Lausunto

05.01.2021 71/0202/2020

Asia: VN/24348/2020

Selvitys tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla; työryhmän väliraportti

Lausunnonantajan lausunto

Ehdotukset poliittisiksi linjauksiksi, kommentit:

Yleisesti

STUKin näkemyksen mukaan väliraportissa esitetyt linjaukset ovat kokonaisuutena hyviä ja tarpeellisia. STUK pitää erittäin kannatettavana, että kriittisille toimialoille säädetään tietoturvaa koskevia nykyistä yksityiskohtaisempia ja selkeämpiä velvoitteita, kunhan riittävä jousto mahdollistetaan esimerkiksi poikkeama- ja siirtymäsäännösten muodossa. Tämä on omiaan lisäämään alalla toimivien viranomaisten, toiminnanharjoittajien ja palveluntarjoajien toimintaedellytyksiä, edistämään tietoturvallisuutta sekä selkeyttämään ja yhtenäistämään viranomaisten keskinäisiä menettelytapoja.

STUK toteaa, ettei kriittisiä toimialoja ole määritelty nyt lausuttavana olevassa väliraportissa. STUK katsoo, että yhdeksi kriittiseksi toimialaksi tulisi määritellä säteilyturvallisuus- ja ydinturvallisuustoimialat, jotka kuuluvat sosiaali- ja terveysministeriön (STM) ja työ- ja elinkeinoministeriön (TEM) hallinnon alaan. STM:n roolia ei raportin linjauksissa ole nostettu esille, miltä osin STUK esittää raporttia täydennettäväksi. Jatkotyöskentelyssä olisi tarpeen selkeyttää sitä, miltä osin vaatimuksia on tarkoitus kohdentaa viranomaisiin, miltä osin myös muihin tahoihin, kuten toiminnanharjoittajiin, alihankkijoihin ja palveluntarjoajiin.

Linjaus kohta 5

Poliittisten linjausten 5. kohdan mukaan tavoitteena on selvittää viranomaisten tarpeet teknologisille ratkaisuille salassa pidettävän ja turvaluokitellun tiedon vaihtamiseen.

STUK toteaa, että on tärkeää, että viranomaisilla on laaja-alaisesti käytössään viranomaisten väliseen operatiiviseen ja muuhun tiedonvälitykseen soveltuvat tietoturvalliset työkalut ja toimintaedellytykset. STUK pitää kannatettavana, että viranomaisilla olisi jatkossa yhdenmukaiset työkalut salassa pidettävän ja turvaluokitellun tiedon vaihtamiseen. Tämä vähentäisi riskiä siitä, että turvallisuusluokiteltua tietoa käsitellään välineissä, joiden tietoturvallisuuden täyttymisessä on tai voi olla puutteita sekä siten osaltaan vähentäisi riskiä tiedon joutumisesta sellaisille tahoille, joilla ei

ole oikeutta salassa pidettävään tietoon. Nykyisin viestintäkanavia on käytössä useita ja niiden tietoturvallisuudesta on esitetty erilaisia näkemyksiä, mistä aiheutuu käytännössä haasteita.

Linjaus kohta 7

Kriittisille toimialoille määritellään selkeät ja oikeasuhtaiset tietoturvavaatimukset lainsäädännössä. Viranomaisilla on oltava laissa riittävät valtuudet antaa tietoturvaa koskevia sitovia määräyksiä.

STUK pitää tärkeänä, että lainsäädännössä on kriittisten toimialojen osalta riittävät ja selkeät tietoturva- ja tietosuojavaatimukset, jotka kuitenkin mahdollistavat riittävän joustavuuden. Edellä mainittujen vaatimuksien todennettu toteutuminen riittävällä tasolla on edellytyksenä luottamukseen rakentamiselle ja tiedonhallintalain edellyttämälle tiedonvaihdolle ja yhteentoimivuudelle. Lainsäädäntö edistää osaltaan sitä, että ja tietoturva ja -suoja huomioidaan ja toteutetaan kussakin organisaatiossa laadukkaasti ja riittävä osaaminen ja resurssointi huomioiden. Samalla se yhdenmukaistaa menettelytapoja ja sujuvoittaa toisaalta viranomaisten välistä, että toisaalta viranomaisen ja yksityisten tahojen välillä tapahtuvaa työskentelyä.

STUK toteaa, että sillä on säteilylain (859/2018) 67 §:n ja ydinenergialain (990/1987) 7 q ja 7 r §:n nojalla mahdollisuus antaa sitovia tietoturvaan liittyviä määräyksiä osana säteily- ja ydinturvallisuuteen liittyviä turvajärjestelyvaatimuksia.

Linjaus kohta 11 ja 12

Väliraportin 11 kohdan mukaan kriittisille toimialoille säädetään velvoite säännöllisesti auditoida kriittiset tieto- ja tietoliikennetekniset prosessit ja toiminnot. Auditointimalli määräytyy laissa riskiperusteisesti sen mukaan, kuinka kriittistä tietoa sisältävästä järjestelmästä tai prosessista tai toiminta ohjaavasta on kyse. Määrittelyssä huomioidaan taloudelliset vaikutukset. Väliraportin 12 kohdan mukaan Kriittisten toimialojen merkittävimpien toimijoiden tulee osoittaa käyttävänsä tietoturvallisuuden hallintajärjestelmää ISO 27001 -sertifioinnilla vuoden 2024 loppuun mennessä.

STUK pitää linjauksen 11-12 kohdan ehdotuksia kannatettavina. STUK toteaa, että työ edellyttää sillä jatkokehitystyötä ja resurssointeja etenkin tietoturvan arvioinnin osalta. Olennaista on, että sääntely mahdollistaa riittävät jousto- ja poikkeamamahdollisuudet sekä siirtymäajan. Raportista ei käy ilmi, keitä merkittävillä toimijoilla tarkoitetaan, ja onko määrittely tarkoitettu koskemaan vain viranomaisia.

Linjaus kohta 15

Väliraportin 15. kohdan linjauksen mukaan ydinvoimaloiden tietoturvallisuusvaatimuksia koskevan ohjeistuksen velvoittavuus varmistetaan. Vastuutahoksi on kirjattu STUK.

STUK toteaa, että ohjeistus on tältä osin ydinenergialain 7 r §:n mukaisesti velvoittavaa, vaikka kyseiset vaatimukset onkin otsikoitu ohjeiksi. Ydinlaitoksen tietoturvallisuuden hallinnasta annetussa ohjeessa YVL A.12 asetetaan ydinlaitoksen luvanhaltijalle tietoturvallisuutta koskevat vaatimukset. Nämä vaatimukset eivät koske vain ydinvoimalaitoksia, vaan kaikkia ydinenergialain 3.1 §:n 5 kohdan mukaisia ydinlaitoksia. Tämän lisäksi STUKin määräyksessä STUK Y/3/2020 annetaan

tietoturvallisuutta koskevia vaatimuksia koskien ydinenergian käyttöä laajemmin. Kyseiset vaatimukset eivät koske vain ydinlaitoksen luvanhaltijoita, vaan määräyksen soveltamisalan mukaisesti tietyiltä osin muitakin ydinenergian käyttäjiä.

Ohjeiksi nimettyjen vaatimusten osalta asia on tarkoituksenmukaista muuttaa vastaamaan paremmin nykyisen perustuslain vaatimuksia ydinenergialainsäädännön kokonaisuudistuksen yhteydessä, jonka käynnistämistä parhaillaan selvitetään työ- ja elinkeinoministeriössä. Eduskunnan perustuslakivaliokunta on kiinnittänyt huomiota siihen, että ydinenergialakia on poikkeuslakina useaan otteeseen uudistettu ja lain systematiikasta on muodostunut sekava. Valiokunta on edellyttänyt, että sääntely kokonaisuudessaan arvioidaan voimassa olevan perustuslain kannalta (PeVL 22/2020 vp).

Edellä lausutun takia STUK katsoo, että linjauksen vastuutahoksi olisi kohdan 15 osalta nimettävä työ- ja elinkeinoministeriö.

Linjaus kohta 23 ja 24

Arvioidaan tarve säätää Valtorin tietosuojaa ja tietoturvaa koskevista vastuista ja velvoitteista vastaavasti kuin on jo tehty Valtion talous- ja henkilöstöhallinnon palvelukeskuksen (Palkeet) osalta. Lähtökohtana on, että Valtorin tarjoamien ja välittämien kriittisten palveluiden on täytettävä voimassa olevan viranomaisten auditointityökalun (Katakri) TL IV -tason vaatimukset.

STUK kannattaa lainsäädännöllisiä toimia 23. kohdanmukaisesti. Tilanne on ollut ja on jossain määrin epäselvä tietoturvan ja -suojan osalta. STUK kannattaa esitettyä24. kohdan linjausta Valtorin resursseista.

Väliraportin muut osat, kommentit:

-

Koskinen Kaisa
Säteilyturvakeskus

Välimäki Minna
Säteilyturvakeskus