaatio ja kyberturvallisuus ovat ratkaisevan tärkeitä tekijöitä keskeisten palvelujen tarjoamiseksi, ja niillä on näin ollen strategista merkitystä kriittisen energiainfrastruktuurin kannalta.

(3) Euroopan parlamentin ja neuvoston direktiivissä (EU) 2022/2555 ([2]) säädetään toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa. Euroopan parlamentin ja neuvoston asetuksella (EU) 2019/941 ([3]) täydennetään direktiiviä (EU) 2022/2555 varmistamalla, että sähköalan kyberturvapoikkeamat tunnistetaan asianmukaisesti riskeiksi ja että niiden torjumiseksi toteutetut toimenpiteet otetaan asianmukaisesti huomioon riskeihinvarautumissuunnitelmissa. Asetuksella (EU) 2019/943 täydennetään direktiiviä (EU) 2022/2555 ja asetusta (EU) 2019/941 vahvistamalla erityisesti sähköalaa koskevia unionin tasoisia sääntöjä. Lisäksi tällä delegoidulla asetuksella täydennetään sähköalaa koskevia direktiivin (EU) 2022/2555 säännöksiä siltä osin kuin on kyse rajat ylittävistä sähkönsiirroista.

(4) Sähköalan yhteenliitettyjen digitalisoitujen järjestelmien tapauksessa kyberhyökkäyksiin liittyvän sähkökriisin ehkäisemistä ja hallintaa ei voida pitää yksinomaan kansallisena tehtävänä. Koko potentiaalin hyödyntämiseksi olisi kehitettävä tehokkaampia ja kustannuksiltaan alhaisempia toimenpiteitä. Tämän vuoksi tarvitaan yhteinen sääntöjen ja paremmin koordinoitujen menettelyjen kehys, jotta jäsenvaltiot ja muut tahot kykenevät tekemään toimivaa rajat ylittävää yhteistyötä jäsenvaltioiden ja sähköalasta ja kyberturvallisuudesta vastaavien toimivaltaisten viranomaisten välisen suuremman avoimuuden, luottamuksen ja yhteisvastuun hengessä.

(5) Tämän asetuksen soveltamisalaan kuuluva kyberturvariskien hallinta edellyttää jäsenneltyä prosessia, joka kattaa muun muassa kyberhyökkäyksistä johtuvien, rajat ylittäviin sähkönsiirtoihin kohdistuvien riskien tunnistamisen, tähän liittyvät käytännön prosessit ja vyöhykerajaukset sekä vastaavat kyberturvallisuuden varotoimet ja todentamismekanismit. Vaikka koko prosessi jakautuu useiden vuosien aikajänteelle, sen kunkin vaiheen olisi edistettävä alan kyberturvallisuuden yhteistä korkeaa tasoa ja osaltaan lievennettävä kyberturvallisuusriskejä. Kaikkien prosessiin osallistuvien olisi parhaansa mukaan pyrittävä kehittämään menetelmiä ja sopimaan niistä mahdollisimman pian ilman aiheetonta viivytystä ja joka tapauksessa viimeistään tässä asetuksessa määritellyissä määräajoissa.

([1]) EUVL L 158, 14.6.2019, s. 54.

([2]) Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi) (EUVL L 333, 27.12.2022, s. 80).

([3]) Euroopan parlamentin ja neuvoston asetus (EU) 2019/941, annettu 5 päivänä kesäkuuta 2019, riskeihin varautumisesta sähköalalla ja direktiivin 2005/89/EY kumoamisesta (EUVL L 158, 14.6.2019, s. 1).

(6) Tässä asetuksessa tarkoitetut unioni-, jäsenvaltio-, alue- ja toimijatason kyberturvariskien arvioinnit voidaan rajoittaa Euroopan parlamentin ja neuvoston asetuksessa (EU) 2022/2554 ([4]) määritellyistä kyberhyökkäyksistä johtuviin arviointeihin, jolloin ulkopuolelle jäävät esimerkiksi fyysiset hyökkäykset, luonnonkatastrofit ja laitosten tai henkilöresurssien menettämisestä johtuvat käyttökatkokset. Unionin laajuiset ja alueelliset sähköalan riskit, jotka liittyvät fyysisiin hyökkäyksiin tai luonnonkatastrofeihin, katetaan jo muulla voimassa olevalla unionin lainsäädännöllä, kuten asetuksen (EU) 2019/941 5 artiklalla tai sähkön siirtoverkon käyttöä koskevista suuntaviivoista annetulla komission asetuksella (EU) 2017/1485 ([5]). Vastaavasti kriittisten toimijoiden häiriönsietokyvystä annetulla Euroopan parlamentin ja neuvoston direktiivillä (EU) 2022/2557 ([6]) pyritään vähentämään kriittisten toimijoiden haavoittuvuuksia ja vahvistamaan niiden fyysistä häiriönsietokykyä, ja se kattaa kaikki asiaankuuluvat luonnon ja ihmisen aiheuttamat riskit, jotka voivat vaikuttaa keskeisten palvelujen tarjoamiseen, mukaan lukien onnettomuudet, luonnonkatastrofit, kansanterveysuhat, kuten pandemiat, hybridiuhat tai muut vihamieliset uhat, mukaan lukien terrorismirikokset, rikollisten soluttautuminen ja sabotaasi.

(7) Tässä asetuksessa käytetty ”vaikutuksiltaan merkittävien ja vaikutuksiltaan kriittisten toimijoiden” käsitepari on olennaisen tärkeä määritettäessä niiden toimijoiden joukkoa, joihin sovelletaan tässä asetuksessa kuvattuja velvoitteita. Asetuksessa hahmotellulla riskiperusteisella lähestymistavalla pyritään tunnistamaan prosessit, niitä tukevat omaisuuserät ja niitä ylläpitävät toimijat, jotka vaikuttavat rajat ylittäviin sähkönsiirtoihin. Riippuen siitä, missä määrin niihin kohdistuvat mahdolliset kyberhyökkäykset vaikuttaisivat rajat ylittäviin sähkönsiirtoihin, niitä voidaan pitää ”vaikutuksiltaan merkittävinä” tai ”vaikutuksiltaan kriittisinä”. Direktiivin (EU) 2022/2555 3 artiklassa vahvistetaan keskeisten ja tärkeiden toimijoiden käsitteet sekä perusteet, joilla toimijat sijoitetaan näihin luokkiin. Vaikka monet niistä katsotaan ja yksilöidään samanaikaisesti sekä direktiivin (EU) 2022/2555 3 artiklassa tarkoitetuiksi keskeisiksi toimijoiksi että tämän asetuksen 24 artiklan mukaisiksi vaikutuksiltaan merkittäviksi tai vaikutuksiltaan kriittisiksi toimijoiksi, tässä asetuksessa säädetyissä kriteereissä viitataan ainoastaan niiden rooliin ja vaikutukseen rajat ylittäviin sähkönsiirtoihin vaikuttavissa sähköalan prosesseissa ottamatta huomioon direktiivin (EU) 2022/2555 3 artiklassa määriteltyjä perusteita.

(8) Tämän asetuksen soveltamisalaan kuuluvat toimijat, joita pidetään tämän asetuksen 24 artiklan mukaisesti vaikutuksiltaan merkittävinä tai vaikutuksiltaan kriittisinä ja joihin sovelletaan tässä asetuksessa säädettyjä velvoitteita, ovat ensisijaisesti ne, joilla on suora vaikutus rajat ylittäviin sähkönsiirtoihin EU:ssa.

(9) Tässä asetuksessa hyödynnetään olemassa olevia mekanismeja ja välineitä, jotka on jo vahvistettu muussa lainsäädännössä, jotta varmistetaan tehokkuuden ja vältetään päällekkäisyydet pyrittäessä samoihin tavoitteisiin.

(10) Jäsenvaltioiden, asiaankuuluvien viranomaisten ja verkonhaltijoiden olisi tätä asetusta soveltaessaan otettava huomioon sovitut eurooppalaisten standardointiorganisaatioiden eurooppalaiset standardit ja tekniset eritelmät ja toimittava tuotteiden markkinoille saattamista tai käyttöönottoa koskevan unionin lainsäädännön mukaisesti.

([4]) Euroopan parlamentin ja neuvoston asetus (EU) 2022/2554, annettu 14 päivänä joulukuuta 2022, finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o 648/2012, (EU) N:o 600/2014, (EU) N:o 909/2014 ja (EU) 2016/1011 muuttamisesta (EUVL L 333, 27.12.2022, s. 1).

([5]) Komission asetus (EU) 2017/1485, annettu 2 päivänä elokuuta 2017, sähkön siirtoverkon käyttöä koskevista suuntaviivoista (EUVL L 220, 25.8.2017, s. 1).

([6]) Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2557, annettu 14 päivänä joulukuuta 2022, kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta (EUVL L 333, 27.12.2022, s. 164).

(11) Kyberturvariskien lieventämiseksi on tarpeen laatia yksityiskohtainen sääntökirja, joka koskee sellaisten sidosryhmien toimia ja yhteistyötä, joiden toiminta liittyy rajat ylittävien sähkönsiirtojen kyberturvanäkökohtiin, jotta voidaan varmistaa järjestelmän turvallisuus. Näillä organisatorisilla ja teknisillä säännöillä olisi varmistettava, että useimpiin sähköalan poikkeamiin, joiden juurisyyt liittyvät kyberturvallisuuteen, puututaan tuloksellisesti operatiivisella tasolla. On tarpeen määritellä, mitä asianomaisten sidosryhmien olisi tehtävä tällaisten kriisien ehkäisemiseksi ja mitä toimenpiteitä ne voivat toteuttaa, jos verkon operatiivisen tason säännöt eivät enää yksin riitä. Sen vuoksi on tarpeen vahvistaa yhteinen sääntökehys, joka koskee samanaikaisten sähkökriisien, joiden juurisyy liittyy kyberturvallisuuteen, ehkäisemistä, niihin varautumista ja hallintaa. Tämä lisää avoimuutta valmisteluvaiheessa ja samanaikaisen sähkökriisin aikana ja varmistaa, että toimenpiteet toteutetaan koordinoidusti ja vaikuttavasti yhdessä kyberturvallisuudesta vastaavien jäsenvaltioiden toimivaltaisten viranomaisten kanssa. Jäsenvaltioita ja asiaankuuluvia toimijoita olisi vaadittava tekemään yhteistyötä alueellisella tasolla ja tarvittaessa kahdenvälisesti yhteisvastuun hengessä. Tämän yhteistyön ja näiden sääntöjen tarkoituksena on parantaa kyberturvariskeihin varautumista pienemmin kustannuksin, myös direktiivin (EU) 2022/2555 tavoitteiden mukaisesti. Vaikuttaa myös tarpeelliselta vahvistaa sähkön sisämarkkinoita lisäämällä luottamusta jäsenvaltioiden välillä, erityisesti vähentämällä riskiä rajat ylittävien sähkönsiirtojen kohtuuttomasta rajoittamisesta ja vähentämällä siten naapurijäsenvaltioihin kohdistuvien kielteisten heijastusvaikutusten riskiä.

(12) Sähkön toimitusvarmuus edellyttää tuloksellista yhteistyötä jäsenvaltioiden, unionin toimielinten, muiden elinten, toimistojen ja virastojen sekä asiaankuuluvien sidosryhmien kesken. Jakeluverkonhaltijoilla ja siirtoverkonhaltijoilla on keskeinen rooli turvallisen, luotettavan ja tehokkaan sähköjärjestelmän varmistamisessa Euroopan parlamentin ja neuvoston direktiivin (EU) 2019/944 ([7]) 31 ja 40 artiklan mukaisesti. Eri sääntelyviranomaisilla ja muilla asiaankuuluvilla toimivaltaisilla kansallisilla viranomaisilla on myös tärkeä rooli sähköntarjonnan kyberturvallisuuden varmistamisessa ja seurannassa osana niille direktiiveissä (EU) 2019/944 ja (EU) 2022/2555 annettuja tehtäviä. Jäsenvaltioiden olisi nimettävä olemassa oleva tai uusi elin tämän asetuksen täytäntöönpanosta vastaavaksi toimivaltaiseksi kansalliseksi viranomaiseksi, jotta voidaan varmistaa kaikkien asianomaisten tahojen avoin ja kattava osallistuminen, tehokas valmistelu ja asianmukainen täytäntöönpano, eri sidosryhmien ja toimivaltaisten viranomaisten välinen yhteistyö sähköalalla ja kyberturvallisuudessa sekä helpottaa sähkökriisien, joiden juurisyy liittyy kyberturvallisuuteen, ennaltaehkäisyä ja jälkiarviointia ja niihin liittyvää tietojenvaihtoa.

(13) Kun vaikutuksiltaan merkittävä tai vaikutuksiltaan kriittinen toimija tarjoaa palveluja useammassa kuin yhdessä jäsenvaltiossa tai sillä on kotipaikka tai muu toimipaikka tai edustaja jossakin jäsenvaltiossa, mutta sen verkko- ja tietojärjestelmät sijaitsevat yhdessä tai useammassa muussa jäsenvaltiossa, kyseisten jäsenvaltioiden olisi kannustettava toimivaltaisia viranomaisiaan tekemään parhaansa mukaan yhteistyötä keskenään ja avustamaan toisiaan tarvittaessa.

(14) Jäsenvaltioiden olisi varmistettava, että toimivaltaisilla viranomaisilla on vaikutuksiltaan merkittävien ja vaikutuksiltaan kriittisten toimijoiden suhteen tarvittavat valtuudet edistää tämän asetuksen noudattamista. Näiden valtuuksien olisi mahdollistettava se, että toimivaltaiset viranomaiset voivat tehdä tarkastuksia paikan päällä ja harjoittaa ulkopuolista valvontaa. Tähän voi sisältyä satunnaistarkastuksia, säännöllisiä auditointeja, riskinarviointeihin tai riskeihin liittyviin saatavilla oleviin tietoihin perustuvia kohdennettuja turvallisuusauditointeja ja turvaskannauksia, jotka perustuvat puolueettomiin, syrjimättömiin, oikeudenmukaisiin ja läpinäkyviin riskinarviointikriteereihin ja joihin sisältyy sellaisten tietojen pyytäminen, joita tarvitaan toimijan toteuttamien kyberturvatoimenpiteiden arvioimiseksi. Näihin tietoihin olisi sisällyttävä dokumentoidut kyberturvaperiaatteet, käyttöoikeus- ja kulunvalvontadata, asiakirjat tai muut tiedot, jotka ovat tarpeen valvontatehtävien suorittamiseksi, sekä näyttö kyberturvaperiaatteiden noudattamisesta, kuten pätevän tarkastajan tekemien turvallisuustarkastusten tulokset ja niiden pohjana oleva näyttö.

([7]) Euroopan parlamentin ja neuvoston direktiivi (EU) 2019/944, annettu 5 päivänä kesäkuuta 2019, sähkön sisämarkkinoita koskevista yhteisistä säännöistä ja direktiivin 2012/27/EU muuttamisesta (EUVL L 158, 14.6.2019, s. 125).

(15) Jotta vältetään vaikutuksiltaan merkittäville ja vaikutuksiltaan kriittisille toimijoille asetettujen kyberturvariskien hallintaa koskevien velvoitteiden aukot tai päällekkäisyydet, direktiivin (EU) 2022/2555 mukaisten kansallisten viranomaisten ja tämän asetuksen mukaisten toimivaltaisten viranomaisten olisi tehtävä yhteistyötä kyberturvariskien hallintatoimenpiteiden täytäntöönpanossa ja näiden toimenpiteiden noudattamisen valvonnassa kansallisella tasolla. Direktiivin (EU) 2022/2555 mukaiset toimivaltaiset viranomaiset voisivat katsoa, että jos toimija täyttää tässä asetuksessa säädetyt kyberturvariskien hallintavaatimukset, se täyttää myös mainitussa direktiivissä säädetyt vastaavat vaatimukset, tai päinvastoin.

(16) Yhteinen lähestymistapa samanaikaisten sähkökriisien ehkäisyyn ja hallintaan edellyttää jäsenvaltioiden yhteisymmärrystä siitä, mikä on samanaikainen sähkökriisi ja milloin kyberhyökkäys on siinä tärkeä tekijä. Jäsenvaltioiden ja asiaankuuluvien toimijoiden välistä koordinointia olisi helpotettava, jotta voidaan puuttua tilanteeseen, jossa vallitsee tai välittömästi uhkaa kyberhyökkäyksestä johtuva riski merkittävästä sähköpulasta tai kyvyttömyydestä toimittaa sähköä asiakkaille.

(17) Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 ([8]) johdanto-osan 1 kappaleessa tunnustetaan verkko- ja tietojärjestelmien sekä sähköisen viestinnän verkkojen ja palvelujen elintärkeä rooli talouden toiminnan tukena keskeisillä aloilla, kuten energia-alalla, kun taas johdanto-osan 44 kappaleessa selitetään, että Euroopan unionin kyberturvallisuusviraston (ENISA) olisi oltava yhteydessä Euroopan unionin energia-alan sääntelyviranomaisten yhteistyövirastoon (ACER).

(18) Asetuksessa (EU) 2019/943 osoitetaan erityisiä kyberturvallisuuteen liittyviä vastuita siirtoverkonhaltijoille ja jakeluverkonhaltijoille. Niiden eurooppalaisten kattojärjestöjen eli sähkön siirtoverkonhaltijoiden eurooppalaisen verkoston, jäljempänä 'Sähkö-ENTSO', ja jakeluverkonhaltijoiden eurooppalaisen elimen, jäljempänä 'EU DSO -elin', on mainitun asetuksen 30 ja 55 artiklan nojalla edistettävä kyberturvallisuutta yhteistyössä asiaankuuluvien viranomaisten ja säänneltyjen toimijoiden kanssa.

(19) Yhteinen lähestymistapa sellaisten samanaikaisten sähkökriisien ehkäisemiseen ja hallintaan, joiden juurisyy liittyy kyberturvallisuuteen, edellyttää myös, että kaikki asiaankuuluvat sidosryhmät käyttävät yhdenmukaistettuja menetelmiä ja määritelmiä sähköntarjonnan kyberturvallisuuteen liittyvien riskien tunnistamiseksi. Eri toimijoiden on myös kyettävä tosiasiallisesti suorittamaan vertailuja siitä, miten hyvin ne itse ja niiden naapuriverkot suoriutuvat tässä asiassa. Sen vuoksi on tarpeen vahvistaa prosessit, roolit ja vastuut, jotta voidaan kehittää ja päivittää riskinhallintamenetelmiä, poikkeamaluokituksia ja kyberturvatoimenpiteitä, joilla voidaan vastata nimenomaan rajat ylittäviin sähkönsiirtoihin vaikuttaviin kyberturvariskeihin.

(20) Jäsenvaltiot vastaavat tätä asetusta varten nimetyn toimivaltaisen viranomaisen välityksellä niiden toimijoiden yksilöimisestä, jotka täyttävät vaikutuksiltaan merkittävän ja vaikutuksiltaan kriittisen toimijan kriteerit. Jotta voidaan poistaa asiaan liittyvät jäsenvaltioiden väliset erot ja varmistaa oikeusvarmuus kaikkien asianomaisten toimijoiden kyberturvallisuusriskien hallintatoimenpiteiden ja raportointivelvoitteiden osalta, olisi vahvistettava kriteerit, jolla määritetään tämän asetuksen soveltamisalaan kuuluvat toimijat. Nämä kriteerit olisi vahvistettava ja niitä olisi päivitettävä säännöllisesti tässä asetuksessa säädetyn, ehtojen ja menetelmien laadintaa ja hyväksymistä koskevan prosessin avulla.

(21) Tämän asetuksen säännökset eivät saisi rajoittaa sellaisen unionin lainsäädännön soveltamista, jossa säädetään tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sertifiointia koskevista erityissäännöistä, eivätkä varsinkaan asetuksen (EU) 2019/881 soveltamista eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien perustamista koskevan kehyksen osalta. Tämän asetuksen yhteydessä tieto- ja viestintätekniikan tuotteisiin olisi sisällyttävä myös tekniset laitteet ja ohjelmistot, jotka mahdollistavat suoran vuorovaikutuksen sähköteknisen verkon kanssa, erityisesti teollisuuden ohjausjärjestelmät, joita voidaan käyttää energian siirtoon, energian jakeluun ja energian tuotantoon sekä asiaan liittyvän tiedon keräämiseen ja siirtämiseen. Säännöksillä olisi varmistettava, että hankittavat tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit täyttävät asetuksen (EU) 2019/881 51 artiklan asiaankuuluvat turvallisuustavoitteet.

([8]) Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus) (EUVL L 151, 7.6.2019, s. 15).

(22) Viimeaikaiset kyberhyökkäykset osoittavat, että toimijoista on tulossa enenevässä määrin toimitusketjuun kohdistuvien hyökkäysten kohteita. Tällaiset toimitusketjuun suunnatut hyökkäykset eivät vaikuta ainoastaan kohteena oleviin yksittäisiin toimijoihin, vaan niillä voi olla myös suuremmaksi hyökkäykseksi muodostuvia kerrannaisvaikutuksia toimijoihin, joihin alkuperäinen kohde on liitetty verkon välityksellä. Sen vuoksi asetukseen on otettu mukaan säännöksiä ja suosituksia, joilla autetaan lieventämään toimitusketjun prosesseihin, erityisesti hankintoihin, liittyviä kyberturvariskejä, jotka vaikuttavat rajat ylittäviin sähkönsiirtoihin.

(23) Koska verkko- ja tietojärjestelmien haavoittuvuuksien hyväksikäyttö voi aiheuttaa merkittäviä energiakatkoksia ja haittaa taloudelle ja kuluttajille, nämä haavoittuvuudet olisi kyettävä nopeasti tunnistamaan ja paikkaamaan. Tämän asetuksen tuloksellisen täytäntöönpanon helpottamiseksi asiaankuuluvien toimijoiden ja toimivaltaisten viranomaisten olisi tehtävä yhteistyötä harjoitellakseen ja testatakseen tähän tarkoitukseen tarkoituksenmukaisiksi katsottuja toimia, mukaan lukien tietojenvaihto kyberuhkista, kyberhyökkäyksistä, haavoittuvuuksista, välineistä ja menetelmistä, taktiikoista, tekniikoista ja menettelyistä, kyberturvakriisinhallintavalmiudesta ja muista harjoituksista. Koska teknologia kehittyy jatkuvasti ja sähköalan digitalisointi etenee nopeasti, tämän asetuksen säännösten täytäntöönpano ei saisi haitata innovointia eikä muodostaa estettä sähkömarkkinoille pääsylle ja myöhemmälle sähköjärjestelmän tehokkuutta ja kestävyyttä edistävien innovatiivisten ratkaisujen käytölle.

(24) Tämän asetuksen täytäntöönpanon seurantaa varten kerättyjen tietojen saatavuutta olisi kohtuudella rajoitettava tiedonsaantitarpeen periaatteen mukaisesti. Sidosryhmille olisi sallittava noudattamiskelpoiset ja toimivat määräajat tällaisten tietojen toimittamiselle. Päällekkäisiä raportointivaatimuksia olisi vältettävä.

(25) Kyberturvallisuuden ylläpito edellyttää yhteistyötä unionin ulkorajojen yli. Järjestelmätason turvallisuuden saavuttaminen edellyttää EU:n naapurimaiden osallistamista. Unionin ja sen jäsenvaltioiden olisi pyrittävä tukemaan niitä EU:n naapurimaita, joiden sähköinfrastruktuuri on liitetty eurooppalaiseen verkkoon, tässä asetuksessa säädettyjen sääntöjen kaltaisten kyberturvasääntöjen käytössä.

(26) Sähkö-ENTSOn, EU DSO -elimen ja toimivaltaisten viranomaisten olisi aloitettava ei-sitovan ohjeistuksen laatiminen välittömästi tämän asetuksen voimaantulon jälkeen, jotta voidaan parantaa turvallisuusasioiden koordinointia jo varhaisessa vaiheessa ja testata tulevaisuudessa sitoviksi tulevia ehtoja ja menetelmiä. Tämä ohjeistus tulee toimimaan pohjana tulevien ehtojen ja menetelmien laadinnalle. Samaan aikaan toimivaltaisten viranomaisten olisi yksilöitävä ehdokkaat vaikutuksiltaan merkittäviksi ja vaikutuksiltaan kriittisiksi toimijoiksi, jotta nämä voisivat mahdollisimman pian vapaaehtoisuuden pohjalta alkaa noudattamaan tulevia velvoitteitaan.

(27) Tämä asetus on laadittu tiiviissä yhteistyössä ACERin, ENISAn, Sähkö-ENTSOn, EU DSO -elimen ja muiden sidosryhmien kanssa, jotta voidaan vahvistaa toimivat, tasapainoiset ja oikeasuhteiset säännöt läpinäkyvällä ja osallistavalla tavalla.

(28) Tällä asetuksella täydennetään ja tehostetaan komission suosituksen (EU) 2017/1584 ([9]) mukaisessa EU:n kyberturvallisuuden kriisinhallintakehyksessä vahvistettuja kriisinhallintatoimenpiteitä. Kyberhyökkäys voisi aiheuttaa myös asetuksen (EU) 2019/941 2 artiklan 9 alakohdassa määritellyn sähkökriisin, myötävaikuttaa siihen tai osua samaan aikaan sen kanssa tavalla, joka vaikuttaa rajat ylittäviin sähkönsiirtoihin. Se voisi johtaa asetuksen (EU) 2019/941 2 artiklan 10 alakohdassa määritellyn kaltaiseen samanaikaiseen sähkökriisiin. Tämänkaltainen poikkeustilanne voisi vaikuttaa myös sähkön toimitusvarmuudesta riippuvaisiin muihin toimialoihin. Jos tällainen poikkeustilanne eskaloituisi direktiivin (EU) 2022/2555 16 artiklassa tarkoitetuksi laajamittaiseksi kyberturvallisuuspoikkeamaksi, olisi sovellettava kyseisen artiklan säännöksiä Euroopan kyberkriisien yhteysorganisaatioiden verkoston, jäljempänä 'EU-CyCLONe', perustamisesta. Unionitason kriisinhallinnassa asianomaisten osapuolten olisi hyödynnettävä EU:n poliittisen kriisitoiminnan integroituja järjestelyjä (ns. 'IPCR-järjestelyjä'), joista säädetään neuvoston täytäntöönpanopäätöksessä (EU) 2018/1993 ([10]).

(29) Tällä asetuksella ei rajoiteta jäsenvaltioiden toimivaltaa toteuttaa tarvittavat toimenpiteet keskeisten turvallisuusetujensa suojaamiseksi, yleisen järjestyksen ja turvallisuuden takaamiseksi sekä rikosten tutkinnan, selvittämisen ja syytteeseenpanon mahdollistamiseksi unionin oikeuden mukaisesti. SEUT-sopimuksen 346 artiklan mukaisesti mitään jäsenvaltiota ei saa velvoittaa antamaan tietoja, joiden ilmaisemisen se katsoo keskeisten turvallisuusetujensa vastaiseksi.

([9]) Komission suositus (EU) 2017/1584, annettu 13 päivänä syyskuuta 2017, koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin (EUVL L 239, 19.9.2017, s. 36).

([10]) Neuvoston täytäntöönpanopäätös (EU) 2018/1993, annettu 11 päivänä joulukuuta 2018, EU:n poliittisen kriisitoiminnan integroiduista järjestelyistä (EUVL L 320, 17.12.2018, s. 28).

(30) Vaikka tätä asetusta sovelletaan periaatteessa toimijoihin, jotka toteuttavat ydinvoimaloiden sähköntuotantoon liittyviä toimintoja, jotkin kyseisistä toiminnoista voivat liittyä kansalliseen turvallisuuteen.

(31) Kaikkeen tämän asetuksen mukaiseen henkilötietojen käsittelyyn olisi sovellettava unionin tietosuojalainsäädäntöä ja yksityisyyden suojaa koskevaa unionin lainsäädäntöä. Tämä asetus ei etenkään rajoita Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 ([11]), Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY ([12]) ja Euroopan parlamentin ja neuvoston asetuksen (EU) 2018/1725 ([13]) soveltamista. Tämä asetus ei sen vuoksi saisi vaikuttaa muun muassa niiden viranomaisten tehtäviin ja valtuuksiin, jotka ovat toimivaltaisia valvomaan sovellettavan unionin tietosuojalainsäädännön ja yksityisyyden suojaa koskevan unionin lainsäädännön noudattamista.

(32) Koska kansainvälinen yhteistyö on kyberturvallisuusasioissa niin tärkeää, jäsenvaltioiden nimeämien toimivaltaisten viranomaisten, jotka vastaavat niille tämän asetuksen nojalla osoitetuista tehtävistä, olisi voitava osallistua kansainvälisiin yhteistyöverkostoihin. Sen vuoksi toimivaltaisten viranomaisten olisi tehtäviensä hoitamiseksi voitava vaihtaa tietoja, myös henkilötietoja, EU:n ulkopuolisten maiden toimivaltaisten viranomaisten kanssa edellyttäen, että unionin tietosuojalainsäädännön mukaiset henkilötietojen siirtoa EU:n ulkopuolelle koskevat edellytykset, muun muassa asetuksen (EU) 2016/679 49 artiklassa säädetyt edellytykset, täyttyvät.

(33) Vaikutuksiltaan merkittävien ja vaikutuksiltaan kriittisten toimijoiden suorittamaa henkilötietojen käsittelyä, siinä määrin kuin se on tarpeen ja oikeasuhteista niiden omaisuuserien turvallisuuden varmistamiseksi, voitaisiin pitää lainmukaisena sillä perusteella, että se on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi asetuksen (EU) 2016/679 6 artiklan 1 kohdan c alakohdan ja 6 artiklan 3 kohdan vaatimusten mukaisesti. Henkilötietojen käsittely voi olla tarpeen myös vaikutuksiltaan merkittävien ja vaikutuksiltaan kriittisten toimijoiden sekä niiden puolesta toimivien turvallisuusteknologioiden ja -palvelujen tarjoajien oikeutettujen etujen perusteella asetuksen (EU) 2016/679 6 artiklan 1 kohdan f alakohdan mukaisesti, myös silloin, kun tällainen käsittely on tarpeen tämän asetuksen mukaisia kyberturvallisuustietojen jakamisjärjestelyjä tai asiaankuuluvien tietojen vapaaehtoista ilmoittamista varten. Toimenpiteet, jotka liittyvät kyberhyökkäysten ehkäisemiseen, havaitsemiseen, tunnistamiseen, rajoittamiseen, analysointiin ja hallitsemiseen, toimenpiteet yksittäisistä kyberuhkista tiedottamiseksi, haavoittuvuuden korjaamiseen ja koordinoituun haavoittuvuuden julkistamiseen liittyvä tietojenvaihto sekä vapaaehtoinen tietojenvaihto kyseisistä kyberhyökkäyksistä, kyberuhkista ja haavoittuvuuksista, vaarantumisindikaattoreista, taktiikasta, tekniikoista ja menettelyistä, kyberturvallisuushälytyksistä ja konfigurointityökaluista, saattavat edellyttää tiettyjen henkilötietoryhmien, kuten IP-osoitteiden, URL-osoitteiden, verkkotunnusten, sähköpostiosoitteiden ja, sikäli kuin niistä käy ilmi henkilötietoja, aikaleimojen käsittelyä. Toimivaltaisten viranomaisten, keskitettyjen yhteyspisteiden ja CSIRT-yksiköiden suorittamaa henkilötietojen käsittelyä voidaan pitää lakisääteisenä velvoitteena tai sen voidaan katsoa olevan tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi asetuksen (EU) 2016/679 6 artiklan 1 kohdan c tai e alakohdan ja 6 artiklan 3 kohdan mukaisesti taikka vaikutuksiltaan merkittävien tai vaikutuksiltaan kriittisten toimijoiden oikeutettujen etujen toteuttamiseksi asetuksen (EU) 2016/679 6 artiklan 1 kohdan f alakohdan mukaisesti. Lisäksi kansallisessa lainsäädännössä saatetaan vahvistaa sääntöjä, joiden nojalla toimivaltaiset viranomaiset, keskitetyt yhteyspisteet ja CSIRT-yksiköt voivat, siinä määrin kuin se on tarpeen ja oikeasuhteista vaikutuksiltaan merkittävien tai vaikutuksiltaan kriittisten toimijoiden verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi, käsitellä erityisiä henkilötietoryhmiä asetuksen (EU) 2016/679 9 artiklan mukaisesti, erityisesti säätämällä asianmukaisista erityistoimenpiteistä luonnollisten henkilöiden perusoikeuksien ja etujen suojaamiseksi, myös tällaisten tietojen uudelleenkäyttöä koskevista teknisistä rajoituksista sekä viimeisintä kehitystä edustavien turvallisuustoimenpiteiden ja yksityisyyden suojan säilyttävien toimenpiteiden, kuten pseudonymisoinnin, käytöstä tai salauksen käytöstä, jos anonymisointi voi vaikuttaa merkittävästi aiottuun käyttötarkoitukseen.

([11]) Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (EUVL L 119, 4.5.2016, s. 1).

([12]) Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi) (EUVL L 201, 31.7.2002, s. 37).

([13]) Euroopan parlamentin ja neuvoston asetus (EU) 2018/1725, annettu 23 päivänä lokakuuta 2018, luonnollisten henkilöiden suojelusta unionin toimielinten, elinten ja laitosten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta sekä asetuksen (EY) N:o 45/2001 ja päätöksen N:o 1247/2002/EY kumoamisesta (EUVL L 295, 21.11.2018, s. 39).

(34) Kyberhyökkäykset vaarantavat monissa tapauksissa henkilötietojen suojan. Niinpä toimivaltaisten viranomaisten olisi tehtävä yhteistyötä ja vaihdettava tietoja kaikista merkityksellisistä asioista asetuksessa (EU) 2016/679 ja direktiivissä 2002/58/EY tarkoitettujen viranomaisten kanssa.

(35) Euroopan tietosuojavaltuutettua on kuultu asetuksen (EU) 2018/1725 42 artiklan 1 kohdan mukaisesti, ja hän on antanut lausunnon 17 päivänä marraskuuta 2023,

ON HYVÄKSYNYT TÄMÄN ASETUKSEN:

I LUKU

YLEISET SÄÄNNÖKSET

1 artikla

Kohde

Tässä asetuksessa vahvistetaan verkkosääntö, jossa esitetään rajat ylittäviä sähkönsiirtoja koskevat toimialakohtaiset kyberturvasäännöt, kuten säännöt yhteisistä vähimmäisvaatimuksista, suunnittelusta, seurannasta, raportoinnista ja kriisinhallinnasta.

2 artikla

Soveltamisala

1. Tätä asetusta sovelletaan rajat ylittävien sähkönsiirtojen kyberturvanäkökohtiin seuraavien toimijoiden toiminnassa, jos ne on määritelty 24 artiklan mukaisesti vaikutuksiltaan merkittäviksi tai vaikutuksiltaan kriittisiksi toimijoiksi:

a) sähköalan yritykset, siten kuin ne on määritelty direktiivin (EU) 2019/944 2 artiklan 57 alakohdassa;

b) nimitetyt sähkömarkkinaoperaattorit, siten kuin ne on määritelty direktiivin (EU) 2019/943 2 artiklan 8 alakohdassa;

c) organisoidut markkinapaikat tai komission täytäntöönpanoasetuksen (EU) N:o 1348/2014 ([14]) 2 artiklan 4 alakohdassa määritellyt 'järjestäytyneet markkinapaikat' tai 'järjestäytyneet markkinat', jotka järjestävät rajat ylittävien sähkönsiirtojen kannalta merkityksellisiä tuotteita koskevia liiketoimia;

d) tämän asetuksen 3 artiklan 9 alakohdassa tarkoitetut kriittiset tieto- ja viestintätekniikan palveluntarjoajat;

e) asetuksen (EU) 2019/943 28 artiklan nojalla perustettu Sähkö-ENTSO;

f) asetuksen (EU) 2019/943 52 artiklan nojalla perustettu EU DSO -elin;

g) tasevastaavat, siten kuin ne on määritelty (EU) 2019/943 2 artiklan 14 alakohdassa;

h) direktiivin (EU) 2022/2555 liitteessä I määritellyt latauspisteiden operaattorit,

i) asetuksen (EU) 2019/943 35 artiklan nojalla perustetut alueelliset koordinointikeskukset;

j) direktiivin (EU) 2022/2555 6 artiklan 40 alakohdassa määritellyt tietoturvapalveluntarjoajat; ja

k) muut toimijat tai kolmannet osapuolet, joille on delegoitu tai osoitettu tämän asetuksen mukaisia vastuita.

2. Seuraavilla viranomaisilla on nykyisten toimeksiantojensa puitteissa vastuita tässä asetuksessa osoitettujen tehtävien suorittamiseen liittyen:

a) Euroopan parlamentin ja neuvoston asetuksella (EU) 2019/942 ([15]) perustettu Euroopan energia-alan sääntelyviranomaisten yhteistyövirasto, jäljempänä 'ACER';

b) jäsenvaltioiden tämän asetuksen 4 artiklan nojalla nimeämät kansalliset toimivaltaiset viranomaiset, jotka vastaavat niille tämän asetuksen nojalla annettujen tehtävien suorittamisesta, jäljempänä 'toimivaltaiset viranomaiset';

c) kunkin jäsenvaltion direktiivin (EU) 2019/944 57 artiklan 1 kohdan nojalla nimeämät kansalliset sääntelyviranomaiset;

([14]) Komission täytäntöönpanoasetus (EU) N:o 1348/2014, annettu 17 päivänä joulukuuta 2014, tietojen ilmoittamisesta energian tukkumarkkinoiden eheydestä ja tarkasteltavuudesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1227/2011 8 artiklan 2 ja 6 kohdan täytäntöönpanemiseksi (EUVL L 363, 18.12.2014, s. 121).

([15]) Euroopan parlamentin ja neuvoston asetus (EU) 2019/942, annettu 5 päivänä kesäkuuta 2019, Euroopan unionin energia-alan sääntelyviranomaisten yhteistyöviraston perustamisesta (EUVL L 158, 14.6.2019, s. 22).

d) asetuksen (EU) 2019/941 3 artiklan nojalla perustetut riskeihin varautumisesta vastaavat toimivaltaiset viranomaiset;

e) direktiivin (EU) 2022/2555 10 artiklan nojalla nimetyt tai perustetut tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt, jäljempänä 'CSIRT-yksiköt';

f) direktiivin (EU) 2022/2555 8 artiklan nojalla nimetyt tai perustetut kyberturvallisuudesta vastaavat toimivaltaiset viranomaiset;

g) asetuksen (EU) 2019/881 nojalla perustettu Euroopan unionin kyberturvallisuusvirasto; ja

h) muut viranomaiset tai kolmannet osapuolet, joille on delegoitu tai osoitettu vastuita tämän asetuksen 4 artiklan 3 kohdan nojalla.

3. Tätä asetusta sovelletaan myös kaikkiin toimijoihin, jotka eivät ole sijoittautuneet unioniin, mutta jotka tarjoavat palveluja toimijoille unionissa edellyttäen, että toimivaltaiset viranomaiset ovat yksilöineet ne 24 artiklan 2 kohdan nojalla vaikutuksiltaan merkittäviksi tai vaikutuksiltaan kriittisiksi toimijoiksi.

4. Tämä asetus ei vaikuta jäsenvaltioiden velvollisuuteen taata kansallinen turvallisuus eikä niiden valtuuksiin huolehtia muista keskeisistä valtion tehtävistä, myös valtion alueellisen koskemattomuuden turvaamisesta ja yleisen järjestyksen ylläpitämisestä.

5. Tämä asetus ei vaikuta perussopimusten mukaiseen jäsenvaltioiden velvollisuuteen taata kansallinen turvallisuus, kun on kyse sähköntuotannosta ydinvoimaloissa, mukaan lukien koko ydinalan arvoketju.

6. Toimijat, toimivaltaiset viranomaiset, toimijoiden keskitetyt yhteyspisteet ja CSIRT-yksiköt käsittelevät henkilötietoja siinä määrin kuin se on tarpeen tämän asetuksen soveltamiseksi ja asetuksen (EU) 2016/679 mukaisesti, ja tällaisen käsittelyn on oltava erityisesti viimeksi mainitun asetuksen 6 artiklan mukaista.

3 artikla

Määritelmät

Tässä asetuksessa tarkoitetaan:

1) 'omaisuuserällä' mitä tahansa verkko- ja tietojärjestelmissä olevaa aineellista tai aineetonta tietoa, ohjelmistoa tai laitteistoa, jolla on arvoa yksityishenkilölle, organisaatiolle tai valtiolle;

2) 'riskeihin varautumisesta vastaavalla toimivaltaisella viranomaisella' asetuksen (EU) 2019/941 3 artiklan nojalla nimettyä toimivaltaista viranomaista;

3) 'CSIRT-yksiköllä' yksikköä, joka vastaa riskien ja poikkeamien käsittelystä direktiivin (EU) 2022/2555 10 artiklan mukaisesti;

4) 'vaikutuksiltaan kriittisellä omaisuuserällä' omaisuuserää, joka on välttämätön vaikutuksiltaan kriittisen prosessin läpiviemiseksi;

5) 'vaikutuksiltaan kriittisellä toimijalla' toimijaa, joka vastaa vaikutuksiltaan kriittisestä prosessista ja jonka toimivaltaiset viranomaiset ovat sellaiseksi 24 artiklan nojalla yksilöineet;

6) 'kriittisten vaikutusten vyöhykkeellä' 2 artiklan 1 kohdassa tarkoitetun toimijan määrittelemää vyöhykettä, joka sisältää kaikki vaikutuksiltaan kriittiset omaisuuserät, jonka sisällä mahdollisuutta päästä käsiksi näihin omaisuuseriin voidaan valvoa ja joka määrittää tiukemmin kyberturvavarotoimin suojatun alueen;

7) 'vaikutuksiltaan kriittisellä prosessilla' toimijan prosessia, jonka sähköalan kyberturvavaikutusindeksit ylittävät kriittisten vaikutusten kynnystason;

8) 'kriittisten vaikutusten kynnystasolla' 19 artiklan 3 kohdan b alakohdassa tarkoitettujen sähköalan kyberturvavaikutusindeksien (ECII) arvoja, joiden ylittyessä prosessiin kohdistuva kyberhyökkäys aiheuttaa kriittisiä häiriöitä rajat ylittäville sähkönsiirroille;

9) 'kriittisellä tieto- ja viestintätekniikan palveluntarjoajalla' rajat ylittävien sähkönsiirtojen kyberturvaan kohdistuvilta vaikutuksiltaan kriittisen tai merkittävän prosessin kannalta välttämättömän tieto- tai viestintäteknisen palvelun tai tieto- tai viestintäteknisen prosessin tuottavaa toimijaa, jonka tuottaman palvelun tai prosessin vaarantuminen voi johtaa kyberhyökkäykseen, jonka vaikutukset ylittävät kriittisten tai merkittävien vaikutusten kynnystason;

10) 'rajat ylittävällä sähkönsiirrolla' rajat ylittävää siirtoa siten kuin se on määritelty asetuksen (EU) 2019/943 2 artiklan 3 alakohdassa;

11) 'kyberhyökkäyksellä' asetuksen (EU) 2022/2554 3 artiklan 14 alakohdassa määriteltyä poikkeamaa;

12) 'kyberturvallisuudella' ja 'kyberturvalla' kyberturvallisuutta siten kuin se on määritelty asetuksen (EU) 2019/881 2 artiklan 1 alakohdassa;

13) ’kyberturvavarotoimilla’ toimia tai menettelyjä, joiden tarkoituksena on välttää, havaita, torjua tai minimoida kyberturvariskejä;

14) ’kyberturvapoikkeamalla’ poikkeamaa siten kuin se on määritelty direktiivin (EU) 2022/2555 6 artiklan 6 alakohdassa;

15) ’kyberturvallisuuden hallintajärjestelmällä’ toimintaperiaatteita, menettelyjä, ohjeistoja ja niihin liittyviä resursseja ja toimintoja, joita toimija hallinnoi kokonaisuutena tietovarantojensa suojaamiseksi kyberuhkilta luomalla, toteuttamalla, valvomalla, seuraamalla, uudelleentarkastelemalla, ylläpitämällä ja parantamalla järjestelmällisesti verkko- ja tietojärjestelmiensä tietoturvaa;

16) ’kyberturvaoperaatiokeskuksella’ erityistä keskusta, jossa yhdestä tai useammasta asiantuntijasta koostuva tekninen ryhmä hoitaa kyberturvatietojärjestelmien tuella tietoturvaan liittyviä tehtäviä, kuten käsittelee kyberhyökkäyksiä ja tietoturvakonfiguraatiovirheitä, seuraa tietoturvatilannetta, analysoi lokitietoja ja pyrkii havaitsemaan kyberhyökkäyksiä;

17) ’kyberuhkalla’ kyberuhkaa siten kuin se on määritelty asetuksen (EU) 2019/881 2 artiklan 8 alakohdassa;

18) ’kyberturvahaavoittuvuuksien hallinnalla’ pyrkimystä haavoittuvuuksien tunnistamiseen ja korjaamiseen;

19) ’toimijalla’ toimijaa siten kuin se on määritelty direktiivin (EU) 2022/2555 6 artiklan 38 alakohdassa;

20) ’ennakkovaroituksella’ tarvittavia tietoja siitä, epäilläänkö huomattavan poikkeaman johtuvan laittomista tai vihamielisistä teoista tai voiko sillä olla rajat ylittäviä vaikutuksia;

21) ’sähköalan kyberturvavaikutusindeksillä (ECII)’ indeksiä tai luokitusasteikkoa, jolla asetetaan merkittävyysjärjestykseen kyberhyökkäysten mahdolliset seuraukset rajat ylittäviin sähkövirtoihin liittyville prosesseille;

22) ’eurooppalaisella kyberturvallisuuden sertifiointijärjestelmällä’ asetuksen (EU) 2019/881 2 artiklan 9 alakohdassa määriteltyä järjestelmää;

23) ’vaikutuksiltaan merkittävällä toimijalla’ toimijaa, joka vastaa vaikutuksiltaan merkittävästä prosessista ja jonka toimivaltaiset viranomaiset ovat sellaiseksi 24 artiklan nojalla yksilöineet;

24) ’vaikutuksiltaan merkittävällä prosessilla’ toimijan prosessia, jonka sähköalan kyberturvavaikutusindeksit (ECII) ylittävät merkittävien vaikutusten kynnystason;

25) ’vaikutuksiltaan merkittävällä omaisuuserällä’ omaisuuserää, joka on välttämätön vaikutuksiltaan merkittävän prosessin läpiviemiseksi;

26) ’merkittävien vaikutusten kynnystasolla’ 19 artiklan 3 kohdan b alakohdassa tarkoitettujen sähköalan kyberturvavaikutusindeksien (ECII) arvoja, joiden ylittyessä prosessiin kohdistuva kyberhyökkäys onnistuessaan aiheuttaa merkittäviä häiriöitä rajat ylittäville sähkönsiirroille;

27) ’merkittävien vaikutusten vyöhykkeellä’ 2 artiklan 1 kohdassa tarkoitetun toimijan määrittelemää vyöhykettä, joka sisältää kaikki vaikutuksiltaan merkittävät omaisuuserät, jonka sisällä mahdollisuutta päästä käsiksi näihin omaisuuseriin voidaan valvoa ja joka määrittää vähimmäistason kyberturvavarotoimin suojatun alueen;

28) ’tieto- ja viestintätekniikan tuotteella’ tieto- ja viestintätekniikan tuotetta siten kuin se on määritelty asetuksen (EU) 2019/881 2 artiklan 12 alakohdassa;

29) ’tieto- ja viestintätekniikan palvelulla’ tieto- ja viestintätekniikan palvelua siten kuin se on määritelty asetuksen (EU) 2019/881 2 artiklan 13 alakohdassa;

30) ’tieto- ja viestintätekniikan prosessilla’ tieto- ja viestintätekniikan prosessia siten kuin se on määritelty asetuksen (EU) 2019/881 2 artiklan 14 alakohdassa;

31) ’aiemman sukupolven järjestelmällä’ aiemman sukupolven tieto- ja viestintäteknistä järjestelmää siten kuin se on määritelty asetuksen (EU) 2022/2554 3 artiklan 3 alakohdassa;

32) ’kansallisella keskitetyllä yhteyspisteellä’ keskitettyä yhteyspistettä, jonka kukin jäsenvaltio on nimennyt tai perustanut direktiivin (EU) 2022/2555 8 artiklan 3 kohdan nojalla;

33) ’verkko- ja tietoturvan kyberkriisinhallintaviranomaisilla’ direktiivin (EU) 2022/2555 9 artiklan 1 kohdan nojalla nimettyjä tai perustettuja viranomaisia;

34) ’tietojen alkuperällä’ toimijaa, joka käynnistää tiedonvaihto-, tiedonjako- tai tiedontallennustapahtuman;

35) ’hankintaeritelmillä’ eritelmiä, jotka toimijat määrittelevät uusien tai päivitettyjen tieto- ja viestintätekniikan tuotteiden, prosessien tai palvelujen hankintaa varten;

36) ’edustajalla’ unioniin sijoittautunutta luonnollista tai oikeushenkilöä, joka on nimenomaisesti nimetty toimimaan sellaisen vaikutuksiltaan merkittävän tai vaikutuksiltaan kriittisen toimijan puolesta, joka ei ole sijoittautunut unioniin mutta joka tarjoaa palveluja toimijoille unionissa, ja johon toimivaltainen viranomainen tai CSIRT-yksikkö voi vaikutuksiltaan merkittävän tai vaikutuksiltaan kriittisen toimijan sijaan olla yhteydessä kyseisen toimijan tämän asetuksen mukaisten velvoitteiden osalta;

37) ’riskillä’ riskiä siten kuin se on määritelty direktiivin (EU) 2022/2555 6 artiklan 9 alakohdassa;

38) ’riskivaikutusmatriisilla’ matriisia, jota käytetään riskinarvioinnin aikana määritettäessä kunkin arvioidun riskin riskivaikutustaso;

39) ’samanaikaisella sähkökriisillä’ sähkökriisiä siten kuin se on määritelty asetuksen (EU) 2019/941 2 artiklan 10 alakohdassa;

40) ’toimijan keskitetyllä yhteyspisteellä’ 38 artiklan 1 kohdan c alakohdan nojalla nimettyä toimijan keskitettyä yhteyspistettä;

41) ’sidosryhmällä’ mitä tahansa osapuolta, jolla on intressi organisaation tai prosessin onnistumiseen ja jatkuvaan toimintaan, kuten työntekijät, johtajat, osakkeenomistajat, sääntelyviranomaiset, järjestöt, alihankkijat ja asiakkaat;

42) ’standardilla’ standardia siten kuin se on määritelty Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 1025/2012 ([16]) 2 artiklan 1 alakohdassa;

43) ’käyttöalueella’ käyttöalueita siten kuin ne on määritelty asetuksen (EU) 2019/943 36 artiklan mukaisen, käyttöalueiden määrittelystä tehdyn ACERin päätöksen 05–2022 liitteessä I;

44) ’verkonhaltijoilla’ direktiivin (EU) 2019/944 2 artiklan 29 ja 35 alakohdassa määriteltyjä ’jakeluverkonhaltijaa’ ja ’siirtoverkonhaltijaa’;

45) ’unionitason vaikutuksiltaan kriittisellä prosessilla’ mitä tahansa sähköalan prosessia, johon mahdollisesti osallistuu useita toimijoita ja jonka osalta kyberhyökkäyksen mahdollisia vaikutuksia voidaan pitää kriittisinä unionitason kyberturvariskien arvioinnin yhteydessä;

46) ’unionitason vaikutuksiltaan merkittävällä prosessilla’ mitä tahansa sähköalan prosessia, johon mahdollisesti osallistuu useita toimijoita ja jonka osalta kyberhyökkäyksen mahdollisia vaikutuksia voidaan pitää merkittävinä unionitason kyberturvariskien arvioinnin yhteydessä;

47) ’aktiivisesti hyväksikäytetyllä paikkaamattomalla haavoittuvuudella’ haavoittuvuutta, jota ei ole vielä julkistettu ja paikattu, ja jonka osalta on luotettavaa näyttöä siitä, että jokin taho on ajanut haitallista koodia järjestelmässä ilman järjestelmän omistajan lupaa;

48) ’haavoittuvuudella’ haavoittuvuutta siten kuin se on määritelty direktiivin (EU) 2022/2555 6 artiklan 15 alakohdassa.

4 artikla

Toimivaltainen viranomainen

1. Kunkin jäsenvaltion on mahdollisimman pian ja joka tapauksessa viimeistään 13 päivänä joulukuuta 2024 nimettävä kansallinen valtiollinen tai sääntelyviranomainen, joka vastaa sille tässä asetuksessa annettujen tehtävien hoitamisesta, jäljempänä ’toimivaltainen viranomainen’. Siihen saakka, kunnes toimivaltaiselle viranomaiselle on osoitettu tämän asetuksen mukaiset tehtävät, näiden tehtävien hoitamisesta vastaa kunkin jäsenvaltion direktiivin (EU) 2019/944 57 artiklan 1 kohdan nojalla nimeämä sääntelyviranomainen.

2. Jäsenvaltioiden on ilmoitettava viipymättä komissiolle, ACERille, ENISAlle, direktiivin (EU) 2022/2555 14 artiklan nojalla perustetulle verkko- ja tietoturva-alan yhteistyöryhmälle ja 15 päivänä marraskuuta 2012 annetun komission päätöksen ([17]) 1 artiklalla perustetulle sähköalan koordinointiryhmälle tämän artiklan 1 kohdan nojalla nimetyn toimivaltaisen viranomaisensa nimi ja yhteystiedot sekä näiden myöhemmät muutokset.

([16]) Euroopan parlamentin ja neuvoston asetus (EU) N:o 1025/2012, annettu 25 päivänä lokakuuta 2012, eurooppalaisesta standardoinnista, neuvoston direktiivien 89/686/ETY ja 93/15/ETY sekä Euroopan parlamentin ja neuvoston direktiivien 94/9/EY, 94/25/EY, 95/16/EY, 97/23/EY, 98/34/EY, 2004/22/EY, 2007/23/EY, 2009/23/EY ja 2009/105/EY muuttamisesta ja neuvoston päätöksen 87/95/ETY ja Euroopan parlamentin ja neuvoston päätöksen N:o 1673/2006/EY kumoamisesta (EUVL L 316, 14.11.2012, s. 12).

([17]) Komission päätös, annettu 15 päivänä marraskuuta 2012, sähköalan koordinointiryhmän perustamisesta (2012/C 353/02) (EUVL C 353, 17.11.2012, s. 2).

3. Jäsenvaltiot voivat sallia toimivaltaiselle viranomaiselleen mahdollisuuden siirtää sille tässä asetuksessa osoitettuja tehtäviä muille kansallisille viranomaisille, lukuun ottamatta 5 artiklassa lueteltuja tehtäviä. Kunkin toimivaltaisen viranomaisen on valvottava, miten viranomaiset, joille se on siirtänyt tehtäviä, soveltavat tätä asetusta. Toimivaltaisen viranomaisen on ilmoitettava niiden viranomaisten, joille tehtäviä on siirretty, nimet, yhteystiedot, tehtävät ja näiden myöhemmät muutokset komissiolle, ACERille, sähköalan koordinointiryhmälle, ENISAlle ja verkko- ja tietoturva-alan yhteistyöryhmälle.

5 artikla

Asiaan liittyvien viranomaisten ja elinten yhteistyö kansallisella tasolla

Toimivaltaisten viranomaisten on koordinoitava toimintaansa ja varmistettava asianmukainen yhteistyö kyberturvallisuudesta vastaavien toimivaltaisten viranomaisten, kyberkriisinhallintaviranomaisten, kansallisten sääntelyviranomaisten, riskeihin varautumisesta vastaavien toimivaltaisten viranomaisten ja CSIRT-yksiköiden välillä tässä asetuksessa säädettyjen asiaankuuluvien velvoitteiden täyttämiseksi. Toimivaltaisten viranomaisten on koordinoitava toimintaansa myös kunkin jäsenvaltion määrittelemien muiden elinten tai viranomaisten kanssa tehokkaiden menettelyjen varmistamiseksi ja tehtävien ja velvoitteiden päällekkäisyyksien välttämiseksi. Toimivaltaisten viranomaisten on voitava ohjeistaa asianomaisia kansallisia sääntelyviranomaisia pyytämään ACERilta lausuntoja 8 artiklan 3 kohdan nojalla.

6 artikla

Ehdot, menetelmät ja suunnitelmat

1. Siirtoverkonhaltijoiden on yhteistyössä EU DSO -elimen kanssa laadittava ehdotuksia 2 kohdan mukaisista ehdoista tai menetelmistä tai 3 kohdan mukaisista suunnitelmista.

2. Seuraaville ehdoille tai menetelmille ja niiden muutoksille on saatava kaikkien toimivaltaisten viranomaisten hyväksyntä:

a) 18 artiklan 1 kohdan mukaiset kyberturvariskien arviointimenetelmät;

b) 23 artiklan mukainen kattava rajat ylittävien sähköalan kyberturvariskien arviointiraportti;

c) 29 artiklan mukaiset vähimmäistason ja tiukemmat kyberturvavarotoimet ja 34 artiklan mukainen sähköalan kyberturvavarotoimien kartoitus suhteessa standardeihin, mukaan lukien 33 artiklan mukaiset vähimmäistason ja tiukemmat kyberturvavarotoimet toimitusketjussa;

d) 35 artiklan mukainen kyberturvahankintasuositus; ja

e) 37 artiklan 8 kohdan mukainen kyberhyökkäysten luokittelumenetelmä.

3. Jäljempänä olevan 22 artiklan mukaisille ehdotuksille alueellisiksi kyberturvariskien lieventämissuunnitelmiksi on saatava kyseisen käyttöalueen kaikkien toimivaltaisten viranomaisten hyväksyntä.

4. Edellä 2 kohdassa lueteltuja ehtoja tai menetelmiä tai 3 kohdassa lueteltuja suunnitelmia koskeviin ehdotuksiin on sisällyttävä niiden ehdotettu toteutusaikataulu ja kuvaus niiden odotetusta vaikutuksesta tämän asetuksen tavoitteisiin.

5. EU DSO -elin voi antaa asianomaisille siirtoverkonhaltijoille asiasta perustellun lausunnon viimeistään kolme viikkoa ennen määräaikaa, johon mennessä ehdot, menetelmät tai suunnitelmat on esitettävä toimivaltaisille viranomaisille. Ehtoja, menetelmiä tai suunnitelmia koskevasta ehdotuksesta vastaavien siirtoverkonhaltijoiden on otettava huomioon EU DSO -elimen perusteltu lausunto ennen kuin ehdotus esitetään toimivaltaisille viranomaisille hyväksyttäväksi. Siirtoverkonhaltijoiden on esitettävä perustelut, jos ne eivät ota EU DSO -elimen lausuntoa huomioon.

6. Siirtoverkonhaltijoiden on ehtoja, menetelmiä ja suunnitelmia laatiessaan tehtävä tiivistä yhteistyötä. Siirtoverkonhaltijoiden on Sähkö-ENTSOn avustuksella ja yhteistyössä EU DSO -elimen kanssa säännöllisesti tiedotettava toimivaltaisille viranomaisille ja ACERille edistymisestään ehtojen, menetelmien ja suunnitelmien laadinnassa.

7 artikla

Siirtoverkonhaltijoiden äänestyssäännöt

1. Jos ehtoja tai menetelmiä koskevista ehdotuksista päättävät siirtoverkonhaltijat eivät pääse yhteisymmärrykseen, niiden on äänestettävä asiasta ja tehtävä päätös määräenemmistöllä. Tällaisten päätösten tapauksessa määräenemmistö muodostuu seuraavasti:

a) siirtoverkonhaltijat, jotka edustavat vähintään 55 prosenttia jäsenvaltioista; ja

b) siirtoverkonhaltijat, joiden edustamat jäsenvaltiot kattavat vähintään 65 prosenttia unionin väestöstä.

2. Tämän asetuksen 6 artiklan 2 kohdassa lueteltuja ehtoja tai menetelmiä koskevista ehdotuksista tehtävissä päätöksissä määrävähemmistössä on oltava vähintään neljää jäsenvaltiota edustavia siirtoverkonhaltijoita; muussa tapauksessa katsotaan, että määräenemmistö on saavutettu.

3. Jos tietyn käyttöalueen siirtoverkonhaltijat, jotka päättävät 6 artiklan 2 kohdassa lueteltuja suunnitelmia koskevista ehdotuksista, eivät pääse yhteisymmärrykseen ja jos kyseinen käyttöalue koostuu useammasta kuin viidestä jäsenvaltiosta, siirtoverkonhaltijoiden on tehtävä päätöksensä määräenemmistöllä. Edellä 6 artiklan 2 kohdassa luetelluista ehdotuksista äänestettäessä määräenemmistö muodostuu seuraavasti:

a) siirtoverkonhaltijat, jotka edustavat vähintään 72 prosenttia asianomaisista jäsenvaltioista; ja

b) siirtoverkonhaltijat, joiden edustamat jäsenvaltiot kattavat vähintään 65 prosenttia asianomaisen alueen väestöstä.

4. Suunnitelmaehdotuksia koskevissa päätöksissä ehkäisevässä asemassa olevassa määrävähemmistössä on oltava siirtoverkonhaltijoita, jotka edustavat yli 35 prosenttia osallistuvien jäsenvaltioiden väestöstä, ja lisäksi siirtoverkonhaltijoita, jotka edustavat vähintään yhtä muuta asianomaista jäsenvaltiota; muussa tapauksessa katsotaan, että määräenemmistö on saavutettu.

5. Kun siirtoverkonhaltijat tekevät päätöksiä 6 artiklan 2 kohdan mukaisista ehtoja tai menetelmiä koskevista ehdotuksista, kullakin jäsenvaltiolla on yksi ääni. Jos jäsenvaltion alueella toimii useampi kuin yksi siirtoverkonhaltija, kyseisen jäsenvaltion on jaettava äänioikeudet siirtoverkonhaltijoiden kesken.

6. Jos siirtoverkonhaltijat eivät yhteistyössä EU DSO -elimen kanssa esitä ensimmäistä tai muutettua ehdotusta ehdoista, menetelmistä tai suunnitelmista asianomaisille toimivaltaisille viranomaisille tässä asetuksessa säädetyissä määräajoissa, niiden on esitettävä asianomaisille toimivaltaisille viranomaisille ja ACERille ehtojen, menetelmien tai suunnitelmien luonnokset. Niiden on selitettävä, mikä on estänyt yhteisymmärrykseen pääsemisen. Toimivaltaisten viranomaisten on yhdessä toteutettava tarvittavat toimet vaadittujen ehtojen, menetelmien tai suunnitelmien hyväksymiseksi. Tämä voidaan tehdä esimerkiksi pyytämällä tämän kohdan nojalla muutoksia luonnoksiin, tarkistamalla ja täydentämällä kyseisiä luonnoksia tai, jos luonnoksia ei ole esitetty, määrittelemällä ja hyväksymällä vaaditut ehdot, menetelmät tai suunnitelmat.

8 artikla

Ehdotusten esittäminen toimivaltaisille viranomaisille

1. Siirtoverkonhaltijoiden on toimitettava ehdot, menetelmät tai suunnitelmat asianomaisille toimivaltaisille viranomaisille hyväksyntää varten 18, 23, 29, 33, 34, 35 ja 37 artiklassa säädetyissä määräajoissa. Toimivaltaiset viranomaiset voivat yhdessä pidentää näitä määräaikoja poikkeustapauksissa, erityisesti tapauksissa, joissa määräaikaa ei voida noudattaa siirtoverkonhaltijoista tai EU DSO -elimestä riippumattomien olosuhteiden vuoksi.

2. Edellä 1 kohdassa tarkoitetut ehdot, menetelmät tai suunnitelmat on toimitettava ACERille tiedoksi samaan aikaan kun ne esitetään toimivaltaisille viranomaisille.

3. ACERin on annettava kansallisten sääntelyviranomaisten yhteisestä pyynnöstä lausunto ehtoja, menetelmiä tai suunnitelmia koskevasta ehdotuksesta kuuden kuukauden kuluessa ehdotuksen vastaanottamisesta ja toimitettava lausuntonsa kansallisille sääntelyviranomaisille ja toimivaltaisille viranomaisille. Kansallisten sääntelyviranomaisten, kyberturvallisuudesta vastaavien kansallisten toimivaltaisten viranomaisten ja muiden toimivaltaisiksi viranomaisiksi nimettyjen viranomaisten on koordinoitava toimintaansa keskenään ennen kuin kansalliset sääntelyviranomaiset pyytävät lausuntoa ACERilta. ACER voi sisällyttää tällaiseen lausuntoon suosituksia. ACERin on kuultava ENISAa ennen kuin se antaa lausunnon 6 artiklan 2 kohdassa luetelluista ehdotuksista.

4. Toimivaltaisten viranomaisten on kuultava toisiaan, tehtävä tiivistä yhteistyötä ja koordinoitava toimintaansa, jotta ehdotetuista ehdoista, menetelmistä tai suunnitelmista päästäisiin yhteisymmärrykseen. Ennen ehtojen, menetelmien tai suunnitelmien hyväksymistä niiden on tarvittaessa tarkistettava ja täydennettävä ehdotuksia Sähkö-ENTSOa ja EU DSO -elintä kuultuaan sen varmistamiseksi, että ehdotukset ovat linjassa tämän asetuksen kanssa ja edistävät kyberturvallisuuden yhteistä korkeaa tasoa kaikkialla unionissa.

5. Toimivaltaisten viranomaisten on päätettävä ehdoista, menetelmistä tai suunnitelmista kuuden kuukauden kuluessa siitä, kun asianomainen toimivaltainen viranomainen tai tapauksen mukaan viimeinen asiaan liittyvä toimivaltainen viranomainen on saanut niitä koskevat ehdotukset.

6. Jos ACER antaa asiassa lausunnon, asianomaisten toimivaltaisten viranomaisten on otettava se huomioon ja tehtävä päätöksensä kuuden kuukauden kuluessa ACERin lausunnon saamisesta.

7. Jos toimivaltaiset viranomaiset yhdessä edellyttävät ehdotettuihin ehtoihin, menetelmiin tai suunnitelmiin ne hyväksyäkseen muutoksia, siirtoverkonhaltijoiden on laadittava yhteistyössä EU DSO -elimen kanssa tällaisia muutoksia koskeva ehdotus. Siirtoverkonhaltijoiden on toimitettava muutettu ehdotus hyväksyttäväksi kahden kuukauden kuluessa toimivaltaisten viranomaisten pyynnöstä. Toimivaltaisten viranomaisten on päätettävä muutetuista ehdoista, menetelmistä tai suunnitelmista kahden kuukauden kuluessa niiden esittämisestä.

8. Jos toimivaltaiset viranomaiset eivät ole päässeet yhteisymmärrykseen 5 tai 7 kohdassa tarkoitetussa määräajassa, niiden on ilmoitettava asiasta komissiolle. Komissio voi toteuttaa tarvittavat toimet mahdollistaakseen vaadittujen ehtojen, menetelmien tai suunnitelmien hyväksymisen.

9. Siirtoverkonhaltijoiden, Sähkö-ENTSOn avustuksella, ja EU DSO -elimen on julkaistava ehdot, menetelmät tai suunnitelmat verkkosivustoillaan asianomaisten toimivaltaisten viranomaisten hyväksynnän jälkeen, lukuun ottamatta tietoja, joita pidetään 47 artiklan mukaisesti luottamuksellisina.

10. Toimivaltaiset viranomaiset voivat yhdessä pyytää siirtoverkonhaltijoilta ja EU DSO -elimeltä ehdotuksia hyväksyttyjen ehtojen, menetelmien tai suunnitelmien muuttamiseksi ja asettaa määräajan ehdotusten esittämiselle. Siirtoverkonhaltijat voivat yhteistyössä EU DSO -elimen kanssa ehdottaa muutoksia toimivaltaisille viranomaisille myös omasta aloitteestaan. Ehtojen, menetelmien tai suunnitelmien muuttamista koskevat ehdotukset laaditaan ja hyväksytään tässä artiklassa säädettyä menettelyä noudattaen.

11. Siirtoverkonhaltijoiden on yhteistyössä EU DSO -elimen kanssa tarkasteltava uudelleen ehtojen, menetelmien tai suunnitelmien toimivuutta vähintään joka kolmas vuosi niiden ensimmäisen hyväksymisen jälkeen ja raportoitava tarkastelun tuloksista ilman aiheetonta viivytystä toimivaltaisille viranomaisille ja ACERille.

9 artikla

Kuuleminen

1. Siirtoverkonhaltijoiden on Sähkö-ENTSOn avustuksella ja yhteistyössä EU DSO -elimen kanssa kuultava sidosryhmiä, mukaan lukien ACER, ENISA ja kunkin jäsenvaltion toimivaltainen viranomainen, 6 artiklan 2 kohdassa lueteltuja ehtoja tai menetelmiä ja 6 artiklan 3 kohdassa tarkoitettuja suunnitelmia koskevista ehdotusluonnoksista. Kuulemisen on kestettävä vähintään kuukausi.

2. Siirtoverkonhaltijoiden yhteistyössä EU DSO -elimen kanssa esittämät 6 artiklan 2 kohdassa tarkoitettuja ehtoja tai menetelmiä koskevat ehdotukset on julkaistava ja niistä on järjestettävä kuuleminen unionin tasolla. Asianomaisten siirtoverkonhaltijoiden yhteistyössä EU DSO -elimen kanssa esittämät 6 artiklan 3 kohdassa tarkoitettuja suunnitelmia koskevat aluetason ehdotukset on julkaistava ja niistä on järjestettävä kuuleminen vähintään alueellisella tasolla.

3. Ehtoja, menetelmiä tai suunnitelmia koskevasta ehdotuksesta vastaavien Sähkö-ENTSOn avustuksella toimivien siirtoverkonhaltijoiden ja EU DSO -elimen on otettava asianmukaisesti huomioon 1 kohdan mukaisesti järjestetyissä kuulemisissa saadut sidosryhmien näkemykset ennen kuin ehdotukset toimitetaan viranomaisten hyväksyttäviksi. Kaikissa tapauksissa ehdotuksen esittämisen yhteydessä on annettava vankat perustelut sille, kuinka kuulemisessa esitetyt näkökannat on otettu huomioon tai jätetty huomioimatta, ja ne on julkaistava viipymättä ennen ehtoja tai menetelmiä koskevan ehdotuksen julkaisemista tai yhtä aikaa sen julkaisemisen kanssa.

10 artikla

Sidosryhmien osallistaminen

ACER vastaa tiiviissä yhteistyössä Sähkö-ENTSOn ja EU DSO -elimen kanssa sidosryhmien osallistamisesta, muun muassa järjestämällä säännöllisiä tapaamisia sidosryhmien kanssa tämän asetuksen täytäntöönpanoon liittyvien ongelmien tunnistamiseksi ja parannusten ehdottamiseksi.

11 artikla

Kulujen korvaaminen

1. Kunkin jäsenvaltion asianomaisen kansallisen sääntelyviranomaisen on arvioitava verkkotariffisääntelyn piiriin kuuluville siirtoverkonhaltijoille ja jakeluverkonhaltijoille aiheutuvat kulut, jotka johtuvat tässä asetuksessa säädetyistä velvoitteista, mukaan lukien Sähkö-ENTSOlle ja EU DSO -elimelle aiheutuvat kulut.

2. Kohtuullisiksi, tehokkaasti toimien aiheutuneiksi ja oikeasuhteisiksi arvioidut kulut on katettava verkkotariffeilla tai muilla asianmukaisilla mekanismeilla, jotka asianomainen kansallinen sääntelyviranomainen määrittää.

3. Edellä 1 kohdassa tarkoitettujen siirtoverkonhaltijoiden ja jakeluverkonhaltijoiden on asianomaisten kansallisten sääntelyviranomaisten pyynnöstä toimitettava niiden määrittämässä kohtuullisessa ajassa tiedot, jotka ovat tarpeen aiheutuneiden kulujen arvioimiseksi.

12 artikla

Seuranta

1. ACERin on seurattava tämän asetuksen täytäntöönpanoa asetuksen (EU) 2019/943 32 artiklan 1 kohdan ja asetuksen (EU) 2019/942 4 artiklan 2 kohdan mukaisesti. Tässä seurannassa ACER voi tehdä yhteistyötä ENISAn kanssa ja pyytää tukea Sähkö-ENTSOlta ja EU DSO -elimeltä. ACERin on säännöllisesti tiedotettava sähköalan koordinointiryhmälle ja verkko- ja tietoturva-alan yhteistyöryhmälle tämän asetuksen täytäntöönpanosta.

2. ACERin on julkaistava vähintään joka kolmas vuosi tämän asetuksen voimaantulon jälkeen raportti, jossa:

a) luodaan katsaus vaikutuksiltaan merkittävien ja vaikutuksiltaan kriittisten toimijoiden kyberturvariskien hallintatoimien tilanteeseen;

b) kuvataan, voisivatko yhteisiä vaatimuksia, suunnittelua, seurantaa, raportointia ja kriisinhallintaa koskevat lisäsäännöt olla tarpeen sähköalan riskien ehkäisemiseksi; ja

c) yksilöidään tämän asetuksen tarkistusta silmällä pitäen kehityskohteita ja uusia osa-alueita, joita saattaa nousta esiin teknologian kehityksen myötä.

3. ACER voi 13 päivään kesäkuuta 2025 mennessä antaa yhteistyössä ENISAn kanssa ja kuultuaan Sähkö-ENTSOa ja EU DSO -elintä ohjeistusta ACERin seurantatarkoituksiin tarvitsemista, 5 kohdan mukaisesti määriteltyihin suoritusindikaattoreihin pohjautuvista tiedoista sekä tiedonkeruuprosessista ja -tiheydestä.

4. Toimivaltaiset viranomaiset saavat tutustua ACERin hallussa oleviin tietoihin, jotka se on kerännyt tämän artiklan mukaisesti.

5. ACERin on yhteistyössä ENISAn kanssa sekä Sähkö-ENTSOn ja EU DSO -elimen tuella määriteltävä ei-sitovat suoritusindikaattorit, joilla voidaan arvioida rajat ylittävien sähkönsiirtojen kyberturvanäkökohtia operatiivisen luotettavuuden näkökulmasta.

6. Tämän asetuksen 2 artiklan 1 kohdassa lueteltujen toimijoiden on toimitettava ACERille tiedot, joita se tarvitsee 2 kohdassa lueteltujen tehtävien suorittamiseksi.

13 artikla

Vertailuanalyysi

1. ACERin on yhteistyössä ENISAn kanssa laadittava 13 päivään kesäkuuta 2025 mennessä kyberturvatason vertailuanalyysiä koskeva ei-sitova opas. Oppaassa on selitettävä kansallisille sääntelyviranomaisille tämän artiklan 2 kohdan mukaisen kyberturvavarotoimien vertailuanalyysin periaatteet ottaen huomioon toimista aiheutuvat kustannukset sekä valvonnassa käytettyjen prosessien, tuotteiden, palvelujen, järjestelmien ja ratkaisujen vaikuttavuus. ACERin on opasta laatiessaan otettava huomioon jo olemassa olevat vertailuanalyysiraportit. ACERin on annettava ei-sitova opas kansallisille sääntelyviranomaisille tiedoksi.

2. Kansallisten sääntelyviranomaisten on 12 kuukauden kuluessa 1 kohdan mukaisen oppaan hyväksymisestä suoritettava vertailuanalyysi, jossa arvioidaan, tehtyjä kyberturvainvestointeja seuraavista näkökulmista:

a) lieventävätkö investoinnit rajat ylittäviin sähkönsiirtoihin vaikuttavia riskejä;

b) tuottavatko investoinnit toivottuja tuloksia ja saadaanko niillä aikaan tehokkuushyötyjä sähköjärjestelmien kehittämisen suhteen; ja

c) ovatko investoinnit tehokkaita ja onko ne integroitu omaisuuserien ja palvelujen yleiseen hankintaan.

3. Vertailuanalyysissä kansalliset sääntelyviranomaiset voivat ottaa huomioon ACERin laatiman ei-sitovan kyberturvavertailuoppaan, ja niiden on arvioitava erityisesti seuraavia seikkoja:

a) keskimääräiset kyberturvamenot, joilla lievennetään rajat ylittäviin sähkönsiirtoihin vaikuttavia riskejä, varsinkin vaikutuksiltaan merkittävien ja vaikutuksiltaan kriittisten toimijoiden osalta;

b) yhteistyössä Sähkö-ENTSOn ja EU DSO -elimen kanssa sellaisten kyberturvapalvelujen, -järjestelmien ja -tuotteiden keskihinnat, jotka osaltaan suuressa määrin parantavat ja ylläpitävät kyberturvariskien hallintatoimia sähkön eri käyttöalueilla; ja

c) tämän asetuksen täytäntöönpanoon soveltuvien kyberturvapalvelujen, -järjestelmien ja -ratkaisujen kustannusten ja toimintojen olemassaolo ja vertailtavuus ja mahdolliset toimet varainkäytön tehostamiseksi, varsinkin kun saatetaan tarvita investointeja kyberturvateknologiaan.

4. Kaikkia vertailuanalyysiin liittyviä tietoja on käsiteltävä ja prosessoitava tämän asetuksen tietoluokitteluvaatimusten, vähimmäistason kyberturvavarotoimien ja rajat ylittävien sähköalan kyberturvariskien arviointiraportin mukaisesti. Edellä 2 ja 3 kohdassa tarkoitettua vertailuanalyysia ei saa julkistaa.

5. Tämän artiklan 2 ja 3 kohdassa tarkoitetun vertailuanalyysin tulokset on jaettava kaikille kansallisille sääntelyviranomaisille, kaikille toimivaltaisille viranomaisille, ACERille, ENISAlle ja komissiolle, sanotun kuitenkaan rajoittamatta 47 artiklassa säädettyjä luottamuksellisuusvaatimuksia ja tarvetta suojella tämän asetuksen säännösten piiriin kuuluvien toimijoiden turvallisuutta.

14 artikla

Sopimukset unionin ulkopuolisten siirtoverkonhaltijoiden kanssa

1. Kolmanteen maahan rajautuvan käyttöalueen siirtoverkonhaltijoiden on 18 kuukauden kuluessa tämän asetuksen voimaantulosta pyrittävä tekemään kyseisen kolmannen maan siirtoverkonhaltijoiden kanssa asiaa koskevan unionin lainsäädännön mukaisia sopimuksia, joissa vahvistetaan perusta yhteistyölle kybersuojauskysymyksissä ja kyberturvaa koskevat yhteistyöjärjestelyt kyseisten siirtoverkonhaltijoiden kanssa.

2. Siirtoverkonhaltijoiden on ilmoitettava toimivaltaiselle viranomaiselle 1 kohdassa tarkoitetuista sopimuksista.

15 artikla

Lailliset edustajat

1. Toimijoiden, joilla ei ole toimipaikkaa unionissa, mutta jotka tarjoavat palveluja toimijoille unionissa ja joiden on ilmoitettu olevan vaikutuksiltaan merkittäviä tai vaikutuksiltaan kriittisiä toimijoita 24 artiklan 6 kohdan mukaisesti, on kolmen kuukauden kuluessa ilmoittamisesta nimettävä kirjallisesti edustajansa unionissa ja tiedotettava asiasta ilmoituksen tehneelle toimivaltaiselle viranomaiselle.

2. Edustajalla on oltava riittävät valtuudet, jotta mikä tahansa toimivaltainen viranomainen tai CSIRT-toimija unionissa voi ottaa edustajaan tämän asetuksen mukaisten velvoitteiden osalta yhteyttä vaikutuksiltaan merkittävän tai vaikutuksiltaan kriittisen toimijan sijaan tai ohella. Vaikutuksiltaan merkittävän tai vaikutuksiltaan kriittisen toimijan on taattava lailliselle edustajalleen tarvittavat toimivaltuudet ja riittävät resurssit, jotta voidaan varmistaa edustajan tehokas ja nopea yhteistyö toimivaltaisten viranomaisten tai CSIRT-yksiköiden kanssa.

3. Edustajan on oltava sijoittautunut johonkin niistä jäsenvaltioista, joissa toimija tarjoaa palvelujaan. Toimijan katsotaan kuuluvan sen jäsenvaltion lainkäyttövallan piiriin, johon edustaja on sijoittautunut. Vaikutuksiltaan merkittävien ja vaikutuksiltaan kriittisten toimijoiden on ilmoitettava laillisen edustajansa nimi, postiosoite, sähköpostiosoite ja puhelinnumero sen jäsenvaltion toimivaltaiselle viranomaiselle, jossa laillinen edustaja sijaitsee tai johon tämä on sijoittautunut.

4. Nimettyä laillista edustajaa on voitava pitää vastuussa tämän asetuksen mukaisten velvoitteiden noudattamatta jättämisestä, sanotun kuitenkaan rajoittamatta vastuuta ja oikeustoimia, joihin voidaan ryhtyä vaikutuksiltaan merkittävää tai vaikutuksiltaan kriittistä toimijaa itseään vastaan.

5. Jos toimijalla ei ole unionissa tämän artiklan mukaista nimettyä edustajaa, mikä tahansa jäsenvaltio, jossa toimija tarjoaa palveluja, voi ryhtyä oikeustoimiin toimijaa vastaan tämän asetuksen mukaisten velvoitteiden noudattamatta jättämisen vuoksi.

6. Laillisen edustajan nimeäminen unionissa 1 kohdan nojalla ei ole sijoittautumista unioniin.

16 artikla

Sähkö-ENTSOn ja EU DSO -elimen yhteistyö

1. Sähkö-ENTSOn ja EU DSO -elimen on tehtävä yhteistyötä 19 ja 21 artiklan nojalla suoritettavissa kyberturvariskien arvioinneissa ja varsinkin seuraavissa tehtävissä:

a) 18 artiklan 1 kohdan mukaisten kyberturvariskien arviointimenetelmien laatiminen;

b) 23 artiklan mukaisen kattavan rajat ylittävien sähköalan kyberturvariskien arviointiraportin laatiminen;

c) yhteisen sähköalan kyberturvakehyksen laatiminen III luvun mukaisesti;

d) kyberturvahankintasuosituksen laatiminen 35 artiklan nojalla;

e) 37 artiklan 8 kohdan mukaisen kyberhyökkäysten luokittelumenetelmän laatiminen;

f) alustavan sähköalan kyberturvavaikutusindeksin (ECII) laatiminen 48 artiklan 1 kohdan a alakohdan nojalla;

g) vaikutuksiltaan merkittävien ja vaikutuksiltaan kriittisten toimijoiden alustavan koontiluettelon laatiminen 48 artiklan 3 kohdan nojalla;

h) unionitason vaikutuksiltaan merkittävien ja vaikutuksiltaan kriittisten prosessien alustavan luettelon laatiminen 48 artiklan 4 kohdan nojalla;

i) eurooppalaisten ja kansainvälisten standardien ja varotoimien alustavan luettelon laatiminen 48 artiklan 6 kohdan nojalla;

j) unionitason kyberturvariskien arvioinnin suorittaminen 19 artiklan nojalla;

k) alueellisten kyberturvariskien arviointien suorittaminen 21 artiklan nojalla;

l) alueellisten kyberturvariskien lieventämissuunnitelmien laatiminen 22 artiklan nojalla;

m) tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä koskevan ohjeistuksen laatiminen 36 artiklan mukaisesti; ja

n) tämän asetuksen täytäntöönpanon suuntaviivojen laatiminen kuullen ACERia ja ENISAa.

2. Sähkö-ENTSOn ja EU DSO -elimen yhteistyö voidaan järjestää kyberturvariskejä käsittelevän työryhmän muodossa.

3. Sähkö-ENTSOn ja EU DSO -elimen on säännöllisesti tiedotettava ACERille, ENISAlle, verkko- ja tietoturva-alan yhteistyöryhmälle ja sähköalan koordinointiryhmälle edistymisestä 19 ja 21 artiklan nojalla tehtävissä unionitason ja aluetason kyberturvariskien arvioinneissa.

17 artikla

ACERin ja toimivaltaisten viranomaisten yhteistyö

ACERin on yhteistyössä kunkin toimivaltaisen viranomaisen kanssa:

1) seurattava 12 artiklan 2 kohdan a alakohdan mukaisesti kyberturvariskien hallintatoimien toteutumista ja seurattava 27 ja 39 artiklan mukaisten raportointivelvoitteiden noudattamista; ja

2) seurattava 6 artiklan 2 ja 3 kohdan mukaisten ehtojen, menetelmien tai suunnitelmien hyväksymisprosessia ja noudattamista. ACERin, ENISAn ja kunkin toimivaltaisen viranomaisen välinen yhteistyö voidaan järjestää erityisen kyberturvariskien seurantaelimen muodossa.

II LUKU

RISKIEN ARVIOINTI JA OLENNAISTEN KYBERTURVARISKIEN TUNNISTAMINEN

18 artikla

Kyberturvariskien arviointimenetelmät

1. Siirtoverkonhaltijoiden on Sähkö-ENTSOn avustuksella, yhteistyössä EU DSO -elimen kanssa ja verkko- ja tietoturva-alan yhteistyöryhmää kuultuaan 13 päivään maaliskuuta 2025 mennessä esitettävä ehdotus kyberturvariskien arviointimenetelmistä unionitasolla, aluetasolla ja jäsenvaltiotasolla.

2. Unionitason, aluetason ja jäsenvaltiotason kyberturvariskien arviointimenetelmien on katettava seuraavat tekijät:

a) luettelo tarkasteltavista kyberuhkista, mukaan lukien ainakin seuraavat toimitusketjuun kohdistuvat uhat:

   i) toimitusketjun vakava ja odottamaton korruptoituminen;

   ii) tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien poistuminen toimitusketjusta;

iii) toimitusketjun toimijoiden kautta käynnistetyt kyberhyökkäykset;

iv) arkaluonteisten tietojen vuotaminen toimitusketjun kautta, mukaan lukien toimitusketjun seurannan ja jäljityksen kautta; ja

v) heikkouksien tai takaporttien sijoittaminen tieto- ja viestintätekniikan tuotteisiin, palveluihin tai prosesseihin toimitusketjun toimijoiden kautta;

b) kriteerit, joiden perusteella kyberturvariskien vaikutukset arvioidaan merkittäviksi tai kriittisiksi käyttäen määritettyjä seurausten ja todennäköisyyden kynnystasoja;

c) lähestymistapa, jolla analysoidaan aiemman sukupolven järjestelmistä periytyviä, kyberhyökkäysten kerrannaisvaikutuksista johtuvia ja verkkoa operoivien järjestelmien reaaliaikaisesta luonteesta johtuvia kyberturvariskejä; ja

d) lähestymistapa, jolla analysoidaan riippuvuudesta yksittäisestä tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien toimittajasta johtuvia kyberturvariskejä.

3. Unionitason, aluetason ja jäsenvaltiotason kyberturvariskien arviointimenetelmissä on arvioitava kyberturvariskejä käyttäen samaa riskivaikutusmatriisia. Riskivaikutusmatriisissa on mitattava:

a) kyberhyökkäysten seurauksia seuraavien kriteerien perusteella:

i) tehonmenetys;

ii) sähköntuotannon väheneminen;

iii) taajuuden tasaamisessa käytettävän primäärisen taajuusreservin kapasiteetin menetys;

iv) sellaisen kapasiteetin menetys, jota tarvitaan sähköverkon palauttamiseksi toimintaan ilman ulkoista siirtoverkkoa verkon täydellisen tai osittaisen sulkemisen jälkeen (ns. pimeäkäynnistys);

v) asiakkaisiin vaikuttavan sähkökatkon odotettu kesto yhdistettynä asiakasmäärinä ilmaistuun sähkökatkon laajuuteen; ja

vi) muut määrälliset tai laadulliset kriteerit, jotka voisivat kohtuudella toimia indikaattorina kyberhyökkäyksen vaikutuksesta rajat ylittäviin sähkönsiirtoihin;

b) poikkeaman todennäköisyyttä kyberhyökkäysten esiintymisenä vuositasolla.

4. Unionitason kyberturvariskien arviointimenetelmissä on kuvattava, miten merkittävän vaikutuksen ja kriittisen vaikutuksen kynnystasojen ECII-arvot määritellään. ECII:n on mahdollistettava se, että toimijat kykenevät arvioimaan riskien vaikutukset toimintaprosessiinsa 2 kohdan b alakohdassa tarkoitettujen kriteerien avulla osana 26 artiklan 4 kohdan c alakohdan i alakohdan nojalla tekemäänsä vaikutustenarviointia.

5. Sähkö-ENTSOn on koordinoidusti EU DSO -elimen kanssa tiedotettava sähköalan koordinointiryhmälle 1 kohdan nojalla laadituista ehdotuksista, jotka koskevat kyberturvariskien arviointimenetelmiä.

19 artikla

Unionitason kyberturvariskien arviointi

1. Sähkö-ENTSOn on yhteistyössä EU DSO -elimen kanssa ja kuullen verkko- ja tietoturva-alan yhteistyöryhmää yhdeksän kuukauden kuluessa 8 artiklan nojalla hyväksyttyjen kyberturvariskien arviointimenetelmien hyväksymisestä ja sen jälkeen joka kolmas vuosi suoritettava, sanotun kuitenkaan rajoittamatta direktiivin (EU) 2022/2555 22 artiklan soveltamista, unionitason kyberturvariskien arviointi ja laadittava unionitason kyberturvariskien arviointiraportin luonnos. Tässä niiden on käytettävä 18 artiklan nojalla laadittuja ja 8 artiklan nojalla hyväksyttyjä menetelmiä tunnistaakseen, analysoidakseen ja arvioidakseen sähköjärjestelmän toimintavarmuuteen vaikuttavien ja rajat ylittäviä sähkönsiirtoja häiritsevien kyberhyökkäysten mahdolliset seuraukset. Unionitason kyberturvariskien arvioinnissa ei tarkastella kyberhyökkäysten oikeudellisia, taloudellisia tai mainehaittaan liittyviä kielteisiä vaikutuksia.

2. Unionitason kyberturvariskien arviointiraportissa on kuvattava seuraavat seikat:

a) unionitason vaikutuksiltaan merkittävät prosessit ja unionitason vaikutuksiltaan kriittiset prosessit; ja

b) riskivaikutusmatriisi, jota toimijoiden ja toimivaltaisten viranomaisten on käytettävä arvioidessaan kyberturvariskejä, jotka on yksilöity 20 artiklan nojalla suoritetussa jäsenvaltiotason kyberturvariskien arvioinnissa ja 26 artiklan 2 kohdan b alakohdan nojalla suoritetussa toimijatason kyberturvariskien arvioinnissa.

3. Unionitason vaikutuksiltaan merkittävien prosessien ja unionitason vaikutuksiltaan kriittisten prosessien osalta unionitason kyberturvariskien arviointiraportissa on kuvattava seuraavat seikat:

a) arvio kyberhyökkäyksen mahdollisista seurauksista käyttäen mittareita, jotka on määritelty 18 artiklan 2, 3 ja 4 kohdan nojalla laaditussa ja 8 artiklan nojalla hyväksytyssä kyberturvallisuusriskien arviointimenetelmässä; ja

b) ECII-arvot ja merkittävien vaikutusten ja kriittisten vaikutusten kynnystasot, joita toimivaltaisten viranomaisten on 24 artiklan 1 ja 2 kohdan nojalla käytettävä yksilöidessään unionitason vaikutuksiltaan merkittäviin prosesseihin ja unionitason vaikutuksiltaan kriittisiin prosesseihin osallistuvia vaikutuksiltaan merkittäviä ja vaikutuksiltaan kriittisiä toimijoita.

4. Sähkö-ENTSOn on yhteistyössä EU DSO -elimen kanssa toimitettava ACERille lausuntoa varten unionitason kyberturvariskien arviointiraportin luonnos yhdessä unionitason kyberturvariskien arvioinnin tulosten kanssa. ACERin on annettava lausuntonsa raportin luonnoksesta kolmen kuukauden kuluessa sen vastaanottamisesta. Sähkö-ENTSOn ja EU DSO -elimen on otettava ACERin lausunto mahdollisimman tarkasti huomioon laatiessaan lopullista raporttia.

5. Sähkö-ENTSOn on yhteistyössä EU DSO -elimen kanssa annettava ACERille, komissiolle, ENISAlle ja toimivaltaisille viranomaisille tiedoksi lopullinen unionitason kyberturvariskien arviointiraportti kolmen kuukauden kuluessa ACERin lausunnon vastaanottamisesta.

20 artikla

Jäsenvaltiotason kyberturvariskien arviointi

1. Kunkin toimivaltaisen viranomaisen on suoritettava jäsenvaltiotason kyberturvariskien arviointi kaikille vaikutuksiltaan merkittäville ja vaikutuksiltaan kriittisille toimijoille jäsenvaltiossaan käyttäen 18 artiklan nojalla laadittuja ja 8 artiklan nojalla hyväksyttyjä menetelmiä. Jäsenvaltiotason kyberturvariskien arvioinnissa on yksilöitävä ja analysoitava rajat ylittäviä sähkönsiirtoja häiritsevien sähköjärjestelmän käyttövarmuuteen vaikuttavien kyberhyökkäysten riskit. Jäsenvaltiotason kyberturvariskien arvioinnissa ei tarkastella kyberhyökkäysten oikeudellisia, taloudellisia tai mainehaittaan liittyviä kielteisiä vaikutuksia.

2. Kunkin toimivaltaisen viranomaisen on 21 kuukauden kuluessa 24 artiklan 6 kohdan nojalla tehdystä vaikutuksiltaan merkittävien ja vaikutuksiltaan kriittisten toimijoiden ilmoittamisesta ja tämän jälkeen joka kolmas vuosi sähköalan kyberturvallisuudesta vastaavia kansallisia toimivaltaisia viranomaisia kuultuaan toimitettava Sähkö-ENTSOlle ja EU DSO -elimelle jäsenvaltiotason kyberturvariskien arviointiraportti, jonka on sisällettävä kustakin vaikutuksiltaan merkittävästä ja kustakin vaikutuksiltaan kriittisestä prosessista seuraavat tiedot:

a) jäljempänä olevan 29 artiklan nojalla toteutettavien vähimmäistason ja tiukempien kyberturvavarotoimien tilanne;

b) jäljempänä olevan 38 artiklan 3 kohdan nojalla vaadittava luettelo kaikista kolmen edeltävän vuoden aikana ilmoitetuista kyberhyökkäyksistä;

c) jäljempänä olevan 38 artiklan 6 kohdan nojalla vaadittava tiivistelmä kolmen edeltävän vuoden aikana ilmoitetuista kyberuhkatiedoista;

d) kunkin unionitason vaikutuksiltaan merkittävän tai kriittisen prosessin osalta arvio riskeistä, jotka liittyvät tietojen ja asiaankuuluvien omaisuuserien luottamuksellisuuden, eheyden ja saatavuuden vaarantumiseen; ja

e) tarvittaessa luettelo 24 artiklan 1, 2, 3 ja 5 kohdan mukaisista uusista vaikutuksiltaan merkittäviksi tai kriittisiksi todetuista toimijoista.

3. Jäsenvaltiotason kyberturvariskien arviointiraportissa on otettava huomioon asetuksen (EU) 2019/941 10 artiklan nojalla laadittu jäsenvaltion riskeihinvarautumissuunnitelma.

4. Jäsenvaltiotason kyberturvariskien arviointiraporttiin 2 kohdan a–d alakohdan nojalla sisällytettäviä tietoja ei saa liittää tiettyihin toimijoihin tai omaisuuseriin. Jäsenvaltiotason kyberturvariskien arviointiraporttiin on sisällyttävä lisäksi riskiarviointi jäsenvaltioiden toimivaltaisten viranomaisten 30 artiklan nojalla myöntämistä väliaikaisista vapautuksista.

5. Sähkö-ENTSO ja EU DSO -elin voivat pyytää toimivaltaisilta viranomaisilta lisätietoja 2 kohdan a ja c alakohdassa tarkoitetuista seikoista.

6. Toimivaltaisten viranomaisten on varmistettava, että niiden toimittamat tiedot ovat tarkkoja ja paikkansapitäviä.

21 artikla

Aluetason kyberturvariskien arvioinnit

1. Sähkö-ENTSOn on yhteistyössä EU DSO -elimen kanssa ja asianomaista alueellista koordinointikeskusta kuullen suoritettava kullekin käyttöalueelle aluetason kyberturvariskien arviointi käyttäen 19 artiklan nojalla laadittuja ja 8 artiklan nojalla hyväksyttyjä menetelmiä tunnistaakseen, analysoidakseen ja arvioidakseen sähköjärjestelmän toimintavarmuuteen vaikuttavien ja rajat ylittäviä sähkönsiirtoja häiritsevien kyberhyökkäysten riskit. Aluetason kyberturvariskien arvioinneissa ei tarkastella kyberhyökkäysten oikeudellisia, taloudellisia tai mainehaittaan liittyviä kielteisiä vaikutuksia.

2. Sähkö-ENTSOn on yhteistyössä EU DSO -elimen kanssa ja kuullen verkko- ja tietoturva-alan yhteistyöryhmää laadittava 21 kuukauden kuluessa 24 artiklan 6 kohdan nojalla tehdystä vaikutuksiltaan merkittävien ja vaikutuksiltaan kriittisten toimijoiden ilmoittamisesta ja tämän jälkeen joka kolmas vuosi aluetason kyberturvariskien arviointiraportti kustakin käyttöalueesta.

3. Aluetason kyberturvariskien arviointiraportissa on otettava huomioon asiaankuuluvat tiedot, jotka sisältyvät unionitason kyberturvariskien arviointiraportteihin ja jäsenvaltiotason kyberturvariskien arviointiraportteihin.

4. Aluetason kyberturvariskien arvioinnissa on tarkasteltava kyberturvallisuuteen liittyviä asetuksen (EU) 2019/941 6 artiklan nojalla määritettyjä alueellisia sähkökriisiskenaarioita.

22 artikla

Aluetason kyberturvariskien lieventämissuunnitelmat

1. Siirtoverkonhaltijoiden on Sähkö-ENTSOn avustuksella ja yhteistyössä EU DSO -elimen kanssa ja kuullen alueellisia koordinointikeskuksia ja verkko- ja tietoturva-alan yhteistyöryhmää laadittava 36 kuukauden kuluessa 24 artiklan 6 kohdan nojalla tehdystä vaikutuksiltaan merkittävien ja vaikutuksiltaan kriittisten toimijoiden ilmoittamisesta ja viimeistään 13 päivänä kesäkuuta 2031 ja tämän jälkeen joka kolmas vuosi aluetason kyberturvariskien lieventämissuunnitelma kullekin käyttöalueelle.

2. Aluetason kyberturvariskien lieventämissuunnitelmien on katettava seuraavat seikat:

a) vähimmäistason ja tiukemmat kyberturvavarotoimet, jotka vaikutuksiltaan merkittävien ja vaikutuksiltaan kriittisten toimijoiden on toteutettava käyttöalueella; ja

b) edellä a alakohdassa tarkoitettujen varotoimien toteuttamisen jälkeen jäljelle jäävät kyberturvariskit käyttöalueilla.

3. Sähkö-ENTSOn on esitettävä aluetason riskinlieventämissuunnitelmat asianomaisille siirtoverkonhaltijoille, toimivaltaisille viranomaisille ja sähköalan koordinointiryhmälle. Sähköalan koordinointiryhmä voi suositella suunnitelmiin muutoksia.

4. Siirtoverkonhaltijoiden on Sähkö-ENTSOn avustuksella, yhteistyössä EU DSO -elimen kanssa ja verkko- ja tietoturva-alan yhteistyöryhmää kuullen päivitettävä aluetason riskinlieventämissuunnitelmat joka kolmas vuosi, elleivät olosuhteet edellytä tiheämpää päivittämistä.

23 artikla

Kattava rajat ylittävien sähköalan kyberturvariskien arviointiraportti

1. Siirtoverkonhaltijoiden on Sähkö-ENTSOn avustuksella, yhteistyössä EU DSO -elimen kanssa ja verkko- ja tietoturva-alan yhteistyöryhmää kuullen 40 kuukauden kuluessa 24 artiklan 6 kohdan nojalla tehdystä vaikutuksiltaan merkittävien ja vaikutuksiltaan kriittisten toimijoiden ilmoittamisesta esitettävä sähköalan koordinointiryhmälle raportti kyberturvariskien arvioinnin tuloksista rajat ylittävien sähkönsiirtojen suhteen (eli 'kattava rajat ylittävien sähköalan kyberturvariskien arviointiraportti').

2. Kattavan rajat ylittävien sähköalan kyberturvariskien arviointiraportin on perustuttava unionitason kyberturvariskien arviointiraporttiin, jäsenvaltiotason kyberturvariskien arviointiraportteihin ja aluetason kyberturvariskien arviointiraportteihin, ja sen on katettava seuraavat seikat:

a) luettelo 19 artiklan 2 kohdan a alakohdan mukaisesti unionitason kyberturvariskien arviointiraportissa yksilöidyistä unionitason vaikutuksiltaan merkittävistä ja kriittisistä prosesseista, mukaan lukien arvio 21 artiklan 2 kohdan ja 19 artiklan 3 kohdan a alakohdan nojalla laadituissa aluetason kyberturvariskien arviointiraporteissa esiin tuotujen kyberturvariskien todennäköisyydestä ja vaikutuksista;

b) vallitsevat kyberuhat, keskittyen erityisesti esiin nousemassa oleviin uhkiin ja sähköjärjestelmään kohdistuviin riskeihin;

c) edellisellä raportointikaudella unionin tasolla tehdyt kyberhyökkäykset sekä kriittinen katsaus siihen, miten tällaiset kyberhyökkäykset ovat saattaneet vaikuttaa rajat ylittäviin sähkönsiirtoihin;

d) kyberturvallisuustoimenpiteiden toteutuksen yleinen tilanne;

e) jäljempänä 37 ja 38 artiklassa edellytettyjen tietovirtojen toteutuksen tilanne;

f) jäljempänä 46 artiklassa edellytetty luettelo tiedoista tai näiden tietojen luokittelukriteerit;

g) tunnistetut ja esiin nostetut riskit, jotka voivat johtua toimitusketjun puutteellisesta hallinnasta;

h) jäljempänä olevan 44 artiklan nojalla järjestetyistä alueellisista ja alueiden välisistä kyberturvaharjoituksista saadut tulokset ja kokemukset;

i) analyysi yleisten rajat ylittävien kyberturvallisuuden kokonaisriskien kehittymisestä sähköalalla viimeisimpien aluetason kyberturvariskien arviointien jälkeen;

j) kaikki muut tiedot, joista voi olla hyötyä tämän asetuksen ja siinä säädettyjen toimintamallien mahdollisten parannus- tai tarkistustarpeiden tunnistamiseksi; ja

k) anonymisoidut koontitiedot 30 artiklan 3 kohdan nojalla myönnetyistä vapautuksista.

3. Edellä 2 artiklan 1 kohdassa luetellut toimijat voivat osallistua kattavan rajat ylittävien sähköalan kyberturvariskien arviointiraportin laadintaan, kunhan 47 artiklan mukaisia tietojen luottamuksellisuutta koskevia vaatimuksia noudatetaan. Siirtoverkonhaltijoiden on Sähkö-ENTSOn avustuksella ja yhteistyössä EU DSO -elimen kanssa kuultava näitä toimijoita jo varhaisessa vaiheessa.

4. Kattavaan rajat ylittävien sähköalan kyberturvariskien arviointiraporttiin sovelletaan 46 artiklan mukaisia tietojenvaihdon suojaamista koskevia sääntöjä. Sähkö-ENTSOn ja EU DSO -elimen on julkaistava raportista julkinen versio, joka ei saa sisältää tietoja, jotka voivat aiheuttaa vahinkoa 2 artiklan 1 kohdassa luetelluille toimijoille, sanotun kuitenkaan rajoittamatta 10 artiklan 4 kohdan ja 47 artiklan 4 kohdan soveltamista. Raportin julkinen versio voidaan julkaista ainoastaan verkko- ja tietoturva-alan yhteistyöryhmän ja sähköalan koordinointiryhmän suostumuksella. Sähkö-ENTSO vastaa koordinoidusti EU DSO -elimen kanssa raportin julkisen version koostamisesta ja julkaisemisesta.

24 artikla

Vaikutuksiltaan merkittävien ja vaikutuksiltaan kriittisten toimijoiden yksilöinti

1. Kunkin toimivaltaisen viranomaisen on yksilöitävä 19 artiklan 3 kohdan b alakohdan mukaiseen unionitason kyberturvariskien arviointiraporttiin sisältyviä ECII-arvoja ja merkittävien ja kriittisten vaikutusten kynnystasoja käyttäen unionitason vaikutuksiltaan merkittäviin prosesseihin ja unionitason vaikutuksiltaan kriittisiin prosesseihin osallistuvat vaikutuksiltaan merkittävät ja vaikutuksiltaan kriittiset toimijat jäsenvaltiossaan. Toimivaltaiset viranomaiset voivat pyytää tietoja oman jäsenvaltionsa toimijalta määrittääkseen kyseisen toimijan ECII-arvot. Jos toimijan määritetty ECII-arvo ylittää merkittävien tai kriittisten vaikutusten kynnystason, yksilöity toimija on mainittava 20 artiklan 2 kohdassa tarkoitetussa jäsenvaltiotason kyberturvariskien arviointiraportissa.

2. Kunkin toimivaltaisen viranomaisen on yksilöitävä 19 artiklan 3 kohdan b alakohdan mukaiseen unionitason kyberturvariskien arviointiraporttiin sisältyviä ECII-arvoja ja merkittävien ja kriittisten vaikutusten kynnystasoja käyttäen unioniin sijoittumattomat vaikutuksiltaan merkittävät ja vaikutuksiltaan kriittiset toimijat, joilla on toimintaa unionissa. Toimivaltainen viranomainen voi pyytää unioniin sijoittumattomalta toimijalta tietoja määrittääkseen kyseisen toimijan ECII-arvot.

3. Kukin toimivaltainen viranomainen voi yksilöidä muita toimijoita jäsenvaltiossaan vaikutuksiltaan merkittäviksi tai vaikutuksiltaan kriittisiksi toimijoiksi, jos seuraavat kriteerit täyttyvät:

a) toimija on osa toimijaryhmää, johon liittyy huomattava riski siitä, että kyberhyökkäys vaikuttaa koko ryhmään samanaikaisesti; ja

b) toimijaryhmän tasolla määritelty ECII ylittää merkittävien vaikutusten tai kriittisten vaikutusten kynnystason.

4. Jos toimivaltainen viranomainen yksilöi 3 kohdan mukaisesti muita toimijoita, kaikkia näiden toimijoiden prosesseja, joiden toimijaryhmän tasolla määritelty ECII ylittää merkittävien vaikutusten kynnystason, on pidettävä vaikutuksiltaan merkittävinä prosesseina, ja kaikkia näiden toimijoiden prosesseja, joiden toimijaryhmän tasolla määritelty ECII ylittää kriittisten vaikutusten kynnystason, on pidettävä vaikutuksiltaan kriittisinä prosesseina.

5. Jos toimivaltainen viranomainen yksilöi 3 kohdan a alakohdassa tarkoitettuja toimijoita useammassa kuin yhdessä jäsenvaltiossa, sen on ilmoitettava asiasta muille toimivaltaisille viranomaisille, Sähkö-ENTSOlle ja EU DSO -elimelle. Sähkö-ENTSOn on yhteistyössä EU DSO -elimen kanssa esitettävä kaikilta toimivaltaisilta viranomaisilta saatujen tietojen perusteella toimivaltaisille viranomaisille analyysi useammassa kuin yhdessä jäsenvaltiossa sijaitsevien toimijoiden kokonaisuudesta, joka voi aiheuttaa hajautuvan häiriön rajat ylittäville sähkönsiirroille ja johtaa kyberhyökkäykseen. Jos toimijoista useassa jäsenvaltiossa koostuva ryhmä yksilöidään kokonaisuudeksi, jonka ECII ylittää merkittävien tai kriittisten vaikutusten kynnystason, kaikkien asianomaisten toimivaltaisten viranomaisten on yksilöitävä tällaiseen kokonaisuuteen kuuluvat toimijat oman jäsenvaltionsa vaikutuksiltaan merkittäviksi tai vaikutuksiltaan kriittisiksi toimijoiksi toimijaryhmän tasolla määritellyn ECII:n perusteella, ja yksilöidyt toimijat on lueteltava unionitason kyberturvariskien arviointiraportissa.

6. Kunkin toimivaltaisen viranomaisen on yhdeksän kuukauden kuluessa siitä, kun Sähkö-ENTSO ja EU DSO -elin ovat 19 artiklan 5 kohdan nojalla antaneet niille tiedoksi unionitason kyberturvariskien arviointiraportin, ja joka tapauksessa 13 päivään kesäkuuta 2028 mennessä ilmoitettava luettelossa oleville toimijoille, että ne on yksilöity vaikutuksiltaan merkittäviksi tai vaikutuksiltaan kriittisiksi toimijoiksi kyseissä jäsenvaltiossa.

7. Kun toimivaltaiselle viranomaiselle raportoidaan 27 artiklan c kohdan nojalla tietyn palveluntarjoajan olevan kriittinen tieto- ja viestintätekniikan palveluntarjoaja, toimivaltaisen viranomaisen on ilmoitettava asiasta sen jäsenvaltion toimivaltaiselle viranomaiselle, jonka alueella palveluntarjoajan toimipaikka tai edustaja sijaitsee. Viimeksi mainitun toimivaltaisen viranomaisen on ilmoitettava palveluntarjoajalle, että se on yksilöity kriittiseksi palveluntarjoajaksi.

25 artikla

Kansalliset todentamisjärjestelmät

1. Toimivaltaiset viranomaiset voivat perustaa kansallisen todentamisjärjestelmän varmistaakseen, että 24 artiklan 1 kohdan nojalla yksilöidyt vaikutuksiltaan kriittiset toimijat noudattavat kansallista lainsäädäntöä, joka sisältyy 34 artiklassa tarkoitettuun vastaavuusmatriisiin. Kansallinen todentamisjärjestelmä voi perustua toimivaltaisen viranomaisen suorittamaan tarkastukseen, riippumattomiin turvallisuusauditointeihin tai saman jäsenvaltion vaikutuksiltaan kriittisten toimijoiden suorittamiin keskinäisiin vertaisarviointeihin, joita toimivaltainen viranomainen valvoo.

2. Jos toimivaltainen viranomainen päättää perustaa kansallisen todentamisjärjestelmän, sen on varmistettava, että todentaminen suoritetaan seuraavien vaatimusten mukaisesti:

a) vertaisarvioinnin, auditoinnin tai tarkastuksen suorittavan osapuolen on oltava riippumaton todennettavasta vaikutuksiltaan kriittisestä toimijasta, eikä sillä saa olla eturistiriitoja tämän suhteen;

b) vertaisarvioinnin, auditoinnin tai tarkastuksen suorittavalla henkilöstöllä on todistettavasti oltava osaamista seuraavilta osa-alueilta:

   i) sähköalan kyberturvallisuus;

   ii) kyberturvallisuuden hallintajärjestelmät;

   iii) auditoinnin periaatteet;

   iv) kyberturvariskien arviointi;

   v) yhteinen sähköalan kyberturvallisuuskehys;

   vi) todentamisen kohteena oleva kansallinen lainsäädäntö- ja sääntelykehys sekä eurooppalaisten ja kansainvälisten standardien kokonaisuus; ja

   vii) todentamisen piiriin kuuluvat vaikutuksiltaan kriittiset prosessit;

c) vertaisarvioinnin, auditoinnin tai tarkastuksen suorittavalle osapuolelle on annettava riittävästi aikaa tehtäviensä suorittamiseen;

d) vertaisarvioinnin, auditoinnin tai tarkastuksen suorittavan osapuolen on toteutettava asianmukaiset toimenpiteet todentamisen aikana keräämiensä tietojen suojaamiseksi kulloisenkin luottamuksellisuustason mukaisesti; ja

e) vertaisarvioinnit, auditoinnit tai tarkastukset on suoritettava vähintään kerran vuodessa, ja niiden on katettava todentamisen koko kohdeala vähintään joka kolmas vuosi.

3. Jos toimivaltainen viranomainen päättää perustaa kansallisen todentamisjärjestelmän, sen on raportoitava ACERille vuosittain, kuinka usein se on tehnyt kyseisen järjestelmän mukaisia tarkastuksia.

26 artikla

Kyberturvariskien hallinta toimijatasolla

1. Toimivaltaisten viranomaisten 24 artiklan 1 kohdan mukaisesti yksilöimän kunkin vaikutuksiltaan merkittävän ja vaikutuksiltaan kriittisen toimijan on huolehdittava kyberturvariskien hallinnasta merkittävien vaikutusten ja kriittisten vaikutusten vyöhykkeillään sijaitsevien kaikkien omaisuuserien suhteen. Kunkin vaikutuksiltaan merkittävän ja vaikutuksiltaan kriittisen toimijan on harjoitettava riskienhallintaa, joka kattaa joka kolmas vuosi läpikäytävät 2 kohdassa tarkoitetut vaiheet.

2. Kunkin vaikutuksiltaan merkittävän ja vaikutuksiltaan kriittisen toimijan on perustettava kyberturvariskien hallintansa lähestymistapaan, jolla pyritään suojaamaan sen verkko- ja tietojärjestelmiä ja joka käsittää seuraavat vaiheet:

a) kontekstin selvittäminen;

b) kyberturvariskien arviointi toimijatasolla;

c) kyberturvariskien käsittely; ja

d) kyberturvariskien hyväksyminen.

3. Kontekstinselvittämisvaiheessa kunkin vaikutuksiltaan merkittävän ja vaikutuksiltaan kriittisen toimijan on:

a) määriteltävä kyberturvariskien arvioinnin kohdeala, mukaan lukien Sähkö-ENTSOn ja EU DSO -elimen yksilöimät vaikutuksiltaan suuret ja vaikutuksiltaan kriittiset prosessit sekä muut prosessit, jotka voivat olla sellaisten kyberhyökkäysten kohteina, joilla on merkittävä vaikutus tai kriittinen vaikutus rajat ylittäviin sähkönsiirtoihin; ja

b) määriteltävä riskinarviointia ja riskin hyväksymistä koskevat kriteerit noudattaen riskivaikutusmatriisia, jota toimijoiden ja toimivaltaisten viranomaisten on käytettävä arvioidessaan kyberturvariskejä Sähkö-ENTSOn ja EU DSO -elimen 19 artiklan 2 kohdan mukaisesti laatimin kyberturvariskien arviointimenetelmin unionitasolla, aluetasolla ja jäsenvaltiotasolla.

4. Kyberturvariskien arviointivaiheessa kunkin vaikutuksiltaan merkittävän ja vaikutuksiltaan kriittisen toimijan on:

a) yksilöitävä kyberturvariskit ottaen huomioon seuraavat tekijät:

   i) kaikki unionitason vaikutuksiltaan merkittäviä ja vaikutuksiltaan kriittisiä prosesseja tukevat omaisuuserät sekä arvio mahdollisista vaikutuksista rajat ylittäviin sähkönsiirtoihin, jos tällainen omaisuuserä vaarantuu;

   ii) mahdolliset kyberuhat ottaen huomioon 23 artiklassa tarkoitetussa viimeisimmässä kattavassa rajat ylittävien sähköalan kyberturvariskien arviointiraportissa yksilöidyt kyberuhat ja toimitusketjuun kohdistuvat uhat;

   iii) haavoittuvuudet, mukaan lukien aiemman sukupolven järjestelmistä periytyvät haavoittuvuudet;

   iv) mahdolliset kyberhyökkäysskenaariot, mukaan lukien kyberhyökkäykset, jotka vaikuttavat sähköjärjestelmän käyttövarmuuteen ja häiritsevät rajat ylittäviä sähkönsiirtoja;

   v) asiaa koskevat unionitason riskinarvioinnit ja arviot, mukaan lukien direktiivin (EU) 2022/2555 22 artiklan mukaisesti tehdyt kriittisten toimitusketjujen koordinoidut riskinarvioinnit; ja

   vi) käytössä olevat varotoimet;

b) analysoitava a alakohdassa yksilöityjen kyberturvariskien todennäköisyyttä ja seurauksia ja määritettävä kyberturvariskitaso noudattaen riskivaikutusmatriisia, jota käytetään arvioitaessa kyberturvariskejä siirtoverkonhaltijoiden Sähkö-ENTSOn avustuksella ja yhteistyössä EU DSO -elimen kanssa 19 artiklan 2 kohdan mukaisesti laatimin kyberturvariskien arviointimenetelmin unionitasolla, aluetasolla ja jäsenvaltiotasolla;

c) luokiteltava omaisuuserät kyberturvallisuuden vaarantumisen mahdollisten seurausten mukaan ja määriteltävä vaikutuksiltaan merkittävä ja vaikutuksiltaan kriittinen vyöhyke seuraavien vaiheiden mukaisesti:

   i) suoritetaan kaikille kyberturvariskien arvioinnin kattamille prosesseille toimintaan kohdistuvien vaikutusten arviointi käyttäen ECII-indeksiä;

   ii) luokitellaan prosessi vaikutuksiltaan merkittäväksi, jos sen ECII-arvo ylittää merkittävän vaikutuksen kynnystason, tai vaikutuksiltaan kriittiseksi, jos sen ECII-arvo ylittää kriittisen vaikutuksen kynnystason;

   iii) määritellään kaikki vaikutuksiltaan merkittävät omaisuuserät omaisuuseriksi, joita tarvitaan vaikutuksiltaan merkittävissä prosesseissa, sekä vaikutuksiltaan kriittiset omaisuuserät omaisuuseriksi, joita tarvitaan vaikutuksiltaan kriittisissä prosesseissa;

   iv) määritellään vaikutuksiltaan merkittävät vyöhykkeet, jotka sisältävät kaikki vaikutuksiltaan merkittävät omaisuuserät sekä vaikutuksiltaan kriittiset vyöhykkeet, jotka sisältävät kaikki vaikutuksiltaan kriittiset omaisuuserät, jotta pääsyä näille vyöhykkeille voidaan valvoa asianmukaisesti; ja

d) arvioitava kyberturvariskit priorisoimalla ne 3 kohdan b alakohdassa tarkoitettujen riskinarviointikriteerien ja riskinhyväksyntäkriteerien avulla.

5. Kyberturvariskien käsittelyvaiheessa kunkin vaikutuksiltaan merkittävän ja vaikutuksiltaan kriittisen toimijan on laadittava toimijatason riskinlieventämissuunnitelma valitsemalla riskien hallinnan ja jäännösriskien tunnistamisen kannalta asianmukaiset riskinkäsittelyvaihtoehdot.

6. Kyberturvariskien hyväksymisvaiheessa kunkin vaikutuksiltaan merkittävän ja vaikutuksiltaan kriittisen toimijan on päätettävä, hyväksyykö se jäännösriskin 3 kohdan b alakohdan mukaisesti vahvistettujen riskinhyväksyntäkriteerien perusteella.

7. Kunkin vaikutuksiltaan merkittävän ja vaikutuksiltaan kriittisen toimijan on kirjattava 1 kohdan mukaiset omaisuuseränsä erityiseen inventaariin. Inventaaria ei saa sisällyttää riskinarviointiraporttiin.

8. Toimivaltainen viranomainen voi tarkastuksen aikana tutkia inventaariin sisällytetyt omaisuuserät.

27 artikla

Toimijatason riskinarvioinnista raportoiminen

Kunkin vaikutuksiltaan merkittävän ja vaikutuksiltaan kriittisen toimijan on 12 kuukauden kuluessa 24 artiklan 6 kohdan nojalla tehdystä vaikutukseltaan merkittävien ja vaikutukseltaan kriittisten toimijoiden tiedoksiantamisesta ja sen jälkeen joka kolmas vuosi esitettävä toimivaltaiselle viranomaiselle raportti, joka sisältää seuraavat tiedot:

1) luettelo 26 artiklan 5 kohdan nojalla tehtävään toimijatason riskinlieventämissuunnitelmaan valituista varotoimenpiteistä sekä kunkin varotoimenpiteen toteutuksen tilanne;

2) kunkin unionitason vaikutuksiltaan merkittävän tai kriittisen prosessin osalta arvio riskeistä, jotka liittyvät tietojen ja asiaankuuluvien omaisuuserien luottamuksellisuuden, eheyden ja saatavuuden vaarantumiseen; riskiarvio on esitettävä käyttäen 19 artiklan 2 kohdan nojalla laadittua riskivaikutusmatriisia; ja

3) luettelo niiden vaikutuksiltaan kriittisissä prosesseissaan käyttämistä kriittisistä tieto- ja viestintätekniikan palveluntarjoajista.

III LUKU

YHTEINEN SÄHKÖALAN KYBERTURVAKEHYS

28 artikla

Yhteisen sähköalan kyberturvakehyksen rakenne, toiminta ja uudelleentarkastelu

1. Yhteinen sähköalan kyberturvakehys koostuu seuraavasta varotoimien kokonaisuudesta ja kyberturvallisuuden hallintajärjestelmästä:

a) jäljempänä olevan 29 artiklan mukaisesti määritellyt vähimmäistason kyberturvavarotoimet;

b) jäljempänä olevan 29 artiklan mukaisesti määritellyt tiukemmat kyberturvavarotoimet;

c) jäljempänä olevan 34 artiklan mukaisesti laadittu vastaavuusmatriisi, jossa esitetään vastaavuudet a ja b alakohdassa tarkoitettujen varotoimien ja valittujen eurooppalaisten ja kansainvälisten standardien ja kansallisten lainsäädäntö- tai sääntelykehysten välillä; ja

d) jäljempänä olevan 32 artiklan mukaisesti perustettu kyberturvallisuuden hallintajärjestelmä.

2. Kaikkien vaikutuksiltaan merkittävien toimijoiden on toteutettava 1 kohdan a alakohdassa tarkoitetut vähimmäistason kyberturvavarotoimet merkittävien vaikutusten vyöhykkeellään.

3. Kaikkien vaikutuksiltaan kriittisten toimijoiden on toteutettava 1 kohdan b alakohdassa tarkoitetut tiukemmat kyberturvavarotoimet kriittisten vaikutusten vyöhykkeellään.

4. Edellä 1 kohdassa tarkoitettua yhteistä sähköalan kyberturvakehystä on täydennettävä 7 kuukauden kuluessa 19 artiklan 4 kohdan mukaisesta ensimmäisen unionitason kyberturvariskien arviointiraportin luonnoksen esittämisestä 33 artiklan nojalla määritellyillä toimitusketjulta edellytettävillä vähimmäistason ja tiukemmilla kyberturvavarotoimilla.

29 artikla

Vähimmäistason ja tiukemmat kyberturvavarotoimet

1. Siirtoverkonhaltijoiden on Sähkö-ENTSOn avustuksella ja yhteistyössä EU DSO -elimen kanssa 7 kuukauden kuluessa 19 artiklan 4 kohdan mukaisesta ensimmäisen unionitason kyberturvariskien arviointiraportin luonnoksen toimittamisesta laadittava ehdotus vähimmäistason ja tiukemmista kyberturvavarotoimista.

2. Siirtoverkonhaltijoiden on Sähkö-ENTSOn avustuksella ja yhteistyössä EU DSO -elimen kanssa 6 kuukauden kuluessa 21 artiklan 2 kohdan mukaisen ensimmäisen aluetason kyberturvariskien arviointiraportin valmistumisesta esitettävä toimivaltaiselle viranomaiselle vähimmäistason ja tiukempia kyberturvavarotoimia koskeva tarkistusehdotus. Ehdotus on laadittava 8 artiklan 10 kohdan mukaisesti ja siinä on otettava huomioon aluetason riskinarvioinnissa todetut riskit.

3. Vähimmäistason ja tiukempien kyberturvavarotoimien on oltava todennettavissa kansallisessa todentamisjärjestelmässä 31 artiklassa esitetyn menettelyn mukaisesti tai kohdistamalla niihin riippumattoman kolmannen osapuolen tekemiä 25 artiklan 2 kohdassa luetellut vaatimukset täyttäviä turvallisuusauditointeja.

4. Edellä olevan 1 kohdan nojalla määriteltyjen ensimmäisten vähimmäistason ja tiukempien kyberturvavarotoimien on perustuttava riskeihin, jotka on yksilöity 19 artiklan 5 kohdassa tarkoitetussa unionitason kyberturvariskien arviointiraportissa. Edellä olevan 2 kohdan nojalla määriteltyjen tarkistettujen vähimmäistason ja tiukempien kyberturvavarotoimien on perustuttava 21 artiklan 2 kohdassa tarkoitettuun aluetason kyberturvariskien arviointiraporttiin.

5. Vähimmäistason kyberturvavarotoimien on katettava myös varotoimet 46 artiklan nojalla vaihdettujen tietojen suojaamiseksi.

6. Edellä olevan 2 artiklan 1 kohdassa lueteltujen ja 24 artiklan nojalla vaikutuksiltaan merkittäviksi tai vaikutuksiltaan kriittisiksi yksilöityjen toimijoiden on 12 kuukauden kuluessa 8 artiklan 5 kohdan mukaisesta vähimmäistason ja tiukempien kyberturvavarotoimien hyväksymisestä ja jokaisen 8 artiklan 10 kohdan mukaisen niiden päivityksen jälkeen sovellettava 26 artiklan 5 kohdan mukaisen toimijatason riskinlieventämissuunnitelman laadinnan aikana merkittävien vaikutusten vyöhykkeellään vähimmäistason kyberturvavarotoimia ja kriittisten vaikutusten vyöhykkeellään tiukempia kyberturvavarotoimia.

30 artikla

Vapautukset vähimmäistason ja tiukemmista kyberturvavarotoimista

1. Edellä olevan 2 artiklan 1 kohdassa luetellut toimijat voivat pyytää asianomaiselta toimivaltaiselta viranomaiselta vapautusta 29 artiklan 6 kohdassa tarkoitetusta velvoitteestaan soveltaa vähimmäistason ja tiukempia kyberturvavarotoimia. Toimivaltainen viranomainen voi myöntää tällaisen vapautuksen jommallakummalla seuraavista perusteista:

a) poikkeuksellisissa olosuhteissa, joissa toimija voi osoittaa, että asianmukaisten kyberturvavarotoimien kustannukset olisivat huomattavasti niiden hyötyjä suuremmat. ACER ja Sähkö-ENTSO voivat yhteistyössä EU DSO -elimen kanssa laatia toimijoiden avuksi yhdessä ohjeistusta kyberturvavarotoimien kustannusten arviointia varten;

b) jos toimija esittää toimijatason riskinkäsittelysuunnitelman, jolla lievennetään kyberturvariskejä vaihtoehtoisilla varotoimilla tasolle, joka on hyväksyttävissä 26 artiklan 3 kohdan b alakohdassa tarkoitettujen riskin hyväksyttävyyskriteerien perusteella.

2. Kunkin toimivaltaisen viranomaisen on päätettävä kolmen kuukauden kuluessa 1 kohdassa tarkoitetun pyynnön vastaanottamisesta, voidaanko vapautus vähimmäistason tai tiukemmista kyberturvavarotoimista myöntää. Vapautukset vähimmäistason tai tiukemmista kyberturvavarotoimista voidaan myöntää enintään kolmen vuoden uusittavissa olevaksi ajanjaksoksi.

3. Anonymisoidut koontitiedot myönnetyistä vapautuksista on lisättävä liitteenä 23 artiklassa tarkoitettuun kattavaan rajat ylittävien sähköalan kyberturvariskien arviointiraporttiin. Sähkö-ENTSOn ja EU DSO -elimen on tarvittaessa yhdessä päivitettävä luetteloa.

31 artikla

Yhteisen sähköalan kyberturvakehyksen noudattamisen todentaminen

1. Viimeistään 24 kuukauden kuluttua 28 artiklan 1 kohdan a, b ja c alakohdassa tarkoitettujen varotoimien hyväksymisestä ja mainitun artiklan d alakohdassa tarkoitetun kyberturvallisuuden hallintajärjestelmän perustamisesta kunkin 24 artiklan 1 kohdan mukaisesti yksilöidyn vaikutuksiltaan kriittisen toimijan on toimivaltaisen viranomaisen pyynnöstä kyettävä osoittamaan, että se noudattaa kyberturvallisuuden hallintajärjestelmää ja on toteuttanut vähimmäistason tai tiukemmat kyberturvavarotoimet.

2. Kunkin vaikutuksiltaan kriittisen toimijan on täytettävä 1 kohdassa tarkoitettu velvoite läpikäymällä riippumattoman kolmannen osapuolen suorittamat 25 artiklan 2 kohdassa lueteltujen vaatimusten mukaiset turvallisuusauditoinnit tai osallistumalla 25 artiklan 1 kohdan mukaiseen kansalliseen todentamisjärjestelmään.

3. Todennettaessa, että vaikutuksiltaan kriittinen toimija noudattaa kyberturvallisuuden hallintajärjestelmää ja on toteuttanut vähimmäistason tai tiukemmat kyberturvavarotoimet, on käytävä läpi kaikki vaikutuksiltaan kriittisen toimijan kriittisten vaikutusten vyöhykkeellä sijaitsevat omaisuuserät.

4. Sen todentaminen, että vaikutuksiltaan kriittinen toimija noudattaa kyberturvallisuuden hallintajärjestelmää ja on toteuttanut vähimmäistason tai tiukemmat kyberturvavarotoimet, on toistettava viimeistään 36 kuukauden kuluttua ensimmäisen todentamisen päättymisestä ja sen jälkeen joka kolmas vuosi.

5. Kunkin 24 artiklan mukaisesti yksilöidyn vaikutuksiltaan kriittisen toimijan on osoitettava, että se on toteuttanut 28 artiklan 1 kohdan a, b ja c alakohdassa tarkoitetut varotoimet ja perustanut mainitun artiklan 1 kohdan d alakohdassa tarkoitetun kyberturvallisuuden hallintajärjestelmän raportoimalla todentamisen tuloksista toimivaltaiselle viranomaiselle.

32 artikla

Kyberturvallisuuden hallintajärjestelmä

1. Saatuaan toimivaltaiselta viranomaiselta 24 artiklan 6 mukaisesti ilmoituksen nimeämisestään vaikutuksiltaan merkittäväksi tai vaikutuksiltaan kriittiseksi toimijaksi kunkin vaikutuksiltaan merkittävän ja kunkin vaikutuksiltaan kriittisen toimijan on 24 kuukauden kuluessa perustettava kyberturvallisuuden hallintajärjestelmä, jota on tämän jälkeen tarkasteltava uudelleen joka kolmas vuosi ja jonka tarkoituksena on:

a) määrittää kyberturvallisuuden hallintajärjestelmän kohdeala ottaen huomioon rajapinnat ja riippuvuudet muiden toimijoiden suhteen;

b) varmistaa, että toimijan ylin johto on tietoinen asiaankuuluvista oikeudellisista velvoitteista ja osallistuu aktiivisesti kyberturvallisuuden hallintajärjestelmän toteutukseen oikea-aikaisten päätösten ja nopeiden reaktioiden kautta;

c) varmistaa, että kyberturvallisuuden hallintajärjestelmää varten on käytössä riittävät resurssit,

d) vahvistaa kyberturvaperiaatteet, jotka on dokumentoitava ja viestittävä toimijan sisäisesti ja tahoille, joihin turvallisuusriskeillä voi olla vaikutuksia;

e) osoittaa ja viestiä kyberturvallisuuden kannalta merkityksellisten toimenkuvien vastuut;

f) harjoittaa kyberturvariskien hallintaa toimijatasolla 26 artiklan mukaisesti;

g) määrittää ja tarjota tarvittavat resurssit kyberturvallisuuden hallintajärjestelmän toteuttamiseen, ylläpitoon ja jatkuvaan parantamiseen ottaen huomioon kyberturvaresursseihin liittyvä tarvittava pätevyys ja tietämys;

h) määritellä kyberturvallisuuden kannalta merkityksellinen sisäinen ja ulkoinen viestintä;

i) laatia, pitää ajan tasalla ja valvoa kyberturvallisuuden hallintajärjestelmään liittyvää dokumentoitua tietoa;

j) arvioida kyberturvallisuuden hallintajärjestelmän toimivuutta ja vaikuttavuutta;

k) suorittaa määräajoin sisäisiä tarkastuksia sen varmistamiseksi, että kyberturvallisuuden hallintajärjestelmää tosiasiallisesti käytetään ja ylläpidetään; ja

l) tarkastella määräajoin uudelleen kyberturvallisuuden hallintajärjestelmän toteutusta sekä valvoa, että resurssit ja toiminnot ovat kyberturvallisuuden hallintajärjestelmän toimintaperiaatteiden, menettelyjen ja ohjeistuksen mukaisia ja korjata mahdolliset puutteet.

2. Kyberturvallisuuden hallintajärjestelmän on katettava kaikki omaisuuserät vaikutuksiltaan merkittävän toimijan ja vaikutuksiltaan kriittisen toimijan merkittävien vaikutusten vyöhykkeellä ja kriittisten vaikutusten vyöhykkeellä.

3. Toimivaltaisten viranomaisten on tietyntyyppistä teknologiaa edellyttämättä tai suosimatta kannustettava käyttämään hallintajärjestelmiin liittyviä eurooppalaisia tai kansainvälisiä standardeja ja eritelmiä, joilla on merkitystä verkko- ja tietojärjestelmien turvallisuuden kannalta.

33 artikla

Vähimmäistason ja tiukemmat kyberturvavarotoimet toimitusketjussa

1. Siirtoverkonhaltijoiden on Sähkö-ENTSOn avustuksella ja yhteistyössä EU DSO -elimen kanssa 7 kuukauden kuluessa 19 artiklan 4 kohdan mukaisesta ensimmäisen unionitason kyberturvariskien arviointiraportin luonnoksen toimittamisesta laadittava ehdotus toimitusketjun vähimmäistason ja tiukemmista kyberturvavarotoimista, joilla lievennetään unionitason kyberturvariskien arvioinneissa yksilöityjä toimitusketjun riskejä ja täydennetään 29 artiklan nojalla määriteltyjä vähimmäistason ja tiukempia kyberturvavarotoimia. Toimitusketjuun kohdistettavat vähimmäistason ja tiukemmat kyberturvavarotoimet on määriteltävä yhdessä 29 artiklan nojalla määriteltävien vähimmäistason ja tiukempien kyberturvavarotoimien kanssa. Toimitusketjuun kohdistettavien vähimmäistason ja tiukempien kyberturvavarotoimien on katettava vaikutuksiltaan merkittävän tai vaikutuksiltaan kriittisen toimijan merkittävien vaikutusten vyöhykkeellä tai kriittisten vaikutusten vyöhykkeellä sijaitsevien kaikkien tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien koko elinkaari. Laadittaessa ehdotusta toimitusketjuun kohdistettavista vähimmäistason ja tiukemmista kyberturvavarotoimista on kuultava verkko- ja tietoturva-alan yhteistyöryhmää.

2. Toimitusketjuun kohdistettavien, vaikutuksiltaan merkittävien ja vaikutuksiltaan kriittisten toimijoiden vähimmäistason kyberturvavarotoimien on:

a) sisällettävä kyberturvallisuuseritelmiin viittaavat tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien hankintasuositukset kattaen ainakin seuraavat seikat:

   i) toimitusketjuun osallistuvan ja arkaluonteista tietoa käsittelevän tahon tai sellaisen tahon, joka pääsee käsiksi toimijan vaikutuksiltaan kriittisiin omaisuuseriin, henkilöstön taustojen selvittäminen; taustatarkistuksessa voidaan muun muassa todentaa toimijan henkilöstön tai alihankkijoiden henkilöllisyys ja taustat noudattaen kansallista lainsäädäntöä ja kansallisia menettelyjä sekä asiaa koskevaa sovellettavaa unionin lainsäädäntöä, kuten asetusta (EU) 2016/679 ja Euroopan parlamentin ja neuvoston direktiiviä (EU) 2016/680 ([18]); taustatarkistusten on oltava oikeasuhteisia ja rajattuja välttämättömään; ne on toteutettava ainoastaan asianomaiseen toimijaan kohdistuvan mahdollisen turvallisuusriskin arvioimiseksi; niiden on oltava oikeassa suhteessa toiminnan asettamiin vaatimuksiin, käsiteltäviksi tulevien tietojen luottamuksellisuustasoon ja oletettuihin riskeihin, ja ne voi suorittaa toimija itse, taustatarkistuksia tekevä ulkopuolinen yritys tai taustatarkistuksia tekevä valtion elin;

   ii) tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien turvallista ja valvottua suunnittelua, kehittämistä ja tuotantoa koskevat prosessit, suosien sellaista tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien suunnittelua ja kehittämistä, jossa otetaan huomioon asianmukaiset tekniset ratkaisut kyberturvallisuuden varmistamiseksi;

   iii) verkko- ja tietojärjestelmien järjestäminen niin, että laitteisiin ei luoteta edes silloin, kun ne ovat suojatulla vyöhykkeellä, edellytetään järjestelmille esitettyjen kaikkien pyyntöjen todentamista ja sovelletaan vähäisimpien oikeuksien periaatetta (*principle of least privilege*);

   iv) kyseisen tahon pääsy käsiksi toimijan omaisuuseriin;

([18]) Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta (EUVL L 119, 4.5.2016, s. 89).

v) kyseisen tahon sopimusperusteiset velvoitteet suojata toimijan arkaluonteisia tietoja ja rajoittaa pääsyä niihin;

vi) kyseisen tahon alihankkijoita koskevat kyberturvallisia hankintoja ohjaavat eritelmät;

vii) kyberturvallisuuseritelmien noudattamisen jäljitettävyys tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien kehittämisestä tuottamiseen saakka;

viii) tietoturvapäivitystuki tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien koko elinkaaren ajan;

ix) oikeus auditoida kyseisen tahon suunnittelu-, kehitys- ja tuotantoprosessien kyberturvallisuus; ja

x) kyseisen tahon riskiprofiilin arviointi;

b) vaadittava tällaisia toimijoita ottamaan huomioon a alakohdassa tarkoitetut hankintasuositukset, kun ne tekevät sopimuksia alihankkijoiden, yhteistyökumppaneiden ja muiden toimitusketjun osapuolten kanssa kattaen tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien tavanomaiset toimitukset sekä poikkeukselliset tapahtumat ja olosuhteet, kuten sopimusten irtisanominen ja siirtäminen sopimuskumppanin laiminlyöntitapauksissa;

c) vaadittava tällaisia toimijoita ottamaan huomioon direktiivin (EU) 2022/2555 22 artiklan 1 kohdan mukaisesti tehtyjen, kriittisten toimitusketjujen koordinoitujen riskinarviointien tulokset;

d) sisällettävä kriteerit sellaisten tahojen valinnalle, jotka voivat täyttää a alakohdassa tarkoitetut kyberturvavaatimukset ja joiden kyberturvataso on asianmukainen suhteessa kyseisen tahon toimittamien tieto- ja viestintätekniikan tuotteiden, palvelujen tai prosessien kyberturvariskeihin;

e) sisällettävä kriteerit tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien hankintalähteiden monipuolistamiseksi ja toimittajariippuvuuden riskin pienentämiseksi; ja

f) sisällettävä kriteerit toimittajan sisäisten toimintaprosessien kyberturvavaatimusten seuraamiseksi, tarkastamiseksi tai auditoimiseksi säännöllisesti kunkin tieto- ja viestintätekniikan tuotteen, palvelun ja prosessin koko elinkaaren ajan.

3. Edellä 2 kohdan a alakohdassa tarkoitettuun kyberturvahankintasuositukseen sisältyvien kyberturvavaatimusten osalta vaikutuksiltaan merkittävien tai vaikutuksiltaan kriittisten toimijoiden on käytettävä Euroopan parlamentin ja neuvoston direktiivin 2014/24/EU ([19]) sisältämiä hankintaperiaatteita 35 artiklan 4 kohdan mukaisesti tai määriteltävä omat vaatimuksensa toimijatason kyberturvariskien arvioinnin tulosten perusteella.

4. Toimitusketjun tiukempiin kyberturvavarotoimiin on sisällyttävä varotoimet, joiden myötä vaikutuksiltaan kriittiset toimijat voivat todentaa hankintamenettelyissä, että vaikutuksiltaan kriittisinä omaisuuserinä käytettävät tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit täyttävät kyberturvavaatimukset. Tieto- ja viestintätekniikan tuote, palvelu tai prosessi on hyväksyttävä joko 31 artiklassa tarkoitetulla eurooppalaisella kyberturvallisuuden sertifiointijärjestelmällä tai toimijan valitsemilla ja järjestämillä hyväksymismenettelyillä. Hyväksymismenettelyjen on oltava riittävän perusteellisia ja kattavia, jotta saadaan varmuus siitä, että tieto- ja viestintätekniikan tuotetta, palvelua tai prosessia voidaan käyttää toimijatason riskinarvioinnissa yksilöityjen riskien lieventämiseen. Vaikutuksiltaan kriittisen toimijan on dokumentoitava toimenpiteet, jotka on toteutettu yksilöityjen riskien lieventämiseksi.

5. Toimitusketjuun kohdistettavia vähimmäistason ja tiukempia kyberturvavarotoimia on sovellettava asiaankuuluvien tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien hankintoihin. Toimitusketjuun kohdistettavia vähimmäistason ja tiukempia kyberturvavarotoimia sovelletaan 24 artiklan nojalla vaikutuksiltaan merkittäviksi ja vaikutuksiltaan kriittisiksi toimijoiksi yksilöityjen toimijoiden hankintaprosesseihin, jotka alkavat kuuden kuukauden kuluttua 29 artiklassa tarkoitettujen vähimmäistason ja tiukempien kyberturvavarotoimien hyväksymisestä tai päivittämisestä.

([19]) Euroopan parlamentin ja neuvoston direktiivi 2014/24/EU, annettu 26 päivänä helmikuuta 2014, julkisista hankinnoista ja direktiivin 2004/18/EY kumoamisesta (EUVL L 94, 28.3.2014, s. 65).

6. Siirtoverkonhaltijoiden on Sähkö-ENTSOn avustuksella ja yhteistyössä EU DSO -elimen kanssa 6 kuukauden kuluessa 21 artiklan 2 kohdan mukaisen ensimmäisen aluetason kyberturvariskien arviointiraportin valmistumisesta esitettävä toimivaltaiselle viranomaiselle toimitusketjuun kohdistettavia vähimmäistason ja tiukempia kyberturvavarotoimia koskeva tarkistusehdotus. Ehdotus on laadittava 8 artiklan 10 kohdan mukaisesti ja siinä on otettava huomioon aluetason riskinarvioinnissa todetut riskit.

34 artikla

Sähköalan kyberturvavarotoimien ja standardien vastaavuusmatriisi

1. Siirtoverkonhaltijoiden on Sähkö-ENTSOn avustuksella, yhteistyössä EU DSO -elimen kanssa ja ENISAa kuullen 7 kuukauden kuluessa 19 artiklan 4 kohdan mukaisesta ensimmäisen unionitason kyberturvariskien arviointiraportin luonnoksen toimittamisesta laadittava ehdotus vastaavuusmatriisiksi, jossa esitetään vastaavuudet 28 artiklan 1 kohdan a ja b alakohdassa esitettyjen varotoimien ja valittujen eurooppalaisten ja kansainvälisten standardien sekä asiaankuuluvien teknisten eritelmien välillä. Sähkö-ENTSOn ja EU DSO -elimen on dokumentoitava eri varotoimien vastaavuus 28 artiklan 1 kohdan a ja b alakohdassa esitettyjen varotoimien kanssa.

2. Toimivaltaiset viranomaiset voivat toimittaa Sähkö-ENTSOlle ja EU DSO -elimelle 28 artiklan 1 kohdan a ja b alakohdassa esitettyjen varotoimien vastaavuudet viittauksin asiaa koskeviin kansallisiin lainsäädäntö- tai sääntelykehyksiin, mukaan lukien direktiivin (EU) 2022/2555 25 artiklan mukaiset jäsenvaltioiden asiaa koskevat kansalliset standardit. Jos jäsenvaltion toimivaltainen viranomainen toimittaa tällaisen vastaavuusselvityksen, Sähkö-ENTSOn ja EU DSO -elimen on sisällytettävä se vastaavuusmatriisiin.

3. Siirtoverkonhaltijoiden on Sähkö-ENTSOn avustuksella, yhteistyössä EU DSO -elimen kanssa ja ENISAa kuullen 6 kuukauden kuluessa 21 artiklan 2 kohdan mukaisen ensimmäisen aluetason kyberturvariskien arviointiraportin valmistumisesta esitettävä toimivaltaiselle viranomaiselle vastaavuusmatriisia koskeva tarkistusehdotus. Ehdotus on laadittava 8 artiklan 10 kohdan mukaisesti ja siinä on otettava huomioon aluetason riskinarvioinnissa todetut riskit.

IV LUKU

KYBERTURVAHANKINTASUOSITUKSET

35 artikla

Kyberturvahankintasuositukset

1. Siirtoverkonhaltijoiden on Sähkö-ENTSOn avustuksella ja yhteistyössä EU DSO -elimen kanssa laadittavassa työohjelmassa, joka vahvistetaan ja päivitetään aina, kun aluetason kyberturvariskien arviointiraportti hyväksytään, esitettävä ei-sitovia kyberturvahankintasuosituksia, joita vaikutuksiltaan merkittävät ja vaikutuksiltaan kriittiset toimijat voivat käyttää perustana hankkiessaan tieto- ja viestintätekniikan tuotteita, palveluja ja prosesseja merkittävien vaikutusten vyöhykkeille ja kriittisten vaikutusten vyöhykkeille. Työohjelman on sisällettävä seuraavat tekijät:

a) vaikutuksiltaan merkittävien ja vaikutuksiltaan kriittisten toimijoiden merkittävien vaikutusten vyöhykkeillään ja kriittisten vaikutusten vyöhykkeillään käyttämien tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien tyyppien kuvaus ja luokitus; ja

b) luettelo tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien tyypeistä, joita varten laaditaan ei-sitovia kyberturvasuosituksia asiaankuuluvien aluetason kyberturvariskien arviointiraporttien sekä vaikutuksiltaan merkittävien ja vaikutuksiltaan kriittisten toimijoiden prioriteettien perusteella.

2. Sähkö-ENTSOn on yhteistyössä EU DSO -elimen kanssa toimitettava ACERille kuuden kuukauden kuluessa aluetason kyberturvariskien arviointiraportin hyväksymisestä tai päivityksestä yhteenveto kyseisestä työohjelmasta.

3. Siirtoverkonhaltijoiden on Sähkö-ENTSOn avustuksella ja yhteistyössä EU DSO -elimen kanssa pyrittävä varmistamaan, että kunkin aluetason kyberturvariskien arvioinnin perusteella laaditut ei-sitovat kyberturvahankintasuositukset ovat samankaltaisia tai vastaavia kaikilla käyttöalueilla. Kyberturvahankintasuositusten on katettava vähintään 33 artiklan 2 kohdan a alakohdassa tarkoitetut eritelmät. Eritelmät on mahdollisuuksien mukaan valittava eurooppalaisista ja kansainvälisistä standardeista.

4. Siirtoverkonhaltijoiden on Sähkö-ENTSOn avustuksella ja yhteistyössä EU DSO -elimen kanssa varmistettava, että kyberturvahankintasuositukset:

a) noudattavat direktiivissä 2014/24/EU säädettyjä hankintaperiaatteita; ja

b) ovat yhteensopivia tieto- ja viestintätekniikan tuotteen, palvelun tai prosessin kannalta merkityksellisten viimeisimpien saatavilla olevien eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien kanssa ja ottavat ne huomioon.

36 artikla

Ohjeistus eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien käytöstä tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien hankinnassa

1. Edellä olevan 35 artiklan nojalla laaditut ei-sitovat kyberturvahankintasuositukset voivat sisältää toimialakohtaista ohjeistusta eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien käytöstä siltä osin kuin käytettävissä on sopiva järjestelmä tietyntyyppiselle vaikutuksiltaan kriittisten toimijoiden käyttämälle tieto- ja viestintätekniikan tuotteelle, palvelulle tai prosessille, sanotun kuitenkaan vaikuttamatta asetuksen (EU) 2019/881 46 artiklan mukaiseen eurooppalaiseen kyberturvallisuuden sertifiointikehykseen.

2. Siirtoverkonhaltijoiden on Sähkö-ENTSOn avustuksella ja yhteistyössä EU DSO -elimen kanssa tehtävä tiivistä yhteistyötä ENISAn kanssa antaessaan 1 kohdan mukaista kyberturvahankintasuosituksiin sisältyvää ei-sitovaa alakohtaista ohjeistusta.

V LUKU

TIEDONKULKU, KYBERHYÖKKÄYKSET JA KRIISINHALLINTA

37 artikla

Tietojen jakamista koskevat säännöt

1. Jos toimivaltainen viranomainen saa tietoa raportoitavasta kyberhyökkäyksestä, sen on:

a) arvioitava tietojen luottamuksellisuuden taso ja ilmoitettava kyseiselle toimijalle arviointinsa tuloksesta ilman aiheetonta viivytystä ja viimeistään 24 tunnin kuluessa tietojen vastaanottamisesta;

b) pyrittävä tunnistamaan unionissa muita samankaltaisia kyberhyökkäyksiä, joista on ilmoitettu muille toimivaltaisille viranomaisille, jotta raportoitavan kyberhyökkäyksen yhteydessä saadut tiedot voidaan yhdistää muiden kyberhyökkäysten yhteydessä toimitettuihin tietoihin ja täydentää olemassa olevaa tietoa sekä vahvistaa ja koordinoida reagointitapoja;

c) vastattava liikesalaisuuksien poistamisesta ja tietojen anonymisoinnista asiaa koskevien kansallisten ja unionin sääntöjen mukaisesti;

d) jaettava tiedot kansallisille keskitetyille yhteyspisteille, CSIRT-yksiköille ja kaikille 4 artiklan nojalla nimetyille muiden jäsenvaltioiden toimivaltaisille viranomaisille ilman aiheetonta viivytystä ja viimeistään 24 tunnin kuluessa raportoitavaa kyberhyökkäystä koskevan tiedon vastaanottamisesta ja toimitettava kyseisille viranomaisille tai elimille säännöllisesti päivityksiä;

e) jaettava kyberhyökkäystä koskevat tiedot, sen jälkeen, kun ne on anonymisoitu ja niistä on poistettu c alakohdassa tarkoitetut liikesalaisuudet, jäsenvaltionsa vaikutuksiltaan kriittisille ja vaikutuksiltaan merkittäville toimijoille ilman aiheetonta viivytystä ja viimeistään 24 tunnin kuluessa a alakohdan mukaisten tietojen vastaanottamisesta ja toimitettava säännöllisesti päivityksiä, jotta toimijat voivat tuloksellisesti organisoida vastatoimensa;

f) niin halutessaan pyydettävä raportoivia vaikutuksiltaan merkittäviä tai vaikutuksiltaan kriittisiä toimijoita jakamaan raportoitavaa kyberhyökkäystietoa edelleen suojatusti muille toimijoille, joihin asia voi vaikuttaa, jotta voidaan vahvistaa tilannetietoisuutta sähköalalla ja estää sellaisen riskin toteutuminen, joka voi sähköalalla eskaloitua rajat ylittäväksi kyberturvallisuuspoikkeamaksi; ja

g) esitettävä ENISAlle tiedot kyberhyökkäyksestä sisältävä anonymisoitu tiivistelmäraportti, josta on poistettu liikesalaisuudet.

2. Jos CSIRT-yksikkö tulee tietoiseksi aktiivisesti hyväksikäytetystä paikkaamattomasta haavoittuvuudesta, sen on:

a) ilmoitettava siitä ENISAlle viipymättä asianmukaisen suojatun tietojenvaihtokanavan kautta, jollei muussa unionin lainsäädännössä toisin säädetä;

b) autettava kyseessä olevaa toimijaa saamaan valmistajalta tai palveluntarjoajalta tuloksellinen, koordinoitu ja nopea ratkaisu tai tuloksellinen ja tehokas lieventämistoimien kokonaisuus aktiivisesti hyväksikäytetyn paikkaamattoman haavoittuvuuden suhteen;

c) toimitettava saatavilla olevat tiedot laitteiston tai ohjelmiston myyjälle ja pyydettävä valmistajaa tai palveluntarjoajaa laatimaan mahdollisuuksien mukaan luettelo CSIRT-yksiköistä niissä jäsenvaltioissa, joita aktiivisesti hyväksikäytetty paikkaamaton haavoittuvuus koskee, ja joille on ilmoitettava asiasta;

d) jaettava saatavilla olevat tiedot edellä olevan alakohdan mukaisesti yksilöityjen CSIRT-yksiköiden kanssa noudattaen tiedonsaantitarpeen periaatetta; ja

e) jaettava mahdolliset tiedot aktiivisesti hyväksikäytettyä paikkaamatonta haavoittuvuutta koskevista lieventämisstrategioista ja -toimenpiteistä.

3. Jos toimivaltainen viranomainen tulee tietoiseksi aktiivisesti hyväksikäytetystä paikkaamattomasta haavoittuvuudesta, sen on:

a) jaettava jäsenvaltionsa CSIRT-yksiköiden kanssa koordinoidusti mahdolliset tiedot aktiivisesti hyväksikäytettyä paikkaamatonta haavoittuvuutta koskevista lieventämisstrategioista ja -toimenpiteistä; ja

b) jaettava kyseiset tiedot sen jäsenvaltion CSIRT-yksikön kanssa, jossa aktiivisesti hyväksikäytetty paikkaamaton haavoittuvuus on raportoitu.

4. Jos toimivaltainen viranomainen saa tietoonsa paikkaamattoman haavoittuvuuden, jonka aktiivisesta hyväksikäytöstä ei vielä ole näyttöä, sen on ilman aiheetonta viivytystä ryhdyttävä koordinoimaan toimintaansa CSIRT-yksikön kanssa direktiivin (EU) 2022/2555 12 artiklan 1 kohdassa säädettyä koordinoitua haavoittuvuuden julkistamista silmällä pitäen.

5. Jos CSIRT-yksikkö saa 38 artiklan 6 kohdan nojalla kyberuhkiin liittyviä tietoja yhdeltä tai useammalta vaikutuksiltaan merkittävältä tai vaikutuksiltaan kriittiseltä toimijalta, sen on toimitettava kyseiset tiedot tai muut tiedot, jotka ovat tärkeitä asiaan liittyvän riskin ehkäisemiseksi, havaitsemiseksi, riskiin reagoimiseksi tai sen lieventämiseksi vaikutuksiltaan kriittisille ja vaikutuksiltaan merkittäville toimijoille jäsenvaltiossaan ja tarvittaessa kaikille asiaan liittyville CSIRT-yksiköille ja kansalliselle keskitetylle yhteyspisteelleen ilman aiheetonta viivytystä ja viimeistään neljän tunnin kuluessa tietojen vastaanottamisesta.

6. Jos toimivaltainen viranomainen saa yhdeltä tai useammalta vaikutuksiltaan merkittävältä tai vaikutuksiltaan kriittiseltä toimijalta tietoa kyberuhkista, sen on 5 kohdan tarkoituksia varten toimitettava nämä tiedot edelleen CSIRT-yksikölle.

7. Toimivaltaiset viranomaiset voivat siirtää kokonaan tai osittain 3 ja 4 kohdan mukaiset vastuut, jotka koskevat yhtä tai useampaa useammassa kuin yhdessä jäsenvaltiossa toimivaa vaikutuksiltaan merkittävää tai vaikutuksiltaan kriittistä toimijaa, jollekin toiselle toimivaltaiselle viranomaiselle jossakin näistä jäsenvaltioista, jos tästä on sovittu asianomaisten toimivaltaisten viranomaisten kesken.

8. Siirtoverkonhaltijoiden on Sähkö-ENTSOn avustuksella ja yhteistyössä EU DSO -elimen kanssa laadittava 13 päivään kesäkuuta 2025 mennessä kyberhyökkäysten luokittelumenetelmä. Siirtoverkonhaltijat voivat Sähkö-ENTSOn ja EU DSO -elimen avustuksella pyytää toimivaltaisia viranomaisia kuulemaan ENISAa ja niiden kyberturvallisuudesta vastaavia toimivaltaisia viranomaisia saadakseen apua luokittelumenetelmän laatimisessa. Menetelmän on mahdollistettava kyberhyökkäyksen luokittelu vakavuusasteeltaan viiden tason mukaan siten, että kaksi korkeinta tasoa ovat ’merkittävä’ ja ’kriittinen’. Luokituksen on perustuttava seuraavien muuttujien arviointiin:

a) potentiaaliset vaikutukset 26 artiklan 4 kohdan c alakohdan mukaisesti määriteltyihin altistuviin omaisuuseriin ja vyöhykkeisiin; ja

b) kyberhyökkäyksen vakavuus.

9. Sähkö-ENTSOn on 13 päivään kesäkuuta 2026 mennessä tehtävä yhteistyössä EU DSO -elimen kanssa toteutettavuustutkimus, jossa arvioidaan mahdollisuutta kehittää yhteinen väline, jonka avulla kaikki toimijat voivat jakaa tietoja asiaankuuluvien kansallisten viranomaisten kanssa, ja tästä aiheutuvia kustannuksia.

10. Toteutettavuustutkimuksessa on tarkasteltava mahdollisuutta, että tällainen yhteinen väline:

a) tukisi vaikutuksiltaan kriittisiä ja vaikutuksiltaan merkittäviä toimijoita asiaankuuluvalla rajat ylittäviin sähkönsiirtoihin liittyvällä turvallisuustiedolla, kuten kyberhyökkäysten lähes reaaliaikailla raportoinnilla, kyberturvakysymyksiin liittyvillä ennakkovaroituksilla ja tiedoilla sähköjärjestelmässä käytössä olevien laitteiden julkistamattomista haavoittuvuuksista;

b) olisi ylläpidettävissä tarkoituksenmukaisessa ja erittäin luotettavassa ympäristössä; ja

c) mahdollistaisi tietojen keräämisen vaikutuksiltaan kriittisiltä ja vaikutuksiltaan merkittäviltä toimijoilta ja helpottaisi luottamuksellisten tietojen poistamista ja tietojen anonymisointia ja niiden nopeaa levittämistä vaikutuksiltaan kriittisille ja vaikutuksiltaan merkittäville toimijoille.

11. Sähkö-ENTSOn on yhteistyössä EU DSO -elimen kanssa:

a) kuultava toteutettavuutta arvioidessaan ENISAa ja verkko- ja tietoturva-alan yhteistyöryhmää, kansallisia keskitettyjä yhteyspisteitä ja tärkeimpien sidosryhmien edustajia; ja

b) esitettävä toteutettavuustutkimuksen tulokset ACERille ja verkko- ja tietoturva-alan yhteistyöryhmälle.

12. Sähkö-ENTSO voi yhteistyössä EU DSO -elimen kanssa analysoida ja tukea vaikutuksiltaan kriittisten ja vaikutuksiltaan merkittävien toimijoiden aloitteita tällaisten tiedonvaihtovälineiden arvioimiseksi ja testaamiseksi.

38 artikla

Vaikutuksiltaan merkittävien ja vaikutuksiltaan kriittisten toimijoiden rooli tietojen jakamisessa

1. Kunkin vaikutuksiltaan merkittävän ja vaikutuksiltaan kriittisen toimijan on:

a) luotava 26 artiklan 4 kohdan c alakohdan nojalla määritetyillä kyberturvavyöhykkeillään sijaitsevien kaikkien omaisuuserien osalta vähintään kyberturvaoperaatiokeskukselle valmiudet, joiden turvin voidaan:

   i) varmistaa, että asiaankuuluvat verkko- ja tietojärjestelmät ja sovellukset tuottavat tietoturvalokeja turvallisuusseurantaa varten, jotta voidaan havaita poikkeamat ja kerätä tietoa kyberhyökkäyksistä;

   ii) harjoittaa turvallisuusseurantaa, kuten huomata tunkeutumiset verkko- ja tietojärjestelmiin ja arvioida verkko- ja tietojärjestelmien haavoittuvuuksia;

   iii) tehdä tarvittavat analyysit ja tarvittaessa toteuttaa kaikki kyberturvaoperaatiokeskuksen vastuulla olevat ja sen kapasiteetin puitteissa mahdolliset toimet toimijan suojaamiseksi; ja

   iv) osallistua tässä artiklassa kuvattuun tietojen keruuseen ja jakamiseen;

b) omattava oikeus hankkia osittain tai kokonaan tietoturvapalveluntarjoajilta a alakohdan nojalla edellytetyt valmiudet; vaikutuksiltaan kriittiset ja vaikutuksiltaan merkittävät toimijat pysyvät vastuussa tietoturvapalveluntarjoajien toiminnasta ja niiden on valvottava näiden toimintaa; ja

c) nimettävä toimijatasolla keskitetty yhteyspiste tietojen jakamista varten.

2. ENISA voi osana asetuksen (EU) 2019/881 6 artiklan 2 kohdassa määriteltyä tehtäväänsä antaa ei-sitovaa ohjeistusta tällaisten valmiuksien rakentamisesta tai hankkimisesta tietoturvapalveluntarjoajilta.

3. Kunkin vaikutuksiltaan kriittisen ja vaikutuksiltaan merkittävän toimijan on jaettava raportoitavaan kyberhyökkäykseen liittyvät asiaankuuluvat tiedot CSIRT-yksikkönsä ja toimivaltaisen viranomaisensa kanssa ilman aiheetonta viivytystä ja viimeistään neljän tunnin kuluessa tultuaan tietoiseksi siitä, että kyseinen poikkeama on raportoitava.

4. Kyberhyökkäykseen liittyvät tiedot katsotaan raportoitaviksi, kun asianomainen toimija arvioi kyberhyökkäyksen vakavuuden 37 artiklan 8 kohdan nojalla laaditulla kyberhyökkäysten luokitusasteikolla 'merkittäväksi' tai 'kriittiseksi'. Edellä olevan 1 kohdan c alakohdan nojalla nimetyn toimijatason keskitetyn yhteyspisteen on ilmoitettava poikkeaman luokitus.

5. Kun vaikutuksiltaan kriittiset ja vaikutuksiltaan merkittävät toimijat toimittavat CSIRT-yksikölle tietoa aktiivisesti hyväksikäytetyistä paikkaamattomista haavoittuvuuksista, se voi toimittaa tiedot edelleen toimivaltaiselle viranomaiselleen. Ilmoitettujen tietojen arkaluonteisuuden perusteella CSIRT-yksikkö voi pidättäytyä toimittamasta tietoja tai lykätä niiden toimittamista edelleen perustelluista kyberturvallisuuteen liittyvistä syistä.

6. Kunkin vaikutuksiltaan kriittisen ja vaikutuksiltaan merkittävän toimijan on ilman aiheetonta viivytystä toimitettava CSIRT-yksiköilleen kaikki sellaiseen raportoitavaan kyberuhkaan liittyvät tiedot, jolla voi olla rajat ylittäviä vaikutuksia. Kyberuhkaan liittyvät tiedot katsotaan raportoitaviksi, jos vähintään yksi seuraavista edellytyksistä täyttyy:

a) tiedot auttavat muita vaikutuksiltaan kriittisiä ja vaikutuksiltaan merkittäviä toimijoita ehkäisemään tai havaitsemaan riskin, reagoimaan siihen tai lieventämään sen vaikutuksia;

b) hyökkäyksen yhteydessä tunnistetut tekniikat, taktiikat ja menettelyt antavat tietoa esimerkiksi vaarantuneista URL- tai IP-osoitteista, hajakoodeista (*hash*) tai muista tekijöistä, joista voi olla hyötyä hyökkäyksen kontekstualisoinnissa ja korreloinnissa; ja

c) kyberuhkaa voidaan arvioida ja kontekstualisoida tarkemmin tämän asetuksen soveltamisalaan kuulumattomien palveluntarjoajien tai kolmansien osapuolten toimittamien lisätietojen avulla.

7. Kunkin vaikutuksiltaan kriittisen ja vaikutuksiltaan merkittävän toimijan on tämän artiklan nojalla tietoja jakaessaan täsmennettävä seuraavat seikat:

a) maininta siitä, että tiedot toimitetaan tämän asetuksen nojalla;

b) koskevatko tiedot:

   i) edellä 3 kohdassa tarkoitettua raportoitavaa kyberhyökkäystä;

   ii) edellä 4 kohdassa tarkoitettuja aktiivisesti hyväksikäytettyjä paikkaamattomia haavoittuvuuksia, jotka eivät ole julkisesti tiedossa; vai

   iii) edellä 5 kohdassa tarkoitettua raportoitavaa kyberuhkaa;

c) jos kyseessä on raportoitava kyberhyökkäys, 37 artiklan 8 kohdassa tarkoitetun kyberhyökkäysten luokitusmenetelmän mukainen kyberhyökkäyksen luokka ja tämän luokituksen syy, mukaan lukien ainakin kyberhyökkäyksen vakavuus.

8. Kun vaikutuksiltaan kriittinen tai vaikutuksiltaan merkittävä toimija ilmoittaa merkittävästä poikkeamasta direktiivin (EU) 2022/2555 23 artiklan nojalla ja kyseisen artiklan mukainen poikkeamaraportointi sisältää tämän artiklan 3 kohdassa vaaditut asiaankuuluvat tiedot, kyseisen direktiivin 23 artiklan 1 kohdan mukainen toimijan raportointi on katsottava tämän artiklan 3 kohdan mukaiseksi tietojen ilmoittamiseksi.

9. Kunkin vaikutuksiltaan kriittisen ja vaikutuksiltaan merkittävän toimijan on raportoinnissaan toimivaltaiselle viranomaiselleen tai CSIRT-yksikölle yksilöitävä selkeästi tietyt tiedot, jotka on jaettava ainoastaan toimivaltaisen viranomaisen tai CSIRT-yksikön kanssa tapauksissa, joissa tietojen jakaminen voisi olla kyberhyökkäyksen lähde. Kullakin vaikutuksiltaan kriittisellä ja vaikutuksiltaan merkittävällä toimijalla on oltava oikeus toimittaa tiedoista ei-luottamuksellinen versio toimivaltaiselle CSIRT-yksikölle.

39 artikla

Kyberhyökkäysten havaitseminen ja niihin liittyvän tiedon käsittely

1. Vaikutuksiltaan kriittisten ja vaikutuksiltaan merkittävien toimijoiden on kehitettävä tarvittavat valmiudet havaittujen kyberhyökkäysten käsittelemiseksi asiaankuuluvan toimivaltaisen viranomaisen, Sähkö-ENTSOn ja EU DSO -elimen tarvittavalla tuella. Vaikutuksiltaan kriittiset ja vaikutuksiltaan merkittävät toimijat voivat saada jäsenvaltionsa nimetyltä CSIRT-yksiköltä tukea osana direktiivin (EU) 2022/2555 11 artiklan 5 kohdan a alakohdassa CSIRT-yksiköille osoitettua tehtävää. Vaikutuksiltaan kriittisillä ja vaikutuksiltaan merkittävillä toimijoilla on oltava toimivat prosessit sellaisten kyberhyökkäysten tunnistamiseksi, luokittelemiseksi ja niihin reagoimiseksi, jotka vaikuttavat tai voivat vaikuttaa rajat ylittäviin sähkönsiirtoihin, jotta niiden vaikutus voidaan minimoida.

2. Jos kyberhyökkäys vaikuttaa rajat ylittäviin sähkönsiirtoihin, vaikutuksiltaan kriittisten ja vaikutuksiltaan merkittävien toimijoiden toimijatason keskitettyjen yhteyspisteiden on tehtävä yhteistyötä tietojen jakamiseksi niiden kesken sen jäsenvaltion toimivaltaisen viranomaisen koordinoimina, jossa kyberhyökkäyksestä raportoitiin ensimmäisen kerran.

3. Vaikutuksiltaan kriittisten ja vaikutuksiltaan merkittävien toimijoiden on:

a) varmistettava, että niiden toimijatason keskitetyllä yhteyspisteellä on tiedonsaantitarpeen perusteella pääsy tietoihin, jotka ne ovat saaneet kansalliselta keskitetyltä yhteyspisteeltä toimivaltaisen viranomaisensa kautta;

b) ellei näin ole jo tehty direktiivin (EU) 2022/2555 3 artiklan 4 kohdan nojalla, ilmoitettava sen jäsenvaltion toimivaltaiselle viranomaiselle, johon ne ovat sijoittautuneet, ja kansalliselle keskitetylle yhteyspisteelle luettelo niiden kyberturvasta vastaavista toimijatason keskitetyistä yhteyspisteistä:

   i) joista kyseinen toimivaltainen viranomainen ja kansallinen keskitetty yhteyspiste voivat odottaa saavansa tietoa raportoitavista kyberhyökkäyksistä; ja

   ii) joille toimivaltaiset viranomaiset ja kansalliset keskitetyt yhteyspisteet saattavat joutua toimittamaan tietoja;

c) määriteltävä kyberhyökkäysten hallintamenettelyt, mukaan lukien roolit ja vastuut, tehtävät ja reaktiot, jotka perustuvat kyberhyökkäyksen havaittavissa olevaan etenemiseen kriittisten vaikutusten ja merkittävien vaikutusten vyöhykkeillä; ja

d) testattava kyberhyökkäysten hallintamenettelyjä vähintään kerran vuodessa testaamalla vähintään yhdellä skenaariolla, joka vaikuttaa suoraan tai välillisesti rajat ylittäviin sähkönsiirtoihin. Vaikutuksiltaan kriittiset ja vaikutuksiltaan merkittävät toimijat voivat suorittaa kyseisen vuotuisen testin 43 artiklassa tarkoitettujen säännöllisten harjoitusten aikana. Kyberhyökkäyksiä koskevan reagointisuunnitelman vuotuisena testinä voidaan pitää mahdollista toteutunutta reagointia 37 artiklan 8 kohdassa tarkoitetun luokitusjärjestelmän mukaisesti vähintään tasolle 2 luokiteltuun tosielämän kyberhyökkäykseen, jonka juurisyy liittyy kyberturvallisuuteen.

4. Jäsenvaltiot voivat siirtää 1 kohdassa tarkoitetut tehtävät myös alueellisille koordinointikeskuksille asetuksen (EU) 2019/943 37 artiklan 2 kohdan mukaisesti.

40 artikla

Kriisinhallinta

1. Kun toimivaltainen viranomainen toteaa, että sähkökriisi liittyy useampaan kuin yhteen jäsenvaltioon vaikuttavaan kyberhyökkäykseen, vaikutusten kohteena olevien jäsenvaltioiden toimivaltaisten viranomaisten, kyberturvallisuudesta vastaavien kansallisten toimivaltaisten viranomaisten, riskeihin varautumisesta vastaavien toimivaltaisten viranomaisten ja verkko- ja tietoturvan kyberkriisinhallintaviranomaisten on yhdessä perustettava tilapäinen rajat ylittävä kriisikoordinointiryhmä.

2. Tilapäisen rajat ylittävän kriisikoordinointiryhmän on:

a) koordinoitava kaikkien merkityksellisten kyberturvatietojen tehokasta hankintaa ja jakamista kriisinhallintaprosessiin osallistuville toimijoille;

b) järjestettävä viestintä kaikkien kriisin vaikutuspiiriin kuuluvien toimijoiden ja toimivaltaisten viranomaisten välillä päällekkäisyyksien vähentämiseksi ja analyysien ja teknisten vastatoimien tehokkuuden lisäämiseksi, jotta voidaan korjata samanaikaiset sähkökriisit, joiden juurisyy liittyy kyberturvallisuuteen;

c) tarjottava käyttöön yhteistyössä toimivaltaisten CSIRT-yksiköiden kanssa tarvittavaa asiantuntemusta, mukaan lukien operatiivinen neuvonta poikkeaman vaikutusten kohteena oleville toimijoille mahdollisten lieventävien toimenpiteiden toteuttamisesta;

d) ilmoitettava komissiolle ja sähköalan koordinointiryhmälle päivitettävät tiedot poikkeaman tilanteesta noudattaen 46 artiklassa säädettyjä suojausperiaatteita; ja

e) pyydettävä neuvoja asiaankuuluvilta viranomaisilta, virastoilta tai muilta tahoilta, joista voisi olla apua sähkökriisin lieventämisessä.

3. Jos kyberhyökkäys muodostaa tai sen odotetaan muodostavan laajamittaisen kyberturvapoikkeaman, tilapäisen rajat ylittävän kriisikoordinointiryhmän on välittömästi ilmoitettava asiasta direktiivin (EU) 2022/2555 9 artiklan 1 kohdan mukaisille kansallisille kyberkriisinhallintaviranomaisille niissä jäsenvaltioissa, joihin poikkeama vaikuttaa, sekä komissiolle ja Euroopan kyberkriisien yhteysorganisaatioiden verkostolle (EU CyCLONe). Tällaisessa tilanteessa tilapäisen rajat ylittävän kriisikoordinointiryhmän on tuettava EU CyCLONe -verkostoa toimialakohtaisten erityispiirteiden osalta.

4. Vaikutuksiltaan kriittisten ja vaikutuksiltaan merkittävien toimijoiden on luotava ja pidettävä käytettävissään valmiudet, sisäiset ohjeistot, valmiussuunnitelmat ja henkilöstö, jotta ne voivat osallistua rajat ylittävien kriisien havaitsemiseen ja lieventämiseen. Vaikutuksiltaan kriittisen tai vaikutuksiltaan merkittävän toimijan, johon samanaikainen sähkökriisi vaikuttaa, on selviteltävä tällaisen kriisin juurisyytä yhteistyössä toimivaltaisen viranomaisensa kanssa sen määrittämiseksi, missä määrin kriisi liittyy kyberhyökkäykseen.

5. Jäsenvaltiot voivat siirtää 4 kohdan mukaiset tehtävät myös alueellisille koordinointikeskuksille asetuksen (EU) 2019/943 37 artiklan 2 kohdan mukaisesti.

41 artikla

Kyberturvallisuuden kriisinhallinta- ja reagointisuunnitelmat

1. ACERin on tiiviissä yhteistyössä ENISAn, Sähkö-ENTSOn, EU DSO -elimen, kyberturvallisuudesta vastaavien kansallisten toimivaltaisten viranomaisten, toimivaltaisten viranomaisten, riskeihin varautumisesta vastaavien kansallisten toimivaltaisten viranomaisten, kansallisten sääntelyviranomaisten ja kansallisten verkko- ja tietoturvan kyberkriisinhallinta-viranomaisten kanssa laadittava 24 kuukauden kuluessa siitä, kun sille on annettu tiedoksi unionitason kyberturvariskien arviointiraportti, unionitason kyberturvallisuuden kriisinhallinta- ja reagointisuunnitelma sähköalalle.

2. Kunkin toimivaltaisen viranomaisen on 12 kuukauden kuluessa siitä, kun ACER on laatinut unionitason kyberturvallisuuden kriisinhallinta- ja reagointisuunnitelman sähköalalle 1 kohdan mukaisesti, laadittava rajat ylittäviä sähkönsiirtoja koskeva kansallinen kyberturvallisuuden kriisinhallinta- ja reagointisuunnitelma, jossa otetaan huomioon unionitason kyberturvallisuuden kriisinhallintasuunnitelma ja asetuksen (EU) 2019/941 10 artiklan mukaisesti laadittu kansallinen riskeihinvarautumissuunnitelma. Suunnitelman on oltava johdonmukainen suhteessa direktiivin (EU) 2022/2555 9 artiklan 4 kohdan nojalla laadittuun laajamittaisten kyberturvallisuuspoikkeamien ja kriisien hallintasuunnitelmaan. Toimivaltaisen viranomaisen on koordinoitava toimintaansa jäsenvaltionsa vaikutuksiltaan kriittisten ja vaikutuksiltaan merkittävien toimijoiden ja riskeihin varautumisesta vastaavien kansallisten toimivaltaisten viranomaisten kanssa.

3. Direktiivin (EU) 2022/2555 9 artiklan 4 kohdan nojalla edellytettyä kansallista laajamittaisten kyberturvallisuus-poikkeamien ja kriisien hallintasuunnitelmaa on pidettävä tämän artiklan mukaisena kansallisena kyberturvallisuuden kriisinhallintasuunnitelmana, jos se sisältää rajat ylittäviä sähkönsiirtoja koskevia kriisinhallinta- ja reagointimenettelyjä.

4. Jäsenvaltiot voivat siirtää 1 ja 2 kohdassa luetellut tehtävät myös alueellisille koordinointikeskuksille asetuksen (EU) 2019/943 37 artiklan 2 kohdan mukaisesti.

5. Vaikutuksiltaan kriittisten ja vaikutuksiltaan merkittävien toimijoiden on varmistettava, että niiden kyberturvallisuuteen liittyvät kriisinhallintaprosessit:

a) sisältävät yhteensopivat direktiivin (EU) 2022/2555 6 artiklan 8 kohdassa määritellyn mukaiset poikkeaman käsittelymenettelyt rajat ylittäviä kyberturvapoikkeamia varten ja nämä menettelyt on virallisesti kirjattu niiden kriisinhallintasuunnitelmiin; ja

b) ovat osa niiden yleistä kriisinhallintatoimintaa.

6. Vaikutuksiltaan kriittisten ja vaikutuksiltaan merkittävien toimijoiden on 12 kuukauden kuluessa siitä, kun ne on nimetty sellaisiksi 24 artiklan 6 kohdan nojalla, ja sen jälkeen joka kolmas vuosi laadittava kyberturvallisuuteen liittyvää kriisiä varten toimijatason kriisinhallintasuunnitelma, joka on sisällytettävä niiden yleisiin kriisinhallintasuunnitelmiin. Suunnitelman on katettava ainakin seuraavat:

a) kriisiksi julistamista koskevat säännöt asetuksen (EU) 2019/941 14 artiklan 2 ja 3 kohdan mukaisesti;

b) selkeät roolit ja vastuut kriisinhallintaa varten, mukaan lukien muiden asiaankuuluvien vaikutuksiltaan kriittisten ja vaikutuksiltaan merkittävien toimijoiden rooli; ja

c) ajantasaiset yhteystiedot sekä säännöt, jotka koskevat viestintää ja tietojen jakamista kriisitilanteen aikana, mukaan lukien yhteys CSIRT-yksiköihin.

7. Direktiivin (EU) 2022/2555 21 artiklan 2 kohdan c alakohdassa nojalla edellytetyt kriisinhallintatoimenpiteet on katsottava tämän artiklan mukaiseksi sähköalan toimijatason kriisinhallintasuunnitelmaksi, jos ne täyttävät kaikki 6 kohdassa luetellut vaatimukset.

8. Kriisinhallintasuunnitelmia on testattava 43, 44 ja 45 artiklassa tarkoitettujen kyberturvaharjoitusten aikana.

9. Vaikutuksiltaan kriittisten ja vaikutuksiltaan merkittävien toimijoiden on sisällytettävä toimijatason kriisinhallintasuunnitelmansa vaikutuksiltaan kriittisiä ja vaikutuksiltaan merkittäviä prosesseja koskeviin toiminnan jatkuvuussuunnitelmiinsa. Toimijatason kriisinhallintasuunnitelmien on katettava:

a) tietoteknisten palvelujen saatavuudesta, eheydestä ja luotettavuudesta riippuvaiset prosessit;

b) kaikki toiminnan jatkuvuuteen vaikuttavat paikat, mukaan lukien laitteistojen ja ohjelmistojen sijaintipaikat; ja

c) kaikki toiminnan jatkuvuuteen vaikuttaviin prosesseihin liittyvät sisäiset tehtävät ja vastuut.

10. Vaikutuksiltaan kriittisten ja vaikutuksiltaan merkittävien toimijoiden on päivitettävä toimijatason kriisinhallintasuunnitelmansa vähintään joka kolmas vuosi ja aina kun se on tarpeen.

11. ACERin on päivitettävä 1 kohdan nojalla laadittu unionitason kyberturvallisuuden kriisinhallinta- ja reagointisuunnitelma sähköalalle vähintään joka kolmas vuosi ja aina kun se on tarpeen.

12. Kunkin toimivaltaisen viranomaisen on päivitettävä 2 kohdan nojalla laadittu kansallinen kyberturvallisuuden kriisinhallinta- ja reagointisuunnitelma rajat ylittäville sähkönsiirroille vähintään joka kolmas vuosi ja aina kun se on tarpeen.

13. Vaikutuksiltaan kriittisten ja vaikutuksiltaan merkittävien toimijoiden on testattava toiminnan jatkuvuussuunnitelmiaan vähintään joka kolmas vuosi tai vaikutuksiltaan kriittisten prosessien mittavampien muutosten jälkeen. Toiminnan jatkuvuussuunnitelmaa koskevien testien tulokset on dokumentoitava. Vaikutuksiltaan kriittiset ja vaikutuksiltaan merkittävät toimijat voivat sisällyttää toiminnan jatkuvuussuunnitelmansa testauksen kyberturvaharjoituksiin.

14. Vaikutuksiltaan kriittisten ja vaikutuksiltaan merkittävien toimijoiden on päivitettävä toiminnan jatkuvuussuunnitelmansa aina kun se on tarpeen ja vähintään joka kolmas vuosi ottaen huomioon testin tulokset.

15. Jos testissä havaitaan puutteita toiminnan jatkuvuussuunnitelmassa, vaikutuksiltaan kriittisen ja vaikutuksiltaan merkittävän toimijan on korjattava puutteet 180 kalenteripäivän kuluessa testistä ja suoritettava uusi testi, jolla osoitetaan, että korjaustoimet ovat poistaneet puutteet.

16. Jos vaikutuksiltaan kriittinen tai vaikutuksiltaan merkittävä toimija ei pysty korjaamaan puutteita 180 kalenteripäivän kuluessa, sen on perusteltava tämä toimivaltaiselle viranomaiselleen 27 artiklan mukaisesti toimitettavassa raportissa.

42 artikla

Kyberturvallisuuden ennakkovaroitusvalmiudet sähköalalla

1. Toimivaltaisten viranomaisten on yhteistyössä ENISAn kanssa määriteltävä sähköalalle ennakkovaroitusvalmiudet osana asetuksen (EU) 2019/881 6 artiklan 2 ja 7 kohdan nojalla jäsenvaltioille annettavaa apua.

2. Näiden valmiuksien myötä ENISAn on kyettävä asetuksen (EU) 2019/881 7 artiklan 7 kohdassa lueteltuja tehtäviä suorittaessaan:

a) keräämään vapaaehtoisuuteen perustuen jaettavaa tietoa:

   i) CSIRT-yksiköiltä ja toimivaltaisilta viranomaisilta;

   ii) tämän asetuksen 2 artiklassa luetelluilta toimijoilta; ja

   iii) miltä tahansa muulta toimijalta, joka vapaaehtoisesti haluaa jakaa asian kannalta merkityksellistä tietoa;

b) arvioimaan ja luokittelemaan kerätyt tiedot;

c) arvioimaan tietoja, joita ENISAlla on käytettävissään rajat ylittäviin sähkönsiirtoihin liittyviä näkökohtia koskevien kyberriskien edellytysten ja asiaankuuluvien indikaattorien määrittämiseksi;

d) tunnistamaan olosuhteita ja indikaattoreita, jotka usein korreloivat sähköalan kyberhyökkäysten kanssa;

e) määrittelemään riskitekijöiden arviointien ja tunnistamisen kautta, tarvitaanko lisäanalyyseja ja ennaltaehkäiseviä toimia;

f) tiedottamaan toimivaltaisille viranomaisille tunnistetuista riskeistä ja suositelluista ennaltaehkäisevistä toimista asianomaisten toimijoiden suhteen;

g) tiedottamaan kaikille asianomaisille 2 artiklassa luetelluille toimijoille tämän kohdan b, c ja d alakohdan mukaisten arviointien tuloksista;

h) sisällyttämään säännöllisesti asianmukaiset tiedot asetuksen (EU) 2019/881 7 artiklan 6 kohdan mukaisesti laadittavaan tilanneraporttiin; ja

i) johtamaan mahdollisuuksien mukaan kerätyistä tiedoista viitteitä potentiaalisesta tietoturvaloukkauksesta tai kyberhyökkäyksestä.

3. CSIRT-yksiköiden on jaettava ENISAlta saadut tiedot viipymättä asianomaisille toimijoille direktiivin (EU) 2022/2555 11 artiklan 3 kohdan b alakohdassa määriteltyjen tehtäviensä puitteissa.

4. ACERin on seurattava ennakkovaroitusvalmiuksien toimivuutta. ENISAn on asetuksen (EU) 2019/881 6 artiklan 2 kohdan ja 7 artiklan 1 kohdan nojalla avustettava ACERia toimittamalla kaikki tarvittavat tiedot. Tämän seurannan tuloksena syntyvä analyysi on osa tämän asetuksen 12 artiklan nojalla harjoitettavaa seurantaa.

VI LUKU

SÄHKÖALAN KYBERTURVAHARJOITUSTEN PUITTEET

43 artikla

Kyberturvaharjoitukset toimija- ja jäsenvaltiotasolla

1. Kunkin vaikutuksiltaan kriittisen toimijan on nimeämistään seuraavan vuoden 31 päivään joulukuuta mennessä ja sen jälkeen joka kolmas vuosi toteutettava kyberturvaharjoitus, joka kattaa vähintään yhden sellaisen kyberhyökkäysskenaarion, joka vaikuttaa suoraan tai välillisesti rajat ylittäviin sähkönsiirtoihin ja liittyy 20 artiklan ja 27 artiklan mukaisissa jäsenvaltiotason ja toimijatason riskinarvioinneissa yksilöityihin riskeihin.

2. Poiketen 1 kohdasta, riskeihin varautumisesta vastaava kansallinen toimivaltainen viranomainen voi toimivaltaista viranomaista ja direktiivin (EU) 2022/2555 9 artiklan mukaisesti nimettyä tai perustettua asianomaista kyberkriisinhallintaviranomaista kuultuaan päättää järjestää 1 kohdassa kuvatun kyberturvaharjoituksen jäsenvaltiotasolla toimijatason sijaan. Tällöin toimivaltaisen viranomaisen on ilmoitettava asiasta:

a) kaikille jäsenvaltionsa vaikutuksiltaan kriittisille toimijoille, kansalliselle sääntelyviranomaiselle, CSIRT-yksiköille ja kyberturvallisuudesta vastaaville kansallisille toimivaltaisille viranomaisille viimeistään toimijatason kyberturvaharjoitusta edeltävän vuoden 30 päivään kesäkuuta mennessä; ja

b) kullekin toimijalle, jonka on osallistuttava jäsenvaltiotason kyberturvaharjoitukseen, viimeistään kuusi kuukautta ennen harjoitusta.

3. Riskeihin varautumisesta vastaavan kansallisen toimivaltaisen viranomaisen on CSIRT-yksiköidensä teknisellä tuella järjestettävä 2 kohdassa kuvattu jäsenvaltiotason kyberturvaharjoitus erillisenä tai kyseisessä jäsenvaltiossa toteutettavan toisen kyberturvaharjoituksen yhteydessä. Voidakseen koota näitä harjoituksia yhteen riskeihin varautumisesta vastaava kansallinen toimivaltainen viranomainen voi lykätä 1 kohdassa tarkoitettua jäsenvaltiotason kyberturvaharjoitusta yhdellä vuodella.

4. Toimija- ja jäsenvaltiotason kyberturvaharjoitusten on oltava johdonmukaisia suhteessa direktiivin (EU) 2022/2555 9 artiklan 4 kohdan d alakohdan mukaisiin kansallisiin varautumiskeinoihin.

5. Sähkö-ENTSOn on 31 päivään joulukuuta 2026 mennessä ja sen jälkeen joka kolmas vuosi yhteistyössä EU DSO -elimen kanssa asetettava käyttöön harjoitusskenaariomalli 1 kohdassa tarkoitettuja toimija- ja jäsenvaltiotason kyberturvaharjoituksia varten. Mallissa on otettava huomioon viimeisimpien toimija- ja jäsenvaltiotason kyberturvariskien arviointien tulokset ja sen on sisällettävä keskeiset onnistumiskriteerit. Sähkö-ENTSOn ja EU DSO -elimen on otettava ACER ja ENISA mukaan mallin laatimiseen.

44 artikla

Aluetason tai alueidenväliset kyberturvaharjoitukset

1. Sähkö-ENTSOn on yhteistyössä EU DSO -elimen kanssa järjestettävä 31 päivään joulukuuta 2029 mennessä ja sen jälkeen joka kolmas vuosi kullakin käyttöalueella aluetason kyberturvaharjoitus. Käyttöalueen vaikutuksiltaan kriittisten toimijoiden on osallistuttava aluetason kyberturvaharjoitukseen. Sähkö-ENTSO voi yhteistyössä EU DSO -elimen kanssa järjestää aluetason kyberturvaharjoituksen sijaan samassa aikataulussa alueidenvälisen kyberturvaharjoituksen, joka kattaa useampia käyttöalueita. Harjoituksessa olisi otettava huomioon muut olemassa olevat unionin tasolla laaditut kyberturvariskien arvioinnit ja skenaariot.

2. ENISAn on tuettava Sähkö-ENTSOa ja EU DSO -elintä aluetason tai alueidenvälisen kyberturvaharjoituksen valmistelussa ja järjestämisessä.

3. Sähkö-ENTSOn on koordinoidusti EU DSO -elimen kanssa tiedotettava asiasta vaikutuksiltaan kriittisille toimijoille, joiden on osallistuttava aluetason tai alueidenväliseen kyberturvaharjoitukseen, kuusi kuukautta ennen harjoitusta.

4. Asetuksen (EU) 2019/881 7 artiklan 5 kohdan mukaisen säännöllisen unionitason kyberturvaharjoituksen tai minkä tahansa sähköalaan samalla maantieteellisellä alueella liittyvän pakollisen kyberturvaharjoituksen järjestäjä voi kutsua Sähkö-ENTSOn ja EU DSO -elimen mukaan harjoitukseen. Tällaisissa tapauksissa ei sovelleta 1 kohdan mukaista velvoitetta edellyttäen, että kaikki käyttöalueen vaikutuksiltaan kriittiset toimijat osallistuvat samaan harjoitukseen.

5. Jos Sähkö-ENTSO ja EU DSO -elin osallistuvat 4 kohdassa tarkoitettuun kyberturvaharjoitukseen, ne voivat lykätä 1 kohdassa tarkoitettua aluetason tai alueidenvälistä kyberturvaharjoitusta yhdellä vuodella.

6. Sähkö-ENTSOn on 31 päivään joulukuuta 2027 mennessä ja sen jälkeen joka kolmas vuosi koordinoidusti EU DSO -elimen kanssa asetettava käyttöön harjoitusmalli aluetason ja alueidenvälisiä kyberturvaharjoituksia varten. Mallissa on otettava huomioon viimeisimmän aluetason kyberturvariskien arvioinnin tulokset ja sen on sisällettävä keskeiset onnistumiskriteerit. Sähkö-ENTSOn on kuultava komissiota, ja se voi pyytää ACERilta, ENISAlta ja Yhteiseltä tutkimuskeskukselta (JRC) neuvoja aluetason ja alueidenvälisten kyberturvaharjoitusten järjestämisestä ja toteuttamisesta.

45 artikla

Toimija-, jäsenvaltio- tai aluetason tai alueidenvälisten kyberturvaharjoitusten lopputulokset

1. Kriittisten palveluntarjoajien on vaikutuksiltaan kriittisen toimijan pyynnöstä osallistuttava 43 artiklan 1 ja 2 kohdassa ja 44 artiklan 1 kohdassa tarkoitettuihin kyberturvaharjoituksiin, jos ne tuottavat kyseiselle vaikutuksiltaan kriittiselle toimijalle palveluja kyseisen kyberturvaharjoituksen kohdealaa vastaavalla alueella.

2. Edellä 43 artiklan 1 ja 2 kohdassa ja 44 artiklan 1 kohdassa tarkoitettujen kyberturvaharjoitusten järjestäjien on analysoitava ja saatettava päätökseen kulloinenkin kyberturvaharjoitus laatimalla kaikille osallistujille osoitettu yhteenveto saaduista kokemuksista; ne voivat tätä varten pyytää asetuksen (EU) 2019/881 7 artiklan 5 kohdan nojalla neuvoja ENISAlta. Yhteenvedon on katettava seuraavat tekijät:

a) harjoitusskenaariot, kokousraportit, kannat pääpiirteittäin, onnistumiset ja saadut kokemukset sähkön arvoketjun kaikilla tasoilla;

b) täyttyivätkö keskeiset onnistumiskriteerit; ja

c) kyberturvaharjoitukseen osallistuneille toimijoille annettavat suositukset kyberturvakriiseihin liittyvien prosessien, menettelyjen, ohjausmallien ja kriittisten palveluntarjoajien kanssa tehtyjen sopimusjärjestelyjen korjaamiseksi, mukauttamiseksi tai muuttamiseksi.

3. Edellä 43 artiklan 1 ja 2 kohdassa ja 44 artiklan 1 kohdassa tarkoitettujen kyberturvaharjoitusten järjestäjien on CSIRT-yksiköiden verkoston, verkko- ja tietoturva-alan yhteistyöryhmän tai Euroopan kyberkriisien yhteysorganisaatioiden verkoston (EU CyCLONe) pyynnöstä toimitettava niille kyseisen kyberturvaharjoituksen lopputulokset. Järjestäjien on toimitettava kullekin harjoituksiin osallistuneelle toimijalle tämän artiklan 2 kohdan a ja b alakohdassa tarkoitetut tiedot. Järjestäjien on toimitettava tämän artiklan 2 kohdan c alakohdassa tarkoitetut suositukset yksinomaan suosituksissa käsitellyille toimijoille.

4. Edellä 43 artiklan 1 ja 2 kohdassa ja 44 artiklan 1 kohdassa tarkoitettujen kyberturvaharjoitusten järjestäjien on luotava säännöllisesti harjoituksiin osallistuneiden toimijoiden kanssa katsaus siihen, miten tämän artiklan 2 kohdan c alakohdan nojalla annettuja suosituksia on noudatettu.

VII LUKU

TIETOJEN SUOJAAMINEN

46 artikla

Vaihdettavien tietojen suojaamista koskevat periaatteet

1. Edellä 2 artiklan 1 kohdassa lueteltujen toimijoiden on varmistettava, että tämän asetuksen nojalla toimitetut, vastaanotetut, vaihdetut tai siirretyt tiedot ovat saatavilla ainoastaan tiedonsaantitarpeen perusteella ja asiaankuuluvien unionin ja kansallisten tietoturvasääntöjen mukaisesti.

2. Edellä 2 artiklan 1 kohdassa lueteltujen toimijoiden on varmistettava, että tämän asetuksen nojalla toimitettuja, vastaanotettuja, vaihdettuja tai siirrettyjä tietoja käsitellään asianmukaisesti ja seurataan tietojen koko elinkaaren ajan ja että ne voidaan julkistaa niiden elinkaaren päätyttyä vasta anonymisoinnin jälkeen.

3. Edellä 2 artiklan 1 kohdassa lueteltujen toimijoiden on varmistettava, että käytössä on käytetyistä keinoista riippumatta kaikki tarvittavat organisatoriset ja tekniset suojatoimenpiteet tämän asetuksen nojalla toimitettujen, vastaanotettujen, vaihdettujen tai siirrettyjen tietojen luottamuksellisuuden, eheyden, saatavuuden ja kiistämättömyyden turvaamiseksi ja suojaamiseksi. Suojaustoimenpiteiden on:

a) oltava oikeasuhteisia;

b) otettava huomioon tunnettuihin aiempiin ja kehittymässä oleviin uhkiin liittyvät kyberturvariskit, joita tämän asetuksen yhteydessä esiintyviin tietoihin voi kohdistua;

c) perustuttava mahdollisimman pitkälti kansallisiin, eurooppalaisiin tai kansainvälisiin standardeihin ja parhaisiin käytäntöihin; ja

d) oltava dokumentoituja.

4. Edellä 2 artiklan 1 kohdassa lueteltujen toimijoiden on varmistettava, että kaikille henkilöille, joille myönnetään pääsy tämän asetuksen nojalla toimitettuihin, vastaanotettuihin, vaihdettuihin tai siirrettyihin tietoihin, selvitetään toimijatasolla sovellettavat turvallisuussäännöt sekä tietojen suojaamiseen liittyvät toimenpiteet ja menettelyt. Näiden toimijoiden on varmistettava, että asianomainen henkilö tunnustaa velvollisuutensa suojata tiedot hänelle selvitetyllä tavalla.

5. Edellä 2 artiklan 1 kohdassa lueteltujen toimijoiden on varmistettava, että pääsy tämän asetuksen nojalla toimitettuihin, vastaanotettuihin, vaihdettuihin tai siirrettyihin tietoihin rajoitetaan henkilöihin:

a) joilla on valtuudet tutustua kyseisiin tietoihin tehtäviensä perusteella ja ainoastaan kyseisten tehtävien suorittamisen ajan; ja

b) joiden osalta toimija on voinut arvioida eettisten ja integriteettiin liittyvien periaatteiden noudattamista ja joiden osalta taustatarkistuksessa ei ole käynyt ilmi näyttöä kielteisistä tekijöistä arvioitaessa henkilön luotettavuutta toimijan parhaiden käytäntöjen ja yleisten turvallisuusvaatimusten sekä tarvittaessa kansallisten lakien ja asetusten mukaisesti.

6. Edellä 2 artiklan 1 kohdassa lueteltujen toimijoiden on saatava tiedot alun perin luoneen tai toimittaneen luonnollisen tai oikeushenkilön kirjallinen suostumus ennen tietojen toimittamista kolmannelle osapuolelle, joka ei kuulu tämän asetuksen soveltamisalaan.

7. Edellä 2 artiklan 1 kohdassa lueteltu toimija voi todeta, että tiedot on jaettava tämän artiklan 1 ja 4 kohdan vastaisesti, jotta voidaan estää samanaikainen sähkökriisi, jonka juurisyy liittyy kyberturvallisuuteen, tai rajat ylittävä kriisi unionissa muulla toimialalla. Tällaisessa tapauksessa sen on:

a) kuultava toimivaltaista viranomaista ja saatava siltä lupa jakaa tällaisia tietoja;

b) anonymisoitava tällaiset tiedot menettämättä tietoelementtejä, jotka ovat tarpeen, jotta yleisölle voidaan tiedottaa rajat ylittäviin sähkönsiirtoihin kohdistuvasta välittömästä ja vakavasta riskistä ja mahdollisista riskiä lieventävistä toimenpiteistä; ja

c) pidettävä salassa tietojen alkuperä ja tietoja tämän asetuksen nojalla käsitelleet toimijat.

8. Tämän artiklan 6 kohdasta poiketen toimivaltaiset viranomaiset voivat luovuttaa tämän asetuksen nojalla toimitettuja, vastaanotettuja, vaihdettuja tai siirrettyjä tietoja 2 artiklan 1 kohdan luetteloon kuulumattomalle kolmannelle osapuolelle ilman tietojen alkuperän kirjallista etukäteissuostumusta, mutta ilmoittaen tästä sille mahdollisimman pian. Ennen kuin asianomainen toimivaltainen viranomainen luovuttaa tämän asetuksen mukaisesti toimitettuja, vastaanotettuja, vaihdettuja tai siirrettyjä tietoja 2 artiklan 1 kohdan luetteloon kuulumattomalle kolmannelle osapuolelle, sen on kohtuudella varmistettava, että asianomainen kolmas osapuoli on tietoinen voimassa olevista turvallisuussäännöistä, ja hankittava kohtuullinen varmuus siitä, että asianomainen kolmas osapuoli kykenee suojaamaan saamansa tiedot tämän artiklan 1–5 kohdan mukaisesti. Toimivaltaisen viranomaisen on anonymisoitava tällaiset tiedot menettämättä tietoelementtejä, jotka ovat tarpeen, jotta yleisölle voidaan tiedottaa rajat ylittäviin sähkönsiirtoihin kohdistuvasta välittömästä ja vakavasta riskistä ja mahdollisista riskiä lieventävistä toimenpiteistä, sekä pidettävä tietojen alkuperä salassa. Tällaisessa tapauksessa 2 artiklan 1 kohdan luetteloon kuulumattoman kolmannen osapuolen on suojattava vastaanotetut tiedot toimijatasolla jo voimassa olevien sääntöjen mukaisesti tai, jos tämä ei ole mahdollista, asianomaisen toimivaltaisen viranomaisen sääntöjen ja ohjeiden mukaisesti.

9. Tätä artiklaa ei sovelleta 2 artiklan 1 kohdan luetteloon kuulumattomiin toimijoihin, joille luovutetaan tietoja tämän artiklan 6 kohdan nojalla. Tällöin on sovellettava tämän artiklan 7 kohtaa tai toimivaltainen viranomainen voi antaa kyseiselle toimijalle kirjallisia määräyksiä, joita niiden on noudatettava vastaanottaessaan tietoja tämän asetuksen nojalla.

47 artikla

Tietojen luottamuksellisuus

1. Kaikkia tämän asetuksen nojalla toimitettuja, vastaanotettuja, vaihdettuja tai siirrettyjä tietoja koskevat tämän asetuksen tämän artiklan 2–5 kohdassa säädetty salassapitovelvollisuus ja asetuksen (EU) 2019/943 65 artiklassa säädetyt vaatimukset. Kaikki tämän asetuksen 2 artiklassa lueteltujen toimijoiden kesken tämän asetuksen täytäntöönpanoa varten toimitetut, vastaanotetut, vaihdetut tai siirretyt tiedot on suojattava ottaen huomioon tietojen alkuperän tietoihin soveltama luottamuksellisuustaso.

2. Salassapitovelvollisuus koskee 2 artiklassa lueteltuja toimijoita.

3. Kyberturvallisuudesta vastaavien kansallisten toimivaltaisten viranomaisten, kansallisten sääntelyviranomaisten, riskeihin varautumisesta vastaavien kansallisten toimivaltaisten viranomaisten ja CSIRT-yksiköiden on vaihdettava keskenään kaikki tehtäviensä edellyttämät tiedot.

4. Kaikki 2 artiklan 1 kohdassa lueteltujen toimijoiden kesken 23 artiklan täytäntöönpanoa varten toimitetut, vastaanotetut, vaihdetut tai siirretyt tiedot on anonymisoitava ja koottava yhteen koontitiedoksi.

5. Tämän asetuksen soveltamisalaan kuuluvien toimijoiden tai viranomaisten tehtäviensä yhteydessä saamaa tietoa ei saa paljastaa muulle toimijalle tai viranomaiselle, sanotun kuitenkaan rajoittamatta kansallisen oikeuden, tämän asetuksen muiden säännösten tai muun asiaan liittyvän unionin lainsäädännön soveltamista niiden soveltamisalaan kuuluviin tapauksiin.

6. Tämän asetuksen nojalla tietoja saava viranomainen, toimija tai luonnollinen henkilö ei saa käyttää niitä mihinkään muuhun tarkoitukseen kuin tämän asetuksen mukaisten tehtäviensä hoitamiseen, sanotun kuitenkaan rajoittamatta kansallisen tai unionin lainsäädännön soveltamista.

7. ACERin on ENISAa, kaikkia toimivaltaisia viranomaisia, Sähkö-ENTSOa ja EU DSO -elintä kuultuaan annettava 13 päivään kesäkuuta 2025 mennessä kaikkia 2 artiklan 1 kohdassa lueteltuja toimijoita koskevat ohjeet, joissa käsitellään tiedonvaihtomekanismeja ja erityisesti oletettuja tiedonkulkuja, sekä menetelmiä tietojen anonymisoimiseksi ja koostamiseksi koontitiedoksi tämän artiklan täytäntöönpanoa varten.

8. Unionin sääntöjen ja kansallisten sääntöjen nojalla luottamuksellisia tietoja voidaan vaihtaa komission ja muiden asiaankuuluvien viranomaisten kanssa ainoastaan, jos tällainen vaihto on tarpeen tämän asetuksen soveltamiseksi. Vaihdettava tieto on rajattava siihen, mikä on tarpeen ja oikeasuhteista kyseisen tiedonvaihdon tarkoituksia varten. Tiedonvaihdossa on säilytettävä kyseisten tietojen luottamuksellisuus sekä suojeltava vaikutuksiltaan kriittisten tai vaikutuksiltaan merkittävien toimijoiden turvallisuusetuja ja kaupallisia etuja.

VIII LUKU

LOPPUSÄÄNNÖKSET

48 artikla

Tilapäiset säännökset

1. Siihen saakka kunnes 6 artiklan 2 kohdassa tarkoitetut ehdot tai menetelmät tai 6 artiklan 3 kohdassa tarkoitetut suunnitelmat on hyväksytty, Sähkö-ENTSOn on yhteistyössä EU DSO -elimen kanssa annettava ei-sitovaa ohjeistusta seuraavista tekijöistä:

a) tämän artiklan 2 kohdan mukainen alustava sähköalan kyberturvavaikutusindeksi (ECII);

b) tämän artiklan 4 kohdan mukainen alustava luettelo unionitason vaikutuksiltaan merkittävistä ja unionitason vaikutuksiltaan kriittisistä prosesseista; ja

c) tämän artiklan 6 kohdan mukainen alustava luettelo eurooppalaisista ja kansainvälisistä standardeista ja varotoimista, joita edellytetään kansallisessa lainsäädännössä ja joilla on merkitystä rajat ylittävien sähkönsiirtojen kyberturvanäkökohtien kannalta.

2. Sähkö-ENTSOn on yhteistyössä EU DSO -elimen kanssa 13 päivään lokakuuta 2024 mennessä laadittava suositus alustavaksi ECII-indeksiksi. Sähkö-ENTSOn on yhteistyössä EU DSO -elimen kanssa annettava suositeltu alustava ECII tiedoksi toimivaltaisille viranomaisille.

3. Toimivaltaisten viranomaisten on neljän kuukauden kuluessa suositellun alustavan ECII-indeksin vastaanottamisesta tai viimeistään 13 päivään Helmikuu 2025 mennessä yksilöitävä ehdokkaat vaikutuksiltaan merkittäviksi ja vaikutuksiltaan kriittisiksi toimijoiksi jäsenvaltiossaan suositellun ECII-indeksin perusteella ja laadittava alustava luettelo vaikutuksiltaan merkittävistä ja vaikutuksiltaan kriittisistä toimijoista. Alustavassa luettelossa yksilöidyt vaikutuksiltaan merkittävät ja vaikutuksiltaan kriittiset toimijat voivat varautumisperiaatteen mukaisesti vapaaehtoisesti täyttää tässä asetuksessa säädetyt velvoitteensa. Toimivaltaisten viranomaisten on 13 päivään maaliskuuta 2025 mennessä ilmoitettava alustavassa luettelossa yksilöidyille toimijoille, että ne on määritelty vaikutuksiltaan merkittäviksi tai vaikutuksiltaan kriittisiksi toimijoiksi.

4. Sähkö-ENTSOn on yhteistyössä EU DSO -elimen kanssa 13 päivään joulukuuta 2024 mennessä laadittava alustava luettelo unionitason vaikutuksiltaan merkittävistä ja unionitason vaikutuksiltaan kriittisistä prosesseista. Edellä olevan 3 kohdan mukaisen ilmoituksen saaneiden toimijoiden, jotka varautumisperiaatteen mukaisesti vapaaehtoisesti päättävät täyttää tässä asetuksessa säädetyt velvoitteensa, on käytettävä alustavaa luetteloa vaikutuksiltaan merkittävistä ja vaikutuksiltaan kriittisistä prosesseista määrittääkseen väliaikaiset merkittävien ja kriittisten vaikutusten vyöhykkeet ja määrittääkseen, mitkä omaisuuserät on sisällytettävä ensimmäiseen toimijatason kyberturvariskien arviointiin.

5. Kunkin 4 artiklan 1 kohdan mukaisen toimivaltaisen viranomaisen on 13 päivään syyskuuta 2024 mennessä toimitettava Sähkö-ENTSOlle ja EU DSO -elimelle luettelo rajat ylittävien sähkönsiirtojen kyberturvanäkökohtien kannalta merkityksellisestä kansallisesta lainsäädännöstään.

6. Sähkö-ENTSOn on yhteistyössä EU DSO -elimen kanssa 13 päivään kesäkuuta 2025 mennessä laadittava alustava luettelo eurooppalaisista ja kansainvälisistä standardeista ja varotoimista, joita edellytetään kansallisessa lainsäädännössä ja joilla on merkitystä rajat ylittävien sähkönsiirtojen kyberturvanäkökohtien kannalta, ottaen huomioon toimivaltaisten viranomaisten toimittamat tiedot.

7. Eurooppalaisten ja kansainvälisten standardien ja varotoimien alustavan luettelon on sisällettävä:

a) eurooppalaiset ja kansainväliset standardit ja kansallinen lainsäädäntö, joissa annetaan ohjeita kyberturvariskien hallintamenetelmistä toimijatasolla; ja

b) kyberturvavarotoimet, jotka vastaavat varotoimia, joiden oletetaan olevan osa vähimmäistason ja tiukempia kyberturvavarotoimia.

8. Sähkö-ENTSOn ja EU DSO -elimen on otettava huomioon ENISAn ja ACERin näkemykset laatiessaan alustavaa standardiluetteloa. Sähkö-ENTSOn ja EU DSO -elimen on julkaistava eurooppalaisten ja kansainvälisten standardien ja varotoimien siirtymävaiheen luettelo verkkosivustoillaan.

9. Sähkö-ENTSOn ja EU DSO -elimen on kuultava ENISAa ja ACERia 1 kohdan nojalla laatimistaan ei-sitovaa ohjeistusta koskevista ehdotuksistaan.

10. Siihen saakka, kunnes vähimmäistason ja tiukemmat kyberturvavarotoimet on 29 artiklan nojalla laadittu ja 8 artiklan nojalla hyväksytty, kaikkien 2 artiklan 1 kohdassa lueteltujen toimijoiden on pyrittävä asteittain soveltamaan 1 kohdan nojalla laadittua ei-sitovaa ohjeistusta.

49 artikla

Voimaantulo

Tämä asetus tulee voimaan kahdentenakymmenentenä päivänä sen jälkeen, kun se on julkaistu *Euroopan unionin virallisessa lehdessä*.

Tämä asetus on kaikilta osiltaan velvoittava, ja sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa.

Tehty Brysselissä 11 päivänä maaliskuuta 2024.

Komission puolesta
Puheenjohtaja
Ursula VON DER LEYEN