Jyväskylän yliopisto

Lausunto

16.11.2023 1373/00.01.04.00/2023

Asia: VN/18157/2023

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

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Yleisesti ottanen luonnoksen luku 2.1 esittää direktiivin tavoitteet ja tarkoituksen tiivistetysti

Soveltamisalaa koskevat huomiot

Yksi NIS 1 -direktiivin suurimmista ongelmista oli sen ehtojen epäselvyys ja jäsenvaltioille myönnetty liiallinen itsemääräämisoikeus sen soveltamisalaan kuuluvien yksiköiden määrittämisessä. Tämä johti epäjohdonmukaisuuksiin direktiivin täytäntöönpanossa eri jäsenvaltioissa. NIS 2 näyttäisi käsittelevän tätä ongelmaa liian itsenäisesti ottamalla käyttöön luettelon sektoreista, joita olisi pidettävä joko olennaisina tai tärkeinä kokonaisuuksina ja jotka olisi sisällytettävä NIS 2:n soveltamisalaan. tämä toki yhdenmukaistaa täytäntöönpanoprosessia jäsenvaltioiden kesken, mutta esim. pk-yritysten autonomiaongelma on edelleen olemassa (NIS2 koskee vain keskisuuria ja suuria yrityksiä). Myös epäselvien termien ongelma on edelleen olemassa.

Riskienhallintavelvoitetta koskevat huomiot

Direktiivi sisältää ao. riskienhallintatoimenpiteet, jotka asianomaisten yritysten ja laitosten on täytettävä. Tämä on kattava lista ja lausunnossa voisi miettiä sen soveltamista eri organisaatioissa.

Tietoturvapolitiikat: Kaikkia riskejä koskevien ohjeiden käyttöönotto ja tietoturvan toteuttaminen.

Tapahtumanhallinta: Turvavälikohtausten ehkäisy, havaitseminen ja hallinta.

Liiketoiminnan jatkuvuus: Liiketoiminnan jatkuvuuden varmistaminen varmuuskopioiden hallinnan, katastrofipalautuksen ja kriisinhallinnan avulla.

Toimitusketju: Toimitusketjun turvallisuus ja turvatoimenpiteet IT- ja verkkojärjestelmien hankinnassa ja ylläpidossa.

Tehokkuus: Määritykset kyber- ja riskimittausten mittaamiseksi.

Koulutus: Kyberturvallisuushygieniakoulutus ja koulutus

Kryptografia: Salauksen ja salauksen tekniset tiedot kaikille olennaisille alueille

Henkilöstö: Henkilöstöturvallisuus

Kulunvalvonta: Kaikkien pääsyjen valvonta ja kirjaaminen

Asset Management (ISMS): Tietoturvan hallintajärjestelmä sisältää sääntöjä, menettelyjä, menetelmiä ja työkaluja tietoturvan lisäämiseksi. ISO 27001 pidetään kultastandardina

Todennus: Monitekijätodennuksen (MFA) ja kertakirjautumisen (SSO) käyttö

Viestintä: Salatun puhe-, video- ja tekstiviestinnän käyttö

Hätäviestintä: Turvallisten hätäviestintäjärjestelmien käyttö

Lisäksi tehostetaan viranomaisten ja yritysten välistä valvontaa ja yhteistyötä sekä otetaan käyttöön raportointivelvollisuus. 24 tunnin sisällä kyberturvallisuushäiriön havaitsemisesta vaaditaan välitön ilmoitus. Tarvittaessa valvontaviranomainen tekee päivityksen ja alustavan arvioinnin 72 tunnin kuluessa alkuperäisestä ilmoituksesta. Loppuraportti on toimitettava viimeistään kuukauden kuluttua ensimmäisen ilmoituksen tekemisestä. Raportointivaatimuksen tarkoituksena on parantaa läpinäkyvyyttä ja koordinaatiota kyberturvallisuushäiriöiden torjumiseksi tehokkaasti.

Raportointivelvoitetta koskevat huomiot

NIS2:ssa eri tahojen on raportoitava paitsi "merkittävistä tapahtumista" myös tapauksista, joita voidaan mahdollisesti pitää uhkana tai "läheltä piti". Organisaatiot voivat tulkita näitä "potentiaalisuuteen" perustuvia tapauksia liian laajasti, mikä johtaa raskaisiin raportointivaatimuksiin niille ja kansallisille viranomaisille. On ratkaisevan tärkeää käydä keskusteluja kansallisten viranomaisten kanssa, jotaa saa selvän käsityksen siitä, minkä tyyppiset vaaratilanteet pitäisi luokitella "läheltä piti" tai "mahdollisiksi vaaratilanteiksi". Em. asia tuo haasteita myös raportointivelvoitteeseen.

Valvontaa koskevat huomiot

NIS2-direktiiviin soveltamisalaan kuuluvien toimijoiden määrä kasvaa moninkertaiseksi. Toimialat ja palvelut jaetaan kahteen luokkaan: kriittiseen (essential) ja tärkeään (important). Molemmilta luokilta vaaditaan pohjimmiltaan samanlaista kyberturvallisuutta, mutta niiden valvonta ja seuraamukset eroavat toisistaan.

Valvonta tulee olemaan haastellista suuren organisaatiomäärän vuoksi.

Seuraamusmaksua koskevat huomiot

Sanktiot ovat liian suuria:

Liiketoiminnan väliaikainen keskeyttäminen

Toimitusjohtajan tai vastaavan laillisen edustajan johtotehtäväkielto

Hallinnollinen sakko keskeiselle toimijalle enintään 10 miljoonaa euroa tai 2 % liikevaihdosta

Hallinnollinen sakko tärkeälle toimijalle enintään 7 miljoonaa euroa tai 1,4 % liikevaihdosta

.

CSIRT-yksikön tehtäviä koskevat huomiot

Jokaisen jäsenmaan on perustettava yksi tai useampi CSIRT-yksikkö. CSIRT-yksikön tehtäviä ovat esim.

seurata ja analysoida kyberuhkia, haavoittuvuuksia ja poikkeamia, antaa näitä koskevia ennak-

kovaroituksia, hälytyksiä, ilmoituksia ja tietoja, avustaa direktiivin soveltamisalaan kuuluvia

toimijoita, reagoida poikkeamatilanteisiin, kerätä ja analysoida poikkeamatietoja, ylläpitää ky-

berturvallisuuden tilannekuvaa ja osallistua CSIRT-verkoston toimintaan.

CSIRT- yksikön tehtävät ovat aika väljästi määritelty, joten jokainen jäsenmaa voi organisoida sen toimintaa melko vapaasti.

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Tiedonhallintalaissa käytetyt käsitteet poikkeavat jonkin verran NIS2-direktiivissä käytetyistä,

joten NIS2 –direktiivin voimaan saattamisen kannalta välttämättömät direktiivissä käytetyt käsitteet tulisi lisätä tiedonhallintalakiin.

Verkkotunnusvälittäjiä koskevat huomiot

NIS2 tuo rekisteröintipalvelujen tarjoajille / DNS-palveluntarjoajille lisää velvoitteita;

- Kyberriskienhallinta (vain DNS-palv.tarj.)

- Ilmoitusvelvollisuus merkittävästä poikkeamasta

›- Verkkotunnusten rekisteröintitietojen oikeellisuus

- Tietojen luovutus

- WHOIS-tiedot

› Toimijarekisteriin ilmoittautuminen

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

-

Vaikutustenarviointia koskevat huomiot

-

Muut huomiot ja avoin palaute esityksestä

Kaikkinensa hallituksen esitys kattaa hyvin NIS2:sen tuomat velvollisuudet.

Hämäläinen Timo
Jyväskylän yliopisto