Verohallinto

Lausunto

29.11.2023 VH/5265/00.04.05/2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Verohallinto pitää NIS2 -direktiivin tavoitteita ja tarkoituksia hyvinä ja kannatettavina. Tavoitteet edistävät mm. keskustason julkishallinnon toimijoita kyberturvallisuuden kehittämisessä ja yhdenmukaisen korkean tietoturvatason saavuttamisessa. Lisäksi sääntelyllä edistetään sen soveltamisalaan kuuluvien viranomaisten keskinäistä yhteistyötä sekä Euroopan Unionin tasolla kyvykkyyttä varautua yhteiskunnan toimintaa vaarantaviin uhkiin.

Soveltamisalaa koskevat huomiot

NIS2 -direktiivissä tietoturvallisuutta koskevat velvoitteet laajenevat koskemaan jul-kishallintoa, mikä on perusteltua ottaen huomioon yhteiskunnan keskeisten toimintojen turvaaminen, julkishallinnon hyödyntämien verkko- ja tietojärjestelmien moninaisuus ja niissä käsiteltyjen tietosisältöjen laajuus, kriittisyys ja merkityksellisyys niin yhteiskunnallisella kuin yksilön tasolla.

Verohallinto pitää tärkeänä, että NIS2 velvoitteiden täytäntöönpanossa otetaan huomioon myös CER direktiivin mukaiset velvoitteet siten, että sääntelyiden soveltamisalaan kuu-luvien asioiden ja toimijoiden kohdalla vaatimusten toteuttaminen ei aiheuta päällekkäistä työtä.

Riskienhallintavelvoitetta koskevat huomiot

Ehdotettujen riskienhallinnan toimintamallin ja riskienhallintatoimenpiteiden toimenpidekokonaisuuksien toteuttaminen aiheuttaa Verohallinnoissa jonkin verran työtä nykyisten kyvykkyyksien kartoittamiseksi ja mahdollisten puuttuvien toimenpiteiden toteuttamiseksi.

Verohallinto pitää erityisen tärkeänä, säädöstason vaatimuksilla edistetään niin johdon kuin koko henkilöstön osaamista kyberturvallisuuden alalla.

Raportointivelvoitetta koskevat huomiot

Verohallinto pitää raportointivelvoitetta hyvänä. Verohallinnossa on vakiintunut toimintatapa tietosuojasääntelyn mukaisten tietoturvaloukkausten ilmoittamisessa Tietosuojavaltuutetulle.

Ehdotettu kolmivaiheinen ilmoitusjärjestelmä on selkeä mutta se aiheuttaa jonkin verran työtä ilmoittamista koskevien prosessien ja menettelyiden määrittelyssä ja ympärivuoro-kautisen valvonnan järjestämisessä sekä menettelyn toteuttamisessa laissa säädetyissä aikarajoissa.

Viranomaisille laissa säädetyt tietoturvallisuus- ja tietosuojavelvoitteet ovat lisääntyneet viime vuosina. Nämä velvoitteet edellyttävät viranomaisilta poikkeaminen havainnoinnin, tunnistamisen ja korjaamisen lisäksi myös päivystyksen järjestämistä sekä dokumentointia ja raportointia valvontaviranomaisille määräajassa. Valtion tuottavuusohjelman valmistelussa pitää lisätä viranomaisten kehyksiin myös nämä lisätyöt. Tällä varmistetaan se, että viranomainen voi perustehtävän lisäksi hoitaa myös nämä muut kuin perus-tehtävään kuuluvat velvoitteet tehokkaasti.

Verohallinto pitää tärkeänä, että ennen ilmoittamismenettelyn aloittamista ilmoittamisesta vastuussa oleville tahoille annetaan menettelyohjeet siitä, miten ilmoitukset annetaan teknisesti oikein. Menettelyn suunnittelussa tulisi hyödyntää Tietosuojavaltuutetun kokemuksia tietoturvaloukkaus ilmoitusten vastaanottamisessa. Teknisen ratkaisun tulisi olla sellainen, että ilmoittaja saa myös itse tallennettua lähetetyn ilmoituksen eikä sitä tarvitse pyytää valvovalta viranomaiselta erikseen.

Valvontaa koskevat huomiot

Verohallinto pitää ehdotettuja valvontamenettelyitä selkeänä.

Ehdotettu sääntely pitää sisällään myös valvontaviranomaisen tarkastusoikeuden ja oi-keuden asettaa viranomaiselle velvollisuus teettää itse kyberturvallisuuden riskienhallin-taan kohdistuva arviointi. Verohallinto pitää tärkeänä, että valvontaviranomainen antaisi linjauksen niistä tilanteista ja kriteereistä, joiden vallitessa arvioinnin teettämisvelvoite asetetaan kuten esimerkiksi sellaisista seikoista, joita pidetään olennaisena ja vakavana laiminlyöntinä velvoitteiden noudattamisessa.

Ehdotettu sääntely sisältää myös valvontaviranomaisen oikeuden velvoittaa viranomainen julkistamaan em. laiminlyönteihin liittyvät tiedot. Julkistamistilanteissa tulee arvioida miten näissä tilanteissa suojataan asiaan mahdollisesti liittyvät salassa pidettävät tiedot.

Seuraamusmaksua koskevat huomiot

Verohallinto pitää ehdotettuja seuraamuksia ja tehosteita tarkoituksenmukaisina eikä pidä tarpeellisena kohdistaa seuraamusmaksua viranomaisiin.

Ehdotetun lain kyberturvallisuuden riskienhallinnasta 38 §:n mukaisesti seuraamusmaksulautakunnalla olisi tiedonsaantioikeus, jonka mukaisesti se saisi salassapitosäännösten estämättä tehtäviensä hoidon kannalta välttämättömät tiedot. Ehdotetun säännöksen perusteluiden mukaan lautakunta hankkisi tämän nojalla tiedot asiaan vaikuttavista seikoista seuraamusmaksun määräämiseksi tai määräämättä jättämiseksi. Seuraamusmaksun määrä on perustuisi prosenttiosuuteen liikevaihdosta tai se olisi euromääräinen. Silloin, jos ehdotettua tiedonsaantioikeutta on tarkoitus soveltaa myös seuraamusmaksun suuruuden määrittämiseen esimerkiksi pyytämällä Verohallinnosta yritysten liikevaihtoa koskevia tietoja, olisi tästä hyvä mainita ainakin esityksen perusteluissa.

CSIRT-yksikön tehtäviä koskevat huomiot

Verohallinto pitää hyvänä ratkaisuna sitä, että Kyberturvallisuuskeskus jatkaa toimintaa CSIRT-yksikkönä sekä keskeisenä yhteyspisteenä tietoturvaloukkausten osalta.

CSIRT-yksikkö koordinoisi kyberturvallisuuden riskienhallinnasta annetun lain 22 §:n mukaisia kyberturvallisuuden vapaaehtoisia jakamisjärjestelyitä, joihin niin yksityisen kuin julkishallinnon organisaatioiden on mahdollista osallistua. Kyberturvallisuustietojen jakamisjärjestelyn osapuolilla tulisi olla mahdollisuus sopia menettelyistä ja toimintatavoista jaettujen tietojen käsittelemisessä tai tietojen luottamuksellisuuden osalta. Osallistuminen vapaaehtoiseen jakamisjärjestelyyn vaatii julkisen hallinnon organisaatiolta tarkempaa harkintaa ja arviointia menettelytapojen määrittämiseksi ja tietojen luottamuksellisuuden varmistamiseksi tiedonsaantioikeuksien ollessa sellaisenaan kohtuullisen laajoja jakamisjärjestelyihin osallistuvien tahojen välillä.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

-

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

-

Vaikutustenarviointia koskevat huomiot

-

Muut huomiot ja avoin palaute esityksestä

-

Konow von Taito
Verohallinto