Sosiaali- ja terveysministeriö

Lausunto

10.10.2016

Asia: VM136:09/2013

Luonnos VAHTI 3/2016 Tietoturvapoikkeamatilanteiden hallinta

Yleistä ohjeeseen liittyen

Yleiset kommentit ja havainnot ohjeeseen

Ohjetta on odotettu ja sille on käyttöä.

Ohjeluonnos on tarkoitettu yhdenmukaistamaan ja kehittämään tietoturvapoikkeamien hallintatapaa, lisäämään eri tahojen yhteistyötä sekä yleisesti parantamaan valtionhallinnon tietoturvallisuutta. Ohje ei käsittele yleisiä tieto- ja viestintäteknologian häiriötilanteiden hallintaa ja toiminnan jatkuvuuden turvaamista.

Ohjeessa on seikkaperäisesti selostettu hallintaprosessin vaiheistus, valmiusvaatimukset, toimenpiteet sekä organisoinnin että päätöksenteon osalta. Viranomaisorganisaatioiden osalta yksityiskohtainen ohjeistus on tarpeen oman toiminnan varmistamiseksi.

Yhteistyön merkitys on suuri, kuten ohjeen yhtenä tavoitteenakin on mainittu. Yhteistyön tulisi kattaa myös tietojen vaihto ja keräys, jotta niiden hyödyntäminen olisi käytännössä mahdollista.

Poikkeamatilanteiden luokituksen yhteismitallisuus on tärkeää. Myös poikkeamatilanteiden ja ICT-häiriötilanteiden rajan tulisi olla selkeä.

Poikkeamatilanteiden käsittelykyvyn muodostaminen ja poikkeamatilanteista toipuminen tulee kytkeä myös riskienhallintaan ja organisaation jatkuvuussuunnitelmaan.

Yleisenä kommenttina olisi toivottavaa, että ohjeessa olisi esim. kuvio kaikista keskeisistä valtionhallinnon toimijoista ja niiden roolista tietoturvapoikkeamatilanteissa. Nyt epäselväksi jää, kuka viranomainen viime kädessä vastaa kokonaisuuden koordinaatiosta.

Sosiaali- ja terveydenhuollon osalta tulisi huomioida ja korostaa sitä, miten tietoturvapoikkeamat vaikuttavat varsinaisten palvelujen järjestämiseen ja mitä erityistoimenpiteitä tämä mahdollisesti vaatii. Esimerkkinä tilanne, jossa potilastietojärjestelmää ei pysty käyttämään. Tietoturvapoikkeamien käsittelyryhmässä täytyy siis olla linkki organisaation johtoon, jonka täytyy saada ajantasainen tilannekuva tietoturvapoikkeaman käsittelystä mahdollista päätöksentekoa ja henkilökunnalle tiedottamista varten.

Poikkeamista siis ilmoitetaan Kyberturvallisuuskeskukseen / Viestintävirastoon ja valtionhallinnon VIRT-ryhmälle.

Keskuksen tulee jatkossa panostaa myös siihen, että se antaa tilannekuvaa relevanteille toimijoille (=toimialoittain).

Sote-toimialaa kiinnostavat tietenkin oman toimialan toimintaa uhkaavat poikkeamat. Tälle tilannekuvan antamiselle pitää tarkentaa toimialoittain pelisäännöt: mitä ilmoitetaan ja mille foorumille. Käytännössä foorumi koostuu ministeriöstä ja sosiaalihuollon ja terveydenhuollon (sairaanhoitopiirit) keskeisistä edustajista.

Ohjeessa olisi hyvä huomioida tulevia trendejä uhkien osalta.

1. Johdanto

Lausuntomme:

Myös palveluntuottajien rooli tulisi olla mainittuna. Asia tulisi huomioida mm. sopimuksissa.

Voisiko jo tässä olla mainittuna myös VIRT-toimintamalli ja sen rooli kokonaisuudessa.

Koska ohjeessa ei käsitellä toiminnan jatkuvuutta yleisissä ICT-häiriötilanteissa, tulisi tässä yhteydessä tarkemmin kuvata mitä tarkoitetaan ICT-häiriötilanteilla.

2. Tietoturvapoikkeaman hallintaprosessi

Lausuntomme:

Tietoturvapoikkeamien hallintaa tulee harjoitella. Poikkeamasta johtuvaa häiriötilannetta varten luotu organisaatiota tehtävineen ja vastuineen tulee testata säännöllisesti. Tämä, kuten muutinkin poikkeamien hallinnan valmiusvaatimukset, pitäisi saada osaksi organisaation johtamista sekä sen myötä tähän tulee turvata riittävät resurssit. Koko henkilöstön tietoisuus tietoturvapoikkeamien hallinasta organisaatiossa lisää myös yleistä tietoturvallisuutta ja ehkäisee tahattomien tietoturvapoikkeamien riskiä.

Tietoturvapoikkeamien hallinta ei jää yksin organisaation tehtäväksi vaan kyseessä on monien palveluntuottajien kanssa tehtävä yhteistyö. Ohjeessa voisi vielä nostaa esiin palveluntuottajien roolin.Keskeinen palveluntuottaja on Valtori. Viranomaisorganisaatiolla ei itsellään ole välttämättä valmiuksia tai mahdollisuuksia esimerkiksi seurata eri järjestelmien lokitiedostojen tapahtumia tai

käyttäjäpalautteesta tulevaa epäilyä, varsinkin kun reagointiaika poikkeamaan saattaa jäädä lyhyeksi.

Kaavion 2 tekstejä on vaikea lukea, koska teksti liian pientä ja vaikeasti erottuvaa. Toimintalaatikoita ja tekstiä tulisi suurentaa.

Ohjeessa tulisi olla tarkemmin kuvattuna miten hallintaprosessi on riippuvainen turvakontrolleista.

Onko kaikista poikkeamista aina tarpeen laatia raportti vai voiko olla sellaisia poikkeamia joista niitä ei olisi tarpeen laatia?

3. Tietoturvapoikkeamien käsittelykyvyn muodostaminen

Lausuntomme:

Luku 3.1.

Tietoturvapoikkeamien käsittelyryhmän roolit asiantuntija, omistaja, viestijä, usein myös tietotekniikkapalvelujen vastuuhenkilö tulevat kulloinkin mukaan siitä toiminnosta tai järjestelmästä, jota poikkeama on kohdannut. Ohjeessa voisi käsitellä aihetta, kuinka organisoida tällainen tapauskohtaisesti vaihteleva kokoonpano.

Osaamisvaatimukset olisi hyvä luetella tietoturvapoikkeamien hallitsemiseksi.

Luku 3.3.3.

Ohjeessa kerrotaan, että ” Tietoturvapoikkeaman havaitsemisen jälkeen on ensisijaisesti otettava yhteyttä Viestintäviraston Kyberturvallisuuskeskukseen”. Vaikka keskukseen voinee ottaa yhteyttä kuka tahansa poikkeaman havainnut (?) voisi täsmentää, että henkilön tulee ilmoittaa havainnostaan myös oman organisaationsa vastuutaholle.

Yhteystiedot ohjeeseen!

Luku 3.3.7

Ohjeessa voisi mainita suoraan, mikä (nykyään) on kansallinen turvallisuusviranomainen ja Kansallisen turvallisuusviranomaisen roolia ja tehtäviä tulisi avata tarkemmin.

Koska tietoturvapoikkeamien käsittelyryhmä tulisi ohjeen mukaan olla, olisiko myös ohjeistettava keitä ainakin ryhmässä tulisi olla, olisiko esim. joitakin rooleja organisaatiosta joiden ainakin pitäisi olla edustettuina. Olisiko ryhmä jollain tasolla myös luonteeltaan pysyvä? Ohjeessa voisi ottaa esiin myös liittymän palveluiden seurantaryhmiin.

Tietoturvapoikkeamien käsittelemiseksi ja yhteistyön toteutumiseksi tulisi olla joku, joka ylläpitää valtionhallinnon tilannekuvaa.

Poikkeamatilanteiden harjoittelua pitäisi järjestää myös eri tasoilla: valtioneuvostotaso, hallinnonalataso, organisaatiotaso.

3.3.9 Otsikko tummennettava. Viestintäsuunnitelmassa on huomioitava myös varasuunnitelma.

3.5. Poikkeamien havaitsemiseen, analysointiin ja käsittelyyn liittyvät velvollisuudet ja oikeudet on kirjattava sopimuksiin - voisiko liitteenä olla esimerkki? Huomioitava myös, vanhojen sopimusten päivitystarve.

4. Tietoturvapoikkeaman havaitseminen ja analysointi

Lausuntomme:

Tarpeen korostaa myös ulkoisten palveluntuottajien velvollisuutta ilmoittaa poikkeamista asiakkaalle.

Vakavuusasteen luokittelussa termit voisivat olla yhteismitallisia esim. vähäinen, vakava ja kriittinen.

5. Tietoturvapoikkeamaan reagointi

Lausuntomme:

Todistusaineistojen säilytysajalle voisi olla ohjeessa myös jonkinlaisia ehdotuksia.

6. Toipuminen tietoturvapoikkeamatilanteista

Lausuntomme:

-

Liite 1. Sanasto

Palautetta sanastosta, puuttuuko sanastosta esimerkiksi keskeisiä termejä?

ICT-häiriötilanne puuttuu sanastosta. Tämä olisi tärkeä ohjeen rajaukseen liittyen.

Turvakontrolli voisi myös olla sanastossa selitettynä.

Liitteet 2-5

Lausuntomme:

Kansainvälinen CERT-toimijoiden yhteistyöjärjestö on muuttanut määritelmää (Traffic Light Protocol) - onko tarpeen muuttaa tähän?

Liitteet 6-9

Lausuntomme:

Kaikki lait ja asetukset on kahteen kertaan listassa

Vaatimus-Excel ja vaatimukset

Palaute, kommentit ja kehittämisideat koskien vaatimuksia

Palaute, kommentit ja kehittämisideat koskien vaatimuksia

- riittääkö vahva suositus ”organisaatiolla on menettelytapa ja -ohje tietoturvahavaintojen keräämiseksi ja analysoimiseksi”?

- Vaatimus ”organisaation on ylläpidettävä tapahtumapäiväkirjaa tietoturvapoikkeamatilanteista” voisi koskea vain vakavampia poikkeamatilanteita pakollisena, muissa voisi olla suositus.

- Vaatimus ”organisaatiolla on ajantasaiset toipumissuunnitelmat järjestelmistä” on raskas, jos oltava kaikista järjestelmistä.

Muutokset vaatimuksiin aiempiin ohjeisiin verrattuna voisi näkyä myös liitteessä, jos eroja on.

Ehdotetut perustason vaatimukset ovat

-

Muuta palautetta tai toiveita ohjeluonnokseen liittyen

Mitä muuta palautetta haluatte antaa ohjeen valmisteluryhmälle tai VAHTIlle?

-

Ohje soveltuu organisaatiomme sellaisenaan tai sopivasti muokattuna:

-

Puhto Maarit
Sosiaali- ja terveysministeriö