STM

Lausunto

05.01.2021

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

Yleisesti linjaukset ovat hyviä.

Tietoturvallisuuden ohjaus on Suomessa hajautunutta. Sektoriministeriön lisäksi toimintaa ohjaavat sekä

valtiovarainministeriö että liikenne- ja viestintäministeriö. Näiden lisäksi tietosuojan osalta oikeusministeriö ja

varautumisen osalta työ- ja elinkeinoministeriö. Sosiaali- ja terveysministeriö ehdottaa, että yleinen vastuu

tietoturvallisuuden kokonaisuudesta keskitetään selkeästi yhdelle ministeriölle nykyisen kahden sijasta.

Toimialakohtaisen vastuun tulisi säilyä sektoriministeriöllä. Kyberturvallisuuskeskusta ohjaavana ministeriönä LVM

olisi luonteva taho ottamaan vastuun kyberturvallisuudesta kokonaisuutena. Tässä yhteydessä tulee pohtia myös

eri toimijoiden, yksityiset yritykset mukaan lukien, tukemista joko rahallisesti tai tarjoamalla keskitetysti

kyberturvallisuuden asiantuntijapalvelua myös heille.

Linjauksissa ei oteta kantaa tietojen luokitteluun. Tiedonhallintalautakunnan alaisuudessa on valmistelussa ohje

turvaluokitellun tiedon käsittelystä, mutta kyseinen luokittelu on rajoitettu tiettyyn erikoistarkoitukseen eikä ole

käytettävissä laajasti yhteiskunnassa. Tietojen luokittelu ja yhdenmukainen käsittely ovat keskeisiä keinoja

pyrittäessä tietojen turvaamiseen. STM esittää, että käynnistetään työ, jossa määritellään yleisesti yhteiskunnassa

käytettävät turvaluokat ja niiden käsittelyperiaatteet.

Vaatimus ISO 27001-sertifioinnista merkittäville toimijoille on hyvä, mutta kuten myöhemmässä tekstissä todetaan,

sen saavuttaminen pienille toimijoille on vaikeaa ja kallista. Sosiaali- ja terveydenhuollossa suurin osa toimijoista

on pieniä organisaatioita. Tämä tarkoittaa sitä, että nämä toimijat eivät olisi sertifiointivelvollisuuden piirissä.

Ehdotettu siirtymäaika on lyhyt. Vaatimusten sisällyttäminen sektorikohtaiseen lainsäädäntöön ja ohjeistuksiin vie

aikaa, samoin kuin niiden toteuttaminenkin organisaatioissa.. Tämä vaatimus lisää myös sertifioinnin tarvetta ja voi

aiheuttaa sertifiointipalveluiden ruuhkautumisen. Ehdotettu määräaika on riittävä lainsäädäntömuutoksiin ja

sektorikohtaisten ohjeiden valmisteluun, mutta liian lyhyt siihen, että kaikki merkittävät organisaatiot olisi sertifioitu.

Väliraportin muut osat, kommentit:

Raportissa on käsitelty laajasti malleja, jotka liittyvät organisaatioiden motivaatioon ylläpitää riittävän korkeaa

tietoturvallisuuden tasoa. Sosiaali- ja terveydenhuollon näkökulmasta on kuitenkin jäänyt kaksi näkökulmaa

käsittelemättä.

Sosiaali- ja terveydenhuollossa tasapainoillaan jatkuvasti salassa pidettävien tietojen suojaamisen ja toiminnan

kannalta elintärkeiden tietojen saatavuuden kanssa. Käsiteltävät tiedot ovat usein hyvin arkaluontoisia ja salassa

Hakari Kari
Sosiaali- ja terveysministeriö

Virtanen Teemupekka
STM