



Turvallisuuskomitea
Säkerhetskommittén
The Security Committee

SUOMEN KYBERTURVALLISUUS- STRATEGIA 2019

Valtioneuvoston periaatepäätös 3.10.2019



SISÄLLYS

JOHDANTO	4
STRATEGISET LINJAUKSET	5
1. KANSAINVÄLISEN YHTEISTYÖN KEHITTÄMINEN	
– kybertoimintaympäristön rajatonta turvaamista	5
2. KYBERTURVALLISUUDEN JOHTAMISEN, SUUNNITTELUN JA VARAUTUMISEN	
parempi koordinaatio	6
3. KYBERTURVALLISUUDEN OSAAMISEN KEHITTÄMINEN	
– arkiosaaminen ja huipputaitajat kyberturvallisuuden varmistajina	8



JOHDANTO

Suomen kyberturvallisuusstrategiassa 2019 asetetaan keskeisimmät kansalliset tavoitteet kybertoimintaympäristön kehittämiseksi ja siihen liittyvien elintärkeiden toimintojen turvaamiseksi.¹ Strategian tarkoituksena on myös tukea luotettavien digitaalisten palveluiden saatavuuden ja liiketoiminnan kehittämistä. Strategia nojautuu Suomen kyberturvallisuusstrategian 2013 yleisiin periaatteisiin. Suomen tavoite on edelleen olla kansainvälisesti kyberturvallisuuden kärkiosaajien joukossa. Kansallisen kyberturvallisuuden toteutus kytkeytyy Yhteiskunnan turvallisuusstrategiaan (2017) ja siinä kuvattuihin yleisiin varautumisen ja turvallisuuden yhteensovittamisen sekä toimivaltaisen viranomaisen periaatteisiin. Strategia ja sen toimeenpano ovat myös osa EU:n kyberturvallisuusstrategian toimeenpanoa.

Kyberturvallisuusstrategian päivittämistarpeeseen ovat vaikuttaneet toimintaympäristössä tapahtuneet merkittävät muutokset ja kansallisessa toiminnassa havaitut kehittämiskohteet. Digitaalisen toimintaympäristön kehitys tarjoaa uusia merkittäviä mahdollisuuksia, jotka liittyvät esimerkiksi

alustatalouteen, ekosysteemeihin, uusien palveluiden tuotantomalleihin ja päätelaitteiden sekä tietoliikenteen kehittämiseen. Toisaalta toimintaympäristöön kohdistuu paitsi vanhoja riskejä, kuten ihmisen tekemät virheet, myös kehittyviä ja muuttuvia uhkia, jotka voivat vaarantaa yhteiskunnan elintärkeitä toimintoja erityisesti kyberrikollisuuden, vaikoilun, valtiollisen tiedustelun ja erilaisin hybridi-vaikuttamisen keinoin. Suomen kansallisen kyberturvallisuuden tilasta on tehty useita selvityksiä². Niissä tehtyjä ehdotuksia on huomioitu tässä strategiassa ja ne otetaan huomioon myös strategian pohjalta valmisteltavassa kehittämisohjelmassa.

Kyberturvallisuusstrategia 2019 käynnistää kansallisen kyberturvallisuuden kehittämisohjelman valmistelun. Kehittämisohjelman valmistelua tukee uusi johtamisen koordinaatiomalli, jossa huomioidaan julkisen hallinnon ja elinkeinoelämän kyberturvallisuuden suunnittelu ja yhteistyö. Ohjelma parantaa kyberturvallisuuden tilannekuvaa ja liittää suunnittelun selkeämmin muuhun toimintaan, kuten talouden suunnitteluun.

¹ Kyberturvallisuudella ymmärretään tilaa, jossa kybertoimintaympäristöön voidaan luottaa ja sen toiminta on turvattu (Kyberturvallisuuden sanasto 2018). Kybertoimintaympäristö puolestaan voidaan käsittää samana kuin digitaalinen toimintaympäristö, joka kehittyy yhteiskunnan osana ja palveluina nopeasti.

² VTT:n selvityksessä kyberosaamisesta Suomessa (2016) on esitetty 12 toimenpidettä Suomen kyberturvallisuusosaamisen edelleen kehittämiseksi ja vahvistamiseksi. Jyväskylän yliopiston ja Aalto-yliopiston selvityksessä Suomen kyberturvallisuuden nykytilasta (2017) on nostettu esille Suomen kyberturvallisuuden nykytilassa tunnistettuja puutteita ja kehityskohteita luokiteltuna 12 osa-alueeseen. Näiden lisäksi Valtiontalouden tarkastusvirasto on julkaissut tarkastuskertomuksen kybersuojauksen järjestämisestä Suomessa (2017). Kertomuksessa on viisi kannanottoa sekä neljä suositusta kokonaisuuden kehittämiseksi. Oikeusministeriön raportissa Nettiäänestyksen edellytykset Suomessa (2017) selvitettiin nettiäänestyksen toteuttamista. Työryhmä ei suositellut nettiäänestyksen käyttöönottoa, koska tällä hetkellä riskit ovat suuremmat kuin hyödyt. Jyväskylän yliopisto ja Aalto-yliopisto laativat selvityksen kyberturvallisuuden strategisesta johtamisesta Suomessa (2018). Selvityksessä laadittiin toimenpide-ehdotuksia yhteiskunnan ja julkisen hallinnon strategisen kyberturvallisuuden johtamiseen, kybertoimintaympäristön laajojen häiriötilanteiden hallintaan sekä kyberturvallisuuden tilan mittaamiseen.

STRATEGISET LINJAUKSET



KANSAINVÄLISEN YHTEISTYÖN KEHITTÄMINEN – kybertoiminta- ympäristön rajatonta turvaamista

Suomi huolehtii kybertoimintaympäristöstään aktiivisen kansainvälisen ja EU-yhteistyön tukemana.

Kansainvälinen yhteistyö on Suomen kyberturvallisuudelle elintärkeää. Suomen etu on tehdä tiivistä yhteistyötä kansainvälisten toimijoiden kanssa monenvälisesti, alueellisesti ja kahdenvälisesti. Tämä koskee teknistä ja poliittisen tason yhteistyötä sekä vuoropuhelua.

Kansainvälinen yhteistyö nojaa voimassa olevaan kansainväliseen oikeuteen, kansainvälisiin sopimuksiin ja ihmisoikeuksien kunnioittamiseen myös kybertoimintaympäristössä. Suomi haluaa säilyttää universaalin, vapaan ja vakaan internetin ja mahdollistaa sen turvallisen käytön. Suomi ei hyväksy pyrkimystä rajoittaa internetin vapautta ja avoimuutta ja sitä kautta yksilön perusoikeuksia ja -vapauksia. Suomi korostaa kaikessa kyberturvallisuuden yhteistyössä oikeusvaltionäkökohtia, demokratiaa ja läpinäkyvyyttä.

Suomi vaikuttaa kansainväliseen kyberturvallisuusagendaan aktiivisesti Euroopan unionissa ja keskeisissä kansainvälisissä järjestöissä (mm. YK, OECD, ETYJ, EN, Nato-kumppanuuden puitteissa). Tämä on osa kansainvälisen sääntöpohjaisen jär-

jestelmän vahvistamista, mikä on Suomen ulkopolitiikan keskeinen tavoite.

Euroopan unionin päätökset sekä EU:ssa tehtävä yhteistyö luovat selkärangan Suomen kansalliselle kyberturvallisuuspolitiikalle ja sen kehittämiseksi. Suomi on aktiivisesti mukana kehittämässä EU:n kyberturvallisuuteen liittyvää yhteistä ulko- ja turvallisuuspolitiikkaa. Lisäksi EU:n uudistettu kyberturvallisuusstrategia sekä keskeiset lainsäädäntöhankkeet, esimerkiksi EU:n verkko- ja tietoturvadirektiivi (NIS), vaikuttavat vahvasti kyberturvallisuuden kehittämiseen myös kansallisella tasolla.

Kybertoimintaympäristöä suojataan kasvattamalla kynnystä erityyppisiin kyberhyökkäyksiin muun muassa parantamalla kyberhyökkäysten havainnointi- ja attribuutiokykyä sekä kykyä vastatoimiin. Vastatoimet voivat koostua esimerkiksi lainvalvontatoimista, diplomaattisista toimenpiteistä tai aktiivisista kybervastatoimista. Vastatoimien kehittämisessä otetaan huomioon EU:n vahvan kyberpuolustuksen kehittämisen linjaukset. Kyberrikollisuuden torjuntaan osallistutaan EU:n puitteissa oikeus- ja lainvalvontaviranomaisten kansainvälisellä yhteistyöllä sekä osallistumalla kansainvälisen oikeuden ja sopimusten kehittämiseen.



KYBERTURVALLISUUDEN JOHTAMISEN, SUUNNITTELUN JA VARAUTUMISEN parempi koordinaatio

Kansallisen kyberturvallisuuden kokonaistilaa parannetaan kehittämisohjelmalla sekä sen suunnittelua ja seuranta edistävällä yhteistyöllä.

Vuoden 2013 kyberturvallisuusstrategian toimeenpano-ohjelmat ovat tähän mennessä perustuneet vain kehittämiseen sitoutuneiden toimijoiden esityksiin ja toimivaltaisten viranomaisten osittain sektorimaiseen työskentelyyn. Tuloksekas kyberturvallisuuden suunnittelu edellyttää, että sen edellyttämät taloudelliset voimavarat ja yhteistointiminta huomioidaan riittävällä tarkkuudella kullakin hallinnonalalla. Tätä parantaa hallituskausiensa yli ulottuva kyberturvallisuuden kehittämisohjelma, joka korvaa aikaisemman toimeenpano-ohjelman. Ohjelma konkretisoi kyberturvallisuuden kansallisia linjauksia sekä selkeyttää kyberturvallisuuden hankkeiden, tutkimuksen ja kehittämisohjelmien kokonaiskuva.

Kyberturvallisuuden kansallista kehittämistä koordinoimaan perustetaan liikenne- ja viestintäministeriöön kyberturvallisuusjohtajan tehtävä.

Kyberturvallisuusjohtajan rooli on kyberturvallisuuden kehittämistä, suunnittelua ja varautumista yhteiskunnallisesti yhteensovittava. Tehtävän

perustaminen ei muuta ministeriöiden ja toimivaltaisten viranomaisten kyberturvallisuuteen liittyviä vastuita ja toimivaltuuksia. Kyberturvallisuusjohtaja toimii myös valtioneuvoston neuvonantajana kyberturvallisuuteen liittyvissä asioissa. Hänen johdolla laaditaan ministeriöiden, Turvallisuuskomitean ja kyberturvallisuustoimijoiden asiantuntevasta hyödyntäen kyberturvallisuuden kokonaiskuva ja kehittämisohjelma.

Kyberturvallisuuden kehittämisohjelmaa laadittaessa huolehditaan siitä, että sen valmisteluun osallistuvat kyberturvallisuusteollisuuden, kybertutkimuslaitosten sekä julkisen sektorin tärkeitä palveluista vastaavien avainorganisaatioiden edustajat. Tämän verkostorakenteen tavoitteena on tiivistää julkisen hallinnon ja elinkeinoelämän kyberturvallisuuden yhteistyötä.

Kybertoimintaympäristöön kohdistuvien häiriötilanteiden johtamista ja yhteistyötä operatiivisella tasolla kehitetään kyberturvallisuustoimijoiden kesken. Häiriötilanteiden hallinnassa tukeudutaan yleiseen häiriötilanteiden hallintamalliin ja hyödynnetään tarvittaessa valmiuspäällikkökokousta.

Kyberturvallisuuden varautuminen edellyttää yhteiskunnan eri toimijoiden, julkishallinnon ja elinkeinoelämän välistä yhteistyötä ja osaamisen

vahvistamista eri sektoreilla. Digitaalisen toimintaympäristön keskinäisriippuvuudet edellyttävät kyberturvallisuuden huomioivaa kokonaisarkkitehtuuria. Toiminnan jatkuvuus ja häiriötilanteisiin varautuminen edellyttävät hankinta- ja kilpailuttamisosaamista, sopimusvelvoitteiden toteutumisen arviointia sekä kokonaisvaltaista toimittajaverkoston ja toimitusketjujen hallintaa.

Muita strategisia toimenpiteitä osa-alueen kehittämiseksi:

- Yhteiskunnan elintärkeille toiminnoille välttämättömät tietovarannot, digitaaliset palvelut ja infrastruktuuri määritetään. Näihin liittyviin toimintoihin ja palveluketjuihin asetetaan kansallisen toiminnan jatkuvuuden hallinnan edellyttämät tavoitetasot.
- Kansallisen turvallisuuden edellyttämää ja standardien mukaista vaatimustenhallintaa parannetaan ja yhtenäistetään turvallisuuskriittisissä palveluissa. Kriittisiin toimintoihin liittyvien tuotteiden ja kokonaisten ratkaisuympäristöjen toteutuksen todentamista, testausta, arviointia ja käyttösuosituksia kehitetään vaatimusten toteutumisen varmistamiseksi.
- Viranomaisten kyberturvallisuusyhteistyötä kehitetään uuden tiedustelu- ja muun toimialaa koskevan lainsäädännön osalta kehittämissuunnitelmassa. Keskeisiä kehittämisen osa-alueita ovat kyberpuolustus ja kansallista turvallisuutta vaarantavien kyberuhkien torjunta. Lisäksi kyberrikollisuuden torjunnan mahdollistavaa lainsäädäntöä kehitetään siten, että lainsäädäntö mahdollistaa tehokkaan kyberrikosten ennalta estämisen ja tutkimisen.
- Kyberturvallisuuskeskuksen kykyä 24/7 tilannekuvan kokoamisessa ja yhteistyötä viranomais- ja elinkeinoelämän välillä kehitetään edelleen. Tämä edistää Suomen kykyä tunnistaa tietoturva-uhkia ja varoittaa niistä sekä parantaa elinkeinoelämän ja julkishallinnon mahdollisuuksia varautua tietoturva-uhkiin.
- Turvallisuusviranomaisten ja elinkeinoelämän kriittisten toimijoiden digitaalisten palvelujen käyttö ja kehittäminen turvataan kaupallisia palveluja hyödyntävillä ja niitä täydentävillä erityissuojatuilla ratkaisuilla voimassa olevan lainsäädännön mukaisesti.
- Yhteiskunnan elintärkeisiin toimintoihin liittyvien yritysten kriittisten palvelujen tuottamista ja jatkuvuuden hallintaa tuetaan. Tehtävien tavoitetaso kuvaaminen ja viranomaisten tarjoamien tukimekanismien kehittäminen selkiyttävät yritysten asemaa. Vastuuviranomaisille asetetaan selkeät tavoitteet kyberturvallisuuden kehittämiseksi. Viranomaiset voivat edistää kyberturvallisuustavoitteiden toteutumista muun muassa sisällyttämällä niitä kaupallisiin sopimuksiin, ja tärkeimmiltä osin myös lainsäädäntöä on tarpeen mukaan täsmennettävä.



Digitaalisen toimintaympäristön keskinäisriippuvuudet edellyttävät kyberturvallisuuden huomioivaa kokonaisarkkitehtuuria.



KYBERTURVALLISUUDEN OSAAMISEN KEHITTÄMINEN – arkiosaaminen ja huippu- taitajat kyberturvallisuuden varmistajina

Kansallinen kyberturvallisuuden osaaminen varmistetaan tunnistamalla osaamistarve sekä vahvistamalla koulutusta ja tutkimusta.

Suomalainen yhteiskunta tarvitsee kyberturvallisuuden osaamista sekä julkisessa hallinnossa että elinkeinoelämässä. Kansallinen kyberturvallisuus rakennetaan viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyönä, ja jokainen voi osaltaan vaikuttaa yhteiseen kyberturvallisuuteemme. Jokainen yksilö on siten tärkeä kyberturvallisuustoimija, joka omilla arjen kyberturvallisuutta parantavilla teoilla voi vaikuttaa omaan ja muiden kyberturvallisuuteen. Kansallisesti on varmistettava, että jokaisella on riittävät valmiudet toimia turvallisesti digitaalisessa toimintaympäristössä.

Viranomaiset ja yritykset tarvitsevat erittäin monipuolista osaamista niin työntekijöiden kuin ali-hankkijoidensa piirissä hallitakseen kyberturvallisuutta koskevia riskejä. Kansallisella tasolla on varmistettava, että yrityksillä on sekä huippuosaajia että muuta osaavaa henkilöstöä riittävästi saatavilla. Osaamisen kehittäminen korostuu myös elinkeinoelämän ja tutkimuksen välisessä yhteistyössä. Tiiviillä yhteistyöllä, vaihtamalla tietoja asiakas-tarpeista ja kehittämällä palvelunkehitystä voidaan

luoda merkittävää uutta osaamista jo pelkästään kansallisilla sisämarkkinoilla.

Osaamiskysymyksen ja kilpailukyvyn kannalta on tärkeää löytää uusia keinoja, joilla kansalliset yritykset saisivat pidettyä huippuosaajansa kansainvälisen kilpailun kasvaessa. Suomen kilpailukyvyn kannalta olisi myös olennaista, että kansainväliset tietoturvastandardit tukevat tuotteita, joiden valmistuksessa suomalaisilla yrityksillä on vahvuuksia. On tärkeää jatkaa aktiivista osallistumista standardintyöhön ja valmistaa tuotteita, joihin turvallisuus on sisäänrakennettua. Näin voidaan samalla parantaa näillä aloilla vahvojen kansallisten yritystemme mahdollisuuksia menestyä kansainvälisessä kilpailussa.

Yhteiskunnan kyberturvallisuuden ja elinkeinoelämän näkökulmasta on keskeistä, kuinka kyberturvallisuus saadaan tärkeäksi osaksi myös muiden kuin kyberturvallisuustuotteita, -palveluita ja ratkaisuja tuottavien yritysten toimintaa. Yhä merkittävämmässä roolissa ovat tulevaisuudessa ne yritykset, joiden varsinainen liiketoiminta on kyberturvallisuusalan ulkopuolella mutta joiden toimintaan kyberturvallisuus ja siihen liittyvät häiriöt vaikuttavat merkittävästi. Tällaisia aloja on hahmotettu erityisesti verkko- ja tietoturvaa koskevissa lainsäädäntöhankkeissa, joissa tällai-



Kansallinen kyberturvallisuus rakennetaan viranomaisten, elinkeinoelämän, järjestöjen ja kansalaisten yhteistyönä, ja jokainen voi osaltaan vaikuttaa yhteiseen kyberturvallisuuteemme.

siksi aloiksi katsottiin muun muassa tietoliikenne, energiantuotanto ja -jakelu, finanssi- ja vakuutusala ja terveydenhuolto.

Kyberturvallisuuden kehittäminen asettaa julkiselle hallinnolle osaamisvaatimuksia ja yhteistyövelvoitteita. Kriittisistä toiminnoista vastaavien viranomaisten kyberturvallisuuden ohjaus-, tuki- ja valvontavastuita sekä näiden edellyttämiä resursseja ja keinovalikoimaa parannetaan kaikilla hallinnon aloilla ja tasoilla.

Muita strategisia toimenpiteitä kyberturvallisuuden osaamisen edistämiseksi:

- Ammatillisen koulutuksen, ammattikorkeakoulujen ja yliopistojen kyber- ja tietoturvallisuuteen, ohjelmisto- ja sovelluskehitykseen sekä tietoverkkoihin ja tietoliikenteeseen liittyviä koulutusohjelmia vahvistetaan.
- Kansallisesti kriittisten kyberosaamisalueiden edellyttämä korkeatasoinen koulutus varmistetaan. Tätä tuetaan sekä kansallisella että kansainvälisellä koulutuksella ja harjoitustoiminnalla.
- Kansallista kyberturvallisuuden tutkimus-, kehitys- ja testaustoimintaa vahvistetaan.

- Valtakunnallista digiturvallisuuden koulutus- ja harjoitusjärjestelmää vahvistetaan osana julkisen hallinnon digitaalisen turvallisuuden koulutusta. Sillä kehitetään julkishallinnon, yritysten ja muiden sidosryhmien työntekijöiden sekä kansalaisten osaamista.
- Julkisen hallinnon, elinkeinoelämän ja yksityisten ihmisten tietoisuutta lisätään uusien palveluiden ja tuotteiden tietoturvasta. Kyberturvallisuus on datatalouden ja tekoälyyn perustuvien sovellusten ehdoton edellytys. Tämä edellyttää valmistajien ja palveluntarjoajien luottamusta toisiinsa sekä kansalaisten luottamusta heille tarjottuihin palveluihin ja tuotteisiin.

SUOMEN KYBERTURVALLISUUS- STRATEGIA 2019



www.turvallisuuskomitea.fi



Turvallisuuskomitea
Säkerhetskommittén
The Security Committee