WithSecure Consulting

Lausunto

09.08.2024

Asia: VN/36693/2023

Lausuntopyyntö Suomen kyberturvallisuusstrategiasta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

WithSecure Oyj (“WithSecure”) kiittää mahdollisuudesta lausua asiasta. WithSecure on suomalainen yritys, joka tarjoaa tietoturvaratkaisuja ja palveluita Suomessa, Euroopassa, Yhdysvalloissa ja Aasian maissa.

Haluamme kiinnittää huomiota seuraaviin seikkoihin luonnoksessa Suomen kyberturvallisuusstrategiaksi 2024 - 2025:

#Johdanto – kyberturvallisuus on osa kokonaisturvallisuutta

WithSecure katsoo, että kyberturvallisuuden nostaminen merkittäväksi osaksi Suomen kokonaisturvallisuutta ja sen tunnistaminen yhteiskuntakriittisten toimintaedellytysten mahdollistajana on äärimmäisen tärkeää. Tämä avaa ovet kyberturvallisuuden laajempaan tietoisuuden nostamiseen, julkiseen keskusteluun, yhteistyöhön ja kehittämiseen. Suomen hallinnon ja lainsäädännön tuki kyberturvallisuuden kehittämiselle on välttämätöntä yhteiskuntamme digitaalisen turvallisuustason eteenpäin viemiselle.

Katsomme, että Suomen kyberturvallisuusstrategian vision tulee olla vahvasti ja selkeästi muotoiltu. Luonnoksessa strategian visio jää kuitenkin hieman hajanaiseksi, osittaisia tavoitteita on kuvattu pitkin asiakirjaa, mutta kokonaisvisiota Suomen kyberturvallisuudesta 2035 ei ole mielestämme riittävän selkeästi kuvattu.

Onko visiona olla ”mahdollisimman hyvä, niin hyvä kuin näillä toimenpiteillä saadaan aikaiseksi” vai voisiko tavoitetilan määritellä tarkemmin?

Strategian osa-alueet (pilarit) ovat enemmänkin mahdollistajia (enabler), kuin varsinaisia strategian osa-alueita. Katsomme, että visiossa tulisi näkyä selkeästi, miten nyt tunnistetut ongelmat on ratkaistu vuonna 2035. Näin vision mukaisen tilan saavuttaminen olisi merkittävämpää, erillisten kehitystoimien tekemisen sijaan.

#Toimintaympäristön muutos

Toimintaympäristö on muuttunut radikaalisti viimeisen muutaman vuoden aikana. Strategiassa mainitaan kybervakoilu ulko- ja turvallisuuspoliittisena uhkana, mutta myös teollisuusvakoilu taloudellisen kilpailukyvyn uhkana.

WithSecure katsoo, että Suomen kyberturvallisuustrategiassa olisi viimeisimpien kokemusten valossa syytä korostaa enemmän uhkaa yhteiskunnan kriittisiin toimintoihin ja prosesseihin. Näihin tahoihin kohdistuvilla kyberhyökkäyksillä voi olla merkittäviä vaikutuksia ihmisten turvallisuuteen ja yhteiskunnan toimivuuteen.

#Tavoitetila ja rakenne

#Pilari l: Osaaminen, teknologia ja TKI

Lainsäädännöllä, kuten kyberturvallisuusdirektiivin (NIS2-direktiivi) käynnissä olevalla toimeenpanolla tavoitellaan tietoturvallisuuden tason nostamista jäsenvaltioissa. Valtiovallan pitäisi velvoitteiden säätämisen lisäksi osallistua tietoturvan resurssointiin, jotta parannuksia saadaan aikaiseksi. Niin julkisella sektorilla kuin yksityisellä sektorillakin tarvitaan lisää osaamista ja oikeita mahdollisuuksia, suunnitella ja toteuttaa toimivaa tietoturvaa. Tämä aspekti olisi hyvä olla näkyvästi myös rakenteen kaavakuvassa.

WithSecure katsoo, että tietoturvaosaaminen olisi hyödyllistä ottaa osaksi jo varhaiskasvatusta, koska tämän päivän lapset käyttävät/altistuvat tietotekniikalle hyvin varhain. On tärkeää, että ns. digitaalikasvatukseen kuuluu ikätasoon sopivalla tasolla myös tietoturvatietoisuus.

Perustasoiset kansalaisille suunnatut tietoturvakoulutukset voisi sisällyttää vaikkapa YLEn toimintasuunnitelmaan.

Tavoite kriittisen salausteknologian omavaraisuuteen (kvanttiteknologia) on tärkeä, mutta haastava. Jos halutaan koulutuksen kautta lisätä omien osaajien määrää niin päätöksiä pitää tehdä heti lähitulevaisuudessa, koska tulosten aikahorisontti on pitkä.

#Pilari ll: Varautuminen

Varautuminen on resurssi-intensiivistä. Varautumisen ytimessä on ajatus, että joukko ihmisiä allokoidaan miettimään etukäteen, mikä voi mennä pieleen, miten tilanteesta voitaisiin missäkin olosuhteissa palautua ja etenkin mitä investointeja mahdollisesti tarvitaan toimintakyvyn turvaamiseksi. Tämän osalta katsomme, että olisi hyvä miettiä erilaisia resurssienkäytön optimointimahdollisuuksia ja tällaista toimintaa tukevaa rahoitusta.

WithSecure katsoo, että teknologian uudistuessa, varautumisen kyvykkyyttä tulisi upottaa operatiivisiin toteutuksiin, sen sijaan, että tehdään erillisiä varautumiseen liittyviä ratkaisuja. Normaalit valvonta- ja häiriöprosessit yhdistettynä tehokkaisiin teknologiaratkaisuihin vahvistaa kybersietoisuutta arjessa ja ratkaisut toimivat sellaisenaan varautumisessa yhteiskunnan kannalta poikkeustilanteisiin.

Julkisten palvelujen tulee olla luotettavia, mutta lisäksi niiden tulee olla käyttäjäystävällisiä ja tukea kyberturvallista käyttöä. Julkisten palveluiden vaatimuksenmukaisuuden tulisi pohjautua selkeästi yhtenevään kriteeristöön, joka pohjautuu yleiseen ylläpidettyyn standardiin. Toimialakohtaisesti viranomaisen tulee täydentää/tarkentaa vaatimuksia toimialaan sopiviksi ja kerätä parhaita käytäntöjä.

Automaattinen tekninen seuranta ja valvonta ovat avainasemassa kyberturvallisuuden tilannekuvan ja käytön turvallisuuden mahdollistamiseksi. Tätä tulisi painottaa voimakkaammin.

Kyberrikollisuuden ehkäisemisestä on hyvin nostettu esiin, että se nojaa välttämättä yhteiskunnan kaikkien toimijoiden aktiiviseen toimintaan. Tämä tulisi avata tavoitteessa (ennaltaehkäistään kyberrikollisuutta).

#Pilari lll: Yhteistoiminta

Tilannekuvan luominen on tärkeää ja se perustuu riittävään tiedonvaihtoon ja -jakamiseen. Nykytilanteessa haasteita luovat niin tietojenvaihdon rajoitteet, puutteelliset toimintatavat kuin edellytyksetkin. Näiden lisäksi haasteita aiheuttaa myös luottamuksen puute siitä, että vastaanottaja käsittelee tietoa turvallisesti.

WithSecure katsoo, että tiedonjakamisen osalta on tärkeää määritellä myös yhteiset pelisäännöt siitä, mitä tietoa jaetaan, miten sitä jaetaan, prosessoidaan ja tallennetaan tietoturvallisesti. Tiedon tuottajan täytyy pystyä varmistumaan siitä, että jaetut tiedot pysyvät turvassa myös vastaanottajalla ja mahdollisella kolmannella osapuolella.

WithSecure toivoisi strategiassa voimakkaampaa painotusta eri organisaatioiden ja yritysten omaan toimintaan liittyvän riskiymmärryksen tärkeyteen. NIS2 on tietoturvallisuuden minimiregulaatio, joka pitäisi olla täytettynä kaikkien toimijoiden osalta jo ihan liiketoimintariskienkin valossa. Kriittisen infrastruktuurin toimijoiden tulisi pyrkiä täyttämään sen vaatimukset kirkkaasti, ei minimitasoja juuri juuri täyttäen. Kyberympäristöjen suojaamisessa yksityiskohdilla on valtava merkitys, ja ruohonjuuritason kyberhygieniakäytännöillä toimijoiden IT ympäristöissä on suora johdettavissa oleva vaikutus koko yhteiskunnan kyberresilienssiin, tässä strategiassa hyvin kuvattujen yhteyksien vuoksi.

Aina kuitenkaan parempi ohjeistus tai sääntely ei tarkoita deskriptiivisempää ja yksityiskohtia määräävämpää ohjausta, vaan enemmänkin korotettua ymmärrystä ja tietoisuutta olennaisten asioiden merkityksestä suurempaan kuvaan. Olisiko tämä kyberpuolustusdokriinin mahdollisia asiakohtia?

#Pilari lV: Reagointi ja vastatoimet

WithSecure katsoo, että viranomaisten yhteistyö on sujuvaa ja saumatonta, mutta vastuut pitää olla selkeät, koska kyberhäiriön tai -hyökkäyksen tunnistaminen alkuvaiheessa on erittäin vaikeaa. Vastuuta ei voi määritellä hyökkäyksen toimijan tai tämän motivaation varassa, vaan vastatoimien kyvykkyyden näkökulmasta. Tämä tulee huomioida myös keskitetyissä kyberturvallisuuspalveluissa.

Tarkan ja perusteltavissa olevan attribuoinnin yksi olennaisimmista elementeistä on ruohonjuuritasolla tehtävä IT -forensiikka, ja sitä tukevat ruohonjuuritason IT -prosessit kuten lokien käsittely, turvatapahtumien analysointi ja hyökkäyksen tunnuspiirteiden tunnistamisen lokimassoista (Indicators of Compromise, IoC). Tällä WithSecure viittaa edellisessa kappaleessa avattua ajatusta, että NIS2 tulee nähdä toimintaa ohjaavana minimitasona, ja olennaista on nähdä regulaation läpi siihen yhteiskunnalliseen kyberturvallisuuden tasoon mihin organisaation tuottama kriittinen rooli heitä edellyttää.

#Resursointi, toimeenpano ja seuranta

Strategiassa on ymmärretty hyvin resursoinnin ja investointien kasvattamisen tarve. Kun arvioidaan kyberturvallisuuden nurjan puolen kustannukset, pitäisi olla selkeää, että nyt on korkea aika investoida ennaltaehkäisyyn.

WithSecure katsoo, että Naton ja EU:n kehittämisrahoituksen hyödyntäminen edellyttää hallinnonalojen välisen joustavan yhteistyön lisäksi kiinteän yhteyden kyberalan yrityksien kanssa.

#Strategiset kehittämisehdotukset

WithSecure katsoo, että strategian seurannalle tulee määritellä mittarit, jolla 5 vuotisjaksoissa seurataan edistymistä. Traficom on julkaissut Kybermittarin, joka soveltuu tähän tarkoitukseen erinomaisesti. Vuosittaisen seurannan mittareina voidaan hyödyntää esitettyä Kyberturvallisuuden suorituskykyindikaattoria.

#Liite 1: Kyberturvallisuuden kansallinen yhteistoimintamalli

Hajautettu rakenne toimii tilannekuvan, ennakoinnin ja koulutuksen näkökulmasta, mutta kyberkriisitilanteessa johtamisen tulisi olla selkeää ja tällä taholla osaavat resurssit.

WithSecure katsoo, että osaaminen ja kyky johtaa ovat avainasemassa, jolloin myös tulee rajata pois päällekkäiset viranomaistoimet.

Tässä kappaleessa tuodaan esiin yksi tämän strategian avainkohdista, yksittäisessä lauseessa: ”Elinkeinoelämä tuottaa valtaosan yhteiskunnan tieto- ja kyberturvallisuuspalveluista”. Tätä asian tilaa olisi WithSecuren mielestä syytä peilata myös muihin strategian pilareihin, jotka ovat voimakkaan virkakoneisto- ja virastokeskeisiä. Miten se tosiasia että Suomen tietoturvaosaamisesta valtaosa on mukana elinkeinoelämässä, tulisi ottaa huomioon ja käyttöön rauhanajan kehitys- ja valvontatyössä, ja miten tämä tulisi ottaa huomioon mahdollisissa poikkeusoloissa?

Kunnioittavasti

WithSecure Oyj

Tiina Sarhimaa

Lakiasiainjohtaja

Lisätietoja:

Antti Laatikainen, Johtava kyberturvakonsultti Sari Lindroos, Tietoturvapäällikkö,

antti.laatikainen@withsecure.com sari.lindroos@withsecure.com

+358 406372163 +358 405174623

Laatikainen Antti
WithSecure Consulting