Suomen Kuntaliitto ry

Lausunto

29.11.2023

Asia: VN/18157/2023

Lausuntopyyntö: luonnos hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Suomen Kuntaliitto ry, jäljempänä Kuntaliitto, kiittää mahdollisuudesta kommentoida luonnosta hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi. Yleisesti voidaan todeta, että NIS2-direktiivin soveltaminen kansallisessa lainsäädännössä on ehdotettu toteutettavaksi riittävällä tavalla. NIS2-direktiivin kansallinen jalkauttaminen luo kansallisen tason kyberturvallisuuslainsäädännön. Näin ollen ymmärrys ja tietoisuus sisällöstä ja sen vaikutuksista on osa tietoturvallisuuden, kyberturvallisuuden johtamista.

Kuntien kannalta huomiot kohdistuvat siihen, että soveltaminen erityisesti kuntia koskettavilla toimialoilla tulee olla riittävän selkeää.

- Kunnan on hyvä selvittää oma roolinsa NIS2-direktiivin keskeisten sekä tärkeitten toimialojen suhteen.

- Kuntien järjestämisvastuulla tai kuntaomisteisilla toimialoilla lakia kyberturvallisuuden riskienhallinnasta sovellettaisiin vesihuollossa (juomavesi ja jätevesi), energiasektorilla (sähkö, öljy, maakaasu, kaukolämmitys ja -jäähdytys, maakaasu, vety), jätehuollossa ja vesiliikenteessä (satamat).

- Kunnilla voi olla omistuksessaan lentoasemia ja yksityisraiteita, joissa myös soveltaminen voi tulla kyseeseen.

- Kunnat saattavat järjestää tietoverkkopalvelutoimintoja esim. omalle vesihuollolle, jolloin selvitettäväksi tulee, kuuluuko kunta soveltamisalan piiriin verkkopalveluiden tarjoajan roolissa.

Kuntaliiton näkemyksen mukaan lausunnolla oleva luonnos laajasti tulkittuna - määrittelyjen osalta - laajentaisi NIS2-direktiivin soveltamisalojen toimijoitten lukumäärää huomattavasti arvioidusta sekä mahdollisesti asettaisi kuntia erilaiseen asemaan suhteessa lakiin kyberturvallisuuden riskienhallinnasta. Määritelmiin (keskeinen/keskisuuri/tärkeä toimija) tulee kiinnittää huomiota,

jotta vältyttäisiin lain soveltamisen osalta lain eri tulkinnoilta toimivaltaisten viranomaisten ja soveltamisaloihin kuuluvien toimijoiden välillä. Asia tulisi tarkastella uudelleen ja selkiyttää lakiehdotuksessa.

Kyberturvallisuuden ja tietoturvallisuuden haasteita ratkaistaessa ja velvoittavia toimenpiteitä toteutettaessa joudutaan asioita tarkastelemaan riskipohjaisen lähestymisen kautta - sovittamaan asioita organisaation toimintaan ja toimintaympäristöön. Laki kyberturvallisuuden riskienhallinnasta on uutta sääntelyä kuntakentälle.

- Uusi, organisaation toiminnan kannalta vaikea sääntely edellyttää koordinoivaa, ohjaavaa neuvontaa riittävillä resursseilla ja auktoriteetilla varustettuna esim. ministeriön yhteyteen perustetun neuvontatoimen kautta.

- Neuvonnan tulee koskea niin keskeisiä kuin tärkeitäkin toimialoja ja niitä toteuttavia toimijoita.

Kuntajohtaminen on kokonaisuus, joka muodostuu useista toisiaan täydentävistä näkökulmista. Kunnat ovat ajan saatossa eriytyneet toisistaan. Erilaisilla kunnilla on myös hyvin erilaiset resurssit. Johtamiseen liittyviin raportointeihin sekä arviointeihin ja valvontaan ei kaikilla kunnilla ole samanlaisia mahdollisuuksia. Toimintoja ja toiminnallisuuksia toteutettaessa taustalla on sopimusoikeudelliset asiat. Olemassa olevien sopimusten sisällöllisyys, niihin liittyvät määritellyt vastuut ja velvoitteet sekä seurannan ja valvonnan toteutuminen.

- Kuntaa johdetaan myös häiriötilanteissa ja poikkeusoloissa, kuntakonsernissa valtuuston ja kunnanhallituksen päätösten mukaisesti.

Riskienhallinta, varautuminen, ennakointi palvelevat johtamista - toiminnan kokonaisuutta. Keskeisiä palveluja tuotetaan kuntayhtiöissä tai on ulkoistettu. Kriittiset palvelut turvataan riippumatta palveluja tuottavasta tahosta.

- Tarkoituksenmukainen toiminta edellyttää NIS2-direktiivin mukaisten velvoitteitten, ja tarvittavien pelisääntöjen tuntemista ja ymmärtämistä.

Soveltamisalaa koskevat huomiot

Laissa kyberturvallisuuden riskienhallinnasta 3 §:ssä todetaan, että ”tämän lain soveltamisalaan kuuluvalla toimijalla tarkoitetaan oikeushenkilöä tai luonnollista henkilöä, joka harjoittaa liitteessä I tai II tarkoitettua toimintaa tai on liitteessä I tai II tarkoitettua toimijatyyppiä ja täyttää tai ylittää keskisuuren toimijan määritelmän.”

Kunnan harjoittaessa liitteessä I tai II tarkoitettua toimintaa taseyksikkönä, liikelaitosmuotoisena tai jossakin erityistapauksessa kokonaan omana toimintana, katsotaan kunta silloin lain tarkoittamaksi oikeushenkilöksi, joka harjoittaa kyseistä toimintaa. Esimerkiksi vesihuolto, joka usein on kunnissa taseyksikkö- tai liikelaitosmuotoisena, ei ole oma oikeushenkilönsä. Jos kunta tulkitaan näissä

tapauksissa koko toimintansa osalta soveltamisalan piiriin kuuluvaksi ja kokokriteeri määritetään suhteessa koko kunnan toimintaan, täyttää suurin osa kunnista lain mukaisen vähintään keskisuuren toimijan määritelmän, useissa tapauksissa myös keskeisen toimijan määritelmän.

Kunnan harjoittaessa vastaavaa toimintaa yhtiömuotoisena, tulkittaisiin soveltamiskriteeristöä vain harjoitettavaan yhtiömuotoiseen toimintaan kohdistuen, ei koko kuntaan kohdistuen. Täten kunnat olisivat keskenään eriarvoisessa asemassa suhteessa kyberturvallisuuden riskienhallinnasta annettuun lakiin riippuen siitä, onko niiden vesihuoltolaitos tai muu vastaava direktiivin liitteiden mukainen toiminta yhtiöitetty.

Tulkittaessa kunnan harjoittavan toimintaa oikeushenkilönä lain soveltamisaloilla, tulee määritellä selkeästi millä tavoin komission suositusta yritysten koon määrittämisestä sovellettaisiin kuntiin. Huomioituna laskennalliset kriteerit soveltamisalan piiriin kuuluvan toimijan henkilökunnan määrän osalta. Eri määritelmät ja niiden soveltaminen erilaisiin toimijatahoihin tuleekin kirjata selkeästi lakiin.

Kuntaliiton näkemyksen mukaan määritelmät keskisuuri toimija, keskeinen toimija ja tärkeä toimija eivät ole riittävän yksiselitteisesti määriteltyjä tai ainakin niiden soveltaminen jää osin epäselväksi. Jos tulkitaan, että kunta harjoittaa oikeushenkilönä toimintaa lain soveltamisalalla, tulee määritellä millä kriteerein lasketaan soveltamisalan piiriin kuuluvan henkilökunnan määrä, ja millä tavoin komission suositusta yritysten koon määrittämisestä sovellettaisiin kuntiin.

Tiedonhallintalaki 18 a § määrittää hyvinvointialueet ja Helsingin kaupungin tärkeiksi toimijoiksi julkisen hallinnon toimialalla. Tärkeälle toimijalle asetettu vaatimustaso on alempi kuin kyberturvallisuuslain mukainen keskeiselle toimijalle asetettu vaatimustaso. Esimerkiksi Kaarinan kaupunki täyttänee kyberturvallisuuslain mukaan keskeisen toimijan kriteerin (vesihuollon toimiala), jos se tulkitaan koko kaupunkina kuuluvaksi lain piiriin oman vesihuollon takia. Kaarinan kaupunkiin sovelletaan tällöin korkeampaa NIS2-vaatimustasoa kuin hyvinvointialueisiin ja Helsingin kaupunkiin. Tämä asetelma ei vaikuta perustellulta NIS2-direktiivin tavoitteet huomioiden, eikä lakia kyberturvallisuuden riskienhallinasta tule soveltaa esimerkissä mainitulla tavalla.

NIS2-velvoitteiden soveltamista yritys- ja konsernirakenteisiin tulisi tarkentaa. Jos yrityksen yksikön tietty toiminto kuuluu NIS2-soveltamisalaan, jättää lakiehdotus epäselväksi, mihin toimintoihin NIS2-velvoitteet kohdistuvat: vain kyseisen yksikön soveltamisalaan kuuluvaan toimintaan, koko yksikön toimintoihin vai jopa koko yrityksen/konsernin kaikkiin toimintoihin. ”Toimijan” käsite vaikuttaa myös valvonta- ja seuraamusjärjestelmään ja sitä tulisi selventää. Ehdotuksessa seuraamusmaksu on sidottu "toimijan" liikevaihtoon, mikä voi johtaa merkittävään vaihteluun seuraamus-maksun suuruudessa riippuen siitä, tulkitaanko "toimijaksi" koko konserni vai esimerkiksi yksittäinen tytäryhtiö.

Kuntaliiton näkemyksen mukaan ehdotuksessa tulee selkeyttää, millä tavoin kyberturvallisuuden riskienhallintaa koskevaa lakia sovelletaan niiden kuntien toimintaan, jotka järjestävät jotakin

liitteissä I ja II kuvattua toimintaa taseyksikkö- tai liikelaitosmuotoisena tai omana toimintana. Lisäksi tulisi tarkastella yksityiskohtaisemmin vaikutuksia kuntatoimijoihin näissä tilanteissa. On myös tarkennettava, miten kriittisen toimijan kokokriteeri määritetään, jos kunta oikeushenkilönä harjoittaa soveltamisalan piiriin kuuluvaa toimintaa.

Kuntaliiton näkemyksen mukaan NIS2-direktiivin soveltamisalaan kuulumisessa tulisi tarkastella ensisijaisesti vain soveltamisalan piiriin kuuluvan toiminnan taloutta ja laajuutta, ei koko kunnan toiminnan laajuutta. Muunlainen tarkastelu johtaa siihen, että NIS2-direktiivin soveltamisala laajenee lähes kaikkiin kuntiin, vaikka esimerkiksi kunnan harjoittama vesihuoltotoiminta on laajuudeltaan pienimuotoista.

Edellä esitetyt asiat tulisi huomioida myös ehdotetun lain alemman asteisen sääntelyn osalta. ”Lakiin sisältyisi myös säännös, jonka nojalla valtioneuvoston asetuksella voitaisiin tietyin edellytyksin säätää toimijan kuulumisesta lain soveltamisalaan sen koosta riippumatta.”

Kuntaliitto nostaa esiin esimerkit lain mahdollisista vaikutuksista vesihuolto-, jätehuolto- ja kaukolämpö- sekä digitaalinen infrastruktuuri ja digitaalisen palvelun tarjoajien että tieto- ja viestintätekniikan palvelujen (TVT) hallinnan toimialoilla:

Esimerkkinä - vesihuolto

Vesihuolto sisältyy toimintona lain liitteeseen I. Hyvin monen kunnan vesihuoltolaitos toimii joko taseyksikkönä tai liikelaitoksena, joten laitoksilla ei ole omaa Y-tunnusta eivätkä ne ole oikeushenkilöitä, vaan ne kuuluvat osaksi kuntaa. Vesihuoltolaki edellyttää kuitenkin laitoksen talouden eriyttämistä kunnan kirjanpidossa ja palvelu katetaan maksurahoitteisesti.

Hallituksen esityksen vaikutusarvioinnin mukaan sekä juomavesi että jätevesi ovat kuuluneet NIS1-direktiivin mukaiseen kansalliseen soveltamisalaan (kriteerinä vähintään 5000 m3:n veden toimittaminen tai jätevesien vastaanottaminen). Sääntely koskee siten nykyisellään talousvesilaitoksia, jätevesilaitoksia ja tukkuvesihuoltolaitoksia ja toimijoita on arviolta noin 70 kpl. Esityksessä todetaan, että siirtymisen kokokriteerin käyttöön ei ennakoida lisäävän NIS2-direktiivin juoma- ja jätevesisektorilla soveltamisalaan kuuluvien toimijoiden määrää olennaisesti. Vesihuolto kuuluu myös CER-direktiivin soveltamisalaan.

Lain valmistelijat eivät näytä tarkoittaneen, että lain soveltamisen piiriä laajennettaisiin kovinkaan paljon merkittävän kokoisista vesihuoltolaitoksista pienempiin, mikä olisikin tarkoituksenmukaista. Kuntaliiton näkemyksen mukaan niin on kuitenkin käymässä, mikäli kokokriteerinä tulkitaan ja tutkitaan koko kunnan henkilöstömäärää ja talouslukuja. Koska miltei kaikki kunnat täyttävät kokokriteerien osalta vähintään keskisuuren toimijan määritelmän, niin tällöin myös niiden lukuisat pienet, alle keskisuuren kokokriteerin taseyksiköinä ja liikelaitoksina toimivat vesihuoltolaitoksetkin

sisältyisivät NIS2-soveltamisalaan. Se ei liene ollut lainsäätäjän alkuperäinen tarkoitus, ainakaan vaikutusarviointiin kirjoitetun perusteella. Kuntaliitto arvioi, että kyberturvallisuuden soveltamisalan piiriin vesihuollossa voisi joutua arvioidun 70 toimijan lisäksi noin 200 muuta toimijaa. Moni toimijoista ylittäisi myös NIS2-direktiivin mukaisen keskeisen toimijan kynnysarvon, joten niihin tulisi kohdentaa myös ennakkovalvontaa. Tältä osin tehdyt vaikutusarviot eivät pitäisi lainkaan paik-kansa.

Esimerkiksi Kaarinan kokoisen kaupungin (35 000 as) voidaan arvella olevan direktiivin soveltamisalan keskeinen toimija (noin 900 työntekijää, tase 2022 noin 277 miljoonaa euroa), vaikka sen vesihuoltoliikelaitoksen vastaavat luvut jäävät alle keskisuuren toimijan (liikevaihto n. 8 milj. e, tase 50 milj. e, työntekijämäärä alle 50). Vastaavasti Raisiossa (25 000 as) toimiva Raision Vesi Oy ei olisi itsenäisenä toimijana liikevaihtonsa ja henkilöstömääränsä puolesta keskisuuri yritys, eikä se siten kuuluisi NIS2-direktiivin soveltamisalaan.

Esimerkkinä - jätehuolto

Vastaavasti jätehuollosta todetaan esityksessä seuraavaa: ”NIS2-direktiivin soveltamisalaan kuuluvia toimijoita olisivat keskisuuret ja suuremmat toimijat, joiden pääasiallinen toimiala on jätehuolto. Tällaisia yrityksiä Suomessa on tilastokeskuksen ja yritys- ja yhteisötietojärjestelmä YTJ:n mukaan henkilöstön määrän osalta noin 30 kappaletta. Suuriksi yrityksiksi ja siten keskeisiksi toimijoiksi henkilöstön perusteella voidaan luokitella näistä 6 yritystä. Liikevaihdon ja lopputaseen perusteella sääntelyn soveltamisalaan kuuluisi noin 30 yritystä. Joukossa on useita kuntien omistamia yrityksiä tai kuntayhtymiä. Suurimmat toimijat ovat osa yrityskonserneja, jotka voivat kuulua sääntelyn soveltamisalaan myös muun toiminnan kuin jätehuollon osalta.” Nähtävästi lukuun on laskettu jätehuollon toimialalta vain kokokriteerin täyttävät kunnalliset osakeyhtiöt ja kuntayhtymät sekä yksityiset jätehuoltoyritykset.

On huomattava, että jätehuollossakin toimii noin 30 taseyksikköä tai liikelaitosta kunnan yhteydessä, vaikka valtaosa kunnallisesta jätehuollosta järjestetäänkin kuntien välisenä yhteistoimintana joko kunnallisissa jätehuoltoyhtiöissä tai kuntayhtymissä. Nämä kunnan osana toimivat yksiköt ovat usein melko pienten kuntien pieniä jätehuollosta vastaavia toimijoita. Mutta koska useiden kuntien kokokriteerit ylittävät vähintään keskisuuren toimijan kynnysarvon, toisi tämäkin NIS2-soveltamisalan piiriin useita lisätoimijoita. Esimerkkinä mainittakoon vaikkapa noin 19 000 asukkaan Jäm-sän kaupunki, jossa on runsaat 600 työntekijää ja noin 2000 asukkaan Rääkkylän kunta, jossa vuonna 2022 oli 83 työntekijää ja jonka tase oli runsaat 15 milj. e. Vuodesta 2023 lukien tosin SOTE-palveluiden poistuminen kuntien tehtävistä on pienentänyt kuntien henkilöstömääriä ja talouslukuja huomattavasti.

Esimerkkinä - kaukolämpö

Energia-alalla NIS2-direktiivin soveltamisalaan kuuluisivat esityksen mukaan uusina toimijoina mm. sähköverkonhaltijat, sähköntuottajat, sähkönmyyjät, kaukolämpö/-kylmätoimijat. Näistä sähköala on lakisääteisesti yhtiöitetty, mutta kaukolämpötoiminnassa on muitakin toimintamuotoja.

Kuntien omistamista kaukolämpötoimijoista valtaosa on yhtiöitetty, mutta etenkin pienissä kunnissa on myös liikelaitoksia ja taseyksikköjä. Tarkka määrä ei ole Kuntaliiton tiedossa, mutta vuotuisen lämpölaitoskyselyn (Tietoja pienistä lämpölaitoksista) aineistossa taseyksikköjä ja liikelaitoksia on ollut viime vuosina kymmenkunta. Koko maassa niitä lienee lämpölaitoskyselyn otoksen perusteella 10–20 kunnassa, joista valtaosa on pieniä, muutaman tuhannen asukkaan kuntia.

Tyypillisesti pienten lämpölaitosten (lämpöteho yleensä alle 10 MW) henkilökuntaan kuuluu enintään muutama työntekijä, niiden vuotuinen liikevaihto on pieni (yleensä 0,5– 1,0 M€/vuosi) ja tase enimmillään 5–10 M€ suuruusluokkaa. Luvut ovat suuntaa-antavia, mutta niiden perusteella voi päätellä, että taseyksikkönä tai kunnallisena liikelaitoksena toimiva kaukolämpöliiketoiminta ei ylitä NIS2-direktiivin soveltamisrajoja (henkilöstö, liikevaihto, tase). Pienillä kaukolämpölaitoksilla liiketoiminnan kasvupotentiaali ei yleensä ole kovin suuri, koska kaukolämpöverkon suunnitteluvaiheessa on jo otettu huomioon taajaman keskeisin asiakaspotentiaali.

Liikelaitos- tai taseyksikkömuotoista kaukolämpötoimijaa koskevat samat ongelmat, joita edellä on esitetty vesihuollosta ja jätehuollosta. Mikäli tarkastellaan toiminnan omistajakunnan kokokriteeriä kokonaisuutena, nämäkin toimijat ja kunnat joutuisivat lain soveltamisalan piiriin.

Esimerkkinä - digitaalinen infrastruktuuri ja digitaalisen palvelun tarjoajat, tieto- ja viestintätekniikan palvelujen (TVT) hallinta

Kunnat saattavat tarjota tietoverkkopalveluita toimijalle, esimerkiksi vesihuoltolaitokselle, joka kuuluu kyberturvallisuudesta annetun lain soveltamisen piiriin. Myöskään hyvinvointialueet eivät ole vielä kyenneet täysin irrottautumaan kuntien (tieto)verkkopalveluista. Kunta voisi tällöin kuulua kokonaisuudessaan lain soveltamisalan piiriin verkkopalvelutoimittajana tai sitten siltä osin kuin kunta antaa palvelua omille yksiköilleen, jotka kuuluvat soveltamisalan piiriin (esim. kunnallinen vesihuolto). Kunnan verkkopalvelut ovat kokonaisuus ja niiden jakaminen hallitusti osiin, joissa erotettaisiin kyberturvallisuudesta annetun lain soveltamisalaan kuuluva toiminta on haastavaa, kokonaiskustannuksia lisäävää toimintaa. Myös toimijakoon määrittäminen näissä tilanteissa voi olla haastavaa, jos laskennallisesti täytyy määrittää soveltamisalan piiriin kuuluvien palveluiden osuus kokonaisuudesta.

Riskienhallintavelvoitetta koskevat huomiot

Esitetyn lain kyberturvallisuuden riskienhallinnasta 7-9 §:ssä olevat kyberturvallisuuden riskienhallintavelvoite, riskienhallinnan toimintamalli ja riskienhallinnan toimenpiteet vastaavat NIS2-direktiivin vaatimuksia. NIS2-direktiivin riskienhallintavelvoitteet ovat vähimmäistason velvoitteita. Kyberturvallisuuden riskienhallinnan tavoiteasetelma on kirjattu kansallisella tasolla muodostaen yleisen riskienhallintavelvoitteen direktiivin tunnistamilla soveltamisaloilla. Toimijalla on oltava käytössään ajantasainen riskienhallinnan toimintamalli. Kyberturvallisuuden riskienhallinnan toimintamalli ohjaa riskienhallintatoimenpiteitä. Kuntaliiton näkemyksen mukaan 8 §:n tar-koittaman kyberturvallisuuden riskienhallinnan toimintamallin olisi hyvä noudattaa riskienhallinnan yleistä ja vakioitua konseptia, johon kuuluu vaarojen tunnistus, riskinarviointi ja riskienhallinta.

Lakiesityksessä ei ole esitetty siirtymäaikaa riskienhallinnan velvoitteiden toimeenpanolle (esim. 8 §). Kuntaliiton näkemyksen mukaan kansallisen täytäntöönpanon osalta tulisi tätä mahdollisuuksien mukaan harkita. Harvalla kuntatoimijalla, esim. vesihuoltolaitoksella on käytössään systemaattinen toimintamalli kyberturvallisuuden riskien hallintaan eikä toteuttamiseen ole myöskään konkreettista valmista kullekin toimijalle sopivaa työvälinettä. Kunnallisten vesihuoltolaitoksien kokemus systemaattisesta talousveden laaturiskien, viemäröinnin sekä jätevedenpuhdistuksen terveys- ja ympäristöriskien hallinnasta olemassa olevilla verkkopohjaisilla WSP- ja SSP-välineillä on laitostasolla kuukausien prosessi.

Kuntaliitto pitää erittäin tärkeänä, että lain soveltamisalaan kuuluville toimijoille järjestetään jatkossa yleistä kyberturvallisuuden riskienhallinnan koulutusta ja että toimijoille on tarjolla asianmukaista ja resursoitua neuvontaa. Esityksen mukaisesti kyberturvallisuutta koskevat riskit tulisi huomioiminen omana kokonaisuutenaan ei vain osana tietoturvallisuutta. Esimerkkinä tulokulma: ”Toimijalla tulisi olla pääsynhallintaan liittyvät määrittelyt ja käytännöt, joilla varmistetaan kattavasti luotettava tunnistaminen ja joilla sallitaan pääsy vain tarvittaviin viestintäverkkoihin ja tietojärjestelmiin, suojattaviin tietoihin sekä muihin resursseihin.”

Raportointivelvoitetta koskevat huomiot

Kuntaliiton näkemyksen mukaan tulisi vaikutuksia kuntatoimijoihin raportoinnin osalta tarkastella nykyistä yksityiskohtaisemmin (mm. yhtiöittämiset, taloudelliset vaikutukset). Raportointiin kuuluu se, että keskeisten ja tärkeiden toimijoiden tulee mm. raportoida merkittävästä poikkeamasta CSIRT-yksikölle tai toimivaltaiselle valvovalle viranomaiselle (ennakkovaroitus, poikkeamailmoitus, loppuraportti, väliraportti; pyynnöstä). Toimijan on myös ilman aiheetonta viivytystä tiedotettava palvelujensa vastaanottajille (kyberuhan vaikutuksen alaisille) toimenpiteistä ja korjaavista toimista (vastaanottajien toteutettavissa olevista). Lisäksi tarvittaessa palvelujen vastaanottajille tulee tiedottaa myös itse kyberuhasta.

Kuntaliitto toteaa, että lakiin kirjattua kahden viikon ilmoitusaikaa valvontaviranomaiselle toimijatyyppiin kohdentuvista muutoksista voidaan pitää kohtuuttoman tiukkana.

Valvontaa koskevat huomiot

Valvonnan toteutuessa hajautetun mallin mukaisesti (NIS2-yleislaki), pitää Kuntaliitto tärkeänä valvonnan resurssoinnin ja ohjeistuksen riittävää toteuttamista. Kysymys siitä, millä valvontataholla tai mahdollisella muulla taholla on velvollisuus ja vastuu neuvoa sekä antaa etukäteistietoa soveltamiseen liittyen. Kuntaliiton näkemyksen mukaan laissa on tarpeen määrittää konkreettisesti, kenellä on vastuu neuvoa ja ohjeistaa soveltamiseen liittyen.

On myös tärkeää, että valvoville viranomaisille valvonnan yhteydessä kertyvät tiedot valvonnan kohteesta säilytetään tavalla, joka ei vaaranna toimijan toiminnan turvallisuutta. Jälkikäteisvalvonta ei saa olla ensisijainen ohjausmekanismi, vaan lain soveltamiseksi tarvitaan riittäviä resursseja

etukäteisohjaamiseen ja neuvontaan. On tärkeää, että kyberturvallisuuden yleisvalvonnassa ja mahdollisessa toimijakohtaisessa sanktioinnissa noudatetaan tarkoituksenmukaisia valvonta- ja sanktiointiperiaatteita valvojatahosta riippumatta, jotta varmistetaan eri toimialojen toimijoiden yhdenmukainen kohtelu.

Valvonnan osalta tulisi täsmentää, miten valvotaan esimerkiksi monialayhtiöitä. Tyypillinen esimerkki kuntapuolen monialayhtiöstä on yhdistetty energia- ja vesiyhtiö. Sen lisäksi kuntayhtymänä toimiva HSY harjoittaa sekä liitteeseen I sisältyvää vesi-huolto- että liitteeseen II sisältyvää jätehuoltotoimintaa. Lakiehdotuksen perusteella ei selviä, valvooko toimintaa tällöin jokaisen harjoitettavan eri toimialan mukainen valvontaviranomainen vai keskitetäänkö valvonta yhdelle taholle. Hajautetussa valvonnassa valvonnan keskittäminen yhdelle taholle tarkoittaisi, että ko. valvojalla ei toisaalta välttämättä olisi kaikkiin toimialoihin liittyvää substanssiasiantuntemusta.

Seuraamusmaksua koskevat huomiot

NIS2-direktiivi mahdollistaa kansallisen liikkumavaran siten, ettei julkishallinnon toimijoille määrätä direktiivin edellyttämiä hallinnollisia sanktioita. Tämä liikkumavara on nyt käytetty ehdotetun lain 37 §:n 2. momentissa. Ko. lain kohta ja sen perustelut jättävät hieman epäselväksi, miten seuraamusmaksua sovelletaan kuntien taseyksikköinä, liikelaitoksina tai osakeyhtiöinä toimiviin toimijoihin. Kuntaliiton näkemyksen mukaan myös kunnat (joutuessaan lain soveltamisen piiriin), yhtä lailla kuin valtion virastot ja hyvinvointialueet, julkishallinnon toimijoina tulee jättää seuraamusmaksu-en ulkopuolelle. Kuntaliitto pyytää tarkentamaan laissa ja sen perusteluissa vielä tätä asiaa.

Kuntaliitto toteaa vielä, että hallinnollinen sanktio on kansalliselle oikeusjärjestelmälle haastava kokonaisuus. Valvovilla viranomaisilla voi tilanteesta riippuen olla epäselvää, onko hallinnollinen sanktio luonteeltaan hallinnollinen vai rikosoikeudellinen seuraamus (KHO on ottanut kantaa tietosuojan hallinnollisiin sanktioihin ja todennut, että hallinnollisen seuraamuksen täyttyessä tulisi rikosprosessin menetelmiä silti noudattaa prosessissa). Kaksinkertaisen rangaistuksen kieltoa (ne bis in idem -kielto) tulisi tarkasti miettiä ja arvioida (hallinnollisten sanktioiden suhde esimerkiksi vahingonkorvausvastuisiin, rikosvastuisiin ja virkavastuuseen). Prosessuaalisesti on tärkeä kiinnittää huomiota valvovan viranomaisen selvittämisvelvollisuuteen sanktiota määrättäessä ja vastaavasti kohteena olevan tahon oikeuksiin.

CSIRT-yksikön tehtäviä koskevat huomiot

-

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Julkisen hallinnon toimialaa koskevia velvoitteita (näillä näkymin TiHL:iin sisällytettävät kyberturvallisuuden hallintatoimenpiteet) ei sovellettaisi kuntiin ja kuntayhtymiin.

Esityksen mukaisesti hyödynnettäisiin paikallishallinnon osalta kansallista liikkumavaraa (vähimmäissoveltamisala). Kuitenkin on huomioitava, että kunnan, kuntayhtymän tai muun kuntatoimijan ollessa CER-direktiivin nojalla määritelty kriittinen toimija, ovat NIS2-direktiivin

mukaiset velvoitteet (automaattisesti) sitä velvoittavia. Ohjauksen osalta tulee huomioida kukin vastuuviranomainen. Julkisen hallinnon toimialan osalta on nimetty keskitetty toimivaltainen viranomainen (Traficom/LVM).

Tiedonhallintalain (TiHL) uusi luku 4a luku määrittelee kyberturvallisuuteen liittyvät velvoitteet ja niiden noudattamisen valvonnan julkishallinnon toimialalla (keskeinen toimiala). Ja riippuen siitä, mitä CER-direktiivin nojalla säädetään, kunnasta tai kuntayhtymästä saattaisi tulla TiHL:n 4a-luvun soveltamisalan alainen. Velvoitteitten koskiessa kuntaa katettaisiin niiden osalta syntyneet mahdolliset kustannukset kunnille. Esityksen mukaisesti: ”Aiheutuvat kustannukset olisi katettava valtion talouden kehyspäätösten ja valtion talousarvion mukaisista määrärahoista”

Tiedonhallintalakia (TiHL) luettaessa NIS2-yleislain rinnalla on hyvä huomioida, että TiHL:n määritelmissä käytetään toimijan sijaan viranomaisen käsitettä. TiHL:ssa säädetyt julkishallinnon toimialan toimijat ovat viranomaisia. Laissa on määritelty (4§) mitä tiedonhallintayksiköt ovat ja mitkä ovat sen velvoitteet. Kuntalain (410/2015) 38 §:n 2 momentin mukaan kunnanhallitus yhdessä kunnanjohtajan kanssa johtavat kunnan toimintaa, hallintoa ja taloutta - toimien lähtökohtaisesti tiedonhallintayksikön johtona (TiHL 4§ 2 momentti - johdon velvollisuudet).

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

-

Vaikutustenarviointia koskevat huomiot

Kyberturvallisuusdirektiivin toimeenpanolla tulee mahdollisesti olemaan vaikutuksia myös kuntien johtamiseen ja talouteen. Nämä vaikutukset voivat kohdistua ja toteutua seuraavasti:

- erilaisten järjestelmien ajantasaisuuden ja tarkoituksenmukaisuuden varmistaminen (järjestelmien päivittäminen/uusiminen)
- kerta- (päivitykset, uushankinnat) ja toistuvat kustannukset (seuranta, ylläpito, mahdolliset lisenssikustannukset); jakautuminen - budjetointi
- tarvittavien tietoteknisten yhteyksien ja integraatioitten huomioiminen eri yhteistyötahoihin (yhteisten pelisääntöjen, käytäntöjen ja politiikkojen läpikäyminen - olemassa olevien sopimusten läpikäynti)

Käsiteltäessä ja valvottaessa kyberturvallisuutta omana kokonaisuutena NIS2-yleislain mukaisesti, kyse on varsin usein uusista tehtävistä, uusine toimintaprosesseineen sekä niiden mukanaan tuomine vastuineen. Tarvittaessa kunnan tulee voida tehokkaasti ja tarkoituksenmukaisesti sisällyttää kyberturvallisuuden vaatimukset sisäisen valvonnan ja kunnan omien riskien hallinnan periaatteisiin. Osaksi kunnan yleistä riskienhallintaa. On varmistuttava, aiheutuuko järjestelyistä kuntatoimijoille merkittäviä kustannuksia (välittömät/välilliset).

NIS2-yleislaki koskettaa erikokoisia ja erityyppisiä kuntia, esimerkiksi kun kunnalla on merkittävä konserni. Vaikutustenarvioinnin osalta ymmärrys ja tietoisuus lain sisällöstä ja sen vaikutuksista ovat merkityksellisiä mm. seuraavista tulokulmista:

- ulkoisen hyökkäyksen ja sisäisen toiminnan synnyttämän riskin käsittely ja hallinta sekä toimintaa tukeva hallintamalli
- kustannusten taustat ja suuruudet riippuvat kunnan koosta sekä kunnan toiminnan painopisteistä ja olemassa olevasta valmiusasteesta
- riskienhallintaa toteutettaessa läpi koko kuntakonsernin, konsernin laajuudesta ja toimialoista riippuen syntyy erilaisia kustannuksia
- resurssien tarve uuden toimintatavan käynnistämiseen/seurantaan

Kunta hankkii tuloja kattaakseen menonsa, joita katetaan erilaisilla tuloilla (pääasiassa veroilla ja valtionosuuksilla). Mikäli lakia kyberturvallisuuden riskienhallinnasta sovelletaan kuntiin silloin, kun kunta harjoittaa liitteissä I ja II mainittua toimintaa liike-laitosmuodossa, taseyksikkönä tai omana toimintana, tarvitaan yksityiskohtaisempi vaikutustenarviointi. Kuntaliiton mukaan toimijoita tulisi olemaan paljon nyt arvioitua enemmän. Jos soveltamisalaa rajoitetaan, on perusteluissa nyt esitetty vaikutustenarviointi oletettavimmin riittävä. NIS2-yleislakia sovellettaessa kuntaan kokonaisuutena korostuu kyberturvallisuuden riskienhallinta osana sisäistä valvontaa.

Muut huomiot ja avoin palaute esityksestä

”Lain 43 § koskien toimijoiden velvoitetta ilmoittaa tietoja valvovalle viranomaiselle ehdotetaan kuitenkin tulevaksi voimaan vasta 1.1.2025 alkaen, mikä antaisi toimijoille ja valvoville viranomaisille siirtymäaikaa toimijaluettelon muodostamisen ja siihen tietojen ilmoittamisen osalta”.

Ko. velvoitteen tehokas toimeenpano edellyttää selkeää ja tehokasta viestintää lain soveltamisalaan kuuluville toimijoille. Viestinnän tulee sisältää tietoa lain soveltamisalaan kuuluvien toimijoiden kriteereistä, toimialan soveltamisalaan kuulumisesta ja ilmoittamisvelvoitteesta. Koska toimijoiden koko voi kasvaa, niin lain soveltamisen kriteeri voi ylittyä myös myöhemmässä vaiheessa. Toimijoiden tiedot voivat myös muuttua ja lakiin kirjattua kahden viikon ilmoitusaikaa valvontaviranomaiselle muutoksista voidaan pitää kohtuuttoman tiukkana. Koska lainsäädäntöön liittyy toiminnan sanktiointi, Kuntaliitto katsoo, että ko. asiassa viestintään tulisi kiinnittää erityistä huomiota.

Pauni Markus
Suomen Kuntaliitto ry

Ylikoski Jari
Suomen Kuntaliitto ry