Keskuskauppakamari

Lausunto

29.11.2023 VN/18157/2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Keskuskauppakamari kiittää mahdollisuudesta lausua luonnoksesta hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi. Kannatamme, että EU:n laajuisesti kyperturvallisuutta parannetaan ja hyviä kyperturvallisuuskäytänteitä kehitetään. Kun uusi kyperturvallisuusdirektiivi NIS2 laajentaa aiempaa soveltamisalaa lisäten uusia toimialoja sääntelyn piiriin, voidaan toivoa, että myös kyberturvallisuuden taso paranee tulevina vuosina.

Direktiivin velvoitteiden noudattaminen parantaa yritysten varautumista. Yrityksille on olennaista, että uudet direktiivistä aiheutuvat velvoitteet ovat toteutettavissa niin, että ne tukevat yrityksen toiminnan jatkuvuutta ja ettei yrityksen varsinaiselle toiminnalle aiheudu kohtuutonta hallinnollista taakkaa. On tärkeää, että yritykset pystyvät itsenäisesti tunnistamaan, milloin NIS-direktiivin mukaiset velvoitteet kohdistuvat sen toimintaan.

Soveltamisalaa koskevat huomiot

NIS2-direktiivin täytäntöönpanon kautta kyperturvallisuuslainsäädännön soveltamisala laajenee Suomessa olennaisesti suhteessa aiempaan.

Sitä miten NIS2-direktiivistä aiheutuvat velvoitteet kohdistuvat erilaisiin ”toimijoihin” tulisi jatkotyössä selventää, sillä termin ”toimija” sisältö on olennainen ja tällä hetkellä ehdotuksessa epäselvä. Se kuitenkin vaikuttaa keskeisesti yritysten varautumiseen ja toteutettaviin riskienhallintajärjestelmiin. NIS2-velvoitteiden soveltuminen konsernin sisäisesti ei ole selvä. On tulkinnanvaraista, tuleeko esimerkiksi konsernin emoyhtiön tai muiden konserniyhtiöiden alkaa toteuttamaan NIS2:n mukaisia velvoitteita, jos jokin konsernin kuuluvista tytäryrityksistä kuuluu NIS2-direktiivin soveltamisalaan ja siihen kohdistuu valvonta- ja raportointivelvoitteita. Jos NIS2-velvoitteet soveltuvat tytäryhtiöön, herää kysymys, voiko riskienhallinnan kybertoiminnot sijoittaa konsernin esikuntaan, jos se ei ole lain tarkoittama toimija. Lainsäädännöllä ei pitäisi estää konserniyhtiöiden mahdollisuutta järjestää tietoturvatoimintojaan haluamallaan tavalla esimerkiksi keskitetysti.

Myös liitteessä II mainittu termi ”kuriiripalvelun tarjoajat” on epäselvä ja se tulisi täsmentää.

Riskienhallintavelvoitetta koskevat huomiot

Ehdotetun kyberturvallisuuden riskienhallintalain 10 §:ssä ehdotetaan säädettäväksi johdon vastuusta tavalla, joka on vieras suomalaiselle yhtiöoikeudelle ja osakeyhtiölain vastuurakenteille. Ehdotuksessa myös näyttäisi sekoittuvan keskenään riskienhallinnan strategiset linjaukset ja operatiivinen toteutus.

Osakeyhtiölain mukaiset toimielimet ovat hallitus, mahdollinen hallintoneuvosto sekä toimitusjohtaja. Toimitusjohtaja hoitaa yhtiön juoksevaa hallintoa. Toimitusjohtajan välittömässä alaisuudessa toimivan johtoryhmän ei ole Suomessa katsottu olevan EU-direktiivien tarkoittama hallinto-, johto- tai valvontaelin. Osakeyhtiön hallituksen yleistoimivaltaan kuuluva velvollisuus huolehtia yhtiön hallinnosta ja sen toiminnan asianmukaisesta järjestämisestä.

Hallituksen yleistoimivallan sekä osakeyhtiön toimielinten jäseniä koskevan huolellisuusvelvollisuuden voidaan katsoa pitävän sisällään myös kyberturvallisuuden riskienhallinnan järjestämiseen liittyvät velvoitteet. Jos direktiivin 20 artiklan täytäntöönpanon katsotaan kuitenkin edellyttävän nimenomaista säännöstä, tulisi ehdotetun 10 §:n 1 momentissa tehdä selkeämpi ero hallituksen strategisen tason linjausten sekä valvontatehtävän ja toimitusjohtajan operatiivisten tehtävien välillä. Toimitusjohtajan alaisuudessa työskenteleviin säännöstä ei tulisi ulottaa.

Keskuskauppakamari pitää lisäksi 10 §:ssä ehdotettua hallituksen osaamiseen liittyviä lakisääteisiä velvoitteita ongelmallisina siitä näkökulmasta, että hallituksen riittävää osaamista ja kokemusta liiketoiminnasta, siihen liittyvistä riskeistä ja niiden hallinnasta (ml. kyberriskien hallinta) tulisi arvioida kokonaisuutena. Hallituksille asetetaan lakisääteisiä osaamisvaatimuksia yhä useampaan eri osa-alueeseen liittyen, mikä jo nyt vaikeuttaa hallitusten jäsenten rekrytointia.

Raportointivelvoitetta koskevat huomiot

Niiden toimijoiden osalta, jotka toimivat monikansallisesti, tulisi selkiyttää sitä, miten kyseisten yritysten muualla EU:ssa tai kolmansissa maissa olevat yksiköt tulisi huomioida NIS2-direktiivin mukaisten raportointivelvoitteiden osalta Suomen lainsäädännön näkökulmasta.

Valvontaa koskevat huomiot

Keskuskauppakamari viittaa edellä esittämiinsä huomioihin ehdotettuun 10 §:ään liittyen ja toteaa, että johdon määritelmää on tarpeen rajata myös ehdotetussa 33 §:ssä. Ehdotettu 33 § vaikuttaa lisäksi olevan direktiivin 32(5) artiklaa olennaisesti ankarampi ilman, että tätä olisi mitenkään perusteltu ehdotuksessa. Direktiivin mukaan toimintakiellon tulisi koskea vain toimintaa velvoitteita rikkoneessa toimijassa, kun taas ehdotetun säännöksen sanamuoto vaikuttaisi mahdollistavan kiellon ulottamisen koskemaan toimintaa minkä tahansa keskeisen toimijan johtotehtävissä. Lisäksi direktiivin mukaan kieltoa tulisi soveltaa vain siihen asti, kun korjaavat toimenpiteet on suoritettu. Ehdotetussa säännöksessä tällaista rajausta ei ole, vaan toimintakielto voisi olla jopa viisi vuotta. Säännöksessä tulisi myös asettaa valvovalle viranomaiselle velvollisuus kuulla kiellon kohteena

olevaa luonnollista henkilöä ennen kiellon asettamista, pelkkä oikeushenkilön kuuleminen ei tältä osin ole riittävää.

Ehdotuksessa lain velvoitteiden valvonta on jaettu useille eri viranomaisille sen mukaan, mistä toimialasta on kyse. Tällöin monien yritysten liiketoiminta voi olla useiden eri viranomaisten valvomaa, mistä voi aiheutua tulkinnallisuutta ja jopa ristiriitaisia neuvoja muun muassa tilanteessa, jossa eri viranomaisten ohjaus ja neuvot ovat erilaisia saman toimijan eri yksiköille. Myös viranomaisvalvonnan jakautuminen useille eri valvoville viranomaisille voi aiheuttaa epävarmuutta seuraamusjärjestelmän ennakoitavuuteen nähden, erityisesti kun pyritään hahmottamaan toimijan johdon vastuuta.

Seuraamusmaksua koskevat huomiot

Termin ”toimija” tulkinnallisuus vaikuttaa myös seuraamusmaksujen hahmottamiseen, sillä seuraamusmaksu määräytyy ehdotuksen mukaan ”toimijan” edellisen tilikauden maailmanlaajuisen vuotuisen kokonaisliikevaihdon mukaan. Tällöin seuraamusmaksun suuruus voi yhtiörakenteesta riippuen vaihdella olennaisesti riippuen siitä tulkitaanko toimijan olevan koko konserni vai yksittäinen yhtiö.

Katsomme, että seuraamusmaksun suuruutta määriteltäessä tulisi ottaa huomioon vain NIS2-direktiivin soveltamisalaan kuuluva toiminta. Tällöin jos vain osa yrityksen toimintaa kuuluu direktiivin soveltamisalaan, tulisi tämä asia huomioida seuraamusmaksua määrättäessä kohtuullistavana tekijänä.

CSIRT-yksikön tehtäviä koskevat huomiot

Ei lausuttavaa.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Ei lausuttavaa.

Verkkotunnusvälittäjiä koskevat huomiot

Ei lausuttavaa.

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ei lausuttavaa.

Vaikutustenarviointia koskevat huomiot

Ehdotuksen vaikutusarviointi on puutteellinen, sillä siinä ei ole käsitelty sitä, että ehdotus toimijan johdosta (ja sen laajuudesta) poikkeaa NIS2-direktiivistä. Muutos vaikuttaisi olennaisesti Suomen vallitsevaan oikeustilaan.

Muut huomiot ja avoin palaute esityksestä

Ei lausuttavaa.

Aalto-Setälä Minna
Keskuskauppakamari