Rakennusteollisuus RT ry

Lausunto

23.11.2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Vaikka NIS2-direktiivi huomioi fyysisen ympäristön ja siihen liittyvät kyberturvallisuusriskit vain perustasolla, niin se on selvä parannus aiempaan tilanteeseen. Direktiivin perusteella annettavassa laissa ja sen perusteluissa onkin syytä kiinnittää huomioita jäljempänä esitettäviin kohtiin, jotta mahdollinen tulkinnanvaraisuus vähenisi, katso myös viimeinen kohta "Muut huomiot ja avoin palaute esityksestä".

Soveltamisalaa koskevat huomiot

Ei lausuttavaa.

Riskienhallintavelvoitetta koskevat huomiot

8 §. Kyberturvallisuuden riskienhallinnan toimintamalli

Pykälässä asetetaan vaatimus kyberturvallisuuden riskienhallinnan toimintamallin käytölle ja kuvataan siltä vaadittava kattavuus.

Pykälän perusteluissa todetaan, että kyberturvallisuuden riskienhallinnan tulisi ulottua kaikki vaaratekijät huomioiden myös tietojärjestelmien ja niiden avulla harjoitetun toiminnan sekä tarjottavien palveluiden fyysiseen ympäristöön, kuten toimitilat.

Perustelujen neljännessä kappaleessa ”Kaikki vaaratekijät huomioivan lähestymistavan tulisi kattaa…” mainitaan kuitenkin vain tietoturvallisuusriskit. Selvyyden vuoksi perustelujen tässä kohdassa tulisi mainita myös kyberturvallisuus, jotta fyysiseen ympäristöön ja sen toimintaan tietoverkkojen kautta vaikuttaminen olisi aukottomasti riskienhallinnan piirissä. Kappaleen tekstiä tulisi laajentaa esim. seuraavaksi:

”Kaikki vaaratekijät huomioivan lähestymistavan tulisi kattaa viestintäverkkojen ja tietojärjestelmien tieto- ja kyberturvallisuusriskit kuten hallinnollisen, henkilöstö-, laitteisto- ja ohjelmisto-, tietoaineisto- sekä käyttöturvallisuuden riskit ja niiden fyysisen ympäristön, toimitilojen ja välttämättömien resurssien osalta sellaisia tapahtumia, kuten varkaus, tulipalo, tulva, televiestintähäiriö tai sähkökatko, luvaton fyysinen pääsy toimijan tietoihin tai tietojenkäsittely-ympäristöön sekä vahinko ja häirintä, joka vaarantaisi viestintäverkoissa ja tietojärjestelmissä tai niiden välityksellä käsiteltävien tietojen tai palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden sekä fyysisen toimintaympäristön ja siltä vaadittavat olosuhteet.”

9 §. Kyberturvallisuuden riskienhallinnan toimenpiteet

Pykälässä asetetaan vaatimukset kyberturvallisuuden riskienhallinnan toimintamallin toimenpiteille ja luetellaan valvovalle viranomaiselle mahdollistetut tarkempien teknisten määräysten anto mahdollisuudet.

Pykälän kohdan neljä perusteluissa käsitellään toimitusketjusta niin toimittajien, kuin palveluntarjoajien kyberturvallisuuskäytäntöjä. Toimijalla tulisi olla ajantasainen tieto kaikista toimintaan ja palveluntarjontaan vaikuttavista välittömistä toimittajista ja palveluntarjoajista, jotta se voisi riskienhallinnassaan ottaa huomioon toimitusketjuhäiriön vaikutuksen omaan toimintaansa sekä varautua mahdolliseen toimitushäiriöön etenkin toimitusketjunsa välittömien laite- tai palvelutoimittajien osalta. Riskien hallintatoimenpiteitä harkitessa tulisi ottaa huomioon välittömälle toimittajalle ja palveluntarjoajalle ominaiset haavoittuvuudet, tuotteiden ja palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt. Tässä laissa säädettyjen vaatimusten kannalta toimija vastaa itse siitä, että se hankkii omaan toimintaansa sellaisia tuotteita ja palveluita, että toimijan riskienhallinnan vaatimukset täyttyvät. Lain vaatimukset eivät siis koske alihankkijaa, ellei se itsekin ole toimija, jonka toimintaa sääntely koskee. Tällaisena toimittajana tai palveluntarjoajana, jota sääntely ei koske, voitaneen pitää esimerkiksi toimijan käyttämän kiinteistön vuokranantajaa ja omistajaa.

Pykälän kohdan neljä perusteluissa tulisi ottaa kantaa sekä toimijan, että koko toimitusketjun käyttämien vuokrattujen tilojen riskienhallintaan tilanteessa, jossa vuokrasopimus jatkuu pitkälle NIS2-lain voimaantulon jälkeen. Mikäli vuokranantajalta ei saada tarvittavia tietoja ja toimijaa uhkaa sen vuoksi seuraamukset, oikeuttaisi tilanne irtisanomaan vuokrasopimuksen välittömästi ilman muita seuraamuksia.

Pykälän kohdan viisi perusteluissa käsitellään omaisuudenhallintaa ja turvallisuuden kannalta tärkeiden toimintojen tunnistamista. Omaisuudenhallinta on kyberturvallisuusriskien hallinnassa keskeinen keino, jonka huolellinen hoitaminen ennalta ehkäisee riskien toteutumista ja auttaa

riskienhallinnassa. Omaisuudella tarkoitetaan esimerkiksi tiloja, laitteita, ohjelmistoja, palveluita, henkilöitä, aineetonta omaisuutta ja resursseja kuten immateriaalioikeuksia tai IP-osoitteita.

Pykälän kohdan viisi perusteluissa tulisi selvyyden vuoksi todeta, että omaisuudella tarkoitetaan tässä yhteydessä myös toimijan hallussa olevia tai käyttämiä vuokrattuja resursseja, kuten esimerkiksi tiloja, laitteita ja ohjelmistoja.

Pykälän kohdan kaksitoista perusteluissa käsitellään toimenpiteitä viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön ja tilaturvallisuuden sekä välttämättömien resurssien varmistamiseksi.

Pykälän kohdan kaksitoista perusteluissa tulisi selvyyden vuoksi todeta, että pykälän kohtien 2, 3 sekä 5–11 toimenpiteet on ulotettava kattamaan myös viestintäverkkojen ja tietojärjestelmien fyysinen ympäristö ja niiden tilaturvallisuuden sekä välttämättömien resurssien järjestelmät ja palvelut.

Raportointivelvoitetta koskevat huomiot

Ei lausuttavaa.

Valvontaa koskevat huomiot

25 §. Valvovat viranomaiset

Pykälässä käsitellään lain noudattamista valvovia viranomaisia. Laissa tarkoitettaisiin valvovalla viranomaisella NIS2-direktiivin mukaista toimivaltaista viranomaista. Pykälän 3 momentissa säädettäisiin valvonnasta tilanteessa, jossa yksi toimija harjoittaisi toimintaa laaja-alaisesti usealla toimialalla siten, että toimijaan kohdistuisi 1 momentin nojalla useamman kuin yhden viranomaisen valvontatoimivalta. Valvovilta viranomaisilta edellytettäisiin tällöin yhteistyötä valvonnan toteuttamiseksi tavalla, joka säästää valvonnan kohteen ja valvovien viranomaisten resursseja.

Voitaneen olettaa, että kaikilla valvonnan piiriin kuuluvilla toimijoilla on joku viestintäverkkojen ja tietojärjestelmien fyysinen ympäristö ja niiden tilaturvallisuuden sekä välttämättömien resurssien järjestelmät ja palvelut, joihin kohdistettava viranomaisvalvonta on vaatimuksiltaan ja sisällöltään jokseenkin sama riippumatta sektorista tai toimialasta. Päällekäisyydestä voi toki olla hyötyäkin, mutta tehokkaampaa resurssiem käyttöä ja todennäköisesti parempaa palvelua saatanen keskittämällä fyysiseen ympäristöön liittyvä valvonta.

Viranomaisresurssien säästämiseksi olisi syytä määrittää mille mainituista valvovista viranomaisista tai jollekin mainitsemattomalle viranomaiselle, esimerkiksi SYKE, keskitetään toimijoiden viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön ja sen tilaturvallisuuden sekä välttämättömien resurssien järjestelmien ja palveluiden valvonta.

27 §. Valvovan viranomaisen tiedonsaantioikeus

Pykälässä käsitellään valvovan viranomaisen tarpeellisia tiedonsaantioikeuksia valvontatehtävän toteuttamiseksi. Pykälä liittyy tai sivuaa 9 § 4. kohtaa.

Pykälän 27 perusteluissa tulisi ottaa kantaa myös sellaisten tietojen saatavuuteen, joissa toimija on esimerkiksi tilojen suhteen vuokralainen. Säädettävän lain voimaantulon jälkeen voi vuokrasopimuksissa edellyttää otettavan huomioon tiedonhankinnan velvoittavuus, mutta nykyisten sopimusten ollessa voimassa, voi vaatimus olla mahdoton toteuttaa. Sama koskee vuokrattuja laitteistoja. Perusteluissa olisi myös syytä harkita mainintaa siitä, että toimijasta riippumattoman, mutta vuokranantajan vastuulla olevan tiedon luovuttamattomuus oikeuttaa toimijan irtisanomaan kyseisen vuokrasopimuksen (vastaava) välittömästi.

29 §. Tarkastusoikeus

Pykälässä käsitellään valvovan viranomaisen tarkastusoikeutta.

Pykälän 29 perusteluissa tulisi ottaa kantaa pykälän 27 mukaisesti myös sellaisiin tarkastuksiin, joissa toimija on esimerkiksi tilojen suhteen vuokralainen, jolloin tarkastus rajataan vain toimijan itsensä vastuulla oleviin järjestelmiin ja palveluihin.

30 §. Turvallisuusauditointi

Pykälässä käsitellään valvovan viranomaisen oikeutta velvoittaa toimija teettämään kyberturvallisuuden riskienhallintaan kohdistuva turvallisuusauditointi ja saada sen tulokset.

Pykälän 30 perusteluissa tulisi ottaa kantaa pykälien 27 ja 29 mukaisesti myös sellaisiin auditointeihin, joissa toimija on esimerkiksi tilojen suhteen vuokralainen, jolloin auditointi rajataan vain toimijan itsensä vastuulla oleviin järjestelmiin ja palveluihin.

Seuraamusmaksua koskevat huomiot

Ei lausuttavaa.

CSIRT-yksikön tehtäviä koskevat huomiot

Vaikka toimijoiden viestintäverkkojen ja tietojärjestelmien fyysinen ympäristö ja sen tilaturvallisuuden sekä välttämättömien resurssien järjestelmät ja palvelut eivät ole NIS2-direktiivin soveltamisaloissa oma sektorinsa, tulee alan erityspiirteet huomioida Kyberturvallisuuskeskuksen CSIRT-toiminnan organisoinnissa.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Edellä lausuttu tulisi huomioida julkishallinnossa vastaavalla tavalla.

Verkkotunnusvälittäjiä koskevat huomiot

Ei lausuttavaa.

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Ei lausuttavaa.

Vaikutustenarviointia koskevat huomiot

Ei lausuttavaa.

Muut huomiot ja avoin palaute esityksestä

Hallituksen esitys huomioi perustasolla fyysiseen ympäristön liittyvät kyberturvallisuusriskit. Vähintään perustelumuistiossa olisi kuitenkin ennestään selvennettävä riskienhallinnan ja vaadittavien toimenpiteiden ulottamista myös säädöksen piiriin kuuluvien toimijoiden käyttämiin kiinteistöihin, rakennuksiin ja niiden talotekniikkaan. Myös sellaisten tilanteiden, joissa toimija on vuokrannut käyttöönsä tiloja, kiinteistöjä, laitteita ja ohjelmistoja, kohdalla olisi säännöstöä selvennettävä erilaisten vastuiden sekä tiedonsaanti- ja tarkastusoikeuksien osalta. Viranomaisvalvonnan kohdalla tulisi harkita fyysiseen ympäristöön kohdistuvan valvonnan keskitettyä toteutusta.

Järvinen Ari
Rakennusteollisuus RT ry