Valvira
Sosiaali- ja terveysalan lupa- ja valvontavirasto

Dnro 6283/00.04.00.03/2016

10.10.2016

lausuntopalvelu.fi

Valtiovarainministeriön lausuntopyyntö (VM136:09/2013); Luonnos VAHTI 3/2016
Tietoturvapoikkeamatilanteiden hallinta

Lausunto VAHTI ohjeeseen tietoturvapoikkeamatilanteiden hallinnasta

Sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira) on tutustunut VAHTIn ohje-luonnokseen tietoturvapoikkeamatilanteiden hallinnasta.

Ohessa yleisiä kommentteja liittyen ohjeen sisältöön. Lopuksi lisäksi luku-kohtaisesti kommentit ohjeeseen.

Kokonaisuudessaan ohje on tarpeellinen, mutta rakennetta ja visualisointia selkeyttämällä siitä saisi käyttökelpoisemman ja helpommin hyödynnettävän. Ohjeessa olevat esimerkit ja liitteet ovat sellaisenaan hyödyllisiä.

Osassa prosessin vaiheista on visualisoitu tarkemmalla tasolla, mutta visualisointia kaipaisi kaikkien vaiheiden osalta luvun alkuun antamaan yleiskuvaa vaiheen/luvun sisällöstä. Tekstin kulku ei täysin vastaa kaavioiden kulkua, joka tekee kaavioista hieman irrallisia tekstiin nähden. Myös viittaukset kaavioihin/kuviin puuttuvat. Kuvien ja kaavioiden parempi vastaavuus tekstin kanssa helpottaisi ohjeen lukua.

Poikkeamatilanteiden hallinnan roolit ja vastuut voisi olla liitteinä RACI-taulukon muodossa, joita ohjeita hyödyntävä organisaatio voisi tarpeidensa mukaisesti muokata omaan organisaatioon sopivaksi.

Ohjeessa kehotetaan viestiä sidosryhmille ja muille viranomaisille poikkeamista, mutta tilanteet, joissa on viestittävä jäävät hieman epäselviksi ja organisaation itsensä arvioitaviksi. Olisi hyvä olla jokin ohjesääntö, minkä tyyppisien poikkeamien osalta aina tiedotetaan sidosryhmiä ja muita viranomaisia.

Luku 2. Kohdassa mainitaan " Tietoturvapoikkeamien hallintaprosessi koostuu useista eri osista. Prosessin tarkoituksena on varautua häiriötilanteisiin, turvata toiminnan jatkuvuus ja pyrkiä estämään häiriötilanteiden muodostuminen jatkossa."

Lisäksi tulisi mainita jo tässä kohtaa poikkeamien aiheuttaman vahingon minimointi, joka on myöhemmin ohjeessa kyllä mainittu.

Luku 3.2 Tietoturvatiedon luokittelu-kohdassa Traffic Light Protocol (TLP):n käyttö ja yhteys käytäntöön jää jokseenkin irralliseksi. Ohjeessa on kyllä hyvä tuoda esiin poikkeamasta viestinnän sisällön suojaaminen ja asianmukainen tiedon käsittely. Se, että kyseinen luokittelu saattaa olla käytössä jossakin

kirjaamo@valvira.fi Puhelin 0295 209 111 www.valvira.fi

PL 210, 00281 Helsinki
Mannerheimintie 103b, 00280 Helsinki
Faksi 0295 209 700

Koskenranta 3, 96100 Rovaniemi
Faksi 0295 209 704

organisaatiossa jättää luokittelun esittämisen tarpeenmukaisuuden tässä ohjeessa kuitenkin kyseenalaiseksi.

Luku 5.3 Kohdassa 5.3.1 mainitut luvut 4.3.1 ja 2.3 puuttuvat ohjeesta.

Viestintää sidosryhmille ja muille viranomaisille tulisi selkeyttää ohjeeseen. Viestintää käsitellään useammassa luvussa ja lukijalle ei jää selvää kuvaa halutusta yhteydenpidon ja tiedottamisen tasosta poikkeamatilanteiden osalta. Ohjeessa kehotetaan viestiä sidosryhmille ja muille viranomaisille poikkeamista, mutta tilanteet joissa on viestittävä jäävät hieman epäselviksi. Olisi hyvä luoda tarkempi ohjesääntö, minkä tyyppisien poikkeamien osalta aina tiedotetaan mm. sidosryhmiä ja muita viranomaisia.

Kokonaistilannekuvan muodostamisesta ja tilannetietoon reagointiin olisi hyvä olla lukunsa.

Ohjeen liitteenä ehdotetut perustason vaatimukset ovat Mahdollista täyttää Valvirassa, mutta vaatii jonkin verran toimintamme kehittämistä.

Ohje soveltuu organisaatiomme hyvin sellaisenaan.

Ylijohtaja Marja-Liisa Partanen

Erityisasiantuntija Mika Kuivamäki