

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Suomen varustamot ry (SV) kiittää mahdollisuudesta lausua otsikossa mainittuun asiaan.

Toimiva ja kustannustehokas merilogistiikka on ulkomaankauppamme elinehto. NIS2-direktiivin tavoitteena on vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa kriittisiksi katsottujen sektoreiden ja toimijoiden osalta. Kyberturvallisuustyö on tärkeää ja SV suhtautuu myönteisesti NIS2-direktiivin tarkoitukseen.

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

SV kannattaa, että NIS2-direktiivin täytäntöönpano ehdotetaan tehtäväksi sen vähimmäistason mukaisesti ja kansallinen liikkumavara täysimääräisesti hyödyntäen. NIS2-velvoitteita pitää voida toteuttaa siten, ettei se aiheuta kohtuutonta rasitetta varsinaiselle toiminnalle vaan tukee toiminnan prosesseja ja niiden jatkuvuus.

Merenkulun kansainvälinen sääntely perustuu Kansainvälisen merenkulkujärjestön IMO:n yleissopimukseen. Varustamoiden riskienhallintaan liittyvistä velvoitteista säädetään SOLAS-yleissopimukseen perustuvassa kansainvälisessä turvallisuusjohtamissäännöstössä (ISM). EU:ssa säännöstö on pantu täytäntöön kansainvälisen turvallisuusjohtamissäännöstön täytäntöönpanosta yhteisössä annetulla Euroopan parlamentin ja neuvoston asetuksella (EY) N:o 336/2006. SV muistuttaa, että merenkulun kansainvälisen luonteen takia on äärimmäisen tärkeää, että NIS2 direktiiviä sovelletaan yhdenmukaisesti eri maiden välillä merenkulun osalta.

Soveltamisalaa koskevat huomiot

SV huomauttaa että nykyisillä tiedoilla ei ole mahdollista arvioida missä määrin NIS2 direktiivi koskee varustamoja ja merenkulkua. Ehdotuksen mukaan toimija merenkulussa on ISM-yhtiö, eli DOC-todistuskirjassa (Document of Compliance) mainittu yhtiö. ”Vesiliikenne: a) Alusten ja satamarakenteiden turvatoimien parantamisesta annetun Euroopan parlamentin ja neuvoston

asetuksen (EY) N:o 725/2004 liitteessä I merenkulun osalta määritellyt sisävesillä, merillä ja rannikoilla matkustaja- ja rahtiliikennettä hoitavat yhtiöt, lukuun ottamatta tällaisten yhtiöiden liikennöimiä yksittäisiä aluksia.”

Yllä mainittuun tulkintaan toimijasta olisi saatava varmuutta kuten myös siitä, mitä “lukuun ottamatta tällaisten yhtiöiden liikennöimiä yksittäisiä aluksia” tarkoittaa käytännössä. Edellä mainittu lause voi vaikuttaa yhtiön koon määrittämiseen ja sen mukaan mikäli toimija on keskeinen tai tärkeä, tai mikäli yhtiö ollenkaan kuuluu soveltamisalaan.

Tarvitaan myös selvyyttä mikäli matkustaja ja rahtiliikennettä hoitavat yhtiöt määritellään pelkästään kokonsa ja vuosiliikevaihdon tai taseen mukaan, vai myös muiden kriteereiden mukaan. Esimerkiksi, kuuluuko merenkulku aina soveltamisalaan toimijan koosta riippumatta, tai vain tietyt yhtiöt, kuten esim. öljy ja polttoainetta kuljettavat alusten yhtiöt. Olisi myös selvennettävä mikäli Valtioneuvoston asetuksella aiotaan säätää että meriliikennettä hoitavat yhtiöt soveltavat direktiiviä koosta riippumatta, kohdan 3§ 3 mukaisesti.

Mikäli alukset eivät kuulu soveltamisalaan olisi tarpeen että valvonta viranomainen tarkentaa alusten ja yhtiön väliset rajapinnat tarkemmin pystytään toimimaan oikein esimerkiksi valvonnan ja poikkemaraportoinnin suhteen.

Mikäli alukset kuuluvat, tai osittain kuuluvat soveltamisalaan, olisi myös selvennettävä mikäli NIS2-velvoitteet kohdistuvatko koko yritykseen, niissä tapauksissa jossa ISM-yhtiö on sisäinen toiminto yrityksessä. Selvennystä pitäisi saada myös tilanteisiin jossa ISM yhtiö vastuut on ulkoistettu kolmannelle osapuolelle, ISM yhtiö sijaitsee toisessa maassa kuin yritys, ISM-yhtiö vastaa useamman yrityksen aluksista samanaikaisesti sekä tapauksista jossa ISM yhtiö vastaa vain osasta jonkun yrityksen aluksista.

Riskienhallintavelvoitetta koskevat huomiot

SV kannattaa esityksessä oleva riittävä liikkumavara, joka mahdollistaisi lain täytäntöönpanoa toimijan olosuhteita huomioon ottaen. Toimijat huomioivat ne haavoittuvuudet, jotka ovat ominaisia toimijan harjoittamalle toiminnalle ja toteuttaa riskienhallintatoimenpiteet siten, että turvallisuuden taso on oikeassa suhteessa riskeihin.

SV pitää myös hyvänä, että Kyberturvallisuuden riskienhallinnan toimintaperiaatteiden ja toimintamallin olisi suositeltavaa perustua ajantasaisiin toimialalla omaksuttuihin parhaisiin käytänteisiin ja standardeihin sekä että toimija voisi luoda kyberturvallisuuden riskienhallinnan toimintamallin itse tai hankkia sen ulkoistetusti. SV kannattaa myös, että riskienhallinnan toimintamalli voisi olla myös osa toimijan laajempaa riskienhallintasuunnitelmaa, jossa huomioidaan myös muita toimintaan kohdistuvia riskejä tai osa muuta turvallisuusvarautumista.

Ottaen huomioon yllä mainittua, sekä sen että valvova viranomainen voi tehdä valvontapäätöksiä, antaa huomautuksia ja varoituksia, päättää keskeisen toimijan luvan tai sertifiointin peruuttamisesta tai johdon toiminnan rajoittamisesta sekä määrätä tuntuvia seuraamusmaksuja, SV pitää tärkeänä, että valvova viranomainen antaa tarkempia määräyksiä toimialallaan. Pyydämme, että määräykset valmistellaan vuorovaikutuksessa toimijoiden kanssa.

Tämän lisäksi SV huomauttaa, että toimijan johdon vastuuseen liittyen esitys toteaa, että toimijan johdolla tulee olla riittävä perehtyneisyys kyberturvallisuuden riskienhallintaan. Tässä yhteydessä riittävä perehtyneisyys määrittäminen on tarpeellista. SV pitää tärkeänä, että valvojan viranomaisen perusteet valvontatoimenpiteille ovat selkeät ja ennakoitavat.

Raportointivelvoitetta koskevat huomiot

SV pitää hyvänä, että poikkeamailmoitukset viranomaisille koskee ainoastaan merkittäviä poikkeamia. SV pitää kuitenkin tarpeellista, että valvoja viranomainen tarkentaa omalla toimialallaan, milloin poikkeama on merkittävä sekä katsoo sen lisäksi että raportoinnin edistämiseksi on hyvä tuottaa poikkeamailmoitukselle, väliraportille sekä loppuraportille valmiita kaavoja, sekä varmistaa mahdollisimman sujuvan ja vähän resursseja vievän ilmoitusmenettelyn.

SV pitää myös tärkeänä tavoitetta, että valvoja viranomainen antaa alustavaa palautetta viranomaisen näkemyksestä poikkeaman merkittävydestä sekä muista poikkeaman hallitsemiseksi tarpeellisista seikoista, ja että valvoja viranomainen sisällyttäisi vastaukseen myös muita tarpeelliseksi katsomiaan seikkoja, kuten yleisiä ohjeita tai neuvoja vaikutuksia lieventävistä toimenpiteistä aina kun se on mahdollista.

Esityksessä todetaan kuitenkin, että valvojan viranomaisen vastaus tulisi antaa viivytyksettä ja mahdollisuuksien mukaan 24 tunnin kuluessa, mutta kuitenkin virka-aikojen puitteissa. Sen lisäksi todetaan, että valvojan viranomaisen on toimitettava ilmoitukset ja raportit CSIRT-yksikölle. CSIRT-yksikkö antaa toimijan pyynnöstä ohjeita tai operatiivisia neuvoja vaikutuksia lieventävien toimenpiteiden osalta.

Ottaen huomioon että toimijat ilmoittavat merkittävistä poikkeamista jotka ovat luonteeltaan vakavia ja että ensi-ilmoitus on tehtävä 24 tunnin kuluessa poikkeaman havaitsemisesta, emme pidä tarkoituksenmukaisena että valvoja viranomainen vastaa poikkeamailmoituksen tehneelle taholle vain virka aikojen puitteissa. SV pitää tärkeänä että valvoja viranomainen varmistaa että ilmoittavalle taholle vastataan, ja tieto välitetään CIRT-yksikölle, 24 tunnin sisällä.

Valvontaa koskevat huomiot

-

Seuraamusmaksua koskevat huomiot

-

CSIRT-yksikön tehtäviä koskevat huomiot

-

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

-

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

-

Vaikutustenarviointia koskevat huomiot

-

Muut huomiot ja avoin palaute esityksestä

SV haluaa mielellään jatkossa osallistua NIS2 liittyvien määräysten kehittämiseen ja lausua niistä.

Ramsay Carolus
Suomen Varustamot ry