Hallituksen esitys eduskunnalle kyberturvallisuuslain muuttamiseksi

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan muutettavaksi kyberturvallisuuslakia (/).

Esityksellä saatettaisiin kyberturvallisuuslain soveltamisala koskemaan sellaisia yhteisöjä, jotka määritetään yhteiskunnan toiminnan kannalta kriittisiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ehdotetun lain nojalla. Esityksellä täydennettäisiin kriittisten toimijoiden häiriönsietokyvystä annetun Euroopan parlamentin ja neuvoston direktiivin sekä kyberturvallisuusdirektiivin kansallista täytäntöönpanoa.

Pääministeri Petteri Orpon hallituksen hallitusohjelman mukaan kyberturvallisuutta ja sitä koskevaa yhteistyötä viranomaisten ja elinkeinoelämän välillä vahvistetaan, hallitus parantaa tietoturvaa kriittisillä toimialoilla ja EU-lainsäädännön toimeenpanon yhteydessä vältetään kansallista lisäsääntelyä.

Laki on tarkoitettu tulemaan voimaan samanaikaisesti yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain kanssa.

SISÄLLYS

PERUSTELUT

1 Asian tausta ja valmistelu

1.1 Tausta

Tieto- ja viestintäteknologia sekä niihin liittyvät palvelut ovat keskeinen osa nykyaikaista yhteiskuntaa ja sen kriittistä infrastruktuuria. Kehittyneet tieto- ja viestintäteknologiset ratkaisut mahdollistavat uusia innovaatioita, toimintatapoja ja palveluita yhteiskunnassa. Samaan aikaan yhä useammat palvelut ja toiminnot ovat kasvavassa määrin riippuvaisia viestintäverkkojen ja tietojärjestelmien luotettavasta toiminnasta. Viestintäverkkojen ja tietojärjestelmien kyberturvallisuuteen kohdistuu monenlaisia riskejä, jotka toteutuessaan aiheuttavat häiriöitä ja haittoja erilaisten syy-yhteyksien seurauksena. Häiriön tai haitan toteutuminen voi olla seurausta tahattomasta vahingosta tai tahallisesta oikeudettomasta teosta, jonka taustalla olevat motiivit vaihtelevat.

Suomi on tietoyhteiskuntana riippuvainen viestintäverkkojen ja tietojärjestelmien toiminnasta ja näin ollen myös haavoittuvainen niihin kohdistuville häiriöille. Yhteiskunnan kokonaisturvallisuuden kannalta on tärkeää kasvattaa kyberturvallisuuden tasoa viestintäverkoissa ja tietojärjestelmissä. Kyberturvallisuuteen liittyvistä häiriöistä voi aiheutua merkittäviä taloudellisia seurauksia, niin yhteiskunnalle kuin yksityisille kansalaisille, yrityksille ja muille yhteisöille. Palveluiden toiminnan kannalta erityisen haitallisia voivat olla häiriöt, joiden seurauksena palvelut tai niissä säilytetyt tiedot, eivät olisi käyttäjiensä käytettävissä. Häiriön aiheuttama taloudellinen vahinko voi johtua esimerkiksi omaisuuden vahingoittumisesta, yrityksen liiketoiminnan keskeytymisestä tai kuluista, jotka syntyvät vahingoilta suojautumisesta. Yhteiskunnan toiminnan kannalta on tärkeää huolehtia kyberturvallisuudesta sellaisissa tietojärjestelmissä ja viestintäverkoissa, joiden avulla tuotetaan palveluita ja harjoitetaan toimintaa, joka on osa yhteiskunnan kriittistä infrastruktuuria.

Esityksen valmisteluun on johtanut kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta annettu Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2557, jäljempänä CER-direktiivi sekä Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi), jäljempänä NIS 2 -direktiivi.

CER-direktiivin kansallista täytäntöönpanoa koskee hallituksen esitys HE 205/2024 vp eduskunnalle laiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ja eräiksi muiksi laeiksi. Hallituksen esityksen käsittely eduskunnassa on kesken. CER-direktiivin täytäntöönpanemiseksi on ehdotettu säädettäväksi uusi laki yhteiskunnan toiminnan kannalta kriittisiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta. CER-direktiivin mukaiset kriittiset toimijat tunnistettaisiin lain nojalla Suomessa CER-direktiivin edellyttämän aikataulun mukaisesti kesään 2026 mennessä.

NIS 2 -direktiivi edellyttää, että CER-direktiivin nojalla kriittisiksi toimijoiksi määritettäviin toimijoihin sovelletaan niiden koosta riippumatta NIS 2 -direktiivin mukaisia velvoitteita kyberturvallisuudesta. Koska kyberturvallisuuslain soveltamisala on laaja, valtaosa kriittiseksi määritettävistä toimijoista kuuluisi ennalta myös kyberturvallisuutta koskevien velvoitteiden soveltamisalaan. Direktiivien täytäntöönpanoa olisi kuitenkin tarpeen täydentää siten, että kyberturvallisuutta koskevat velvoitteet soveltuisivat CER-direktiivin nojalla kriittisiksi toimijoiksi määritettäviin toimijoihin myös silloin, kun kriittinen toimija ei ennalta kuuluisi kyberturvallisuuslain soveltamisalaan.

Hallituksen esityksessä HE 205/2024 vp jaksossa 10 todetaan, että valtioneuvosto valmistelee erikseen esityksen teknisistä lainsäädäntömuutoksista, jotka ovat tarpeen ehdotetun kyberturvallisuuslain (HE 57/2024 vp) velvoitteiden soveltamiseksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain nojalla määritettäviin kriittisiin toimijoihin NIS2- ja CER-direktiivien edellyttämällä tavalla. Tässä esityksessä on kyse viitatuista lainsäädäntömuutoksista.

NIS 2 -direktiivi on pantu kansallisesti täytäntöön kyberturvallisuuslailla (/).

1.2 Valmistelu

Hallituksen esitys on valmisteltu virkatyönä liikenne- ja viestintäministeriössä yhteistyössä sisäministeriön kanssa.

NIS 2 -direktiivin ja sen kansallisen täytäntöönpanon valmistelu kuvataan hallituksen esityksen HE 57/2024 vp jaksossa 1.2.

CER-direktiivin ja sen kansallisen täytäntöönpanon valmistelu kuvataan hallituksen esityksen HE 205/2024 vp jaksossa 1.2.

2 EU-säädöksen tavoitteet ja pääasiallinen sisältö

Tässä jaksossa kuvataan direktiivien sisällöstä keskeisimmät kohdat, jotka liittyvät ehdotettaviin kyberturvallisuuslain muutoksiin. NIS 2 -direktiivin tavoitteet ja pääasiallinen sisältö on kuvattu muilta osin hallituksen esityksen HE 57/2024 vp jaksossa 2 sekä CER-direktiivin tavoitteet ja pääasiallinen sisältö hallituksen esityksen HE 205/2024 vp jaksossa 2.

NIS 2 -direktiivin soveltaminen CER-direktiivin nojalla määritettäviin toimijoihin

NIS 2 -direktiivissä säädetään toimenpiteistä, joilla pyritään saavuttamaan kyberturvallisuuden yhteinen korkea taso kaikkialla unionissa sisämarkkinoiden toiminnan parantamiseksi. CER-direktiivin tarkoituksena on sisämarkkinoiden toiminnan takaaminen kriittisten palvelujen osalta direktiivin soveltamisalalla ja parantaa Euroopan unionin kannalta välttämättömien palvelujen häiriönsietokykyä sekä ylläpitää yhteiskunnan elintärkeitä ja taloudellisia toimintoja määrittäen tietyt kriittiset sektorit, jotka tarjoavat tällaisia palveluja. NIS2-direktiivin tavoitteena on vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa yhteiskunnan toiminnan kannalta keskeisten ja tärkeiden toimialojen ja toimijatyyppien osalta. CER-direktiivin tavoitteena on parantaa kriittisten toimijoiden häiriönsietokykyä sisämarkkinoilla.

NIS 2 -direktiivin yleinen soveltamisala määritellään sen 2 artiklassa. NIS 2 -direktiivin raportointi- ja riskienhallintavelvoitteet kohdistuvat sen 3 artiklassa määriteltäviin keskeisiin ja tärkeisiin toimijoihin.

NIS 2 -direktiivin 2 artiklan 3 kohdan nojalla direktiiviä sovelletaan CER-direktiivin nojalla kriittisiksi toimijoiksi määritettyihin toimijoihin niiden koosta riippumatta. CER-direktiivillä asetetaan kriittisille toimijoille muuhun kuin kyberturvallisuuteen liittyviä velvoitteita riskienhallinnasta ja poikkeamien raportoinnista. Kyberturvallisuutta koskevilta osin kriittisiin toimijoihin olisi sovellettava NIS 2 -direktiivin mukaisia velvoitteita riskienhallinnasta ja poikkeamien raportoinnista.

CER-direktiivin 6 artiklassa säädetään kriittisten toimijoiden määrittämisestä. Jäsenvaltion on määritettävä viimeistään 17.7.2026 kriittiset toimijat CER-direktiivin liitteessä tarkoitetuilla

toimialoilla ja alasektoreilla. Artiklan 2 kohdassa säädetään määrittämisessä huomioon otettavista perusteista. Artiklan 3 kohdassa säädetään jäsenvaltion velvoitteista laatia luettelo kriittisistä toimijoista ja sen varmistamisesta, että asianomaiselle taholle ilmoitetaan, että se on määritetty kriittiseksi toimijaksi. Jäsenvaltion myös ilmoitettava kriittiseksi toimijaksi määritetylle sen velvoitteista. Artiklan 4 kohdassa säädetään siitä, että jäsenvaltioiden on varmistettava, että niiden CER-direktiivin mukaiset toimivaltaiset viranomaiset ilmoittavat NIS 2 -direktiivin mukaisille toimivaltaisille viranomaisille jäsenvaltioiden tämän artiklan mukaisesti määrittämät kriittiset toimijat yhden kuukauden kuluessa niiden määrittämisestä. Kohdan 5 mukaan jäsenvaltioiden on tarvittaessa ja vähintään 4 vuoden välein päivitettävä kriittisten toimijoiden luettelo. Komissio laatii yhteistyössä jäsenvaltioiden kanssa suosituksia ja ei-sitovia ohjeita jäsenvaltioiden tueksi kriittisten toimijoiden määrittämisessä.

Keskeinen toimija

NIS 2 -direktiivin 3 artiklan 1 kohdan f-alakohdan nojalla direktiiviä sovellettaessa CER-direktiivin nojalla kriittisiksi toimijoiksi määritettyjä toimijoita on pidettävä NIS 2 -direktiiviä sovellettaessa keskeisinä toimijoina.

Keskeisten ja tärkeiden toimijoiden erottelu on merkityksellistä NIS 2 –direktiivissä valvonnasta ja hallinnollisista seuraamuksista säädetyn kannalta. Keskeisten toimijoiden osalta valvonnan tulee kattaa etukäteis- ja jälkikäteisvalvonta, mutta tärkeiden toimijoiden osalta pelkkä jälkikäteisvalvonta on direktiivin nojalla riittävää. Lisäksi direktiivi edellyttää keskeisiin toimijoihin kohdistuvia eräitä valvontatoimivaltuuksia, joita tärkeiden toimijoiden osalta ei edellytetä. Lisäksi direktiivi asettaa keskeisiin toimijoihin kohdistuvan seuraamusmaksun alimman sallitun enimmäismäärän korkeammalle tasolle kuin tärkeiden toimijoiden osalla. Edellä todetusti NIS 2 -direktiivi edellyttää, että kriittisiä toimijoita olisi pidettävä keskeisinä toimijoina. Keskeisiin toimijoihin kohdistettavista valvontatoimenpiteistä säädetään NIS 2 -direktiivin 32 artiklassa ja hallinnollisten seuraamusmaksujen tasosta 34 artiklassa.

Poikkeamailmoitukset

NIS 2 -direktiivin 23 artiklassa säädetään toimijan velvollisuudesta ilmoittaa merkittävästä poikkeamasta toimivaltaiselle viranomaiselle ja tietoturvaloukkauksiin reagoivalle ja niitä tutkivalle NIS 2 -direktiivin mukaiselle CSIRT-yksikölle. NIS 2 -direktiivin 30 artiklassa säädetään muusta ilmoittamisesta kuin siitä, johon toimijat ovat velvoitettuja.

NIS 2 -direktiivin 23 artiklan 10 kohdan mukaan CSIRT-yksiköiden tai tapauksen mukaan toimivaltaisten viranomaisten on toimitettava direktiivin (EU) 2022/2557 mukaisille toimivaltaisille viranomaisille tietoa merkittävistä poikkeamista, poikkeamista, kyberuhkista ja läheltä piti -tilanteista, joista direktiivin (EU) 2022/2557 nojalla kriittisiksi toimijoiksi määritetyt toimijat ovat ilmoittaneet NIS 2 -direktiivin 1 kohdan ja 30 artiklan mukaisesti.

Valvovien viranomaisten yhteistyö

NIS 2 -direktiivin 13 artiklassa säädetään kansallisen tason viranomaisyhteistyöstä NIS 2 -direktiivin valvonnassa. Artiklan 4 ja 5 kohdissa säädetään NIS 2 -direktiiviä ja CER-direktiiviä valvovien viranomaisten yhteistyöstä. Artiklan 4 kohdassa edellytetään, että jäsenvaltiot edistävät muun ohella viranomaistyötä lainvalvontaviranomaisten, tietosuojaviranomaisten, siviiliilmailuviranomaisen, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY 274 kumoamisesta annetun Euroopan parlamentin ja neuvoston asetusta (EU) N:o 910/2014 (eIDAS-asetus) valvovan viranomaisen ja finanssialan digitaalisesta häiriönsietokyvystä ja asetusten (EY) N:o 1060/2009, (EU) N:o

648/2012, (EU) N:o 600/2014, (EU) N:o 909/2014 ja (EU) 2016/1011 muuttamisesta annetun Euroopan parlamentin ja neuvoston asetusta (jäljempänä DORA-asetus) valvovan viranomaisen kanssa. Artiklan 5 kohdan nojalla jäsenvaltioiden on varmistettava, että NIS 2 -direktiiviä valvovat viranomaiset ja CER-direktiiviä valvovat viranomaiset tekevät yhteistyötä ja vaihtavat säännöllisesti tietoja kriittisten toimijoiden määrittämisestä sekä riskeistä, kyberuhkista ja poikkeamista ja muista kuin kyberturvallisuuteen liittyvistä riskeistä, uhkista ja poikkeamista, jotka vaikuttavat kriittisiin toimijoihin, sekä tällaisten riskien, uhkien ja poikkeamien hallitsemiseksi toteutetuista toimenpiteistä.

NIS 2 -direktiivin 32 artiklassa säädetään keskeisten toimijoiden valvonnasta. Artiklan 9 kohta edellyttää, että NIS 2 -direktiiviä valvovien viranomaisten on ilmoitettava CER-direktiiviä valvoville saman jäsenvaltion asiaankuuluville viranomaisille, kun ne käyttävät valvonta- ja täytäntöönpanovaltuuksiaan varmistaakseen, että CER-direktiivin nojalla kriittiseksi toimijaksi määritetty toimija noudattaa NIS 2 –direktiiviä. Lisäksi kohdan nojalla CER-direktiivin mukaiset valvovat viranomaiset voivat tarvittaessa pyytää tämän NIS 2 -direktiivin mukaisia valvovia viranomaisia käyttämään valvonta- ja täytäntöönpanovaltuuksiaan suhteessa kriittiseen toimijaan.

Kansallinen liikkumavara

NIS 2 – ja CER-direktiivit ovat luonteeltaan vähimmäisharmonisoivia. Direktiivit eivät estä pitämästä voimassa kansallisia säännöksiä, joilla varmistetaan korkeampi kyberturvallisuuden tai kriittisten toimijoiden häiriönsietokyvyn taso edellyttäen, että tällaiset säännökset ovat yhdenmukaisia unionin oikeuden mukaisten jäsenvaltioiden velvollisuuksien kanssa.

NIS 2 – ja CER-direktiivit eivät sisällä kansallista liikkumavaraa, joka koskisi NIS 2 -direktiivin mukaisten kyberturvallisuuden riskienhallintaa ja merkittävien poikkeamien ilmoittamista koskevien velvoitteiden soveltamista CER-direktiivin mukaisesti kriittisiksi tunnistettuihin toimijoihin tai näiden toimijoiden pitämistä NIS 2 -direktiivissä tarkoitettuina keskeisinä toimijoina. Esityksen kannalta keskeinen kansallinen liikkumavara liittyy siihen, kuinka sääntelyn valvonta ja siihen liittyvät viranomaistehtävät Suomessa järjestetään.

Muilta osin kansallinen liikkumavara kuvataan NIS 2 -direktiivin osalta hallituksen esityksen HE 57/2024 vp jaksossa 2 sekä CER-direktiivin osalta hallituksen esityksen HE 205/2024 vp jaksossa 2.

3 Nykytila ja sen arviointi

Suomessa ei ole määritetty CER-direktiivin nojalla kriittisiä toimijoita. Kriittiset toimijat olisi määritettävä CER-direktiivin mukaisesti ensimmäistä kertaa heinäkuuhun 2026 mennessä. Kriittisten toimijoiden määrittäminen tapahtuisi ehdotetun CER-täytäntöönpanolain eli yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain nojalla. Lakia koskeva hallituksen esitys HE 205/2024 vp on eduskunnan käsiteltävänä.

NIS 2 -direktiivi on pantu täytäntöön uudella kyberturvallisuuslailla (/) ja julkishallintoa koskevilta osin julkisen hallinnon tiedonhallinnasta annetulla lailla (/). Kyberturvallisuuslaki on tullut voimaan (…). Kyberturvallisuuslaissa säädetään NIS 2 -direktiivin mukaisista velvoitteista muille kuin julkishallinnon toimijoille. Kyberturvallisuuslain soveltamisala kattaa lähes kaikki toimialat, joilta kriittisiä toimijoita CER-direktiivin soveltamisalan mukaisesti tunnistetaan.

CER-direktiivin nojalla voidaan määrittää seuraavia toimijoita kriittisiksi, vaikka ne eivät kuulu nykyisin kyberturvallisuuslain soveltamisalaa määrittäviin liitteisiin I tai II:

- Tieliikenne, julkinen liikenne (Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 1370/2007 (13) 2 artiklan d alakohdassa määritellyt julkisen liikenteen harjoittajat)

- Terveys, tukkukaupan harjoittamista koskevan luvan haltijat (Direktiivin 2001/83/EY 79 artiklassa tarkoitetun tukkukaupan harjoittamista koskevan luvan haltijat)

CER-direktiivin nojalla voidaan määrittää kriittisiksi toimijoiksi myös toimijoita, jotka alittavat kyberturvallisuuslain soveltamisalaa koskevan keskisuuren yrityksen kokokynnyksen, eli ovat kooltaan pien- tai mikroyrityksiä.

Kyberturvallisuuslaissa ja yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetussa laissa valvovan viranomaisen tehtäviä on hajautettu sektorikohtaisesti pääosin samoille viranomaisille. Näin ollen CER- ja NIS 2 -direktiivin mukaisia velvoitteita valvoisivat pääosin samat viranomaiset eri toimialoilla. Koska valvovia viranomaisia on kuitenkin useita ja poikkeuksellisesti olisi mahdollista, että velvoitteita eivät kaikissa tapauksissa valvoisi samat viranomaiset samoille toimijoille, olisi tarpeen säätää NIS 2 – ja CER-direktiivien edellyttämällä tavalla valvovien viranomaisten yhteistyöstä ja tiedonvaihdosta.

Koska CER-direktiivi ja NIS 2 -direktiivi edellyttävät, että kriittisiksi määritettäviin toimijoihin sovelletaan NIS 2 -direktiivin mukaisia velvoitteita, direktiivien täytäntöönpanon täydentämiseksi olisi tarpeen esittää lainsäädäntömuutoksia, joilla kyberturvallisuuslain mukaisia velvoitteita sovellettaisiin CER-direktiivin mukaisesti määritettyihin kriittisiin toimijoihin myös silloin, kun toimija ei muutoin kuuluisi kyberturvallisuuslain soveltamisalaan, eli olisi kooltaan pien- tai mikroyritys taikka julkista liikennettä tai lääketukkukauppaa harjoittava toimija. Lisäksi täytäntöönpanon täydentämiseksi olisi tarpeen esittää lainsäädäntömuutoksia, joilla CER-direktiivin mukaisesti määritettyä kriittistä toimijaa pidettäisiin keskeisenä toimijana myös silloin, kun toimija ei muutoin täyttäisi kyberturvallisuuslain keskeisen toimijan määritelmää. Lisäksi kyberturvallisuuslakiin olisi tarpeen tehdä muutoksia liittyen valvonnan yhteensovittamiseen ja viranomaisyhteistyöhän direktiivien edellyttämällä tavalla.

4 Ehdotukset ja niiden vaikutukset

4.1 Keskeiset ehdotukset

Esityksen tavoitteena on täydentää NIS 2 -direktiivin ja CER-direktiivin kansallista täytäntöönpanoa kyberturvallisuutta koskevien velvoitteiden soveltumisesta kriittiseen toimijaan. Esityksen tavoitteena on toteuttaa lainsäädäntömuutokset, jotka ovat tarpeen kyberturvallisuuslain mukaisten velvoitteiden soveltamiseksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain nojalla määritettäviin kriittisiin toimijoihin.

Esityksessä keskeinen ehdotus on, että kyberturvallisuuslakia täydennettäisiin siten, että sen mukaisia velvoitteita kyberturvallisuutta koskevasta riskienhallinnasta ja merkittävistä poikkeamista ilmoittamisesta sovellettaisiin myös yhteisöihin, jotka määritettäisiin kriittisiksi toimijoiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain nojalla. Kriittiseksi määritetty toimija olisi kyberturvallisuuslaissa tarkoitettu keskeinen toimija. Lisäksi esitykseen sisältyy lainsäädäntöteknisiä ehdotuksia muun muassa valvovien viranomaisten toimivallasta ja yhteistyöstä sekä siirtymäajasta velvoitteiden soveltumiselle kriittiseksi määrittämisen jälkeen.

Ehdotukset vastaisivat vähimmäistasoa siitä, mitä NIS 2 -direktiivi ja CER-direktiivi edellyttävät kyberturvallisuutta koskevien velvoitteiden ja niiden valvonnan tasosta kriittisille toimijoille.

4.2 Pääasialliset vaikutukset

Viranomaisvaikutukset

Yrityksen tai yhteisön määrittäminen kriittiseksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain nojalla voi lisätä kyberturvallisuuslain soveltamisalaan kuuluvien toimijoiden määrää sekä erityisesti ennakkovalvonnan piiriin kuuluvien keskeisten toimijoiden määrää. Esityksellä olisi näin ollen vähäinen lisäävä vaikutus kyberturvallisuuslakia valvovien viranomaisten tehtävämäärään sekä CSIRT-yksikön tehtävämäärään, mikä aiheutuu uutena lain soveltamisalaan tulevista toimijoista sekä sellaisten toimijoiden pitämisestä keskeisinä toimijoina, jotka eivät keskeisen toimijan kynnystä muutoin täyttäisi. Viranomaiselle aiheutuvien ennakoitavan tehtävämäärän lisäys suhteessa kyberturvallisuuslaissa nykyisiin tehtäviin riippuu siitä, missä laajuudessa kriittisiksi toimijoiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain nojalla yrityksiä tai yhteisöjä tulevaisuudessa määritetään kriittisiksi toimijoiksi. Tehtävämäärän lisäys arvioidaan vähäiseksi ottaen huomioon kyberturvallisuuslain soveltamisalaan ennalta kuuluvien toimijoiden määrä.

Yritysvaikutukset

Esityksellä ei ole välittömiä taloudellisia vaikutuksia muille yrityksille tai yhteisöille kuin niille, jotka määritetään tulevaisuudessa kriittisiksi toimijoiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain nojalla.

Esityksestä aiheutuvat vaikutukset yrityksille ja yhteisöille, jotka määritetään tulevaisuudessa kriittisiksi toimijoiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain nojalla, riippuvat merkittävästi siitä, onko yritys tai yhteisö kuulunut ennalta kyberturvallisuuslain velvoitteiden soveltamisalaan. Lisäksi vaikutukset riippuvat merkittävästi siitä, millä tavalla ja missä laajuudessa yritys tai yhteisö on ennalta toteuttanut kyberturvallisuutta koskevaa riskienhallintaa ja missä määrin sen toiminnassa käytetään viestintäverkkoja ja tietojärjestelmiä.

Jos yritys tai yhteisö kuuluu ennen kriittiseksi määrittämistä kyberturvallisuuslain soveltamisalaan ja on lain 27 §:n 2 momentissa tarkoitettu keskeinen toimija, esityksestä ei aiheudu välittömiä taloudellisia vaikutuksia yritykselle tai yhteisölle.

Jos yritys tai yhteisö kuuluu ennen kriittiseksi määrittämistä kyberturvallisuuslain soveltamisalaan mutta ei ole lain 27 §:n 2 momentissa tarkoitettu keskeinen toimija, esityksestä aiheutuu vähäisiä taloudellisia vaikutuksia yritykselle tai yhteisölle. Yritystä pidettäisiin kriittiseksi toimijaksi määrittämisen jälkeen keskeisenä toimijana.

Niille yrityksille ja yhteisöille, jotka tulevat kriittiseksi määrittämisen johdosta uusina organisaatioina kyberturvallisuuslain soveltamisalaan, esityksellä olisi taloudellisia vaikutuksia. Taloudellisten vaikutusten määrä riippuu merkittävästi merkittävästi siitä, onko yritys tai yhteisö kuulunut ennalta kyberturvallisuuslain velvoitteiden soveltamisalaan. Lisäksi vaikutukset riippuvat merkittävästi siitä, millä tavalla ja missä laajuudessa yritys tai yhteisö on ennalta toteuttanut kyberturvallisuutta koskevaa riskienhallintaa ja missä määrin sen toiminnassa käytetään viestintäverkkoja ja tietojärjestelmiä.

Uusina organisaatioina kyberturvallisuuslain soveltamisalaan voisi tulla kriittiseksi määritetty yritys tai yhteisö, joka on kooltaan pien- tai mikroyritys, taikka harjoittaa sellaista toimintaa, joka ei kuulu NIS 2 -direktiivin liitteisiin, mutta kuuluu CER-direktiivin liitteisiin. Pien- tai mikroyrityksiä ovat komission suosituksen 2003/361/EY liitteen 2 artiklan nojalla yritykset, joiden palveluksessa on vähemmän kuin 50 työntekijää ja jonka vuosiliikevaihto tai taseen loppusumma on enintään 10 miljoonaa euroa. CER-direktiivin liitteisiin kuuluvat toimialat, jotka eivät kuulu NIS 2 -direktiivin liitteisiin, ovat julkinen liikenne ja lääketukkukaupat.

Koska kyberturvallisuuslain soveltamisalaan kuuluvat ennalta laajasti keskisuuret ja suuremmat yritykset, jotka harjoittavat CER-direktiivin liitteissä tarkoitettua toimintaa, arvioidaan niiden yritysten tai yhteisöiden joukon, joille esityksestä olisi vähäistä suurempia taloudellisia vaikutuksia, jäävän rajalliseksi.

Esityksen vaikutukset riippuvat merkittävästi siitä, missä laajuudessa yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain nojalla määritetään kriittisiä toimijoita ja erityisesti pien- tai mikroyrityksiä taikka julkista liikennettä tai lääketukkukauppaa harjoittavia toimijoita. Lisäksi vaikutukset riippuvat merkittävästi siitä, miten kriittiset toimijat ovat ennalta toteuttaneet kyberturvallisuutta koskevaa riskienhallintaa.

Esityksestä aiheutuu taloudellisia kustannuksia yrityksille erityisesti silloin, jos ne joutuvat lainsäädännön vaatimusten vuoksi panostamaan tietoverkkojensa tietoturvaan uudella tavoin. Kustannusten suuruus riippuu yrityksen tietojärjestelmien tietoturvan lähtötasosta. Kustannuksien suuruus riippuu myös riskienhallintatoimenpiteiden laadusta ja laajuudesta siten kuin ne arvioidaan ennakoitavissa oleviin riskeihin ja toiminnan laatuun nähden oikeasuhtaisiksi. Kustannuksia aiheutuu esimerkiksi investoinneista, joilla tietoturvan tasoa nostetaan sekä esimerkiksi auditoinneista, joilla tietoturvan taso todennetaan. Merkittävimmin taloudellisia vaikutuksia kriittiseksi määrittämisestä kohdistuisi pien- ja mikroyrityksiin, jotka jäisivät muutoin kokonsa vuoksi kyberturvallisuuslain soveltamisalan ulkopuolelle. Riskienhallinnan toteuttamisesta ja poikkeamien käsittelemisestä NIS 2 -direktiivin edellyttämän vähimmäistason mukaisesti voi aiheutua kriittiseksi määritetylle pien- tai mikroyritykselle liikevaihtoon ja henkilöstömäärään nähden olennaisia kustannuksia.

Esityksestä aiheutuvien kustannuksien määrään vaikuttavat yrityksessä ennalta toteutetun kyberturvallisuuden riskienhallinnan taso, toiminnan laatu ja laajuus sekä toiminnassa käytettävien viestintäverkkojen ja tietojärjestelmien määrä ja laatu. Riskienhallinnan kustannukset ovat sitä suurempia, mitä suurempaa ja laajempaa yrityksen toiminta on. Yrityskohtaiset erot IT- ja kyberturvallisuuskustannuksissa ovat merkittäviä ja olennaisessa suhteessa yrityksen toimintaan. Yleisesti IT-kustannukset ovat keskimäärin noin 4−5 % yrityksen liikevaihdosta. Vaihteluväli on toimijan koosta, kybermaturiteetista ja sektorista riippuen 1,5−5%. Yksin kyberturvallisuuteen tai –riskienhallintaan liittyviä kustannuksia on haastavaa erottaa yrityksen muista IT- tai riskienhallintakustannuksista. Kyberturvallisuuslain soveltamisalassa olevalle yritykselle voidaan suuntaa-antaen arvioida aiheutuvan kustannuksia kyberturvallisuuden riskienhallinnasta lain edellyttämällä vähimmäistasolla noin 0,2 – 0,8 % vuotuisesta liikevaihdosta, jos vertailukohtana on tilanne, jossa yritys ei toteuttaisi ennalta lainkaan kyberturvallisuuden riskienhallintatoimenpiteitä. Arvioihin liittyy merkittävää epävarmuutta yrityskohtaisten erojen osalta.

Tarvittavat taloudelliset panostukset yksittäisten kriittisten yritysten järjestelmien tietoturvaan ovat kuitenkin nykyinen turvallisuustilanne huomioon ottaen erittäin perusteltuja ja tarpeen yhteiskunnan näkökulmasta. Ne toimivat myös yritysten itsensä hyödyksi, koska ne lisäävät yrityksen asiakkaiden luottamusta yrityksen palveluihin. Kyberturvallisuuden tason parantamisella on positiivisia vaikutuksia sekä yritysten liiketoimintaedellytyksille, että kansantaloudelle ja yhteiskunnan kriisinkestävyydelle.

Vaikutukset tietoyhteiskuntaan ja turvallisuuteen

Esityksellä olisi myönteisiä vaikutuksia tietoyhteiskunnan kehitykseen, sillä se edistäisi tietoturvallisten palvelujen ja käytänteiden käyttöönottoa ja siten loisi kysyntää tällaisille palveluille sekä kyberturvallisuuden ammattilaisille. Kyberturvallisuustason parantuminen vähentäisi palvelujen käytössä esiintyviä häiriöitä ja edistäisi yleistä luottamusta digitaalisiin palveluihin.

Esityksellä arvioidaan olevan yhteiskunnan häiriöttömän toiminnan edistämisen kautta myönteisiä vaikutuksia kansalaisten turvallisuudelle. Esitys edistää yhteiskunnan toiminnan kannalta kriittisten toimijoiden kykyä sietää kyberhäiriöitä, millä parannetaan kansalaisten turvallisuutta erityisesti silloin, kun toimialassa tai palvelussa kyse on kansalaisten turvallisuuteen vaikuttavista, yhteiskunnan toiminnan kannalta kriittiseen infrastruktuurin liittyvistä toiminnoista. Esityksellä vahvistettaisiin myös yhteiskunnan yleistä kriisinkestävyyttä ja kansallista turvallisuutta tältä osin. Lisäksi näkyvien kyberhäiriöiden yleistyminen olisi omiaan vaikuttamaan kansalaisten kokemukseen turvallisuudesta yhteiskunnassa, minkä ehkäiseminen kriittisten toimijoiden osalta on esityksen tavoite.

5 Muut toteuttamisvaihtoehdot

NIS 2 -direktiivin mukaisten velvoitteiden vähimmäistason soveltamiseen CER-direktiivin nojalla kriittiseksi määriteltäviin toimijoihin ei liity kansallista liikkumavaraa.

Esitetyille muutoksille lainsäädäntöteknisenä vaihtoehtona olisi, että NIS 2 -direktiivin mukaisista velvoitteista kriittisille toimijoille säädettäisiin kyberturvallisuuslain sijasta yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetussa laissa. Sellaiselle yhteisölle, joka ei kuuluisi ennalta kyberturvallisuuslain soveltamisalaan, mutta määritettäisiin kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain nojalla kriittiseksi toimijaksi vaihtoehto voisi selkeyttää sääntelyä, sillä tällöin yhteisölle kriittiseksi määrittämisestä aiheutuvat velvoitteet olisivat keskitetysti mainitussa laissa. Esityksen valmistelussa on kuitenkin arvioitu, että valtaosa kriittisiksi toimijoiksi määritettävistä toimijoista tulisi olemaan ennen kriittiseksi määrittämistä myös kyberturvallisuuslain soveltamisalassa, koska kyberturvallisuuslain soveltamisala on laaja ja soveltamisaloja määrittävät CER- ja NIS 2 -direktiivien liitteet lähes vastaavat toisiaan. Tämän vuoksi, sekä direktiivien keskinäinen yhteys muutoinkin huomioon ottaen, olisi tärkeää valita lainsäädäntöteknisesti se lähestymistapa, joka parhaiten varmistaa, että kyberturvallisuuslain ja kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain sääntelyn välinen suhde on selkeä ja velvoitteet ovat sovellettavissa toisiaan täydentäen yhteisöissä, jotka kuuluvat molempien säädösten soveltamisalaan. Sääntelykokonaisuuden kannalta selkeimmäksi ja päällekkäistä sääntelyä parhaiten välttäväksi vaihtoehdoksi on arvioitu esitetty kyberturvallisuuslain täydentäminen siten, että lakia sovellettaisiin kriittiseksi määritettyihin toimijoihin myös silloin, kun toimija ei muutoin kuuluisi lain soveltamisalaan, mutta olisi määritetty kriittiseksi kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain nojalla.

6 Lausuntopalaute

Hallituksen esitys on ollut lausuttavana x.x. – x.x.2025.

Lausuntoaika on ollut tavanomaista lyhyempi NIS 2 – ja CER-direktiivien täytäntöönpanon täydentämisen kiireellisyyden vuoksi. Määräaika direktiivien täytäntöönpanoa koskevan kansallisen sääntelyn hyväksymiseksi on ollut 17.10.2024. Lisäksi ehdotetut säädösmuutokset ovat olleet keskeisiltä osin lausuttavana NIS 2 -direktiivin täytäntöönpanoa koskevan hallituksen

esityksen luonnoksessa (lausuntopyyntö VN/18157/2023, aineisto Lausuntopalvelussa: www.lausuntopalvelu.fi).

Hallituksen esityksestä annettiin yhteensä x lausuntoa.

[Täydennetään lausuntokierroksen jälkeen…]

Hallituksen esityksen valmistelussa on hyödynnetty myös NIS 2 -direktiivin ja CER-direktiivin kansallisesta täytäntöönpanosta HE 57/2024 vp ja HE 205/2024 vp valmistelun yhteydessä annettuja lausuntoja.

7 Säännöskohtaiset perustelut

3 §. *Toimijat.* Pykälän *2 momentin* listaan toimijoista, joihin lakia sovelletaan niiden koosta riippumatta, ehdotetaan lisättäväksi uusi 5 kohta. Uudessa 5 kohdassa tarkoitettaisiin CER-direktiivin mukaisesti määritettyjä kriittisiä toimijoita eli yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain 10 §:ssä tarkoitettuja kriittisiä toimijoita. Kriittiset toimijat olisivat kyberturvallisuuslaissa tarkoitettuja toimijoita riippumatta niiden koosta tai harjoitettavan toiminnan laadusta. Ratkaisevaa määritelmän täyttymisen kannalta olisi, että toimija olisi määritetty kriittiseksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain nojalla. Lisäyksen johdosta kyberturvallisuuslain velvoitteet koskisivat yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain 10 §:ssä tarkoitettuja kriittisiä toimijoita myös silloin, kun toimija ei täyttäisi 1 momentin nojalla toimijan määritelmää. Momenttia ei muutettaisi muilta osin.

Yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain mukaisia kriittisiä toimijoita ei ole määritetty. Mainitun lakiehdotuksen 30 §:ään sisältyvän siirtymäsäännöksen nojalla päätös kriittisen toimijan määrittämisestä tehtäisiin ensimmäisen kerran 17.7.2026.

Lisäyksellä pantaisiin täytäntöön NIS 2 –direktiivin 2 artiklan 3 kohta.

4 §. *Soveltamisalan rajaukset.* Pykälän *6 momentissa* säädetään kuntaan kohdistuvasta kyberturvallisuuslain soveltamisalan rajauksesta. Momenttia ehdotetaan muutettavaksi siten, että kuntaan sovellettaisiin kyberturvallisuuslakia myös silloin, jos kunta tai osa sen toiminnasta olisi määritetty kriittiseksi toimijaksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain nojalla. Lisäys olisi lainsäädäntötekninen ja tarpeen kyberturvallisuuslain soveltamiseksi silloin, jos kriittiseksi toimijaksi määritetään kunnassa muuta kuin kyberturvallisuuslain liitteissä tarkoitettua toimintaa tai kunta kokonaisuudessaan.

Lisäys olisi tarpeen NIS 2 –direktiivin 2 artiklan 3 kohdan täytäntöönpanemiseksi näissä tilanteissa.

17 §. *Poikkeamailmoitusten käsittely.* Pykälään ehdotetaan lisättäväksi uusi *6 momentti*, jonka nojalla valvovan valvovan viranomaisen tulisi toimittaa yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annettua lakia valvovalle viranomaiselle tieto kyberturvallisuuslaissa tarkoitetuista merkittävistä poikkeamista, kyberuhkista ja läheltä piti –tilanteista, joista yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain nojalla määritetyt kriittiset toimijat ovat sille ilmoittaneet kyberturvallisuuslain 11–13 tai 15 §:n nojalla. Lisäys olisi lainsäädäntötekninen ja tulisi

sovellettavaksi vain, jos kriittistä toimijaa valvova viranomainen olisi eri kyberturvallisuuslain ja yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain osalta.

Lisäyksellä pantaisiin täytäntöön NIS 2 –direktiivin 23 artiklan 10 kohta.

Poikkeaman ja kyberuhkan määritelmästä säädettäisiin kyberturvallisuuslain 2 §:ssä. Läheltä piti –tilanteella tarkoitettaisiin NIS 2 -direktiivin 6 artiklan 5 kohdan määritelmää vastaavasti tapahtumaa, joka olisi voinut vaarantaa viestintäverkoissa ja tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden mutta jonka toteutuminen onnistuttiin estämään tai joka ei toteutunut satunnaisen syyn vuoksi.

26 §. *Valvovat viranomaiset.* Pykälään ehdotetaan lisättäväksi uusi *3 momentti*, jossa säädettäisiin kyberturvallisuuslaissa tarkoitetusta valvovasta viranomaisesta silloin, jos kriittiseksi määritetty toimija ei harjoittaisi kyberturvallisuuslain liitteessä I tai II tarkoitettua toimintaa. Ehdotetun 3 §:n 2 momentin 5 kohdan nojalla velvoitteiden soveltamisalaan kuuluva toimijassa voisi poikkeustapauksessa olla kyse myös muusta kuin kyberturvallisuuslain liitteessä I tai II tarkoitettua toimintaa harjoittavasta toimijasta, koska CER- ja NIS 2 –direktiivien soveltamisalaa koskevat liitteet eivät kaikilta osin ole vastaavia.

Pääsääntönä olisi, että myös kriittisten toimijoiden osalta kyberturvallisuuslakia valvova viranomainen määräytyisi pykälän 1 momentin mukaisesti. Jos toimija ei kuitenkaan harjoittaisi liitteissä I tai II tarkoitettua toimijaa ja sen valvova viranomainen ei siten voisi määräytyä 1 momentin nojalla, kyberturvallisuuslakia valvoisi sama viranomainen, joka olisi toimivaltainen valvomaan toimijaa yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetussa laissa säädettyjen velvoitteiden osalta. Valvovista viranomaisista säädettäisiin lain 19 §:ssä. Lisäys olisi tarpeen 3 §:n 2 momenttiin ehdotetun lisäyksen vuoksi.

27 §. *Valvonnan kohdistaminen.* Pykälän *2 momenttiin* ehdotetaan lisättäväksi uusi 5 kohta, jonka nojalla myös yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain mukaisesti tunnistetut kriittiset toimijat olisivat kyberturvallisuuslaissa ja NIS 2 -direktiivissä tarkoitettuja keskeisiä toimijoita. Momenttia ei tarkoitettaisi muutettavaksi muilta osin.

Lisäyksellä pantaisiin täytäntöön NIS 2 –direktiivin 3 artiklan 1 kohdan f alakohta.

28 §. *Valvovan viranomaisen tiedonsaantioikeus.* Pykälän *4 momenttia* ehdotetaan muutettavaksi siten, että momenttiin lisättäisiin yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetussa laissa tarkoitetut valvovat viranomaiset viranomaisiksi, joille kyberturvallisuuslain mukaisella valvovalla viranomaisella olisi oikeus luovuttaa tietoja momentissa säädettyjen edellytysten täyttyessä. Edellytyksenä tietojen luovuttamiselle olisi, että luovuttaminen on välttämätöntä kyberturvallisuuslaissa tai yhteiskunnan kriittisen infrastruktuurin suojaamisesta annetussa laissa viranomaiselle säädetyn tehtävän suorittamista varten. Tietojen luovuttamisella ei saisi rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä. Säännös olisi tarpeen valvovien viranomaisten sekä CSIRT-yksikön välisen yhteistyön toteuttamiseksi niissä tehtävissä, joita viranomaisille on osoitettu yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetussa laissa ja kyberturvallisuuslaissa.

45 §. *Viranomaisten yhteistyö.* Pykälän *2 momenttia* ehdotetaan muutettavaksi siten, että yhteistyövelvoitteeseen kuuluviin viranomaisiin lisättäisiin myös yhteiskunnan kriittisen

infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 19 §:ssä tarkoitetut valvovat viranomaiset.

Pykälään ehdotetaan lisättäväksi uusi *5 momentti*, joka erityissäännös valvovan viranomaisen ja yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 19 §:n nojalla toimivaltaisen valvovan viranomaisen yhteistyöstä.

Ehdotetun 5 momentin nojalla kyberturvallisuuslaissa tarkoitettujen valvovien viranomaisten tulisi vaihtaa säännöllisesti tietoja kriittisten toimijoiden määrittämisestä sekä riskeistä, kyberuhkista ja poikkeamista ja muista kuin kyberturvallisuuteen liittyvistä riskeistä, uhkista ja poikkeamista, jotka vaikuttavat kriittisiin toimijoihin, sekä näiden riskien, uhkien ja poikkeamien hallintatoimenpiteistä. Edellytys vastaisi NIS 2 -direktiivin 13 artiklan 5 kohtaa.

Kyberturvallisuuslain nojalla kriittistä toimijaa valvovan viranomaisen olisi ilmoitettava yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetussa laissa tarkoitetulle valvovalle viranomaiselle, kun kriittiseen toimijaan kohdistetaan valvontaa ja 4 luvussa säädettyjä toimivaltuuksia. Ilmoittaminen mahdollistaisi yhteistyötä ja koordinaatiota viranomaisten välillä kriittiseen toimijaan kohdistuvassa valvonnassa. Lisäksi valvova viranomainen voisi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetussa laissa tarkoitetun valvovan viranomaisen pyynnöstä kohdistaa 4 luvussa säädettyjä toimivaltuuksia kriittiseen toimijaan. Valvovat viranomaiset olisivat pääosin samoja molempien lakien nojalla, mutta säännökset olisivat merkityksellisiä erityisesti viranomaisten keskinäisen yhteistyön vuoksi sekä sellaisissa tilanteissa, joissa poikkeuksellisesti toimijaa valvoisivat eri viranomaiset velvoitteiden osalta. Milloin kriittistä toimijaa valvoo sama viranomainen molempien lakien osalta, ei viranomaisen olisi tarpeen ilmoittaa itselleen toimivaltuuksiensa käytöstä tai osoittaa itselleen toimivaltuuksien käyttöä koskevaa pyyntöä. Säännökset vastaisivat NIS 2 -direktiivin 32 artiklan 9 kohtaa.

Ehdotetuilla muutoksilla pantaisiin täytäntöön NIS 2 –direktiivin 13 artiklan 4 ja 5 kohta osin sekä 32 artiklan 9 kohta.

46 a §. *Eräiden toimijoiden siirtymäaika.* Pykälässä säädettäisiin siirtymäajasta lain velvoitteiden soveltumiselle kriittisessä toimijassa sen jälkeen, kun yhteisö on määritetty kriittiseksi toimijaksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain nojalla. Kriittisellä toimijalla tarkoitettaisiin siten yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain nojalla kriittiseksi määritettyä toimijaa. Kyberturvallisuuslain velvoitteita sovellettaisiin kriittiseen toimijaan kuukauden kuluttua siitä, kun toimija on saanut tiedon yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 13 §:n nojalla annetusta päätöksestä, jolla toimija on määritetty kriittiseksi. Kuitenkin riskienhallintaa koskevien 7–9 §:n velvoitteiden osalta siirtymäaika olisi yhdeksän kuukautta, vastaten yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 30 §:n nojalla säädettyä siirtymäaikaa riskiarvioinnin tekemiselle kriittisessä toimijassa. Kuukauden siirtymäajalla sovellettaisiin kyberturvallisuuslain velvoitteita tietojen ilmoittamisesta valvovalle viranomaiselle toimijaluetteloa varten sekä merkittävästä poikkeamasta ilmoittamisesta. Määräajat laskettaisiin siitä, kun yhteisö on saanut tiedoksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain 13 §:ssä tarkoitetun päätöksen kriittiseksi määrittämisestä.

8 Voimaantulo

Laki olisi tarkoitettu tulemaan voimaan samanaikaisesti yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain kanssa.

9 Toimeenpano ja seuranta

Liikenne- ja viestintäministeriö seuraa kyberturvallisuuslain toimeenpanoa ja soveltamista.

CER-direktiivin 25 artiklan perusteella komissio tarkastelee määräajoin direktiivin toimivuutta ja laatii kertomuksen Euroopan parlamentille ja neuvostolle. Kertomuksessa arvioidaan erityisesti direktiivin tuomaa lisäarvoa ja vaikutusta kriittisten toimijoiden häiriönsietokyvyn varmistamiseen sekä sitä, olisiko direktiivin liitettä muutettava. Ensimmäinen kertomus annetaan viimeistään 17.6.2029.

NIS 2 -direktiivin 40 artiklan perusteella komissio tarkastelee viimeistään 17.10.2027 ja sen jälkeen 36 kuukauden välein direktiivin toimivuutta ja antaa siitä kertomuksen Euroopan parlamentille ja neuvostolle. Kertomuksessa arvioidaan erityisesti asianomaisten toimijoiden koon sekä NIS2-direktiivin liitteissä I ja II tarkoitettujen toimialojen, toimialan osien ja toimijatyyppien merkitystä talouden ja yhteiskunnan toiminnalle kyberturvallisuuden näkökulmasta.

10 Suhde muihin esityksiin

Hallituksen esitys on tarkoitettu käsiteltäväksi eduskunnassa samanaikaisesti hallituksen esityksen eduskunnalle laiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ja eräiksi muiksi laeiksi (HE 205/2024 vp) kanssa. Ehdotetut lainsäädäntömuutokset ehdotetaan tulemaan voimaan samanaikaisesti hallituksen esityksellä HE 205/2024 vp ehdotetun yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain kanssa.

Hallituksen esityksessä HE 205/2024 vp jaksossa 10 todetaan, että valtioneuvosto valmistelee erikseen esityksen teknisistä lainsäädäntömuutoksista, jotka ovat tarpeen ehdotetun kyberturvallisuuslain (HE 57/2024 vp) velvoitteiden soveltamiseksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain nojalla määritettäviin kriittisiin toimijoihin NIS2- ja CER-direktiivien edellyttämällä tavalla. Tässä esityksessä on kyse näistä lainsäädäntömuutoksista.

11 Suhde perustuslakiin ja säätämisjärjestys

Esitys liittyisi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ehdotetun lain soveltamiseen. Mainitun lakiehdotuksen ja kriittisen toimijan määrittämistä koskevan menettelyn suhteesta perustuslakiin esitetään arvio hallituksen esityksen HE 205/2024 vp jaksossa 11. Esityksen johdosta kyberturvallisuuslain mukaiset velvoitteet ja valvontatoimivaltuudet koskisivat kriittiseksi määritettävää toimijaa. Kyberturvallisuuslain mukaisten toimivaltuuksien ja velvoitteiden suhdetta perustuslakiin arvioidaan hallituksen esityksen HE 57/2024 vp jaksossa 12.

Kriittinen toimija olisi kyberturvallisuuslain nojalla velvollinen toteuttamaan kyberturvallisuuteen kohdistuvaa riskienhallintaa, ilmoittamaan valvovalle viranomaiselle merkittävistä poikkeamista sekä ilmoittamaan ja päivittämään toimijaluetteloa koskevan säännöksen mukaiset tiedot valvovalle viranomaiselle. Ehdotetuista velvoitteista aiheutuisi kustannuksia kriittiselle toimijalle. Ehdotetut säännökset ovat merkityksellisiä perustuslain 18 §:ssä turvatun elinkeinovapauden kannalta.

Ilmoitusvelvollisuuden osalta perustuslakivaliokunta on lausunnossa PeVL 54/2002 vp katsonut, ettei pelkästä ilmoitusvelvollisuudesta säätäminen ole itsessään elinkeinovapauden kannalta ongelmallista etenkään, kun viranomaisen ei edellytetä tekevän ilmoituksen johdosta päätöstä. Ehdotetussa ilmoitusvelvollisuudessa olisi kyse kuvatun kaltaisesta tilanteesta. Vaikka kyberturvallisuuslain mukaisen ilmoituksen tekemättä jättäminen ei sinänsä merkitse kieltoa tarjota palvelua tai harjoittaa toimintaa, ilmoituksen tekemättä jättäminen olisi sanktioitu hallinnollisella seuraamuksella ja valvovalla viranomaisella olisi toimivalta määrätä laiminlyönti oikaistavaksi uhkasakon tai keskeyttämisuhkan nojalla tai viimesijassa muita kyberturvallisuuslaissa säädettyjä toimivaltuuksia käyttäen. Perustuslakivaliokunta on lausuntokäytännössään katsonut, että velvollisuus tehdä toiminnasta ilmoitus valvovalle viranomaiselle ja luovuttaa tälle tietoja tilanteessa, jossa ilmoituksen tekemättä jättäminen johtaa kielteisiin seurauksiin, rinnastuu usein luvanvaraisuuteen ja merkitsee näin ollen puuttumista elinkeinovapauteen (PeVL 45/2001 vp). Ilmoitusvelvollisuudessa on kuitenkin kyse luvanvaraisuutta lievemmin elinkeinonvapauteen puuttuvasta velvoitteesta. Perustuslakivaliokunta ei ole katsonut ilmoitusvelvollisuutta elinkeinovapauden kannalta ongelmallisena, kun ilmoituksen tekemättä jättämiselle ei ole asetettu kieltoa harjoittaa elinkeinotoimintaa (PeVL 16/2009 vp) tai viranomaisen ei edellytetä tekevän ilmoituksen johdosta päätöstä (PeVL 54/2002 vp). Kyberturvallisuuslain mukaisissa ilmoitusvelvollisuuksissa olisi kokonaisuutena arvioiden kyse elinkeinovapauden rajoittamisesta ja ehdotuksen olisi täytettävä perusoikeutta rajoittavalta lailta vaadittavat yleiset edellytykset, kuten hyväksyttävyyden sekä täsmällisyyden ja tarkkarajaisuuden vaatimukset (PeVL 58/2014 vp, s.5, PeVL 19/2009 vp, s.2). Elinkeinovapauden rajoittamiselle tulee perustuslakivaliokunnan mukaan olla hyväksyttävä ja painava peruste (PeVL 15/2008 vp, s.2).

Ehdotuksessa on kyse NIS 2 –direktiivin toimeenpanosta velvoittavalta osin, mihin ei liity kansallista liikkumavaraa. Esityksen tavoitteena on vahvistaa kyberturvallisuuden tasoa yhteiskunnan toiminnan kannalta keskeisten ja tärkeiden toimijatyyppien osalta. Ehdotuksen tavoitteena on parantaa yhteiskunnan kriittisen infrastruktuurin toimijoiden kyberturvallisuutta koskevan riskienhallinnan tasoa ja siten turvata yhteiskunnan toiminnan kannalta kriittisten palvelujen jatkuvuutta. Ehdotuksella arvioidaan olevan ilmoitusvelvollisuuden elinkeinovapaudelle aiheuttaman rajoituksen kannalta painava ja hyväksyttävä syy. Lisäksi sääntely täyttäisi perusoikeuksien yleisten rajoitusedellytyksien mukaiset kriteerit sääntelyn tarkkarajaisuudesta ja täsmällisyydestä eikä ehdotuksen arvioida olevan ristiriidassa perustuslain 18 §:n 1 momentissa turvatun elinkeinovapauden kannalta tavalla, joka estäisi esityksen käsittelemisen tavallisen lain säätämisjärjestyksessä.

Ponsi

Koska kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta annetussa Euroopan parlamentin ja neuvoston direktiivissä (EU) 2022/2555 ja kriittisen toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta annetussa Euroopan parlamentin ja neuvoston direktiivissä (EU) 2022/2557on säännöksiä, jotka ehdotetaan pantaviksi täytäntöön lailla, annetaan eduskunnan hyväksyttäväksi seuraava lakiehdotus:

Lakiehdotus

Laki

kyberturvallisuuslain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan kyberturvallisuuslain (/) 3 §:n 2 momentti, 4 §:n 6 momentti, 27 §:n 2 momentti ja 45 §:n 2 momentti sekä

lisätään 17 §:ään uusi 6 momentti, 26 §:ään uusi 3 momentti, 45 §:ään uusi 5 momentti ja lakiin uusi 45 a § seuraavasti:

3 §

Toimijat

— —

Tätä lakia sovelletaan myös toimijaan, joka koostaan riippumatta on:

1) yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoaja;

2) luottamuspalvelun tarjoaja;

3) aluetunnusrekisterin ylläpitäjä;

4) DNS-palveluntarjoaja; tai

5) yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain (/) 10 §:ssä tarkoitettu kriittinen toimija.

— —

4 §

Soveltamisalan rajaukset

— —

Tätä lakia sovelletaan kuntalaissa (410/2015) tarkoitettuun kuntaan vain liitteessä I tai II tarkoitetun toiminnan osalta sekä yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 10 §:ssä tarkoitetuksi kriittiseksi toimijaksi määritellyltä osalta.

— —

17 §

Poikkeamailmoituksen käsittely

— —

Jos 11–13 tai 15 §:ssä tarkoitetun ilmoituksen tai raportin tekee yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 10 §:ssä tarkoitettu kriittinen toimija, valvovan viranomaisen on toimitettava ilmoituksesta tai raportista tieto viranomaiselle, joka on mainitun lain 19 §:n nojalla toimivaltainen valvomaan kriittistä toimijaa.

26 §

Valvovat viranomaiset

— —

Jos 3 §:n 2 momentin 5 kohdassa tarkoitettu toimija ei harjoita liitteessä I tai II tarkoitettua toimintaa, valvova viranomainen määräytyy yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 19 §:n nojalla.

27 §

Valvonnan kohdistaminen

— —

Keskeisellä toimijalla tarkoitetaan

1) liitteessä I tarkoitettua toimijaa, joka ylittää mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä annetun komission suosituksen 2003/361/EY liitteen 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset;

2) hyväksyttyjä luottamuspalvelun tarjoajia, aluetunnusrekisterin ylläpitäjiä sekä DNS-palveluntarjoajia;

3) yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajia, jotka täyttävät tai ylittävät mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä annetun komission suosituksen 2003/361/EY liitteen 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset;

4) 3 §:n 3 momentissa tarkoitettua toimijaa; sekä

5) yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 10 §:ssä tarkoitettua kriittistä toimijaa.

— —

28 §

Tiedonsaantioikeus

— —

Valvovalla viranomaisella on salassapitosäännösten, 2 momentissa säädetyn salassapitovelvollisuuden ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa tässä laissa säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto toiselle valvovalle viranomaiselle, CSIRT-yksikölle tai yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 19 §:ssä tarkoitetulle valvovalle viranomaiselle, jos se on välttämätöntä tässä laissa tai yhteiskunnan kriittisen infrastruktuurin suojaamisesta annetussa laissa viranomaiselle säädettyä tehtävää varten. Tiedonsaantioikeuden käyttämisellä tai tietojen luovuttamisella ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.

— —

45 §

Viranomaisten yhteistyö

— —

Valvovien viranomaisten, CSIRT-yksikön ja keskitetyn yhteyspisteen on toimittava tarvittaessa yhteistyössä poliisin tai muun esitutkintaviranomaisen, tietosuojavaltuutetun, Liikenne- ja viestintäviraston sille ilmailulaissa, sähköisen viestinnän palveluista annetussa laissa ja eIDAS-

asetuksessa säädettyjen tehtävien osalta ja Finanssivalvonnan kanssa sekä yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 19 §:ssä tarkoitetun valvovan viranomaisen kanssa.

— —

Valvovien viranomaisten ja yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 19 §:ssä tarkoitettujen valvovien viranomaisten on vaihdettava keskenään säännöllisesti tietoja kriittisten toimijoiden määrittämisestä sekä riskeistä, kyberuhkista ja poikkeamista ja muista kuin kyberturvallisuuteen liittyvistä riskeistä, uhkista ja poikkeamista, jotka vaikuttavat kriittisiksi toimijoiksi määritettyihin toimijoihin, sekä näiden riskien, uhkien ja poikkeamien hallintatoimenpiteistä. Valvovan viranomaisen on ilmoitettava yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 19 §:n nojalla toimivaltaiselle valvovalle viranomaiselle, kun kriittiseen toimijaan kohdistetaan 4 luvussa säädettyjä toimivaltuuksia. Valvova viranomainen voi kohdistaa kriittiseen toimijaan valvontaa yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 19 §:n nojalla toimivaltaisen valvovan viranomaisen pyynnöstä.

46 a §

Eräiden toimijoiden siirtymäaika

Tätä lakia sovelletaan kriittiseen toimijaan kuukauden kuluttua siitä, kun tämä on saanut tiedon sen kriittiseksi määrittämistä koskevasta päätöksestä. Tämän lain 7–9 §:ää sovelletaan kriittiseen toimijaan yhdeksän kuukauden kuluttua siitä, kun vastaanottaja on saanut tiedon sen kriittiseksi määrittämistä koskevasta päätöksestä.

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

Helsingissä x.x.20xx

Pääministeri

Etunimi Sukunimi

..ministeri Etunimi Sukunimi

Liite
Rinnakkaisteksti

Laki

kyberturvallisuuslain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan kyberturvallisuuslain (/) 3 §:n 2 momentti, 4 §:n 6 momentti, 27 §:n 2 momentti ja 45 §:n 2 momentti sekä

lisätään 17 §:ään uusi 6 momentti, 26 §:ään uusi 3 momentti, 45 §:ään uusi 5 momentti ja lakiin uusi 45 a § seuraavasti:

Voimassa oleva laki	*Ehdotus*
3 §	3 §
Toimijat	*Toimijat*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Tätä lakia sovelletaan myös toimijaan, joka koostaan riippumatta on: 1) yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoaja; 2) luottamuspalvelun tarjoaja; 3) aluetunnusrekisterin ylläpitäjä; *tai* 4) DNS-palveluntarjoaja.	Tätä lakia sovelletaan myös toimijaan, joka koostaan riippumatta on: 1) yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoaja; 2) luottamuspalvelun tarjoaja; 3) aluetunnusrekisterin ylläpitäjä; 4) DNS-palveluntarjoaja; *tai* *5) yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain (/) 10 §:ssä tarkoitettu kriittinen toimija.*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
4 §	4 §
Soveltamisalan rajaukset	*Soveltamisalan rajaukset*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Tätä lakia sovelletaan kuntalaissa (410/2015) tarkoitettuun kuntaan vain liitteessä I tai II tarkoitetun toiminnan osalta.	Tätä lakia sovelletaan kuntalaissa (410/2015) tarkoitettuun kuntaan vain liitteessä I tai II tarkoitetun toiminnan osalta *sekä yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 10 §:ssä tarkoitetuksi kriittiseksi toimijaksi määritellyltä osalta.*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —

Voimassa oleva laki	*Ehdotus*
17 §	17 §
Poikkeamailmoituksen käsittely	*Poikkeamailmoituksen käsittely*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
(uusi)	Jos 11–13 tai 15 §:ssä tarkoitetun ilmoituksen tai raportin tekee yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 10 §:ssä tarkoitettu kriittinen toimija, valvovan viranomaisen on toimitettava ilmoituksesta tai raportista tieto viranomaiselle, joka on mainitun lain 19 §:n nojalla toimivaltainen valvomaan kriittistä toimijaa.
26 §	26 §
Valvovat viranomaiset	*Valvovat viranomaiset*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
(uusi)	Jos 3 §:n 2 momentin 5 kohdassa tarkoitettu toimija ei harjoita liitteessä I tai II tarkoitettua toimintaa, valvova viranomainen määräytyy yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 19 §:n nojalla.
27 §	27 §
Valvonnan kohdistaminen	*Valvonnan kohdistaminen*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Keskeisellä toimijalla tarkoitetaan 1) liitteessä I tarkoitettua toimijaa, joka ylittää mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä annetun komission suosituksen 2003/361/EY liitteen 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset; 2) hyväksyttyjä luottamuspalvelun tarjoajia, aluetunnusrekisterin ylläpitäjiä sekä DNS-palveluntarjoajia; 3) yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajia, jotka täyttävät tai ylittävät mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä annetun komission suosituksen 2003/361/EY liitteen 2	Keskeisellä toimijalla tarkoitetaan 1) liitteessä I tarkoitettua toimijaa, joka ylittää mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä annetun komission suosituksen 2003/361/EY liitteen 2 artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset; 2) hyväksyttyjä luottamuspalvelun tarjoajia, aluetunnusrekisterin ylläpitäjiä sekä DNS-palveluntarjoajia; 3) yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajia, jotka täyttävät tai ylittävät mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä annetun komission suosituksen 2003/361/EY liitteen 2

Voimassa oleva laki	*Ehdotus*
artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset; *sekä* 4) 3 §:n 3 momentissa tarkoitettua toimijaa.	artiklan mukaiset keskisuuria yrityksiä koskevat edellytykset; 4) 3 §:n 3 momentissa tarkoitettua toimijaa; *sekä* *5) yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 10 §:ssä tarkoitettua kriittistä toimijaa*.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
28 §	28 §
Tiedonsaantioikeus	*Tiedonsaantioikeus*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Valvovalla viranomaisella on salassapitosäännösten, 2 momentissa säädetyn salassapitovelvollisuuden ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa tässä laissa säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto toiselle valvovalle viranomaiselle *ja* CSIRT-yksikölle, jos se on välttämätöntä tässä laissa tai yhteiskunnan kriittisen infrastruktuurin suojaamisesta annetussa laissa viranomaiselle säädettyä tehtävää varten. Tiedonsaantioikeuden käyttämisellä tai tietojen luovuttamisella ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.	Valvovalla viranomaisella on salassapitosäännösten, 2 momentissa säädetyn salassapitovelvollisuuden ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa tässä laissa säädettyjen tehtäviensä hoitamisen yhteydessä saamansa tai laatimansa asiakirja sekä ilmaista salassa pidettävä tieto toiselle valvovalle viranomaiselle, CSIRT-yksikölle *tai yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 19 §:ssä tarkoitetulle valvovalle viranomaiselle*, jos se on välttämätöntä tässä laissa tai yhteiskunnan kriittisen infrastruktuurin suojaamisesta annetussa laissa viranomaiselle säädettyä tehtävää varten. Tiedonsaantioikeuden käyttämisellä tai tietojen luovuttamisella ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
45 §	45 §
Viranomaisten yhteistyö	*Viranomaisten yhteistyö*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Valvovien viranomaisten, CSIRT-yksikön ja keskitetyn yhteyspisteen on toimittava tarvittaessa yhteistyössä poliisin tai muun esitutkintaviranomaisen, tietosuojavaltuutetun, Liikenne- ja viestintäviraston sille ilmailulaissa, sähköisen viestinnän palveluista annetussa	Valvovien viranomaisten, CSIRT-yksikön ja keskitetyn yhteyspisteen on toimittava tarvittaessa yhteistyössä poliisin tai muun esitutkintaviranomaisen, tietosuojavaltuutetun, Liikenne- ja viestintäviraston sille ilmailulaissa, sähköisen viestinnän palveluista annetussa laissa ja eIDAS-asetuksessa säädettyjen

Voimassa oleva laki	*Ehdotus*
laissa ja eIDAS-asetuksessa säädettyjen tehtävien osalta ja Finanssivalvonnan kanssa.	tehtävien osalta ja Finanssivalvonnan kanssa *sekä yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 19 §:ssä tarkoitetun valvovan viranomaisen kanssa*.
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
(uusi)	Valvovien viranomaisten ja yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 19 §:ssä tarkoitettujen valvovien viranomaisten on vaihdettava keskenään säännöllisesti tietoja kriittisten toimijoiden määrittämisestä sekä riskeistä, kyberuhkista ja poikkeamista ja muista kuin kyberturvallisuuteen liittyvistä riskeistä, uhkista ja poikkeamista, jotka vaikuttavat kriittisiksi toimijoiksi määritettyihin toimijoihin, sekä näiden riskien, uhkien ja poikkeamien hallintatoimenpiteistä. Valvovan viranomaisen on ilmoitettava yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 19 §:n nojalla toimivaltaiselle valvovalle viranomaiselle, kun kriittiseen toimijaan kohdistetaan 4 luvussa säädettyjä toimivaltuuksia. Valvova viranomainen voi kohdistaa kriittiseen toimijaan valvontaa yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain 19 §:n nojalla toimivaltaisen valvovan viranomaisen pyynnöstä.
	46 a §
(uusi)	*Eräiden toimijoiden siirtymäaika*
	Tätä lakia sovelletaan kriittiseen toimijaan kuukauden kuluttua siitä, kun tämä on saanut tiedon sen kriittiseksi määrittämistä koskevasta päätöksestä. Tämän lain 7–9 §:ää sovelletaan kriittiseen toimijaan yhdeksän kuukauden kuluttua siitä, kun vastaanottaja on saanut tiedon sen kriittiseksi määrittämistä koskevasta päätöksestä.
Tämä laki tulee voimaan päivänä kuuta 20 . .	Tämä laki tulee voimaan päivänä kuuta 20 . .