

19.1.2012

Valtiovarainministeriö
PL 28
00023 Valtioneuvosto

Viite VM:n lausuntopyyntö VM1814/00.01.00.01/2011

STM:N LAUSUNTO LUONNOKSESTA ICT-VARAUTUMISEN VAATIMUKSET OHJEESTA

Pyydettyinä lausuntona ICT-varautumisen vaatimukset -ohjeesta sosiaali- ja terveysministeriö toteaa seuraavan.

Yleistä

Ohjeluonnos on tiivis eikä liian pitkä. Luettavuuden ja ulkoasun kannalta ohje vaatii vielä viimeistelyä.

Tietoturvasojen vaatimukset ja ICT-varautumisen vaatimukset ovat hyvin lähellä toisiaan, osittain jopa päällekkäisiä.

Varautumisen vaatimuksissa on hyvin paljon samaa tekemistä ja sisältöä kuin tietoturvasojen vaatimuksissa. Varautumiseen liittyvät vaatimukset pitää tarkentaa selkeämmin tai organisaatioita helpottaisi, jos olisi mahdollista selvittää yhteisillä vaatimuksilla päivittämällä tietoturvaso-vaatimuksia.

Varautuminen on olennainen osa häiriötilanteiden ennakointiin liittyvää toimintaa ja on tarpeen kiinnittää huomiota sen varmistamiseen koko valtionhallinnossa. Yhtenäiset toimintamallit ja vaatimukset helpottavat jatkuvuussuunnittelua ja riskienhallintaa.

Varautuminen vaatii usein erillisiä investointeja ja henkilöresursseja, joita organisaatiossa ei kuitenkaan ole mahdollista tarjota.

Valtion yhteisten palveluiden ja järjestelmien myötä on tarpeen ja tarkoituksenmukaista tarjota näille palveluille ja järjestelmille keskitettyjä ratkaisuja varautumiselle: varajärjestelmiä, varalaitteita jne.

Kommentit:

”Ministeriöiden ohjaamina hallinnonalojen ja virastojen tulee: määrittää kullekin organisaatiolle sekä palveluille ja järjestelmille tavoiteltava varautumisen taso sekä määrittää aikataulu palveluiden toteuttamiseksi määritetyn varautumistason mukaisesti”



Kommentti: Kyseinen työ vaatii merkittävästi resursseja sekä sen jälkeinen ICT riskien- ja jatkuvuudenhallinta prosesseineen myös.

”Kunkin ICT-varautumisen tason saavuttamiseksi viranomaisten on ensin toteutettava tietoturva-asetuksen mukainen tietoturvallisuuden perustaso, ja sen lisäksi kaikki kyseisen ICT-varautumisen tason sekä sitä alempien tasojen vaatimukset”

Kommentti: Tämä on erittäin raskas vaatimus ja edellyttää paljon voimavaroja.

Samoin edellytetään, että ”järjestelmän tai palvelun ostajan velvollisuus on varmistua, että hankinnan kohde täyttää sille asetetut varautumisen vaatimukset.” Tämän lisäksi perus- ja korotetulla tasolla pitää tehdä tasojen todentaminen, korotetulla tasolla ulkopuolista arvioijaa käyttäen. Onko näin myös palvelukeskusten tarjoamien palvelujen kohdalla tehtävä? Eivätkö nämä palvelut pidä olla oikealla varautumisen tasolla jo ennen kuin niitä tarjotaan valtion organisaatioille? Todentamisen on joka tapauksessa tapahduttava näiden palveluiden osalta esimerkiksi valtiovarainministeriön toimesta, ei asiakkaiden.

Yleisesti ottaen vaatimukset ovat raskaita organisaatioiden yksin toteuttaa. Tarvitaan selkeät ohjeet, yhteistä koulutusta ja apuvälineitä työtä helpottamaan. ICT-varautumisen tasojen saavuttamisen helpottamiseksi tarvitaan samanlaisia yhteishankkeita valtiovarainministeriön tarjoamina kuin on nyt meneillään tietoturvasasojen osalta.

Aikataulut tasojen saavuttamiseksi tulee olla realistiset ja siirtymäajan riittävä huomioiden tietoturvasasojen vaatimusten täyttämisen edellyttämä määräaika.

Osastopäällikkö


Raimo Ikonen

Järjestelmäpäällikkö


Maarit Puhto

