Ehdotus valtioneuvoston periaatepäätökseksi kyberturvallisuuden kehittämisohjelmasta

13.1.2021

Sisältö

1 Johdanto

Pääministeri Sannan Marinin hallitusohjelmassa on asetettu tavoitteita kansallisen kyberturvallisuuden kehittämisestä liittyen tilannekuvan parantamiseen, kansainvälisen yhteistyön tiivistämiseen sekä kansallisen koordinaation tehostamiseen. Vuonna 2019 annetussa valtioneuvoston periaatepäätöksessä Suomen kyberturvallisuusstrategiasta on tunnistettu tarve kansallisen kyberturvallisuuden kokonaistilan parantamiseksi. Kyberturvallisuusstrategia on osa yhteiskunnan turvallisuusstrategian (2017) ja EU:n kyberturvallisuusstrategian toimeenpanoa. Tämä periaatepäätös kansallisen kyberturvallisuuden kehittämisestä vastaa edellä mainittuihin tavoitteisiin. Valtioneuvoston periaatepäätös julkisen hallinnon digitaalisesta turvallisuudesta ja sen toimeenpanosuunnitelma sekä Huoltovarmuuskeskuksen Digitaalinen turvallisuus 2030 -hanke täydentävät tätä periaatepäätöstä ja vastaavat omasta rahoituksestaan.

Kyberturvallisuuden kokonaistilan parantamista koskevaan tarpeeseen ovat vaikuttaneet yhteiskunnan toimintaympäristössä tapahtuneet merkittävät muutokset, jatkuvasti kehittyvät kyberturvallisuusuhkat, ICT-ympäristöjen kompleksisuuden lisääntyminen, sulautettujen ja perinteisten ICT-järjestelmien konvergenssi sekä kansallisessa toiminnassa havaitut kehittämiskohteet. Kyberturvallisuusuhkien realisoitumisen nähdään aiheuttavan myös entistä suurempia vaikutuksia vahvasti verkottuneeseen yhteiskuntaan. Yhteiskunta on yhä riippuvaisempi digitaalisesta toimintaympäristöstä, minkä vuoksi kyberturvallisuuden tulee olla sisäänrakennettuna kaikessa toiminnassa, prosesseissa ja järjestelmissä, joihin kohdistuu uhkatekijöitä. Hyvä kyberturvallisuuden taso voidaan saavuttaa vain, jos jokainen digitaaliseen yhteiskuntaan kytkeytynyt toimija kantaa oman vastuunsa kyberturvallisuuden toteutumisesta. Kyberturvallisuus tulee nähdä luonnollisena osana jokaisen organisaation ja yksilöiden yhteiskuntavastuuta.

Kehittämisohjelman aikajänne on 2021-2030 (kuva 1) ja se kuvaa kyberturvallisuuden kehittämisen lyhyen ja pitkän aikavälin tavoitteita ja painopistealueita. Kehittämisohjelman toimeenpanosuunnitelma kuvaa puolestaan tavoitteiden saavuttamiseksi tarvittavat toimenpiteet vastuineen ja mittareineen. Kehittämisohjelman toimenpiteiden vai-

kuttavuutta on arvioitu kansainvälisestä, kansallisesta, hallinnon- ja toimialan, yrityksen sekä kansalaisen näkökulmasta huomioiden nyky- ja tavoitetila sekä soveltuvin osin tarvittavat investoinnit. Toimeenpanosuunnitelman ajantasaisuutta arvioidaan ja toimenpiteitä päivitetään vuosittain. Kehittämisohjelman toteuttaminen edellyttää 5,9 miljoonan euron rahoitusta vuosittain ajanjaksolle 2022 – 2025 ja 3,2 miljoonan euron lisärahoitusta vuodelle 2021.

Kyberturvallisuuden kehittämisohjelman toteutusta sekä kehittämistoimien ajantasaisuutta seurataan säännöllisesti liikenne- ja viestintäministeriössä sekä Turvallisuuskomiteassa. Kehittämisohjelman toimeenpano käynnistetään välittömästi.

Kehittämisohjelman toteuttamista tukee kyberturvallisuusstrategiassa asetettu kyberturvallisuuden johtamisen koordinaatiomalli. Koordinaatiomallissa huomioidaan julkisen hallinnon ja elinkeinoelämän kyberturvallisuuden suunnittelu, kehittäminen ja yhteistyö. Liikenne- ja viestintäministeriöön sijoitetun kyberturvallisuusjohtajan tehtävänä on kehittää kybertoimintaympäristön yhteistyötä ja osaamista eri sektoreilla. Näiden lisäksi, osana tätä kehittämisohjelmaa, parannetaan laajojen kyberturvallisuushäiriöiden operatiivisen tilannekuvan muodostamista ja operatiivista johtamista. Lisäksi huomioidaan kansainvälinen toimintaympäristö sekä kansainvälisen tason prosessit ja käytänteet, joilla pyritään parantamaan kyberturvallisuutta muun muassa EU:n piirissä.

Kehittämisohjelman valmisteluun osallistui yli 80 eri organisaatiota. Kehittämisohjelman valmistelun yhteydessä järjestettyihin työpajoihin osallistuivat muun muassa elinkeinoelämä, kyberturvateollisuus, valtionhallinto, yliopistoja sekä eri järjestöjä.

Kuva 1: Kyberturvallisuuden kehittämisohjelma ja sen keskeiset osat

2 Kehittämisohjelman tavoite ja pääteemat

Kyberturvallisuuden kehittämisohjelma lähestyy kansallista kyberturvallisuutta ennen kaikkea mahdollisuuksien näkökulmasta, jotka toteutuessaan vahvistavat kansallista kyberturvallisuutta ja elinvoimaa, pienentäen samalla nykyisistä puutteista tai kapeikoista johtuvia kyberturvariskejä. **Kehittämisohjelman ensisijaisena tavoitteena on luoda Suomeen kyberturvallisuuden ekosysteemi** (kuva 2), joka tuottaa elinvoimaa ja kasvua, lisää alan työpaikkoja, luo tarvittavaa osaamista ja parantaa digitaalisen yhteiskunnan kestävyyttä sekä sietokykyä kybertoimintaympäristön lieveilmiöitä vastaan.

Kehittämisohjelma pureutuu ensin neljään ekosysteemin kasvattamisen näkökulmasta keskeiseen pääteemaan. Nämä neljä teemaa ovat: **huippuluokan osaaminen**, **kiinteä yhteistyö**, **vahva kotimainen kyberturvateollisuus** ja **tehokkaat kansalliset kyberturvakyvykkyydet**. Kehittämisohjelman tulevien päivityskierroksien yhteydessä voidaan ottaa mukaan myös uusia teemoja.

Kuva 2: Suomalaisen kyberturvallisuuden ekosysteemi

3 Huippuluokan osaaminen

Vahva kansallinen kyberturvallisuus edellyttää tarvittavaa osaamista ja laajaa osallistumista yhteiskunnan kaikilla eri tasoilla. Digitaalisten ratkaisujen ja palveluiden tarjoajien on kyettävä tuottamaan turvallisia palveluita. Kansalaisten on osattava puolestaan käyttää digitaalisen tietoyhteiskunnan tuottamia palveluita turvallisesti ja tunnistettava eri laitteiden, tuotteiden ja palveluiden käyttöön liittyvät riskit. Yhteiskunnan on vastattava omalta osaltaan tähän tarpeeseen luottamuksen kasvattamisen mahdollistamiseksi.

Suomalainen elinkeinoelämä, kyberturvateollisuus ja viranomaiset ovat tuoneet esille kyberturva-osaajien määrän riittämättömyyden nyt ja tulevina vuosina. Kyberturvallisuuden huippuosaajista käydään jatkuvasti kovaa kansainvälistä kilpailua. Kansainväliset osaajat ovat usein edellytys alan yritysten kasvulle, kansainvälistymiselle ja uusille innovaatioille. Huippuosaajat ovat myös vetovoimatekijä, joka houkuttelee muitakin erityisosaajia. Huippuosaajia tarvitaan edistämään suomalaisen kyberturvallisuusteollisuuden ja tutkimuksen menestymistä globaaleilla markkinoilla.

Nykyinen koulutusjärjestelmä ei suoraan tuota tarvittavaa osaamista suomalaiselle kyberturvateollisuudelle, elinkeinoelämälle ja viranomaisille. Tämä johtaa tilanteeseen, jossa eri tahot joutuvat myös kilpailemaan jatkuvasti samoista osaajista, sekä jatkokouluttamaan uutta henkilöstöään merkittävästi työtehtävien aloittamisen yhteydessä. Parhaimman vaikuttavuuden varmistamiseksi kyberturvallisuuden koulutusjärjestelmän tuottamat tutkinto-opinnot tulee suunnitella yhteistyössä eri toimijoiden kanssa ja opintojen sisältöjä tulee päivittää säännöllisesti vastaamaan eri toimijoiden tarpeita. Edelleen kyberturvallisuuden opetuksen pitäisi olla sisällytettynä niissä tutkinto-opinnoissa, joissa luodaan osaamista teknologia-aloille. Tämä edistää turvallisuuden toteuttamista sisäänrakennettuna yhteiskunnan eri infrastruktuureihin, toimintoihin ja palveluihin. Osaamisvajeen paikkaamiseksi ja riittävän laaja-alaisen ja monipuolisen osaamisen varmistamiseksi tulee naisia ja tyttöjä kannustaa ja rohkaista kyberalalle.

Kyberturvallisuuden ammatillisen osaamisen edistämiseksi tarvitaan panostuksia tutkintoon johtavaan koulutukseen sekä muunto-, että täydennyskoulutukseen kyberturvaosaajien kasvattamiseksi julkiselle ja yksityiselle sektorille. Lisäksi yliopisto- ja ammatti-korkeakoulutuksessa tulee lisätä kyberturvallisuuden sivuainekoulutusta erillisenä opintokokonaisuutena, jotta kyberturvallisuusopintoja voidaan tarjota muillekin kuin kyberturvallisuusalan opiskelijoille. Kehitysohjelma kannustaa myös työnantajien ja oppilaitosten yhä tiiviimpään yhteistyöhön esimerkiksi työharjoittelujaksojen lisäämisessä. Tämä helpottaa alan opintojen soveltamista työelämässä sekä edistää varsinaista työelämään siirtymistä.

Kansainvälisesti kilpailukykyisten ja turvallisten kyberturvatuotteiden ja -palveluiden kehittäminen edellyttää, että yrityksillä on käytettävissään kyberturvateknologian ja -prosessien huippuosaajia, jotka hallitsevat syvällisesti alan keskeiset osa-alueet. Kansallisen kyberturvallisuuden huippu-osaamisen kehittäminen edellyttää riittävän osaamiskeskittymän muodostumista. Huippuosaamis-keskittymän muodostaminen edellyttää puolestaan korkeakoulujen välistä tiivistä yhteistyötä kansallisesti ja kansainvälisesti, monitieteellisyyttä ja usean muun eri sidosryhmän yhteistyötä. Kehittämiseen tulee sitouttaa mukaan opetus- ja koulutusalan toimijat (yliopistot, ammattikorkeakoulut, peruskoulut), tutkimuslaitokset, julkishallinto, elinkeinoelämän keskeiset toimijat ja yhteistyöekosysteemit, yhteiskunnan kriittiseen infrastruktuuriin liittyvät toimijat sekä kyberturva-alan yritykset ja toimijat. Lisäksi tulee kannustaa vahvistamaan ja syventämään kansainvälistä yhteistyötä ja luoda tiiviitä suhteita kansainvälisiin huippuosaamiskeskittymiin.

Ehdotetut kehittämistoimenpiteet

Kansalaisten kyberturvataidot hyvälle tasolle
Järjestöjen ja vapaaehtoisten yhteisöjen roolia vahvistetaan kansalaisten kyberturvataitojen kehittämisessä. Järjestöjen rooli määritellään kansalaisten kyberturvallisuuden valistus- ja viestintätyössä ja niiden toimintaa tuetaan tässä tehtävässä.

Kansalaisten tietoisuuden kasvattamista tehostetaan edelleen osana Euroopan kyberturvakuukautta sekä Digi- ja väestötietoviraston koordinoimaa kansallista digiturvaviikkoa, jonka osaksi palautetaan myös kansallinen tietoturvapäivä. Vapaaehtoisuuteen perustuvien kyberturvayhteisöjen toimintaa tuetaan ja osaamista hyödynnetään sekä yleisen että syventävän osaamisen kehittämisessä.

Edelleen järjestöjä tuetaan myös vakavien kyberhyökkäystilanteiden jälkihoitoon liittyvissä valmiuksissa sekä näiden toteutuksessa yhteistyössä viranomaisten kanssa. Tämä edellyttää vastuu- ja toimintamallien päivittämistä, sekä jälkihoitoa tarjoavien toimijoiden osaamisen kasvattamista kyberhyökkäyksien vaikutuksista ja niiden seurauksista.

Edellä olevien lisäksi luodaan viestintäsuunnitelma tarvittavine toimenpiteineen kansalaisten kyberturvallisuustietoisuuden kasvattamiseksi.

Kyberturvallisuuden koulutuksen kehittäminen
Kyberturvallisuuden koulutuksen suunnittelussa huomioidaan sekä elinkeinoelämän,

että julkishallinnon kyberturvallisuuden osaamistarpeet. Varhaiskasvatuksessa luodaan lapsille perusteet ymmärtää, kuinka digitaalisen yhteiskunnan tuotteita ja palveluita käytetään turvallisesti. Kyberturvallisuus sisällytetään myös peruskoulun opetussuunnitelmaan. Yleissivistävässä perusopetuksessa varmistetaan, että nuorilla on riittävät taidot toimia digitaalisessa toimintaympäristössä ja he ymmärtävät kyberturvauhkat sekä osaavat suojautua niiltä.

Lukiokoulutuksessa laajennetaan ja syvennetään näitä taitoja ja luodaan perustaa alan erityisosaamiselle korkea-asteen koulutuksessa. Ammatilliseen koulutukseen tulee soveltuvin osin sisällyttää kyberturva-asiat osaksi alan perusammattitaitoa. Turvallinen toimiminen digitaalisessa ympäristössä ja siihen liittyvä osaaminen tulee integroida opiskeluun ammattialaan soveltuvalla tavalla, opiskeltavasta ja ammatista riippumatta. Ammatillisen ja täydentävän kyberturvaosaamisen kehittämiseksi suunnitellaan osaamispolkuja, joissa hyödynnetään jo olemassa olevia sisältöjä ja luodaan tarvittaessa uusia. Kannustetaan naisia ja tyttöjä kiinnostumaan kyberalasta.

Huippu- ja erityisosaamistarpeet tunnistetaan ja osaamista kehitetään tarpeiden mukaisesti. Yhteisiä kyberturvakoulutuksia järjestetään keskitetysti toimialasta riippumatta. Tuetaan kansainvälisten huippukoulutusten ja -kouluttajien tuomista Suomeen ja luodaan suhteita kansainvälisiin huippuosaamiskeskittymiin. Koulutusten järjestämisessä hyödynnetään mahdollisuuksien mukaan virtuaalitoteutuksia sekä muita kustannustehokkaita ratkaisuja.

4 Kiinteä yhteistyö

Yhdeksi merkittäväksi mahdollisuudeksi on tunnistettu yhteistyön edelleen tiivistäminen erityisesti julkishallinnon sekä elinkeinoelämän välillä. Tämä nähdään merkittävänä tekijänä kyberturvallisuuden ekosysteemin vahvistamisessa. Kansallisen kyberturvakentän toimijoiden yhteistyölle halutaan löytää uusia tapoja ja yhteistyön muotoja. Kyberturvayhteisöjä halutaan aktivoida myös enemmän valtionhallinnon digitaalisten palveluiden kyberturvallisuuden jatkuvaan parantamiseen.

Kyberturvallisuuden harjoitustoimintaa ylläpidetään ja edistetään. Aktiivisella harjoitustoiminnalla on keskeinen merkitys kyberhyökkäyksien torjunnan, hallinnan ja niiden ratkaisemisen kehittämisessä. Yhteistyössä toimiminen Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelman 2020–2023 (Haukka) sekä Digitaalinen turvallisuus 2030 -hankkeen kanssa on keskeistä näiden kyvykkyyksien edistämiseksi.

Kehittämisohjelma kannustaa strategisten kumppanuusmallien lisäämiseen yritysten ja yliopistojen sekä korkeakoulujen välillä. Pitkäjänteisen yhteistyön tulisi mahdollistaa tutkimus- ja kehitystyön kautta uusien tuote- ja palveluinnovaatioiden syntyminen. Tämä edistää kotimaisen kyberturvateollisuuden tuotteiden ja ratkaisujen kaupallistamista.

Aktiivinen kansainvälinen yhteistyö luo osaltaan edellytyksiä kyberturvallisuuden ekosysteemin kasvulle ja turvallisen digitaalisen yhteiskunnan ylläpitämiselle sekä kehittämiselle ja laajemmin Suomen turvallisuuden vahvistamiselle. Kansainvälinen yhteistyö nähdään keskeisenä mahdollisuutena turvallisen Suomi-kuvan edistämiselle ja yhteensopivien kyberturvallisuuden viitekehysten rakentamiselle. Kyberturvallisuuden viitekehysten kansainvälinen yhteensopivuus on usein myös kasvun elinehto. Yhteistyö mahdollistaa kansainvälisen kyberturvallisuustason vertailun, joka tukee turvallisen digitaalisen yhteiskunnan edistämistä ja jatkuvan parantamisen kehityspolkua.

Ehdotetut kehittämistoimenpiteet

Kyberturvallisuuden harjoitustoiminnan yhteistyön vahvistaminen
Tehdään tiivistä yhteistyötä kyberturvallisuuden harjoitustoiminnassa viranomaisten, elinkeinoelämän ja järjestöjen välillä yhteiskunnan toimivuuden kannalta kriittisten arvoketjujen toiminnan turvaamiseksi. Kyberturvallisuuden harjoitustoiminnassa hyödynnetään yhteisiä kyberharjoitusympäristöjä. Varmistetaan harjoitustoiminnan jatkuminen ja näiden poikkihallinnollinen ohjaus. Lisäksi tuetaan EU:n kyberturvallisuuteen ja uhkiin liittyvien harjoitusten järjestämistä.

Kansallisen kyberturvallisuuden tutkimus- ja kehitysyhteistyön edistäminen
Kyberturvallisuuden tutkimus- ja kehitysyhteistyötä koordinoidaan yhteisten tavoitteiden saavuttamiseksi. Kyberturvatutkimuksen kotimaisen ja kansainvälisen rahoituksen saatavuutta edistetään, turvallisuusnäkökohdat huomioiden. Teoreettisten tutkimustuloksien lisäksi tunnistetaan entistä enemmän mahdollisuuksia tulosten kaupallistamiseen ja tuetaan näiden edistämistä. Tutkimustoiminta otetaan osaksi yritysten innovaatio-, tuote- ja palvelukehitysprosesseja sekä kansainvälistä yhteistyötä.

Kyberturvayhteisöä aktivoidaan entistä laajemmin valtionhallinnon digitaalisten palveluiden turvallisuuden varmistamiseen. Yhteisön osaamista voidaan hyödyntää esimerkiksi turvallisen ohjelmistokoodin kehittämisessä ja käynnistämällä soveltuvin osin valtionhallinnon ”Bug Bounty” –ohjelmia, digitaalisten palveluiden turvallisuuden jatkuvaksi parantamiseksi.

Aktiivinen osallistuminen ja vaikuttaminen kansalliseen ja kansainväliseen kyberturvallisuuden yhteistyöhön
Osallistutaan aktiivisesti kansainväliseen kyberturvayhteistyöhön Euroopan unionissa, Euroopan unionin kyberturvallisuusvirastossa (ENISA) ja keskeisissä kansainvälisissä järjestöissä (mm. YK, OECD, ETYJ, ITU-T ja Nato - kumppanuuden puitteissa) sekä bilateraaliyhteistyöhön. Työn tavoitteena on suomalaisen kyberturvaosaamisen tunnettuuden kasvattaminen, yhteisten kyberturvavaatimusten, standardien sekä sertifiointiarviointikriteeristöjen valmistelu, tiedonvaihto ja yhteisen suomalaisen kyberturvaagendan edistäminen osana globaalia toimintaympäristöä. Kyberturvateollisuuden osallistumista edellä mainittujen kansainvälisten yhteistyöryhmien kannan muodostamiseen tuetaan perustamalla teema-aiheisia yhteistyöryhmiä. Lisäksi suomalaisten toimijoiden tulee kyetä tehokkaasti vaikuttamaan kansainvälisiin prosesseihin ja käytäntöihin, joiden kautta Suomen kyberturvallisuutta parannetaan.

Suomen menestymistä kansainvälisellä kyberturvakentällä seurataan kansainvälisiin indekseihin perustuen (ITU: Global Cybersecurity Index (GCI) ja e-Governance Academy: National Cyber Security Index (NCSI).

5 Vahva kotimainen kyberturvateollisuus

Vahva kotimainen kyberturvateollisuus on yksi kansallisen kyberturvallisuuden ekosysteemin keskeisimmistä mahdollistajista. Kyberturvateollisuus luo kyvykkyyksiä digitaalisen tietoyhteiskunnan palveluiden turvaamiselle, taloudelliselle kasvulle, osaamisen kasvattamiselle sekä uusille työpaikoille. Vahvan kotimaisen kyberturvateollisuuden kasvamisen edellytykset ovat riippuvaisia tämän kehittämisohjelman muista pääteemoista. Suomi tarvitsee lisää menestyviä kyberturvallisuustuotteita ja -palveluita, uusia kyberturvayrityksiä, olemassa olevien yrityksien kasvun ja kansainvälistymisen tukea sekä eri toimijoiden välistä yhteistyötä. Vahva kyberturvateollisuus luo myös pohjan kansallisen kyberturvallisuuden ekosysteemin omavaraisuuden tavoittelulle.

Kasvavat kansainväliset kyberturvallisuusmarkkinat ovat Suomelle merkittävä mahdollisuus talouskasvun ja työllisyyden näkökulmasta. Suomen tulee olla kansainvälisesti houkutteleva kyberturvallisuus-, ICT-alan liiketoiminta- ja investointiympäristö. Kansainvälisten yritysten sijoittuminen Suomeen, tutkimus- ja tuotekehityspanostukset Suomessa ja toimiva yhteistyö suomalaisten toimijoiden kanssa ovat keskeinen osa kyberturvallisuusalan ekosysteemin syntyä sekä kansallisen ja kansainvälisen kyberturvallisuusmarkkinan kasvua.

Vahvan kotimaisen kyberturvateollisuuden kehittäminen edellyttää useita teknologisia ja kaupallisia kyvykkyyksiä, joiden edistäminen huomioidaan osana kehittämisohjelmaa. Uusien yritysten perustamisen tukeminen, uuden kotimaisen IPR:n (kuten esim. immateriaalioikeudet teknologioissa sekä ohjelmistotuotteissa) syntyminen, tarvittavan osaamisen synnyttäminen ja tukeminen, erilaisten roolien tunnistaminen sekä hyödyntäminen kansainvälisessä ekosysteemissä ovat tärkeitä osatekijöitä kaupallisten kyvykkyyksien rakentamisessa. Uusista kansallisista innovaatioista, tuotteista ja palveluista on haettava kasvua myös kansainvälisesti.

Vuonna 2021 perustettava EU:n kyberturvallisuuden kompetenssikeskus ja sen yhteyspisteeksi ja verkoston osaksi Suomeen nimettävä kansallinen koordinaatiokeskus tulevat rahoittamaan kyberturvallisuuden tutkimushankkeita ja kyberturvallisuuden kompetenssien kehittämistä, kohderyhmänä erityisesti pk-yritykset. Kansallisella koordinaatiokeskuksella tulee olla kyberturvallisuuden substanssiosaamista, sekä kyky auttaa kokoamaan yhteen tutkimushankkeita ja tukea yrityksiä kehittämään kotimaisia tuotteita ja palveluita, jotka edelleen edistävät kansallisen kyberturvallisuuden ekosysteemin rakentumista sekä vientiä.

Ehdotetut kehittämistoimenpiteet

Kotimaisten kyberturvatuotteiden ja -palveluiden kasvun ja kansainvälistymisen tukeminen
Vahvan kotimaisen kyberteollisuuden kehittäminen vaatii kasvua, kansainvälistymistä sekä investointeja. Laaditaan tämän perustaksi kyberturvallisuusalan kasvustrategia, jolla tuetaan markkinoiden kasvua sekä edistetään Suomeen tehtävien kansainvälisten investointien saatavuutta, jotka luovat pohjaa myös kansallisen ekosysteemin kehittymiselle.

Kotimaisen kyberturvateollisuuden innovaatioita, tuotteita ja ratkaisuita hyödynnetään entistä laajemmin ja rohkeammin. Kehitetään hankintaosaamista kyberturvallisuuden tuotteiden ja palveluiden ostoon. Nähdään kokeilevan kulttuurin mahdollisuudet ja tuetaan kokeiluja sekä näiden kaupallistamista. Yhteensovitetaan edellä mainittuja tavoitteita yhteen Kansallisen julkisten hankintojen strategian 2020 toimenpiteiden kanssa.

Aktivoidaan Suomen ulkomaanedustustoja ja erityisesti niiden yhteydessä toimivaa Business Finland -verkostoa entistä enemmän kansainväliseen yhteistyöhön suomalaisen kyberturvaosaamisen tunnettuuden edistämiseksi. Kehitetään kansallista tiedonvaihtoa, jotta Suomen kyberturvaetuja ja edunvalvontaa voidaan ajaa hajautetusti, mutta yhtenä rintamana ja yhtenäisellä viestillä eteenpäin.

Edistetään tuotteiden ja palveluiden tuotteistamista ja konseptointia kansainvälisen markkinan näkökulmasta. Hyödynnetään Suomen vahvuuksia kansainvälistymisessä ja markkinoinnissa. Tuetaan myös Suomeen tehtävien kansainvälisten investointien saatavuutta, mikä luo pohjaa kansallisen ekosysteemin kehittymiselle.

Uusien kyberturvayritysten perustamisen edistäminen
Vahva kotimainen kyberturvateollisuus vaatii toteutuakseen eri elinkaaren vaiheissa olevia kyberturvayrityksiä. Jotta tämä olisi mahdollista, tulee eri elinkaaren vaiheissa olevien kyberturvayritysten kehittymistä tukea sekä niiden syntyä ja kasvua mahdollistaa. Yritykset tarvitsevat kyberturvateollisuudelle relevanttien kotimaisten rahoitusinstrumenttien sekä pääomien saatavuuden parantamista mukaan lukien mahdolliset valtion rahoitus- ja omistusosuudet.

Vahvistetaan erityisesti pk-yritysten kyberturvallisuusosaamisen tukirakenteita vuonna 2021 valittavien EU-rahoitteisten kansallisten keskittymien ja verkostojen avulla. Tässä työssä hyödynnetään EU:n kompetenssikeskuksen ja kansallisen koordinaatiokeskuksen toimintaa kyberturvayritysten perustamisen edistämisessä perustamalla kyberturvallisuuden kasvu- ja osaamiskeskus kansallisen koordinaatiokeskuksen yhteyteen. Jatketaan ja edelleen tiivistetään yhteistyötä mm. työ- ja elinkeinoministeriön,

Business Finlandin, Kyberalan (FISC) sekä muiden tarvittavien yhteistyötahojen kanssa ja käynnistetään uusia kokeiluja tämän yhteistoiminnan edelleen tehostamiseksi.

6 Tehokkaat kansalliset kyberturvakyvykkyydet

Kansalliset kyberturvakyvykkyydet luovat pohjaa koko yhteiskunnan toiminnalle. Kansalliset kyberkyvykkyydet kattavat myös ne menettelyt, joilla tarvittava kyberturvallisuuden taso ja toimintaedellytykset varmistetaan. Edelleen kyberturvakyvykkyydet edistävät suvereniteettiamme kybertoimintaympäristössä sekä kansalaisten luottamusta digitaalisen yhteiskunnan toimintaan kaikissa yhteiskunnallisissa olosuhteissa. Kansallisia kyberturvakyvykkyyksiä kehitettäessä on huomioitava eri sektoreiden ja toimintojen keskinäisriippuvuudet niin kansallisella kuin kansainvälisellä tasolla sekä kansalaisten riippuvuus keskitetyistä digitaalisen yhteiskunnan palveluista. Digitaalisessa toimintaympäristössä on ensiarvoisen tärkeää, että salassa pidettävien ja henkilötietojen eheys sekä luottamuksellisuus säilyvät.

Osana kyberturvakyvykkyyksiä arvioidaan nykyisiä viranomaisten toimintaedellytyksiä tarvittavan kansallisen kyberturvatason varmistamisessa jatkuvasti kehittyvässä kybertoimintaympäristössä, tunnistaen samalla jatkokehitystarpeet.

Osana kehittämisohjelmaa laaditaan ja käynnistetään toimenpideohjelma, jonka avulla Suomi voi hakea EU:n salaustuotteiden sertifiointeja hyväksyvän AQUA-maan (Appropriately Qualified Authority) asemaa viimeistään vuonna 2027. AQUA-statuksen saavuttaminen edistäisi merkittävästi kansallisia salauskyvykkyyksiä, edesauttaisi suomalaisten, korkealaatuisia salaustuotteita kehittävien yritysten pääsyä kansainvälisille markkinoille ja lisäisi Suomen turvallisuusviranomaisiin kohdistuvaa kansainvälistä luottamusta.

Ehdotetut kehittämistoimenpiteet

Jatkokehitetään poikkihallinnollisesti viranomaisten varautumista kyberhäiriötilanteisiin
Arvioidaan viranomaisten toimintaedellytykset kansallisen kyberturvallisuuden varmistamisessa, sekä nopeasti kehittyvissä yhteiskunnan kyberturvallisuutta uhkaavissa tilanteissa ottaen huomioon kansallisen ja kansainvälisen uhkaympäristön jatkuva kehittyminen. Arvioinnissa huomioidaan riskit sekä laaja-alaisesti käytössä olevat kansalliset ja EU:n riskienhallintakeinot ja kyvykkyydet sekä tunnistetaan tarvittavat kehittämistoimet.

Kehitetään kansallisten verkkopalveluiden sisäänrakennettua turvallisuutta

Kehitetään edelleen kyberturvallisuuden kontrollipalveluita koko yhteiskunnan käyttöön osana .fi-domain -nimen käytön sisäänrakennettuja turvallisuusominaisuuksia. Tällaisia sisäänrakennettuja turvallisuusominaisuuksia on otettu jo käyttöön, mutta niitä kehitetään edelleen vastaamaan muuttuvaa uhkatilannetta.

Harmonisoidaan turvallisuusvaatimuksia ja parannetaan havainnointikykyä
Harmonisoidaan huoltovarmuuskriittisten sektoreiden ja -yritysten kyberturvavaatimuksia yhteisen turvallisuustason määrittelemiseksi, jotta eri sektoreiden keskinäisriippuvuuksista johtuvia kyberturvariskejä voidaan pienentää. Tavoitteena on näin kasvattaa yhteiskunnan sietokykyä mahdollisia kyberhyökkäyksiä vastaan. Oleellinen osa kyberturvavaatimusten ja turvallisuustason toteuttamista on valvovien viranomaisten osaamisen ja resurssien turvaaminen.

Tunnistetaan yhteiskunnan rajat ylittävät, huoltovarmuuskriittiset arvoketjut ja kehitetään niiden kyberturvallisuuden tilannekuvaa. Kehitetään operatiivisen, toimialakohtaisen ja valvovien viranomaisten tilannekuvan tuottamiseen liittyviä kyvykkyyksiä kansallisen kyberturvallisuuden tilannekuvan edelleen parantamiseksi.

Jatketaan tiivistä yhteistyötä valvovien viranomaisten, Huoltovarmuuskeskuksen Digitaalinen turvallisuus 2030 -hankkeen ja muiden yllä olevien toimenpiteiden toteuttamiseen liittyvien olennaisten kansallisten ja kansainvälisten toimijoiden kanssa.

Turvataan digitaalisen yhteiskunnan keskeiset tiedot, tietovarannot ja -palvelut
Tunnistetaan yhteiskunnan kannalta kriittiset tietovarannot, -palvelut ja -järjestelmät ja varmistetaan näiden toiminta sekä turvallisuus. Varmistetaan myös uusien, yhteiskunnan toiminnan kannalta kriittisten palveluiden turvallisuus osana niiden kehitystyötä. Näitä tehtäviä edistetään yhteistyössä Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelman 2020–2023 (Haukka) sekä Digitaalinen turvallisuus 2030 -hankkeen kanssa.

Kotimaisen salausteknologian luonti ja AQUA -statuksen saavuttaminen
Parannetaan kansallista salaustuoteperhettä sekä vakiinnutetaan kansallinen kryptostrategiatyö. Rakennetaan AQUA-statuksen saavuttamiseksi vaadittavat kyvykkyydet. Tunnistetaan kansallisesti kriittiset kyberturvayhtiöt ja turvataan niiden kansalliset omistusosuudet. Tuetaan kansallisten, kriittisten toimintaympäristöjen turvaamiseen tarkoitettujen viestintälaitteiden, ohjelmistojen ja palveluiden rakentamista sekä toteuttamista. Edistetään luodun salaustuoteperheen vientiä kansainvälisille markkinoille.

7 Seuranta ja raportointi

Jokaiselle kehittämisohjelman toimeenpanosuunnitelmassa esitetylle kehittämistoimenpiteelle on määritelty toimenpiteen edistymisen ja toteutumisen seurantaa tukevat mittarit. Kehittämistoimenpiteen toteuttamisen yhteydessä kerätään ja raportoidaan määriteltyihin mittareihin liittyvää tietoa säännöllisesti.

Mittareiden toteutumista seurataan osana toimenpiteen toteutusta sekä tämän kehittämisohjelman ohjauksen puitteissa. Kyberturvallisuusjohtaja raportoi kehittämisohjelman edistymisestä liikenne- ja viestintäministeriölle sekä Turvallisuuskomitealle kaksi kertaa vuodessa. Kehittämisohjelman edistymistä raportoidaan sidosryhmille myös laajemmin järjestelmällä seurantatilaisuuksia.

Jotta varmistetaan kehittämisohjelman ajantasaisuus ja kehittämistoimenpiteiden oikea kohdennus, valtion kyberturvallisuusjohtaja koordinoi kehittämisohjelman katselmoinnin vuosittain. Tässä katselmoinnissa huomioidaan muuttunut uhka- tai riskiympäristö, muutokset kansainvälisissä verkostoissa sekä muut kehittämisohjelmaan ja sen toimenpiteisiin vaikuttavat tekijät tai trendit. Tämän arvioinnin jälkeen kehittämisohjelmaa tai sen toimeenpanosuunnitelmaa päivitetään tarvittaessa ja hyväksytetään liikenne- ja viestintäministeriössä sekä Turvallisuuskomiteassa.