HUS-Yhtymä

Lausunto

28.11.2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Kiitämme mahdollisuudesta lausua luonnoksesta hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi. Lakiesityksen päämäärä on tärkeä ja myös HUSin toimialla (sairaanhoito) keskeinen hoidon jatkuvuuden ja potilaiden yksityisyyden turvaamiseksi.

Tavoite kehittää kyberturvallisuutta kansallisella ja EU-tasolla NIS2 direktiivin kautta on lähtökohtaisesti kannatettava. Esitys sisältää organisaatiotoimijoille operatiivisia ja teknisiä toimenpiteitä kyberturvallisuuden kehittämiseksi. Tämä linjaa toimintaprosesseja ja vauhdittaa kyberturvallisuuden edistämistä tavoitteelliseen suuntaan mutta edellyttää toki henkilö- ja/tai taloudellisia resursseja.

Hallituksen esityksen taloudelliset vaikutukset säädöksen määräyksiä toteuttaville toimijoille on arvioitu puutteellisesti.

Soveltamisalaa koskevat huomiot

Valvontaviranomaisia voi olla samalle organisaatiolle useita yhtaikaa (julkishallinto, terveydenhuolto, lääkintälaitteet). Esityksestä ei saa kovin tarkkaa käsitystä siitä, koskeeko soveltaminen aina koko organisaatiota, vai koskeeko se organisaatiossa sitä osaa, joka tekee jotain tiettyä toimintoa. Esim. koskeeko julkisen terveydenhuollon osalta Liikenne- ja viestintäviraston suorittama valvonta koko organisaatiota vai viranhaltijoiden toimintaa julkisen vallan ja verovarojen käyttäjinä. Samoin koskeeko Valviran valvonta koko organisaatiota (mukaan lukien esimerkiksi henkilöstöhallinnon ja taloushallinnon) vai nimenomaisesti terveydenhuoltoon liittyviä tehtäviä.

Raportointivelvoitteesta säädetään NIS2-direktiivin 23 artiklassa. Keskeisten ja tärkeiden toimijoiden tulee raportoida merkittävästä poikkeamasta CSIRT-yksikölle tai toimivaltaiselle valvovalle viranomaiselle. Valvontavastuun jakautuminen tilanteessa, jossa valvontaviranomaisia voi olla

samalle organisaatiolle useita samanaikaisesti vrt. edellytys, että vakavista tietoturvaloukkauksista on ilmoitettava ennakkotieto 24 tunnin sisällä niiden havaitsemisesta valvontaviranomaiselle ja tarvittaessa muille asianosaisille, vaatii suunnittelua. Asetettuja velvoitteita olisi hyvä selventää ja tarkentaa (ks. myös jäljempänä).

Riskienhallintavelvoitetta koskevat huomiot

Laki kyberturvallisuuden riskienhallinnasta 10§ velvoittaa organisaation johdolle riittävän koulutuksen kyberturvallisuuden riskienhallintaan. Tähän ei anneta kovinkaan tarkkaa kuvausta perustelutekstissä ja herää kysymys, antaako valvova viranomainen asiasta määräyksiä ja jos antaa, miten pidetään huoli siitä, että niiden organisaatioiden, joita valvoo usea viranomainen, johto saa ristiriidattoman määräyksen riittävästä koulutustasosta.

Raportointivelvoitetta koskevat huomiot

Laki kyberturvallisuuden riskienhallinnasta, 13§: Loppuraportissa vaaditaan ilmoittamaan juurisyyn tyyppi. On epäselvää, mitä tarkoitetaan juurisyyn tyypillä ja onko julkaistu virallinen juurisyykategoria, jonka mukainen luokittelu on otettava käyttöön.

IT-ympäristöt on tyypillisesti toteutettu alihankintaketjujen avulla. Kun tietoturvapoikkeama kohdistuu tietoteknisten palvelujen toimittajaan, on odotettavissa viranomaisilmoituksia sekä palveluntarjoajalta, että sen asiakkailta, eli sama tietoturvatapahtuma voi aiheuttaa suuren määrän viranomaisilmoituksia eri valvoville viranomaisille. Ensi-ilmoituksien osalta näissä tapauksissa annettu aikaraja voi olla ongelmallinen, koska tiedon välittyminen alihankintaketjussa raportointivelvollisuuden alaiselle organisaatiolle voi kestää.

Raportointivelvoitteen piirissä olevilla organisaatioilla tulisi olla yksi kansallinen raportointikanava, johon poikkeamasta ilmoitetaan ja josta tieto leviää kaikille tarvittaville viranomaisille ja selkeä formaatti tähän. Jos yhteistä raportointikanavaa ei ole, valvottava organisaatio voi joutua varmuuden vuoksi lähettämään poikkeamailmoituksen aina usealle viranomaiselle.

Keskeisten ja tärkeiden toimijoiden tulee raportoida merkittävästä poikkeamasta Kyberturvallisuuskeskukselle 24 tunnin sisällä havaitsemisesta. Muutoinkin jo haasteellisessa rahoitusasemassa oleville sosiaali- ja terveydenhuollon toimijoille tämä voi olla iso haaste. Jos organisaation jollain toiminnolla ei ole ympärivuorokautista toimintaa, voidaan havaintoon reagoida vain ns. virka-aikana, sisäisen toimijoiden ja toimittajien tiedonkulun sujuvuus jne.

Valvovien viranomaisten toiminta ei ole toistaiseksi ollut ympärivuorokautista. Siksi 24 tunnin ensi-ilmoitusvelvoite on ylimitoitettu, sillä se edellyttää merkittävää järjestelyä IT-palvelujen toimintaketjussa päivystysaikaan, jotta saadaan ilmoitus tehtyä, mutta ilmoitusta ei kuitenkaan lueta ennen arkea. Vertaa yleinen tietosuoja-asetus, jossa ilmoitusvelvollisuus on 72 tuntia.

Valvontaa koskevat huomiot

Hallituksen esityksen mukainen tapa jakaa valvontavastuu usealle viranomaiselle johtaa tilanteeseen, jossa HUS on kolmen valvontaviranomaisen valvontavastuulla (Valvira, Liikenne- ja viestintävirasto ja Fimea). Esityksestä ei saa selkeää käsitystä siitä, miten kyseisten viranomaisten valvontavastuut rajataan siten, ettei synny päällekkäistä valvontaa tai vastaavasti jää valvonnan ulkopuolisia osa-alueita. Varsinkin, kun sekä organisaation johto, että moni tekninen ratkaisu, kuten käyttäjähallinta, työasemapalvelut tai tietoliikenneverkkoratkaisut vaikuttavat kaikkiin organisaation toimialoihin, on epäselvää, minkä valvovan viranomaisen vastuulle kuuluu näiden yhteisten osa-alueiden hallintatoimien osalta valvontavastuu. Hallituksen esitys itsekin kritisoi sivulla 97 esityksen tilannetta, jossa häiriöiden raportointi on hajautettu useille viranomaisille.

Kyberturvallisuuden riskienhallintaa koskevan lain 43§: IP-osoitealueet on hieman epäselvästi ilmaistu. Perinteiset IP-osoitealueet, jotka on myönnetty toimijan omalle kiinteälle verkolle, on helppo ilmaista. Sen sijaan IP-osoitteiden ilmoittaminen tuottaa hankaluuksia organisaatioille, jotka käyttävät pilvipalveluja palvelujensa tuottamiseen. Osoitteet voivat muuttua useammin kuin omien kiinteiden verkkojen osoitteet, joten ilmoituskäytännön tulee olla yksinkertainen, mieluiten automatisoitu rajapinta. Ilman kyseistä mekanismia, lakia ei tule tulkita koskemaan pilvipalvelutekniikoin tuotettavia palveluja.

Laki kyberturvallisuuden riskienhallinnasta 34§: Toinen momentti on epäselvä: tarkoitetaanko toisen valtion valvontaviranomaista, joka tekee Suomen tietosuojavaltuutetulle? Jos näin, niin miten tämä eroaa 1. momentista? Vai tarkoittaako tämä sitä, että valvovan viranomaisen kuuluu tehdä ilmoitus tietosuojavaltuutetulle silloinkin, kun ei ole toimivaltainen?

Keskeisiin toimijoihin olisikin sovellettava kattavaa valvontajärjestelmää, johon kuuluu etukäteis- ja jälkikäteisvalvonta, ja tärkeisiin toimijoihin olisi sovellettava kevyttä valvontajärjestelmää, johon kuuluu vain jälkikäteisvalvonta. Tärkeitä toimijoita ei tulisi siten NIS2-direktiivin nojalla vaatia raportoimaan valvovalle viranomaiselle järjestelmällisesti kyberturvallisuusriskien hallintatoimenpiteiden noudattamista, vaan valvovan viranomaisen olisi tärkeiden toimijoiden osalta harjoitettava yleisen valvonnan sijasta jälkikäteisvalvontaa. -> Esityksestä ei saa selkeätä kuvaa siitä, kuinka valvonta toteutettaisiin käytännössä ja mitä se pitää sisällään tai miten vältetään esim. päällekkäiset valvontarakenteet tilanteissa, joissa on useita valvovia viranomaisia.

Seuraamusmaksua koskevat huomiot

Ei ole.

CSIRT-yksikön tehtäviä koskevat huomiot

Termi CSIRT on englanninkielinen lyhenne, eikä sovi siten Suomen julkishallinnon yksikön nimeksi. Termiä ei ole myöskään avattu eikä määritelty lain kyberturvallisuuden riskienhallinnasta 2§:n määritelmäluettelossa.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Tiedonhallintalain 4 luvusta suuri osa tekstistä on samaa kuin esitetyssä laissa kyberturvallisuuden riskienhallinnasta. Koska on organisaatioita, joita koskee molempien lakien säätely, olisi selkeämpää, että tiedonhallintalaissa viitattaisiin lain kyberturvallisuuden riskienhallinnasta määräyksiin ja eriteltäisiin vain ne asiat selkeästi, jotka ovat täydennyksiä lakiin kyberturvallisuuden riskienhallinnasta tai poikkeavat siitä. Nykymuotoisesta esityksestä on vaikea saada käsitystä, miten nämä lait poikkeavat toisistaan ja miten niiden poikkeavat vaatimukset koskevat organisaatioita, joita koskee molempien lakien määräykset. Tiedonhallintalain uutta lukua koskevat samat terminologiset ongelmat kuin lakia kyberturvallisuuden riskienhallinnasta.

Verkkotunnusvälittäjiä koskevat huomiot

Ei ole.

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ei ole.

Vaikutustenarviointia koskevat huomiot

Ei ole.

Muut huomiot ja avoin palaute esityksestä

1) Käytettyyn terminologiaan olisi syytä kiinnittää huomiota. Lait kohdistuvat organisaatioihin, jotka joutuvat noudattamaan muitakin lakeja. Lisäksi kansainvälisiin standardeihin liittyy oma vakiintunut sanastonsa. Turvallisuuskomitean sivustolta löytyy myös kyberturvallisuuden sanasto. Jotta vältettäisiin sekaannuksilta, olisi parasta, että käytettäisiin mahdollisimman johdonmukaisesti termejä.

Laissa kyberturvallisuuden riskienhallinnasta käytetään termiä ”poikkeama” tarkoittamaan ”tietoturvahäiriötä” tai ”tietoturvapoikkeamaa”. Sanaa käytetään kansainvälisissä ISO-standardien mukaisissa hallintajärjestelmissä tarkoittamaan myös määräyksestä tai sovitusta käytännöstä poikkeamista ilman, että tapahtumaan liittyy häiriötä. Laissa sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023) käytetään tätä termiä merkityksessä, jossa poiketaan määräyksistä, jotka koskevat järjestelmän olennaisia tietoturvavaatimuksia. Hallituksen esitystä tekee epäselväksi myös se, että esitetyssä muutoksessa kyseisen lain 90§:ään käytetään termiä ”tietoturvallisuuden häiriö” sekä ”tietoturvallisuuteen liittyvä häiriö” samassa merkityksessä, jossa tiedonhallintalain ja kyberturvallisuuden riskienhallinnan lain kohdalla käytetään termiä poikkeama. Käsitteiden yhdenmukaistaminen parantaisi lakien yhteentoimivuutta.

Organisaatioissa, joissa on käytössä kansainvälisiin ISO9001, ISO27001 tai vastaavia hallintajärjestelmiä, tulee valittu termi aiheuttamaan sekaannuksia ja hämmennystä. Olisi parempi korvata lakiesityksissä termi ”poikkeama” termillä ”tietoturvahäiriö” ja jos tämä ei jostain syystä voi onnistua, termillä ”tietoturvapoikkeama”.

Termi ”tietoturvaloukkaus” on Yleisen tietosuoja-asetuksen käytössä erityisesti henkilötietoihin liittyvä termi. Koska lain kyberturvallisuuden riskienhallinnasta §19 ja §23 tietoturvaloukkausten havainnointipalvelu ei ole nimenomaisesti tietosuojan varmistamiseksi toteutettava palvelu, termi tulee aiheuttamaan hämmennystä. Tässä yhteydessä voisi hyvin käyttää esim. ”tietoturvahäiriöiden havainnointipalvelua” tai ”tietoturvapoikkeamien havainnointipalvelua”, joista ei synny tätä mielleyhtymää ja siitä mahdollisesti syntyviä väärinkäsityksiä.

2) Laki kyberturvallisuuden riskienhallinnasta 22§ on mainio pykälä, koska se selkiyttää julkishallinnon osallistumista ISAC-toimintaan. Julkisuuslain 24.1§:n 7k. kieltää lähtökohtaisesti turvajärjestelyistä tiedon antamisen, mutta tällä lailla saadaan hyvä pohja yhteistyöverkostojen (jakamisjärjestelyjen) toiminnalle. Nykyisestä muotoilusta tulee sellainen vaikutelma, että organisaatioiden halutaan vaihtavan tietoja akuuteista uhista ja tapahtumista, mutta ei haluta mahdollistaa jakamisjärjestelyyn liittyneille organisaatioille keskinäistä keskustelua ja parannusten pohdintaa liittyen lain 8§:n mukaisesta riskienhallinnan toimintamallista tai 9§:n mukaisista hallintatoimenpiteistä. Jotta jakamisjärjestelyistä saataisiin paras hyöty, tulisi mahdollistaa myös yhteinen sparraus alan hallintatoimenpidekäytäntöjen jakamiseen ja niistä keskusteluun ja tämä olisi hyvä kirjata suoraan lakiin.

Karvo Jouni
HUS-Yhtymä