Työ- ja elinkeinoministeriö
Arbets- och näringsministeriet

Lausunto

15.8.2024

VN/1/2024
VN/1/2024-TEM-82

TEMin vastaus lausuntopyyntö Suomen kyberturvallisuusstrategiasta

Työ- ja elinkeinoministeriö
Lausunto
09.08.2024
Asia: VN/36693/2023

Lausuntopyyntö Suomen kyberturvallisuusstrategiasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Työ- ja elinkeinoministeriö kiittää mahdollisuudesta lausua valtioneuvoston periaatepäätöksestä Suomen kyberturvallisuusstrategiaksi vuosille 2024-2035. Ministeriö on osallistunut strategian valmisteluun työryhmän jäsenenä.

Yleiset huomiot strategian sisältöön liittyen
Luonnos Suomen kyberturvallisuusstrategiksi on laaja ja kattava kokonaisuus, jossa tuodaan monipuolisesti esille kyberturvallisuuteen liittyviä yleisiä elementtejä, mutta myös työ- ja elinkeinoministeriön hallinnonalalle relevantteja teemoja. Esimerkiksi strategiassa kuvataan kyberturvallisuusalan ekosysteemin merkitystä, ja strategia huomioi myös sen, miten korkea kyberturvallisuuden taso hyödyttää kaikkia, ml. yritystoiminta toimialasta riippumatta, osaamiskeskittymien kehittymistä ja tuo investointeja ulkomailta.

Strategissa tuodaan esille, miten toimintaympäristön muutoksen vuoksi tiedonvaihto ja siihen käytettävät välineet sekä tilanneymmärryksen muodostaminen eivät nykyisellään ole tarpeeksi riittäviä. Lisäksi strategiassa todetaan, että lainsäädännön, viranomaisten toimivaltuuksien ja yhteistyörakenteiden ja –verkostojen kehittäminen onkin välttämätöntä. Ministeriö pitää tärkeänä, että edellä mainittuja asioita kehitetään ja edistetään yhteistyössä eri toimijoiden kesken konkreettisella toimenpideohjelmalla. On myös tärkeää, että eri tahojen välistä tiedonvaihtoa ja yhteisiä toimintatapoja kehitetään. Yhteistyön, tiedonhankinnan, -jakamisen sekä –vaihdon merkitys tulee tulevaisuudessa entisestään korostumaan, esim. toimintaympäristön ajantasaisen tilannekuvan sis. kyberuhkat muodostamisen ja seurannan yhteydessä.

Ministeriö pitää tärkeänä sitä, että kyberturvallisuusstrategian tavoitetilasta johdettuja kehittämisehdotuksia priorisoidaan samassa yhteydessä, kun kehittämisehdotuksia suunnitellaan ja

Postiosoite Postadress Postal Address	Käyntiosoite Besöksadress Office	Puhelin Telefon Telephone	Faksi Fax Fax	s-posti, internet e-post, internet e-mail, internet
Työ- ja elinkeinoministeriö				
PL 32 00023 Valtioneuvosto	Aleksanterinkatu 4 Helsinki	0295 16001 +358 295 16001	09 1606 2160 +358 9 1606 2160	kirjaamo.tem@gov.fi www.tem.fi

tarkennetaan. On erityisen tärkeää, että olemassa olevat resurssit saadaan kohdennettua oikein ja kustannustehokkaasti. Lisäksi ennen kehittämisehdotusten toimeenpanoa on hyvä varmistaa, että riittävät edellytykset toimeenpanolle on olemassa, jotta kehittämisehdotusten toimenpiteet saadaan käytännön tasolla konkreettisesti toteutettua.

Pilari I: Osaaminen, teknologia ja TKI
Pilarissa I strategisena tavoitteena on: "Kyberturvallisuuden tietopääoma on suojattu ja Suomi pyrkii kriittisen salausteknologian osalta omavaraisuuteen.” Lisäksi asiaa on muotoiltu tekstissä myöhemmin seuraavasti: "Pyrimme salausteknologiseen omavaraisuuteen" ja "Suomen yhtenä strategisena tavoitteena on olla kriittisten salausteknologioiden osalta omavarainen ja kvanttiuhkaan varautunut valtio 2030-luvun alkuun mennessä. Herää kysymys, onko realistista, että Suomi olisi omavarainen kriittisten salausteknologioiden osalta. Jos ajatellaan salausteknologioita pyramidina, joka rakentuu leveästä pohjasta kohti soveltamisen huippua, tämä vaatii perustutkimuksesta ja esim. kvanttiteknologiasta alkaen hyvin laajaa osaamista ja ekosysteemiä, ja huipulla taas tarvitaan erilaisia, yleensä kaupallisia sovelluksia ja palveluntarjoajia. Tämän tarjoaminen kotimaisesti kokonaisuutena on erittäin haastavaa. Toinen kysymys on, mitä tarkoittaa kriittinen salausteknologia. Jos se tarkoittaa edellä kuvatun pyramidimallin mukaisesti, että tietyn tärkeän salauksen onnistumiseen tarvittavat komponentit ovat kansallisesti järjestettyjä pohjalta sovellukseen saakka, niin tämä on myös kova vaatimustaso. Tulisi harkita, voisiko omavaraisuuden sijaan pyrkiä, esim. siihen, että Suomi pystyy takaamaan pääsyn kriittisiin salausteknologioihin omien kyvykkyyksien pohjalta yhteistyössä liittolaisten/kumppanien kanssa. Myös kansallisen kvanttistrategian valmistelussa pyritään siihen, että suomalaisilla toimijoilla on pääsy luotettaviin arvoverkostoihin samanmielisten maiden kanssa.

Kvanttiteknologiasta ja salaustekniikoista lukiessa lukijalle jäi hieman epäselväksi, mikä valtion rooli tulee jatkossa olemaan liittyen kvanttiteknologian hyödyntämiseen ja salaustekniikoiden osalta sekä niiden kehittämisessä, jotta mahdollisesti Suomen ja yritysten kilpailukykyä saadaan lisättyä ja kasvatettua. Ehdotamme, että valtion roolia voitaisi hieman avata ja tarkentaa joko esim. strategian liitteisiin tai asiasta voisi käydä tarkempaa keskustelu toimenpidesuunnitelman laatimisen yhteydessä.

Pilari I osa-alueen strategiset tavoitteet ovat kattavat. Sen sijaan resursoinnin ja toimeenpanon osalta kirjaukset ovat aika niukahkoja: resurssien osalta viitataan ainoastaan järjestöihin, vaikka keskeinen toimija ovat eri oppilaitokset, yksityiset koulutuksen järjestäjät, ml. työvoimakoulutus ja yritysten henkilöstökoulutus. Kehittämisehdotuksissa osaamisen osalta on kirjattu "Kehitetään osaamista sekä kansalaisten ja kansalaisyhteiskunnan kybervalmiuksia ja varautumista.", mikä jää melko yleiselle tasolle. Toimijoissa ei juuri mainita koulutussektorin ja osaamisen kehittämisen toimijoita. Palveluntuottajina mainitaan tutkimuslaitokset ja korkeakoulut, mutta keskeisiä osaamisen levittäjiä voisivat olla myös muut koulutusasteet, yksityiset koulutuksen järjestäjät, työvoimaviranomaiset, yritykset ja kansalaisopistot. Järjestöjen rooli sen sijaan on vahvasti kirjattu.

Voisi olla tarpeen suunnitella mekanismia, jossa turvallisuusviranomaiset kävisivät keskustelua osaamisen kehittämisen toimijoiden kanssa, jotta tarvittavaa koulutusta osattaisiin järjestää? Olisi mahdollista esittää, että työvoimakoulutustarjontaa suunniteltaessa työllisyysalueet ottaisivat huomioon myös kyberturvallisuuteen liittyvät osaamistarpeet. Tarpeet eivät kuitenkaan välttämättä ole työvoimaviranomaisten tiedossa, joten osaamistarpeiden kommunikointi koulutussektorin toimijoille olisi tarpeen.

Ministeriö pitää hyvänä asiana sitä, että kyberturvallisuusstrategiassa on huomioitu mm. kansalaisten medialukutaito ja sen tärkeys, tietoisuus kyberturvallisuudesta ja siihen liittyvistä riskeistä. Kansalaisten tietoisuuden kasvattamisella kyberturvallisuuden osaaminen tulee jatkossa lisääntymään. On oletettavaa, että esimerkiksi uusien teknologioiden ja kehityksen myötä myös verkkorikollisuus ja siihen liittyvät yritykset määrällisesti tulevat jatkossa kasvamaan. Tekoäly tarjoaa

verkkorikollisille uusia tapoja toteuttaa erilaisia huijauksia ja huijausyrityksiä tms. Sen lisäksi, että vastuullisesti kybertoimintaympäristössä toimivat kansalaiset lisäävät merkittävällä tavalla yhteisöjen ja organisaatioiden turvallisuutta on tärkeää, että myös kansalaisten oma turvallisuus tulee huomioitua.

Ministeriö pitää tärkeänä, että kyberharjoitustoimintaa, siihen liittyviä käytäntöjä ja –ympäristöjä kehitetään aktiivisesti vastaamaan toimintaympäristössä tapahtuvia muutoksia, jolloin harjoitustoiminnasta tulee tehokkaampaa ja samalla tulee huomioitua toimintaympäristön asettamat vaatimukset ja kyseisen ajanhetken uhkatilanteet. Ajantasaisella kyberharjoitustoiminnalla rakennetaan ja vahvistetaan koko yhteiskunnan kyberresilienssiä. Lisäksi on tärkeää, että harjoitustoimintaa kehitetään yhteistyössä eri toimialojen ja hallinnonalojen välillä, jossa mukana ovat eri ministeriöt, virastot ja kunnat.

Liite 1: Kyberturvallisuuden kansallinen yhteistoimintamalli
Ministeriö pitää tärkeänä sitä, että julkinen sektori yhdessä elinkeinoelämän kanssa tarjoaa jatkossakin keskitettyjä kyberturvallisuuspalveluita, jotka tukevat organisaatioita ja kansalaisia varautumisessa erilaisissa häiriötilanteissa, jolloin varmistetaan yhdenmukainen toiminta, vältytään päällekkäisiltä kustannuksilta ja yleisesti tarvittavat palvelut kuten verkkokoulutukset, kybertilannekuva ja ohjeistus ovat kaikkien saatavilla. Ministeriö ehdottaa, että parhaiksi ja hyvin toimiviksi todettuja käytänteitä, poikkeamatilanteissa opittuja toimintatapoja ja niihin liittyviä materiaaleja jaetaan laajemmin kaikkien saataville ja nähtäviksi. Esimerkiksi DVV on tehnyt hyvää työtä ja edistänyt digiturvaa mm. digiturvatilaisuuksissa tuoden avoimesti esiin kyberhyökkäyksistä saatuja oppeja. Tätä ja vastaavaa toimintaa on hyvä jatkaa ja kehittää eteenpäin myös tulevaisuudessa.

Strategia sisältää yhteiskunnan elintärkeän toiminnon määritelmän. Määritelmää olisi hyvä täydentää viittauksilla lainsäädäntöön, lainsäädännön nojalla annettuihin normeihin tai muihin viranomaislähteisiin, joissa yhteiskunnan elintärkeitä toimintoja on määritelty. Näitä ovat esimerkiksi

YTS, VnP Huoltovarmuuden tavoitteista sekä valmiuslaki, jonka sääntely kohdistuu tiettyihin kriittisiin toimintoihin ja näiden turvaamiseen. Lisäksi määrittelyyn voi hakea tukea esim. ValmL tai HuovaL esitöistä.

Termit
Termien osalta dokumentissa on todettu, että strategiassa käytetyt termit poikkeavat osin tai kokonaan olemassa olevista sanastoista kuten TEPA-termipankki tai Kyberturvallisuuden sanasto, sillä kyberturvallisuuteen liittyvien kansallisten käsitteiden osalta on tunnistettu päivitystarve, joka johtuu mm. pyrkimyksestä kansainvälisesti yhdenmukaiseen käsitteistöön sekä lainsäädännön, erityisesti EU-regulaation, sisältämien käsitteiden tuomisesta sanastoon. On hyvä täsmentää, miltä osin kyberturvallisuusstrategiassa nykyisellään käytetyt käsitteet vastaavat kansainvälisesti yhdenmukaisia käsitteistöä.

Ehdotamme, että olemassa olevia jo käytössä olevia sanastoja
päivitetään vastaamaan kyberturvallisuusstrategiassa käytetyillä ajantasaisilla termeillä.
Ministeriö ehdottaa termistöä täydennettävän seuraavilla käsitteillä ja niiden määritteillä: murrokselliset teknologiat, uudet matkaviestiverkkosukupolvet, kyberturvallisuuden tietopääoma, kriittinen tietopääoma, kvantinkestävä salaus, kokonaisturvallisuuden malli (aikaisemmin kokonaisturvallisuuden yhteistoimintamalli), varautumisen toimintamalli, kansallinen ja kansainvälinen yhteistoimintamalli, kyberturvallisuuden yhteistoimintamalli (aikaisemmin kyberturvallisuuden kansallinen yhteistoimintamalli), kyberpuolustusdoktriini, kyberturvallisuuden

suorituskykyindikaattori, kyberkestävyyden indikaattori, yleinen kyberturvallisuustietoisuus, kyberdiplomatia ja kyberriski.

Karvonen Tanja
Työ- ja elinkeinoministeriö