Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 - 2020

Turvallisuuskomitea
Säkerhetskommittén
The Security Committee

Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 - 2020

Sisällys

Turvallisuuskomitea
Säkerhetskommittén
The Security Committee

www.turvallisuuskomitea.fi

ISBN: 978-951-25-2908-7 (pdf)

Johdanto

Suomen ensimmäinen kansallinen kyberturvallisuusstrategia julkaistiin valtioneuvoston periaatepäätöksenä 24.1.2013. Siinä määriteltiin ne tavoitteet ja toimintalinjat, joiden avulla vastataan kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistetaan sen toimivuus. Strategiassa kuvattiin kyberturvallisuuden visio ja strategiset linjaukset sekä todettiin, että strategisten linjausten toteuttamiseksi ja vision kuvaamaan tavoitetilaan pääsemiseksi laaditaan toimeenpano-ohjelma. Turvallisuuskomitea hyväksyi strategian ensimmäisen toimeenpano-ohjelman 11.3.2014 ja on säännöllisesti arvioinut toimeenpano-ohjelman toteutumista.

Tässä uudessa toimeenpano-ohjelmassa vuosille 2017–2020 tarkastellaan kyberturvallisuuden kehittämistä valtion, maakuntien, kuntien, yritystoiminnan ja kolmannen sektorin muodostamassa palvelukokonaisuudessa, jossa kansalainen, yksilö on asiakkaana. Digitaalisista palveluista ja niiden kyberturvallisuudesta valtaosa tuotetaan elinkeinoelämän toimesta kansallisissa ja kansainvälisissä palvelukokonaisuuksissa ja -verkostoissa.

Kyberturvallisuusstrategian julkaisun jälkeen kyberturvallisuuden toimintaympäristö on muuttunut uusien palvelutuotantomallien, teknologioiden ja niihin kohdistuvien uusien uhkien myötä. Helmikuussa 2017 julkaistun valtioneuvoston selvityksen ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” (jatkossa Suomen kyberturvallisuusselvitys 2017) mukaan viime vuosien kyberuhkien merkittävimmät trendit ovat olleet kiristyshaittaohjelmien kasvu, haavoittuvuuksien hyödyntäminen, laitteistoihin kohdistuvat uhkat sekä liiketoiminnan tuhoamiseen tai henkilötietojen varastamiseen tähtäävät hyökkäykset. Myös huijaukset ja tietojen kalastelut, palvelunestohyökkäykset sekä kohdistetut hyökkäykset ovat edelleen ajankohtaisia uhkia. Eri toimialoista etenkin terveystoimiala, valmistus ja tuotanto, pankki- ja rahoitustoimiala, julkishallinto sekä liikenne ja kuljetus ovat sellaisia kohteita, joihin on eniten kohdistunut kyberhyökkäyksiä. Tulevaisuudessa nähdään todennäköisesti yhä kehittyneempiä kyberhyökkäyksiä ja tietovuotojen kasvua. Verkkoon liitettävien esineiden määrä kasvaa, joten tulevat kyberhyökkääjät saavat valtavasti lisää hyökkäysmahdollisuuksia esineiden internetin kasvun myötä.

Lisäksi Suomen kyberturvallisuusselvityksessä 2017 todettiin, että ”vaikka Suomessa on viime vuosina vahvemmin ymmärretty kybertoimintaympäristöön liittyvien asioiden poliittinen luonne ja poliittisen ymmärryksen tarpeellisuus kyberturvallisuusstrategian vision saavuttamisessa, voi poliittisen sitoutumisen vahvistamista pitää edelleen kehityskohteena. Poliittisessa sitoutumisessa on kyse myös kansallisen tahtotilan (kyberturvallisuusstrategian vision) edistämisestä ja viestimisestä kansainvälisesti.” Selvityksen mukaan myös Suomen kansainvälinen toiminta kyberasioissa vaatii edelleen vahvistamista: ”Suomen on luotava selkeä ”kyber-agenda” eli määritettävä julkisesti tavoitteet, joita Suomi pyrkii kansainvälisessä yhteistoiminnassa edistämään.”

Hallinnonalojen, elinkeinoelämän, akatemian ja järjestöjen antamien arvioiden perusteella, Turvallisuuskomitean sihteeristö laati arvion kyberturvallisuusstrategian toimeenpano-ohjelman toteutumisesta tammikuussa 2016. Arvioinnissa korostui kyberturvallisuuden johtamismallien kehittämisen tarve. Arvion perusteella Turvallisuuskomitea päätti 14.3.2016 päivittää ja luoda kansallisena tahtotilana Suomen Kyberturvallisuusstrategian toimeenpano-ohjelman. Tahtotila osoitetaan johtajuudella ja resurssien uudelleen kohdentamisella.

Vuonna 2014 hyväksytty, kyberturvallisuusstrategian ensimmäinen toimeenpano-ohjelma koostui yhteensä 74 toimenpiteestä, jotka jakaantuivat ministeriöiden ja osin yksittäisten toimijoiden toteutusvastuulle. Arvioinnissa seuraavilla toimenpiteillä tunnistettiin olleen merkittäviä vaikutuksia:

- Hallinnon turvallisuusverkko (TUVE) -hanke ja toimialariippumattomien ICT-tehtävien kehittäminen,
- Kyberturvallisuuskeskuksen perustaminen Viestintävirastoon ja siihen liittyvän CERT-toiminnan kehittäminen,
- Valtion ympärivuorokautisen tietoturvatoiminnan kehittämishanke ja siihen liittyvä havainnointikyvyn parantaminen,
- Jyväskylä Security Technology:n (JYVSECTEC) turvallisuusteknologian kehittämishanke sekä
- Maanpuolustuskoulutusyhdistyksen kyberturvallisuuskurssit.

Digitalisoitumisen ja siinä tarvittavan muutoksen johtamisen, tiedolla johtamisen, keinoälyn, robotisaation sekä esineiden internetin myötä kyberturvallisuuden merkitys on yhä keskeisempää myös yhteiskunnan elintärkeiden toimintojen turvaamisessa kansallisessa ja kansainvälisessä toimintaympäristössä. Toiminnan digitalisaatio on hallitusohjelman läpileikkaava teema, jota toteutetaan useassa eri hankkeessa. Julkisen hallinnon digitalisaation kärkihankkeesta ”Digitalisoidaan julkiset palvelut” toteuttamisesta vastaa valtiovarainministeriön JulkICT-osasto. Kyberturvallisuus nähdään tässä yhteydessä digitalisaation mahdollistajana; se pitää rakentaa toimintaan ja palveluihin sisäänrakennetusti. Tätä toteutetaan kahdella yhdeksästä digitalisoinnin periaatteesta ”rakennamme helppokäyttöisiä ja turvallisia palveluita” sekä ”palvelemme myös häiriötilanteissa”.

Liikenne- ja viestintäministeriön vuonna 2016 julkaiseman tietoturvallisuusstrategian visiona on se, että maailman luotetuin digitaalinen liiketoiminta tulee Suomesta. Suomella nähdään olevan hyvät edellytykset tulla tunnetuksi osaavana, menestyvänä ja luotettavana maana, jossa on turvallista tarttua digitalisaation mukanaan tuomiin mahdollisuuksiin. Talouskasvun luominen ja kiihdyttäminen riippuu siitä, että kehitämme, omaksumme ja kokeilemme uudenlaisia, digitaalisen tiedon hyödyntämiseen perustuvia liiketoiminnan ja ansainnan malleja. Tämän edellytyksenä on arvioitu tarvittavan luottamusta uusiin palveluihin, liiketoimintamalleihin ja markkinatoimijoihin sekä vahvaa otetta tietoturvallisuuden osaamisesta ja markkinoiden kehittämisestä.

Globalisaatiosta ja digitalisoitumisesta johtuen, Suomen turvallisuusympäristö on muuttunut nopeasti. Turvallisuus- ja toimintaympäristön muutosten myötä kansallisen turvallisuuden uhat, kuten vakoiluun ja terrorismiin liittyvät ilmiöt ja hankkeet, tapahtuvat yhä useammin tietoverkoissa. Tämä muutos edellyttää myös kybertoimintaympäristöön ulottuvia viranomaisvaltuuksia. Uuden tilanteen myötä on Suomessakin aloitettu sisäministeriön ja puolustusministeriön toimialoilla tiedustelulainsäädännön valmistelut.

Toimeenpano-ohjelma 2017–2020 on muodostettu valmistelun aikana kerättyjen toimenpide-ehdotusten perusteella. Ehdotuksia on kerätty sekä kohdennetulla pyynnöllä ministeriöille ja virastoille että valmistelun yhteydessä järjestetyissä haastatteluissa ja keskustelutilaisuuksissa tiede- ja tutkimusmaailman, hallinnon ja elinkeinoelämän kanssa. Toimeenpano-ohjelman laadinnassa on otettu huomioon valtioneuvoston periaatepäätöksenä hyväksytyt sekä muut strategia-asiakirjat sekä mahdollisuuksien mukaan työn aikana valmistelussa olleet strategia-asiakirjat, kuten yhteiskunnan turvallisuusstrategian päivitystyö. Toimenpiteet valittiin siten, että ne edistävät vision saavuttamista ja ovat strategisten linjausten mukaisia. Toimenpiteiden valinnassa on painotettu vaikuttavuuden näkökulmaa korostaen kansalaista julkisen hallinnon palveluiden asiakkaana, elintärkeiden toimintojen turvaamista sekä julkisen hallinnon ja elinkeinoelämän, tiede- ja tutkimusmaailman välistä yhteistyötä. Toimeenpano-ohjelma kokoaa julkisen hallinnon sisäiset ja yhdessä elinkeinoelämän sekä järjestöjen kanssa toteutettavat laaja-alaiset ja merkittävät tieto- ja kyberturvallisuutta parantavat hankkeet ja toimenpiteet yhteen ja tuo ne näkyville yhdenmukaisesti jäsennettynä ja vastuutettuina. Toimeenpano-ohjelmaan sisällytettynä hankkeiden ja toimenpiteiden etenemistä on mahdollista säännöllisesti seurata ja mitata, jolloin on mahdollista saada parempi kokonaiskuva kyberturvallisuuden kehittämisen tilanteesta. Mittaamisen keinoja on jatkuvasti kehitettävä erityisesti toimenpiteiden laadun seurannassa. Toimeenpano-ohjelmaan valittujen laajasti vaikuttavien toimenpiteiden lisäksi kyberturvallisuutta parannetaan jatkuvasti myös muilla hallinnonalakohtaisilla toimenpiteillä sekä kyber- ja tietoturvallisuuden ja toiminnan jatkuvuuden hallinnan kehittämiseen liittyvällä työllä.

Toimeenpano-ohjelmaa tarkastellaan ja mitataan vuosittain ja siinä yhteydessä toimenpiteitä voidaan muuttaa, lisätä ja poistaa. Toimeenpano-ohjelman päivittämistä on valmisteltu työryhmässä, jonka puheenjohtajana on toiminut erikoistutkija Pentti Olin Turvallisuuskomitean sihteeristöstä ja jäseninä turvallisuuspäällikkö, dosentti Tuija Kuusisto ja VAHTI-pääsihteeri Kimmo Rousku valtiovarainministeriöstä, apulaisjohtaja Rauli Paananen Viestintävirastosta sekä asiantuntija Nadja Nevaste Turvallisuuskomitean sihteeristöstä.

Toimeenpano-ohjelman 2017–2020 sisältö

Suomen Kyberturvallisuusstrategiassa on määritelty kyberturvallisuuden visio sekä kymmenen strategista linjausta, joiden mukaisesti kansallista kyberturvallisuutta kehitetään. Vision mukaan

- Suomi kykenee suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan.
- Kansalaisilla, viranomaisilla ja yrityksillä on mahdollisuus tehokkaasti hyödyntää turvallista kybertoimintaympäristöä ja sen suojaamiseen syntyvää osaamista sekä kansallisesti että kansainvälisesti.
- Vuonna 2016 Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa.

Vision kolmannen kohdan osalta vuoteen 2016 sidottu tavoite muutetaan pysyväksi: Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa.

Saatavilla olevien kansainvälisten vertailujen ja arvioiden perusteella, Suomi sijoittuu tällä hetkellä kärkikymmenikköön arvioitaessa eri valtioiden kyvykkyyksiä kyberturvallisuuden valmiuden ja toimeenpanon edistymisen alueilla.

Kyberturvallisuusstrategian strategiset linjaukset ovat:

1. Luodaan kansallisen kyberturvallisuuden ja kyberuhkien torjunnan edistämiseksi viranomaisten ja muiden toimijoiden välinen tehokas yhteistoimintamalli.

2. Parannetaan yhteiskunnan elintärkeiden toimintojen turvaamiseen osallistuvien keskeisten toimijoiden kokonaisvaltaista kyberturvallisuuden tilannetietoisuutta ja tilanneymmärrystä.

3. Ylläpidetään ja kehitetään yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta tärkeiden yritysten ja organisaatioiden kykyä havaita ja torjua elintärkeää toimintoa vaarantavat kyberuhkat ja -häiriötilanteet sekä toipua niistä osana elinkeinoelämän jatkuvuuden hallintaa.

4. Huolehditaan, että poliisilla on tehokkaat edellytykset ennalta ehkäistä, paljastaa ja selvittää kybertoimintaympäristöön kohdistuvia ja sitä hyödyntäviä rikoksia.

5. Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään.

6. Vahvistetaan kansallista kyberturvallisuutta osallistumalla aktiivisesti ja tehokkaasti kyberturvallisuuden kannalta keskeisten kansainvälisten organisaatioiden ja yhteistyöfoorumeiden toimintaan.

7. Parannetaan kaikkien yhteiskunnan toimijoiden kyberosaamista ja -ymmärrystä.

8. Kansallisella lainsäädännöllä varmistetaan tehokkaan kyberturvallisuuden toteuttamisen edellytykset.

9. Määritellään viranomaisille ja elinkeinoelämän toimijoille kyberturvallisuutta koskevat tehtävät ja palvelumallit sekä yhteiset perusteet kyberturvallisuuden vaatimusten hallinnalle.

10. Strategian toimeenpanoa valvotaan ja toteumaa seurataan.

Toimeenpano-ohjelma jakaantuu kolmeen kokonaisuuteen, joissa vastataan seuraaviin kysymyksiin:

1) Johtamisella on varmistettu kyberturvallisuuden vision saavuttaminen
Mitä johtamisen ja ohjauksen rakenteita, malleja ja lainsäädäntöä tulisi luoda kyberturvallisuuden vision saavuttamiseksi? Mitä hallinnon ja elinkeinoelämän sekä järjestöjen yhteisiä tilanneymmärryksen keräämisen ja jakamisen malleja tulisi luoda ja kehittää?

2) Yhteiskunnan digitalisoidut elintärkeät toiminnot ovat turvatut
Mitä laaja-alaisesti vaikuttavia hallinnollisia ja teknisiä toimenpiteitä tarvitaan, jotta kybertoimintaympäristöön voidaan luottaa normaalioloissa, normaaliolojen häiriötilanteissa ja poikkeusoloissa?

3) Kansalaisten, elinkeinoelämän ja hallinnon kyberosaaminen edistää digitalisaation kehitystä
Mitä osaamisen kehittämisen kokonaisuuksia tulisi olla saatavilla kansalaisille, elinkeinoelämälle ja hallinnolle? Kuka tarjoaa osaamisen kehittämisen kokonaisuuksia ja tuottaa tutkittua tietoa?

Ohjelman toimenpiteet on kuvattu strategisten linjausten mukaisesti oheisessa matriisissa. Toimenpiteet on lajiteltu tämän ohjelman kolmen kokonaisuuden mukaisesti.

	Toimenpide/ Linjausalue	1	2	3	4	5	6	7	8	9	10
1	Strateginen johtajuus on määritetty	x			x	x	x			x	
2	Valtionhallinnon kyberturvallisuuden johtamisen malli on luotu ja organisoitu	x	x	x							
3	Julkisen hallinnon kyberhäiriötilanteiden operatiivinen hallintamalli on toteutettu ja toiminnassa	x	x	x	x	x				x	
4	Julkisen hallinnon strategiset tieto- ja kyberturvallisuuden linjaukset on vahvistettu	x		x						x	
5	Suomi osallistuu aktiivisesti ja tehokkaasti kyberturvallisuuteen liittyvään kansainväliseen toimintaan				x	x	x				
6	Suomen kyberturvallisuusfoorumi toimii hallinnon, elinkeinoelämän ja akatemian yhteistyöelimenä	x	x				x			x	x
7	Toimeenpano-ohjelman seurantamittaristo on laadittu									x	x
8	Kybertoimintaympäristössä tapahtuvan vaikuttamisen edellytykset on varmistettu					x					
9	Valtiojohdon riittävästä ja oikea-aikaisesta tiedon saannista kansallista turvallisuutta vaarantavien uhkien torjumiseksi on huolehdittu	x	x			x			x		
10	Kyberrikostorjunnan edellytykset on varmistettu				x						
11	Tietoturvallisuuden sekä tietosuojan lainsäädäntö on selkiytetty ja täydennetty sekä EU:n yleisen tietosuojalainsäädännön vaatimukset on toteutettu kansallisessa lainsäädännössä								x		
12	Yhteiskunnan elintärkeille toiminnoille välttämättömät julkisen hallinnon digitaaliset palvelut ja niiden tarvitsema infrastruktuuri on tunnistettu ja hallinnassa			x	x	x	x			x	
13	Maakunta ja sote-uudistuksessa toiminnallisten prosessien jatkuvuus sekä tieto- ja kyberturvallisuus on varmistettu			x						x	

	Toimenpide/ Linjausalue	1	2	3	4	5	6	7	8	9	10
14	Valtioneuvostolla on käytössä valmiuden ja varautumisen johtamiseen liittyvät tiedonsiirron ja -käsittelyn ratkaisut ja palvelut kaikissa turvallisuustilanteissa		x	x	x	x	x				
15	Kriittisten perusrekisterien ja tietovarantojen eheys ja saatavuus on hallittu kaikissa turvallisuustilanteissa			x							
16	Sähköenergian toimitusvarmuuden riittävä taso ja yhteiskunnan kannalta keskeisten kohteiden sähkönjakelu on varmistettu			x							
17	Huoltovarmuuskriittisten yritysten kyberturvallisuus on edistynyt			x							
18	Vaalien toteuttamisen tieto- ja kyberturvallisuus on selvitetty								x	x	
19	Verottamiseen ja talousarvioesitysten valmisteluun sekä valtion maksuvalmiuden hallintaan ja maksuliikenteeseen liittyvien järjestelmien ja prosessien varautumista ja häiriöiden hallintaa on parannettu		x	x						x	
20	Kansallinen kevyt kyberturvallisuusarviointi, jonka avulla organisaatiot voivat huolehtia minimitason saavuttamisesta turvallisuuden osalta, on laadittu							x		x	
21	Tietoturvallinen kasvuympäristö digitaaliselle liiketoiminnalle on luotu	x	x	x	x		x	x	x	x	
22	Koulutus- ja harjoitustoiminta on suunniteltu ja toteutettu	x	x				x	x			

I Johtamisella on varmistettu kyberturvallisuuden vision saavuttaminen

Suomen kyberturvallisuusselvityksessä 2017 todetaan: ”Kyberturvallisuuden kokonaisvaltainen, koko yhteiskunnan eri kybertoiminnot kattava ja yhdistävä, johtajuuden epämääräisyys ja puuttuminen nousivat tutkimuksessa vahvasti esille. Johtopäätöksenä voi todeta, että strategisen johtajuuden selkeyttäminen ja vahvistaminen ovat hyvin oleellinen asia Suomen kyberturvallisuuden vision saavuttamisen varmistamisessa.”

1) Strateginen johtajuus on määritetty

Liittyy strategiseen linjaukseen: 1,4,5,6,9

Vastuutaho: Turvallisuuskomitean sihteeristö, valtioneuvoston kansia, valtiovarainministeriö sekä muut tarvittavat toimijat

Toteutetaan hanke, jossa määritellään kyberturvallisuuden strateginen johtajuus ja sen selkiyttäminen ja vahvistaminen. Hankkeessa otetaan huomioon myös kriisinjohtamismallin toteutuminen kybertoimintaympäristön häiriötilanteissa.

2) Valtionhallinnon kyberturvallisuuden johtamisen malli on luotu ja organisoitu

Vastuutaho: Valtiovarainministeriö

Liittyy strategiseen linjaukseen: 1,2,3

Valtiovarainministeriö luo valtionhallinnon kyberturvallisuuden johtamiselle uuden kehikon osana valtiovarainministeriön strategian VM 2020 toimeenpanoa.

3) Julkisen hallinnon kyberhäiriötilanteiden operatiivinen hallintamalli on toteutettu ja toiminnassa

Liittyy strategiseen linjaukseen: 1,2,3,4,5,9

Vastuutaho: Valtiovarainministeriö, liikenne- ja viestintäministeriö, Valtion tieto- ja viestintätekniikkakeskus Valtori

Suomen kyberturvallisuusselvityksessä 2017 todetaan: ”Suomessa on viime vuosien aikana kehitetty kyberturvallisuuden tilannekuvan muodostamista sekä eri toimijoiden keräämien tietojenvaihtoa, mutta tietojenvaihdon sekä havaintokyvyn parantaminen on edelleen Suomessa kehitettävä asia kyberturvallisuudessa. On myös tärkeää, että esimerkiksi tietoisuutta havaituista haavoittuvuuksista jaetaan aktiivisesti eri toimijoiden välillä, ja mahdollisista tietomurroista ilmoitetaan luottamuksellisella tavalla, jotta vastaavien tietomurtojen estäminen muualla yhteiskunnassa mahdollistuu.”

Valtiovarainministeriön johdolla Valtori yhdessä liikenne- ja viestintäministeriön, Viestintäviraston ja muiden toimijoiden kanssa suunnittelee edelleen kehitetyn poikkihallinnollisen kyberhäiriötilanteiden operatiivisen hallintamallin ja havainnointikyvyn (VIRT), joka sisältää kuvauksen tietovirroista ja toimintaprosesseista julkisen hallinnon ja elinkeinoelämän välillä merkittävissä julkisen hallinnon kyberhäiriö-, ja tietoturvapoikkeamatilanteissa. Toteutetaan tutkimushankkeena kybertilannekuvan ja analysointikyvykkyyden kehittäminen.

Niiltä osin, kuin toimijat eivät kuulu NIS- direktiivin ilmoitusvelvollisten piiriin, valtiovarainministeriö varmistaa, että ministeriöt, hallinnonalat ja palvelukeskukset sekä maakunta- ja kuntatoimijat ja niiden omistamat yritykset ilmoittavat Viestintävirastolle julkisen hallinnon toimintaa ja palveluita koskevista kyberhäiriötilanteista sekä tietoturvapoikkeamista. Ilmoitusvelvollisuus on otettava huomioon alihankkijoiden kanssa tehtävissä sopimuksissa. Valtiovarainministeriö ohjeistaa ilmoitusvelvollisuuden toteuttamisesta tarkemmin. Lisäksi toteutetaan sopimuksiin perustuva varautuminen yksityissektorin toimijoiden kanssa.

4) Julkisen hallinnon strategiset tieto- ja kyberturvallisuuden linjaukset on vahvistettu

Liittyy strategiseen linjaukseen:1,3,9

Vastuutaho: Valtiovarainministeriö

Valtiovarainministeriö asettaa toimikaudelle 2017–2019 julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI). Se käsittelee ja yhteen sovittaa julkisen hallinnon keskeiset strategiset tieto- ja kyberturvallisuuden linjaukset. Lisäksi valtiovarainministeriö arvioi nykyisen tietoturvallisuuslainsäädännön kehittämistarpeet ja – mahdollisuudet. VAHTIn toiminnasta raportoidaan vuosittain.

5) Suomi osallistuu aktiivisesti ja tehokkaasti kyberturvallisuuteen liittyvään kansainväliseen toimintaan

Liittyy strategiseen linjaukseen: 4,5,6

Vastuutaho: Ulkoasiainministeriö, ja muut ministeriöt toimialoillaan

Suomi vaikuttaa aktiivisesti kansainväliseen kybertoimintaympäristöön liittyvien kysymysten käsittelyyn niin EU:ssa, YK:ssa, Etyjissä, NATO:ssa, OECD:ssä, EN:ssa ja muissa keskeisissä järjestöissä sekä kahdenvälisesti. Ulkoasiainministeriöllä on keskeinen rooli ulko- ja turvallisuuspoliittisten aspektien tunnistamisessa kybertoimintaympäristön kysymyksissä.

Ulkoasiainministeriö osaltaan koordinoi Suomen kannanmuodostusta kybertoimintaympäristön kysymyksissä kansainvälisillä foorumeilla. Ulkoasiainministeriö osaltaan edesauttaa suomalaisten kyberturvallisuusyritysten kansainvälisiä toimintamahdollisuuksia osana viennin ja kansainvälistymisen edistämistä.

6) Suomen kyberturvallisuusfoorumi toimii hallinnon, elinkeinoelämän ja akatemian yhteistyöelimenä

Liittyy strategiseen linjaukseen: 1,2,6,9,10

Vastuutaho: Turvallisuuskomitean sihteeristö

Suomen kyberturvallisuusfoorumi toimii yhteistyön ja tiedonvälityksen parantamista varten tiede- ja tutkimusmaailman, hallinnon, yritysten ja järjestöjen kesken. Foorumi seuraa kyberturvallisuusstrategian ja tämän toimeenpano-ohjelman toteutumista ja arvioi niiden ajantasaisuutta. Foorumin tilaisuuksiin kutsutaan Turvallisuuskomitean jäsenten lisäksi kyberturvallisuuden alan professoreita, toimitusjohtajia ja järjestöjen johtajia. Foorumille selostetaan toimeenpano-ohjelman edistymistä ja Suomen kyberturvallisuuden tilannetta sekä tutkimushankkeiden tuloksia.

7) Toimeenpano-ohjelman seurantamittaristo on laadittu

Liittyy strategiseen linjaukseen: 9,10

Vastuutaho: Turvallisuuskomitean sihteeristö ja valtiovarainministeriö

Kyberturvallisuuden toimeenpanoa seurataan tällä hetkellä olemassa olevin mittarein. Turvallisuuskomitean sihteeristön ja valtiovarainministeriön johdolla toteutetaan tutkimushanke ja laaditaan Suomen kyberturvallisuuden tilaa ja tämän toimeenpano-ohjelman tavoitteiden seurantaa varten päivitetty kypsyysmalli ja mittaristo. Kypsyysmallin ja mittariston avulla toteutetaan säännöllinen raportointi toimeenpano-ohjelman tilanteesta Turvallisuuskomitealle, valtioneuvostolle, Kyberturvallisuusfoorumille sekä muille sidosryhmille. Tätä toimeenpano-ohjelmaa tarkastellaan vuosittain ja siinä yhteydessä toimenpiteitä voidaan muuttaa, lisätä ja poistaa.

8) Kybertoimintaympäristössä tapahtuvan vaikuttamisen edellytykset on varmistettu

Liittyy strategiseen linjaukseen: 5

Vastuutaho: Puolustusministeriö, sisäministeriö

Puolustusvoimat kehittää ja ylläpitää kyberturvallisuusstrategian määrittelemällä tavalla kokonaisvaltaista kyberpuolustuksen suorituskykyä lakisääteisissä tehtävissään, joka sisältää myös vaikuttamisen kybertoimintaympäristössä. Puolustusministeriö yhdessä muiden relevanttien tahojen kanssa määrittelee vaikuttamiseen liittyvän prosessin. Prosessi sisältää mm. toimivaltuudet, muille viranomaisille annettavaan virka-apuun liittyvät käytännöt, hallinnonalojen yhteistoimintatavat, tiedonvaihdon eri viranomaisten välillä, johtovastuut sekä lainsäädännölliset edellytykset.

9) Valtiojohdon riittävästä ja oikea-aikaisesta tiedon saannista kansallista turvallisuutta vaarantavien uhkien torjumiseksi on huolehdittu

Liittyy strategiseen linjaukseen: 1,2,5,8

Vastuutaho: Sisäministeriö, puolustusministeriö, ulkoasiainministeriö

Digitalisoinnin aikaan saamiin muutoksiin vastaaminen edellyttää lainsäädännön tarkistamista niin, että kansallisesta turvallisuudesta vastaavat viranomaiset pystyvät hoitamaan lakisääteiset tehtävänsä riittävän tehokkaasti. Tällä hetkellä on valmisteilla hallituksen esitys siitä, että Suomeen luodaan uusi tiedustelulainsäädäntö. Lainsäädännön myötä pyritään vastaamaan aiempaa paremmin turvallisuusympäristön muutoksiin ja Suomea koskeviin uudenlaisiin uhkiin.

Puolustusministeriö ja sisäministeriö yhteistyössä oikeusministeriön kanssa jatkavat tiedustelua koskevien säädösehdotusten valmistelua valtioneuvoston linjausten mukaisesti.

10) Kyberrikostorjunnan edellytykset on varmistettu

Liittyy strategiseen linjaukseen: 4

Vastuutaho: Poliisi ja muut viranomaiset

Sisäministeriö huolehtii siitä, että poliisilla ja muilla viranomaisilla on hyvät edellytykset ennalta estää, paljastaa ja selvittää kyberrikollisuutta. Tietoverkkorikollisuuden tilannekuvaa ja tietojen vaihtoa kehitetään viranomaisten yhteisen tilannetietoisuuden parantamiseksi sekä yksityisen sektorin toimijoiden paremman varautumisen turvaamiseksi. Lisäksi poliisi kehittää digitaalisen todistusaineiston käsittelyä ja analysointia laatuohjelman avulla.

11) Tietosuojan lainsäädäntö on selkiytetty ja täydennetty sekä EU:n yleisen tietosuojalainsäädännön vaatimukset on toteutettu kansallisessa lainsäädännössä

Liittyy strategiseen linjaukseen:8

Vastuutaho: Oikeusministeriö, muut ministeriöt

Oikeusministeriö yhdessä muiden ministeriöiden kanssa toteuttavat EU:n yleisen tietosuojalainsäädännön vaatimukset kansalliseen lainsäädäntöön. Kukin organisaatio toteuttaa muutetun lainsäädännön vaatimukset toiminnassaan.

II Yhteiskunnan digitalisoidut elintärkeät toiminnot ovat turvatut

Suomen kyberturvallisuusselvityksessä 2017 todetaan: ”Suomalaisessa verkottuneessa tietoyhteiskunnassa on nykyistä paremmin tunnistettava elintärkeisiin toimintoihin vaikuttavat ja kriittisen infrastruktuurin kohteet sekä etenkin tunnistettava ne kriittiset palvelut ja toiminnot, joita tarvitaan itsessään ja ne tahot, jotka ovat riippuvaisia näiden kriittisten palveluiden ja toimintojen toiminnasta. Kriittisten kybertoimintaympäristön tahojen ja toimintojen tunnistamiseen yhdistyy myös harkinta niin sanotusta kyberomavaraisuudesta eli varmistaa kriittisten infrastruktuurien ylläpidon kannalta riittävä kansallisen omavaraisuuden aste. Lainsäädännön kehittäminen on yksi tärkeä osakokonaisuus valtiollisen kyberturvallisuuden kehittämisessä ja vahventamisessa.”

12) Yhteiskunnan elintärkeille toiminnoille välttämättömät julkisen hallinnon digitaaliset palvelut sekä niiden tarvitsema infrastruktuuri on tunnistettu ja hallinnassa

Liittyy strategiseen linjaukseen: 3,4,5,6,9

Vastuutaho: Valtiovarainministeriö, Valtion tieto ja viestintätekniikkakeskus, muut julkishallinnolle palveluita tuottavat palvelukeskukset ja yritykset

Valtiovarainministeriö selvittää mahdolliset julkisen hallinnon yhteisten uusien digitaalisten palveluiden ja niissä käytettävien teknologioiden tarvitsemat säädösmuutostarpeet. Valtiovarainministeriön johdolla Valtori toteuttaa elintärkeille toiminnoille välttämättömien ja kriittiseen infrastruktuuriin kuuluvien julkisen hallinnon digitaalisten palvelujen ja niiden keskinäisriippuvuuksien kuvaukset sisältävän hallintajärjestelmän. Tunnistetaan julkisen hallinnon ja elinkeinoelämän välisissä arvoketjuissa yhteistyötahot ja varmistetaan toiminnallisten prosessien turvallisuus. Tunnistetaan kriittiset palvelut ja rajapinnat, joista kriittiset palvelut ovat riippuvaisia.

Toteutetaan tutkimushankkeena yhteiskunnan elintärkeiden julkisen hallinnon toimintojen tarvitseman kriittisen infrastruktuurin ja kyberomavaraisuuden kuvaaminen osana kansallista kyberresilienssiä.

13) Maakunta ja sote-uudistuksessa toiminnallisten prosessien jatkuvuus sekä tieto- ja kyberturvallisuus on varmistettu

Liittyy strategiseen linjaukseen: 3,9

Vastuutaho: Sosiaali- ja terveysministeriö, valtiovarainministeriö, sisäministeriö, muut ministeriöt, maakunnat

Sosiaali- ja terveydenhuollon ja maakuntauudistuksen tuloksena maakunnat ja niiden liikelaitokset sekä palveluja tuottavat yritykset, yhteisöt, säätiöt ja laitokset muodostavat ekosysteemin, jonka toiminnan jatkuvuuden sekä tieto- ja kyberturvallisuuden turvaaminen on erittäin keskeistä maakuntien asiakkaille/kansalaisille.

Maakunnat, sekä jokainen ministeriö toimialallaan, vastaavat asukkaille järjestettävien palveluiden ja käyttämiensä ICT-palveluiden jatkuvuuden hallinnasta ja tieto- ja kyberturvallisuudesta. Tämä toteutetaan lainsäädännön mukaan sekä sosiaali- ja terveysministeriön, sisäministeriön ja valtiovarainministeriön ja muiden maakuntien tehtäviä ohjaavien ministeriöiden ohjauksen mukaisesti.

Lisäksi sosiaali- ja terveysministeriön hallinnonalalla suunnitellaan toteutettavaksi laaja selvitys kyberturvallisuuden nykytilasta ja tarvittavista jatkotoimenpiteistä vuodesta 2017 eteenpäin (sote-kyberhanke) sekä tuotetaan vuosien 2017–18 aikana valtakunnallinen sosiaali- ja terveydenhuollon varautumisen ja jatkuvuuden hallinnan ohjeistus.

14) Valtioneuvostolla on käytössä valmiuden ja varautumisen johtamiseen liittyvät tiedonsiirron ja -käsittelyn ratkaisut ja palvelut kaikissa turvallisuustilanteissa

Liittyy strategiseen linjaukseen: 2,3,4,5,6

Vastuutaho: Valtioneuvoston kanslia

Valtioneuvoston kanslia yhtenäistää ja toimeenpanee valtioneuvostolle valmiuden ja varautumisen johtamiseen liittyvät ratkaisut ja palvelut, joiden jatkuvuus on soveltuvin osin varmistettu kaikissa turvallisuustilanteissa. Ministeriöillä on käytössään valtioneuvoston verkossa toimiva yhteinen päätelaiteratkaisu, joka on käytettävissä myös häiriötilanteissa ja poikkeusoloissa. Korkean varautumisen ja tietoturvallisuuden suojaustasojen (STII-III) osalta käytetään erillisratkaisuja, kuten hallinnon turvallisuusverkon palveluita.

15) Kriittisten perusrekisterien ja tietovarantojen eheys, saatavuus ja luottamuksellisuus on hallittu kaikissa turvallisuustilanteissa

Liittyy strategiseen linjaukseen: 3

Vastuutaho: Valtiovarainministeriö, Väestörekisterikeskus, Maa- ja metsätalousministeriö, Maanmittauslaitos sekä Patentti- ja rekisterihallitus

Valtiovarainministeriö määrittää sekä yhdessä selvittää asiasta vastaavien organisaatioiden kanssa kriittisten tietovarantojen eheyden ja saatavuuden kaikissa turvallisuustilanteissa. Selvityksessä otetaan huomioon tietojen ja tarvittavan teknologian saatavuus sekä tiedon luottamuksellisuuden osalta edellytettävä tietojen salaus. Tavoitteena on, että keskeiset tietovarannot ovat eheinä saatavilla kaikissa turvallisuustilanteissa niitä tarvitseville organisaatioille tiedon luottamuksellisuuden edellyttämällä tavalla.

16) Sähköenergian toimitusvarmuuden riittävä taso ja yhteiskunnan kannalta keskeisten kohteiden sähkönjakelu on varmistettu

Liittyy strategiseen linjaukseen: 3

Vastuutaho: Työ- ja elinkeinoministeriö

Varmistetaan energia- ja ilmastostrategian mukaisesti sähköenergian toimitusvarmuuden riittävä taso valtakunnallisella tasolla. Määritetään yhteiset kriteerit sähkönjakelun asiakkaiden priorisoinnille häiriötilanteissa, huomioiden erityisesti ICT-järjestelmien kriittisyyden kasvu.

17) Huoltovarmuuskriittisten yritysten kyberturvallisuus on edistynyt

Liittyy strategiseen linjaukseen: 3

Vastuutaho: Huoltovarmuuskeskus

Huoltovarmuuskeskus johtaa ja resursoi huoltovarmuuskriittisen elinkeinoelämän tarpeisiin kohdennetun kyberturvallisuutta parantavan KYBER 2020 -ohjelman. Ohjelma liittää yhteen kaikki Huoltovarmuuskeskuksen toimenpiteet kyberturvallisuuden alueella. KYBER 2020 synnyttää pysyviä rakenteita, joiden puitteissa kyberturvallisuutta kehitetään ja tuetaan pitkällä aikavälillä. Ohjelma sitouttaa keskeisiä kyberturvallisuuden asiantuntijaorganisaatioita koordinoimaan ja osallistumaan ohjelman toteuttamiseen pitkällä aikavälillä. Huoltovarmuuskeskus osoittaa ohjelman käynnistämiseen ja ensimmäisiin rahoitettaviin kehityshankkeisiin noin 20 M€ ja 10 htv vuosina 2016 – 2020 sisältäen jo nyt Viestintäviraston Kyberturvallisuuskeskukselle varatut resurssit.

Lisäksi osana ohjelmaa Huoltovarmuuskeskus tukee hanketta, jonka myötä luodaan sanastotyön menetelmin kyberturvallisuussanasto. Hankkeen tavoitteena on selvittää keskeisten tieto- ja kyberturvallisuuteen liittyvien käsitteiden sisällöt, koota niistä sanasto ja antaa tarvittavat suositukset termistöstä.

Yritysten kyberturvallisuutta tukevien muiden toimenpiteiden ja viranomaisten kyberturvallisuuden kehittämisen yhteensovittamiseen sekä energia-alan kyberturvallisuuteen tulee ohjelmassa kiinnittää erityistä huomiota. Huoltovarmuuskeskus myös raportoi ohjelman tavoitteista, toimenpiteistä ja tuloksista osana tämän toimeenpano-ohjelman vuosittaista raportointia ja seurantaa.

18) Vaalien toteuttamisen tieto- ja kyberturvallisuus on selvitetty

Liittyy strategiseen linjaukseen: 8,9

Vastuutaho: Oikeusministeriö

Sipilän hallituksen linjausten mukaisesti Suomessa siirrytään sähköiseen äänestykseen perinteisen äänestyksen rinnalla kaikissa vaaleissa. Oikeusministeriö teettää selvityksen nettiäänestyksen käyttöönotosta yleisissä vaaleissa ja asettaa työryhmän, joka valmistelee selvityksen nettiäänestyksen toteuttamisesta. Selvityksessä arvioidaan nettiäänestyksen käyttöönottoa, teknisiä toteuttamisvaihtoehtoja, kustannuksia ja vaikutuksia vaalijärjestelmään ja se pyritään saamaan valmiiksi vuoden 2017 aikana. Selvityksessä on kiinnitettävä erityistä huomiota tieto- ja kyberturvallisuuden toteutumiseen vaaleissa.

19) Verottamiseen ja talousarvioesitysten valmisteluun sekä valtion maksuvalmiuden hallintaan ja maksuliikenteeseen liittyvien järjestelmien ja prosessien varautumista ja häiriöiden hallintaa on parannettu

Liittyy strategiseen linjaukseen: 2,3,9

Vastuutaho: Valtiovarainministeriö

Verotuksessa sekä julkisen talouden suunnitelman/kehysten ja valtion talousarvioesitysten valmistelussa tarvittavien digitaalisten prosessien ja niitä tukevien ICT-järjestelmien (Buketti) jatkuvuus sekä prosesseissa tarvittavien tietojen saatavuus on turvattu kaikissa turvallisuustilanteissa ja kaikissa työskentelytiloissa. Valtion maksuvalmiuden hallintaan ja maksuliikenteeseen liittyen vahvistetaan yhteistyötä ja varautumisen ohjausta sekä vahvistetaan edellytyksiä häiriötilanteiden tehokkaalle hallinnalle.

a) Valtion rahoitus- ja maksuliiketoimintojen prosessien ja järjestelmien havainnointi- ja torjuntakykyä kyberhyökkäyksiä ja -rikoksia vastaan on parannettu

Liittyy strategiseen linjaukseen: 2,3,9

Vastuutaho: Valtiovarainministeriö, sisäministeriö, Valtiokonttori, Palkeet

Valtiokonttori toteuttaa esiselvityksen (2016–2017) valtion rahoitus- ja maksuliiketoimintojen kybersietokyvyn kehittämisestä. Tämän perustella valmistellaan tarkempi esitys v 2017 tarvittavien hallinnollisten ja teknisten osa-alueiden kehittämisestä eri toimijoiden ja prosessien osalta.

b) Verotuksessa tarvittavien sähköisten prosessien ja niitä tukevien ICT-järjestelmien varautumisen kyvykkyyttä on aktiivisesti kehitetty

Liittyy strategiseen linjaukseen: 2,3,9

Vastuutaho: Valtiovarainministeriö, Vero

Vero suunnittelee ja toteuttaa sähköisten prosessien ja niitä tukevien ICT-järjestelmien varautumisen kyvykkyyden kehittämisen.

20) Kansallinen kevyt kyberturvallisuusarviointi, jonka avulla organisaatiot voivat huolehtia minimitason saavuttamisesta turvallisuuden osalta, on laadittu

Liittyy strategiseen linjaukseen: 7,9

Vastuutaho: Jyväskylän ammattikorkeakoulu

Jyväskylän ammattikorkeakoulun Cyber Scheme Finland - pilottihankkeessa rakentama ja pilotoima FINCSC (Finnish Cyber Security Certificate) -toimintamalli on tarkoitettu erityisesti pk-yritysten kyberturvallisuuden arviointia, akkreditointia ja siihen perustuvaa kehittämistä varten. Toimintamallin käyttöönottoa edistetään ja tuetaan kansallisin toimenpitein.

III Kansalaisten, elinkeinoelämän ja hallinnon kyberosaaminen edistää digitalisaation kehitystä

Suomen kyberturvallisuusselvityksessä 2017 todetaan: ” Kyberturvallisuus on digitalisaation mahdollistaja. Suomella on vahva kansainvälinen luottamuspääoma ja tätä luottamusta sekä suomalaista kyberturvallisuuden osaamista on oleellista pystyä hyödyntämään. Suomi ei voi olla edelläkävijä kyberturvallisuudessa ilman uskottavaa alan yksityisen sektorin liiketoimintaa. Kyberturvallisuusstrategian vision saavuttaminen edellyttää merkittävää lisäpanostusta resurssien osalta esimerkiksi Kyberturvallisuuskeskuksen toiminnan vahvistamiseksi.”

21) Tietoturvallinen kasvuympäristö digitaaliselle liiketoiminnalle on luotu

Liittyy strategiseen linjaukseen 1,2,3,4,6,7,8,9

Vastuutaho: Liikenne- ja viestintäministeriö sekä muut ministeriöt

Toimeenpannaan 2015 hallitusohjelman toimeenpanosuunnitelman osana liikenne- ja viestintäministeriön hyväksymä luottamusta internetiin sekä digitaalisiin palveluihin lisäävä tietoturvastrategia.

Strategia painottuu kilpailukyvyn ja vientiedellytysten varmistamiseen, EU:n digitaalisten sisämarkkinoiden kehittämiseen, yksityisyyden suojan ja muiden perusoikeuksien vahvistamiseen sekä kannustamista innovointiin. Strategia tähtää muutokseen, jonka tuloksena tietoturva on sisäänrakennettu erilaisiin järjestelmiin, päätelaitteisiin ja palveluihin. Strategia myös edellyttää, että viranomaiset auttavat yhteisöjä ja kansalaisia tietoturvan parantamisessa.

Osana tietoturvastrategian täytäntöönpanoa huolehditaan mm. seuraavista toimenpiteistä:

- Verkko- ja tietoturvadirektiivin kansallinen voimaansaattaminen. Liikenne- ja viestintäministeriö on koonnut työryhmän arvioimaan nykyisen sääntelyn riittävyyttä sekä mahdollisia säädöstarpeita kullakin verkko- ja tietoturvadirektiivin soveltamisalaan kuuluvalla toimialalla.
- Viestintäviraston Kyberturvallisuuskeskuksen tietoturvatoiminnan kehittäminen: Ylläpidetään tietoturvallisuuden tilannekuvaa Viestintäviraston, yritysten ja muiden yhteisöjen luottamukseen perustuvan tiedonvaihdon avulla.

22) Koulutus- ja harjoitustoiminta on suunniteltu ja toteutettu

Suomen kyberturvallisuusselvityksessä 2017 todetaan: ”Yleinen tietous ja osaaminen kyber- ja tietoturvallisuuden perusasioista on arvioitava peruskansalaistaidoksi tämän päivän suomalaisessa digitalisoituneessa tietoyhteiskunnassa. Yleinen tietous kyberturvallisuuden perusasioista ja näiden omaksuminen käyttäytymiseen kaipaa Suomessa aktiivista kehittämistä. Osaajien kouluttaminen edellyttää hajanaisen koulutuksen ja tutkimuksen nykyistä parempaa koordinaatiota oppilaitosten välillä sekä tutkimustoiminnan monipuolistamista.”

a) Julkisen hallinnon tieto- ja kyberturvallisuushenkilöstön osaamista on parannettu

Liittyy strategiseen linjaukseen: 7

Vastuutaho: Turvallisuuskomitean sihteeristö, valtiovarainministeriö

Turvallisuuskomitean sihteeristö seuraa kyberturvallisuusharjoitusten vaikuttavuutta vuosittain tehtävän toimeenpano-ohjelman arvioinnin yhteydessä.

Valtiovarainministeriö osana VAHTI-toimintaa suunnittelee ja toteuttaa julkisen hallinnon henkilöstön osaamisen kehittämisen hankkeita ja palveluita tieto- ja kyberturvallisuuden alueella. Valtiovarainministeriö määrittelee yhteistoiminnassa muiden viranomaisten kanssa kryptologian alueella tarvittavan omavaraisuuden.

b) Kansalaisten tieto- ja kyberturvallisuusosaaminen on edistynyt

Liittyy strategiseen linjaukseen: 7

Vastuutaho: Maanpuolustuskoulutusyhdistys, Vanhustyön keskusliitto ry

Maanpuolustuskoulutusyhdistys toteuttaa vuosittain kyberturvallisuuskoulutusohjelman, joka koostuu kaikille kansalaisille avoimista peruskursseista, sekä ammattilaisille suunnatuista jatko- ja erikoiskursseista.

Vanhustyön keskusliitto on luonut valtakunnallisen ikääntyneille ihmisille tarkoitetun vertaisoppimiseen perustuvan toimintamallin ja levittää sitä tarvitsevien ulottuville. Tässä mallissa ylläpidetään ja valtakunnallisesti levitetään ikääntyneille ihmisille tarkoitettuja yleisiä tietotekniikan oppimisen keinoja. Yksi sisällöistä käsittelee tietoturva- ja kyberasioita, jotta ikääntyneiden ihmisten tietoverkoissa tapahtuvat toiminnot (etähoito, apteekki, pankki yms. asiat) voitaisiin toteuttaa turvallisesti ja että sähköisen asioinnin käyttö ja kiinnostavuus sekä tietous niihin liittyvistä riskeistä lisääntyisivät ikääntyneiden ihmisten kohdalla.

c) Kansallinen tieto- ja kyberturvallisuusviikko on toteutettu vuosittain

Liittyy strategiseen linjaukseen: 6,7

Vastuutaho: Elinkeinoelämän keskusliitto, Valtiovarainministeriö, Turvallisuuskomitean sihteeristö

Elinkeinoelämän keskusliitto yhdessä valtiovarainministeriön, yritysten sekä Turvallisuuskomitean sihteeristön kanssa toteuttaa tieto- ja kyberturvallisuusviikon vuosittain lokakuussa osana Euroopan Unionin kyberturvallisuuskuukautta (ECSM). Viikon aikana tietoiskuin ja tilaisuuksin viestitään tieto- ja kyberturvallisuustietoutta kansalaisille, yrityksille ja hallinnolle. Viikko huipentuu kansalliseen tieto- ja kyberturvallisuuspäivään.

d) Kyberturvallisuuden ja digitaalisen toimintaympäristön perustaidot – yleissivistävä ja ammatillinen koulutus on edistynyt

Liittyy strategiseen linjaukseen: 7

Vastuutaho: Opetus- ja kulttuuriministeriö, Opetushallitus

Opettajien täydennyskoulutuksessa kehitetään ja edistetään osana monilukutaitoa tieto- ja kyberturvallisuuteen liittyviä sisältöjä. Opetushallitus lisämateriaalia tuottamalla edistää monilukutaitoa sekä tieto- ja kyberturvallisuuden perustaitoja.

e) Kyberturvallisuuden tutkimusyhteistyötä on tiivistetty viranomaisten ja tutkimusorganisaatioiden sekä elinkeinoelämän kesken.

Liittyy strategiseen linjaukseen: 1,7

Vastuutaho: Turvallisuuskomitean sihteeristö

Suomen kyberturvallisuusselvityksessä 2017 todetaan, että jatkotutkimusta tarvitaan ainakin seuraavista aiheista: kyberturvallisuuden strateginen johtaminen Suomessa (toimenpide 1,2), kybertilannekuvan ja analysointikyvykkyyden kehittäminen (toimenpide 3) sekä yhteiskunnan elintärkeiden toimintojen, kriittisen infrastruktuurin ja kyberomavaraisuuden määrittely osana kansallista kyberresilienssiä (toimenpide 12).

Kyberturvallisuuden tutkimuksen osalta on tarve tilannekuvalle ja koordinaatiolle. Turvallisuuskomitean sihteeristö rakentaa yhdessä muiden tahojen kanssa tutkimustoiminnan yhteistyömallin.

Toimeenpano-ohjelman valmistelutyöryhmä:
Nadja Nevaste, Rauli Paananen, Pentti Olin, Tuija Kuusisto ja Kimmo Rousku.

www.turvallisuuskomitea.fi