Senaatti-kiinteistöt
Tomi Flink

Lausunto

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Yleisellä tasolla direktiivin tavoite on tärkeä ja tarkoitus asianmukainen.

Soveltamisalaa koskevat huomiot

Pidämme soveltamisalaa ja sen rajauksia perusteltuina.

NIS2 direktiivi eivätkä sen kansalliset täytäntöönpanosäännökset koske maanpuolustuksen toimijoita, mistä johtuen Puolustuskiinteistöt -liikelaitos ei kuulu säännösten soveltamisalaan, vaikka Puolustuskiinteistöt muutoin onkin osa julkishallintoa ja myös kyberturvallisuuden näkökulmasta kriittinen toimija. Direktiivin lähtökohtana on, että maanpuolustusta palvelevat toimijat huolehtivat kyberturvallisuudestaan itsenäisesti eivätkä voi asemastaan johtuen osallistua haavoittuvuuksien ja käytänteiden jakoon muiden toimijoiden kanssa. Vaikka Puolustuskiinteistöt direktiivin soveltamisalaan säädettäisiin kuuluvankin, jäisi säännösten sovellettavuus joka tapauksessa Puolustuskiinteistöjen osalta vajaaksi, koska valvovilla viranomaisilla ei olisi tiedonsaantioikeutta mm. maanpuolustuksen tai kansallisen turvallisuuden vuoksi turvallisuusluokiteltuihin tietoihin.

Riskienhallintavelvoitetta koskevat huomiot

Yleisvelvoite huomioida tunnistaa, arvioida ja hallita kyberturvallisuuteen liittyviä riskejä on tärkeä ja pykälä muotoiltu sinänsä asiallisesti.

Ongelmana ovat ulkopuolisten toimittajien ympäristöt, jotka yhä useammin ovat pilvipalvelupohjaisia ja joihin KATAKRI-kehys ei tällöin kovinkaan hyvin sovellu niiden arviointiin.

Muita työkaluja ovat toimittajien mahdolliset yritysturvallisuustodistukset ja voimassa olevat ISO 27001 -sertifioinnit.

Kiinnitämme huomiota myös siihen, että poikkeusoloissa operaattoreita koskee oma lainsäädäntönsä, jonka mukaan liikenne- ja viestintäministeriöllä on oikeus ohjata teleoperaattoreiden toimintaa. Lainsäädännön valmistelussa tulee selvittää mahdolliset ristiriidat teleoperaattoreita koskevan lainsäädännön kanssa ja huomioida viranomaisten välinen yhteistyö ja toimivallat myös poikkeusoloissa.

Kyberturvallisuuden riskienhallinnan toimintamallissa ja siihen perustuvissa hallintatoimenpiteissä on säädettäväksi esitetyn lain 9 §:n mukaan huomioitava ja ylläpidettävä ajantasaisena vähintään:

1) kyberturvallisuuden riskienhallinnan toimintaperiaatteet ja riskienhallinnan toimenpiteiden vaikuttavuuden arviointi;

2) viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet;

3) viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus sekä tarvittavat menettelyt haavoittuvuuksien käsittelyyn ja julkistamiseen;

4) toimitusketjun toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt;

5) omaisuudenhallinta ja turvallisuuden kannalta tärkeiden toimintojen tunnistaminen;

6) henkilöstöturvallisuus ja kyberturvallisuuskoulutus;

7) pääsynhallinnan ja todentamisen menettelyt;

8) salausmenetelmien käyttämistä koskevat toimintaperiaatteet ja menettelyt sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttöön;

9) poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi;

10) varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan jatkuvuuden hallinta ja tarvittaessa suojattujen varaviestintäjärjestelmien käyttö toimijan toiminnassa;

11) perustason kyberhygieniakäytännöt toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi; sekä

12) toimenpiteet viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön ja tilaturvallisuuden sekä välttämättömien resurssien varmistamiseksi.

Näiden sisällöllisten vaatimusten osalta lausumme alakohdittain seuraavaa:

Kohdat 1-3 ovat ainakin osittain päällekkäisiä vaatimuksia.

Kohdassa 4 puhutaan toimitusketjun toimittajien tuotteiden ja palvelujen yleisestä laadusta. Sanamuodon voi ymmärtää niin, että siinä edellytettäisiin palveluntuottajan toiminnan laadukkuuden arviointia yleisesti (toimittajatasolla). Sen enempää direktiivistä kuin hallituksen esityksestäkään ei tällä hetkellä saa asiaan tarkempaa ohjeistusta, mutta vaatimuksella lienee tarkoitettu kriittisellä toimijalla käytössä olevien tuotteiden ja palvelujen yleistä laatua ts. tarkastelua ei tarvitsisi ulottaa sellaisiin palveluntuottajan palveluihin, joita toimija ei käytä. Ehdotamme sanamuotoa selkeytettäväksi tältä osin.

Kohdassa 5 käytetty termi omaisuudenhallinta on tulkinnanvarainen. Laajasti ymmärrettynä sillä voidaan tarkoittaa kaikkea organisaation omaisuutta, mutta suppeasti tulkittuna henkilöstön hallussa olevan omaisuuden, kuten työvälineiden, hallinnoinniksi. Samoin sana ”turvallisuus” esiintyy tässä kohdassa ilman kyber -etuliitettä, jolloin sen sisältö laajenisi merkittävästi. Kohta vaatii täsmentämistä.

Kohdassa 10 käytetään termiä kriisinhallinta, joka esiintyy lainsäädännössämme varsin eri merkityksessä (sotilaallinen- tai siviilikriisinhallinta). Sanamuotoa on syytä muokata.

Raportointivelvoitetta koskevat huomiot

Viranomaisille tehtäville poikkeamailmoituksille laissa asetettavien aikamääreiden (11- 13 §:t ja tiedonhallintalain 18 d §) saavuttaminen edellyttää toimijoilta käytännössä jonkinlaista 24/7 järjestelyä, jolla on sekä henkilöstö että kustannusvaikutuksia. Päivystysmenettelyn lisäksi on luotava ja ylläpidettävä kyvykkyys tehdä verkoissa ja järjestelmissä poikkeamahavainnointia ja on oltava osaamista arvioida ja analysoida poikkeamia. Tämä on etenkin haasteellista LVIS/RAU-verkkojen ja järjestelmien kyberturvallisuuden osalta. Mikäli poikkeama havaittaisiin esimerkiksi perjantaina illalla, tulisi ensi-ilmoitus alustavine tietoineen olla annettuna lauantai-iltaan mennessä ja jatko-ilmoitus maanantaina. Jatkoilmoituksessa edellytetään jo vaikutustenarviointia, jolloin vastaaminen edellyttää selvitystoimenpiteitä ja tilannearviota tehtäväksi mahdollisesti siis jo viikonlopun aikana. Säännös vastaa näiltä osin direktiiviä, joten sen sisältöön ei kansallisesti ole näiltä osin mahdollista vaikuttaa.

Säännöksen soveltamisala on rajattu vain merkittäviin poikkeamiin (ja huomattaviin vaikutuksiin). Esitettävän uuden lainsäädännön sisältämistä rangaistus- ja vastuusäännöksistä johtuen pidämme tärkeänä, että valvova viranomainen antaa tarkempaa ohjausta siitä, milloin poikkeaman merkittävyyskynnys ylittyy.

Vaatimus poikkeaman väliraportoinnista perustuu suoraan direktiiviin, mutta hallituksen esityksen perusteluista saa kuvan, että poikkeaman pitkäkestoisuudella tarkoitetaan itse poikkeaman käsilläolon sijaan sitä, että poikkeaman käsittely on kesken vielä kuukauden kuluttua jatkoilmoituksen antamisesta. Tämä tulkinta ei perustu suoraan direktiivin sanamuotoon. Poikkeaman käsillä olo ja sen käsittelyn keskeneräisyys ovat kaksi eri asiaa. Pitkäkestoinen yli 1kk kestävä poikkeama lienee kohtalaisen harvinainen, mutta poikkeama, jonka vaikutuksia arvioidaan vielä kuukauden kuluttua, lienee yleinen. Näkemyksemme mukaan oma-aloitteinen

väliraportointivelvollisuus tulisi rajata ensin mainittuihin tilanteisiin eli joissa poikkeustilanne on edelleen päällä.

14 §:n ja tiedonhallintalain 18 g §:n mukaiset raportointivelvoitteet muille kuin viranomaisille on jostain syystä kirjoitettu kansallisessa säännöksessä hieman eri sanamuodoin kuin direktiivissä. Kyberuhkan hallitsemiseksi käytettävillä toimenpiteillä tarkoitetaan direktiivissä ja hallituksen esityksen perustelujen mukaan myös kansallisessa laissa toimenpiteitä, joita palvelujen käyttäjät voivat [itse] toteuttaa vaikutusten hallitsemiseksi ja mitigoimiseksi. Näkemyksemme mukaan säännöksen tekstiä olisikin syytä täsmentää vastaamaan paremmin perusteluja ja direktiiviä, koska nyt sanamuodosta saa kuvan, että toimijan on tarjottava jonkinlaista vahinkojen välttelypalvelua.

Valvontaa koskevat huomiot

Esityksen mukaisen 9 §:n ja vastaavasti tiedonhallintalain 18 c §:n mukaan valvova viranomainen voi säännöksen mukaan toimialallaan antaa tarkempia teknisiä määräyksiä:

1) kyberturvallisuuden riskienhallinnan toimintamallissa huomioitavista osa-alueista ja riskienhallinnan ja viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden hallinnan menettelyistä;

2) kehittämisen ja ylläpidon sekä haavoittuvuuksien käsittelyn menettelyistä;

3) omaisuudenhallinnasta ja toimintojen tärkeysluokittelun perusteista;

4) henkilöstöturvallisuuden, kyberturvallisuuskoulutuksen, poikkeamien havainnoinnin ja hallinnan sekä jatkuvuuden hallinnasta;

5) pääsynhallinnan, todentamisen ja salauksen menetelmistä;

6) perustason kyberhygieniakäytännöistä, joilla varmistetaan viestintäverkko- ja tietojärjestelmäturvallisuuden perusluonteiset hallintatoimenpiteet;

7) viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön, tilaturvallisuuden ja välttämättömien resurssien hallintatoimenpiteistä.

Asetuksenantovaltuudet ovat pääpiirteissään asianmukaiset.

Kyberhygianiakäytäntöjä (6-kohta) ei kuitenkaan ole määritelty laissa erikseen. Myöskään hallituksen esityksen ko. pykälän yksityiskohtaisissa perusteluissa ei ole tätä määritelmää, vaan se löytyy yleisestä osiosta viittauksella direktiivin johdanto-osaan. Määritelmä olisi syytä nostaa esiin myös säännöksen yksityiskohtaisiin perusteluihin. Kyberhygieniakäytännöillä tarkoitetaan yleisiä hyviä tietoturvatoimenpiteitä, joilla varmistetaan järjestelmien, ohjelmien ja palveluiden turvallisen käytön perustaso. Kyberhygieniakäytännöillä tarkoitettaisiin perustason teknisiä ja muita toimenpiteitä kohdassa kuvattujen kohteiden turvallisuuden varmistamiseksi. Kyberhygieniakäytännöt voisivat sisältää muun muassa viestintäverkon rakenteellista turvallisuutta, haitallisen liikenteen havainnointia ja estämistä, toimintojen jäljitettävyyttä ja monitorointia, laitteiden ja ohjelmistojen turvallista konfigurointia, ohjelmistojen päivityksiä, kattavaa ja

luotettavaa tunnistamista sekä käyttäjien osaamisen parantamista ja tietoisuuden lisäämistä. Perustason kyberhygieniakäytäntöihin voidaan lukea esimerkiksi luottamattomuuden periaate (zero-trust), ajantasaiset ohjelmistopäivitykset, laitteiden ja ohjelmistojen turvallinen konfigurointi, verkon segmentointi, identiteetin- ja pääsynhallinta sekä käyttäjien osaamisen parantaminen ja tarvittaessa viestintäverkkojen ja tietojärjestelmien turvallisuutta parantavien teknologioiden käyttöönotto tarpeellisilta osin.

Kiinnitämme huomiota myös terminologiaan ja käännösten johdonmukaisuuteen: direktiivin virallisessa suomenkielisessä käännöstekstissä puhutaan kyberhygieniaperiaatteista (engl. cyber hygiene policies). Käytännön tasolla ei liene merkitystä kumpaa termiä käytetään, mutta selvyyden vuoksi esitämme käytettäväksi samaa käännöstermiä kuin direktiivin virallisessa käännöksessä on käytetty.

Kohta 7 on ratkaistu Suomessa nykyisin muualla kuin lainsäädännössä (esim. katakri).

Seuraamusmaksua koskevat huomiot

Seuraamusmaksun suuruus ja määräämiskynnys on linjassa muun EU-direktiiveihin perustuvan sääntelymme kanssa. Ei kommentoitavaa.

CSIRT-yksikön tehtäviä koskevat huomiot

CSIRT-yksikön tiedonsaantioikeus on säädetty direktiivin mukaisesti varsin laajaksi ulottuen metatiedoista aina tietojärjestelmässä käsiteltyyn, tallennettuun tai välitettyyn viestiin saakka edellyttäen, että tällainen tieto on välttämätöntä velvoitteiden noudattamisen valvomiseksi tai merkittävän poikkeaman selvittämiseksi.

Kiinnitämme huomiota ristiriitaan tiedonsaantioikeuksia koskevan säännöksen ja yksikön tehtäviä koskevan säännöksen välillä, sillä poikkeaman selvittämistä ei ole säädetty CSIRT-yksikön tehtäväksi, vaan CSIRT-yksikön tehtäviin kuuluu avustaminen [vain] pyynnöstä poikkeaman käsittelyyn ja yleisen ohjeistuksen antaminen poikkeamien käsittelemiseksi. Näin säädettynä epäselväksi jää, millaisessa tilanteessa valvovan viranomaisen tiedonsaantioikeus voisi olla välttämätöntä poikkeaman käsittelemiseksi, kun poikkeaman käsittely ei ylipäätään kuulu valvovan viranomaisen virkatehtäviin.

Tiedonsaantioikeutta koskevan säännöksen viimeisen momentin mukaan valvovan viranomaisen automaattinen tiedonsaantioikeus ei koske sellaisia maanpuolustukseen ja kansalliseen turvallisuuteen liittyviä tietoja, jotka ovat turvallisuusluokiteltuja. Valtaosa Senaatti-konsernin käsittelemistä turvaluokitelluista tiedoista on tällaisia (julkisuusL 24 §:n 8-10 -kohdat). Sen sijaan tiedonsaantioikeuden piirissä olisivat mm. sisäiset valmisteluasiakirjat sekä liikelaitoksen ja/tai liikelaitoksen kumppanien liikesalaisuuksia sisältävät viestit. Tapauskohtaisesti tulkittavaksi jäisivät

julkisuuslain 24 §:n 7-kohdan nojalla salassa pidettävät, turvallisuusluokitellut tiedot (= henkilöiden, rakennusten, laitosten, rakennelmien sekä tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevat ja niiden toteuttamiseen vaikuttavat asiakirjat, jollei ole ilmeistä, että tiedon antaminen niistä ei vaaranna turvajärjestelyjen tarkoituksen toteutumista).

22 §:n mukaisen tiedonvälitysverkoston perustaminen juontuu suoraan direktiivistä. Koordinoituun kyberuhkien tunnistamis- ja haavoittuvuuksien ratkaisemisfoorumiin osallistuminen on vapaaehtoista ja ideana kannatettavaa. Em. säännöksen viimeinen momentti on kuitenkin ongelmallisesti muotoiltu eikä vastaa direktiivin vähimmäisvaatimusta. On ymmärrettävää, että virkavastuulla toimivalla CSIRT-yksiköllä voi laissa nimenomaisesti säädetyin edellytyksin olla oikeus käsitellä myös salassapidettäviä tietoja ml. tällaisen tiedon sisältävää viestiä. Sen sijaan CSIRT-yksiköllä ei voi olla oikeutta luovuttaa tällaista tietoa edelleen vapaaehtoiseen tietojenvaihtoon osallistuvalle muulle taholle. Direktiivin sanamuoto perustuu enemmän hyvien käytäntöjen, haavoittuvuuksien ja metadatan jakamiselle, mutta salassapidettävän viestin suojan murtaminen vapaaehtoisen järjestelyn piirissä on ongelmallista. Erityisen ongelmallista se on siksi, ettei tällaisen tiedon luovuttamista ole pykälässä rajattu niihin viesteihin ja tietoihin, jotka CSIRT-yksikölle on toimitettu vapaaehtoisesti vaan kaikkiin CSIRT-yksikön laajan tiedonsaantioikeutensa nojalla saamiin tietoihin.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Julkishallinnon kannalta velvoittavat säännökset tulevat pääasiassa tiedonhallintalakiin, johon tulee uusi kyberturvallisuutta koskeva luku 4a. Velvoitteet ovat kuitenkin myös julkishallinnon osalta valtaosassa säännöksiä sanatarkasti samat kuin kyberturvallisuusdirektiivin täytäntöönpanolaissakin. Velvoitteita on kuitenkin tiedonhallintalaissa jaoteltu ja niputettu hieman eri tavoin.

Verkkotunnusvälittäjiä koskevat huomiot

Ei kommentoitavaa.

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ei kommentoitavaa.

Vaikutustenarviointia koskevat huomiot

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.

Em. katkelma on poimittu taloudellisten vaikutusten arvioinnin yleisestä osiosta. Perusteluiden osion 4.4 Vaikutukset viranomaisten tehtäviin ja julkistalouteen -otsikkotason ensimmäisen kappaleen mukaan ko. alaluvussa kuvataan esityksen vaikutuksia [valvoville] viranomaisille viranomaistoiminnan osalta. Sääntelyn noudattamisesta muille julkishallinnon toimijoille aiheutuvia vaikutuksia todetaan käsiteltävän seuraavassa alaluvussa. Seuraava alaluku 4.5 käsittelee kuitenkin

ehdotuksen yleisiä yhteiskunnallisia vaikutuksia eikä sisällä arviota vaikutuksista direktiivin soveltamisalaan nyt ensimmäistä kertaa tuleville julkishallinnon toimijoille. Vaikutusten arviointia tulisi näiltä osin täydentää oikeasuhteisen kokonaiskuvan saamiseksi direktiivin vaikutuksista julkistalouteen ja jotta julkishallinnon toimijat voivat ennakoida tulevia resurssitarpeitaan.

Viranomaisille tehtäville poikkeamailmoituksille laissa asetettavien aikamääreiden saavuttaminen edellyttää toimijoilta käytännössä jonkinlaista 24/7 järjestelyä, jolla on sekä henkilöstö että kustannusvaikutuksia. Päivystysmenettelyn lisäksi on luotava ja ylläpidettävä kyvykkyys tehdä verkoissa ja järjestelmissä poikkeamahavainnointia ja on oltava osaamista arvioida ja analysoida poikkeamia. On syytä myös huomioida, ettei ulkopuolisten toimittajien kanssa tehdyissä nykyisissä ostosopimuksissa ole välttämättä sovittu yhtenevästi poikkeamaraportoinnista, jolloin kustannusvaikutuksia syntyy myös välillisesti, kun jo tehtyjä sopimuksia joudutaan muuttamaan kesken sopimuskauden tai kilpailuttamaan ennenaikaisesti uudelleen.

Erityisen haastavana pidämme rakennusten LVIS- ja rakennusautomaatiojärjestelmien kyberturvallisuuden riskienhallinnan saattamista direktiivin ja täytäntöönpanolain edellyttämälle tasolle. Näiden taloteknisten järjestelmien elinkaari on suunniteltu pitkäksi ja mikäli niitä joudutaan ennenaikaisesti uusimaan esimerkiksi raportointivelvoitteiden täyttämiseksi, aiheutuu tästä merkittäviä kustannuksia, joita vaikutustenarvioinnissa tai komissionkaan arvioissa ei ole toistaiseksi huomioitu oikeasuhtaisesti.

Muut huomiot ja avoin palaute esityksestä

Lakiesityksen 10 § (ja vastaavasti tiedonhallintalain 18 b §) säätelevät johdon vastuuta.

Toteamme, että täytäntöönpanolain sanamuoto on direktiiviä huomattavasti ankarampi ja poikkeaa lainsäädännössämme yleisesti omaksutusta linjasta johdon vastuun osalta. Johdon vastuu on yleisesti ymmärretty huolehtimisvelvollisuutena, mutta nyt säännöksen sanamuoto näyttäisi muodostavan johdolle aktiivisen itsenäisen toimintavelvoitteen kyberturvallisuuden riskienhallinnan toteuttamisen ja valvonnan järjestämisestä.

Lisäksi sanamuoto näyttäisi tarkoittavan johdon kollektiivista vastuuta, jolloin organisaatiossa johtavassa asemassa olevat vastaisivat kyberturvallisuuden riskienhallinnan toteuttamisen ja valvonnan järjestämisestä sekä riskienhallinnan toimintamallin hyväksymisestä omasta vastuualueestaan ja tehtävästään riippumatta. Näin säädettynä täytäntöönpanolaki asettaa tosiasiallisesti vaatimuksia myös organisaatioiden sisäisille päätöksentekovaltuuksille ja hallintorakenteille, mikä ei liene tarkoitus.

Direktiivin sanamuodon täyttämiseksi riittäisi, että keskeisten ja tärkeiden toimijoiden hallintoelimet (ei siis hallitus, toimitusjohtaja ja muu operatiivinen johto kollektiivisesti, vaan hallintoelimet eli

tyypillisesti hallitus) hyväksyvät kyberturvallisuusriskien hallintatoimenpiteet ja valvovat niiden täytäntöönpanoa. Valvonta voisi tapahtua normaalin operatiivisen johtamisjärjestelmän puitteissa.

Direktiivin 20 artiklan 2 kohta asettaa hallintoelimien jäsenille nimenomaisen kouluttautumisvelvoitteen (”… velvollisuus osallistua koulutukseen.”), mikä ei täytäntöönpanolaissa esityksen mukaisena täyty. Kansallisessa täytäntöönpanolaissa puhutaan esityksen mukaan nyt vain perehtyneisyydestä.

Senaatti-kiinteistöjen ja Puolustuskiinteistöjen puolesta

Tomi Flink
juristi
+358504911540
tomi.flink@senaatti.fi