INKA - INNNOVATIIVISET KAUPUNGIT 2014–2020

KYBERTURVALLISUUSTEEMAN

TOIMINTASUUNNITELMA

30.8.2013

TIIVISTELMÄ

Innovatiiviset kaupungit 2014–2020 -kyberturvallisuusteeman visiona on luoda Suomesta kansainvälisesti tunnustettu kyberturvallisuuden liiketoiminnan ja osaamisen sekä kyberuhkiin varautumisen maailmanlaajuinen edelläkävijä.

Tavoitteena on kehittää kyberturvallisuusliiketoimintaa, luoda uusia alan yrityksiä ja saada ulkomaisia yrityksiä etabloitumaan Suomeen sekä muodostaa kansallinen kyberturvallisuuden innovaatiokeskittymä.

Kyberturvallisuusteema vahvistaa alan osaamista ja tutkimusta sekä käynnissä olevia ja alkavia kehittämishankkeita, joiden avulla Suomessa mahdollistetaan uusien tuote- ja palveluinnovaatioiden kehittäminen kansalaisille, yrityksille ja julkiselle sektorille. Kyberturvallisuudesta muodostuu yrityksille niiden liiketoiminnan varmistaja ja kilpailuetu sekä lisäksi se on oma kasvava liiketoiminta-alansa.

Kyberturvallisuusteema rakentuu kahden pilarin varaan, jotka ovat kyberliiketoiminta ja kyberosaaminen. Kyberturvallisuuden innovaatiokeskittymä muodostaa Suomeen kansainvälisen huipputason tutkimus- ja koulutusosaamista sekä kansainvälisesti houkuttelevan ja kilpailukykyisen toimintaympäristön kyberturvallisuusalan huippuosaajille ja yrityksille.

Kyberturvallisuuden innovaatiokeskittymä rakentuu eri kaupunkiseutujen toimijoiden ympärille ja yhteistyölle, jossa osapuolet vahvistavat toistensa osaamista. Kyberturvallisuusteeman eri hankkeissa tuotetaan kansainvälisen tason huippututkimuksella ja koulutuksella osaamista, jolla voidaan lisätä uusia liiketoimintamahdollisuuksia ja mahdollistaa Suomen kehittyminen edelläkävijäksi kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa.

Vision saavuttamiseksi on asetettu seuraavia tavoitteita:

1. Suomi saavuttaa kansainvälisellä tasolla maineen kyberturvallisuusliiketoiminnan edelläkävijänä.
2. Suomeen muodostuu kansainvälisen huipputason kyberturvallisuuden innovaatiokeskittymä.
3. Kyberturvallisuuden tutkimus- ja koulutus kytketään entistä vahvemmin yritysten kilpailukykyyn ja kilpailuedun saavuttamiseen sekä sen ylläpitämiseen.
4. Suomeen luodaan kyberturvallisuuden osaamisverkostoja sekä tutkimuksella ja koulutuksella edistetään tieteellisiä läpimurtoja, innovaatioiden syntymistä, teknologista kehitystä, tuottavuuden kasvua ja kansallista hyvinvointia.

Kehittämisessä uudistetaan olemassa olevien toimialojen osaamisperustaa, ja samalla luodaan edellytyksiä uusien kasvu- ja liiketoiminta-alueiden syntymiselle kyberturvallisuuden alueelle.

Kyberturvallisuusteeman 2014–2020 toteuttaminen jakaantuu kahteen vaiheeseen:

Vaiheessa 1 (2014–2017) organisoidaan kansallinen kyberturvallisuustoiminta, koordinoidaan käynnissä olevia kyberturvallisuuden liiketoimintahankkeita ja käynnistetään kyberturvallisuuden uusia liiketoimintahankkeita. Analysoidaan ja kartoitetaan kansallinen kyberturvallisuuden koulutustarjonta sekä luodaan koordinoitu tutkimushankekokonaisuus, jolla tuotetaan kyberturvallisuuden eri osa-alueiden tarvitsemia tutkimustuloksia. Tehdään uusia avauksia tutkimustulosten perusteella. Vahvistetaan uuden yritystoiminnan muodostumista ja kansainvälisten yritysten etabloitumista Suomeen. Muodostetaan kansainvälinen kyberturvallisuuden liiketoiminnan ja osaamisen verkosto ja viedään kyberturvallisuuden kärkituotteita ja -palveluita kansainvälisille markkinoille. Aloitetaan Cyber Science Parkin ja Kankaan kyberturvallisen kaupunkiympäristön rakentaminen.

Vaiheessa 2 (2018–2020) syvennetään ja laajennetaan liiketoimintahankkeita ja tehdään uusia avauksia tutkimustulosten perusteella priorisoidusti kansainvälisille markkinoille. Vahvistetaan edelleen alan uutta yritystoimintaa ja kansainvälisten yritysten sijoittumista Suomeen. Laajennetaan kyberturvallisuuden osaamisvientiä kansainvälisille markkinoille ja laajennetaan ja syvennetään tutkimushankkeita sekä implementoidaan osaamista yrityskenttään. Laajennetaan ja syvennetään kansainvälistä verkostoa ja viedään kyberturvallisuuden kärkituotteita ja -palveluita kansainvälisille markkinoille. Laajennetaan Cyber Science Parkin ja Kankaan kyberturvallisen kaupunkiympäristön toiminta kansainvälisen tason innovaatioympäristöiksi.

1. LÄHTÖKOHDAT JA ISO KUVA

Globaali kybertoimintaympäristö muodostuu monimutkaisesta ja -kerroksisista informaatioverkostoista, joihin kuuluu kansallisia julkishallinnon, yritysmaailman ja turvallisuusviranomaisten kommunikaatioverkkoja sekä teollisuuden ja kriittisen infrastruktuurin valvonta- ja ohjausjärjestelmiä, jotka internetin välityksellä muodostavat maailmanlaajuisen verkoston. Tähän globaaliin verkostoon käyttäjät ovat liittyneet lähes lukemattomien erilaisen älykkäiden päätelaitteiden avulla. Tämän verkoston fyysinen osa muodostuu kiinteistä, langattomista ja mobiileista verkoista sekä satelliittiyhteyksistä.

Kybertoimintaympäristö yhdistää valtioita, yrityksiä ja kansalaisia aivan uudella tavalla. Ajan ja paikan merkitys kommunikaatiossa on muuttunut. Digitaalinen tietoyhteiskunta on merkittävästi lisännyt hyvinvointia, mutta kehityksen kääntöpuolena on riski erilaisista kybertoimintaympäristön uhkista.

Tämä kybertoimintaympäristön kehitys vaikuttaa myös Suomeen. Suomi on yksi kehittyneimmistä digitaalisista tietoyhteiskunnista, jonka toiminnat ovat riippuvaisia erilaisista digitaalisista verkoista ja niiden antamista palveluista. Yhteiskunnan kriittinen infrastruktuuri koostuu erilaisista julkisinten ja yksityisten organisaatioiden verkostoista. Tietoteknisten laitteiden ja järjestelmien toimimattomuus, informaatioinfrastruktuurin luhistuminen tai vakavat kyberhyökkäykset voivat aiheuttaa kielteisiä vaikutuk-

sia julkisiin palveluihin, liike-elämään ja hallintoon ja siten koko yhteiskunnan elintärkeisiin toimintoihin.

Informaatioteknologian vallankumous on kehittänyt Suomea 1990-luvulta alkaen kohti tietoyhteiskuntaa. Muutoksen voimana on ollut kansallinen tietotekniikkaosaaminen ja tehokas telekommunikaatioklusteri. Kansalaisten ja elinkeinoelämän tarpeista lähtevä tiedon monipuolinen jalostaminen ja hyödyntäminen ovat yhteiskunnan tärkeimpiä menestystekijöitä. Tiedosta on tullut yhteiskunnan keskeinen voimavara, jota informaatioteknologian avulla voidaan hyödyntää tehokkaammin kuin koskaan aikaisemmin. Tämän seurauksena yhteiskunta on digitalisoitunut hyvin nopeasti. Erilaiset vuorovaikutteiset sähköiset palvelut ovat saatavissa ajasta ja paikasta riippumatta. Julkishallinto, talous- ja liike-elämä sekä kansalaiset hyötyvät globaalisti verkottuneista palveluista, mutta samalla uusi kybertoimintaympäristön infrastruktuuri sisältää haavoittuvuuksia, jotka voivat aiheuttaa turvallisuusriskejä yhteiskunnan elintärkeille toiminnoille.

Yhteiskunnan turvallisuusstrategian (2010) asettamien tavoitteiden mukaan yhteiskunnan organisaatioiden ja väestön käytössä olevien sähköisten tieto- ja viestintäjärjestelmien tulee olla luotettavia ja turvallisia. Tieto- ja viestintäjärjestelmien varassa olevat kriittiset toiminnot varmistetaan ja viestintäverkkojen tietoturvallisuudesta huolehditaan.

Suomen kyberturvallisuusstrategian (2013) mukaan ”Suomella on pienenä, osaavana ja yhteistyökykyisenä maana erinomaiset edellytykset nousta kyberturvallisuuden kärkimaaksi.” Kyberturvallisuuteen tähtäävän tutkimuksen, kehittämisen ja koulutuksen toteuttaminen eri tasoilla vahvistaa kansallista osaamista ja Suomea tietoyhteiskuntana. Kyberturvallisuuden kehittämisessä panostetaan voimakkaasti kybertoimintaympäristön tutkimukseen, koulutukseen, työllistymiseen ja tuotekehitykseen, jotta Suomi voisi kehittyä yhdeksi kyberturvallisuuden johtavista maista. Strategiseksi tavoitteeksi asetettiin, että ”lisätään panostuksia tutkimukseen, tuotekehitykseen ja koulutukseen sekä toimenpiteitä kyberturvallisuuden osaamisen kehittämiseksi koko yhteiskunnan osalta.”

Suomessa on pula kyberturvallisuusalan ammattilaisista. Tämän perusteella **ICT 2015 -työryhmä** (2013) on tunnistanut Suomen menestymisen kannalta teknologiseen osaamiseen liittyvinä kehityskohteina syvällisen tietojenkäsittelyn osaamisen kehittämisen ja kriittisten avainteknologioiden osaamiskeskittymän luomisen (digitaaliset palvelut ja sisällöt, pelillisyys, tietoturva, mobiliteetti ja big data). Kansainvälisesti kilpailukykyisen ja turvallisen ICT-intensiivisen tuotteen ja palvelun kehittämiseen tarvitaan laajaa osaamista. Onnistuminen edellyttää, että yrityksillä on käytettävissään kyberturvallisuusteknologian huippuosaajien ydintiimi, joka hallitsee syvällisesti alan keskeiset osaalueet.

Kyberturvallisuuden tutkimus ja opetus, alan teknologioiden kehittäminen sekä liiketoimintainnovaatiot ovat keskeisiä tulevaisuuden talouskasvun lähteitä ja kansallisia erottautumistekijöitä. Tutkimus ja koulutus kytkevät entistä vahvemmin tiedonhallin-

nan ja tietointensiivisen osaamisen yritysten kilpailukykyyn ja kilpailuedun saavuttamiseen ja ylläpitämiseen. Vahvistamalla alan tutkimusta ja opetusta edistetään tieteellisiä läpimurtoja, innovaatioiden syntymistä, teknologista kehitystä, tuottavuuden kasvua ja tätä kautta kansallista hyvinvointia.

2. KYBERLIIKETOIMINTAPOTENTIAALI

Globaalin kyberturvallisuusmarkkinan arvioidaan kasvavan vuoden 2011 63,7 miljardin dollarin tasosta yli 120 miljardiin dollariin vuoteen 2018 mennessä, vuosikasvun ollessa yli 11 prosenttia.

Erilaiset kyberhyökkäykset ovat lisääntyneet voimakkaasti viime vuosien aikana. Hyökkäysten määrä on yli kaksinkertaistunut viimeisen kolmen vuoden aikana. Samalla hyökkäysten taloudelliset kustannukset ovat nousseet lähes 40 prosenttia. Kyberrikollisuudesta aiheutuneet taloudelliset tappiot ovat nykyisin jopa lähes 400 miljardia dollaria vuodessa. Ennusteiden mukaan palvelunestohyökkäysten torjuntaan käytettävien ratkaisuiden arvo kasvaa 18,2 prosenttia vuodessa ollen 870 miljoonaa dollaria vuonna 2017.

Euroopalla on erinomaiset tutkimus- ja kehitysvalmiudet, mutta monet maailman johtavista innovatiivisten tieto- ja viestintäteknisten tuotteiden ja palvelujen tarjoajista tulevat EU:n ulkopuolelta. Tämä tilanne edellyttää uusien ja innovatiivisten kyberturvallisuusratkaisuiden ja -palveluiden kehittämistä niin julkishallintoon kuin yksityiselle sektorille.

Kyberturvallisuustuotteiden markkinoiden edistäminen voidaan varmistaa vain, jos kaikki arvoketjun toimijat (laitevalmistajat, ohjelmistokehittäjät, palvelujen tarjoajat) nostavat kyberturvallisuuden riittävän korkealle tasolle. Kyberturvallisuustuotteiden koko arvoketjussa tulisi noudattaa asianmukaisia kyberturvallisuusvaatimuksia.

Teknologiateollisuuden arviot työvoimasta lähivuosille pohjautuvat EU-komission arvioon, jonka mukaan vuonna 2015 ICT-alan töissä on Euroopassa jopa 700 000 tekijän vaje. Kyberturvallisuusalan yritykset hakeutuvat sinne, missä koulutettua työvoimaa on tarjolla. Suomessa on pula kyberturvallisuus alan huippuosaajista. Tämän perusteella ICT 2015 -työryhmä on tunnistanut Suomen menestymisen kannalta teknologiseen osaamiseen liittyvinä kehityskohteina syvällisen tietojenkäsittelyn osaamisen kehittämisen ja kriittisten avainteknologioiden osaamiskeskittymän varmistamisen.

INKA-ohjelman Kyberturvallisuusteemalla tavoitellaan kykyä edesauttaa olemassa olevia yrityksiä laajentamaan ja syventämään liiketoimintaansa kyberturvallisuuden uusille liiketoiminta-alueille alan yritysten, tutkimus- ja koulutuslaitosten sekä muiden toimijoiden yhteistyöllä. Samalla voidaan lisätä suomalaisen yhteiskunnan ja yritysten valmiutta ja kykyä puolustautua kyberhyökkäyksiä vastaan.

Kansainvälisesti tunnustetun, kilpailukykyisen ja vientimahdollisuudet omaavan kyberturvallisuuden ekosysteemin syntyminen Suomeen edellyttää kybertoimintaympäris-

töä säätelevän kansallisen lainsäädännön ajantasaisuutta niin, että liiketoiminnan kehittämiselle on olemassa suotuisat edellytykset. Näin Suomesta kehittyy houkutteleva kyberturvallinen toimintaympäristö, johon kannattaa tehdä investointeja sekä yritysten ja toimintojen sijoituspäätöksiä.

3. TIEKARTTA JA KÄRKITOIMENPITEET

Kyberturvallisuusteeman toteuttaminen rakentuu kahden pilarin varaan, joita ovat kyberliike*toiminta ja kyberosaaminen. Kyberosaaminen muodostuu kahdesta osa-alueesta, joita ovat* alan tutkimus ja koulutus. Tavoitteena on kehittää kyberturvallisuuden innovaatiokeskittymä, jossa Suomeen muodostuu kansainvälisen huipputason tutkimus- ja koulutusosaamista sekä kansainvälisesti houkutteleva ja kilpailukykyinen toimintaympäristö kyberturvallisuusalan huippuosaajille ja yrityksille.

Kyberturvallisuusteeman toteuttaminen jakaantuu kahteen vaiheeseen. Molemmat vaiheet sisältävät liiketoimintaan ja osaamiseen liittyviä toimenpiteitä valituilla toimenpidealueella. Vaiheen 1 (2014–2017) kärkitoimenpiteitä ovat innovaatioverkoston luominen, liiketoimintaedellytysten analysointi, Cyber Science Parkin ja Kankaan kyberturvallisen kaupunkikehitysympäristön rakentaminen sekä startup- ja spinoff-yritysten toimintaedellytysten luonti. Vaiheen 2 (2018–2020) kärkitoimenpiteitä ovat innovaatioverkoston syventäminen ja kansainvälistäminen, liiketoiminnan laajentamien kansainvälisille markkinoille, startup- ja spinoff-yritysten toiminnan vahvistaminen sekä Cyber Science Parkin ja Kankaan kyberkaupunkiympäristön kansainvälistäminen.

Kyberturvallisuusteeman suunnittelussa on tunnistettu viisi toimenpidealuetta, joita ovat:

1. Kyberosaaminen
2. Kybertilannetietoisuus
3. Kybervarautuminen
4. Kyberinfrastruktuuri
5. Kyberturvallisuusratkaisut

3.1 Kyberosaaminen

Kyberosaamisen toimenpidealueeseen kuuluu sellaisia osa-alueita kuten kybertutkimus, kyberkoulutus ja kybereksperimentointi. Näille osa-alueille on suunniteltu seuraavia kehittämiskohteita:

- kyberfoorumin ja asiantuntijaverkoston luominen
- kyberturvallisuuden varhaiskasvatuksen-, perusopetuksen, II asteen koulutuksen, lukiokoulutuksen rakenteet ja mallit
- kyberturvallisuuden ammatillisen koulutuksen rakenteet ja mallit
- kyberturvallisuuden ylemmän ammattikorkeakoulutuksen rakenteet ja mallit
- kyberturvallisuuden maisteri- ja jatkokoulutuksen rakenteet ja mallit
- kyberturvallisuuden aikuiskoulutuksen rakenteet ja mallit
- erilaisten kyberharjoitusten toteuttaminen kansallisesti ja kansainvälisesti
- kansainvälisen tutkimusverkoston muodostaminen
- perus- ja soveltavan tutkimuksen toteuttaminen
- kyberturvallisuuden tohtorikoulutusverkoston perustaminen

3.2 Kybertilannetietoisuus

Kybertilannetietoisuuden toimenpidealueeseen kuuluu sellaisia osa-alueita kuten kybertiedonhankinta, kyberinformaation hallinta sekä kyberturvallisuustiedon ja -tapahtumien hallinta. Näille osa-alueille on suunniteltu seuraavia kehittämiskohteita:

- poikkeamien havaitseminen
- huijausyritysten havaitseminen
- anomaliahavaintojen yhdistäminen, korrelointi/fuusiointi kybertilannekuvan syötteeksi
- kybertilannekuvan esittäminen ja jakaminen
- turvallisuustiedon ja tapahtumien hallintajärjestelmän (SIEM) ja verkkoon tunkeutumisen havaitsemisjärjestelmien (IDS) kehittäminen
- tietoverkon valvontatyökalut

3.3 Kybervarautuminen

Kybervarautumisen toimenpidealueeseen kuuluu sellaisia osa-alueita kuten kyberresilienssi, kyberrobustisuus ja kyberturvallisuuden testaus. Näille osa-alueille on suunniteltu seuraavia kehittämiskohteita:

- riskien ja jatkuvuuden hallinta
- loppukäyttäjän suojaaminen
- kyberturvallisuus kriisinhallintaoperaatioissa
- laitteiden, palveluiden ja järjestelmien testaus
- kyberturvallisuusvaatimukset julkisissa ja yksityisissä hankinnoissa
- vaatimustenmukaisuuden hallinta
- kyberuhkien simulointi ja mallintaminen
- haavoittuvuusanalyysit
- digitaalinen rikostutkinta
- kyberturvallisuus ja inhimillinen tekijä
- turvallinen tietojärjestelmäsuunnittelu
- kehittävien ICT-ratkaisujen turvallisuuden varmistaminen

3.4 Kyberinfrastruktuuri

Kyberinfrastruktuurin toimenpidealueeseen kuuluu sellaisia osa-alueita kuten kriittinen infrastruktuuri, kriittinen informaatioinfrastruktuuri ja SCADA-järjestelmät (Supervisory Control and Data Acquisition). Näille osa-alueille on suunniteltu seuraavia kehittämiskohteita:

- kyberturvallisuuden toteuttaminen sulautetuissa järjestelmissä ja teollisuusautomaatiojärjestelmissä
- tunkeutuminen ja vaikuttaminen sulautetuissa järjestelmissä ja teollisuusautomaatiojärjestelmissä
- kyberturvallisuus ja uudistuva teollisuusympäristö
- kriittisen infrastruktuurin suojaaminen
- kriittisen informaatioinfrastruktuurin suojaaminen
- turvallisen liiketoimintaympäristön luominen
- tietoverkkojen ja -järjestelmien suojaaminen

3.5 Kyberturvallisuusratkaisut

Kyberturvallisuusratkaisuiden toimenpidealueeseen kuuluu sellaisia osa-alueita kuten palvelut, tuotteet, kriisinhallinta sekä turvallisuusprosessit ja toimintatapamallit. Näille osa-alueille on suunniteltu seuraavia kehittämiskohteita:

- kyberturvallisuuden johtaminen ja hallinta
- salausalgoritmien kehittäminen
- kansalaisen kyberturvallisuuspalvelut ja -ratkaisut
- kyberturvallisuusriskien hallinta
- yritysten ja organisaatioiden kyberturvallisuusohjelma
- tietoliikenneratkaisujen turvallisuus
- langattomien verkkojen ja palveluiden suojaaminen
- mobiilipäätelaitteiden turvallisuus
- pilvipalveluiden turvallisuus
- avoin lähdekoodi ja kyberturvallisuus
- kyberkriisinhallinnan työkalut
- digitaalisen rikostutkinnan tuotteet
- kyberturvalliset hyvinvointipalvelut

Kyberturvallisuusteeman tavoitteiden saavuttamiseksi muodostetaan osallistuvien kaupunkien ja eri organisaatioiden yhteistyöverkosto, jonka koordinoimana eri toimenpiteitä toteutetaan. Kyberturvallisuus uutena alana edellyttää alkuvaiheessa toiminnan suunnittelua, yhteisten toimintamallien aikaansaamista ja tehokkaan yhteistyöverkoston luomista.

4. KÄRKITOIMENPITEIDEN KÄYNNISTÄMINEN

1. vaiheen alkaessa käynnistetään seuraavia kärkitoimenpiteitä:

4.1 Yhteistyöverkoston luominen

Toiminnan käynnistysvaiheessa laajennetaan kansallista asiantuntijaverkostoa, jonka avulla voidaan innovoida uusia liiketoimintaideoita ja kehittää alan osaamista. Toiminta organisoidaan usealle kyberturvallisuuden osa-alueelle hallinnollisesta tietoturvasta aina yksittäisiin teknisiin menetelmiin keskittyviin ryhmiin. Toimintaa varten suunnitellaan toteutettavaksi julkaisualusta, jonne eri toimijat voivat tuottaa sisältöä muiden käytettäväksi.

4.2 Kybertoimintaympäristön analyysi

Luodaan kybertoimintaympäristöanalyysejä uhka- ja mahdollisuusnäkökulmista ulottuen yhteiskunnan eri kerroksiin ja elintärkeisiin toimintoihin. Tuloksina eri kansallisten toimijoiden kanssa toteutetuista analyyseistä on yksityiskohtaisia ja konkreettisia toimenpiteitä sisältäviä suunnitelmia, joissa on otettu huomioon eri osapuolien innovaatiotarpeita, tavoitteita ja haasteita sekä rahoitukseen ja markkinointiin liittyviä tukitarpeita ja -ratkaisuja.

4.3 Poikkeamien havaitseminen

Anomalioiden tunnistus ja tuotteiden kaupallistamishankkeessa kehitetään poikkeamien havaitsemista erilaisista tietomassoista ja tuotetaan erilaisia valvontajärjestelmäsovelluksia tietoverkkojen valvontaan ja videokuvien automaattiseen analysointiin. Kehittäminen perustuu usean vuoden tutkimustuloksiin, hankittuun osaamiseen ja toteutettuihin verkkohyökkäysten tunnistamisjärjestelmiin.

4.4 Tietoturvalliset julkiset hankinnat

Turvalliset hankinnat -hankkeessa tuotetaan ja pilotoidaan tietoturvavaatimusten uudelleenkäyttöä julkisissa hankinnoissa. Tavoitteena on sekä parantaa tietoturvavaatimusten laatua julkisissa hankinnoissa että vähentää niiden määrittelyyn kuluvaa työmäärää.

4.5 Kriittisten palveluiden kyberresilienssi

Kriittisten palveluiden kyberresilienssihankkeessa selvitetään miten nykyaikaisessa sairaalahankkeessa tulisi varautua kybersietoisuuden maksimoimiseen sekä laatia ohjeistus sekä toimintamallit kiinteistön koko elinkaaren ajalle. Hankkeen tuloksia voidaan hyödyntää kansallisesti myös muissa vastaavissa hankkeissa.

4.6 Digitaalinen rikostorjunta ja kriisinhallinta

Jatketaan ja laajennetaan digitaalisen ja kyberuhkien rikostorjunnan ja kriisinhallinnan hankkeita, joiden avulla luodaan uusia innovatiivisia työkaluja teknisen rikostutkimuksen ja kriisinhallintaoperaatioiden käyttöön.

4.7 Kriittisen infrastruktuurin suojaaminen

Jatketaan ja syvennetään tutkimus- ja liiketoimintahankkeita, jotka keskittyvät kriittisen infrastruktuurin suojaamiseen kyberhyökkäyksiltä ja tekijäoikeuksien suojaamiseen tietoverkoissa.

4.8 JYVSECTEC-ympäristön kehittäminen

JYVSECTEC-ympäristön avulla pystytään testaamaan järjestelmiin kohdistuvia tietoturvauhkia evaluoimalla hyökkäyksiä ja samalla kehittämään erilaisia suojamekanismeja hyökkäyksiä vastaan eristetyssä ympäristössä. Ympäristössä toteutetaan tuotekehitystä sekä koulutetaan kyberturvallisuutta kolmansille osapuolille yksityisellä ja julkishallinnollisella sektorilla. Jatketaan RGCE (Realistic Global Cyber Environment) -ympäristön kehittämistä, sekä kyberturvallisuustilannekuvan ja sen pohjalta tehtävän johtamisen kehittämistä.

4.9 Kyberturvallisuuskoulutus

Jatketaan kyberturvallisuuden YAMK-, maisteri- ja jatkokoulutuksen kehittämistä laajentamalla ja syventämällä opetustarjontaa ja luomalla kansallinen alan osaamisverkosto tuottamaan huippuopetusta ja vahvistamalla kansallista osaamispääomaa. Kehittämisessä etsitään uusia tapoja toteuttaa koulutusta eri seutukuntien yhteistyönä kehittäen innovatiivisia etäopetusmenetelmiä ja internetin hyödyntämistä opetuksessa.

4.10 Tunkeutumistestaus tietoverkkoihin

Kyberturvallisuuskoulutukseen nivelletään tunkeutumistestaus, jossa kehitetään ja evaluoidaan metodiikkaa arvioida tietoteknisten verkkopohjaisten järjestelmien tietoturvaa sisäsyntyisiä ja ulkoisia uhkia vastaan. Tietoturvahaavoittuvuuksia arvioidaan teknologian, prosessien ja ihmisen näkökulmasta.

4.11 Oppiminen ja yritystoiminta

Kyberturvallisuuden opetukseen liitetään yrityslähtöisiä projekteja, joissa yritysten omia ideoita kerätään opiskelijoiden kehitettäväksi ja opiskelijat etsivät niihin ratkaisuja yhdessä yritysten omien asiantuntijoiden kanssa. Yritys saa uusinta tietoa ja tuoreita ideoita ja opiskelijat tutustuvat alan huippuosaajiin.

4.12 Kyberturvallisuuden ad hoc -johtaminen

Hankkeessa tutkitaan ad hoc -verkkoja kyberturvallisuuden osana, kehitetään ratkaisuja ja rakennetaan ympäristö käytännön kokeille näiden ratkaisujen testaamiseksi. Tällaisia dynaamisia verkkoja tarvitaan esim. katastrofin jälkeisissä tilanteissa.

4.13 Kyberturvallisuusprosessin kehittäminen

Kehittämisessä lähestytään kyberuhkiin varautumista, vaikutusten arviointia ja kyberhyökkäyksestä toipumista niin julkisen tason, yritystason kuin myös yksilötason näkökulmista. Teemoja tarkastellaan laajasti ja luodaan kokonaisvaltaisia ratkaisuja.

4.14. Kankaan kyberturvallinen kaupunkiympäristö

Kehitetään Jyväskylän Kankaan aluetta elävänä tutkimus- ja oppimisympäristönä, jonka monipuolinen verkkoympäristö mahdollistaa kriittisen infrastruktuurin kyberturvallisuuden tutkimuksen sekä tutkimuksen todellisessa yksilöiden ja yritysten hybridikaupungissa. Eri kehittämishankkeiden tavoitteena on mallintaa innovatiivinen ja luova toimintaympäristö, uusia asioita ja asenteita hyväksyvä kulttuuri, teknologian edistyksellinen ja uraauurtava käyttö kaupunkien ja kuntien julkisissa palveluissa. Kehittämisessä kansalaisten osallistuminen ja hyväksyntä luovat kestävän ja kehittyvän perustan tulevaisuuden uudenlaisille palveluille. Yritysten vahvalla osallistumisella taataan palvelujen suorituskyky, tekninen toimivuus, kiinnostavuus, turvallisuus ja laajuus sekä kustannustehokkuus.

4.15 Cyber Science Park

Aloitetaan Cyber Science Parkin rakentamisen suunnittelu Jyväskylään, millä luodaan yrityksille ja muille toimijoille kyberturvallisuuden innovaatioympäristö kehittämisalustana ja liiketoiminnan kasvun mahdollistajana. Cyber Science Park voi toimia uudentyyppisten internetkauppojen kokeiluympäristönä, mobiilisovellusten testikenttänä ja sosiaaliseen mediaan liittyvien kybertodellisuusratkaisujen innovaatioalustana. Tavoitteena on edullisen ja houkuttelevan kyberturvallisen ympäristön avulla varmentaa uusien palvelujen, järjestelmien ja konfiguraatioiden tekninen ja toiminnallinen sekä liiketoimintamallien toimivuus.

4.16 Kyberturvallisuuden strateginen tutkimusohjelma

Osallistutaan DIGILE:n (entinen TIVIT) syyskuun alussa käynnistämään kyberturvallisuuden strategisen tutkimussuunnitelman (SRA) valmisteluun. Tavoitteena on käynnistää teollisuusvetoisia tutkimusohjelmia ja kansainvälisiä hankkeita SRA:n linjausten perusteella.

5. AVAINKUMPPANIT

Avainkumppaneiksi INKA-ohjelman Kyberturvallisuusteeman kehittämisessä on tunnistettu Tampereen ja Oulun kaupunkiseudut. Lisäksi Turun kaupunkiseudulta löytyvä osaaminen (esim. Turun yliopiston kryptografian ja tietoturvallisuuden maisteriohjelma) ja tutkimusinfrastruktuuri täydentävät hyvin muiden kaupunkiseutujen tarjontaa. Edellisten lisäksi myös mm. Hämeenlinnan kaupunkiseutu, Aalto-yliopisto ja Laurea-ammattikorkeakoulu ovat ilmoittaneet halukkuutensa yhteistyöhön.

6. KYBER-SUOMI VUONNA 2020

Suomesta on muodostunut kyberturvallisuusalan liiketoiminnan yksi johtavista maista. Suomeen on luotu kyberturvallisuusalan tutkimusta, koulutusta, tuotekehitystä ja testausta mahdollistavia avoimia innovaatio- ja kehitysympäristöjä. Nämä ympäristöt muodostavat monialaisia kokonaisuuksia ja niillä on vahva yhteys käyttäjiin. Kehitysympäristöjen avulla on aikaansaatu yritysten kasvuedellytykset ja kansainvälisen verkostoitumisen globaaleille markkinoille. Kehitysympäristöt ovat luoneet yrityksille yhteisen toimintaympäristön, jossa he voivat kehittää kyberturvallisuuteen pohjautuvaa liiketoimintaa ja yrittäjyyttä. Kehitysympäristöt tuottavat liiketoiminnan kehittämispalveluita, jotka liittyvät tuotteistukseen, markkinointiin ja kansainvälistymiseen. Ydintoimintaa on tunnistettujen kärkituotteiden ja -toimintamallien edistäminen ja jatkokehittäminen kansainvälisillä markkinoilla. Suomeen on rakennettu yksi maailman turvallisimmista informaatioinfrastruktuureista joka on saanut useita kansainvälisiä suuryrityksiä etabloitumaan Suomeen. Turvallisesta infrastruktuuriosaamisesta on tullut yksi menestystuote kansainvälisillä markkinoilla. Suomesta on tullut kyberturvallisuuden globaalien kehitystrendien kärkimaa maailmassa.

Suomen kansainvälisesti tunnustettu ja arvostettu kyberturvallisuuden innovaatiokeskittymä on tuottanut dynaamisia tieto-, oppimis- ja tutkimusverkostoja ja -ympäristöjä eri puolelle maata. Oppivan ja osaavan Suomen toimintatavat, avoimuus ja luottamus, ulottuvat laajasti kansainväliseen yhteistyöhön. Suomalainen kyberturvallisuuden koulutusosaamisen asiantuntijaverkosto tuottaa monenlaisia asiakaslähtöisiä koulutus- ja kehittämispalveluja kansallisille ja kansainvälisille markkinoille. Suomeen on luotu laaja kansallinen ja kansainvälinen yhteistyöverkosto, jonka avulla täällä järjestetään alan kansainvälisten huippuosaajien vierailuja, seminaareja ja tieteellisiä konferensseja ja on saatu aikaan kiinteä yhteistoiminta tutkija- ja opiskelijavaihtoineen tärkeimpiin alan kansainvälisiin yliopistoihin ja korkeakouluihin. Kiinteä yhteistoiminta kytkee Suomen alan parhaaseen osaamisen maailmalla ja hankittu osaaminen on ankkuroitu Suomeen.

Kyberturvallisuudesta on tullut Suomelle uusi vientisektori huipputuotteineen ja palveluineen, mikä vahvistaa kaupunkiseutujen liiketoimintaa kansallisesti ja kansainvälisesti. Kansallisen yhteistyön avulla on lisätty kaupunkiseutujen kansallisten osaamiskärkien profiloitumista ja vetovoimaisuuden vahvistumista koko Suomessa ja siten kehitetty kansallista hyvinvointia. Kyberturvallinen Suomi on maailmanlaajuisesti tunnistettava brändi.