VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Muistio

9.8.2024

VN/36693/2023
VN/36693/2023-VM-57

VM; Lausunnon valmistelu; lausunto Valtioneuvoston periaatepäätöksestä Suomen kyberturvallisuusstrategiaksi 2024-2035

Liikenne- ja viestintäministeriö on pyytänyt valtiovarainministeriöltä lausuntoa otsikkoasiassa. Valtiovarainministeriö (VM) antaa asiassa seuraavan lausunnon.

VM pitää strategialuonnosta kannatettavana. Sen ratkaisut ovat perusteltuja ja VM puoltaa luonnoksessa esitettyjä strategisia kehittämisehdotuksia. VM kuitenkin esittää muutamia yksittäisiä huomioita strategialuonnoksesta.

Huomioita resursseista

Periaatepäätösluonnoksessa todetaan, että *tavoitetilan saavuttamiseksi varmistetaan riittävät resurssit ja käytetään niitä tehokkaasti*. Sivulla 41 todetaan, että ”*Kaikkien strategisten tavoitteiden ja kehittämistoimien toteuttamiseen on suunnattava lisää resursseja*.”

Valtiovarainministeriö kiinnittää huomiota siihen, että periaatepäätösluonnoksessa tarkoitetuista resursseista ja niiden kohdentamisesta ja yhteensovittamisesta päätetään valtion talousarvioita koskevin päätöksentekoprosessein ja ne määräytyvät julkisen talouden suunnitelmien ja valtion talousarvioiden mukaisten määrärahojen ja henkilötyövuosimäärien puitteissa, mikä on perusteltua todeta periaatepäätöksessä.

Ministeriö toteaa, että nykyisessä julkisen talouden tilanteessa on resursoinnin suunnittelussa ja toteuttamisessa kiinnitettävä erityistä huomiota mahdollisuuksiin tehostaa käytettävissä olevien resurssien kokonaisvaltaista, keskeisiin tehtäviin priorisoitua suunnittelua ja kohdentamista. Tämä edellyttää selkeän kokonaiskuvan muodostamista

Postiosoite Postadress Postal Address	Käyntiosoite Besöksadress Office	Puhelin Telefon Telephone	Faksi Fax Fax	s-posti, internet e-post, internet e-mail, internet
Valtiovarainministeriö PL 28 00023 Valtioneuvosto	 Snellmaninkatu 1 A Helsinki	 0295 16001 +358 295 16001		 kirjaamo.vm@gov.fi

kansallisista kyberturvallisuuteen liittyvistä tehtävistä ja tarpeista, joilla varmistetaan perustellun tasoinen kyberturvallisuus realististen voimavarojen puitteissa.

Tarpeellisin osin tulee myös edelleen tarkentaa julkisen sektorin sisäistä koordinointia ja vastuita eri organisaatioiden välillä päällekkäisten ja perusteettomien tehtävien, toimintojen ja resursoinnin välttämiseksi. Myös julkisen sektorin ja yksityisen sektorin välistä työnjakoa sekä valtion tarjoamista, kyberturvallisuuteen liittyvistä palveluista perittävien maksujen kokonaisuutta tulee tarpeellisin osin tarkastella kyberturvallisuuteen liittyvien tehtävien, hankkeiden, suoritteiden yms. järkevien synergioiden ja perustellun kustannusvastaavuuden toteuttamiseksi.

Yleisiä ja yksittäisiä huomioita strategian rakenteesta

Strategialuonnoksessa on kuvattu jatkuvuuden hallintaa ja sen merkitystä yleisellä tasolla. Esityksestä kuitenkin jää puuttumaan kuvaus siitä, että jatkuvuuden hallinta toimiakseen edellyttää olemassa olevia ja jo käytännössä harjoiteltuja toimintatapoja ja teknistä suorituskykyä. Strategiat ovat yleisellä tasolla. Niiden täytäntöönpanokelpoisuudesta olisi syytä huolehtia. Kyberturvallisuusstrategialuonnos on kattava. Laveita kuvauksia olisi voinut merkittävästi tiivistää ja kuvata myös visuaaliseen muotoon. Toisaalta kuvaukset antavat kyllä kuvan haasteiden laajuudesta koko toimintakentällä. Strategialuonnoksen alkukuvauksessa oleva tilannekatsaus on laaja (20 sivua). Strategia ja nykytilan yleiskuvaus voisivat olla erillisiä; kyberstrategiasta oma tiivis kuvauksensa ja tilannekuvasta oma raporttinsa.

Strategian tavoitteen kuvaaminen ja sen laajuuden huomioonottaminen, jäntevöittäisi strategiaa ja siihen liittyvää jatkosuunnittelutyötä. Strategian tulisi olla tiivis strateginen kuvaus tavoitteista ja suunnasta. Asiakirjassa voisi kuvata muun muassa konkreettisesti yhtenäisellä tavalla kyberuhkien erilaiset ilmenemismuodot ja tasot. Näin lukija saisi yhtenäisen kuvan kokonaisuudesta. Aikaisemmassa kyberstrategiassa on näistä hyviä esimerkkejä. Uhkana voidaan nähdä muun muassa kybervakoilu ja sen ulottuminen yhteiskunnan joka tasolle, tiedustelua unohtamatta. Tässä yhteydessä voisi ottaa esille mahdollisia uusia avauksia, kuten kybervaikuttamiseen pyrkivät mahdolliset kiristykseen liittyvät eri ilmenemismuodot. Lisäksi uhkien selvittämiseen liittyvien eri tahojen roolit olisi hyvä kuvata selkeästi. Tältä osin on vielä selkeyttämisen tarvetta.

Strategiassa on kuvattu toimeenpanoa, mutta kuvaus jää osin aika karkealle tasolle. Tältä osin olisi tarpeen kuvata jatkuvuudenhallinnan merkitys kyberriskeistä toipumiseksi. Toimintojen jatkuvuuden näkökulmasta tulisi tehdä arviointia siitä onko toimenpide riittävä ja pitäisikö sitä muuttaa tai tarkentaa toimintaympäristön muutoksien mukaisesti. Strategiassa voisi myös kuvata sekä virastojen, että muiden kybertoimijoiden sisäisiä riskejä. Kyberturvallisuus edellyttää myös julkisen hallinnon ja muiden ICT-toimijoiden omasta henkilöstöstä tulevien uhkien tunnistamista ja niihin varautumista.

Riskienarvioinnin voisi kuvata prosessinomaisesti etenevänä. Sisäiset riskit sisältyvät riskienarviointikokonaisuuteen. Riskienarviointikokonaisuudessa voisi tuoda esiin turvallisuusselvityslain (726/2014) antamat mahdollisuudet henkilö- ja yritysturvallisuusselvitysten teettämiseksi. Varautumiseen liittyvät kirjaukset ovat kannatettavia.

Yksittäisenä huomiona vielä, että sivulla 22 ja 23 on eri kohdissa sama väliotsikko ”Innovatiivinen ja kokeileva kyberekosysteemi” ja viimeisen kappaleen otsikko on kyberekoekosysteemi. Kun viitataan kokonaisturvallisuuteen, niin tässä voisi käyttää myös kokonaisturvallisuuden strategiaan sisältyvien asiakokonaisuuksien jäsentelyä.

Strategian tilannekuva ja liite, jossa kuvataan yhteistoimintamalli ja eri toimijoiden roolit, ovat ansiokkaita. Myös strategialuonnoksen tavoitteet ovat kannatettavia, mutta luonnos on itsessään varsin visiomainen. Strategian tarkoitusta voisi vieläkin selventää. Myös jatkossa laadittavaan toimeenpanosuunnitelmaan tarvitaan enemmän konkretiaa.

Johdanto-luvussa kyberturvallisuus määritellään osaksi yhteiskunnan kokonaisturvallisuutta. Lähtökohta on kannatettava mutta tekstissä se jää konkretisoimatta. Tekstissä tulisi edelleen selventää sitä, kuinka tällä strategialla kyberturvallisuus liitetään osaksi olemassa olevaa kansallista kokonaisturvallisuuden mallia. Myös esiin nostettu liityntä NIS2-kyberturvallisuusdirektiivin kansalliseen toimeenpanoon jää epäselväksi; ”Kyberturvallisuusstrategian uudistamisessa on otettu huomioon kyberturvallisuusdirektiivin (NIS2) vaatimukset kansalliselle kyberturvallisuusstrategialle sekä muu aiheeseen liittyvä keskeinen strategia- ja selontekotyö.” Sekä liityntää kokonaisturvallisuuden malliin, että kyberturvallisuusdirektiiviin voisi selkeyttää jäsentämällä ja konkretisoimalla nykytilaa kuvaavaa lukua molempien edellä mainittujen lähtökohtien osalta sekä osoittamalla ”Pilarit ja niiden strategiset tavoitteet” -luvussa kuinka tavoitteet parantavat edellä mainittujen lähtökohtien toimintaa ja toimeenpanoa.

Nykytilaa kuvaava luku jää yleiselle tasolle. Johdannossa kerrotaan, että ”strategian valmistelussa on otettu huomioon muu aiheeseen liittyvä kansallinen strategia- ja selontekotyö, joista keskeisimpiä ovat seuraavat valtioneuvoston periaatepäätökset: Suomen kyberturvallisuuden kehittämisohjelma, Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla (TITUKRI) ja Julkisen hallinnon digitaalinen turvallisuus sekä Valtioneuvoston selonteko Suomen digitaalisesta kompassista ja sen toimeenpanosuunnitelma. Lisäksi valmistelussa on huomioitu vuonna 2023 tehty selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa ja tästä työstä saadut huomiot ja kehittämiskohteet.” Nykytila-luvusta ei kuitenkaan selviä, mitkä siinä esitetyistä arvoista ovat edellä mainittuihin lähteisiin perustuvia ja mitkä kirjoittajaryhmän omaa analyysiä. Lukija jää muutoinkin kaipaamaan viitteitä eräisiin tekstissä esitettyihin väittämiin;

- johdantoluvussa mainittu ”Suomi käyttää tällä hetkellä vuosittain lähes 300 miljoonaa euroa valtionhallinnon kyberturvallisuuden varmistamiseen. Julkisten investointien lisäksi myös elinkeinoelämä investoi kyberturvallisuuteen varovaisen arvion mukaan noin kymmenkertaisesti verrattuna julkisiin investointeihin.” Mihin tämä luku perustuu ja mitä se sisältää? Mikä on kehittämisen osuus ja kuinka paljon käytetään rahaa ylläpitoon? Jos lukua ei pystytä perustelemaan, se tulee jättää pois.
- toimintaympäristön muutoksesta ja etenkin uhista nyt ja tulevaisuudessa. Onko nämä tiedot uhista arvailua vai perustuvatko tutkittuun tietoon?
- nykytilaluvussa esitetty näkemys ”Kyberturvallisuus on Suomessa kansainvälisten arviointien ja kansallisen itsearvioinnin perusteella verrattain hyvällä tasolla”. Tämä vaatii viitteet mainittuihin tai pääkohtien avaamisen tekstissä.

Erityisesti tulisi tuoda esiin havaitut kehittämistarpeet, jotka kansainvälisten arviointien osalta lienevät julkisia.

Nykytila-luvussa tulisi avata sitä, mikä on kyberturvallisuuden tila suhteessa tämän strategian tavoitteisiin ja kuvassa 1 esitettyyn tavoitetilaan ja sen osa-alueisiin. Tekstistä olisi hyvä selvitä myös se, mitä on saatu aikaan aiemmilla strategioilla (Suomen uudistettu kyberturvallisuusstrategia on järjestyksessään kolmas) ja kehittämisohjelmilla ja mitkä vallitsevassa turvallisuustilanteessa ovat ensisijaisia kehittämiskohteita. Tämä tarve korostuu erityisesti, koska selvitysten ja arviointien perusteella ”kyberturvallisuus on jo hyvällä tasolla”. Näiden asioiden esittäminen on välttämätöntä tässä taloudellisessa tilanteessa, jotta strategiaan perustuen laadittavassa toimeenpanosuunnitelmassa kehittäminen ja resurssit pystytään kohdentamaan vaikuttavasti ja resurssien päätöksenteolle on olemassa riittävät perusteet.

Nykytilan kuvauksen asiasisällöissä on esitetty asioita, jotka tulisi siirtää ”Toimintaympäristön muutos” -lukuun. Kokonaisuudessaan nykytilaa kuvaava luku osoittaa sen, että meiltä puuttuu kansallinen kyky asetta kyberturvallisuudelle konkreettisia tavoitteita, seurata kehittymistä ja olemassa olevaa kyvykkyyttä sekä raportoida suorituskykyjen ja resilienssin kehittymisestä. Tämä puute tulee huomioiduksi vain osittain luvussa ”Strategiset kehittämisehdotukset”.

Kuvassa 1 on esitetty kyberturvallisuuden tavoitetila ja rakenne. Päämäärä-laatikossa esitetyt asiat ovat kannatettavia. Kuvaa katsoessa jää kuitenkin kaipaamaan sellaista tiivistystä kyberturvallisuuden tavoitetilasta, joka jäisi lukijan mieleen. Esimerkiksi ”kolme pointtia”; kyky suojata kriittinen infra ja palvelut, vakioidut yhteistyörakenteet ja osaamisen kehittäminen (tämä vain esimerkkinä).

Pilarit ja niiden strategiset tavoitteet -luvussa esitetyt osa-alueiden tavoitteet tulisi priorisoida ja kytkeä strategian johdannossa esitettyyn tarkoitukseen. Resurssien kohdentamisen osalta olisi myös hyvä pohtia, voisiko tavoitteita esittää aikaan sitoen. Mitkä tavoitteista olisivat saavutettavissa jo tämän hallitusohjelman aikana ja mitkä ovat pitkäaikaista pysyvää toiminnan muutosta. Esimerkiksi ensimmäisessä pilarin mukaan kyberturvallisuusosaamisen ja kybervalmiuksien tulisi olla kansalaistaito. On hyvä, että kansalaisosaaminen on huomioitu tavoitteissa. Kun strategiakausi on vain 10 vuotta, tavoite on kunnianhimoinen. Miten lisätään kybervalmiuksia ja opetetaan kyberturvallisuusosaamista niille kansalaisille, jotka eivät enää ole koulutusjärjestelmän piirissä?

Luettavuutta ja asian hahmottamista haittaa myös se, että laatikoissa esitetyt ”Osa-alueen strategiset tavoitteet” ja pilarin tekstit eivät kohtaa. Teksti ei noudata laatikoissa esitettyjen tavoitteiden sisältöä eikä järjestystä. Pilari I:n tekstissä esiintyy väliotsikko ”Innovatiivinen ja kokeileva kyberekosysteemi” kahteen kertaan eri asiasisällöllä. Kokonaisuutena Pilarit-luku on jäsentymätön. Laatikoidut tavoitteet ja painopisteet jäävät epäselväksi. Tavoitteista muodostuu temppuluettelo, jolloin strategian selkeys ja toimeenpanosuunnitelman sisällöllinen ohjausvaikutus heikkenee.

Kehittämisehdotukset on laadittu niin yleiseen muotoon, että niillä ei tosiasiallisesti voida ohjata kehittämistä. Esimerkiksi ehdotuksen ”Muutetaan säädöspohjaa, normeja ja ohjeita strategian kehittämistoimien edellyttämällä tavalla” perusteet eivät käy

selvästi ilmi strategian tekstistä. Tarkennettavaksi jää millaisia säädösmuutoksia tarvittaisiin (mitä lakeja pitäisi muuttaa, kenen tiedonsaantia pitäisi lisätä).

Kehittämisehdotuksissa on myös useita koordinaatio- ja yhteistyötarpeita hallinnon, viranomaisten, yksityisten ja kolmannen sektorin välillä, mutta teksti on ristiriitaista sen suhteen mikä nykyisessä yhteistyössä ei riitä tai toimi. Luonnoksen mukaan nykytilassa olisi kehitettävää viranomaisten yhteisessä tilannekuvassa ja tilanneymmärryksessä sekä hallinnon ja elinkenoelämän välisessä tietojen jakamisessa. Toisaalta kuitenkin sanotaan että ”kansalliset toimialakohtaiset tiedonvaihtoverkostot ovat elinvoimaisia”. Liitteessä 1 on kuvattu nykyinen varsin kattava kyberturvallisuuden kansallinen yhteistoimintamalli, mutta ei kerrota, että siihen liittyisi mitään ongelmia. Yhteistyön lisääminen ja uudet yhteistyörakenteet nähdään kuitenkin ratkaisuna lähes kaikkiin tavoitteisiin. Strategiaan olisi hyvä tarkentaa, mitkä yhteistyötarpeet vaativat kokonaan uusia rakenteita ja mitkä toimisivat nykyisen kansallisen yhteistoimintamallin puitteissa.

Liitteen 1 tekstiin ja kuvaan tulisi myös kirjoittaa auki ja lisätä kuvaus siitä kuinka jatkuvasti lisääntyvä kansainvälinen yhteistyö on järjestetty kansallisesti. Kuinka Suomi esiintyy erilaisilla kyberturvallisuutta kehittävillä kansainvälisillä foorumeilla ja kuinka erilaisissa kyberturvallisuustilanteissa tilannetta hallitaan monikansallisesti.

Kyberturvallisuuden ekosysteemi otetaan esille kolmessa kohdassa, mutta mitään varsinaisia tavoitteita ei tälle kuvailulle kuitenkaan anneta. Olisi hyvä tarkentaa mihin kyberturvallisuuden ekosysteemillä tähdätään.

Sivulla 28 kyberrikollisuudesta todetaan ”Tämän vuoksi kansalaisille tarjottavat palvelut on suunniteltava, toteutettava ja ylläpidettävä siten, että kyberrikollisten hyökkäyspinta-ala pienenee.”. Tämä on hyvä ajatus, mutta vaikuttaa olevan nykykehityksen vastainen. Sitä mukaan, kun palveluita viedään lähemmäs kansalaisia ja sähköistetään, hyökkäyspinta-ala kasvaa.

Resursseista on todettu, että kaikki tavoitteet edellyttävät lisäresursseja ja ”tarvitaan merkittäviä taloudellisia investointeja” (sivu 41). Huomioiden nykyiset resurssien ja talouden sopeutuspaineet kehittämisehdotukset olisi hyvä priorisoida ja vaiheistaa. Samalla olisi syytä arvioida miten nykyinen kyberturvallisuuden taso voidaan säilyttää, mikäli resursseja joudutaan tulevaisuudessa ennemminkin karsimaan kuin lisäämään. Valintoja olisi hyvä tehdä jo strategiatasolla, mutta viimeistään toimenpanosuunnitelmassa. Lisäksi tärkeää olisi seurata resurssien käyttöä ja saavutettavia hyötyjä, jotta varmistetaan, että resurssit ovat tarkoituksenmukaisesti kohdennettu.

Pienempinä huomioina tekstissä käytetään joitain erikoistermejä, kuten termiä matkaviestinverkkosukupolvet sivulla 24. Sivulla 35 tekstistä jää epäselväksi onko kyse kansallisista vai kansainvälisestä keskitetyistä kyberturvallisuuspalveluista. Sivulla 37 johtamismalliin eivät näytä sisältyvän yksityiset toimijat, joiden kanssa tehtävää yhteistyötä kuitenkin muualla luonnoksessa korostetaan.

Toimeenpanoon tarvitaan konkreettiset keinot ja kehittämisehdotukset tulee priorisoida, jotta hyviin tavoitteisiin kyetään varmistamaan resurssit.

Kyberrikollisuus ja finanssialan valvonnan roolien tarkentaminen

Strategialuonnoksessa todetaan, että kyberrikollisuuden ennalta estäminen edellyttää koko yhteiskunnan kaikkein toimijoiden tavoitteellisia ja aktiivisia toimia. On tärkeää, että käyttäjät voivat luottaa palvelujen turvallisuuteen ja heillä on riittävä osaaminen tunnistaa väärennetyt palvelut ja huijaukset.

VM painottaa, että rahoitusmarkkinoilla tapahtuvat huijaukset ovat teknisesti entistä taidokkaampia eikä hyvien digitaitojen omaaminen välttämättä tarjoa suojaa huijauksilta. On valitettavasti todennäköistä, että huijaukset ovat jatkossa entistä taidokkaampia. Niiden tunnistaminen edellyttää palvelujen käyttäjien osaamisen jatkuvaa kehittämistä. Tämän vuoksi VM ehdottaa, että strategialuonnoksen sivulla 28 olevaa kirjausta ”Kyberrikollisuuteen liittyvistä uhkista on viestittävä ymmärrettävästi ja ohjeistettava ja neuvottava oikeista tavoista toimia” kehitettäisiin siten, että se huomioisi paremmin tarpeen käyttäjien osaamisen jatkuvalle kehittämiselle.

Vaikka strategiassa käsitellään kansallista kyberturvallisuutta, VM kiinnittää huomiota siihen, että on samalla tärkeää varmistaa kyberturvallisuutta koskevan EU-sääntelyn tehokas toimeenpano ja valvontaresurssien riittävyys. Yhtenä esimerkkinä tällaisesta EU-sääntelystä voidaan mainita finanssialan digitaalista häiriönsietokykyä koskeva EU-asetus, nk. DORA (2022/2554/EU). Strategialuonnoksen sivulla 32 todetaan, että ”EU:n yhteinen kyberpolitiikka ja kyberturvallisuuteen vaikuttava sääntely luovat kehikon myös Suomen kyberturvallisuuden lainsäädännölle. Uuden sääntelyn toimeenpanoon, sen vaikutusten arviointiin ja viranomaisten riittävään resursointiin on kiinnitettävä huomiota”. VM esittää, että kirjausta muokattaisiin siten, että uuden sääntelyn tehokas toimeenpano ja viranomaisten riittävä resursointi varmistetaan.

VM kiinnittää huomiota siihen, että kyberturvallisuusstrategian sivulla 50 mainitaan valvovana viranomaisena myös Suomen Pankki. VM toteaa, että **Suomen Pankin valvonnan rooli on ns. yleisvalvonnallinen** eli se valvoo maksu- ja selvitysjärjestelmiä seuraamalla, analysoimalla ja arvioimalla säännöllisesti näiden järjestelmäkokonaisuuksien tilaa ja kehitystä. Suomen Pankki ei valmistele osana yleisvalvontaa hallintopäätöksiä, eikä sillä ole perinteisiä viranomaisen toimivaltuuksia yleisvalvontaa suorittaessaan. **Finanssivalvonta toimii rahoitusmarkkinoiden valvovana viranomaisena**. Sivulla 50 olevaa kirjausta olisi syytä tarkentaa tältä osin väärinkäsitysten välttämiseksi.

Hyvinvointialueet ja kunnat tarkemmin strategiaan

Julkisen hallinnon osana kunnat ja hyvinvointialueet ovat aivan keskeisiä kaikista näkökulmista, mutta niiden näkökulma puuttuu strategialuonnoksesta lähes kokonaan. Esimerkiksi näiden tietovarannot ja -järjestelmät sisältävät valtavat määrät kaikkia kansalaisia koskettavaa arkaluonteista ja muuta suojeltavaa tietoa.

Hyvinvointialueet ovat rakenteena uusi ja niiden integraatiota kyberturvallisuuden julkisen hallinnon kokonaisuuteen tulisi erityisesti vauhdittaa ja varata tähän työhön erikseen taloudellisia resurssejakin. Luonnoksessa on kyllä mainittu, että valtio kohdistaa 300 milj. euroa vuosittaista rahoitusta kyberturvallisuuteen. Suhteessa koko julkisen hallinnon kokonaisuuteen summa vaikuttaa melko pieneltä. Valtiovarainministeriön näkemyksen mukaan esityksessä olisi syytä täsmentää miten mainittua rahoitusta olisi tarkoitus kohdentaa. Kattaako se julkisen hallinnon, kaikki asianosaiset toimijat sisältäen

myös yksityisen ja kolmannen sektorin, vai esimerkiksi vain valtion omat virastot ja tietotekniikka-asiat jne.?

Luonnoksessa korostuu jonkin verran valtionhallinnon keskusorganisaatioiden ja ”ulkoisten toimijoiden”, kuten NATO ja EU, yhteys kyberturvallisuusasioissa, mutta samaan aikaan huomio jää vähemmälle, kun edetään pienempiin toimijoihin Suomen julkisessa hallinnossa. Valtiovarainministeriö suositteleekin lausunnon pyytäjää vielä tarkastelemaan tätä näkökulmaa, sillä kyberuhkien realisoituminen on erittäin todennäköistä juuri sellaisten pienenpien toimijoiden kautta, joilla haavoittuvuus näissä asioissa on tyypillisesti suurempaa kuin isommilla toimijoilla, joilla lähtökohtaisesti on enemmän resursseja ja osaamista varautua erilaisiin kybertapahtumiin.

Valtiovarainministeriön käsityksen mukaan kyberturvan strateginen ohjaus näyttäytyy hyvinvointialueille vielä sekavalta ja sen osalta strategiaan ja sen toimeenpanoon olisi hyvä nostaa asiaa edistäviä toimenpiteitä. Hyvinvointialueiden kyberturvallisuustoiminta periytyy kuntapuolelta ja sairaanhoitopiirien toiminnasta, jolloin sairaanhoitopiireillä oli iso rooli sosiaali- ja terveydenhuollon kyberturva-asioissa. Nykytilanteessa alueiden olisi järjestämisvastuunsa myötä edelleen aktivoiduttava näissä asioissa ja edistää kyberturvallisuutta omilla alueillaan, mutta kuitenkin hyvässä yhteistyössä koko julkisen hallinnon kyberturvaekosysteemin kanssa.

VM ehdottaa strategiaan uutta konkreettista kehittämiskohdetta (s.44): Kansallisen kyberturvallisuuden johtamisen hallintomallin kehittäminen edelleen niin, että myös hyvinvointialueet otetaan siinä selkeästi huomioon”

Strategialuonnoksessa olisi valtiovarainministeriön käsityksen mukaan hyvä olla jonkin verran enemmän konkreettisia esimerkkejä uhista ja haavoittuvuuksista. Esimerkiksi erilaiset rajapinnat ja integraatiot kriittisten järjestelmien ja tietovarantojen välillä jäävät vähälle huomiolle. Esimerkiksi DVV:n (esim. VTJ) ja alueiden APT-järjestelmien liittymät muodostavat tällaisen kriittisen osakokonaisuuden. Näihin kuitenkin sisältyy paljon isoja riskejä, jotka toteutuessaan voivat halvaannuttaa ja vaarantaa yhteiskunnan toimintaa laajasti.

Kyberturvallisuuden rahoituksen pitkäjänteisyyttä olisi valtiovarainministeriön ajatuksen mukaan käsiteltävä strategialuonnoksessa vielä tarkemmin. Tätä pitäisi korostaa ulottuen myös hyvinvointialueiden ja kuntien rahoitusjärjestelmiin ja esimerkiksi huomioida JTS-kauden rahoitussuunnittelu.

Nykytilan kuvauksen osiossa (s. 16 alkaen) olisi valtiovarainministeriön näkemyksen mukaan hyvä kuvata julkisen hallinnon lähtökohtia. Kun asiaa suhteuttaa esim. s. 48 kuvan toimijakuvaukseen yhteiskunnan kyberturvallisuuden varmistamiseksi (siinä korostuvat julkisen hallinnon toimijat), niin tässä asiassa voidaan nähdä epätasapainoa.

Toimijuuksien osalta olisi valtiovarainministeriön suosituksen mukaan tarkasteltava tarkemmin Suomen sisäistä vs. ulkoista toimintaa tällä saralla. Luonnoksessa on jossain määrin sekaisin molempia. Suomen sisäisen tilanteen (valmiuden, varautumisen parantamisen, vastuunjakojen) kuvaukset ovat luonnoksessa vielä hiukan kevyitä ja niiden osalta olisi luontevaa lisätä täsmällisyyttä.

Valtiovarainministeriö rohkaisee lausunnonpyytäjiä vielä pohtimaan ovatko tilannekuvatietojen muodostamista koskevat strategiset tavoitteet ja kirjaukset riittäviä. Tilannekuvan voi ymmärtää olevan tässä kokonaisuudessa tärkeän, ja se on eri tavoin mainittukin – mutta erilaisissa konteksteissa ja melko suuripiirteisesti. Erityisesti huomio kiinnittyy siihen, että kansallisessa ja erityisesti julkisen sektorin tilannekuvassa viitataan ainoastaan valtiotoimijoihin ja valtion virastoihin, mutta hyvinvointialueet ja kunnat puuttuvat kokonaan. Vastuutusten osalta (erityisesti muodostamisvastuut ja toimintatavat) pitäisi strategia-asiakirjassa olla jo kirjauksia. Mainittuna on toki johtamisjärjestelmä, joka luonnoksen mukaan on selkeä, mutta onko syytä arvioida, miten asia halutaan esittää. Johtamisjärjestelmän koettu selkeys varmaankin riippuu tarkastelijasta ja näkökulmasta, mutta varmaa on, että johtamisjärjestelmän kehittäminen ja selkeyttäminen on edelleenkin hyvää pitää mukana jatkuvan kehittämisen prosessissa.

Valtiovarainministeriö pitää ansiokkaana luonnoksen termipankkia, joka on liitteeksi laitettu. Se on maallikkolukijalle hyvä apu. Samoin erityisen tärkeä asia on kokonaisturvallisuuden näkökulma, joka alussa korostuu. Toisaalta kokonaisturvallisuuden näkökulmaa tarkasteltaessa valtiovarainministeriö suosittelee strategian valmistelijoita pohtimaan, onko kaikki osa-alueet ja osalliset kuitenkaan riittävällä tavoin huomioitu; elinkeinoelämä, valtiotoimijat kyllä, mutta hyvinvointialueet ja kunnat vähemmän kuten yllä todettua. Järjestöjen ja kansalaisten roolien huomioiminen ja sen tarve on tässä yhteydessä vielä jokseenkin epäselvä.

Kyberturvallisuuden kokonaisuuden kannalta lukemattomat raja- ja yhdyspinnat ovat olennaisia niin teknisesti kuin toiminnallisestikin. Tämän osalta käsittely strategialuonnoksessa jää jonkin verran pinnalliseksi ja valtiovarainministeriö suosittaakin valmisteluryhmää vielä tarkastelemaan tätä näkökulmaa.

Strategialuonnoksessa mainitaan useita kehittämiskokonaisuuksia (pilarit) ja kehitysehdotuksia, joiden toteuttaminen vaatii asianosaisilta uusia voimavaroja ja rahoituksenkin järjestämistä. Valtiovarainministeriö suosittelee lausunnonpyytäjää vielä pohtimaan olisiko tästä jollain lailla vielä erikseen mainittava, että varmistettaisiin myös satsaaminen näihin asioihin. Strategia jää hieman puolitiehen ja juhlapuheen tasolle, jos sen toteuttamiseen ei aidosti varata ja priorisoida resursseja.

Kyberturvallisuusstrategia on tärkeä osa Suomen ja julkishallinnon varautumista. Strategian tekstistä jää yleisellä tasolla helposti käsitys, että kunnat ja hyvinvointialueet olisivat jotenkin sivuroolissa kyberturvallisuudessa. Tämä ei todennäköisesti ole tarkoitus.

Vaikuttaa, että strategialuonnoksessa vältellään termien ”kunta” ja ”hyvinvointialue” käyttöä. Osa linjauksista jää sisällöltään epäselviksi, kun tekijöinä on alue- ja paikallishallinto, mutta kuntia tai hyvinvointialueita ei mainita lainkaan. Varsinkin aluehallinto viittaa vahvasti valtion aluehallintoon.

Kunnat mainitaan nykytilassa heterogeenisenä joukkona ja kokonaisuutena sektorina, jonka tilanne on heikompi kuin muiden yhteiskunnan toimijoiden. Tästä huolimatta kuntia ei erikseen mainita strategian 1 pilarissa, joka käsittelee osaamista.

Varautumispilarissa käsitellään julkisten palvelujen turvallisuutta ja yhdessä varautumista tavalla, joka edellyttäisi varautumisen johtamista. Kuntien ja hyvinvointialueiden osalta kyberiin varautumisen johtaminen ei ole yksiselitteisesti säädetty, mikä pitäisi

ottaa strategiassa huomioon. Nämä itsehallinnolliset toimijat tuottavat valtaosan yhteiskunnan välttämättömistä palveluista ja niillä on suuria suojattavia tietomassoja. Strategiassa pitäisi olla myös jokin hieman konkreettisempi näkymä näiden varautumisen johtamiseen, jotta strategia voisi aidosti edistää tavoitteitaan reaalimaailmassa.

Pilarin 3 tilannekuvaa käsittelevissä teksteissä kunnat ja hyvinvointialueet mainitaan oikeassa yhteydessä ja hengessä. Strategian tavoitteiden saavuttamiseksi ja konkretisoimiseksi tulee myös kyberturvallisuutta koskevan tilannekuvatyön olla mukana syksyllä 2024 alkavassa sisäministeriön vetämässä työryhmätyössä. Pilarin teksteissä, kuten muuallakin, käytetään usein ilmaisua ”viranomaiset”, joka sulkee kunnat ja hyvinvointialueet kokonaisuuksina ulkopuolelle. Näiden osat voivat olla viranomaisia, mutta erityisesti kyberturvallisuuden kannalta niiden tulisi sisältyä jokaiseen pilariin kokonaisuuksina. Tulisikin harkita, että tekstissä mainittaisiin myös kunnat ja hyvinvointialueet erikseen niissä yhteyksissä, joissa nyt puhutaan viranomaisista.

Pilarin 4 tavoitteet eivät ole saavutettavissa, ellei varautumisen johtaminen ja toiminta ulotu myös kuntiin ja hyvinvointialueisiin, koska nämä hoitavat suurta osaa tehtävistä ja tietovarannoista. Tämä tulisi todeta selkeästi strategiassa, jotta toimenpiteitä voitaisiin valmistella ja tehdä strategian avulla. On olemassa riski, että järjestelmä jää hyvin vajavaiseksi, jos kuntia ja hyvinvointialueita ei integroida kokonaan kyberturvallisuuteen samalla tavalla kuin valtion toimijoita.

Logistiikka ja viranomaisten toimintakyvyn varmistaminen

Logistiikan huomioimisen osalta johdannossa (s. 8) on tuotu esille se, että kyberturvallisuus ja siihen liittyvät toimet liittyvät osaltaan kansallisen turvallisuuden ja samalla huoltovarmuuden turvaamiseen. Toimintaympäristön muutoksen yhteydessä (s. 16) todetaan, että kybertoiminta kohdistuu yhä laajemmin myös yrityselämään ja, että elinkeinoelämällä on merkittävä rooli kansallisen kyberturvallisuuden varmistamisessa. Tullin toiminnalle keskeisen logistiikkasektorin osalta voidaan tässä yhteydessä todeta, että kansallinen ja kansainvälinen logistiikka nojaa pitkälti yksityissektorin prosessien varaan ja strategiassa onkin infrastruktuurin osalta tuotu esille se, että elinkeinoelämä omistaa merkittävän osan Suomen kriittisestä infrastruktuurista ja vastaa sen kyberturvallisuuden varmistamisesta (s. 41). Tämä korostaa yksityisen ja julkisen sektorin PPP-yhteistyön ja vuoropuhelun tärkeyttä, josta Tullilla on jo vuosien kokemusta MoU- ohjelmansa (*Memorandum of Understanding*) ja sopimustensa kautta mm. logistiikkasektorin toimijoiden kanssa. Tämä yksityisen sektorin kanssa tehtävä yhteistyö on strategiassa nostettu esiin toteamalla, että kyberturvallisuuden ekosysteemi käsittää laajasti yksityisen ja julkisen sektorin toimijat, yhteiskunnan eri tasojen osaamisen ja kyvykkyydet, toimijoiden välisen yhteistyön ja toimintatavat, vahvan kotimaisen kyberteollisuuden ja tutkimuslaitokset.

Strategiassa on myös nostettu esille palvelu- ja toimitusketjujen pidentyminen ja monimutkaistuminen (s.14), samoin kuin logistiikan ja infrastruktuurin keskinäisriippuvuus. Strategian luonnoksessa onkin hyvin todettu, että yhteiskunnan toimintakyvyn kannalta kriittisten toimijoiden täytyy varmistaa, että myös niiden palveluntuottajat ja toimitusketjut ovat kyberturvallisia. Vastapainona on syytä vahvistaa myös huoltovarmuuden ja

logistiikan kannalta keskeisten viranomaisten, riittävät valmiudet ja kyvykkyydet kyberuhkien torjunnassa.

Viranomaisten toimintakyvyn varmistamisen osalta VM toteaa, että valtiontalouden ongelmat ja viranomaisresurssien väheneminen yhdessä alati haastavammaksi muuttuvan toimintaympäristön kanssa ovat näinä viranomaisille suuria haasteita.

Valtiosihteeri kansliapäällikkönä Juha Majanen

Tietohallintoneuvos Aku Hilve

Liitteet

Jakelu

Tiedoksi

VN/36693/2023-VM-57

Seuraavat henkilöt ovat allekirjoittaneet tämän asiakirjan sähköisesti /

Följande personer har undertecknat denna handling elektroniskt /

This document has been signed electronically by the following persons:

Hilve Aku 91275434U	Majanen Juha 91237851F
2024-08-09	2024-08-12