

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Valtiokonttori kiittää mahdollisuudesta lausua hallituksen esityksestä kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi. Yleisesti ottaen Valtiokonttorin näkemyksen mukaan valmisteltu esitys on kannatettava ja arvion mukaan se tulee parantamaan niin julkishallinnon kuin kriittisestä infrastruktuurista vastaavien yksityisten toimijoiden kyberturvallisuuskyvykkyksiä.

Soveltamisalaa koskevat huomiot

Julkishallinnon osalta tiedonhallintalain muutokset vaikuttavat tarkoituksenmukaisilta ja on perusteltua, että ne koskettavat julkishallintoa laajasti. NIS2-direktiivin soveltamisalan osalta hallituksen esityksen kirjaukset voivat eräiltä osin olla tulkinnanvaraisia ja Valtiokonttori katsoo, että näitä voisi olla tarpeen vielä tarkastaa ja täsmentää. Hallituksen esityksessä todetaan ”On huomioitavaa, että jos julkinen toimija toimii jollain direktiivin muista toimialoista, se voi kuulua NIS2-sääntelyn piiriin ehdotetun kyberturvallisuuden riskienhallinnasta annetun lain nojalla.” Esimerkiksi Valtiokonttorin kohdalla NIS2-direktiivikin täydessä laajuudessaan voisi olla sovellettavissa, koska virasto toimii myös finanssi- ja vakuutusalan kaltaisissa tehtävissä vastaten valtion velan- ja kas-sanhallinnasta, valtion henkilöstön tapaturmasuojasta sekä korvauksista kansalaisille niissä vahingoissa, joista valtio on vastuussa ja lukuisista muista korvausten maksatustehtävistä.

Riskienhallintavelvoitetta koskevat huomiot

-

Raportointivelvoitetta koskevat huomiot

NIS2-direktiivi ja tiedonhallintalain muutokset tulevat edellyttämään toimijoilta aiempaa kattavammin ja velvoittavammin erilaisia ilmoituksia toiminnassa kohdatuista kyberpoikkeamista. Ilmoitusvelvollisuuden laajentaminen on kannatettavaa ja perusteltua. Muodostuneen tilannekuvan täysimääräinen hyödyntäminen edellyttää kuitenkin myös mahdollisuutta jakaa sitä tehokkaasti ja tarkoituksenmukaisesti. Vallitsevassa tilanteessa on havaittu haasteelliseksi se, ettei esimerkiksi

Kyberturvallisuuskeskus kaikissa tilanteissa voi jakaa tilannetietoa saamatta vahvistusta raportoineelta organisaatiolta. Valtiokonttorin arvion mukaan Kyberturvallisuuskeskuksella voisi olla mahdollisuus salassapitovelvollisuuksien estämättä jakaa tilannetietoa silloin, kun se tapauksesta laaditun riski- ja vaikutusarvion mukaan olisi perusteltua, jotta kyberuhkaan kyetään reagoimaan tilanteen edellyttämällä nopeudella.

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

Hallituksen esityksen mukaan ”Komission arvion mukaan NIS2-direktiivin mukaisilla velvoitteilla arvioidaan olevan ensimmäisten toimeenpanovuosien aikana soveltamisalaan kuuluvan toimijan nykyisiä kyberturvallisuuteen liittyviä IT-kustannuksia keskimäärin 12–22 % korottava vaikutus riippuen siitä, onko velvoitteiden kohteena oleva toimija kuulunut NIS1-direktiivin soveltamisalaan.” Tiedonhallintalaki edellyttää jo nykyisellään riskiperusteista tiedon suojaamista, mutta on nähtävissä, että NIS2-direktiivin mukaiset velvoitteet tulevat edellyttämään lisäresursointia. Tämän resursoinnin kohdentaminen taloudellisesti vaikeassa tilanteessa voi olla haastavaa.

Kangas Heikki
Valtiokonttori - Riskienhallinta ja tietoturvallisuus