Pohde
Pohjois-Pohjanmaan hyvinvointialue

Kyberturvallisuuden riskienhallinnan toimintamalli

Tietoturvapäällikkö Anssi Huhtala

16.6.2025

Esityksen sisältö

- Tausta ja kyberturvallisuuslain keskeisimmät vaatimukset
- Kyberturvallisuuslain vaatimukset johdolle
- Pohteen kyberturvallisuuden riskienhallinnan toimintamallin esittely
- Esittelijän ehdotus

Tausta ja keskeiset vaatimukset

- NIS2-direktiivi, eli verkko- ja tietoturvadirektiivi, astui voimaan EU:ssa joulukuussa 2022. Jäsenvaltioiden oli saatava se osaksi kansallista lainsäädäntöään 17. lokakuuta 2024 mennessä. NIS2-direktiivin perusteella annettu kyberturvallisuuslaki tuli voimaan 8.4.2025
- 11 § Poikkeamailmoitukset viranomaiselle. Toimijan on viipymättä ilmoitettava valvovalle viranomaiselle merkittävästä poikkeamasta.
    - Ensi-ilmoitus 24 tunnin kuluessa merkittävän poikkeaman havaitsemisesta, jatkoilmoitus 72 tunnin kuluessa, tarvittaessa väliraportti kuukauden kuluessa, loppuraportti kuukauden kuluessa poikkeaman päättymisestä.
    - Ilmoitusprosessi ja vastuut on sovittu ja toimeenpantu.
- Lain 41 §:ssä tarkoitettu valvovan viranomaisen toimijaluetteloon on ilmoittauduttava viimeistään kuukauden kuluessa lain voimaantulosta
    - Pohde ilmoitettu Traficomin ja Valviran luetteloihin, Fimea ilmoitti, ettei valvo kyberturvallisuuslain osalta.
- Lain 10 § mukaan toimijan johto vastaa kyberturvallisuutta koskevan riskienhallinnan toteuttamisen ja valvonnan järjestämisestä sekä hyväksyy kyberturvallisuutta koskevan riskienhallinnan toimintamallin ja valvoo sen toteuttamista.
- Lain 8 §:ssä tarkoitettu riskienhallinnan toimintamalli on laadittava kolmen kuukauden kuluessa lain voimaantulosta.

10 § Johdon vastuu

- Toimijan johto vastaa kyberturvallisuutta koskevan riskienhallinnan toteuttamisen ja valvonnan järjestämisestä sekä hyväksyy kyberturvallisuutta koskevan riskienhallinnan toimintamallin ja valvoo sen toteuttamista. Toimijan johdolla tulee olla riittävä perehtyneisyys kyberturvallisuutta koskevaan riskienhallintaan.
- Johdolla tarkoitetaan toimijan hallitusta, hallintoneuvostoa ja toimitusjohtajaa sekä muussa niihin rinnastettavassa asemassa olevaa, joka tosiasiallisesti johtaa sen toimintaa.
- Riittävä perehtyneisyys varmistetaan ylimmän johdon tietoturvakoulutuksella.
    - Koulutus laadittu yhteistoiminnassa SOTE-ISAC:in (sosiaali- ja terveysalan kyberturvallisuuden tiedonvaihtoryhmä) kanssa
    - Julkaistaan Mediecon koulutusalustalla syksyllä 2025
    - Toistaiseksi julkaistu Pohteen intranetissä Ilonassa tietoturvan sivuilla

Lisäksi huomioitavaa

- Kyberturvallisuuslain lisäksi Laki julkisen hallinnon tiedonhallinnasta (906/2019) määrittää tietoturvaan liittyviä vastuita tiedonhallintayksikön johdolle.
- Lain 4 § toinen momentti, Tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on:
    - 2) ajantasaiset ohjeet tietoaineistojen käsittelystä, tietojärjestelmien käytöstä, tietojenkäsittelyoikeuksista, tiedonhallinnan vastuiden toteuttamisesta, tiedonsaantioikeuksien toteuttamisesta, tietoturvallisuustoimenpiteistä sekä poikkeusoloihin varautumisesta.
- Tiedonhallintayksikön johdoksi on määritelty hallintosäännön 65 § mukaisesti aluehallitus yhdessä hyvinvointialuejohtajan kanssa.
- Hallintosäännön luku 8 kahdeksan määrittää aluehallitukselle tiedonhallintaan ja asiakirjahallintoon liittyviä vastuita.

Kyberturvallisuuslain soveltamisala

- 3 § Toimijat kohta 1) harjoittaa liitteessä I tai II tarkoitettua toimintaa tai on mainituissa liitteissä tarkoitettu toimija.
- Liite 1 kohta 13. Terveys a)
    - Sosiaali- ja terveydenhuollon valvonnasta annetun lain (741/2023) 4 §:n 2 kohdassa tarkoitetut palveluntuottajat, jotka tuottavat mainitun pykälän 4 kohdassa tarkoitettua terveyspalvelua.
- Laki sosiaali- ja terveydenhuollon valvonnasta (741/2023) 4 § kohta 2)
    - *palveluntuottajalla* hyvinvointialuetta, Helsingin kaupunkia, HUS-yhtymää jne.
- Laki sosiaali- ja terveydenhuollon valvonnasta (741/2023) 4 § kohta 4)
    - *terveyspalvelulla* potilaan terveydentilan määrittämiseksi, hänen terveytensä palauttamiseksi tai ylläpitämiseksi tehtäviä toimenpiteitä, terveyden- ja sairaanhoitoa taikka muuta käsittelyä, jossa käytetään lääketieteellisiä tai hammaslääketieteellisiä menetelmiä tai joka perustuu lääketieteeseen tai hammaslääketieteeseen ja, joita suorittavat terveydenhuollon ammattihenkilöt tai joita suoritetaan terveydenhuollon palveluyksikössä, liikkuvana palveluna, etä- tai digiyhteydellä taikka potilaan luona tai terveydenhuoltolain (1326/2010) 40 §:ssä tarkoitettuna ensihoitopalveluna;

8 §Kyberturvallisuutta koskeva riskienhallinnan toimintamalli

Pohde
Pohjois-Pohjanmaan hyvinvointialue

- Toimijalla on oltava käytössä ajantasainen kyberturvallisuutta koskeva riskienhallinnan toimintamalli viestintäverkkojen ja tietojärjestelmien ja niiden fyysisen ympäristön suojaamiseksi poikkeamilta ja niiden vaikutuksilta.
- Kyberturvallisuutta koskevassa riskienhallinnan toimintamallissa on tunnistettava viestintäverkkoihin ja tietojärjestelmiin ja niiden fyysiseen ympäristöön kohdistuvat riskit ottaen huomioon kaikki vaaratekijät huomioiva lähestymistapa.
- Toimintamallissa on määritettävä ja kuvattava kyberturvallisuutta koskevan riskienhallinnan tavoitteet, menettelyt ja vastuut sekä 9 §:n mukaiset toimenpiteet, joilla viestintäverkkoja ja tietojärjestelmiä ja niiden fyysistä ympäristöä suojataan kyberuhkilta ja poikkeamilta (hallintatoimenpiteet).

9 §Toimenpiteet kyberturvallisuutta koskevien riskien hallinnassa

Pohde
Pohjois-Pohjanmaan hyvinvointialue

Toimintamallissa ja siihen perustuvissa hallintatoimenpiteissä on otettava huomioon ja pidettävä yllä ajantasaisesti ainakin:

1) kyberturvallisuutta koskevan riskienhallinnan toimintaperiaatteet ja hallintatoimenpiteiden vaikuttavuuden arviointi;

2) viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet;

3) viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus sekä tarvittavat menettelyt haavoittuvuuksien käsittelemiseksi ja julkistamiseksi;

4) toimitusketjun välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, niihin sisällytetyt hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt;

5) omaisuudenhallinta ja sen 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 käyttämiseksi;

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;

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

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

Pohteen kyberturvallisuuden riskienhallinnan toimintamalli

Pohde
Pohjois-Pohjanmaan hyvinvointialue

- Perustuu Liikenne- ja viestintäministeriön traficomin suositukseen NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä, Valtionvarainministeriön ohjetta riskienhallintaan ja Riskienhallinnan käsikirja valtionhallinnon toimijoille.
- Hallintamalli noudattaa täysin traficomin suosituksen rakennetta.
- Hallintamalli määrittää ja kuvaa kyberturvallisuutta koskevan riskienhallinnan tavoitteet, menettelyt ja vastuut sekä lain 9 §:n mukaiset toimenpiteet.
- Lain 7 § mukaisesti hallintamallin avulla tunnistetaan, arvioidaan ja hallitaan riskejä, joita kohdistuu Pohteen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuuteen.
- Kyberturvallisuuteen liittyviä riskienhallinnan toimenpiteitä on rakennettu HVA-valmistelusta lähtien NIS2-direktiivin perusteella.
- Mallissa kuvatut kyberturvallisuuteen liittyvät riskienhallintatoimenpiteet ja prosessit on jo pääosin toimeenpantu, eivätkä aiheuta enää isoja muutoksia toiminnalle.

Keskeiset periaatteet

- Jokaiselle tunnistetulle kyberturvallisuusriskille määritetään omistaja.
- Strategisen tason vakavien kyberriskien hallintapäätökset tekee Pohteen strateginen tietoturva-tietosuojaryhmä ja tarvittaessa päätökset siirretään aluehallitukselle.
    - Täyttää lain 10 § mukaiset johdon velvoitteet.
- Vakavuudeltaan tai vaikutuksiltaan matalamman tason riskeille määritetään omistaja, joka vastaa riskienhallintatoimenpiteiden seuraamisesta ja toteuttamisesta.
- Pohteen tietoturvayksikkö laatii suositukset riskienhallintatoimenpiteistä ja seuraa niiden toteutumista.
- Sisäisen valvonnan kanssa sovitaan riskienhallinnan vaikuttavuuden mittaamisesta.

Hallintamallin kehittäminen ja toimeenpano

- Pohteen tietoturvapäällikkö vastaa mallin kehittämisestä ja toimeenpanosta.
- Malli yhteensovitetaan Pohteen kokonaisriskienhallinnan kanssa.
- Hyvinvointialuejohtaja voisi hyväksyä tekniset muutokset
    - Teknisillä muutoksilla tarkoitetaan kirjoitusasun muokkauksia, muihin asiakirjoihin viittaavia muutoksia (esim. tietoturvasuunnitelma, tietoturva-tietosuojapolitiikka, muissa prosesseissa tapahtuvat muutokset)
- Muut kuin tekniset muutokset tuotaisiin aluehallituksen hyväksyttäväksi tarvittaessa vuosittain.

Esittelijän ehdotus

1. Aluehallitus hyväksyy kyberturvallisuuslaki 124/2025 10 § mukaisesti kyberturvallisuutta koskevan riskienhallinnan toimintamallin ja valvoo sen toteuttamista.
2. Hallintamallin kehittämisestä ja toimeenpanosta vastaa Pohteen tietoturvapäällikkö.
3. Aluehallitus valtuuttaa hyvinvointialuejohtajan hyväksymään tekniset muutokset hallintamalliin. Muut muutokset käsitellään ja hyväksytään aluehallituksessa vuosittain.