Huoltovarmuuskeskus

Lausunto

09.08.2024 HVK/2024/00620-2

Asia: VN/36693/2023

Lausuntopyyntö Suomen kyberturvallisuusstrategiasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Huoltovarmuuskeskuksen lausunto Suomen kyberturvallisuusstrategiasta

Keskeiset huomiot strategiasta

Kyberturvallisuusstrategia on kattava esitys kansallisen kyberturvallisuuden tilasta ja antaa runsaasti hyviä suuntaviivoja tulevalle kehitykselle. Strategian rakenne vaikuttaa toimivalta ja loogiselta kokonaisuudelta, jota on hyvä lähteä konkretisoimaan luonnoksessa mainitun toimeenpanosuunnitelman avulla. Lausunnossaan Huoltovarmuuskeskus kiinnittää erityisesti huomioita, miten strategia vastaa elinkeinoelämän kriittisten toimijoiden kyberturvallisuuden kehittämiseen ja toteuttamiseen osana yhteiskunnan varautumista ja turvallisuutta.

Huoltovarmuuskeskuksesta on erittäin hyvä, että strategiassa yritykset on tunnistettu tärkeinä toimijoina kansallisessa kyberturvallisuudessa. Strategiassa myös todetaan aivan oikein, että yritykset vastaavat suurimmasta osasta kriittisestä infrasta ja joidenkin yritysten kyberturvan tilanne on heikko. Ratkaisuna ehdotetaan, että yritykset sisällyttävät kyberturvaresurssit toiminto- ja taloussuunnitelmiinsa. Suomen kyberturvallisuusstrategiaksi asiakirja kuitenkin painottaa voimakkaasti julkishallinnon näkökulmaa, jolloin elinkeinoelämän ja muun kansalaisyhteiskunnan rooli kokonaisuudessa jää ohueksi suhteessa todelliseen todettuun merkitykseen. Esimerkiksi NIS-direktiiviin merkitys osana kriittisten toimintojen kyberturvallisuuden vahvistamista olisi tärkeä selkeyttää. Sen yhteydessä on tärkeää osoittaa, mitä Suomi kansallisesti tekee yhteisen EU-direktiivin vaatimusten lisäksi korostaakseen erinomaista kansallista kyberturvallisuuden toteutusta ja näyttäytyen kansainvälisesti kilpailukykyisenä turvallisena maana.

Strategiassa korostuu selkeästi julkisten toimijoiden vastuun ja tehtävien kehittäminen ja resurssointi sekä kansalaisten valistaminen. Strategiassa todetaan, että tarve viranomaisten ja elinkeinoelämän väliselle yhteistyölle on erityisesti kasvanut. Kautta linjan olisi hyvä lisätä tekstiä, jossa kerrotaan, mikä on elinkeinoelämän rooli ja vastuut, miten elinkeinoelämälle jaetaan tilannekuvaa ja mitä muita julkisen ja yksityisen sektorin yhteistoimintamalleja on olemassa tai halutaan kehittää. Näin elinkeinoelämän olisi helpompi sitoutua strategiaan ja kokonaisuus palvelisi

paremmin koko yhteiskunnan etuja. Kokonaisuudessa strategian luonnoksessa ei kuvata kenen vastuulla on edistää mitäkin strategista tavoitetta. Muutoksen aikaansaamiseksi tämä on tärkeä täsmennyt, joka oletettavasti huomioidaan viimeistään toimeenpanosuunnitelmassa.

Strategian tavoitetila on varsin kannatettava, mutta siihen tarvittavat resurssien perustelu kaipaavat täsmennystä erityisesti valtiontalouden nykyisten säästötavoitteiden valossa. Resurssointia käsittelevässä osuudessa todetaankin, että yksityisen sektorin panostukset kyberturvallisuuteen ovat varovaistenkin arvioiden mukaan kymmenkertaiset suhteessa julkiseen rahaan. Strategian kuuluu olla ylätasoinen, mutta jo tässä vaiheessa on tärkeää varmistaa, että ymmärretään resurssien suuruusluokka, mitä tavoitteiden toteutuminen vaatii. Nyt yksi osa-alue tavoitetilasta on riittävät resurssit tavoitetilan saavuttamiseksi.

Jos strategian ytimeksi muodostuu siinä mainittuihin kehitysehdotuksiin keskittyvä toimenpideohjelma, voisi olla tarve arvioida onko kehitysehdotuksissa tarpeeksi kyvykkyyksien kasvattamiseen liittyviä ehdotuksia. Ehdotukset painottuvat melko vahvasti yhteistoimintaan ja toimintamalleihin. Strategiassa olisi hyvä kuvata konkreettisemmin, mitä tarkoitetaan, kun strategisissa kehittämisehdotuksissa todetaan ”Varaudutaan uusien murrosteknologioiden, erityisesti kvanttilaskennan, kehittymisen tuomiin uhkiin ja mahdollisuuksiin” tai ”edistetään teknologisen suvereniteetin ja kyberturvallisuuden ekosysteemin kehittämistä ja varmistetaan Suomen teknologinen edelläkävijyys ja uudet innovaatiot.”. Nämä vaativat tyypillisesti merkittävää osaamis-, henkilöstö- kuin myös resurssipanosta.

Strategiassa mainittu osallistuminen erilaisiin EU- ja Nato-rahastojen kehityshankkeisiin on hyvä asia. Jos tavoitteena on korkeatasoinen ja kilpailukykyinen kyberturvallisuusosaaminen Suomessa, resursseja tulisi ohjata yritysten kansainväliseen kilpailukykyyn ja toimintaedellytyksiin vastaten Suomen nykyistä profiilia varautumisen edelläkävijänä myös digitaalisessa toimintaympäristössä. Resurssien lisäksi tulee pyrkiä purkamaan esteitä yritysten kilpailukyvylle ja varmistaa, että yrityksille kulkee tasainen virta tilannetietoa, jonka avulla kyberturvallisuuden taso säilyy hyvänä ja Suomen viranomaistoiminta tarjoaa elinkeinoelämälle kyvyn ylläpitää ja innovatiivisesti kehittää erityisesti kriittisten toimintojen kyberturvallisuutta.

Huoltovarmuusorganisaation kuvausta (s. 52) tulee tarkentaa ja vastata huoltovarmuusorganisaation toiminnan määritteitä. Lausuntoversion teksti kuvaus toiminnasta sisältää asiavirheitä, kuten poolien määrä. Ajantasainen kuvaus löytyy esim. Huoltovarmuuskeskuksen internet-sivuilta.

Strategiassa esitellään virastotason yhteistyörakenne, jonka tarkoituksena on koordinoida operatiivisen yhteistyön toimeenpanoa, vastuita sekä vakaviin kyberuhkiin ja -häiriöihin varautumista ja niihin vastaamista. Yhteistyörakenteen muodostavat Liikenne- ja viestintävirasto Traficom, keskusrikospoliisi, Puolustusvoimat sekä suojelupoliisi. Huoltovarmuuskeskuksella on keskeinen rooli elinkeinoelämän kybervarautumisen tukemisessa, jonka takia HVK:n osallistuminen ryhmän toimintaan on perusteltua. Tällöin huoltovarmuustoiminnan kyvyt kyberturvallisuuden parantamiseksi ja nopeaan reagointiin ovat tehokkaasti ja aikasensitiivisesti kansallisessa käytössä. Tämä vastaa monella muulla hallinnonalla olevaa rakenteellista käytäntöä osana varautumista.

Huoltovarmuuskeskus haluaa huomioida, että informaatiovaikuttaminen on tietoisesti jätetty strategian ulkopuolelle. Nykyisessä maailman turvallisuustilanteessa informaatiovaikuttamisen huomiointi kyberstrategiaan kytköksissä olisi tärkeää. On oletettavaa, että informaatiovaikuttamisen määrä ei ole laskussa vaan pikemminkin voimakkaassa nousussa. On tärkeää harkita informaatiovaikuttamiselle oman erillisen strategian laatimista.

Oppilaitosten osuus ja rooli kyberosaamisen tuottamisessa ei käy asiakirjasta järjestelmällisesti ilmi. Vaihtelevasti mainitaan koulut, tutkimuslaitokset tai korkeakoulut. Oppilaitos terminä voisi kattaa yliopistot, ammattikorkeakoulut ja ammattikoulut. Näin muotoiltuna strategian tavoitteet aukeaisivat eri tahoille täsmällisemmin.

Strategiassa käytetään sanaa ’Suomi’ eri merkityksissä. Aina ei ole selvää mihin sanalla viitataan (valtionhallinto, julkishallinto, yhteiskunta). Riskinä on, että eri toimijat ymmärtävät tekstin ja siihen liittyvät vastuut eri tavoin. Strategiassa tulisi täsmentää, missä kohtaa sanalla ’Suomi’ tarkoitetaan toimijana valtiota, missä kohtaa organisaatioita.

Strategian toimintakaudeksi on määritelty 10 vuotta, joka on nykyisissä turvallisuustilanteen muutoksissa ja digitalisaation kehityksessä varsin pitkä aika. Strategiassa ei ole mainintaa miksi aikajännettä on pidennetty aikaisemmasta. Tavoitetila ei tue pitkää strategiakautta. Huoltovarmuuskeskus näkee tarpeelliseksi arvioida, voisiko kautta lyhentää, määrittää säännölliset strategian tarkastusvälit tai vastaavasti avata miksi kausi on määritelty niin pitkäksi.

Muutosehdotukset ja tarkentavat huomiot strategiaan

Johdannossa todetaan, että toimintaympäristöä määrittävät voimakkaasti digitalisaatio, uusien teknologioiden kehitys ja niihin liittyvä globaali kilpailu, keskinäisriippuvuudet ja väestön ikääntyminen. Strategian pitkän aikajänteen näkökulmasta tässä olisi hyvä tuoda myös ilmastonmuutoksen vaikutukset kyberturvallisuudelle, jotka näkyvät mm. toimitusketjuissa kuten esim. Taiwanin mikrosirutuotannossa, säätilojen ääri-ilmiöissä, jotka saattavat vaikuttaa globaaliin kriittiseen infraan (mm. merenalaiset kaapelit ja datakeskukset) tai vihreässä siirtymässä, jossa uudella teknologialla on keskeinen rooli, joka samalla laajentaa elintärkeiden toimintojen uhkavektoria. Lisäksi johdannossa todetaan, että ”Yhteiskunnan perusrakenteiden ja -palvelujen kuten tieto- ja viestintäverkkojen ja niihin kytkeytyvän infrastruktuurin on toimittava kaikissa olosuhteissa.”. Infrastruktuurin lisäksi tieto- ja viestintäverkkoja hyödyntävien prosessien on toimittava. Hyvänä esimerkkinä taloushallintoala, joka ei itsessään ole mikään infrastruktuuri, vaan prosessi. Tätä prosessiajattelua ei ehkä ole aiemmin tuotu tarpeeksi esille, mutta se olisi hyvä ottaa mukaan, sillä on oleellinen osa digitalisaation kytkeytymistä osaksi muiden alojen toimintaa.

Strategiassa todetaan sivulla 10, että Suomi käyttää tällä hetkellä vuosittain lähes 300 miljoonaa euroa valtionhallinnon kyberturvallisuuden varmistamiseen. Voisiko samalla tuoda esille, että rahoitus on 0,34 % valtion kokonaisbudjetista tai verrata summaa johonkin muuhun kokonaisuuteen? Näin lukijalle annetaan parempi kuva nykyisen rahoituksen määrästä ja miten se suhtautuu yleiseen digitalisaatiokehitykseen sekä sen turvaamiseen. Vastaavasti valtion varsin hajanainen erilaisten järjestelmien kokonaisuus lisää kyberturvallisuuden varmistamisen kuluja. Kulunäkökulmasta siis olisi järkevää mahdollisuuksien mukaan yhtenäistää eri hallinnonalojen järjestelmäympäristöjä huomioiden toki tähän yhtenäistämiseen liittyvät riskit. Ei siis riitä pelkkä kyberiin rahojen laittaminen, vaan olisi hyvä yhdistää tarkastelu siitä mitä on järkevää olla olemassa, jotta kyberiin panostettavat rahat olisivat mahdollisimman tehokkaasti käytössä. Rahamäärä ei kuitenkaan tule todennäköisesti laskemaan, vaikka elinkaaren päässä olevista hallinnonalojen omista järjestelmistä luovuttaisiin ja otettaisiin käyttöön yhteisiä järjestelmiä (kyberpuolustuksen kustannustason nousu monimutkaisuuden lisääntyessä).

Sivun 11 toimintaympäristön muutoksessa voisi mainita yhtenä kohtanaan kvanttiteknologian myötä kasvava nykyisen salauksen helpommin murtava laskentateho tai tekoälyn myötä taitavammiksi

kehittyvät kyberrikollisten menetelmät, joita voidaan hyödyntää ja hyödynnetään valtiollisessa tiedonhankinnassa ja tiedustelutoiminnassa. Ne ovat muuttuvan toimintaympäristömme olennainen osa. Tekstin vuosi muuttaa muotoon: ”Kiihtyvä digitalisaatio ja sitä entisestään vauhdittanut COVID19-pandemia, tekoälyn ja kvanttiteknologian edistyminen, Venäjän hyökkäyssota Ukrainassa, maailmanlaajuisesti kiristynyt geopoliittinen tilanne ja Suomen Nato-jäsenyys sekä voimakkaasti kehittynyt kyberturvallisuuteen vaikuttava EU-sääntely korostavat kyberturvallisuuden merkitystä osana yhteiskunnan suojaamista.”. Myöhemmin strategiatekstissä käsitellään tekoäly ja kvanttiteknologia kattavasti, mutta voisi ne ottaa puheeksi jo alusta alkaen.

Muotoiluehdotus kohtaan Suomeen kohdistuva vihamieleinen kybertoiminta lisääntyy (s. 11): ”Teknisten häiriöiden lisäksi myös vihamielisen toiminnan vaikutukset voivat yltää Suomeen valtion rajojen ulkopuoleltakin ja levitä ennalta-arvaamattomasti, vaikka Suomi ei olisikaan niiden pääasiallisena kohteena. Kun vihamielinen kybertoiminta lisääntyy ja kohdistuu yhä laajemmin myös hallituksiin, demokraattisiin instituutioihin, yrityselämään ja kansalaisiin, kasvaa myös tarve valtioiden ja toimialojen/elinkeinoelämän sektoreiden rajat ylittävälle yhteistyölle. Tämän vuoksi oman toimintaympäristön, tietojärjestelmien ja etenkin näiden välisten keskinäisriippuvuuksien tuntemus on entistä tärkeämpää.”.

Muotoiluehdotus kohtaan ”Teknologinen murros lisää kaikkien vastuuta kyberturvallisuudesta” (s. 12): ”Teknologisia häiriötilanteita aiheuttavat esimerkiksi inhimilliset virheet ohjelmistokehityksessä ja niiden toimitusketjuissa sekä tarkoituksella luodut haavoittuvuudet kuten takaportit teknologiaan. Ne luovat rikollisille ja valtiollisille toimijoille pääsyn tietojärjestelmiin sekä niiden kautta toimijoiden tavoittelemaan tietoon. Organisaatioiden ja kansalaisten vastuu ohjelmistojen päivityksissä on jatkossakin tärkeää. Sääntelyllä voidaan edistää turvallisen teknologian kehittymistä, mutta samaan aikaan kun turvallisuustoimenpiteitä tehdään, myös hyökkääjät kehittävät uusia tapoja niiden kiertämiseksi.”.

Muotoiluehdotus kohtaan ”Kansainvälinen yhteistyö vahvistaa Suomen kyberturvallisuutta” (s. 13): ”Viime vuosina merkittävästi kehittynyt kyberturvallisuuteen vaikuttava EU-sääntely vahvistaa Suomen ja muiden EU-maiden kyberturvallisuutta. Sääntelyn kansallinen täytäntöönpano ja organisaatioiden toiminnan mukauttaminen sen mukaisesti haastavat tulevina vuosina niin viranomaisia kuin elinkeinoelämääkin. Nämä kasvattavat osaamis- ja koulutustarpeita ja kustannuksia riittävän suojan rakentamiseksi ja edellyttävät lisätoimenpiteitä kyberriskien hallitsemiseksi. Sääntelyllä luodaan edellytykset parantaa yhteiskunnan kriittisten toimijoiden kyberturvaa ja laitteiden ja ohjelmistojen sisäänrakennettua turvallisuutta. Samalla kehitetään viranomaisten ja elinkeinoelämän toimijoiden toimintaa varautumista sekä toimintaa häiriötilanteissa, sekä reagoinnissa ja vastatoimissa.”.

Muotoiluehdotus kohtaan ”Kansallista toimintamallia kehitetään” (s. 13): ”Kansallinen kyberturvallisuuden toimintamalli kyberturvallisuudessa on perustunut kykyyn parantaa jatkuvasti tietojärjestelmien ja organisaatioiden toimintaa kyberhyökkäyksien ja teknisten häiriöiden sietämiseksi ja niistä palautumiseksi. Organisaatioiden toiminnan jatkuvuuden kannalta elintärkeän tiedon tunnistamisen ja suojaamisen merkitys kasvaa. Toimintaympäristön ja kyberuhkien muutos haastaa aikaisemmat toimintatavat ja tarve varautumistoimien ja reagoinnin kehittämiselle sekä aiempaa proaktiivisemmille varhemmin ennakoivien koordinoitujen vastatoimien tarve on kasvanut. Kokonaisturvallisuuden malli mahdollistaa myös kyberturvallisuusalan varautumisen ja yhteistyön kehittämisen yhteiskunnan turvallisuusstrategian mukaisesti.”.

Tietojärjestelmien ja organisaatioiden toiminta ei välttämättä sisällä ajatusta toiminnalla suojattavasta aineettomasta pääomasta. Siksi sen voisi erikseen sivulla 13 mainita.

Muotoiluehdotus kohtaan ”Toimitusketjujen turvallisuus korostuu” (s. 14, 1. kpl, viimeinen virke): ”---. Yhteiskunnan toimintakyvyn kannalta kriittisten toimijoiden täytyykin varmistaa, että myös niiden palveluntuottajat ja toimitusketjut ovat kyberturvallisia ja pystyvät suojaamaan toiminnan jatkuvuuden kannalta elintärkeät tiedot.”

Tekstissä olisi hyvä korostaa tiedon suojaamista, koska nyt teksti keskittyy järjestelmiin. Ne ovat kuitenkin vain väline, kun taas tieto on kiinnostava ja haluttu kohde, jota välineellä suojataan. Toki tämä on kyberturvallisuusstrategia ja siten teknologia on sen ytimessä, mutta teknologiakaan ei ole itsetarkoitus vaan väline.

Muotoiluehdotus kohtaan ”Kyberturvallisuus mahdollistaa liiketoiminnan kasvun” (s. 15, 1 kpl, viimeinen virke): ”---. Toimintaympäristön muutoksen myötä kasvaa uudenlaisten ja tehokkaiden kyberturvallisuutta vahvistavien innovaatioiden tarve. Samalla painottuu organisaatioiden vastuu aineettoman pääomansa tuntemisesta ja suojaamisesta.”

Sivu 18, ”Kyberhäiriöiden aiheuttamat vahingot voivat olla sellaisia, ettei niitä pystytä täysin korvaamaan esimerkiksi tietojen tuhouduttua tai vuodettua pysyvästi. Jotkin pienet yritykset ovat jopa joutuneet lopettamaan toimintansa kyberturvallisuusriskien toteuduttua. Tämä korostaa entisestään riittävien resurssien kohdentamista kyberturvallisuuteen sekä yhteistyön ja yhteisten menettelytapojen tärkeyttä.”

Tekstiä voisi tästä vielä tarkentaa, koska sen viesti jää vähän epäselväksi. Jos kyberturvariski toteutuessaan johtaa pienen yrityksen toiminnan lopettamiseen ja syynä olisi se, että pieni yritys ei ollut kohdistanut riittäviä resursseja kyberturvansa toteuttamiseen, tehnyt yhteistyötä (kenen kanssa?) tai noudattanut (mitä) yhteisiä menettelytapoja, niin kenelle tai mille taholle näiden keinojen tärkeys korostuu? Lisäksi tekstissä olisi hyvä mainita sääntelyn noudattamisen tärkeys [joka mahdollisesti on eri asia kuin yllä mainittu menettelytapojen tärkeys].

Sivulla 18 todetaan, että ”Kyberympäristössä valtiollisten toimijoiden tiedonhankinnan ja vaikuttamisen kohteena ovat poliittisen päätöksenteon ohella myös viranomaisten ja elinkeinoelämän tuottamat yhteiskunnan elintärkeät toiminnot, palvelut ja niitä tukeva kriittinen infrastruktuuri, hallinnon, yritysten ja tutkimuslaitosten tietopääoma sekä innovaatiot.” Missä määrin järjestöt ovat tiedonhankinnan ja vaikuttamisen kohteena? Pitäisikö ne mainita listalla?

Sivu 19: ”Viranomaiset, yritykset ja yhteisöt tuottavat nykytilassa tehtäviensä hoitamiseksi tilannekuvia eri tasoilla, eri käyttötarkoituksiin ja erilaisella sisällöllä. Hallinnonalat tuottavat omaa tilannekuvaansa myös valtionjohdon tarpeisiin. Kansallisen kyberturvallisuuden tilannekuvan ylläpidosta ja analysoinnista vastaa Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus yhteistyötahojen kanssa. Strategisella tasolla toimivan Kyberturvallisuuden koordinaatioryhmän tavoitteena on varmistaa, että ministeriöillä ja kyberturvallisuusviranomaisilla on yhdenmukainen yleistilannekuva yhteiskunnan kyberturvallisuuden tilasta. Valtion kyberturvallisuusjohtaja toimii valtionjohdon neuvonantajana kyberturvallisuuteen liittyvissä asioissa.” Kappaleen alussa luetellaan viranomaiset, yritykset ja yhteisöt. Kappaleen muissa virkkeissä otetaan kantaa vain valtionjohdon ja viranomaisten tilannekuvan saantiin. Voisiko strategiassa ottaa kantaa siihen, onko tavoitteena luoda tilanne ja välineet, joilla yrityksiltä ja yhteisöiltä kerättyä tilannekuvatietoa voitaisiin kanavoida niille takaisinpäin kyberturvallisuuden toteuttamiseksi kriittisissä toiminnoissa?

Muotoiluehdotus osa-alueen osaaminen, teknologia ja TKI strategisiin tavoitteisiin (s. 22): ”Viranomaisten, yritysten ja yhteisöjen tietopääoma on suojattu kyberuhilta ja Suomi pyrkii kriittisen

salausteknologian osalta omavaraisuuteen.”. Kyberturvallisuus on käsite eikä käsitteellä ole pääomaa. Juridisella tai luonnollisella henkilöllä on pääomaa.

Muotoiluehdotus kohtaan ”Innovatiivinen ja kokeileva kyberekosysteemi” (s. 22): ”Kyberturvallisuuden ekosysteemi on kokonaisuus, joka käsittää laajasti yksityisen ja julkisen sektorin toimijat, yhteiskunnan eri tasojen osaamisen ja kyvykkyydet, toimijoiden välisen yhteistyön ja toimintatavat, vahvan kotimaisen kyberteollisuuden, oppilaitokset ja tutkimuslaitokset.”. Ensimmäisen pilarin ensimmäinen sana on osaaminen, mutta tavoitteissa ja sen jälkeen tulevassa tekstissä ei mainita oppilaitoksia. Puhutaan vain kouluista (ala-asteesta lukioon) ja tutkimuslaitoksista (VTT & Co). Siihen väliin jäävät oppilaitokset (yliopistot, ammattikorkeakoulut ja ammattikoulut). Oppilaitokset kattavat koulut.

Sivulla 23 on sama väliotsikko ”Innovatiivinen ja kokeileva kyberekosysteemi”.

Muotoiluehdotus kohtaan ”Osaaminen on kaikilla tasoilla vahvaa” (s. 23): ”Yritysten vastuulliseen toimintaan kuuluu kehittää kyberturvallisia kyvykkyyksiä, kartoittaa ja suojata tieto-omaisuutensa, tunnistaa uhkat, reagoida haitalliseen toimintaan ja ilmoittaa häiriöistä kybertoimintaympäristössä. Oppilaitoksissa opettajien valmiuksia kasvattaa oppilaita ja opiskelijoita kriittiseen medialukutaitoon. Tietoisuutta kyberriskeistä on vahvistettava laajan yhteiskunnallisen resilienssin lujittamiseksi. Kokonaisuudessaan suomalainen kyberturvallisuusosaaminen varmistetaan vahvistamalla kyberturvallisuuden roolia laajasti kasvatuksessa, koulutuksessa ja opetuksessa sekä yhteiskunnan ja työelämän kaikilla tasoilla.”. Tekstissä mainitaan kriittinen medialukutaito, joka liittyy ertiyisesti informaatiovaikuttamiselta suojautumiseen eikä kyberturvallisuuteen. Koska informaatiovaikuttaminen on päätetty jättää strategian ulkopuolelle, tässä voisi pohtia selkeyden vuoksi kuuluuko medialukutaito koko kappaleeseen.

Muotoiluehdotus kohtaan ”Innovatiivinen ja kokeileva kyberekosysteemi” (s. 23): ”---. Julkisen hallinnon henkilöstön kyberturvallisuusosaamista ja tietämystä sekä siihen liittyvistä vastuista kehitetään riittävän osaamistason varmistamiseksi. Innovatiivista kybertoimintaympäristöä tukee aktiivinen tiedon, osaamisen ja tilanneymmärryksen jakaminen.”

Tällä hetkellä lainsäädäntö ei tue aktiivista tiedon, osaamisen ja tilanneymmärryksen jakamista. Pitäisikö siihen ottaa ylle kopioidussa tekstikohdassa kantaa? Pelkkä kyberturvallisuusosaaminen ei riitä, vaan henkilöstöllä on oltava riittävä ymmärrys myös tiedonjakoa koskevasta ja siihen soveltuvasta lainsäädännöstä ja rohkeutta - tai ennemminkin selvä ohjeistus - sen sallimaan tiedonjakoon.

Muotoiluehdotus s. 25, ”Kyberturvallisuuden tietopääoma on turvattu”: ks. kommentti edellä. Käsitteellä ei voi olla tietopääomaa. Otsikon voisi muuttaa muotoon ”Tietopääoma on suojattu kyberuhkilta”. Kappaleessa olisi hyvä mainita myös henkilötiedot palveluiden, prosessien ja patenttien lisäksi. Elinkeinoelämän toimijoiden tietojärjestelmät ovat täynnä asiakastietoja, joista iso osa on henkilötietoja. Muutenkin sekä viranomaisten, elinkeinoelämän toimijoiden, että yhteisöjen olisi syytä tunnistaa elintärkeät tietonsa, koska sitä tietoa ne tarvitsevat pilvipalveluita käyttöön ottaessaan ja kvanttiturvalliseen salaukseen siirtyessään. Johonkin strategian kohtaan tämä perustelu olisi hyvä saada näkyviin.

s. 25, Pyrimme salausteknologiseen omavaraisuuteen: ”Kansallisesti merkittävien tietovarantojen käytettävyys, saatavuus ja luotettavuus kaikissa tilanteissa on tärkeä osa kyberresilienssiä.” Tässä on varmaan tapahtunut ajatusvirhe. Ehdotetaan muutettavaksi muotoon ”Kansallisesti merkittävien

tietovarantojen luottamuksellisuus, eheys ja saatavuus kaikissa tilanteissa on tärkeä osa kyberresilienssiä.”.

s. 26, Pilari II:n tavoite: ”Kyberharjoitusten ympäristöjä ja käytäntöjä kehitetään ja eri toimialojen välistä harjoittelua lisätään”. Ehdotetaan muutettavaksi muotoon ”Kyberharjoitusympäristöjä ja -käytäntöjä kehitetään ja toimialojen yritysten yhteisharjoittelua ja toimialojen välistä harjoittelu lisätään.”.

s. 26: ”Suomi varautuu kyberuhkiin ennakoivasti”. Ehdotetaan muutettavaksi muotoon ”Suomi varautuu kyberuhkiin” tai ”Suomi ennakoi kyberuhkia varautumalla”. Jälkikäteen ei voi enää varautua. Vahingon jälkeen vain korjataan ja toivutaan. Varautua voi vain ennakolta.

s. 27: Muutosehdotus: ”---. Julkisten palveluiden teknologioilta ja palvelutuotannolta edellytetään kyberturvallisuuden, tietoturvallisuuden ja tietosuojan vaatimustenmukaisuutta koko elinkaaren ajan. ---” Pelkkä kyberturva ei riitä digitalisoituneessa toimintaympäristössä.

Sivulla 27 todetaan ensimmäisessä lauseessa, että ”Yritykset ovat kiinnostuneita kehittämään varautumistaan liiketoiminnallisista lähtökohdista. Julkisen hallinnon on huomioitava toimintaympäristön muutokset asettaessaan yrityksille varautumisvaatimuksia turvallisuuden näkökulmasta ja tukiessaan yritysten varautumista.” Tämä on hieman suoraviivainen toteama. Tästä voisi päätellä yritysten kehittävän kyberturvallisuuteen liittyviä asioita vain, jos se on liiketoiminnallisesti kannattavaa ja julkinen puoli asettaa tiukkoja vaateita, koska muuten yritykset eivät tee mitään. Näin suoraviivaisesti asia ei ole ja moni yritys toteuttaa kyberturvallisuutta myös yhteiskunnallisesta ja vastuullisuus näkökulmasta kustannukset huomioiden. Lausetta voisi vielä pohtia uudestaan vastaamaan paremmin todellisuutta.

s. 27: ”---. Kokonaisturvallisuuden mallin mukaisesti viranomaiset tekevät kyberturvallisuuden varautumistyötä tiiviissä yhteistyössä yritysten, järjestöjen ja kansalaisten kanssa.---” Tähän listaan voisi lisätä oppilaitokset ja tutkimuslaitokset. Nykyisen työvoimapulan vallitessa läheinen yhteistyö osaajia kouluttavien tahojen kanssa on merkittävää osaamisen huoltovarmuutta turvattaessa.

Sivulla 27, kohdassa ”Varautumistyötä tehdään yhteistyössä” mainitaan, että kyberturvallisuuden varautumisessa ”tiedustelu tukee varautumista ja ennakointia hankkimalla ja jakamalla tiedustelutietoa…”. Jäljempänä todetaan, että ”Tiedusteluviranomaisten tehtävänä on hankkia tietoa, analysoida ja raportoida sitä turvallisuusviranomaisten ja valtionjohdon tueksi.” (s. 50, kohta operatiiviset viranomaiset). Huomioitava on, että tällainen tieto päätyy tiedon korkean turvaluokan takia harvoin kyberturvallisuuden varautumistyön tueksi, mihin sisällytettynä strategiaan tulisi asettaa muutoksen tavoitetila.

Muutosehdotus kohtaan ”Varautuminen perustuu pitkäjänteiseen resursointiin” (s. 28): ”Kattavan uhka- ja riskiarvion ja lakisääteisten velvoitteiden pohjalta tunnistettujen tarpeiden edellyttämät kyberturvallisuusresurssit sisällytetään julkisen hallinnon, yritysten, ja yhteisöjen, oppilaitosten ja tutkimusyhteisöjen toiminta- ja taloussuunnitelmiin. Kyberturvallisuuden resurssien tehokas käyttäminen edellyttää, että kyberturvallisuustehtävät suunnitellaan ja toteutetaan tehokkaasti laajassa kansallisessa ja kansainvälisessä yhteistyössä valtionhallinnon, yritysten ja yhteisöjen sekä alue- ja paikallishallinnon kanssa.”. Tässäkin on hyvä huomioida oppilaitokset ja tutkimusyhteisöt.

Muutosehdotus kohtaan ”Harjoitustoimintaa lisää” (s. 29): Kyberharjoitusten ympäristöjä > Kyberharjoitusympäristöjä. Kyberharjoituksen ympäristö voi olla vaikkapa kokoustila. Kyberharjoitusympäristö taas on se tekninen järjestelmä, jolla harjoitus toteutetaan. Tässä kohdassa voisi mainita myös toistuvan ja/tai jatkuvan ja/tai säännöllisen harjoittelun. Nykyisellään eri

toimialojen ISAC-harjoituksia järjestetään säännöllisesti, mutta saman toimialan yritykset harvemmin harjoittelevat yhdessä, saati toistuvasti. Niinpä toimialojen välisen harjoittelun lisäksi voisi mainita toimialan sisäisen toistuvan yhteisharjoittelun tilanteen kohentamiseksi nykyisestä. Myös sen voisi mainita, että yritysten ja viranomaisten olisi hyvä harjoitella yhdessä, toistuvasti.

Lisäysehdotus kohtaan ”Yhteinen tilanneymmärrys toiminnan perustana” (s. 33-34): ”Tilannetietoja vakavista kyberuhkista on voitava jakaa entistä tehokkaammin huoltovarmuuskriittisille yrityksille, kunnille, kuntaomisteisille palveluntarjoajille sekä hyvinvointialueille tarkoituksenmukaisella tavalla jakelurajoitteet huomioiden. Korkeasti turvallisuusluokitellun tiedon jakaminen edellyttää siihen soveltuvien järjestelmien kehittämistä ja käyttöönottoa.”. Teknisesti jakelua on varmasti toteutettavissa, ja se vaatii taloudelliset pysyvästi sidotut resurssit toiminnan mahdollistavaan sujuvaan järjestelmään, mutta esteet saattavat löytyä lainsäädännöstä, joka olisi hyvä tuoda esiin myös strategiassa.

Muutosehdotus kohtaan ”Viranomaisten yhteistoiminta on sujuvaa ja saumatonta” (s. 34): Viranomaisten yhteistyö on sujuvaa ja saumatonta: suuri osa kriittisestä infrastruktuurista on yksityisen sektorin, elinkeinoelämän hallussa ja digitaaliset- sekä kyberratkaisut julkishallinnolle pääasiassa tarjoaa ulkoistetusti yksityiset yritykset. Kappaleessa olisi tärkeää ottaa kantaa viranomaisten ja elinkeinoelämän väliseen yhteistyöhön, jotta strategia on kattavasti kansallinen kyberstrategia olematta Suomen julkishallinnon kyberturvallisuusstrategia. Aika usein hv-kriittisten yritysten toivotaan tuottavan osuutensa jaettuun tilannekuvaan, mutta sitten siitä ei pystytä jakamaan niille takaisin toiminnan kannalta merkityksellistä tietoa. Tällöin myös otsikon voisi muuttaa toiseen muotoon. Samassa kappaleessa todetaan, että operatiivisen yhteistyön toimeenpanoa, vastuita sekä vakaviin kyberuhkiin ja -häiriöihin varautumista ja niihin vastaamista koordinoidaan virastotason yhteistyörakenteessa, jonka muodostavat Liikenne- ja viestintävirasto Traficom, keskusrikospoliisi, Puolustusvoimat sekä suojelupoliisi. Huoltovarmuuskeskuksella on ja on olut keskeinen rooli elinkeinoelämän varautumisen tukemisessa ja kansallisten kyvykkyyksien rakentamisessa, mutta sitä ei mainita tässä yhteydessä. Onko ryhmän siis tarkoitus pohtia varautumista vain julkishallinnon näkökulmasta vai miksi Huoltovarmuuskeskus on jätetty ryhmän ulkopuolelle? Jos ryhmä tehtävänä on pohtia myös elinkeinoelämän varautumista, Huoltovarmuuskeskuksen voisi lisätä ryhmään mukaan vastaten jo nykyisellään toteutuvaa kehityksen mahdollistamista ja huomioiden tulevaisuuden tarpeet osana kriittisten toimintojen turvaamista.

Muutosehdotus kohtaan ”Mahdollisuudet ja kyvyt vastata kyberuhkiin varmistetaan” (s. 36): ”---. Yhteiskunnan häiriöttömän toimivuuden edellytyksenä on, että organisaatioilla on kyky palautua kyberhäiriöistä ja hyökkäyksistä nopeasti, ja palauttaa järjestelmät ripeästi ja turvallisesti takaisin käyttöön sekä valmius tarvittaessa jakaa ja saada tietoa yhteistyöverkostossaan.”. Tässä voisi korostaa yhteistoiminnan mahdollisuutta ja tarvetta.

Muutos ehdotus kohtaan ”Mahdollisuudet ja kyvyt vastata kyberuhkiin varmistetaan” (s. 37): ”Operatiivisesta toiminnasta vastaavien viranomaisten tehtävänä on ennaltaehkäistä kyberuhkia, reagoida niihin, selvittää niitä sekä muodostaa niistä tilannekuvaa kyberuhista.”

Muutosehdotus kohtaan ”Kyberhäiriöiden ja -uhkatilanteiden johtamismallia kehitetään” (s. 37): Malli on viranomaiskeskeinen ja siitä unohdettu yksityinen sektori. On tärkeä huomioida, miten malli palvelee tai ohjaa esim. energiasektorin yrityksiä vakavassa tietoturvapoikkeamassa. Strategian ensimmäisessä kappaleessa todetaan, että ”Erityisesti on kasvanut tarve viranomaisten ja elinkeinoelämän väliselle yhteistyölle”. Tämä on konkreettinen paikka, joissa yhteistyö tulee esille ja on tarve huomioida strategisten tavoitteiden toteutus osana kehittyvää toimintaa.

Muutosehdotus kohtaan ”Torjutaan järjestäytynyttä ja vakavaa kyberrikollisuutta” (s. 38): ”---. Viranomaisten tavoitteena on torjua erityisesti järjestäytynyttä ja vakavaa kyberrikollisuutta, heikentää rikollisten toimintaedellytyksiä sekä varmistaa, etteivät järjestäytyneet rikollisryhmät tai muut yhteiskunnalle vaaralliset toimijat laajenna toimintaansa yhteiskunnan rakenteisiin, talouteen tai päätöksentekojärjestelmiin.”. Tähän voisi lisätä vastaavan toteamuksen yksityisen sektorin ja järjestöjen tavoitteesta. Yksityinen sektori varmaankin tavoittelee tietopääomansa ja kilpailuetunsa suojaamista sekä toiminnan jatkuvuuden turvaamista. Voivatko viranomaiset ja yksityinen sektori toimia yhteistyössä kyberrikollisuuden torjumisessa? Millaisista toimenpiteistä tai tavoitteista silloin puhuttaisiin?

Tarkennus kohtaan ”Kyberpuolustuksen tehtäviä ja roolia tarkennetaan” (s. 39): ”…Näitä ovat muun muassa diplomatian, tiedustelun, informaation hallinnan ja strategisen viestinnän, sotilaallisen suorituskyvyn, rikostorjunnan ja finanssialan keinot sekä taloudelliset, oikeudelliset ja muut kyberturvallisuuden keinot.”. Tarkoitetaanko finanssialan keinoilla pakotteita? Tätä voisi ehkä tarkentaa.

Tarkennus kohtaan ”Resursointi, toimeenpano ja seuranta” (s. 41): Tekstissä todetaan, että ”Varovaisen arvion mukaan elinkeinoelämän panostukset kyberturvallisuuteen ovat vähintään kymmenkertaisia verrattuna valtionhallinnon osoittamaan rahoitukseen.”. Miten tämä arvio on tehty? Menetelmää voisi vähän avata tekstiin, jotta arvion todenmukaisuudesta saisi paremman kuvan. Lisäksi saman otsikon alla todetaan, että ”Kaikkien strategisten tavoitteiden ja kehittämistoimien toteuttamiseen on suunnattava lisää resursseja.” (s. 41) ja ”Kansallisten resurssien määrittämisessä keskeistä on arvioida vaihtoehtoiskustannuksia eli kustannuksia, jotka syntyvät, jos strategian kehittämistoimia ei toteuteta tehokkaasti.” (s. 42). Pelkkä rahan lisääminen ei ole ratkaisu, vaan julkisella puolella pitää myös arvioida kriittisesti kuinka eri hallinnonaloilla elinkaarensa päässä olevia järjestelmiä kannattaa uudistaa. Nyt hallinnonaloilla on hyvin itsenäisesti mahdollisuus hankkia järjestelmiä ja miettiä prosessejaan. Olisi hyvä, että osana resursointia digitaalisille rakenteille ja niiden suojaamiselle tehdään resursoinnin ja turvallisuuden näkökulmasta suunniteltuja rakenteelllisiamuutoksia ja sitä kautta pitkällä aikajänteellä tapahtuisi muutos myös kyberturvallisuuden näkökulmasta.

Muutosehdotus kohtaan ”Strategiset kehittämisehdotukset” (s. 44): tällä sivulla on kaksi identtistä tavoitetta, jossa edistetään viranomaisten yhteistoimintaa: ”Kehitetään viranomaisten yhteistoimintaa ja yhteistä tilanneymmärrystä luomalla tarvittavat yhteistyörakenteet ja koordinointimallit, selkeyttämällä roolit ja vastuut sekä varmistamalla tiedonvaihdon ja tiedonsaannin edellytykset.”. Toisen näistä voisi poistaa. Lisäksi vielä kolmannessa kohdassa todetaan, että vahvistetaan viranomaisten yhteistoimintaa: ”Vahvistetaan viranomaisten, alue- ja paikallishallinnon, yksityissektorin ja kansalaisyhteiskunnan yhteistoimintaa ja yhteistä varautumista.”. Viranomaiset voisi jättää tästä kokonaan pois ja sen sijaan keskityttäisiin yksityiseen sektoriin ja muuhun kansalaisyhteiskuntaan.

Muutosehdotus kohtaan ”Huoltovarmuusorganisaatio” (s. 52): Huoltovarmuusorganisaation kuvaus sisältää väärää tietoa kuten esim. ”seitsemän sektoria tai kahdeksan poolia”. Huoltovarmuusorganisaation kuvaus tulee kirjoittaa uudestaan. Ajantasainen kuvaus löytyy esim. osoitteesta https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio. Tuemme mielellään kohdan ajantasaistamisessa toimintaa vastaavaksi.

Lisätietoja:

Juha Ilkka

Johtava varautumisasiantuntija

Digitaalinen turvallisuus

Jarna Hartikainen

Yksikönjohtaja

Varautumisen suunnittelu ja ohjelmajohtaminen -yksikkö

Ilkka Juha
Huoltovarmuuskeskus - Juha Ilkka, johtava varautumisasiantuntija,
varautumisen suunnittelu ja ohjelmajohtaminen -yksikkö