Suomen kyberturvallisuusstrategian toimeenpano-ohjelma vuosille 2017–2020

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

Sisällys

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

Kyberturvallisuusstrategian toimeenpano-ohjelma vuosille 2017–2020

Johdanto

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

Kyberturvallisuusstrategian julkaisun jälkeen kyberturvallisuuden toimintaympäristö on muuttunut uusien uhkien myötä. Helmikuussa 2017 julkaistun valtioneuvoston selvityksen ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” 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.

Samaan aikaan digitalisaatio tuo mukanaan sen kaltaisia mahdollisuuksia julkishallinnolle ja elinkeinoelämälle, että niitä ei yksinkertaisesti voi jättää käyttämättä hyväksi. On siis pyrittävä jollain tavalla yhdistämään sekä internetin ja ylipäätään digitalisaation tarjoamat mahdollisuudet että toisaalta varautuminen digitalisaation mukanaan tuomiin erilaisiin uhkiin.

Suomen kyberturvallisuuden vision saavuttamisen ja kyberturvallisuuden tilan mittaamisen lisäksi on yhteiskunnassa käyty keskustelua myös kyberturvallisuuden johtamismallista. Hallinnonalojen, elinkeinoelämän, akatemian ja järjestöjen antamien arvioiden perusteella, Turvallisuuskomitean sihteeristö laati arvion kyberturvallisuusstrategian toimeenpano-ohjelman toteutumisesta. Arvion perusteella Turvallisuuskomitea päätti 14.3.2016 päivittää Suomen Kyberturvallisuusstrategian toimeenpano-ohjelman sekä luoda toimeenpano-ohjelmaan liittyvän kansallisen tahtotilan, joka osoitetaan johtajuudella ja resurssien uudelleen kohdentamisella.

Vuonna 2014 hyväksytty toimeenpano-ohjelma koostui yhteensä 74 toimenpiteestä, jotka jakaantuivat ministeriöiden ja osin yksittäisten toimijoiden toteutusvastuulle. Vuoden 2016 alussa laaditun arvion perusteella 11 toimenpiteen todettiin valmistuneen ja seuraavilla toimenpiteillä tunnistettiin olleen merkittäviä vaikutuksia:

- Hallinnon turvallisuusverkko (TUVE) -hanke ja toimialariippumattomien ICT-tehtävien kehittäminen,

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

- Kyberturvallisuuskeskuksen perustaminen Viestintävirastoon ja siihen liittyvän CERT-toiminnan kehittäminen,
- Maanpuolustuskoulutusyhdistyksen kyberturvallisuuskurssit,
- Valtion ympärivuorokautisen tietoturvatoiminnan kehittämishanke (SecICT) ja siihen liittyvä havainnointikyvyn parantaminen sekä
- Jyväskylä Security Technology:n (JYVSECTEC) turvallisuusteknologian kehittämishanke.

Digitalisoitumisen ja siinä tarvittavan muutoksen johtamisen, tiedolla johtamisen, keinoälyn, robotiikan 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 yhdellä yhdeksästä digitalisoinnin periaatteesta – ” Rakennamme helppokäyttöisiä ja turvallisia palveluita.” 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. Tämä 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, siirtyvät yhä enemmän verkkoon. Tämä muutos edellyttää myös kybertoimintaympäristöön ulottuvia viranomaisvaltuuksia. Tietoverkoissa tapahtuva toiminta ei ole paikkaan tai aikaan sidottua samalla tapaa kuin reaalimaailmassa tapahtuva toiminta ja lisäksi sen piirteisiin kuuluu kiistettävyys ja tiedon muuntaminen sekä -muuntuminen. Uuden tilanteen myötä on Suomessakin aloitettu Sisäasiainministeriön ja Puolustusministeriön toimialoilla tiedustelulainsäädännön valmistelut.

Toimeenpano-ohjelma 2017–2020 on muodostettu valmistelun aikana kerättyjen toimenpide-ehdotusten perusteella. Toimenpide-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

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

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 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-ohjelman päivittämistä on valmisteltu työryhmässä, jonka puheenjohtajana on toiminut erikoistutkija Pentti Olin Turvallisuuskomitean sihteeristöstä ja jäseninä erityisasiantuntija Tuija Kuusisto ja erityisasiantuntija Kimmo Rousku valtiovarainministeriöstä, apulaisjohtaja Rauli Paananen Viestintävirastosta sekä asiantuntija Nadja Nevaste Turvallisuuskomitean sihteeristöstä.

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

Toimeenpano-ohjelman 2017–2020 sisältö

Suomen Kyberturvallisuusstrategiassa on määritelty kyberturvallisuuden visio sekä kymmenen strategista linjausta, joiden mukaisesti kansallista kyberturvallisuutta kehitetään. Visiona on, että:

- 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 asetettu tavoite muutetaan pysyväksi: Tavoite on se että Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa.

Saatavilla olevien kansainvälisten vertailujen ja arvioiden perusteella, kuten ITU 2014, Suomi sijoittuu sijalle 23 tarkasteltaessa 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.

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

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:

1) Johtaminen varmistaa kyberturvallisuuden vision saavuttamisen

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 elintärkeät digitalisoidut 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?

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

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	Yhteiskunnan kriisijohtamismalli on päivitetty kybertoimintaympäristön häiriötilanteisiin	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 perustetaan vastaamaan toimeenpano-ohjelman vuosittaisesta tarkastelusta ja ajantasaisuuden arvioinnista	x	x				x			x	x
7	Toimeenpano-ohjelman seurantamittaristo on laadittu									x	x
8	Kybertoimintaympäristössä tapahtuvan vaikuttamisen edellytykset varmistetaan					x					
9	Valtiojohdon riittävästä ja oikea-aikaisesta tiedon saannista kansallista turvallisuutta vaarantavien uhkien torjumiseksi on huolehdittu	x	x			x			x		
10	Kyberrikostorjunnan edellytykset varmistetaan				x						
11	Tietoturvallisuuden sekä tietosuojan lainsäädäntö on selkiytetty ja täydennetty sekä EU:n tietosuojalainsäädännön vaatimukset on toteutettu kansallisessa lainsäädännössä								x		
12	Yhteiskunnan elintärkeille toiminnoille välttämättömien julkisen hallinnon ICT-palvelujen yhteinen hallintaprosessi ja -järjestelmä on laadittu ja toiminnassa			x	x	x	x			x	
13	Maakunta ja sote-uudistuksessa toiminnallisten prosessien jatkuvuus sekä tieto- ja kyberturvallisuus on varmistettu			x						x	
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 riittävän tason varmistaminen ja yhteiskunnan kannalta keskeisten kohteiden sähkönjakelun varmistaminen			x							
17	Huoltovarmuuskriittisten yritysten kyberturvallisuus on edistynyt			x							
18	Sähköisen äänestyksen käyttöönotto								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	Luodaan tietoturvallinen kasvuympäristö digitaaliselle liiketoiminnalle.	x	x	x	x		x	x	x	x	
22	Koulutustoiminta on suunniteltu ja toteutettu	x	x				x	x			
23	Julkisen hallinnon kansalliset kyberturvallisuusharjoitukset on toteutettu 2017–2020 sekä harjoitusten opit on viety käytäntöön	x		x	x	x		x		x	

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

I Johtamisella varmistetaan kyberturvallisuuden vision saavuttaminen

1. Yhteiskunnan kriisijohtamismalli on päivitetty kybertoimintaympäristön häiriötilanteisiin

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

Vastuutaho: Turvallisuuskomitean sihteeristö sekä muut tarvittavat toimijat

Turvallisuuskomitea yhteensovittaa kriisinjohtamismallin päivittämisen kybertoimintaympäristön häiriötilanteisiin. Valtioneuvoston kanslian TEAS-tutkimushankkeen ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” – tuloksia hyödynnetään tässä työssä.

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, valtion tieto- ja viestintäkeskus Valtori

Valtiovarainministeriön johdolla Valtori yhdessä muiden toimijoiden kanssa toteuttaa edelleen kehitetyn poikkihallinnollisen kyberhäiriötilanteiden operatiivisen hallintamallin, joka sisältää kuvauksen tietovirroista ja toimintaprosesseista julkisen hallinnon ja elinkeinoelämän välillä merkittävissä julkisen hallinnon kyberhäiriö-, ja tietoturvapoikkeamatilanteissa.

Valtiovarainministeriö varmistaa, että ministeriöt, hallinnonalat ja palvelukeskukset sekä maakunta- ja kuntatoimijat ja niiden omistamat yritykset ilmoittavat Viestintävirastolle kaikista 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

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

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 perustetaan vastaamaan toimeenpano-ohjelman vuosittaisesta tarkastelusta ja ajantasaisuuden arvioinnista

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

Vastuutaho: Turvallisuuskomitean sihteeristö

Suomen kyberturvallisuusfoorumi perustetaan tämän toimeenpano-ohjelman etenemisen seurannan tueksi sekä ajantasaisuuden arvioimiseksi ja päivittämiseksi, kyberturvallisuuden ilmiöiden seuraamista sekä yhteistyön ja tiedonvälityksen parantamista varten tiede- ja tutkimusmaailman, hallinnon, yritysten ja järjestöjen kesken. Foorumin tilaisuuksiin kutsutaan Turvallisuuskomitean jäsenten lisäksi kyberturvallisuuden alan professoreita, toimitusjohtajia ja järjestöjen johtajia. Kyberturvallisuusfoorumi osallistuu toimeenpano-ohjelman vuosittaiseen välitarkasteluun ja tarpeen mukaan toimenpiteiden päivittämiseen. Foorumille esitellään toimeenpano-ohjelman edistyminen ja Suomen kyberturvallisuuden tilanne arviointiin laaditun kypsyysmallin ja mittariston avulla. Foorumissa muodostetaan näkemys toimeenpano-ohjelman päivitystarpeista akatemian, hallinnon, yritysten ja järjestöjen ajankohtaiskatsausten perusteella sekä vahvistetaan päivitetty toimeenpano-ohjelma.

7. Toimeenpano-ohjelman seurantamittaristo on laadittu

Liittyy strategiseen linjaukseen: 9,10

Vastuutaho: Turvallisuuskomitean sihteeristö ja valtiovarainministeriö

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

Turvallisuuskomitean sihteeristön ja valtiovarainministeriön johdolla laaditaan Suomen Kyberturvallisuusstrategian ja tämän toimeenpano-ohjelman tavoitteiden seurantaa varten käytettävä kypsyysmalli ja mittaristo. Kypsyysmallin ja mittariston avulla toteutetaan vuosittainen raportointi toimeenpano-ohjelman tilanteesta Turvallisuuskomitealle, valtioneuvostolle, Kyberturvallisuusfoorumille sekä muille sidosryhmille.

8. Kybertoimintaympäristössä tapahtuvan vaikuttamisen edellytykset varmistetaan

Liittyy strategiseen linjaukseen: 5

Vastuutaho: puolustusministeriö, sisäministeriö

Puolustusvoimat kehittää ja ylläpitää kyberturvallisuusstrategian määrittelemällä tavalla kokonaisvaltaista kyberpuolustuksen suorituskykyä, 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.

Puolustusministeriö, yhdessä sisäministeriön ja oikeusministeriön kanssa, jatkaa sotilastiedustelua koskevien säädösehdotusten valmistelua valtioneuvoston linjausten mukaisesti.

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

Digitalisoinnin aikaan saamiin muutoksiin vastaaminen edellyttää lainsäädännön tarkistamista niin, että kansallisesta turvallisuudesta vastaavat viranomaiset pystyvät hoitamaan lakisääteiset tehtävänsä riittävän tehokkaasti. Hallitus esittää, että Suomeen luodaan uusi tiedustelulainsäädäntö. Lainsäädännön myötä halutaan kyetä vastaamaan aiempaa paremmin turvallisuusympäristön muutoksiin ja Suomea koskeviin uudenlaisiin uhkiin.

10. Kyberrikostorjunnan edellytykset varmistetaan

Liittyy strategiseen linjaukseen: 4

Vastuutaho: Sisäministeriö

Sisäministeriö huolehtii siitä, että poliisilla 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 sisäministeriö kehittää digitaalisen todistusaineiston käsittelyä ja analysointia laatuohjelman avulla.

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

11. Tietoturvallisuuden sekä tietosuojan lainsäädäntö on selkiytetty ja täydennetty sekä EU:n tietosuojalainsäädännön vaatimukset on toteutettu kansallisessa lainsäädännössä

Liittyy strategiseen linjaukseen:8

Vastuutaho: Oikeusministeriö, muut ministeriöt

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

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

II Yhteiskunnan digitalisoidut elintärkeät toiminnot ovat turvatut

12. Yhteiskunnan elintärkeille toiminnoille välttämättömien julkisen hallinnon ICT-palvelujen yhteinen hallintaprosessi ja -järjestelmä on laadittu ja toiminnassa

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

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

Valtiovarainministeriön johdolla Valtori luo ja toteuttaa elintärkeille toiminnoille välttämättömien ja kriittiseen infrastruktuuriin kuuluvien julkisen hallinnon ICT-järjestelmien yhteisen hallintaprosessin ja -järjestelmän. Tunnistetaan julkisen hallinnon ja elinkeinoelämän välisissä arvoketjuissa yhteistyötahot ja varmistetaan toiminnallisten prosessien turvallisuus. Tunnistetaan kriittiset palvelut, joita itse tarvitaan ja ne tahot jotka käyttävät tai ovat muuten riippuvaisia näiden kriittisten palveluiden toiminnasta. Tunnistetaan kybertoimintaympäristön kriittiset pisteet joiden osalta hallinta on oltava valtiollisilla toimijoilla.

Yhteiskunnalle elintärkeät toiminnot on määritelty Yhteiskunnan turvallisuusstrategiassa 2010 ja kriittinen infrastruktuuri Huoltovarmuuspäätöksessä 2013.

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, 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 vastaavat asukkaille järjestettävien palveluiden ja käyttämiensä ICT-palveluiden jatkuvuuden hallinnasta sekä tieto- ja kyberturvallisuudesta sosiaali- ja terveysministeriön, sisäministeriön sekä 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

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

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 ja saatavuus on hallittu kaikissa turvallisuustilanteissa

Liittyy strategiseen linjaukseen: 3

Vastuutaho: Valtiovarainministeriö, Väestörekisterikeskus, Maanmittauslaitos, muut organisaatiot

Valtiovarainministeriö määrittää sekä yhdessä asiasta vastaavan organisaation kanssa selvittää kriittisten tietovarantojen eheyden ja saatavuuden kaikissa turvallisuustilanteissa. Selvityksessä huomioidaan tietojen ja tarvittavan teknologian saatavuus sekä erityisesti tietojen salaus. Tavoitteena on, että keskeiset tietovarannot ovat eheinä saatavilla kaikissa turvallisuustilanteissa niitä tarvitseville organisaatioille tiedon luottamuksellisuuden edellyttämällä tavalla.

16. Sähköenergian toimitusvarmuuden riittävän tason varmistaminen ja yhteiskunnan kannalta keskeisten kohteiden sähkönjakelun varmistaminen

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.

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. Sähköisen äänestyksen käyttöönotto

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.

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

Valtiokonttorin 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 kehitetään aktiivisesti

Liittyy strategiseen linjaukseen: 2,3,9

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

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 - pilottihanke rakentaa ja pilotoi kansallisen toimintamallin/ konseptin erityisesti pk-yritysten kyberturvallisuuden arviointia, akkreditointia ja siihen perustuvaa kehittämistä varten.

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

III Kansalaisten, elinkeinoelämän ja hallinnon kyberosaaminen edistää digitalisaation kehitystä

21. Luodaan tietoturvallinen kasvuympäristö digitaaliselle liiketoiminnalle

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 julkaisema luottamusta internetiin sekä digitaalisiin palveluihin lisäävä tietoturvastrategia.

Strategia painottuu kilpailukyvyn ja vientiedellytysten varmistamiseen, EU:n digitaalisten sisämarkkinoiden kehittämiseen sekä yksityisyyden suojan ja muiden perusoikeuksien vahvistamiseen. 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 kokoaa työryhmän arvioimaan nykyisen sääntelyn riittävyys kullakin verkko- ja tietoturvadirektiivin soveltamisalaan kuuluvalla toimialalla.
- Viestintäviraston Kyberturvallisuuskeskuksen CERT-toiminnan kehittäminen: Ylläpidetään tietoturvallisuuden tilannekuvaa Viestintäviraston, yritysten ja muiden yhteisöjen luottamukseen perustuvan tiedonvaihdon avulla.

22. Koulutustoiminta on suunniteltu ja toteutettu

a) Julkisen hallinnon tieto- ja kyberturvallisuushenkilöstön osaamista on parannettu

Liittyy strategiseen linjaukseen: 7

Vastuutaho: Valtiovarainministeriö

Valtiovarainministeriö osana VAHTI-toimintaa suunnittelee ja toteuttaa julkisen hallinnon henkilöstön osaamisen kehittämisen hankkeita ja palveluita tieto- ja kyberturvallisuuden alueella.

b) Kansalaisten tieto- ja kyberturvallisuusosaaminen on edistynyt

Liittyy strategiseen linjaukseen: 7

Vastuutaho: Maanpuolustuskoulutusyhdistys, Turvallisuuskomitean sihteeristö

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi

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

c) Ikääntyneiden ihmisten tieto- ja kyberturvallisuusosaaminen on edistynyt

Liittyy strategiseen linjaukseen: 7

Vastuutaho: Vanhustyön keskusliitto ry

VTKL 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.

d) 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.

e) 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.

f) Yhteistyötä julkisen hallinnon sekä tieto- ja kyberturvallisuutta antavien tutkimus- ja koulutusorganisaatioiden sekä elinkeinoelämän kesken on tiivistetty

Liittyy strategiseen linjaukseen: 1,7

Vastuutaho: Turvallisuuskomitean sihteeristö

Kyberturvallisuuden tutkimuksessa on selkeä koordinaation tarve ja kattava tutkimuksen tilannekuva puuttuu. Turvallisuuskomitean sihteeristö rakentaa yhdessä muiden keskeisten tahojen kanssa toimintamallin kyberturvallisuustutkimukselle.

g) Haavoittuvuuksien etsimiseen kannustavan palkinto-ohjelman kehittäminen (bug bounty)

Liittyy strategiseen linjaukseen: 7

Vastuutaho: Valtiovarainministeriö

Valtiovarainministeriö osana VAHTI-toimintaa edistää julkisen hallinnon ICT-palveluiden tietoturvahaavoittuvuuksien etsimiseen tähtäävän palkinto-ohjelman kehittämistä ja sellaisen hyödyntämistä tukemaan perinteisiä tietoturvapalveluita ja -auditointeja.

23. Julkisen hallinnon kansalliset kyberturvallisuusharjoitukset on toteutettu 2017–2020 sekä harjoitusten opit on viety käytäntöön

Liittyy strategiseen linjaukseen: 1,3,4,5,7,9

Vastuutaho: Turvallisuuskomitean sihteeristö

Turvallisuuskomitean sihteeristö kokoaa eri tahojen harjoitustiedot yhteiseen avoimeen sovellukseen, jonka käyttökokemusten perusteella kehitetään toimintamalleja. Kyberturvallisuusharjoitusten opit viedään käytäntöön harjoituksiin osallistuvissa organisaatioissa. Harjoitusten vaikuttavuutta seurataan Turvallisuuskomitean sihteeristössä vuosittain tehtävän toimeenpano-ohjelman arvioinnin yhteydessä.

Postiosoite
Postadress
Postal Address
Turvallisuuskomitea
PL 31
FI-00131 Helsinki
Finland

Käyntiosoite
Besöksadress
Office
Eteläinen Makasiinikatu 8
00130 Helsinki
Finland

Puhelin
Telefon
Telephone
0295 16001
Internat. +358 295 16001

Faksi
Fax
Fax
(09) 160 88244
Internat. +358 9 160 88244

s-posti, internet
e-post, internet
e-mail, internet
tk@turvallisuuskomitea.fi
www.turvallisuuskomitea.fi