

Asia: VN/36693/2023

Lausuntopyyntö Suomen kyberturvallisuusstrategiasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Kiitämme lausuntomahdollisuudesta ja toteamme luonnoksesta seuraavaa:

Lausuttava kyberturvallisuusstrategian luonnos on järjestyksessään Suomen kolmas kansallinen kyberturvallisuusstrategia. Nykyinen voimassa oleva strategia on vuodelta 2019 ja sitä edellinen oli vuodelta 2013. Nähdäksemme strategialuonnoksessa on hyvin huomioitu edellisen strategian julkistamisen jälkeen Suomen ja kansainvälisessä kyberturvallisuusympäristössä tapahtuneet moninaiset muutokset, sekä niiden myötä muuttuneet kyberturvallisuustarpeet ja -painotukset. Näin myös strategialuonnoksen tavoitteet ja kehittämissuositukset sinällään ovat mielestämme laajasti kannatettavia. Joitakin kehittämissuositteita niissä kuitenkin on.

Kiinnitämme huomioita kolmeen asiakokonaisuuteen: nykyisen ja esitetyn strategian tavoitteiden vastaavuuteen, tavoitteiden asettamisen ja toimeenpanon keskinäisiin haasteisiin sekä tavoitteiden priorisoinnin tarpeeseen.

Nykyisen ja esitetyn strategian tavoitteiden vastaavuus

Vuoden 2019 strategian keskeiset strategiset linjaukset liittyivät:

1. kansainvälisen yhteistyön kehittämiseen,
2. kyberturvallisuuden kansallisen johtamisen, suunnittelun ja varautumisen parempaan koordinaatioon, jossa kokonaisuudessa korostettiin mm. yhteistyön verkostorakenteiden / ekosysteemin kehittämistä, varautumisyhteistyön ja tiedonvaihdon sekä tilannekuvayhteistyön kehittämistä, häiriötilanteiden johtamisen ja tähän liittyvän yhteistyön kehittämistä, kaikkien

osapuolten osaamisen vahvistamista, turvallisuuskriittisten palveluiden vaatimustenhallinnan kehittämistä, viranomaisyhteistyön kehittämistä, sekä

3. kyberturvallisuuden osaamisen kehittämistä kaikilla tasoilla ja kaikilla yhteiskunnan sektoreilla ja tähän liittyvän koulutuksen, tutkimuksen vahvistamista ja standardointiin panostamista.

Lausuttavan strategialuonnoksen tavoiteosa-alueet eli pilarit ovat:

1. Osaaminen, teknologia ja TKI,
2. Varautuminen,
3. Yhteistoiminta, sekä
4. Reagointi ja vastatoimet.

Vaikka tavoiteosa-alueiden alatavoitteissa on uusiakin elementtejä, niissä on myös hyvin paljon samoja tavoitteita kuin nykyisessä strategiassa, erityisesti kolmessa ensin mainitussa lausuttavan luonnoksen tavoiteosa-alueessa.

Siltä osin kuin tavoitteet ovat samoja tai lähes samoja kuin nykyisessä strategiassa, tulisi nykytilaosuudessa avata nyt tehtyä tarkemmin, miksi kuluvalle strategiakaudella tavoitteisiin ei ole päästy, tai miten tavoitetta ylipäätään on onnistuttu edistämään ja/tai miksi seuraava tasokorotus on edelleen tarpeen. Tämä loisi esitetyille tavoitteistolle uskottavamman perustan ja samalla osoittaisi ongelmakohtat, joihin toimeenpanossa tulee tällä kertaa kiinnittää erityistä huomiota. Hyviä tavoitteita tärkeämpää lopulta on kuitenkin se, että ne, tai vähintäänkin niistä kaikkein keskeisimmät kyetään myös toteuttamaan.

Viittaamme jäsenyhdistyksemme Teknologiateollisuus ry:n ja sen toimialayhdistys Kyberala ry:n yhteiseen lausuntoon ja toteamme, että kyberturvallisuusstrategian sinällään hyvät kehittämissuositukset ovat vahvasti viranomaiskeskeisiä. Mielestämme siinä tulisi tunnistaa paremmin se, millaista tukea elinkeinoelämä tarvitsee. Monilta osin nousussa olevat kyberturvallisuusriskit ottavat toteutuessaan vastaan yritykset ja painopisteenä tulisikin olla, miten julkinen sektori voi niitä kaikin mahdollisin tavoin tukea kyberturvallisuuden riskienhallinnan toimenpiteiden toimeenpanossa. Tällöin strategia tukisi mahdollisimman hyvin myös NIS2-direktiivin toimeenpanoa Suomessa. Asiaa ja siihen liittyviä yksityiskohtaisempia muutosehdotuksia (mm. toimijat, termit) on avattu laajemmin viittaamassamme Teknologiateollisuuden ja Kyberalan yhteislausunnossa.

Tavoitteiden asettamisen ja toimeenpanon keskinäiset haasteet

Strategiaa valmistellut työryhmä on edellisen strategian tavoin rakentanut kokonaisuuden siten, että ensin laaditaan ja hyväksytään strategia ja sen jälkeen sen toteuttamista ohjaava

toimeenpanosuunnitelma / kehittämisohjelma. Valinta on sinällään ymmärrettävä, mutta tuo samalla mukanaan merkittävän haasteen: nyt tavoitteisiin tulisi sitoutua etupainotteisesti tietämättä, mitä niihin pääseminen tulee edellyttämään ja mm. maksamaan. Lisäksi monet tavoitteet ovat strategialuonnoksessa vielä hyvin yleisesti kuvattuja, joten myös tavoitteita on nähdäksemme välttämätöntä vielä konkretisoida.

Vaikka kyseessä olisikin kaksi eri dokumenttia, olisi jatkovalmistelussa edellä kerrotuista syistä tarpeen harkita niiden samanaikaista käsittely- ja hyväksyntäprosessia. Näin vältettäisiin esimerkiksi sellainen riski, että sinällään hyvien tavoitteiden edistämiseen ei löydetäkään rahaa tai muuta resurssia ja kehittämisohjelmassa joudutaan lieventämään tavoitteita vain muutamaa kuukautta strategian hyväksymisen jälkeen. Huomioiden mm. julkisen talouden tilanne ja strategialuonnoksessakin huomioitu kyberturvallisuusammattilaisten puute, tämä riski on valitettavasti aivan ilmeinen.

Strategialuonnoksen sivulla 43 todetaan ”Kyberturvallisuusstrategian uudistamista varten asetetun työryhmän työtä jatketaan strategian valmistuttua, ja ryhmä muutetaan strategian toimeenpanon seurantaryhmäksi. Seurantaryhmä laatii strategian toimeenpanosuunnitelman kuuden kuukauden sisällä strategian valmistumisesta. Toimeenpanosuunnitelmassa määritetään toimeenpanovastuut ja aikataulu hallinnonaloittain ja kuvataan tarkemmin mittarit, joilla strategian toimeenpanoa vuosittain seurataan ja arvioidaan.”

Kohdassa ei mainita, tullaanko myös toimeenpanosuunnitelma lähettämään avoimelle lausuntokierrokselle ja millaisessa prosessissa suunnitelma käsitellään ja hyväksytään. Monesti mahdolliset erimielisyydet eivät liity niinkään tavoitteisiin kuin niiden toimeenpanon tapoihin. Sen vuoksi on mielestämme erittäin tärkeää, että myös toimeenpanosuunnitelma käsitellään joka tapauksessa avoimessa prosessissa ja laajasti osallistaen, jotta mm. monien toimenpiteiden kohteena ja osapuolena olevan elinkeinoelämän edustajatkin voivat ilmaista siitä näkemyksensä.

Strategialuonnoksessa on aivan oikein todettu, että viime vuosina merkittävästi kehittyneen kyberturvallisuuteen vaikuttavan EU-säätelyn kansallinen täytäntöönpano ja organisaatioiden toiminnan mukauttaminen sen mukaisesti haastavat tulevana vuosina niin viranomaisia kuin elinkeinoelämääkin. Myös elinkeinoelämän roolia kyberturvallisuuden toteuttamisessa korostetaan strategialuonnoksessa. Tätä taustaa vasten on kuitenkin outoa, että kyberturvallisuusstrategian strategisissa kehittämisehdotuksissa ehdotetaan säädöspohjaa, normeja ja ohjeita muutettavaksi strategian kehittämistoimien edellyttämällä tavalla (s. 44), käytännössä siis uutta kansallista lisäsääntelyä. Joiltain osin, esim. yksityisten toimijoiden tiedonsaantioikeuksien kannalta kansallisen säätelyn tulkintojen yhdenmukaistaminen ja tarkentaminen voi olla perusteltuakin, mutta sen ei tulisi laajemmin johtaa kansalliseen lisäsääntelyyn, ei varsinkaan yksityisiä toimijoita koskevaan lisäsääntelyyn. Tulevana vuosina on erittäin tärkeää, että kriittisille yrityksille ja organisaatioille annetaan riittävästi aikaa toimeenpanna NIS2- ja CER-vaatimukset omassa toiminnassaan.

Viittaamme tavoitteita ja kehittämisohjelmia koskevien yksityiskohtaisempien havaintojen osalta myös jäsenyhdistyksemme Teknologiateollisuus ry:n ja sen toimialayhdistys Kyberala ry:n yhteiseen

lausuntoon, jossa tavoitteiden ja päämäärien epätasällisyyteen liittyviä riskejä ja tavoitteiden sekä kehittämisehdotuksien puutteita on tarkemmin tarkasteltu.

Strategialuonnoksen pilareihin liittyvistä Teknologiateollisuuden ja Kyberalan huomioista painotamme erityisesti 1) TKI-yhteistyöstä ja -rahoituksesta, 2) osaamisen kehittämisestä sekä 3) yhteistoimintamallin kehittämisestä lausuttua: olisi erittäin tärkeää pohtia TKI-toiminnan tueksi myös kansallisia rahoitusratkaisuja ja osaamisen kehittämistä tulisi tarkastella yksityiskohtaisemmin ja eri tasojen tarpeet eritellen. Yhteistoiminnan kehittämisen osalta on tärkeää muistaa myös elinkeinoelämän tarpeet ja intressit ja se, millaisella rakenteella strategialuonnoksessa mainittua tiiviimpää ja luottamusta vahvistavaa yhteistoimintamallia tulisi rakentamaan.

Lisäksi, kuten Teknologiateollisuuden ja Kyberalan yhteisessä lausunnossa on hyvin todettu, kansallisen kyberpuolustuksen ja kyberturvallisuuden yhtäläisyydet ovat suuremmat kuin luonnoksesta ehkä ymmärtää, ja myös tässä osuudessa tulisi laajemmin miettiä, mikä on elinkeinoelämän rooli ja miten itse asiassa kyberturvallisuuden kehittäminen samalla palvelee kyberpuolustuksen kehittämistä. Näitä osa-alueita ei tulisi nähdä aivan niin erillisinä kuin luonnoksessa nyt näytetään tehdyn.

Osaamiskysymyksiin, resurssointiin ml. rahoitukseen sekä yhteistoimintamalliin ovat ottaneet lausunnoissaan kantaa myös jäsenyhdistyksemme Kaupan Liitto ry ja sen toimialayhdistys Päivittäistavarakauppa ry. Olemme niistä samaa mieltä. Myös FiCom ry:n lausunnossa on kiinnitetty huomiota useisiin tärkeisiin kehittämistarpeisiin strategialuonnoksessa.

Tavoitteiden priorisoinnin tarve

Strategialuonnoksessa esitettyjä tavoitteita erityisesti kunkin tavoiteosa-alueen sisällä tulisi mielestämme jatkovalmistelussa luokitella niiden prioriteetin ja toisaalta sen mukaan, miten ne luovat pohjaa muille tavoitteille. Kaikki tavoitteet eivät voi olla samanarvoisia keskenään ja toisaalta mukana on tavoitteita, jotka luovat perustaa muiden tavoitteiden toteutumiselle ja joiden luonne tukitavoitteena tulisi näin kyetä ajallisesti ja resurssimielessä huomioimaan suhteessa tuettavaan tavoitteeseen. Se, että tavoitteet olisi priorisoitu olisi tärkeää myös sen varalta, että resurssit eivät tule riittämään kaikkien tavoitteiden täysimääräiseen edistämiseen. Rajalliset resurssit tulisi tällöin kohdentaa niihin tavoitteisiin, joiden panos-tuotos-suhde on kokonaisuutena paras.

Kunnioitavasti

Elinkeinoelämän keskusliitto EK

Lainsäädäntö ja hallinto

Tommi Toivola

Johtaja

Rajamäki Markku

Elinkeinoelämän keskusliitto EK - Lainsäädäntö ja hallinto