energiavirasto
energimyndigheten

Ohje Energiaviraston valvomille toimijoille kyberturvallisuuslain noudattamiseksi

1721/040002/2025

Kyberturvallisuuslaki energia-alalla

OHJE ENERGIAVIRASTON VALVOMILLE TOIMIJOILLE KYBERTURVALLISUUSLAIN NOUDATTAMISEKSI

1721/040002/2025

Energiavirasto
Energimyndigheten
Lintulahdenkuja 2 A
FI-00530 Helsinki
Puhelin 029 505 0000
S-posti kirjaamo@energiavirasto.fi
Internet www.energiavirasto.fi

Sisällysluettelo

Versiohistoria

Versio	Pvm	Keskeisimmät muutokset
1	8.4.2025	Ensimmäinen versio
2	11.4.2025	Latauspisteiden operaattoreita koskevasta kohdasta on poistettu maininta sähköautoista.
3	1.10.2025	Lisätty maininta pienimuotoisesta sähköntuotannosta ja Energiaviraston tulkinta, että vain pienimuotoinen sähköntuotanto voi olla vähäistä.

1 Tausta

1.1 Yleistä kyberturvallisuuslaista ja NIS2-direktiivistä

Kyberturvallisuuslailla (124/2025) säädetään kyberturvallisuutta koskevasta riskienhallinnasta ja poikkeamista ilmoittamisesta. Kyberturvallisuuslaki on kansallinen laki, jolla on pantu täytäntöön kyberturvallisuusdirektiivi eli NIS2-direktiivi (EU) 2022/2555[1].

NIS2-direktiivin tavoitteena on varmistaa yhtenäinen kyberturvallisuuden korkea taso koko Euroopan unionin alueella. NIS2-direktiivi on korvannut aiemman verkko- ja tietoturvadirektiivin (NIS1-direktiivi), jonka soveltamisalaan on Suomessa kuulunut energia-alalta sähköverkonhaltijoita ja maakaasun siirtoverkonhaltija. NIS2-direktiivin myötä kyberturvallisuusvelvoitteet koskevat entistä laajempaa joukkoa ja ne ovat aiempaa yksityiskohtaisempia. NIS1-direktiivin myötä tehdyt muutokset sähkömarkkinalakiin (588/2013) ja maakaasumarkkinalakiin (587/2017) on kumottu. Sähkö- ja maakaasuverkonhaltijoihin sovelletaan kyberturvallisuuslain velvoitteita samoin kuin muihinkin sen piiriin kuuluviin yrityksiin.

Kyberturvallisuuslaki on kaikkia toimialoja koskeva yhteinen yleislaki. Energia-alalla lainsäädännön piiriin kuuluu sähkön, kaukolämmityksen ja -jäähdytyksen, kaasun, öljyn sekä vedyn toimijoita.

Huomioitavaa: Energia-alan valvovia viranomaisia ovat Energiavirasto ja Turvallisuus- ja kemikaalivirasto (Tukes). Tämä ohje koskee ainoastaan Energiaviraston valvomia energia-alan toimijoita. Tukesin valvomien toimijoiden on tutustuttava Tukesin kyberturvallisuuslakia koskevaan ohjeistukseen.

1.2 Ohjeen tavoitteet ja luonne

Tähän ohjeeseen on koottu Energiaviraston valvomille energia-alan toimijoille tietoa kyberturvallisuuslain noudattamisesta. Muiden toimijoiden on syytä kääntyä kyseistä toimijatyyppiä valvovan NIS2-viranomaisen puoleen. Tässä ohjeessa ei ole esimerkiksi otettu huomioon muita toimialoja koskevia mahdollisia poikkeuksia.

Energiavirasto päivittää tätä ohjetta tarpeen mukaan. Ajantasaisin versio julkaistaan Energiaviraston verkkosivuilla (www.energiavirasto.fi/kyberturvallisuus) ja VERTTI-valvontatietojärjestelmän ohjeissa.

Toimijoiden on tunnistettava itse, kuuluvatko nämä kyberturvallisuuslain piiriin. Lain piiriin kuuluvien toimijoiden on oma-aloitteisesti ilmoittauduttava sitä valvovalle viranomaiselle toimijaluetteloon, jonne toimija ilmoittaa perustietoja yrityksen toiminnasta ja yhteystiedoista. Ensimmäinen ilmoitus on tehtävä 8.5.2025 mennessä. Energiaviraston valvomat toimijat ilmoittavat tiedot VERTTI-valvontatietojärjestelmään, johon kirjaudutaan Suomi.fi-valtuuden avulla. Ennen

[1] Toimenpiteistä kyberturvallisuuden yhteisen korkean tasonvarmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 (NIS2-direktiivi).

ilmoittautumista toimijoiden on perehdyttävä tarkkaan tähän ohjeeseen ja VERTTI-valvontatietojärjestelmän täyttöohjeeseen (luku 6).

Tällä ohjeella Energiaviraston valvomat toimijat saavat kyberturvallisuuslain soveltamisalan lisäksi yleiskäsityksen kyberturvallisuuslain mukaisista velvoitteista mukaan lukien riskienhallinnasta, poikkeamailmoittamisesta (NIS-ilmoitus) sekä Energiaviraston toimijoihin kohdistamasta valvonnasta.

Energiavirasto antaa tämän ohjeen suositusluonteisena ohjeena. Ohje kuitenkin viittaa oikeudellisesti sitoviin velvoitteisiin, joista säädetään kyberturvallisuuslaissa. Lisäksi oikeudellisista velvoitteista säädetään muissa laeissa kuten mahdollisissa komission täytäntöönpanosäädöksissä ja mahdollisissa erillisissä viranomaisen määräyksissä. Tämä ohje ei ole tyhjentävä esitys kyberturvallisuuslaista tai NIS2-direktiivistä, mutta se tukee toimijoita kyberturvallisuuslain ja NIS2-direktiivin mukaisten velvoitteiden noudattamisessa.

2 Asiaan liittyvä lainsäädäntö

2.1 Kyberturvallisuuslaki

Kyberturvallisuuslaki on julkaistu Finlex-lakiverkkopalvelussa: https://finlex.fi/fi/lainsaadanto/saadoskokoelma/2025/124

3 Soveltamisala

3.1 Yleistä soveltamisalasta ja viranomaisten toimivallanjaosta

Kyberturvallisuuslakia sovelletaan oikeushenkilöön ja luonnolliseen henkilöön, joka harjoittaa lain liitteessä I tai II tarkoitettua toimintaa tai on mainituissa liitteissä tarkoitettu toimija. Lisäksi jotta edellä mainittu taho kuuluu kyberturvallisuuslain piiriin, sen tulee olla kooltaan riittävän suuri tai sen toiminta katsotaan koostaan riippumatta muuten kriittiseksi. Kyberturvallisuuslain piiriin kuuluvia yrityksiä kutsutaan toimijoiksi.

Kyberturvallisuuslain 3 §:ssä säädetään toimijan määritelmästä eli siitä, mitkä tahot olisivat lain soveltamisalaan kuuluvia toimijoita. Pykälän 1 momentissa säädetään toimijan yleisestä määritelmästä, joka on kaksiosainen liittyen toimijan toiminnan laatuun tai tyyppiin ja toimijan kokoon. Pykälän 2 ja 3 momentissa säädetään erikoistapauksista, joissa toimija kuuluu lain soveltamisalaan sen koosta riippumatta. Eräiden toimijoiden osalta rajauksista lain soveltamisalaan säädetään lain 4 §:ssä. Kansainvälisten toimijoiden osalta lainkäyttövallasta ja alueellisuudesta säädetään 6 §:ssä.[2]

Tässä luvussa käsitellään, mitä yrityksen tulee ottaa huomioon selvittäessään, kuuluuko yritys kyberturvallisuuslain soveltamisalaan ja mille valvovalle viranomaiselle yrityksen tulee ilmoittautua toimijaluetteloon. Luvussa 3.2 käsitellään, minkälainen yrityksen harjoittama toiminta kuuluu lain soveltamisalaan. Luvuissa 3.3 ja 3.4 eritellään, milloin lain liitteessä mainittua toimintaa harjoittava yritys kuuluu lain

[2] Kts. HE 57/2024 vp. Hallituksen esitys eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi, s. 145.

soveltamisalaan. Luvussa 3.5 käsitellään CER-direktiivin[3] nojalla kriittiseksi määrättyjä toimijoita ja näiden kuulumista kyberturvallisuuslain piiriin.

Soveltamisalaan kuuluvat toimijat jaetaan tärkeisiin ja keskeisiin toimijoihin. Tärkeitä toimijoita ovat keskisuuret yritykset. Keskeisiä toimijoita ovat keskisuuren yrityksen määritelmän ylittävät toimijat eli suuret yritykset, CER-direktiivin mukaiset kriittiset toimijat ja muut koostaan riippumatta keskeisiksi toimijoiksi määritellyt toimijat. Toimijajaottelusta tärkeisiin ja keskeisiin toimijoihin voi lukea lisää luvusta 3.6.

Energia-alalla lain piiriin kuuluu sähkön, kaukolämmityksen ja -jäähdytyksen, kaasun, öljyn sekä vedyn toimijoita. Energia-alan valvovia viranomaisia ovat Energiavirasto ja Turvallisuus- ja kemikaalivirasto (Tukes). Valvova viranomainen riippuu toimijan harjoittamasta toiminnasta. Luvussa 3.2 eritellään tarkemmin, kuka on valvova viranomainen kunkin lain piiriin kuuluvan toiminnan osalta ja mille viranomaiselle toimijan tulee tällöin ilmoittautua toimijaluetteloon.

Monialayritys voi kuulua useamman viranomaisen valvomaksi toimijaksi, jos yritys harjoittaa useampaa lain liitteen mukaista toimintaa ja toimintoja valvovat eri viranomaiset. Näin on esimerkiksi, jos yritys on sähkön tuottaja (valvova viranomainen Energiavirasto), kaukolämmön jakelija (valvova viranomainen Energiavirasto) ja öljynsiirtoputkistojen haltijat (valvova viranomainen Turvallisuus- ja kemikaalivirasto). Vastaavasti yritys voi harjoittaa myös useampaa lain piiriin kuuluvaa toimintaa, mutta kaikkia näitä toimintoja valvoo sama viranomainen. Esimerkiksi yritys, joka harjoittaa vain kaukolämmön jakelua ja sähkön tuotantoa, kuuluu ainoastaan Energiaviraston valvomaksi toimijaksi.

Kyberturvallisuuslain mukaisen toimijan on ilmoittauduttava erikseen kaikille sitä valvoville viranomaisille toimijaluetteloon (kyberturvallisuuslaki 41 §, kts. luku 4.1 ja 6).

3.2 Soveltamisalaan kuuluva energia-alan toiminta tai toimija

Kyberturvallisuuslain 3 §:n mukaan lakia sovelletaan oikeushenkilöön ja luonnolliseen henkilöön (toimija), joka harjoittaa lain liitteessä I tai II tarkoitettua toimintaa tai on mainituissa liitteissä tarkoitettu toimija. Energia-alalla lain piiriin kuuluu sähkön, kaukolämmityksen ja -jäähdytyksen, kaasun, öljyn sekä vedyn toimijoita.

Kyberturvallisuuslaki on useita toimialoja käsittävä yleislaki. Tässä ohjeessa käsitellään ainoastaan energia-alan mukaista toimintaa harjoittavia ja erityisesti Energiaviraston valvomia toimijoita. Muuta toimintaa harjoittavien yritysten on tarkistettava soveltamisala kyberturvallisuuslaista ja kyseistä toimintaa valvovalta viranomaiselta.

Toimijan määritelmän kannalta ei ole merkitystä toimijan oikeudellisella muodolla, vaan ainoastaan sillä, että toimija harjoittaa pykälässä tarkoitettua toimintaa tai on siinä tarkoitettua toimijatyyppiä sekä täyttää lain 3 §:n 1 momentissa säädetyn

[3] Kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta annetun Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2557 (CER-direktiivi).

kokoedellytyksen tai sitä koskee saman pykälän 2 tai 3 momentissa säädetty poikkeus soveltamisesta toimijan koosta riippumatta.[4]

Toiminnan harjoittamisella viitataan lähtökohtaisesti siihen tahoon, kenen nimissä liitteessä mainittua toimintaa tosiasiassa harjoitetaan.[5] Jos toimija on esimerkiksi sopimuksin järjestänyt huollon, käyttövalvonnan tai muun operatiivisen toiminnan jollekin muulle taholle, tällaista tahoa pidetään palveluntuottajana suhteessa toimijaan, jonka nimissä toimintaa harjoitetaan. Esimerkiksi sähkön tuotantoa harjoittaa se taho, kenen nimissä sähköä tuotetaan (myydään eteenpäin). Jäljempänä tämän ohjeen luvussa 3.3.2 käsitellään, miten lain soveltamisala määräytyy esimerkiksi osakkeenomistajien ja konsernimuotoisten yritysten osalta. Energiavirasto korostaa, että toimijan on huolehdittava palveluntuottajiin kohdistuvien riskien hallinnasta (kts. kyberturvallisuuslaki 9 §:n 2 mom. 4 kohta ja tämän ohjeen luku 4.2–4.3).

Suomen kyberturvallisuuslakia sovelletaan pääsääntöisesti toimijaan, joka on sijoittautunut Suomeen (kyberturvallisuuslain 6.1 §).[6] Suomen lain soveltamisalaan kuuluu Suomeen sijoittautunut toimija kokonaisuudessaan, eli myös kyseisen toimijan sellaiset toiminnot, jotka sijaitsevat esimerkiksi toisessa jäsenvaltiossa tai kolmansissa maissa. Mikäli Suomessa NIS2-direktiivin soveltamisalaan kuuluvaa toimintaa harjoittaa tai palveluja tarjoaa toimija, joka on sijoittautunut toiseen EU-jäsenvaltioon, kuuluu toimija pääsääntöisesti ja vastaavasti sijoittautumisvaltionsa lainsäädännön ja -valvonnan alaan.[7]

Energia-alalla kyberturvallisuuslain piiriin kuuluu sähkön, kaukolämmityksen ja -jäähdytyksen, kaasun, öljyn sekä vedyn toimijoita. Energia-alan valvovia viranomaisia ovat Energiavirasto ja Turvallisuus- ja kemikaalivirasto (Tukes). Energiaviraston valvoo seuraavia toimijoita:

- sähkön ja maakaasun verkonhaltijat
- kaukolämmityksen ja kaukojäähdytyksen jakelijat
- vedyn siirtoa harjoittavat toimijat
- sähkön ja maakaasun toimittajat eli myyjät mukaan lukien jälleenmyyjät
- sähkön tuottajat
- latauspisteiden operaattorit
- nimitetyt sähkömarkkinaoperaattorit

[4] HE 57/2024 vp., s. 146.

[5] Huomioitavaa: Kyberturvallisuuslain piiriin kuuluvat latauspisteiden operaattorit, jotka vastaavat latauspalvelua loppukäyttäjille tarjoavan latauspisteen hallinnoinnista ja toiminnasta, myös silloin, kun tämä tapahtuu liikennepalvelun tarjoajan nimissä ja puolesta.

[6] Kyberturvallisuuslain 6 §:n 1 momentin mukaan lakia sovelletaan toimijaan, joka on sijoittautunut Suomeen, jollei laissa toisin säädetä tai Euroopan unionin lainsäädännöstä tai Suomea sitovasta kansainvälisestä velvoitteesta muuta johdu. Kyseisen säännöksen 2-3 momentissa on eritelty tiettyjä toimijoita, joihin sovelletaan 1 momentista poikkeavia periaatteita. Poikkeusten piirissä ei ole toimintaa tai toimijatyyppejä energiatoimialalta.

[7] HE 57/2024 vp., s. 158.

- muut sähkömarkkinoiden osapuolet, jotka tarjoavat aggregointia, kulutusjoustoa tai energian varastointia

Alla olevassa taulukossa on esitetty kyberturvallisuuslain liitteen mukainen toiminta ja toimijat sekä näitä valvova viranomainen. Taulukko käsittää ainoastaan energia-alan toimijat eli yritysten, jotka harjoittavat myös muuta toimintaa, tulee tarkistaa lain piiriin kuuluminen kyberturvallisuuslaista.

Lain piiriin kuuluva energia-alan toiminta tai toimija	**Huomiot toimijasta**	**Valvova viranomainen**
Sähkö		
Sähkömarkkinalain (588/2013) 3 §:n 1 momentin 21 kohdassa tarkoitetut sähköalan yritykset, jotka harjoittavat momentin 11 kohdassa tarkoitettua sähköntoimitusta	Sähköntoimituksella tarkoitetaan sähkön myyntiä asiakkaille tai jälleenmyyntiin. Asiakkaalla tarkoitetaan niin sähkön tukkuasiakasta kuin loppukäyttäjää. Sähköntoimitusta harjoittavia sähköalan yrityksiä ovat sähkön myyjät ja jälleenmyyjät. Vähittäismyynti on lain piiriin kuuluvaa toimintaa.[8] Kyberturvallisuuslain soveltamisalaan eivät kuulu esimerkiksi asetuksen (EU) 2019/943 2 artiklan 14 alakohdassa määritellyt tasevastaavat tässä roolissaan. Kuitenkin, jos tasevastaavana toimiva yritys harjoittaa lain liitteessä mainittua muuta toimintaa (esimerkiksi sähköntoimitusta), kuuluu se lain soveltamisalaan.	Energiavirasto
Sähkömarkkinalain 3 §:n 1 momentin 10 kohdassa	Jakeluverkonhaltijat mukaan lukien suljetun	Energiavirasto

[8] Energiaviraston lausunnon (3603/040003/2024) mukaan sähköajoneuvojen latauspalvelun tarjoaminen ei ole sähkön vähittäismyyntiä eikä sähkön toimitusta. Kyberturvallisuuslain soveltamisalaan kuuluvat kuitenkin erikseen latauspisteiden operaattorit, jotka vastaavat latauspalvelua loppukäyttäjille tarjoavan latauspisteen hallinnoinnista ja toiminnasta, myös liikennepalvelun tarjoajan nimissä ja puolesta.

tarkoitetut jakeluverkonhaltijat	jakeluverkonhaltijat sekä suurjännitteisen jakeluverkonhaltijat	
Sähkömarkkinalain 7 §:n mukaiset kantaverkonhaltijat		Energiavirasto
Sähkömarkkinalain 3 §:n 1 momentin 15 kohdassa tarkoitetut tuottajat	Kyberturvallisuuslakia ei sovelleta toimijaan, jonka harjoittama toiminta on satunnaista ja vähäistä. Satunnaisena ja vähäisenä toimintana pidetään esimerkiksi pääasiassa omaa käyttöä varten tapahtuvaa sähkön tuottamista aurinkopaneelin tai tuuligeneraattorin avulla, jossa sähköverkkoon syötetään ajoittain sähkön ylituotantoa, joka on määrällisesti vähäistä.[9] Energiaviraston tulkinnan mukaan vähäistä tuotantoa voi olla ainoastaan sähkömarkkinalain pienimuotoiseksi sähköntuotannoksi laskettava tuotanto. Tämä raja on ohjeen julkaisuhetkellä enintään kaksi megavolttiampeeria.[10]	Energiavirasto
Sähkön sisämarkkinoista annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/943 2 artiklan 8 alakohdassa määritellyt nimitetyt sähkömarkkinaoperaattorit		Energiavirasto
Sähkömarkkinalain 3 §:n 1 momentin 37 kohdassa tarkoitetut		Energiavirasto

[9] Kyberturvallisuuslain 4 §:n 5 mom. ja HE 57/2024 vp., s. 155.
[10] Sähkömarkkinalain 3 § 14 kohta. Hallituksen esityksessä (HE 45/2025 vp.) pienimuotoisen tuotannon rajaa ehdotetaan laskettavaksi kahdesta megavolttiampeerista alle yhteen megavolttiampeeriin.

sähkömarkkinoiden osapuolet, jotka tarjoavat sähkömarkkinalain 3 §:n 1 momentin 21 a kohdassa tarkoitettua aggregointia, 30 a kohdassa tarkoitettua kulutusjoustoa tai 21 c kohdassa tarkoitettua energian varastointia		
Latauspisteiden operaattorit, jotka vastaavat latauspalvelua loppukäyttäjille tarjoavan latauspisteen hallinnoinnista ja toiminnasta, myös liikennepalvelun tarjoajan nimissä ja puolesta		Energiavirasto
Kaukolämmitys ja kaukojäähdytys		
Uusiutuvista lähteistä peräisin olevan energian käytön edistämisestä annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2018/2001 2 kohdan 19 alakohdassa määritellyn kaukolämmityksen tai kaukojäähdytyksen haltijat	Soveltamisalaan kuuluvat kaukolämmityksen tai kaukojäähdytyksen haltijat, eli kaukolämmityksen ja -jäähdytyksen jakelijat. Kaukolämmön tai -jäähdytyksen tuottajat, joilla ei ole ollenkaan jakelutoimintaa, eivät kuulu lain soveltamisalaan.[11]	Energiavirasto
Kaasu		
Maakaasumarkkinalain (587/2017) 3 §:n 1 momentin 10 kohdassa tarkoitetut jakeluverkonhaltijat	Jakeluverkonhaltijat mukaan lukien suljetun jakeluverkonhaltijat	Energiavirasto
Maakaasumarkkinalain 3 §:n 1 momentin 9 kohdassa tarkoitetut siirtoverkonhaltijat		Energiavirasto
Maakaasumarkkinalain 3 §:n 1 momentin 14	Maakaasun toimituksella tarkoitetaan maakaasun	Energiavirasto

[11] HE 57/2024 vp., s. 148.

kohdassa tarkoitetut maakaasun toimittajat	ja nesteytetyn maakaasun myyntiä ja jälleenmyyntiä asiakkaille. Asiakkaalla tarkoitetaan maakaasun tukkuasiakasta ja loppukäyttäjää sekä maakaasualan yritystä, joka ostaa maakaasua. Maakaasun toimittajia ovat vähittäismyyjät, shipperit ja traderit.	
Maakaasumarkkinalain 3 §:n 1 momentin 20 kohdassa tarkoitetut varastointilaitteiston haltijat		Tukes
Maakaasumarkkinalain 3 §:n 1 momentin 22 kohdassa tarkoitetut nesteytetyn maakaasun käsittelylaitteiston haltijat		Tukes
Maakaasumarkkinalain 3 §:n 1 momentin 18 kohdassa tarkoitetut maakaasualan yritykset	Jakeluverkonhaltijat, siirtoverkonhaltijat ja maakaasun toimittajat kuuluvat kuitenkin Energiaviraston valvomiksi toimijoiksi.	Tukes
Maakaasun jalostus- ja käsittelylaitteistojen haltijat		Tukes
Öljy		
Öljynsiirtoputkistojen haltijat		Tukes
Öljyn tuotanto-, jalostus- ja käsittelylaitteistojen haltijat sekä öljyn varastointia ja siirtoa hoitavat operaattorit		Tukes
Jäsenvaltioiden velvollisuudesta ylläpitää raaka-öljy- ja/tai öljytuotevarastojen vähimmäistasoa		Tukes

annetun Neuvoston direktiivin 2009/119/EY 2 kohdan f alakohdassa määritellyt keskusvarastointiyksiköt		
Vety		
Vedyn tuotantoa ja varastointia harjoittavat toimijat		Tukes
Vedyn siirtoa harjoittavat toimijat		Energiavirasto

Lisätietoa kyberturvallisuuslain liitteisiin kuuluvasta toiminnasta löytyy kyberturvallisuuslaista: https://finlex.fi/fi/lainsaadanto/saadoskokoelma/2025/124

Kyberturvallisuuslakia ei sovelleta toimijaan, jonka harjoittama liitteessä I tai II tarkoitettu toiminta on satunnaista ja vähäistä (kyberturvallisuuslain 4 §:n 5 mom.). Toiminnan satunnaisuutta ja vähäisyyttä arvioidaan suhteessa toiminnan ajalliseen kestoon, toiminnan pääasialliseen tarkoitukseen, toiminnan laajuuteen ja toiminnasta riippuvien henkilöiden tai asiakkaiden määrään. Satunnaisena ja vähäisenä toimintana pidetään esimerkiksi pääasiassa omaa käyttöä varten tapahtuvaa sähkön tuottamista aurinkopaneelin tai tuuligeneraattorin avulla, jossa sähköverkkoon syötetään ajoittain sähkön ylituotantoa, joka on määrällisesti vähäistä.[12] Energiaviraston tulkinnan mukaisesti sähkön tuottaminen, jota ei voida laskea pienimuotoiseksi sähköntuotannoksi ei myöskään ole vähäistä.

Energiavirasto korostaa, että edellä mainitussa kyse on poikkeuksesta ja sitä tulee tulkita suppeasti. Hallituksen esityksessä on perusteltu poikkeusta siten, että se on tarpeen, jotta lain soveltamisala ei laajenisi sen tarkoituksen vastaisesti kattamaan vähäisen tai satunnaisen liitteessä I tai II tarkoitetun toiminnan johdosta kokonaisuudessaan sellaista oikeushenkilöä tai luonnollista henkilöä, jonka harjoittama toiminta muutoin täyttäisi tai ylittäisi keskisuuren toimijan määritelmän, mutta ei muutoin kuuluisi lain soveltamisalaan.[13]

Kyberturvallisuuslaissa on myös säädetty, että lakia ei sovelleta toimijaan, joka tarjoaa ainoastaan maanpuolustuksen, kansallisen turvallisuuden, yleisen järjestyksen ja turvallisuuden taikka rikosten ennalta estämisen, rikostutkinnan ja syytetoimien toteuttamiseksi toimintaa tai palvelua (kyberturvallisuuslaki 4 §:n 1-2 momentti).

[12] HE 57/2024 vp., s. 155.
[13] HE 57/2024 vp., s. 155.

3.3 Kokoluokan perusteella soveltamisalaan kuuluvat toimijat

3.3.1 Yleistä kokoluokan määrittämisestä

Edellä luvussa 3.2 on kuvattu, millainen toiminta kuuluu kyberturvallisuuslain piiriin. Energia-alan toimijan kuuluminen kyberturvallisuuslain piiriin kuitenkin edellyttää tietyn toiminnan harjoittamisen lisäksi, että yritys on kooltaan riittävän suuri taikka sen toiminta katsotaan muuten kriittiseksi. Tässä luvussa 3.3 käsitellään, miten toimijan koko määrittää lain piiriin kuulumisen. Myöhemmin luvuissa 3.4 ja 3.5 käsitellään koosta riippumattomia kyberturvallisuuslain piiriin kuuluvia toimijoita.

Jotta luvussa 3.2 mainittua toimintaa harjoittava toimija kuuluu lain soveltamisalaan, on sen täytettävä tai ylitettävä komission suosituksen 2003/361/EY liitteessä olevan 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset. Suosituksen liitteessä olevan 3 artiklan 4 kohtaa ei sovelleta toimijan määrittelyssä. Komission suositus löytyy täältä: EUR-Lex - 32003H0361 - FI - EUR-Lex.

Lisäksi edellytyksenä on, että toimija tarjoaa palvelua tai harjoittaa toimintaansa Euroopan unionissa (kts. myös luku 3.2).

Toimijan on tunnistettava, täyttääkö se keskisuuren yrityksen määritelmän vai ylittääkö se keskisuuren yrityksen määritelmän kynnysarvot. Tällä on merkitystä sen kannalta, onko toimija kyberturvallisuuslain 27 §:n mukainen tärkeä vai keskeinen toimija. Tärkeitä ja keskeisiä toimijoita on käsitelty tarkemmin luvussa 3.6.

Komission suosituksessa säädetään mikroyrityksen, pienen yrityksen ja keskisuuren yrityksen enimmäiskoosta. Keskisuuren yrityksen määritelmän ylittävät yritykset ovat suuria yrityksiä. Tässä ohjeessa käydään läpin pääpiirteittäin, miten toimija määrittää kokonsa komission suosituksen mukaan. Komission suosituksesta on julkaistu myös käyttöopas, joka sisältää havainnollistavia esimerkkejä toimijan koon määrittelemisestä. Käyttöopas löytyy täältä: Käyttöopas Pk-yrityksen määritelmä (europa.eu)

Toimija täyttää keskisuuren yrityksen määritelmän silloin, kun se ylittää pienen yrityksen määritelmän reunaehdot, mutta ei ylitä pk-yrityksille asetettuja enimmäiskynnysarvoja. Toimija täyttää siten keskisuuren toimijan määritelmän, kun sen palveluksessa on vähintään 50 työntekijää taikka sen vuotuinen liikevaihto ja tase ylittävät 10 miljoonaa euroa. Jos toimijan palveluksessa on alle 50 työntekijää, mutta sekä liikevaihto että tase ylittävät 10 miljoonaa, toimija täyttää keskisuuren toimijan määritelmän. Jos toimijan palveluksessa on alle 50 työntekijää ja joko liikevaihto tai tase, mutta ei molemmat, ylittää 10 miljoonaa euroa, toimija ei täytä keskisuuren toimijan määritelmää.

Toimija ylittää keskisuuren yrityksen määritelmän silloin, kun se ylittää komission suosituksen mukaiset pk-yritysten määritelmän enimmäiskynnysarvot. Näitä kynnysarvot ylittäviä toimijoita ovat suuret yritykset, joiden palveluksessa on vähintään 250 työntekijää taikka joiden vuotuinen liikevaihto on yli 50 miljoonaa euroa ja tase on yli 43 miljoonaa euroa. Jos toimijan palveluksessa on alle 250 työntekijää, mutta sekä vuotuinen liikevaihto että tase ylittävät kyseiset raja-arvot, toimija ylittää keskisuuren toimijan määritelmän.

Kokokriteerien täyttymistä ja ylittymistä arvioitaessa on tärkeää huomioida, että komission suosituksen mukaiset kynnysarvot eroavat esimerkiksi kirjanpitolain (1336/1997) mukaisista kynnysarvoista.

Arviointi tehdään toimijakohtaisesti ja määritelmää tulkitaan oikeussubjektikohtaisesti.

Jotta toimija voi määrittää, täyttääkö tai ylittääkö se edellä mainittuja kynnysarvoja, on sen tarkasteltava, mitkä tiedot on otettava huomioon ja arvioitava kynnysarvoja vasten. Henkilöstöä, liikevaihtoa ja tasetta koskevissa tiedoissa on otettava huomioon toimijan toiminnan laajuus kokonaisuudessaan, ei ainoastaan kyberturvallisuuslain liitteessä tarkoitetun toiminnan osalta.[14] Mikäli toimija toimii usealla eri toimialalla ja vain osa sen toiminnasta on kyberturvallisuuslain liitteessä tarkoitettua toimintaa, kokorajoitusta arvioitaessa on otettava huomioon toimijan toiminta kokonaisuudessaan. Kokorajoituksen ylittymistä koskevaa arviota ei rajoiteta vain lain liitteessä tai esimerkiksi luvussa 3.2 tarkoitetun toiminnan laajuuteen. Näin ollen liikevaihtoa, tasetta ja henkilöstömäärää arvioidaan koko toimijan osalta, mikä kattaa myös muun kuin liitteessä tarkoitetun toiminnan laajuuden. Poikkeuksena tästä on kuitenkin myöhemmin luvussa 3.3.3 käsitelty ja kyberturvallisuuslain 4 §:n 6 momentissa säädetty rajoitus silloin, jos lain liitteessä tarkoitettua toimintaa harjoittaa kunta.[15]

Keskeisintä on, jotta toimija voi määrittää, täyttääkö tai ylittääkö se edellä mainitut kynnysarvot, selvittää, onko se komission suosituksen mukainen riippumaton yritys, omistusyhteysyritys vai sidosyritys. Jos yrityksellä on omistusyhteys- tai sidosyrityksiä, yrityksen on lisättävä näiden yritysten tietoja omiin tietoihinsa arvioidessaan kynnysarvojen täyttymistä tai ylittymistä. Lisää tietojen yhdistämisestä on tämän ohjeen luvussa 3.3.2 ja komission käyttöoppaassa: Käyttöopas Pk-yrityksen määritelmä (europa.eu).

Komission suosituksen liitteen 3 artiklan 1 kohdan mukaan yritys on riippumaton, jos:

- se on täysin itsenäinen eli sillä ei ole omistuksia muissa yrityksissä eikä
- muilla yrityksillä ole omistuksia siinä

  tai

- sillä on enintään 25 %:n omistus yhden tai useamman muun yrityksen pääomasta tai äänimäärästä (suurempi näistä prosenttiosuuksista) ja/tai
- ulkoisilla tahoilla on enintään 25 %:n omistus kyseisen yrityksen pääomasta tai äänimäärästä (suurempi näistä prosenttiosuuksista)

  tai

[14] Kts. HE 57/2024 vp., s. 192.
[15] HE 57/2024 vp., s. 146.

- se ei ole toisen yrityksen sidosyritys luonnollisen henkilön kautta 3 artiklan 3 kohdassa tarkoitetulla tavalla.

Komission suosituksen liitteen 3 artiklan 2 kohdan a-d alakohdassa on mainittu neljä poikkeusta, jolloin yritystä voidaan pitää itsenäisenä, vaikka edellä mainittu 25 prosentin kynnysarvo saavutettaisiin tai ylitettäisiin, jos kyseessä on tietyistä sijoittajatyypeistä ja nämä eivät yksin tai yhdessä ole 3 kohdan mukaisessa sidossuhteessa yritykseen.

Jos yritys on riippumaton, se käyttää vain tilinpäätöksessään olevia henkilöstömäärää ja rahamääräisiä arvoja koskevia tietoja määrittääkseen, täyttääkö se kokokriteerien kynnysarvot. Jos toimija ei ole riippumaton yritys, on sen huomioitava omistusyhteys- ja sidosyritysten tietoja laskiessaan kynnysarvojen täyttymistä.

Suosituksen 4 artiklassa säädetään henkilöstömäärän ja rahamääräisten arvojen laskennassa käytettävistä tiedoista ja tarkastelujaksosta. Kokokriteerien täyttymisessä tarkastellaan viimeisintä päättynyttä ja tätä edeltävää tilikautta. Jos toimijan vuotuiset tiedot vaihtelevat välillä alittaen ja välillä ylittäen tarkasteltavat kynnysarvot, toimijan katsotaan saavuttavansa ja menettävänsä asemansa kokokategoriassa, kun ylitys tai alitus toistuu kahtena peräkkäisenä tilivuotena.

Komission suosituksesta julkaistussa käyttöoppaassa on havainnollistavia esimerkkejä, miten toimijan koko määritetään. Käyttöoppaassa on myös tietoa esimerkiksi sulautuman tai yrityskaupan vaikutuksista. Käyttöopas ja komission suositus löytyvät täältä: Käyttöopas Pk-yrityksen määritelmä (europa.eu)

3.3.2 Konserniyritykset sekä omistusyhteys- ja sidosyritykset

Toimijoiden, jotka eivät täytä edellä luvussa 3.3.1 mainittua riippumattoman yrityksen määritelmää tulee olla tarkkana, mitä tietoja sen tulee ottaa huomioon arvioidessaan komission suosituksen mukaisia kokokriteerejä. Perinteisesti tämä koskee erityisesti konsernirakenteeseen kuuluvia toimijoita, mutta myös muita, joilla on erilaisia omistussuhteita tai muita yhteyksiä toisiin yrityksiin.

Kriteerien täyttymistä tulee tarkastella oikeushenkilökohtaisesti. Tämän johdosta esimerkiksi konsernirakenteessa, kun emo- ja tytäryhtiö ovat erillisiä oikeushenkilöitä, ovat ne myös erillisiä toimijoita. Näin ollen tytäryhtiön kuuluminen soveltamisalaan ei tarkoita automaattisesti myös emoyhtiön kuulumista soveltamisalaan, jos emoyhtiö ei itsenäisesti täytä toimijan määritelmää.[16]

Omistusyhteysyritysten ja sidosyritysten määritelmät löytyvät komission suosituksen liitteen 3 artiklasta ja ne on havainnollistettu esimerkein edellä linkatussa käyttöoppaassa.

Komission suosituksen liitteen 6 artiklassa säädetään yrityksen tietojen määräytymisestä silloin, kun yrityksellä on omistusyhteys- tai sidosyrityksiä. Toimijan, joka ei ole riippumaton yritys, on otettava huomioon muiden yritysten tietoja arvioidessaan kynnysarvojen täyttymistä. Esimerkiksi omistusyhteysyrityksen on lisättävä osuus sen kumppanin henkilöstömäärästä ja rahoitustiedoista omiinsa

[16] HE 57/2024 vp., s. 147.

määrittäessään kynnysarvojen täyttymistä tai ylittymistä. Tämä osuus kuvastaa sitä osuutta osakkeista tai äänimäärästä (sen mukaan kumpi on suurempi), joka on toisen hallussa. Jos toimijalla taasen on esimerkiksi enemmistö toisen yrityksen osakkeenomistajien äänimäärästä, kyseessä on sidosyritys ja toimijan tietoihin on lisättävä 100 % kyseisen yrityksen tietoihin määrittäessä kynnysarvojen täyttymistä.

Kyberturvallisuuslain 3 §:n 5 momentin mukaan toimijaan ei sovelleta komission suosituksen liitteessä olevan 3 artiklan 4 kohtaa. Kyseinen momentti tarkoittaa, että koska mainittua kohtaa ei sovelleta, myös julkisomisteista yritystä voitaisiin pitää yrityksenä, joka ei täytä tai ylitä 1 momentin 2 kohdassa tarkoitettua kynnystä.[17]

Komission suosituksesta julkaistussa käyttöoppaassa on havainnollistavia esimerkkejä, miten toimijan koko määritetään. Käyttöoppaassa on myös tietoa esimerkiksi sulautuman tai yrityskaupan vaikutuksista. Käyttöopas ja komission suositus löytyvät täältä: Käyttöopas Pk-yrityksen määritelmä (europa.eu)

3.3.3 Kunta toiminnanharjoittajana tai yrityksen omistajana

Kyberturvallisuuslakia sovelletaan kuntalaissa (410/2015) tarkoitettuun kuntaan vain lain liitteessä tarkoitetun toiminnan osalta (kyberturvallisuuslaki 4 §:n 6 momentti). Toisin kuin yllä luvussa 3.3.1 on esitetty muiden toimijoiden osalta, kuntien ei tule ottaa huomioon sen kokotietoja arvioidessaan kunnan toimintaa kokonaisuudessaan. Kun arvioidaan kunnan harjoittaman toiminnan kuulumista soveltamisalaan, tulee kokokriteerin määrittämisessä ottaa huomioon vain lain liitteessä tarkoitettu toiminta, mutta ei kunnan henkilöstöä, tasetta tai liikevaihtoa muilta osin.[18]

Kuten edellisessä luvussa on todettu, kyberturvallisuuslain 3 §:n 5 momentin nojalla toimijaan ei sovelleta komission suosituksen liitteessä olevan 3 artiklan 4 kohtaa. Koska mainittua kohtaa ei sovelleta, myös julkisomisteista yritystä voidaan pitää yrityksenä, joka ei täytä tai ylitä 1 momentin 2 kohdassa tarkoitettua kynnystä. Toisin kuin komission suosituksessa on katsottu, julkisyhteisön tai –laitoksen omistus- tai äänioikeudelle asetettuja rajoituksia ei sovelleta.[19]

3.4 Koosta riippumattomat toimijat

Kuten edellä on luvuissa 3.2 ja 3.3 on esitetty, toimijan on selvitettävä, harjoittaako se kyberturvallisuuslain piiriin kuuluvaa toimintaa ja täyttääkö tai ylittääkö se komission suosituksessa esitetyt kokokriteerit, jotta se kuuluu kyberturvallisuuslain soveltamisalaan. Tähän kuvattuun kokoperusteiseen soveltamisalaan on kuitenkin kaksi energia-alan toimijoita koskevaa poikkeusta, jolloin toimija voi kuulua lain soveltamisalaan sen koostaan riippumatta. Tässä luvussa käsitellään

[17] HE 57/2024 vp., s. 154.
[18] HE 57/2024 vp., s. 155.
[19] HE 57/2024 vp., s. 146 ja 154.

kyberturvallisuuslain 3 §:n 3 momentin mukaisia poikkeuskriteerejä. Seuraavassa luvussa 3.5 käsitellään toista, CER-direktiiviin[20] liittyvää, poikkeusperustetta.

Kyberturvallisuuslain 3 §:n 3 momentissa säädetään eräiden toimijoiden kuulumisesta lain piiriin niiden koosta riippumatta, eli myös silloin, kun toimija ei täytä edellä luvussa 3.3 kuvattua kokoedellytystä. Näitä toimijoita ovat lain liitteessä I tai II tarkoitettua toimintaa harjoittavat tai toimijatyyppiä olevat toimijat, jotka täyttävät yhden tai useamman 3 §:n 3 momentin 1–4 kohdan kriteereistä. Lakia sovelletaan toimijaan sen koosta riippumatta, joka harjoittaa liitteissä tarkoitettua toimintaa tai on mainituissa liitteissä tarkoitettu toimija, jos:

1) se tarjoaa palvelua, joka on yhteiskunnan tai talouden kriittisten toimintojen ylläpitämisen kannalta keskeinen ja jota muut toimijat eivät tarjoa;

2) häiriö sen tarjoamassa palvelussa vaikuttaisi merkittävästi yleiseen järjestykseen, yleiseen turvallisuuteen tai kansanterveyteen;

3) häiriö sen tarjoamassa palvelussa voisi aiheuttaa merkittävän systeemisen riskin erityisesti aloilla, joilla tällaisella häiriöllä voisi olla rajat ylittäviä vaikutuksia; tai

4) se on kriittinen, koska sillä on erityisen suuri merkitys kansallisella tai alueellisella tasolla kyseisen toimialan tai palvelutyypin tai jonkin Euroopan unionin jäsenvaltion muiden keskinäisriippuvaisten toimialojen kannalta.

Valtioneuvoston asetuksella voidaan antaa tarkempia säännöksiä edellä mainituista kriteereistä (kyberturvallisuuslaki 3 §:n 4 mom.). Kyberturvallisuuslakia koskevan hallituksen esityksen mukaan toimijoissa, joita kriteerit koskevat, on kyse erityislaatuista toimintaa harjoittavista toimijoista, jotka kuuluisivat toiminnan erityisen laadun vuoksi poikkeuksellisesti lain velvoitteiden soveltamisalaan niiden koosta riippumatta. Ottaen huomioon 3 momentin 1–4 kohdassa tarkoitettujen kriteerien ja NIS2-direktiivin 2 artiklan 2 kohdan b-e alakohtien laatu, yksittäisen yrityksen käytettävissä olevien tietojen perusteella voi osoittautua epävarmaksi, täyttääkö yritys 1–4 kohdassa tarkoitettuja kriteereitä. Näin ollen kriteerien täsmentäminen valtioneuvoston asetuksella olisi tarpeen oikeustilan tarkentamiseksi siitä, milloin yksittäinen toimija täyttää 3 momentin 1–4 kohdassa tarkoitetun kriteerin EU-säädöksen velvoittavan soveltamisalan täsmentämiseksi.[21]

Edellä mainittua valtioneuvoston asetusta ei ole annettu tämän ohjeen julkaisun aikaan. Näin ollen Energiavirasto ohjeistaa, että poikkeuskriteerien yhdenmukaisen tulkinnan varmistamiseksi toimijat jäävät odottamaan valtioneuvoston asetuksen antamista. Jos toimija luvussa 3.3 esitetyllä tavalla kuuluu kokonsa johdosta kyberturvallisuuslain soveltamisalaan, toimijan tulee ilmoittautua Energiavirastolle valvottavaksi toimijaksi. Kun koosta riippumattomien toimijoiden kriteerejä on täsmennetty valtioneuvoston asetuksella, kriteerit täyttävän toimijan on

[20] Kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta annetun Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2557 (CER-direktiivi).
[21] HE 57/2024 vp., s. 153-154.

ilmoittauduttava tai päivitettävä ilmoituksensa NIS2-toimijaluetteloon. NIS2-toimijaluetteloon ilmoittautumisesta on tarkemmin tämän ohjeen luvuissa 4.1 ja 6.

3.5 CER-toimijat

NIS2-direktiiviä sovelletaan CER-direktiivin nojalla kriittisiksi toimijoiksi määritettyihin toimijoihin niiden koosta riippumatta. CER-direktiivin mukaiset kriittiset toimijat määritetään ensimmäisen kerran vuonna 2026. Energiavirasto päivittää ohjetta CER-direktiivin kansallisen toimeenpanon edetessä.

3.6 Tärkeä vai keskeinen toimija?

Kyberturvallisuuslain piiriin kuuluvat toimijat jaetaan kahteen kategoriaan: tärkeisiin ja keskeisiin toimijoihin. Toimijan on ilmoitettava valvovan viranomaisen ylläpitämään toimijaluetteloon, onko toimija tärkeä vai keskeinen toimija.

Tärkeitä toimijoita ovat keskisuuret yritykset (luku 3.3).

Keskeisiä toimijoita ovat keskisuuren yrityksen määritelmän ylittävät toimijat eli suuret yritykset (luku 3.3), CER-direktiivin mukaiset kriittiset toimijat (luku 3.5) ja muut koostaan riippumatta lain piiriin kuuluvat toimijat (luku 3.4).

Kyberturvallisuuslain velvoitteet koskevat yhtä lailla tärkeitä ja keskeisiä toimijoita, mutta Energiavirasto kohdistaa valvontaa toimijoihin eri tavoin. Valvonta kohdistetaan keskeisiin toimijoihin. Energiavirasto voi kuitenkin kohdistaa valvontaa tärkeään toimijaan, jos on perusteltu syy epäillä, että tämä ei ole noudattanut kyberturvallisuuslakia, sen nojalla annettuja määräyksiä tai NIS2-direktiivin nojalla annettuja säännöksiä (kyberturvallisuuslaki 27.1 §).

4 Velvoitteet

4.1 Ilmoittautuminen toimijaluetteloon

Toimijan on ilmoittauduttava Energiaviraston ylläpitämään toimijaluetteloon (kyberturvallisuuslaki 41 §). Jos toimijaa valvoo useampi viranomainen, sen on ilmoittauduttava erikseen kaikkiin sitä valvovien viranomaisten ylläpitämiin toimijaluetteloihin.

Toimijan on tehtävä ensimmäinen ilmoitus toimijaluetteloon viimeistään kuukauden kuluessa lain voimaantulosta eli viimeistään 8.5.2025 tai kuukauden kuluessa siitä, kun 3 §:n mukaiset toimijan kriteerit täyttyvät.

Energiaviraston valvoman toimijan on ilmoittauduttava VERTTI-valvontatietojärjestelmässä ylläpidettävään NIS2-toimijaluetteloon. Tämän ohjeen luvussa 6 on tarkemmat ohjeet VERTTI-valvontatietojärjestelmään ilmoittautumisesta.

Toimijoiden on ilmoitettava muutoksista 41 §:ssä tarkoitettuihin tietoihin viipymättä. Muutoksista kyberturvallisuuslain 41 §:n 2 momentissa lueteltuihin tietoihin on ilmoitettava Energiavirastolle kahden viikon kuluessa. Näitä tietoja ovat muun muassa ajantasaiset yhteystiedot, IP-osoitealueet ja tieto siitä, onko toimija tärkeä vai keskeinen toimija.

Energiaviraston on toimitettava Traficomin Kyberturvallisuuskeskuksessa toimivalle keskitetylle yhteyspisteelle tietoja toimijaluettelosta. Keskitetyn yhteyspisteen tehtävänä on tehdä NIS 2 -direktiivin 3 artiklan 5 kohdassa tarkoitetut ilmoitukset Euroopan komissiolle, NIS-yhteistyöryhmälle ja Euroopan unionin kyberturvallisuusvirastolle. Kyberturvallisuuskeskuksen CSIRT-yksiköllä on lisäksi oikeus saada tietoja Energiaviraston ylläpitämästä toimijaluettelosta. CSIRT-yksikön tehtävien kannalta merkityksellisiä tietoja ovat erityisesti toimijoiden yhteystiedot ja IP-osoitealueita koskevat tiedot.[22]

4.2 Yleistä riskienhallinnasta ja poikkeamista ilmoittamisesta

Kyberturvallisuuslain 2 luvussa säädetään riskienhallinnasta ja poikkeamista ilmoittamisesta. Toimijoiden riskienhallintavelvoitteista säädetään kyberturvallisuuslain 7-10 §:ssä. Seuraavassa luvussa 4.3 käsitellään kunkin pykälän asettamia velvoitteita ja eritellään, miten kyseistä velvoitetta on avattu sitä koskevassa hallituksen esityksessä. Ohjeessa ei ole käsitelty tyhjentävästi velvoitteiden sisältöä ja lisätietoa voi esimerkiksi hakea hallituksen esityksen pykäläkohtaisista yksityiskohtaisista perusteluista. Poikkeamien ilmoittamisesta on tarkemmin luvussa 4.4.

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus on laatinut suosituksen NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä. Suositus löytyy Traficomin verkkosivuilta. Toimijat voivat hyödyntää suositusta ohjenuorana kyberturvallisuuslain mukaisten toimenpiteiden suunnittelussa ja toteutuksessa.

Lisäksi Kyberturvallisuuskeskuksen verkkosivuilta löytyy monia ohjeita ja oppaita organisaatioille ja yrityksille: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille. Toimijat voivat myös tukea kyberturvallisuuden arviointia ja kehittämisestä Kyberturvallisuuskeskuksen ilmaisella kybermittari-työkalulla: www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari.

Kuten edellä luvussa 3 on todettu, toimijan määritelmää tulkitaan oikeussubjektikohtaisesti. Hallituksen esityksessä on selvyyden vuoksi todettu, että silloin kun lain liitteessä tarkoitettua toimintaa harjoittaa oikeushenkilö, kattaisi laissa tarkoitettu toimijan määritelmä silloin kyseisen oikeushenkilön kokonaisuutena. Lain ja siinä säädettyjen velvoitteiden soveltaminen ei siten ole tarkoitus rajoittua ainoastaan liitteissä tarkoitettua toimintaa harjoittavaan yksikköön tai toimintoon oikeushenkilössä, vaan velvoitteet koskisivat kyseistä oikeushenkilöä sellaisenaan, eli toimijaa kokonaisuutena. Esimerkiksi oikeushenkilö, joka toimii usealla toimialalla, joista vain osa on mainittu lain liitteissä, kuuluisi siten sääntelyn piiriin myös sellaisten toimintojen osalta, joita ei ole mainittu lain liitteissä.[23]

Edellä tässä ohjeessa on käsitelty konsernirakenteeseen kuuluvia toimijoita. Hallituksen esityksessä kyberturvallisuuslaista on todettu, että samaan konserniin kuuluvat yhtiöt voivat tehdä yhteistyötä muiden samaan konserniin kuuluvien yhtiöiden kanssa riskienhallinta- ja raportointivelvoitteiden toteuttamisessa. On hyvä huomioida, että jos konsernirakenteessa tai muussa yhtiöiden keskinäisiä omistuksia

[22] HE 57/2024 vp., s. 205.
[23] HE 57/2024 vp., s. 147.

koskevassa järjestelyssä osa yhtiöistä kuuluisi soveltamisalaan ja osa ei, olisi niiden otettava huomioon esimerkiksi riippuvuus toisten yhtiöiden tarjoamista palveluista osana lain 2 luvussa säädettyjen riskienhallinta- ja raportointivelvoitteiden noudattamista.[24]

Edellä tämän ohjeen luvussa 3.3.3 on käsitelty kuntia, jotka kuuluvat kyberturvallisuuslain soveltamisalaan, koska ne harjoittavat lain liitteessä mainittua toimintaa. Kyberturvallisuuslain 4 §:n 6 momentin mukaan lakia sovelletaan kuntalaissa tarkoitettuun kuntaan vain liitteessä I tai II tarkoitetun toiminnan osalta. Vastaavalla tavalla, miten kunnan kokokriteerejä arvioitaessa, kyberturvallisuuslain nojalla koskevia riskienhallinta-, raportointi- ja ilmoittautumisvelvoitetta ei tulkita kuntaa velvoittavaksi muun kuin lain liitteessä tarkoitetun toiminnan osalta.[25] Tämä on poikkeus edellä mainittuun, jonka mukaan kyberturvallisuuslakia sovelletaan soveltamisalaan kuuluvaan toimijaan kokonaisuutena.

Lisäksi kyberturvallisuuslain mukaan lain 2 lukua ei sovelleta toimintaan eikä palveluihin, joita tarjotaan maanpuolustuksen, kansallisen turvallisuuden, yleisen järjestyksen ja turvallisuuden taikka rikosten ennalta estämisen, rikostutkinnan ja syytetoimien toteuttamiseksi (kyberturvallisuuslaki 4 §:n 1 mom.).

Tässä ohjeessa käsitellään kyberturvallisuuslain mukaisia riskienhallintavelvoitteita. Kyberturvallisuuslain 9 §:n 5 momentin mukaan riskienhallinnassa, riskienhallinnan toimintamallissa ja hallintatoimenpiteissä on noudatettava lisäksi NIS 2 -direktiivin 21 artiklan 5 kohdan nojalla annettavia Euroopan komission täytäntöönpanosäädöksiä.

Edellä mainitun lisäksi on Energiavirasto korostaa, että jos muussa laissa tai sen nojalla annetuissa säännöksissä tai määräyksissä on kyberturvallisuuslaista poikkeavia vaatimuksia kyberturvallisuusriskien hallinnasta tai merkittävistä poikkeamista ilmoittamisesta ja vaatimukset ovat vaikutuksiltaan vähintään kyberturvallisuuslaissa säädettyjä velvoitteita vastaavia, niitä sovelletaan tämän lain vastaavien säännösten asemasta. Samoin, jos Euroopan unionin asetuksessa tai NIS2-direktiivin nojalla säädetyssä komission asetuksessa edellytetään, että toimija ottaa käyttöön kyberturvallisuutta koskevien riskien hallitsemiseksi toimenpiteitä tai ilmoittaa merkittävistä poikkeamista, ja vaatimukset ovat vaikutuksiltaan vähintään kyberturvallisuuslaissa säädettyjä velvoitteita vastaavia, säännöksiä sovelletaan tämän lain 2, 4 ja 5 luvun sekä 41 §:n asemasta (kyberturvallisuuslaki 5 §:n 1-2 mom.). Edellä mainitut poikkeukset tulevat arvioitavaksi muun muassa kyberturvallisuusverkkosäännön (NCCS) täytäntöönpanon myötä.[26]

Toimijan on myös hyvä huomioida, että henkilötietojen käsittelyn tietoturvallisuudesta säädetään edelleen luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY

[24] HE 57/2024 vp., s. 147.

[25] HE 57/2024 vp., s. 155.

[26] 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 (NCCS).

kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksessa (EU) 2016/679 (yleinen tietosuoja-asetus) ja tietosuojalaissa (1050/2018).

4.3 Riskienhallinta

4.3.1 Yleinen riskienhallintavelvoite

Kyberturvallisuuslain 7 §:ssä säädetään yleisestä riskienhallintavelvoitteesta. Sen 1 momentin mukaan toimijan on tunnistettava, arvioitava ja hallittava riskejä, joita kohdistuu sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Kyberturvallisuutta koskevalla riskienhallinnalla tulee estää tai minimoida poikkeamien vaikutus toimintaan, toiminnan jatkuvuuteen, palvelujen vastaanottajiin ja muihin palveluihin. Lain 7 §:n 2 momentin mukaan toimijan on toteutettava riskienhallintatoimenpiteet, jotka ovat ajantasaisia, oikeasuhtaisia ja riittäviä suhteessa toiminnassa käytettäville viestintäverkoille ja tietojärjestelmille aiheutuviin riskeihin ja viestintäverkon tai tietojärjestelmän merkitykseen toimijan toiminnan ja palveluntarjonnan kannalta.

Edellä mainitun pykälän yksityiskohtaisten perustelujen mukaan riskienhallinnalla tarkoitettaisiin toiminnan tai palveluntarjonnan kannalta merkityksellisiin viestintäverkkoihin ja tietojärjestelmiin kohdistuvien riskien tunnistamista, riskien vakavuuksien arvioimista sekä riittävien toimenpiteiden toteuttamista riskien hallitsemiseksi. Riskienhallinnan tarkoituksena on estää tai minimoida viestintäverkkojen ja tietojärjestelmien poikkeamien vaikutusta toimintaan, palvelujen vastaanottajiin ja muihin palveluihin häiriötilanteessa häiriön syystä riippumatta. Riskienhallinnalla on siten pyrittävä turvaamaan toiminnan jatkuvuus tilanteissa, joissa viestintäverkkojen ja tietojärjestelmien toiminta häiriintyisi joko pahantahtoisen toiminnan vuoksi tai muusta syystä. Kyberturvallisuutta koskevien riskien hallinta olisi osa organisaation riskienhallintaa. Riskienhallinnassa lähtökohtana olisi sekä riskien tunnistaminen että tulokset, joilla organisaatio haluaa vähentää riskiä.[27]

Tunnistetun riskin merkityksen määrittely on sekä subjektiivista toimijan omien liiketoiminta- tai palveluintressien perusteella, että objektiivista toimijan viestintäverkon ja tietojärjestelmän luotettavuudesta riippuvaisen palvelun yleisen ja yhteiskunnallisen merkittävyyden ja tärkeyden perusteella. Objektiiviset perusteet kuvataan tarkemmin lain 9 §:ssä ja sen perusteluissa.[28]

Riskienhallintavelvoite kohdistuu toimijan toimintaan, toiminnan jatkuvuuteen ja palveluntarjontaan. Riskienhallintavelvoitetta ei siten ole tarkoitettu kohdentumaan toimijan valmistaman tai markkinoille tarjottavan tuotteen ominaisuuksiin.[29]

Velvoite kyberturvallisuuden riskienhallinnasta olisi luonteeltaan jatkuvaa, sillä viestintäverkkojen ja tietojärjestelmien turvallisuuteen kohdistuvat riskit muuttuvat ja turvallisuustoimet kehittyvät ajan myötä. Riskienhallinnassa toteutettavien toimenpiteiden tulisi ennen kaikkea olla ajantasaisia, eli vastata ajantasaista teknologista kehitystä ja tunnettuja parhaita käytänteitä siitä, kuinka kyberturvallisuusriskeiltä voidaan suojautua tai niiden vaikutuksia minimoida. Riskienhallinnan

[27] HE 57/2024 vp., s. 160.
[28] HE 57/2024 vp., s. 160.
[29] HE 57/2024 vp., s. 161.

riittävyyttä ja oikeasuhtaisuutta arvioitaessa tulisi huomioida muun ohella viestintäverkon tai tietojärjestelmän merkitys toimijan toiminnan tai palveluntarjonnan kannalta, viestintäverkossa tai tietojärjestelmässä käsiteltävien tietojen laatu sekä muiden toimijoiden riippuvuus toimijan toiminnasta, palveluntarjonnasta, viestintäverkosta tai tietojärjestelmästä sekä erityisesti sen merkitys yhteiskunnan kriisinkestävyyden kannalta.

Kyberturvallisuuden riskienarvioinnin tarkoituksena olisi edistää ja kehittää riskienhallintakulttuuria, johon sisältyy riskienarviointi ja riskeihin suhteutettujen kyberturvallisuusriskien hallintatoimenpiteiden toteuttaminen ja seuranta. Mitä merkittävämpiä vaikutuksia riskillä toteutuessaan olisi ja mitä merkittävämpi sen toteutumisen todennäköisyys on, sitä tehokkaampia, korkeatasoisempia tai korkeampia kustannuksia aiheuttavia hallintatoimenpiteitä edellytettäisiin oikeasuhtaiselta riskienhallinnalta.[30]

4.3.2 Kyberturvallisuutta koskeva riskienhallinnan toimintamalli

Kyberturvallisuuslain 8 §:n mukaan toimijalla on oltava käytössä ajantasainen kyberturvallisuutta koskeva riskienhallinnan toimintamalli viestintäverkkojen ja tietojärjestelmien ja niiden fyysisen ympäristön suojaamiseksi poikkeamilta ja niiden vaikutuksilta. Riskienhallinnan toimintamalli on laadittava kolmen kuukauden kuluessa kyberturvallisuuslain voimaantulosta tai siitä, kun toimijan kriteerit täyttyvät (kyberturvallisuuslaki 47.3 §).

Kyberturvallisuutta koskevassa riskienhallinnan toimintamallissa on tunnistettava viestintäverkkoihin ja tietojärjestelmiin ja niiden fyysiseen ympäristöön kohdistuvat riskit ottaen huomioon kaikki vaaratekijät huomioiva lähestymistapa. Toimintamallissa on määritettävä ja kuvattava kyberturvallisuutta koskevan riskienhallinnan tavoitteet, menettelyt ja vastuut sekä 9 §:n mukaiset toimenpiteet, joilla viestintäverkkoja ja tietojärjestelmiä ja niiden fyysistä ympäristöä suojataan kyberuhkilta ja poikkeamilta (hallintatoimenpiteet).

Kyberturvallisuutta koskeva riskienhallinnan toimintamalli voi olla osa toimijan laajempaa riskienhallintasuunnitelmaa, jossa huomioidaan myös muita toimintaan kohdistuvia riskejä tai osa muuta turvallisuusvarautumista.[31] Esimerkiksi sähkö- ja maakaasuverkonhaltijat, joilla on muita varautumiseen liittyviä velvoitteita näitä koskevan erityislainsäädännön perusteella, voisivat ottaa kyberturvallisuuslain mukaiset velvoitteet osana laajempaa riskienhallintaa (sähkömarkkinalaki 28 § ja maakaasumarkkinalaki 27 §).

Kyberturvallisuutta koskeva riskienhallinnan toimintamalli tulisi luoda kaikki vaaratekijät huomioivan lähestymistavan (all-hazard approach) mukaisesti kattamaan sekä viestintäverkot ja tietojärjestelmät että niiden fyysinen ympäristö. Tarkoituksena on suojata viestintäverkkojen ja tietojärjestelmien sekä niiden avulla harjoitettua toimintaa tai tarjottavia palveluita tietoturvaloukkauksilta, järjestelmähäiriöiltä, inhimillisiltä virheiltä, vihamielisiltä teoilta ja luonnonilmiöiltä. Kaikki vaaratekijät huomioivassa lähestymistavassa tulisi siis huomioida kaikki kohtuudella ennakoitavissa olevat viestintäverkkoihin ja tietojärjestelmiin kohdistuvat

[30] HE 57/2024 vp., s. 160.
[31] HE 57/2024 vp., s. 161.

uhkatekijät, olivat ne sitten tietoturvauhkien, luonnon tai ihmisen aiheuttamia, onnettomuuksia tai tahallaan aiheutettuja.

Kaikki vaaratekijät huomioivan lähestymistavan tulisi kattaa viestintäverkkojen ja tietojärjestelmien tieto- ja kyberturvallisuusriskit kuten hallinnollisen, henkilöstö-, laitteisto- ja ohjelmisto-, tietoaineisto- sekä käyttöturvallisuuden riskit ja niiden fyysisen ympäristön, toimitilojen ja välttämättömien resurssien osalta sellaisia tapahtumia, kuten varkaus, tulipalo, tulva, televiestintähäiriö tai sähkökatko, luvaton fyysinen pääsy toimijan tietoihin tai tietojenkäsittely-ympäristöön sekä vahinko ja häirintä, joka vaarantaisi viestintäverkoissa ja tietojärjestelmissä tai niiden välityksellä käsiteltävien tietojen tai palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden. Riskienhallinnassa olisi otettava huomioon se, missä määrin toimija on riippuvainen viestintäverkosta ja tietojärjestelmistä. Mitä merkittävämmästä järjestelmästä palveluntuotannon kannalta on kyse ja mitä merkittävämpiä haitallisia vaikutuksia riski toteutuessaan järjestelmälle aiheuttaisi, sitä korkeampitasoista riskienhallintaa olisi tältä osin edellytettävä.

Kyberturvallisuutta koskeva riskienhallinnan toimintamalli ja siihen perustuvat hallintatoimenpiteet on päivitettävä ja pidettävä ajantasaisena osana edellä luvussa 4.3.1 mainittua 7 §:ssä säädettyä jatkuvaa riskien tunnistamista ja arviointia.[32]

4.3.3 Toimenpiteet kyberturvallisuutta koskevien riskien hallinnassa

Kyberturvallisuuslain 9 §:n 1 momentin mukaan toimijoiden on toteutettava kyberturvallisuutta koskevan riskienhallinnan toimintamallin mukaiset oikeasuhtaiset tekniset, operatiiviset tai organisatoriset hallintatoimenpiteet viestintäverkkojen ja tietojärjestelmien turvallisuuteen kohdistuvien riskien hallitsemiseksi ja haitallisten vaikutusten estämiseksi tai minimoimiseksi.

Pykälän yksityiskohtaisten perustelujen mukaan näiden toimenpiteiden oikeasuhteisuutta arvioitaessa on otettava asianmukaisesti huomioon se, missä määrin toimija altistuu riskeille, toimijan koko ja poikkeamien esiintymisen todennäköisyys ja niiden vakavuus, mukaan lukien niiden yhteiskunnalliset ja taloudelliset vaikutukset. Riskienhallinnassa olisi siten otettava huomioon toisaalta riskin toteutumisen todennäköisyys ja riskin toteutumisesta aiheutuvat kustannukset sekä toisaalta käytettävissä olevista riskinhallintatoimenpiteistä aiheutuva kustannus ja vaikuttavuus.[33]

Kyberturvallisuuslain 9 §:n 2 momentissa säädetään osa-alueista, jotka toimijan on otettava huomioon kyberturvallisuuden riskienhallinnan toimintamallin luomisessa ja tarpeellisten riskienhallintatoimenpiteiden määrittelyssä. Osa-alueiden listaus on vähimmäistason listaus, mikä tarkoittaa, että kaikkien toimijoiden on vähintään otettava huomioon momentissa luetellut seikat. Toimija voi toteuttaa myös laaja-alaisempaa riskienhallintaa arvioidessaan sen tarpeelliseksi.[34]

Riskienhallintatoimenpiteiden osalta olisi myös huomioitava, että ne elävät ajassa, kehittyvät ja ovat myös teknologiasidonnaisia. Lisäksi kyberturvallisuusympäristö

[32] HE 57/2024 vp., s. 161.
[33] HE 57/2024 vp., s. 162.
[34] Kts. HE 57/2024 vp., s. 162.

muuttuu jatkuvasti sekä teknologioiden että kyberturvallisuuteen liittyvien parhaiden käytäntöjen kehittyessä. Toimijoille on kyberturvallisuuslaissa jätetty liikkumavaraa siihen, miten ne huolehtivat riskienhallinnan käytännön toteutuksesta. Riskienhallintatoimenpiteissä tulisi huomioida myös, että menetelmät ja käytetty tekniikka ovat keskenään sidoksissa – esimerkiksi vanhempien verkkoteknologioiden osalta riskienhallintatoimenpiteet eivät teknologisista syistä voi olla yhtä kattavia tai sofistikoituneita verrattuna uudempiin verkkoteknologioihin.[35]

Kaikkien toimijoiden on huomioitava riskienhallinnassa ja riskienhallintatoimenpiteissä vähintään pykälän 2 momentissa tarkoitetut osa-alueet sekä kyettävä dokumentoimaan ja osoittamaan, miten riskienhallintaa osa-alueisiin liittyen toteutetaan.[36]

Pykälän 2 momentin mukaan toimintamallissa ja siihen perustuvissa hallintatoimenpiteissä on otettava huomioon ja pidettävä yllä ajantasaisesti ainakin:

1) kyberturvallisuutta koskevan riskienhallinnan toimintaperiaatteet ja hallintatoimenpiteiden vaikuttavuuden arviointi;

2) viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet;

3) viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus sekä tarvittavat menettelyt haavoittuvuuksien käsittelemiseksi ja julkistamiseksi;

4) toimitusketjun välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, niihin sisällytetyt hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt;

5) omaisuudenhallinta ja sen turvallisuuden kannalta tärkeiden toimintojen tunnistaminen;

6) henkilöstöturvallisuus ja kyberturvallisuuskoulutus;

7) pääsynhallinnan ja todentamisen menettelyt;

8) salausmenetelmien käyttämistä koskevat toimintaperiaatteet ja menettelyt sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttämiseksi;

9) poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi;

10) varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan jatkuvuuden hallinta ja tarvittaessa suojattujen varaviestintäjärjestelmien käyttö;

[35] HE 57/2024 vp., s. 162.
[36] HE 57/2024 vp., s. 162.

11) perustason tietoturvakäytännöt toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi; sekä

12) toimenpiteet viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön ja tilaturvallisuuden sekä välttämättömien resurssien varmistamiseksi.

Toimenpiteet on suhteutettava toiminnan laatuun ja laajuuteen, poikkeamasta kohtuudella ennakoitavissa oleviin välittömiin vaikutuksiin, toimijan viestintäverkkojen ja tietojärjestelmien riskialttiuteen, poikkeamien todennäköisyyteen ja vakavuuteen, toimenpiteistä aiheutuviin kustannuksiin sekä ajantasainen kehitys huomioon ottaen käytettävissä oleviin teknisiin mahdollisuuksiin torjua uhka.

Pykälän yksityiskohtaisissa perusteluissa on käyty läpi kunkin kohdan osalta, mitä velvoite pitäisi sisällään. Lisäksi Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus on laatimassa suositusta NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä. Toimijat voivat hyödyntää suositusta ohjenuorana kyberturvallisuuslain mukaisten toimenpiteiden suunnittelussa ja toteutuksessa.

Energiavirasto voi toimialallaan antaa riskienhallintavelvollisuuksia tarkentavia teknisiä määräyksiä. Energiavirasto antaa toistaiseksi tarkempia tietoja riskienhallintavelvollisuuksista tällä ohjeella. Energiaviraston antamat määräykset julkaistaan Energiaviraston verkkosivuilla (www.energiavirasto.fi) ja Finlexin viranomaisten säädöskokoelmassa (www.finlex.fi/fi/viranomaiset/).

4.3.4 Johdon vastuu

Toimijan johdolle on asetettu vastuu kyberturvallisuuslain mukaisten velvoitteiden noudattamisesta. Kyberturvallisuuslain 10 §:n mukaan toimijan johto vastaa kyberturvallisuutta koskevan riskienhallinnan toteuttamisen ja valvonnan järjestämisestä sekä hyväksyy kyberturvallisuutta koskevan riskienhallinnan toimintamallin ja valvoo sen toteuttamista. Toimijan johdolla tulee olla riittävä perehtyneisyys kyberturvallisuutta koskevaan riskienhallintaan.

Johdolla tarkoitetaan toimijan hallitusta, hallintoneuvostoa ja toimitusjohtajaa sekä muussa niihin rinnastettavassa asemassa olevaa, joka tosiasiallisesti johtaa sen toimintaa.

Pykälän yksityiskohtaisten perustelujen mukaisesti toimijan ylin johto on vastuussa viestintäverkkojen ja tietojärjestelmien kyberturvallisuutta koskevan riskienhallinnan toteuttamisesta ja valvonnasta toimijassa. Vastuu tarkoittaisi viimesijaista vastuuta järjestää ja resursoida riskienhallinta asianmukaisesti, sekä valvoa sen toimintaa. Toimijan johto hyväksyisi kyberturvallisuuden riskienhallinnan toimintamallin sekä valvoisi riskienhallinnan toteuttamista, resursointia, toimenpiteitä, riskiarvioiden ajantasaisuutta ja toimenpiteiden vaikuttavuutta. Toimijan johdolla tulisi niin ikään olla riittävä ja ajantasainen perehtyneisyys kyberturvallisuuden riskienhallintaan, mikä edellyttäisi perehtyneisyyden hankkimista joko kouluttautumalla tai muulla vastaavalla tavalla säännöllisin väliajoin. Osana 9 §:ssä

tarkoitettuja hallintatoimenpiteitä johto huolehtii myös henkilöstön kyberturvallisuuskoulutuksen järjestämisestä.[37]

4.4 Poikkeamista ilmoittaminen

4.4.1 Ilmoituskanava ja yleistä ilmoittamisesta

Toimijan on viipymättä ilmoitettava Energiavirastolle merkittävästä poikkeamasta (jäljempänä NIS-ilmoitus, kyberturvallisuuslaki 11 §:n 1 mom.).

NIS-ilmoitukset tehdään Energiavirastolle Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen ilmoituslomakkeen kautta. Ajantasaista ilmoituslinkkiä ylläpidetään Energiaviraston verkkosivuilla (www.energiavirasto.fi/kyberturvallisuus). Ilmoitussovellus ohjaa ilmoituksen täyttämisessä.

Ilmoituslomakkeen kautta ilmoitettaessa tiedot välittyvät sekä Energiavirastolle että Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskukselle. Toimija voi ilmoituksen yhteydessä pyytää Kyberturvallisuuskeskuksen CSIRT-yksiköltä ohjeita ja operatiivisia neuvoja vaikutuksia lieventävistä toimenpiteistä.

Energiavirasto voi toimialallaan antaa tarkempia teknisiä määräyksiä, joilla tarkennetaan kyberturvallisuuslain nojalla tehtävän ilmoituksen, tiedotuksen tai raportin tietosisältöä, teknistä muotoa ja menettelyä. Energiavirasto antaa toistaiseksi tarkempia tietoja edellä mainituista seikoista tällä ohjeella. Energiaviraston antamat määräykset julkaistaan Energiaviraston verkkosivuilla (www.energiavirasto.fi) ja Finlexin viranomaisten säädöskokoelmassa (www.finlex.fi/fi/viranomaiset/).

4.4.2 NIS-ilmoituskynnys

Merkittävällä poikkeamalla tarkoitetaan poikkeamaa, joka

1. on aiheuttanut tai voi aiheuttaa vakavan palvelujen toimintahäiriön,
2. on aiheuttanut tai voi aiheuttaa huomattavia taloudellisia tappioita asianomaiselle toimijalle, tai
3. on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa.

Poikkeamalla tarkoitetaan tapahtumaa, joka vaarantaa viestintäverkoissa ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden (kyberturvallisuuslaki 2 § 11 kohta).

Toimijan on poikkeaman havaittuaan suoritettava alustava arviointi poikkeaman vakavuudesta. Tällaisessa alustavassa arvioinnissa on otettava huomioon muun muassa verkko- ja tietojärjestelmät, joihin poikkeama vaikuttaa, ja erityisesti niiden merkitys toimijan palvelujen tarjoamisessa, kyberuhkan vakavuus ja tekniset ominaisuudet sekä mahdolliset taustalla olevat haavoittuvuudet, joita käytetään hyväksi, sekä toimijan kokemukset samanlaisista poikkeamista. Indikaattorit,

[37] HE 57/2024 vp., s. 170.

kuten palvelun häiriintymisen laajuus, poikkeaman kesto tai niiden palvelun vastaanottajien lukumäärä, joihin poikkeama vaikuttaa, voivat olla tärkeitä määritettäessä, onko palvelun toimintahäiriö vakava.[38]

Mikäli toimija havaitsee merkittävän poikkeaman kynnyksen täyttävän tapahtuman jonkun muun toiminnassa kuin sen omassa toiminnassa, esimerkiksi välittömän alihankkijan, järjestelmän toimittajan tai sen käyttämän pilvipalvelun toiminnassa, on toimijan ilmoitettava tällaisesta poikkeamasta vain silloin, jos kyseinen poikkeama aiheuttaisi toimijalle itselleen merkittävän poikkeaman kynnyksen ylittävän tapahtuman.[39]

Edellä mainitun lisäksi merkittävällä poikkeamalla tarkoitetaan NIS2–direktiivin 23 artiklan 11 kohdan nojalla annetussa Euroopan komission täytäntöönpanosäädöksessä täsmennettyä tilannetta, jossa poikkeama katsotaan merkittäväksi. Komissio voi hyväksyä tällaisia täytäntöönpanosäädöksiä energia-alan toimijoille.

Energiavirasto suosittelee energia-alan toimijoille, että nämä tekevät NIS-ilmoituksen aina, kun havaitusta poikkeamasta voi aiheutua palvelujen toimintahäiriö. Kyseessä on suositus ja lakisääteinen ilmoitusvelvollisuus koskee aina vain poikkeamia, jotka ovat merkittäviä.[40] Katso lisää vapaaehtoisesta ilmoittamisesta ohjeen luvusta 4.4.6.

4.4.3 Viranomaiselle tehtävien NIS-ilmoitusten ja raporttien sisältö ja aikatauluvaatimukset

NIS-ilmoitusten ja raporttien sisällöstä sekä aikatauluvaatimuksista säädetään kyberturvallisuuslain 11–13 §:ssä. Ensi-ilmoitus on tehtävä 24 tunnin kuluessa merkittävän poikkeaman havaitsemisesta ja jatkoilmoitus 72 tunnin kuluessa merkittävän poikkeaman havaitsemisesta. Toimija voi tehdä ensi- ja jatkoilmoitukset myös kerralla, mikäli sillä on ensi-ilmoituksen määräajassa, eli viipymättä ja viimeistään 24 tunnin kuluessa poikkeaman havaitsemista saatavilla molempien ilmoitusten edellyttämät tiedot.[41]

Toimijan on annettava Energiaviraston pyynnöstä lisätietoja tai väliraportti merkittävää poikkeamaa koskevista tilannepäivityksistä ja käsittelyn edistymisestä. Jos merkittävä poikkeama on pitkäkestoinen, toimijan on oma-aloitteisesti annettava väliraportti viimeistään kuukauden kuluttua jatkoilmoituksen antamisesta (kyberturvallisuuslaki 12 §).

Toimijan on annettava Energiavirastolle merkittävää poikkeamaa koskeva loppuraportti kuukauden kuluessa jatkoilmoituksen toimittamisesta tai, jos kyseessä on pitkäkestoinen poikkeama, kuukauden kuluessa sen käsittelyn päättymisestä (kyberturvallisuuslaki 13.1 §).[42]

---

[38] Kts. HE 57/2024 vp., s. 171, NIS2-direktiivin 23 artiklan 3 kohta ja johdantokappale 101.

[39] HE 57/2024 vp., s. 171.

[40] Kts myös luku 4.4.6 ja kyberturvallisuuslaki 15 § 1 mom.: Toimijat voivat vapaaehtoisesti tehdä valvovalle viranomaiselle ilmoituksia muista kuin 11 §:ssä tarkoitetuista poikkeamista, kyberuhkista ja läheltä piti –tilanteista.

[41] HE 57/2024 vp., s. 171.

[42] Kts. kyberturvallisuuslaki 11-13 §.

NIS-ilmoitukset ja -raportit tehdään Energiavirastolle Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen ilmoituslomakkeen kautta. Ilmoitussovellus ohjaa ilmoituksen täyttämisessä. Toimija voi pyytää ilmoituksen yhteydessä Kyberturvallisuuskeskuksen CSIRT-yksiköltä ohjeita ja operatiivisia neuvoja vaikutuksia lieventävistä toimenpiteistä.

Ajantasaista ilmoituslinkkiä ylläpidetään Energiaviraston verkkosivuilla (www.energiavirasto.fi/kyberturvallisuus). Ilmoitussovellus ohjaa ilmoituksen täyttämisessä.

Ensi-ilmoituksessa on ilmoitettava:

1) merkittävän poikkeaman havaitsemisesta;
2) epäilläänkö merkittävän poikkeaman johtuvan rikoksesta tai muusta lainvastaisesta tai vihamielisestä teosta;
3) rajat ylittävien vaikutuksien mahdollisuus ja todennäköisyys sekä rajat ylittävien vaikutuksien ennakointiin liittyvät tiedot.

Jatkoilmoituksessa on ilmoitettava:

1) arvio merkittävän poikkeaman laadusta, vakavuudesta ja vaikutuksista;
2) tekniset vaarantumisindikaattorit, jos sellaisia on saatavilla;
3) mahdolliset päivitykset ensi-ilmoituksen tietoihin.

Loppuraportin on sisällettävä:

1) yksityiskohtainen kuvaus poikkeamasta, sen vakavuudesta ja vaikutuksista;
2) selvitys poikkeaman todennäköisesti aiheuttaneen uhkan tai juurisyyn tyypistä;
3) selvitys toteutetuista ja meneillään olevista toimenpiteistä poikkeaman vaikutusten lieventämiseksi; ja
4) selvitys mahdollisista rajat ylittävistä vaikutuksista.

4.4.4 Poikkeamailmoituksen vastaanottaminen ja käsittely Energiavirastossa

Energiavirasto vastaa poikkeamailmoituksen tehneelle taholle viivytyksettä. Vastauksessa on alustava palaute merkittävästä poikkeamasta sekä ohjeet siitä ilmoittamisesta esitutkintaviranomaiselle, jos asiassa epäillään rikosta (kyberturvallisuuslaki 16.1 §). Vastaaminen tehdään turvaviestillä virka-aikojen puitteissa. Mikäli toimija ei vastaanota Energiaviraston vastausta kahden päivän sisällä, toimijan on syytä olla yhteydessä Energiaviraston kirjaamoon kirjaamo(at)energiavirasto.fi. Energiavirasto voi vastausviestissään pyytää toimijalta lisätietoja.[43]

[43] Kts. kyberturvallisuuslaki 12 §.

NIS-ilmoitukset ja -raportit tehdään Energiavirastolle Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen ilmoituslomakkeen kautta. Jos ilmoitus tai raportti toimitetaan kuitenkin jotain muuta kautta suoraan Energiavirastolle, Energiavirasto toimittaa ilmoitukset ja raportit Kyberturvallisuuskeskuksen CSIRT-yksikölle välittömästi. Katkeamattoman ja nopean tiedonkulun varmistamiseksi toimijan on syytä kuitenkin tehdä ilmoitukset aina ilmoitussovelluksen kautta. Ilmoitussovellus ohjaa ilmoituksen tekemisessä, jolloin toimija myös varmistuu siitä, että kaikki tarvittavat tiedot on annettu. Ajantasaista ilmoituslinkkiä ylläpidetään Energiaviraston verkkosivuilla (www.energiavirasto.fi/kyberturvallisuus).

Jos merkittävästä poikkeamasta on aiheutunut yleisen tietosuoja-asetuksen 33 artiklassa tarkoitettu henkilötietojen tietoturvaloukkaus, josta on ilmoitettava, Energiaviraston on ilmoitettava poikkeaman havaitsemisesta tietosuojavaltuutetulle (kyberturvallisuuslaki 17.2 §). Energiaviraston velvollisuus tiedottaa asiasta tietosuojavaltuutettua ei vaikuta toimijaan kohdistuviin yleisen tietosuoja-asetuksen velvoitteisiin, eikä Energiaviraston asiassa tekemä ilmoitus siten esimerkiksi täytä rekisterinpitäjän velvollisuutta ilmoittaa itse henkilötietojen tietoturvaloukkauksesta.[44]

Jos merkittävässä poikkeamassa toimijan ilmoituksen perusteella voidaan olettaa tehdyksi rikos, josta säädetty enimmäisrangaistus on vähintään kolme vuotta vankeutta, Energiaviraston on ilmoitettava merkittävän poikkeaman havaitsemisesta poliisille (kyberturvallisuuslaki 17.3 §).[45]

Jos merkittävällä poikkeamalla on vaikutuksia muihin Euroopan unionin jäsenvaltioihin tai muihin toimialoihin, Energiaviraston on tiedotettava siitä keskitetylle yhteyspisteelle eli Liikenne- ja viestintäviraston Kyberturvallisuuskeskukselle ja toimitettava sitä koskevat ilmoitukset, raportit ja muut tiedot yhteyspisteelle. Jos merkittävä poikkeama vaikuttaa toiseen Euroopan unionin jäsenvaltioon, keskitetyn yhteyspisteen on ilmoitettava siitä ilman aiheetonta viivytystä Euroopan unionin kyberturvallisuusvirastolle ja niille jäsenvaltioille, joihin poikkeama vaikuttaa. Keskitetyn yhteyspisteen on pyynnöstä toimitettava myös 11—13 §:ssä tarkoitetut ilmoitukset ja raportit sen Euroopan unionin jäsenvaltion, johon poikkeama vaikuttaa, keskitetylle yhteyspisteelle. Keskitetty yhteyspiste saa luovuttaa tässä tarkoituksessa Euroopan unionin kyberturvallisuusvirastolle ja muiden Euroopan unionin jäsenvaltioiden keskitetyille yhteyspisteille tietoja merkittävästä poikkeamasta (kyberturvallisuuslaki 17.4-5 §).[46]

4.4.5 Toimijan velvollisuus ilmoittaa poikkeamasta ja kyberuhkasta muulle kuin viranomaiselle

Toimijan on ilmoitettava viipymättä merkittävästä poikkeamasta palvelujensa vastaanottajille, jos merkittävä poikkeama todennäköisesti haittaa toimijan palvelujen tarjoamista (kyberturvallisuuslaki 14.1 §).

---

[44] HE 57/2024 vp., s. 176.

[45] HE 57/2024 vp., s. 176: ”Pykälässä tarkoitettuja rikoksia olisivat esimerkiksi rikoslain 35 luvun 3 b §:ssä tarkoitettu törkeä datavahingonteko, 38 luvun 4 §:ssä tarkoitettu törkeä viestintäsalaisuuden loukkaus, 38 luvun 6 §:ssä tarkoitettu törkeä tietoliikenteen häirintä, 38 luvun 7 b §:ssä tarkoitettu törkeä tietojärjestelmän häirintä ja 38 luvun 8 a §:ssä tarkoitettu törkeä tietomurto. Pykälässä tarkoitettuja rikoksia olisivat myös esimerkiksi rikoslain 12 luvun 1–7 §:ssä ja 9 §:ssä tarkoitetut maanpetosrikokset.”

[46] Kts. tarkemmin kyberturvallisuuslaki 17 §.

Toimijan on lisäksi ilmoitettava viipymättä merkittävästä kyberuhkasta sekä kyberuhkan hallitsemiseksi käytettävissä olevista toimenpiteistä niille palvelujensa vastaanottajille, joihin merkittävä kyberuhka saattaa vaikuttaa (kyberturvallisuuslaki 14.2 §).

Jos merkittävästä poikkeamasta tiedottaminen on yleisen edun mukaista, Energiavirasto voi velvoittaa toimijan tiedottamaan asiasta tai tiedottaa asiasta itse (kyberturvallisuuslaki 14.3 §).

4.4.6 Vapaaehtoinen ilmoittaminen

Toimijat voivat vapaaehtoisesti tehdä valvovalle viranomaiselle ilmoituksia muista kuin 11 §:ssä tarkoitetuista poikkeamista, kyberuhkista ja läheltä piti –tilanteista.[47] Kun kyseessä ei ole kyberturvallisuuslain 11 §:ssä tarkoitetusta merkittävästä poikkeamasta ilmoittamisesta ja ilmoituksen tekeminen on vapaaehtoista, ilmoittajan ei tarvitse noudattaa merkittäviin poikkeamiin liittyviä ilmoitusten ja raporttien sisältö- ja aikatauluvaatimuksia.

Energiavirasto suosittelee energia-alan toimijoille, että nämä tekevät NIS-ilmoituksen aina, kun havaitusta poikkeamasta voi aiheutua palvelujen toimintahäiriö. Kyseessä on suositus ja lakisääteinen ilmoitusvelvollisuus koskee aina vain poikkeamia, jotka ovat merkittäviä.[48]

Energiavirasto ottaa vastaan toimialallaan vapaaehtoisia poikkeamailmoituksia merkittävistä poikkeamista, poikkeamista, kyberuhkista ja läheltä piti -tilanteista myös muilta kuin kyberturvallisuuslaissa tarkoitetuilta toimijoilta. Toimialalla viitataan sähkön, kaukolämpö- ja jäähdytyksen, maakaasun ja vedyn toimialoihin. Vapaaehtoisen ilmoittajan on kuitenkin hyvä huomioida, että Energiavirastolla on jaettu toimivalta Tukesin kanssa maakaasun ja vedyn toimialoilla.

Vapaaehtoiset ilmoitukset tehdään Energiavirastolle Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen ilmoitussovelluksen kautta. Ilmoitussovellus ohjaa ilmoituksen täyttämisessä. Jos vapaaehtoinen ilmoitus toimitetaan Energiavirastolle muuta kautta, Energiaviraston on toimitettava tieto ilmoituksesta keskitetylle yhteyspisteelle eli Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskukselle.

Energiavirasto voi asettaa etusijalle kyberturvallisuuslain 11 §:ssä tarkoitettuihin ilmoituksiin vastaamisen ja käsittelyn vapaaehtoisiin ilmoituksiin nähden (kyberturvallisuuslaki 16.2 §).

5 Valvonta

Kyberturvallisuuslain valvonnasta säädetään sen 4 luvussa. Energiaviraston tehtävänä on valvoa kyberturvallisuuslain, sen nojalla annettujen määräysten ja NIS2–direktiivin nojalla annettujen säännösten noudattamista niiden toimijoiden osalta, jotka kuuluvat Energiaviraston toimivaltaan (kts. luku 3.2). NIS-valvovat

[47] Vapaaehtoisesta ilmoittamisesta säädetään kyberturvallisuuslain 15 §:ssä.
[48] Kts. luku 4.4.2.

viranomaiset tekevät keskenään yhteistyötä valvonnan toteuttamisessa (kyberturvallisuuslaki 26 §).

Valvonta kohdistetaan keskeisiin toimijoihin. Energiavirasto voi kuitenkin kohdistaa valvontaa myös muuhun kuin keskeiseen toimijaan, jos on perusteltu syy epäillä, että tämä ei ole noudattanut kyberturvallisuuslakia, sen nojalla annettuja määräyksiä tai NIS2-direktiivin nojalla annettuja säännöksiä (kyberturvallisuuslaki 27.1 § ja kts. luku 3.6).

Energiavirasto voi asettaa sille kyberturvallisuuslaissa säädetyt tehtävät tärkeysjärjestykseen riskiperusteisesti. Energiaviraston ottaa valvonnan kohdistamisessa ja kyberturvallisuuslain 29–34 §:ssä tarkoitettujen toimien käyttämisestä päättäessään huomioon lain liitteessä tarkoitetun toiminnan laatu ja laajuus, tietojärjestelmän tai viestintäverkon merkitys kyseiselle toiminnalle ja lain 37 §:ssä tarkoitetut seikat (kts. kyberturvallisuuslaki 27 §).

Kyberturvallisuuslaissa säädetään Energiaviraston valvontatoimivaltuuksista. Energiavirastolla on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada toimijalta muun muassa kyberturvallisuutta koskevien riskien hallintaa, riskienhallinnan toimintamallia, hallintatoimenpiteitä ja merkittävää poikkeamaa koskevat tiedot sekä muut edellä mainittuihin tietoihin välittömästi liittyvät tiedot, jotka ovat välttämättömiä kyberturvallisuutta koskevan riskienhallintavelvoitteen noudattamisen ja merkittävistä poikkeamista ilmoittamisen ja raportoinnin valvontaa varten. Tiedot on luovutettava viipymättä, Energiaviraston pyytämässä muodossa ja maksutta (kts. kyberturvallisuuslaki 28 §).[49]

Jos tietopyyntö kohdistuu sellaiseen osaan toimijan riskienhallinnasta, jonka toimija on ulkoistanut, toimija on velvollinen toimittamaan tiedon riippumatta siitä, onko tieto toimijan vai ulkoistetun tahon hallussa. Toimija on siten tarvittaessa velvollinen hankkimaan pyydetyt tiedot toimittajaltaan ja toimittamaan ne Energiavirastolle.[50]

Tiedonsaantioikeuden käyttäminen on ensisijainen ja pääasiallinen toimijoihin kohdistuva valvovan viranomaisen toimenpide, jonka tarkoituksena on mahdollistaa riskienhallinta- ja raportointivelvoitteiden noudattamisen valvonta.[51]

Tiedonsaantioikeuden lisäksi Energiavirastolla on oikeus tehdä toimijaa koskeva tarkastus. Tarkastus tehdään kyberturvallisuuslaissa tai sen nojalla annetussa määräyksessä taikka NIS2-direktiivin nojalla annetuissa säännöksissä säädettyjen velvollisuuksien noudattamisen valvomiseksi siinä laajuudessa kuin se on tarpeen (kts. kyberturvallisuuslaki 29 §). Tarkastuksessa voi olla kyse satunnaistarkastuksesta, tarkastuksesta merkittävän poikkeaman jälkeen tai riskiarviointiin perustuvista

[49] Kyberturvallisuuslain 28 §:ssä tarkoitettu tiedonsaantioikeus ei koske salassa pidettäviä tietoja julkisen hallinnon turvallisuusverkkotoiminnasta annetussa laissa (10/2015) tarkoitetusta turvallisuusverkon palvelutuotannosta tai palvelujen käytöstä eikä tietoja, joiden luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin niihin liittyvää tärkeää etua.

[50] Kts. HE 57/2024 vp., s. 195.

[51] HE 57/2024 vp., s. 194.

säännöllisistä tarkastuksista yhteiskunnan toiminnan kannalta kriittisimmille toimijoille.[52]

Energiavirastolla on lisäksi tietyissä tilanteissa oikeus velvoittaa toimija teettämään kyberturvallisuuden riskienhallintaan kohdistuva turvallisuusauditointi (kts. kyberturvallisuuslaki 30 §).

Jos Energiavirasto havaitsee, että toimija ei ole noudattanut edellä mainittuja säädöksiä tai säädettyjen velvollisuuksien noudattamisessa on puutteita, kyberturvallisuuslaissa on säädetty valvontatoimenpiteistä, joihin Energiavirasto voi ryhtyä velvoitteiden noudattamisen varmistamiseksi. Kyberturvallisuuslain 31 §:ssä säädetään valvontapäätöksestä ja varoituksesta. Kyberturvallisuuslain 32 §:ssä säädetään johdon toiminnan rajoittamisesta. Lain 34 §:ssä säädetään mahdollisuudesta asettaa päätöksen tehosteeksi uhkasakko, teettämisuhka tai keskeyttämisuhka.

Liikenne- ja viestintäviraston yhteydessä toimiva seuraamusmaksulautakunta määrää hallinnollisen seuraamusmaksun valvovan viranomaisen eli esimerkiksi Energiaviraston esityksestä. Kyberturvallisuuslain 35 §:n 1 momentin mukaisesti toimijalle voidaan määrätä hallinnollinen seuraamusmaksu, jos se tahallaan tai törkeästä huolimattomuudesta laiminlyö:

1) 7 §:ssä tarkoitetun velvollisuuden hallita riskejä, 8 §:ssä tarkoitetun kyberturvallisuutta koskevan riskienhallinnan toimintamallin laatimisen tai 9 §:n 1 momentissa tarkoitettujen osa-alueiden huomioimisen osana kyberturvallisuuden riskienhallinnan toimintamallia;

2) toteuttaa 9 §:n 2 momentissa tarkoitetut toimenpiteet;

3) antaa 11 §:ssä tarkoitetun poikkeamailmoituksen, 12 §:ssä tarkoitetun väliraportin tai 13 §:ssä tarkoitetun loppuraportin valvovalle viranomaiselle;

4) antaa 41 §:ssä tarkoitetut tiedot valvovalle viranomaiselle.

Seuraamusmaksun määräämisestä, enimmäismäärästä ja määräämättä jättämisestä säädetään tarkemmin kyberturvallisuuslain 5 luvussa.

Energiavirasto voi peruuttaa sähköverkkoluvan, maakaasuverkkoluvan sekä sähkömarkkinalain 12 §:ssä ja maakaasumarkkinalain 11 §:ssä säädetyn vapautuksen tai poikkeusluvan, jos luvanhaltija toistuvasti ja oleellisesti rikkoo kyberturvallisuuslakia, eikä luvanhaltijalle etukäteen annettu varoitus luvan peruuttamisesta ole johtanut toiminnassa esiintyneiden puutteiden korjaamiseen (laki sähkö- ja maakaasumarkkinoiden valvonnasta 590/2013 23 §:n 6 kohta).

[52] HE 57/2024 vp., s. 197.

6 Toimijaluetteloon ilmoittautuminen (VERTTI-valvontatietojärjestelmä)

6.1 NIS2-toimijaluettelo VERTTI-valvontatietojärjestelmässä

Energiaviraston ylläpitämä kyberturvallisuuslain 41 §:n mukainen toimijaluettelo eli NIS2-toimijaluettelo on VERTTI-valvontatietojärjestelmässä. Linkki VERTTI-tietojärjestelmään: https://vertti.energiavirasto.fi/.

Huomioitavaa: Tutustu ennen ilmoituksen aloittamista huolellisesti tämän ohjeen lukuun 3 koskien kyberturvallisuuslain soveltamisalaa.

Toimijaluetteloon ilmoittautumista varten käyttäjä tarvitsee valtuuden ”Kyberturvallisuuteen liittyvien toimijatietojen ilmoittaminen”. Lisätietoa valtuudesta ja valtuuttamisesta löydät suomi.fi-verkkosivuilta: https://www.suomi.fi/valtuudet/valtuusasiat/kyberturvallisuuteen-liittyvien-toimijatietojen-ilmoittaminen/ebecc9b754228fda35055eebd09b89dc.

Kun käyttäjällä on Suomi.fi valtuus, yläreunan valikossa näkyy valittavana otsikko ”NIS2-toimijaluettelo” ja painike, jonka kautta voi muokata käyttäjätietoja.

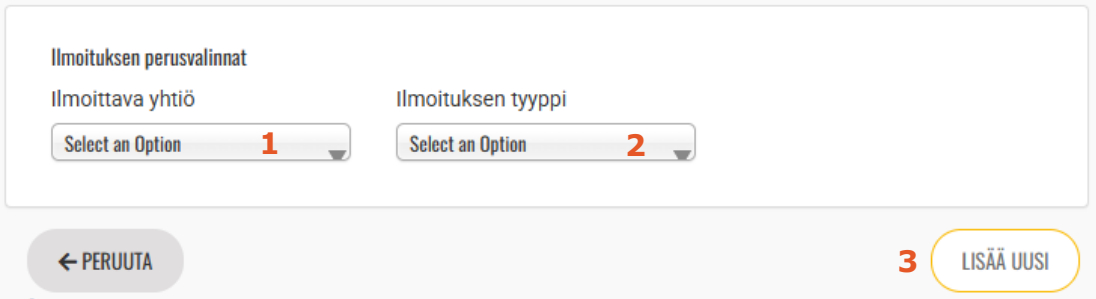
6.2 Uuden ilmoituksen luominen

Uuden ilmoituksen luominen aloitetaan NIS2-toimijaluettelo välilehdeltä painamalla ”Lisää uusi”-painiketta, joka avaa ilmoituksen perusvalinnat.

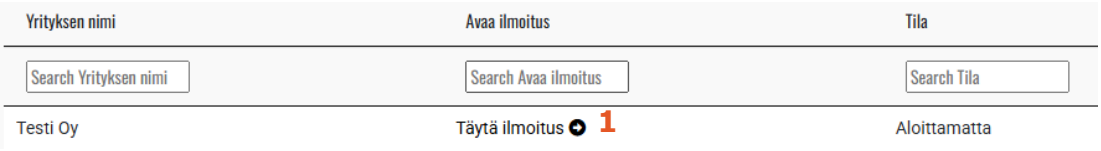
”Lisää uusi”-sivulla ilmoittajan tulee valita ilmoituksen antava yritys (1) ja ilmoituksen tyypiksi valitaan alasvetovalikosta ”Uusi ilmoitus NIS2-toimijaluetteloon”. Uusi ilmoitus luodaan painamalla ”Lisää uusi” (3).

Käyttäjällä on valittavana useampi yritys, jos käyttäjällä on valtuus asioida useamman yrityksen puolesta. Ilmoitus tehdään yrityskohtaisesti eli ilmoitus tulee luoda kullekin ilmoitettavalle yritykselle erikseen.

Yrityksellä voi olla vain yksi aktiivinen ilmoituslomake. Jos ilmoitat muutoksista jo ilmoitettuihin tietoihin tai ilmoitat poistumisesta toimijaluettelosta, avaa ilmoitus edelliseltä sivulta.



NIS2-toimijaluettelo-pääsivulle muodostuu tämän jälkeen uusi ilmoitus, jota pääsee täyttämään valitsemalla ”Avaa ilmoitus”-sarakkeesta ”Täytä ilmoitus” (1).

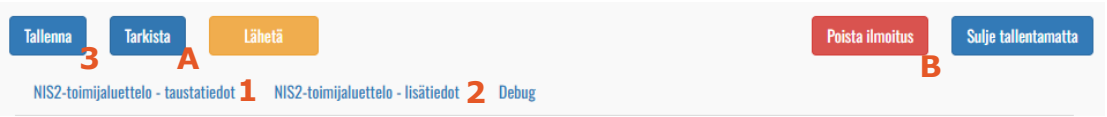


6.3 Uuden ilmoituksen täyttäminen

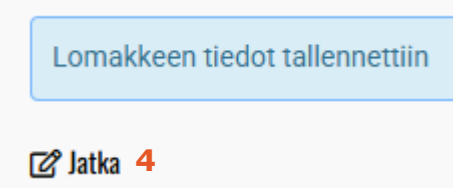
6.3.1 Ilmoituslomakkeen rakenne ja painikkeet

Ilmoituksen täytettävät kohdat avautuvat valittaessa ”NIS2-toimijaluettelo – taustatiedot” (1) ja ”NIS2-toimijaluettelo – lisätiedot” (2). Molemmat välilehdet tulee täyttää ja tallentaa ”Tallenna”-painikkeella (3) ennen ilmoituksen lähettämistä.

”Tarkista”-painikkeella (A) käyttäjä voi tarkistaa, onko kaikkiin pakollisiin kohtiin vastattu. ”Poista ilmoitus”-painikkeella (B) käyttäjä voi poistaa aloitetun ilmoituksen. Kun ilmoitus on poistettu, uusi ilmoitus luodaan luvun 6.2 mukaisesti.



Tallentamisen jälkeen ilmoitukselle voi palata takaisin painamalla ”Jatka” (4).



6.3.2 Ilmoitettavat tiedot: taustatiedot-välilehti

Kohta 1: Yrityksen nimi

Yrityksen nimi täyttyy automaattisesti ilmoituksen perustietovalintojen perusteella.

Kohta 2: Y-tunnus

Y-tunnus täyttyy automaattisesti ilmoituksen perustietovalintojen perusteella.

Yrityksen yhteystiedot

Kohta 3: Katuosoite

Lisää tieto yrityksen yhteystiedoista.

Kohta 4: Postinumero

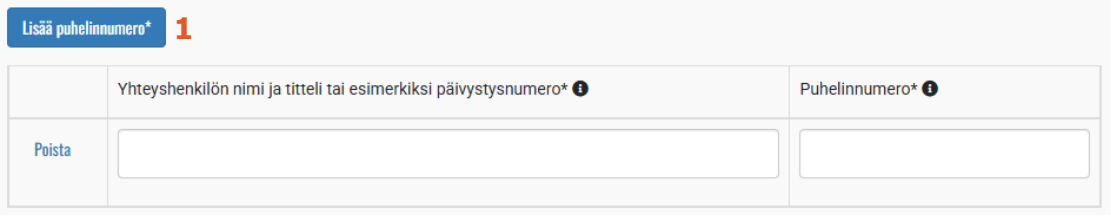
Lisää tieto yrityksen yhteystiedoista.

Kohta 5: Paikkakunta

Lisää tieto yrityksen yhteystiedoista.

Kohta 6: Puhelinnumero

Lisää tieto yrityksen yhteystiedoista. Käyttäjä voi lisätä useamman kuin yhden puhelinnumeron. Puhelinnumeron lisääminen aloitetaan valitsemalla ”Lisää puhelinnumero” (1). Kunkin ilmoitettavan puhelinnumeron kohdalla ilmoita yhteyshenkilön nimi ja titteli tai onko kyseessä esimerkiksi päivystysnumero.



Kohta 7: Sähköpostiosoite

Lisää tieto yrityksen yhteystiedoista. Käyttäjä voi lisätä useamman kuin yhden sähköpostiosoitteen. Sähköpostiosoitteen lisääminen aloitetaan valitsemalla ”Lisää sähköpostiosoite” (1). Kunkin ilmoitettavan sähköpostiosoitteen kohdalla ilmoita yhteyshenkilön nimi ja titteli tai onko kyseessä esimerkiksi kirjaamo.

Kohta 8: Osallistuminen kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn

Yrityksen tulee ilmoittaa, osallistuuko se Traficomin Kyberturvallisuuskeskuksen kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn. Huomioitavaa: Ilmoita nykyhetki.

Kyberturvallisuuslain 23 §:n mukaisena vapaaehtoisena jakamisjärjestelynä pidetään muun muassa Traficomin Kyberturvallisuuskeskuksen CSIRT-yksikön kanssa tiedonvaihtoryhmissä tapahtuvaa yhteistyötä, johon liittyy vapaaehtoista kyberturvallisuustietojen jakamista. Vapaaehtoiseksi jakamisjärjestelyksi katsotaan muun muassa toimijan kuuluminen Traficomin Kyberturvallisuuskeskuksen CSIRT-yksikön ylläpitämälle toimialakohtaiselle sähköpostilistalle. Kaikkien kyberturvallisuuslain kohteena olevien toimijoiden on mahdollista liittyä listalle. Listoille lähetetään toimialaan liittyviä tietoturvatiedotteita ajankohtaisista aiheista.

Lisätietoa listoista ja niille liittymisestä: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/tilannekuvatuotteet?toggle=Toimialakohtainen%20tilannekuva%20ja%20tiedotteet

6.3.3 Ilmoitettavat tiedot: lisätiedot-välilehti

Ilmoita kyberturvallisuuslain liitteessä I tarkoitettu toiminta tai toimijatyyppi

Kohta 8: Valitse, millä toimialan osalla yritys toimii

Valitse alasvetovalikosta ne Energiaviraston valvomat kyberturvallisuuslain liitteessä mainitut toimialan osat, joilla toimija toimii. Valittavia toimialan osia ovat sähkö, kaukolämmitys tai kaukojäähdytys, kaasu ja vety. Ilmoita kaikki toimialan osat, joilla toimija toimii ja kuuluu kyberturvallisuuslain piiriin.

Jos toimija harjoittaa Energiavirasto valvoman toiminnan lisäksi muuta kyberturvallisuuslain piiriin kuuluvaa toimintaa, jota valvoo toinen NIS-valvontaviranomainen, sen on erikseen ilmoittauduttava kaikkien näiden viranomaisten ylläpitämiin toimijaluetteloihin.

Huomioitavaa: Valittavana on vain ne toimialan osat, jotka ovat Energiaviraston valvomia toimialan osia. Energia-alalla esimerkiksi öljyn toimialan osan valvova viranomainen on Turvallisuus- ja kemikaalivirasto (Tukes).

Kohta 8.1: Valitse, mitä valitun toimialan mukaista toimintaa yritys harjoittaa

Kun käyttäjä on valinnut, millä toimialan osalla yritys toimii, käyttäjän on tarkennettava, mitä kyseisen toimialan osan toimintaa yritys harjoittaa. Valitse alasvetovalikosta kyberturvallisuuslain mukaiset toimijatyypit, jotka kuvaavat yritystä ja joiden myötä yritys kuuluu kyberturvallisuuslain soveltamisalaan.

Huomioitavaa: Valittavana ovat vain ne toimijatyypit, jotka ovat Energiaviraston valvomia toimijatyyppejä. Kaasun ja vedyn osalta Energiavirastolla ja Turvallisuus- ja kemikaalivirastolla (Tukes) on jaettu valvontatoimivalta, joka on riippuvainen yrityksen toimialan osalla harjoittamasta toiminnasta (kts. luku 3).

Jos toimija harjoittaa useampaa kyberturvallisuuslain mukaista toimintaa, joista osa kuuluu Energiaviraston valvottavaksi ja osa esimerkiksi Turvallisuus- ja kemikaaliviraston (Tukes), toimijan on ilmoittauduttava erikseen kummankin viranomaisten ylläpitämään toimijaluetteloon.

Tarkempi tieto toimijan harjoittamasta toiminnasta on välttämätöntä kyberturvallisuuslain mukaisten valvontatehtävien hoitamiseksi.

Tärkeä vai keskeinen toimija

Kohta 9: Valitse, onko toimija tärkeä vai keskeinen toimija

Valitse alasvetovalikosta, onko toimija tärkeä vai keskeinen toimija (kts. luku 3.6).

Kohta 9.1: Miksi yritys on keskeinen toimija?

Jos käyttäjä on valinnut, että toimija on keskeinen, käyttäjän on tarkennettava, miksi toimija on keskeinen toimija. Valitse alasvetovalikosta, miksi yritys on keskeinen toimija.

Huomioitavaa: Energiavirasto on ohjeistanut tämän ohjeen luvussa 3.4, että koosta riippumatta soveltamisalaan kuuluvat toimijat jäävät poikkeuskriteerien yhdenmukaisen tulkinnan varmistamiseksi odottamaan valtioneuvoston asetuksen antamista. Jos toimija luvussa 3.3 esitetyllä tavalla kuuluu kokonsa johdosta kyberturvallisuuslain soveltamisalaan, toimijan tulee ilmoittautua Energiavirastolle valvottavaksi toimijaksi. Kun koosta riippumattomien toimijoiden kriteerejä on täsmennetty valtioneuvoston asetuksella, kriteerit täyttävän toimijan on ilmoittauduttava tai päivitettävä ilmoituksensa NIS-toimijaluetteloon.

CER-direktiivin mukaiset toimijat määritetään ensimmäisen kerran vuonna 2026 (kts luku 3.5).

Kohta 9.1.1: Valitse, miksi yritys on keskeinen koostaan riippumatta

Jos käyttäjä on valinnut, että toimija on keskeinen koostaan riippumatta, käyttäjän on tarkennettava, minkä tai mitkä neljästä poikkeusperusteesta toimija täyttää.

Huomioitavaa: Energiavirasto on ohjeistanut tämän ohjeen luvussa 3.4, että koosta riippumatta soveltamisalaan kuuluvat toimijat jäävät poikkeuskriteerien yhdenmukaisen tulkinnan varmistamiseksi odottamaan valtioneuvoston asetuksen antamista. Jos toimija luvussa 3.3 esitetyllä tavalla kuuluu kokonsa johdosta kyberturvallisuuslain soveltamisalaan, toimijan tulee ilmoittautua Energiavirastolle valvottavaksi toimijaksi. Kun koosta riippumattomien toimijoiden kriteerejä on täsmennetty valtioneuvoston asetuksella, kriteerit täyttävän toimijan on ilmoittauduttava tai päivitettävä ilmoituksensa NIS-toimijaluetteloon.

Kohta 9.1.2: Perustele, miksi yritys on koostaan riippumatta keskeinen toimija

Jos käyttäjä on valinnut, että toimija on keskeinen koostaan riippumatta, käyttäjän on perusteltava, miksi yritys on koostaan riippumatta keskeinen toimija. Valitse tarvittaessa useampi peruste. Näin on esimerkiksi, jos toimija ylittää keskisuuren yrityksen kriteerit ja toimija on myös tunnistettu CER-direktiivin mukaiseksi kriittiseksi toimijaksi.

Huomioitavaa: Energiavirasto on ohjeistanut tämän ohjeen luvussa 3.4, että koosta riippumatta soveltamisalaan kuuluvat toimijat jäävät poikkeuskriteerien

yhdenmukaisen tulkinnan varmistamiseksi odottamaan valtioneuvoston asetuksen antamista. Jos toimija luvussa 3.3 esitetyllä tavalla kuuluu kokonsa johdosta kyberturvallisuuslain soveltamisalaan, toimijan tulee ilmoittautua Energiavirastolle valvottavaksi toimijaksi. Kun koosta riippumattomien toimijoiden kriteerejä on täsmennetty valtioneuvoston asetuksella, kriteerit täyttävän toimijan on ilmoittauduttava tai päivitettävä ilmoituksensa NIS-toimijaluetteloon.

Kohta 10: Vapaamuotoinen kuvaus toimijan toiminnasta

Kohta ei ole pakollinen. Kohtaan käyttäjä voi lisätä vapaamuotoisen kuvauksen yrityksen toiminnasta. Konserniin kuuluva toimija voi tuoda esiin, mihin konserniin yritys kuuluu. Käyttäjä voi tuoda myös ilmi, jos yritystä valvoo Energiaviraston lisäksi jokin muu NIS2-valvontaviranomainen.

Toiminnan maantieteellinen laajuus

Kohta 11: EU-jäsenvaltiot, joissa yritys tarjoaa NIS2-direktiivin soveltamisalaan kuuluvia palveluja

Toimijan on ilmoitettava valvovalle viranomaiselle luettelo niistä Euroopan unionin jäsenvaltioista, joissa se tarjoaa NIS2-direktiivin soveltamisalaan kuuluvia palveluja. Käyttäjä valitsee kaikki soveltuvat maat alasvetovalikosta.

IP-osoitealueet

Kohta 12: IP-osoitealueet

Toimijan on ilmoitettava kaikki toimijalle kuuluvat julkiset IP-osoitealueet.

IP-osoitteiden ilmoittaminen mahdollistaa ennakoivan haavoittuvuuksien, kyberuhkien ja turvattomasti määritettyjen viestintäverkkojen ja tietojärjestelmien asetuksien havaitsemisen kyberturvallisuuslain kohteena olevista toimijoista. Näistä havainnoista ilmoitetaan toimijalle, mikä parantaa toimijoiden mahdollisuuksia suojautua haavoittuvuuksien hyväksikäytöltä ja kyberuhilta. Suomessa toimenpiteistä vastaa Liikenne- ja viestintäviraston CSIRT-yksikkö, jolla on oikeus saada Energiavirastolta tietoja toimijaluettelosta.

Mikäli toimijan IP-osoitteita hallinnoi joku toinen osapuoli esimerkiksi teleoperaattori tai palveluntarjoaja, on sääntelyn piirissä olevan toimijan tehtävä hankkia nämä IP-osoitetiedot ja toimittaa tiedot edelleen valvovalle viranomaiselle.

IP-osoite: Internetiin kytketyn tietojenkäsittely- tai tiedonsiirtolaitteen tai verkkoliittymän yksilöivä numeerinen tunnus esimerkiksi 198.51.100.34

IP-osoitealue: Useamman julkisen verkko-osoitteen (IP-osoitteen) muodostama IP-osoitealue.

IP-osoitealueet tulee ilmoittaa NIS2-toimijaluetteloon seuraavassa muodossa:

- Esimerkiksi 198.51.100.0–198.51.100.255 tai 93.190.96.0-93.190.103.255 (IP-range) tai

- Esimerkiksi 198.51.100.0/24 tai 93.190.96.0/21 (CIDR-muoto)

Tiedot on mahdollista ilmoittaa tarvittaessa myös yksittäisinä IP-osoitteina, mikäli laajempi osoitealue ei ole tiedossa: esimerkiksi 198.51.100.34

Tiedot on mahdollista ilmoittaa myös IPv6-muodossa: esimerkiksi 2001:db8:3333:4444:5555:6666:7777:8888

Huomioitavaa: Seuraavat verkot ovat niin sanottuja privaattiverkkoja, eli sisäisiä osoitealueita, eikä niitä tule ilmoittaa toimijaluetteloon:

- IPv4:

  10.0.0.0-10.255.255.255 tai 10.0.0.0/8

  172.16.0.0-172.31.255.254 tai 172.16.0.0/12

  192.168.0.0-192.168.255.255 tai 192.168.0.0/24

- IPv6:

  fc00::/7

  fec0::/10

Mikäli toimijalla on käytössä sekä staattisia että dynaamisia IP-osoitteita, tulee toimijan toimittaa Energiavirastolle tiedot vähintään staattisista IP-osoitteista, sekä pyrkiä toimittamaan dynaamisia IP-osoitteita koskeva tarkoituksenmukaiset tiedot, joita voivat olla esimerkiksi listaus verkkoblokeista tai –lohkoista, joista toimijan IP-osoite on varattu, sekä kyseisten osoitteiden lukumäärä, tai muu vastaava tarkoituksenmukainen tieto.

Tarvittavien tietojen selvittämiseksi suosittelemme olemaan yhteydessä omaan IT-ylläpitoon tai palveluntarjoajaan.

Toimijoiden on ilmoitettava valvovalle viranomaiselle kaikista muutoksista toimitettuihin IP-osoitetietoihin viipymättä ja joka tapauksessa kahden viikon kuluessa muutospäivästä.

Lisätiedot

Kohta 13: Olen tarkistanut, että lomakkeelle täytetyt tiedot ovat oikein

Käyttäjä valitsee, että täytetyt tiedot ovat tarkistettu oikeiksi.

Kohta 14: Suostumus sähköiseen tiedoksiantoon

Käyttäjä valitsee, suostuuko se, että Energiavirasto lähettää kaikki NIS2-toimijaluetteloon liittyvät asiakirjat ja viestit sähköisesti yhteyshenkilön sähköpostiosoitteeseen. Suostumus kattaa päätökset, lisäselvityspyynnöt, muut dokumentit ja viestit.

Vahvistusviestit toimijaluetteloon ilmoittautumisesta, muutettujen tietojen ilmoittamisesta ja toimijaluettelosta poistumisesta sekä ilmoitus korjauspyynnöstä lähetetään aina automaattisesti sähköpostitse yhteyshenkilön sähköpostiosoitteeseen.

Kohta 15: Nimi

Tieto täyttyy automaattisesti ilmoituslomakkeen lähettämisen yhteydessä. Jos tiedoissa on puutteita, tiedot on korjattava käyttäjän omista tiedoista, jotka löytyvät sivun oikeasta yläreunasta.

Kohta 16: Puhelinnumero

Tieto täyttyy automaattisesti ilmoituslomakkeen lähettämisen yhteydessä. Jos tiedoissa on puutteita, tiedot on korjattava käyttäjän omista tiedoista, jotka löytyvät sivun oikeasta yläreunasta.

Kohta 17: Sähköpostiosoite

Tieto täyttyy automaattisesti ilmoituslomakkeen lähettämisen yhteydessä. Jos tiedoissa on puutteita, tiedot on korjattava käyttäjän omista tiedoista, jotka löytyvät sivun oikeasta yläreunasta.

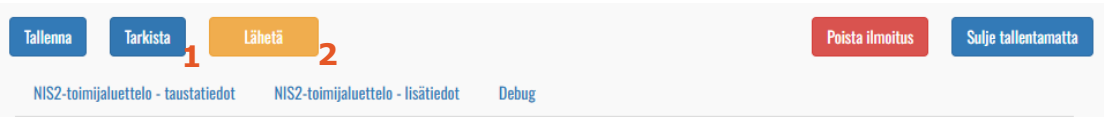
Kohta 18: Lähetetty

Tieto täyttyy automaattisesti ilmoituslomakkeen lähettämisen yhteydessä.

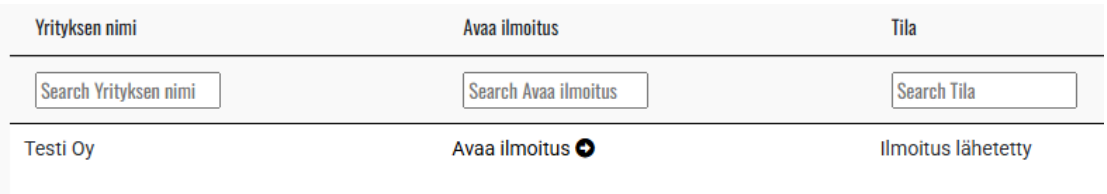
6.4 Uuden ilmoituksen lähettäminen

Käyttäjän täytettyä ilmoituksen, käyttäjä voi tarkistaa ”Tarkista”-painikkeella (1), että kaikki pakolliset kohdat on täytetty. Mikäli pakollisia kohtia on täyttämättä, järjestelmä huomauttaa tästä ja käyttäjän tulee täyttää puuttuvat tiedot. Käyttäjä voi muuttaa tietoja siihen asti, että ilmoitus on lähetetty.

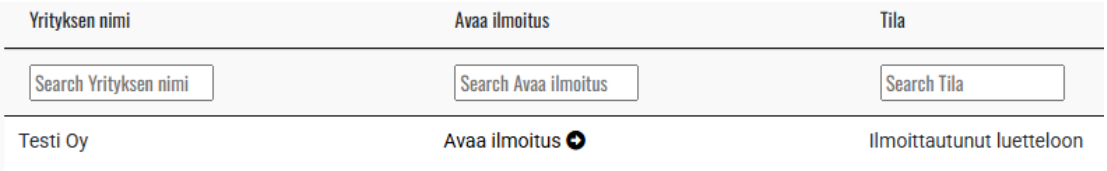
Ilmoitus lähetetään ”Lähetä”-painikkeella (2).



Kun ilmoitus on lähetetty, sen tilaksi muuttuu ”Ilmoitus lähetetty”.

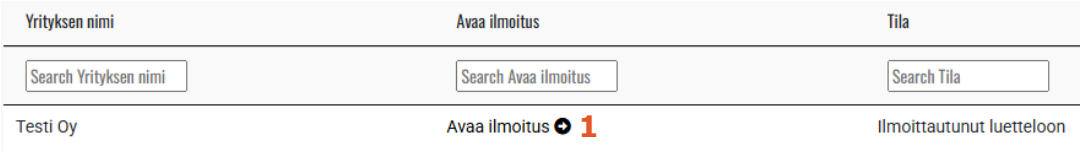


Käyttäjälle lähetetään sähköpostitse vahvistus, kun toimija ilmoittautunut onnistuneesti toimijaluetteloon. Ilmoituksen tilaksi muuttuu tämän jälkeen ”Ilmoittautunut luetteloon”.



6.5 Ilmoita muuttuneista tiedoista toimijaluetteloon

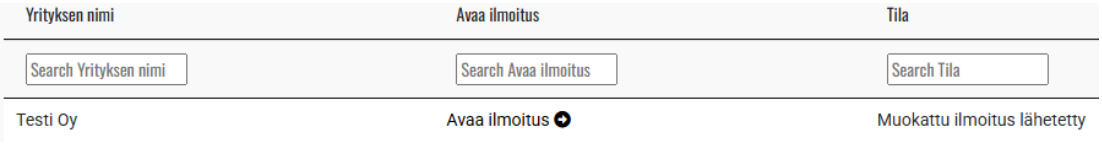
Jos toimijan tiedoissa tapahtuu muutoksia, käyttäjä aloittaa muuttuneiden tietojen ilmoittamisen avaamalla toimijan ilmoitus ”Avaa ilmoitus”-painikkeella.



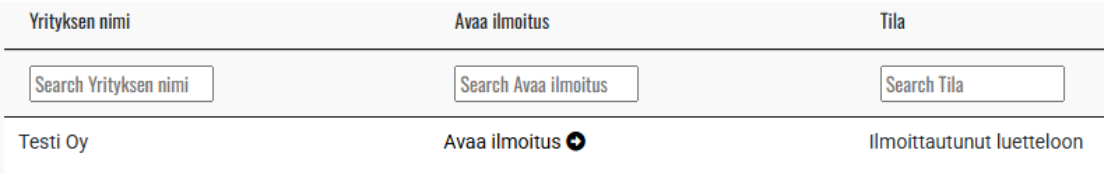
Valitsemalla ”Muokkaa tietoja”-painikkeen (2), käyttäjä voi muokata taustatiedot- ja lisätiedot-välilehtien alla olevia tietoja.

Käyttäjä tallentaa tiedot ”Tallenna”-painikkeella (3) ennen ilmoituksen lähettämistä. Kun käyttäjä on muokannut, lisännyt tai poistanut tarvittavat tiedot, käyttäjä lähettää muokatun ilmoituksen Energiavirastolle ”Lähetä”-painikkeella (4).

Kun muokatut tiedot on lähetetty, ilmoituksen tilaksi muuttuu ”Muokattu ilmoitus lähetetty”.



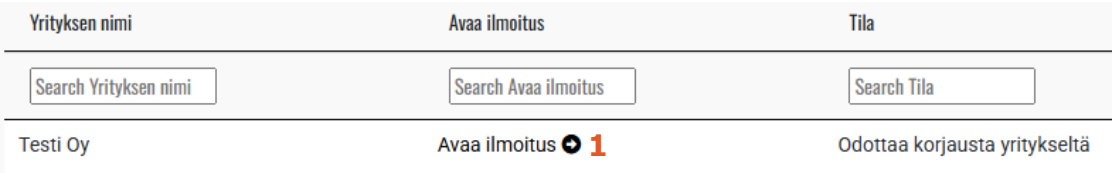
Käyttäjälle lähetetään sähköpostitse vahvistus, kun toimijan muuttuneet tiedot on onnistuneesti ilmoitettu Energiaviraston NIS2-toimijaluetteloon. Ilmoituksen tilaksi muuttuu tämän jälkeen ”Ilmoittautunut luetteloon”.



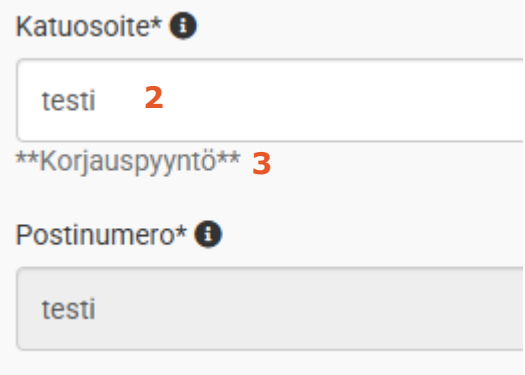
6.6 Energiavirasto pyytää ilmoitukseen korjausta

Jos Energiavirasto katsoo, että lähetetty ilmoitus edellyttää korjausta yritykseltä, Energiavirasto palauttaa ilmoituksen takaisin yritykselle ja avaa muutettavaksi korjattavat kohdat ilmoitukselta. Korjauspyynnöstä lähetetään aina automaattisesti sähköpostiviesti ilmoituksen tehneen käyttäjän sähköpostiosoitteeseen.

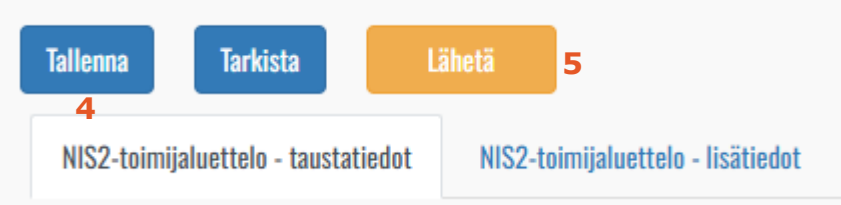
Aloita korjausta vaativien kohtien täydentäminen avaamalla toimijan ilmoitus ”Avaa ilmoitus”-painikkeella (1)



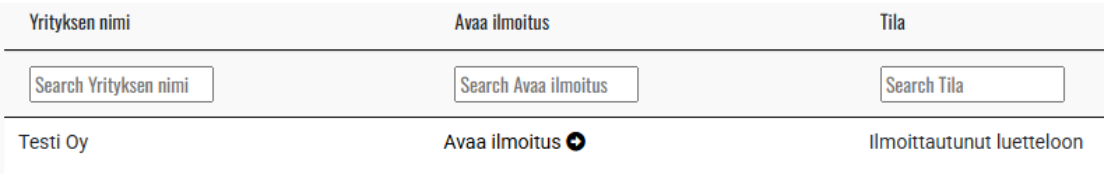
Korjausta vaativat kohdat löytyvät avaamalla ilmoituksen välilehdet. Korjausta vaativan kohdan tunnistaa, että se on avattu muokkausta varten (2) ja sen alla on **-merkeillä lisätty kommentti (3), miksi kohta vaatii korjausta. Alla olevassa kuvassa kohtaa postinumero ei ole avattu.



Käyttäjä tallentaa tiedot ”Tallenna”-painikkeella (4) ennen ilmoituksen lähettämistä. Kun käyttäjä on tehnyt tarvittavat muutokset, korjattu ilmoitus lähetetään ”Lähetä”-painikkeella (5).



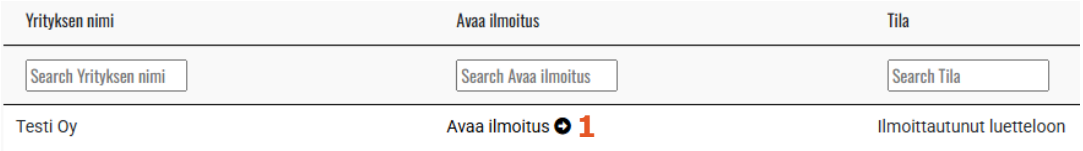
Käyttäjälle lähetetään sähköpostitse vahvistus, kun toimijan tiedot on onnistuneesti ilmoitettu Energiaviraston NIS2-toimijaluetteloon. Ilmoituksen tilaksi muuttuu tämän jälkeen ”Ilmoittautunut luetteloon”.



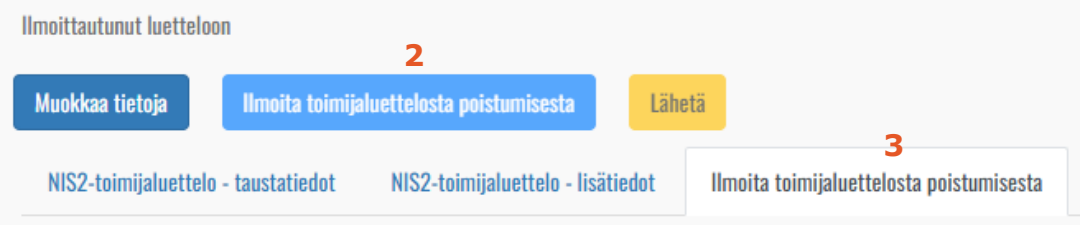
6.7 Ilmoita toimijaluettelosta poistumisesta

Jos toimija ei enää täytä kyberturvallisuuslain edellytyksiä ja se ei enää kuulu kyberturvallisuuslain piiriin, käyttäjä ilmoittaa toimijaluettelosta poistumisesta VERTTI-valvontatietojärjestelmässä.

Ilmoittaminen aloitetaan avaamalla toimijan ilmoitus ”Avaa ilmoitus”-painikkeella (1).

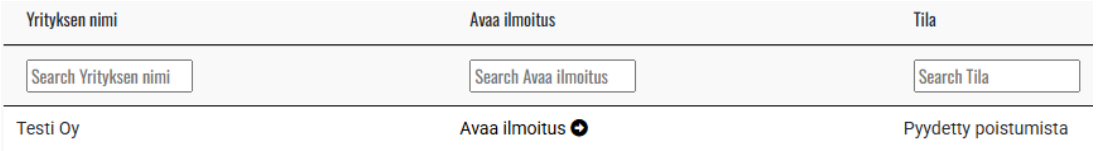


Kun käyttäjä on avannut ilmoituslomakkeen, käyttäjä tekee ilmoituksen valitsemalla ”Ilmoita toimijaluettelosta poistumisesta”-painikkeella (2). Ilmoitukselle avautuu uusi välilehti ”Ilmoita toimijaluettelosta poistumisesta” (3).



Käyttäjän on perusteltava, miksi toimija ei enää kuulu kyberturvallisuuslain piiriin. Kun perustelu on lisätty, käyttäjä voi lähettää ilmoituksen ”Lähetä”-painikkeella (4).

Kun ilmoitus toimijaluettelosta poistumisesta on lähetetty, ilmoituksen tilaksi muuttuu ”Pyydetty poistumista”



Käyttäjälle lähetetään sähköpostitse vahvistus, kun toimija on onnistuneesti poistunut toimijaluettelosta. Ilmoituslomake ei ole enää yrityksen nähtävillä VERTTI-valvontatietojärjestelmässä. Mikäli yrityksen tulee myöhemmin uudelleen ilmoittautua toimijaluetteloon, sen tulee tehdä uusi ilmoitus.

7 Lisätietoa ja linkkejä

Energiaviraston kotisivut kyberturvallisuudesta: www.energiavirasto.fi/kyberturvallisuus

Kyberturvallisuuskeskus on koonnut yleisen tietopaketin NIS2-direktiivistä: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi

Kyberturvallisuuskeskuksen ohjeet ja oppaat organisaatioille ja yrityksille: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille

Kyberturvallisuuskeskuksen kybermittari-työkalu: www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari

Kyberturvallisuuslaki (124/2025): https://finlex.fi/fi/lainsaadanto/saadoskokoelma/2025/124?language=fin&highlightId=591693&highlightParams=%7B%22type%22%3A%22BASIC%22%2C%22search%22%3A%22124%2F2025%22%7D

Komission suositus 2003/361/EY mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä: https://eur-lex.europa.eu/legal-content/FI/ALL/?uri=CELEX%3A32003H0361

Käyttöopas pk-yrityksen määritelmästä: https://publications.europa.eu/resource/cellar/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1.0007.01/DOC_1

NIS2-direktiivi: https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=fi

CER-direktiivi: https://eur-lex.europa.eu/eli/dir/2022/2557/oj?locale=fi