

Asia: VN/36693/2023

## Lausuntopyyntö Suomen kyberturvallisuusstrategiasta

### Lausunnonantajan lausunto

#### **Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään**

Pohjois-Pohjanmaan hyvinvointialue Pohde kiittää mahdollisuudesta lausua kansallisen kyberturvallisuusstrategian luonnosta.

Kansallinen kyberturvallisuusstrategia on kokonaisuutena laadukas ja siihen on sisällytetty paljon keskeisiä asioita kansallisen turvallisuuden parantamiseksi. Toimeenpanon osalta toivomme selkeitä velvoittavia määräyksiä toimeenpanon helpottamiseksi. Erityisesti kvanttilaskennan aiheuttamien riskien pienentämisestä tulisi laatia kansallisen tason suunnitelma mahdollisimman nopeasti. Toimeenpanon osalta taloudellisten vaikutuksien realistinen arviointi on Pohteen näkökulmasta ensiarvoisen tärkeää. Kansallisen kybertilannekuvan määrittely selkeästi ja ymmärrettävästi tulisi myös olla yksi prioriteettitehtävistä.

#### Kansallinen tilannekuva ja yhteinen tilanneymmärrys

Tällä hetkellä kybertilannekuvan määritelmää ei ole, tai se on epäselvä. Kansallista kybertilannekuvaa muodostetaan puutteellisilla tiedoilla, koska yhteiskunnan toiminnan kannalta kriittisten toimijoiden ei ole pakko toimittaa tietoja tilannekuvan muodostamiseksi. Näin ollen kansallinen kybertilannekuva voi muodostua virheelliseksi.

Tilannekuva ja tilannekuvatuotteet tulisi määritellä selkeästi ja asettaa pakottavat vaatimukset yhteiskunnan toiminnan kannalta kriittisille toimijoille tilannekuvatiedon tuottamisesta. Esimerkiksi Havaro voitaisiin määrätä otettavaksi käyttöön teknisen tilannekuvatiedon keräämiseksi.

Kansallisesti tulisi perustaa palvelu millä voidaan automaattisesti ja jatkuvasti valvoa kriittisten toimijoiden julkisia IP-osoitteita haavoittuvuuksien ja virheellisten konfiguraatioiden havaitsemiseksi.

Yhdeksi tilannekuvatuotteeksi voitaisiin asettaa minimivaatimukset julkisille internet-palveluille, jotka ovat tarkoitettu kansalaisten tai viranomaisten käyttöön. Vertaamalla vaatimuksia toteutuneeseen voitaisiin helposti seurata yhteiskunnan toiminnan kannalta kriittisten organisaatioiden tasoa.

"Nykytilassa viranomaisilla on arvioitu olevan riittämättömät toimintaedellytykset tehokkaasti varautua ja torjua vakavimpia, kansallista kyberturvallisuutta ja maanpuolustusta vaarantavia kyberuhkia. Viranomaisten keskenään koordinoimassa ja analysoimassa tilannekuvassa ja tilanneymmärryksessä on edelleen kehitettävää. Myöskään julkisten palveluiden kyberturvallisuustietoja ei nykytilassa riittävästi jaeta strategia-, normi-, resurssi- ja informaatio-ohjauksen näkökulmista kaikkien julkisen hallinnon ja elinkeinoelämän toimijoiden välillä."s.19

"Suomessa ei toistaiseksi ole kuitenkaan riittävässä laajuudessa säädetty viranomaisten välisestä koordinaatiosta ja yhteistoiminnasta kybertoimintaympäristössä, eikä säännöksissä ole otettu riittävästi huomioon kybertoimintaympäristön erityispiirteitä kyberuhkiin vastaamisessa ja tiedonvaihdossa." s. 19

Nämä ovat erittäin tärkeitä havaintoja ja toivomme, että kybertilannekuva määritellään selkeästi. Tämän lisäksi eri viranomaisten väliset vastuut olisi hyvä selkeyttää, sekä rakentaa järjestelmä minkä avulla kyberturvallisuustiedot voidaan jakaa ketterästi eri toimijoiden kesken.

Oleellista olisi myös kyber- tai tietoturvapoikkeamien ilmoittamiseksi niin sanottu yhden luukun periaate, eli ilmoittajaorganisaatio voisi ilmoittaa kaikista havainnosta yhtä kanavaa pitkin. Tällä hetkellä erityisesti sote-alalla tietoturvapoikkeamista raportoimisen vaatimukset ovat epämääräiset ja ne tulisi yhtenäistää.

## Kvanttitekniologiat

" Kvanttitekniologian nopea kehittyminen haastaa entisestään tämänhetkistä kansallista salauskyykyä. Suomi on jäänyt verrokkimaiden suhteen jälkeen salaustekniikoiden kansallisten ratkaisuiden kehittämisessä, eikä Suomessa ole velvoittavaa lainsäädäntöä hyväksytyjen salaustekniologioiden käytölle." s.17

Suomen tulisi valmistautua kvanttilaskennan aiheuttamiin kyberriskeihin nopealla aikataululla ja pakottavin määräyksin tai lainsäädännön keinoin. Kvanttiturvallisten salausmenetelmien ja algoritmien käyttöönottamiseksi tiedonsiirrossa sekä tallennuksessa tulisi laatia selkeä suunnitelma, vaatimukset sekä valvontakeinot yhteiskunnan toiminnan kannalta kriittisille toimijoille.

## Keskitettyt kyberturvallisuuspalvelut

"Hyvinvointialueet ja kunnat tarvitsevat kyberturvallisuuden varmistamisessa nykyistä enemmän tukea, kuten keskitettyjä kyberturvallisuuspalveluja." s. 18

Keskitettyt kyberturvallisuuspalvelut ovat lähtökohtaisesti kannatettava ajatus. Hyvinvointialueiden näkökulmasta tarvitaan ensisijaisesti selkeitä ja valmiita vaatimuksia, valvontaa ja neuvontaa, sekä kunnolliset mittaustyökalut tekniselle- ja hallinnolliselle tietoturvalle.

## Termistö

Lainsäädännön ja määräyksien selkiyttämiseksi olisi hyvä laatia kansallinen kyberturvallisuuden termistö. Yhtenäinen termistö on edellytys sille, että voimme puhua kybertilannekuvasta oikeilla termeillä, jotka ovat kaikkien samalla tavalla ymmärrettävissä. Yhtenäinen termistö vaikuttaa myös kyberturvallisuustason mittaamiseen. Esimerkiksi DVV käyttää Digiturvallisuuden kokonaispalvelussaan termiä digiturvallisuus eri asiayhteyksissä, jota ei kuitenkaan löydy mistään lainsäädännöstä eikä ole yleisesti maailmalla käytössä. Erityisesti sote-alalla käsitellään edelleen paljon paperista salassa pidettävää tietoa, jota digitaalinen turvallisuus ei koske.

Esimerkiksi tietoturvapoikkeama, tai tapahtuma, määritellään usein saatavuuden, eheyden ja luottamuksellisuuden kautta, mutta määrittelyssä ei erotella esimerkiksi tavallisia tuotannollisia häiriöitä ulkopuolisen toimijan aiheuttamista poikkeamista tai uhkista.

Haataja Ilkka  
POHDE

Huhtala Anssi  
Pohjois-Pohjanmaan hyvinvointialue